Defence Research and Development Canada | Recherche et développement pour la défense Canada

CAN UNCLASSIFIED

DRDC | RDDC
technologysciencetechnologie

Public Safety Grade Mobile Application Management Framework (PSG-MAMF)

Nesma Keshta
Yasser Morgan
University of Regina

Prepared by:
University of Regina
3737 Wascana Parkway
Regina, SK Canada S4S 0A2
PSPC Contract Number: W7714-166169/001/SV
Technical Authority: Daniel Charlebois and Joe Fournier, Defence Scientists
Contractor's date of publication: March 2018

Defence Research and Development Canada

Contract Report
DRDC-RDDC-2018-C203
October 2018

Canada

IMPORTANT INFORMATIVE STATEMENTS

This document was reviewed for Controlled Goods by Defence Research and Development Canada using the Schedule to the *Defence Production Act*.

Public Safety Grade Mobile Application Management Framework PSG-MAMF

A study of the public safety grade mobile application management and related security and policy concerns

Nesma Keshta, Research Associate
Dr. Yasser Morgan, Associate Professor and founder of BRiC initiative
University of Regina

Contractor's Document Number: CSSP-2015-CP-2103
PWGSC Contract Number: W7714-166169/001/SV

Contract Technical Authority: Daniel Charlebois and Joe Fournier, Defence Scientists

Contract Report
DRDC-RDDC-2015-[number]

IMPORTANT INFORMATIVE STATEMENT

Public Safety Grade Mobile Application Management Framework PSG-MAMF, Project #CSSP-2015-CP-2103, was supported by the Canadian Safety and Security Program which is led by Defence Research and Development Canada's Centre for Security Science (DRDC-CSS) in partnership with the government of Saskatchewan and the University of Regina.

Canadian Safety and Security Program is a federally funded program to strengthen Canada's ability to anticipate, prevent, mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime and terrorism through the convergence of science and technology with policy, operations and intelligence.

Related Studies

CSSP Project 2015-TI-2186 – "Emerging Wireless Technologies in Support of Public Safety Project" covers a wide variety of wireless technologies related to public safety and security. Some parts of this project is directly related to the Canadian Public Safety Broadband Network (PSBN) but the overall scope covers and assumes communication over many other wireless and wireless-related technologies.

Study Impact on CSSP Outcomes

The mobile applications development, distribution and maintenance system is well developed for the public marketplace. However, the community serving the safety, security and health of the Canadian public and its infrastructure, which includes law enforcement, firefighters, paramedics and emergency management ("Stakeholders") have a unique public service mission implying the need for different mobile applications from the general public. Furthermore, applications on a broadband public safety network have specific interoperability considerations not commonly encountered on commercial networks. The term "Public Safety Grade" is often used to convey the need for design choices that support a greater overall reliability and resiliency to service disruptions compared to commercial mobile services.

Research outcome presented in this document did not require any experimentation with animal or human subjects.

Communications

DRDC CSS reserves the right to disclose and/or use information from projects for which it provides funding. Additionally, the use and publication of information related to this project will require review by DRDC CSS to ensure proper acknowledgement of DRDC CSS/CSSP support/contribution. In order to achieve this, project participants will provide copies of any reports, articles, or publications to DRDC CSS at least 30 days, where possible, prior to any release, distribution or planned publication. No public announcements concerning this project will be made without providing advance notification to DRDC CSS. DRDC CSS must receive a copy of all reports generated under the project.

The above communications requirements apply to all parties related to this Study, including but not limited to CITIG, CATA, SIIG and the Government of Saskatchewan.

Abstract

This study covers in details the Public Safety Grade Mobile Application Management Framework, which is a system that includes a group of trusted components with integral security functions into a single framework, as well as extra security considerations, technologies, standards, and policies. PSG-MAMF is intended to provide semi-closed ecosystem components that can integrate effectively to provide the security functionalities required to address the threats and vulnerabilities of mobile devices, applications, and information in public safety environments. PSG-MAMF improves the security of mobile devices and applications use by the government and public safety, and provides safer ways to access information infrastructure while adhering to organizational policies. The study identifies approaches to monitor, detect, and sense potential attacks taking place from within or outside mobile applications. The study also provides comprehensive ways to identify and mitigate security risks by applying separation of data, applications, algorithms, and keys.

Compared to other advanced security solutions available for mobility management, PSG-MAMF provides a level of integration that is not available in other ecosystems provided by other research studies (e.g. NIST ecosystem) and other existing products supported by different vendors (e.g. Blackberry, AirWatch, etc.).

Significance for Defence and Security

This study provides both Industry and Stakeholders throughout Canada with an effective means of assessing the requirements for public safety grade mobile devices, public safety grade mobile applications, and requirements for secure access to remote information systems. The framework proposed throughout the study would ensure adopting of secure mobile devices, applications, and providing secure remote access to information while maintaining the security of critical infrastructure and emergency response services. The framework also grantee the security of information once it distributed to user's devices. The framework support such capabilities by providing secure environments for applications, and secure storage environments for information, credentials, encryption keys, and other sensitive information. This way, public sector can utilize trustworthy mobile technology, while reinforcing the security of critical infrastructure, healthcare data, and emergency response services

The study also provides the Industry and Stakeholders with a viable framework for the qualification (selection) and validation of PSBN applications with an emphasis on interoperability and application life cycle. The introduction of public safety grade applications has impact on the evolving Public Safety Broadband Network (PSBN). This study serves as a framework to de-risk PSBN evolution through the evidence-based assessment of application requirements, qualification, functional validation methodologies, distribution and use in addition to application life cycle perspective. Additionally, the bodies of work by entities such as NPSTC, APCO Canada, FirstNet, CIRTEC and CITIG will also be referenced.

Connected and Protected Practitioners: Public Safety and national security practitioners are supported by risk and capability gap based technology investments.

This study addresses stakeholder's interest in interoperable applications framework utilizing known requirements in a timely manner, allowing effective communicate and information sharing between stakeholders over PSBN infrastructure.

Résumé

Cette étude couvre en détail le cadre du Cadre de gestion des applications mobiles de niveau sécurité publique. Il définit des moyens sûrs d'accéder à l'infrastructure et à l'information tout en respectant les politiques organisationnelles. L'étude identifie également des approches pour surveiller, détecter et détecter les attaques potentielles qui se produisent à l'intérieur ou à l'extérieur des applications mobiles. L'étude fournit également des moyens complets d'identifier et de mesurer les risques de sécurité en appliquant la séparation des données, des applications, des algorithmes et des clés.

Importance pour la défense et la sécurité

Cette étude fournit à l'industrie et aux intervenants partout au Canada un moyen efficace d'évaluer les exigences pour les applications de qualité de sécurité publique qu'ils souhaitent développer ou acheter en fournissant un cadre viable pour la qualification (sélection) et la validation des applications PSBN en mettant l'accent sur l'interopérabilité et Cycle de vie de l'application.

L'introduction de demandes d'homologation de sécurité publique a des répercussions sur l'évolution du réseau Sécurité publique élargie (PSBN). Cette étude sert de cadre à la dévaluation de l'évolution de la PSBN grâce à l'évaluation fondée sur des données probantes des exigences d'application, de la qualification, des méthodologies de validation fonctionnelle, de la distribution et de l'utilisation en plus du cycle de vie des applications. De plus, les organes de travail des entités telles que NPSTC, APCO Canada, FirstNet, CIRTEC et CITIG seront également référencés.

Praticiens connectés et protégés: Les professionnels de la sécurité publique et de la sécurité nationale sont appuyés par des investissements technologiques basés sur le risque et l'insuffisance de capacités.

Cette étude porte sur les intérêts des parties prenantes dans le cadre des applications interopérables en utilisant les exigences connues en temps opportun, permettant une communication efficace et le partage d'informations entre les parties intéressées par rapport à l'infrastructure PSBN.

Table of contents

Related Studies ... ii
Study Impact on CSSP Outcomes ... ii
Communications ... ii
Abstract ….. ... i
Significance for Defence and Security ... i
Résumé…. ... iii
Importance pour la défense et la sécurité ... iii
Table of contents ... iv
List of figures ... x
List of tables ... xii
Acknowledgements ... xiii
1 Introduction ... 1
1.1 Purpose and Scope ... 1
1.2 Public Safety Grade ... 2
1.3 Document Structure: ... 3
2 Summary of Related Work ... 5
2.1 Mobile Devices Security Best Practices ... 6
2.1.1 Guidelines on Hardware-Rooted Security in Mobile Devices ... 7
2.1.2 Guidelines for Managing the Security of Mobile Devices in the Enterprise ... 7
2.1.3 Guidelines on Mobile Device Forensics ... 8
2.2 Authentication and Identity Management Practices ... 9
2.2.1 Electronic Authentication Guideline ... 9
2.2.2 Mobile, PIV, and Authentications ... 10
2.2.3 Electronic Credential and Authentication Standard ... 10
2.2.4 The Global Federated Identity and Privilege Management (GFIPM) initiative ... 11
2.2.5 National Information Exchange Model (NIEM) ... 11
2.2.6 Federal Identity, Credential, and Access Management (FICAM) ... 12
2.3 Mobile Applications Security Best Practices ... 14
2.3.1 Vetting the Security of Mobile Applications ... 14
2.3.2 An Overview of Mobile Application Vetting Services for Public Safety ... 14

2.3.3 Adoption of Commercial Mobile Applications within agencies of U.S. Federal Government 15
2.3.4 Open Web Application Security Project (OWASP) – Mobile Security Project 17
2.3.4.1 Mobile App Security Requirements and Verification document: 17
2.3.4.2 Mobile Security Testing Guide (MSTG) 18
2.3.4.3 Mobile App Security Checklist 18
2.3.5 Mobile application Security Testing Initiative 18
2.4 Preliminary Study on Systems and efforts Closer to PSG-MAMF 18
2.4.1 Mobile Computing Decision Framework (MCDF) 19
2.4.2 Mobile Security Reference Architecture (MSRA) 20
2.4.3 Federal Mobile Computing Security Baseline 24
2.4.4 The Definitive Guide To Enterprise Mobile Security 24
2.4.5 Enterprise Mobility Management (EMM) Suites – (Different Vendors) 25
2.4.6 Practice Guide – Mobile Device Security 26
2.4.7 Mobile Device Security for Enterprises (MDSE) project 27
2.5 Summary of security threats and identified Gaps 27
3 Definitions, Assumptions, and Basics Principals of PSG-MAMF 31
3.1 PSG-MAMF assumptions 31
3.2 PSG-MAMF principals 31
3.2.1 Public Safety Broadband Network (PSBN): 32
3.2.2 Opportunistic RAN Connectivity 32
3.2.3 Interoperability 32
3.2.4 Multi fencing Tenet: 33
3.2.5 Mobility Management Frameworks 33
3.2.6 Containerization Approach 33
3.2.7 Root of Trust 34
3.2.8 Semi-closed Ecosystem 35
3.2.8.1 Public Safety Grade-Application Store (PSG-AS) 35
3.2.8.2 Application vetting 35
3.2.8.3 Management and Monitoring of Applications 35
3.2.8.4 Applications sharing and access management 35
3.2.9 Federation of identity and authentication management 35

3.2.10 Access Right Management (ARM) 36
3.2.11 Court Admissible Logging and Record Keeping 36
4 PSG-MAMF Architectural Components 39
4.1 Application Developer 40
4.2 User 40
4.3 Information Provider 41
4.4 Framework Management and Administration 42
4.4.1 Compliance Management and Administration: 42
4.4.2 Application Management and Administration 43
4.4.3 Information Management and Administration 44
4.5 Public Safety Grade – Mobile Device (PSG-MD) 45
4.6 Identity and Authentication Management Framework 46
4.7 Public Safety Grade - Information Infrastructure (PSG-II) 46
4.8 Public Safety Grade-Application Store (PSG-AS) 47
4.8.1 Public Safety Grade – Application Store – Support System (PSG-AS-SS) 48
4.8.2 Public Safety Grade Application Store – Device System (PSG-AS-DS) 49
4.9 Access Rights Management (ARM) 49
4.9.1 Access Rights Management Support System (ARM-SS) 50
4.9.2 Access Rights Management Device System (ARM-DS) 51
4.10 Mobile Application Monitoring (MAM) 51
4.10.1 Mobile Application Monitoring Support System (MAM-SS) 51
4.10.2 Mobile Application Monitoring Device System (MAM-DS) 52
5 Overall Management Framework Architecture 54
5.1 Adding and updating mobile applications on PSG-AS 54
5.2 Downloading mobile applications to PSG-MD 56
5.3 The Requesting of information and services process 57
6 System Component : Public Safety Grade-Mobile Device (PSG-MD) 60
6.1 Classes of PSG-MD 61
6.1.1 Public Safety Owned Devices (PSOD) 61
6.1.2 Bring Your Own Device (BYOD) 61
6.2 Finding a Root-of-Trust 62
6.3 Device Components 63
6.3.1 Hardware Layer 64

6.3.2 Firmware Layer 64
6.3.2.1 Secure Boot 65
6.3.2.2 Measured Boot 66
6.3.3 Operating System Layer 67
6.4 PSG-MD Security Components 69
6.4.1 Chain of Trust 69
6.4.2 Roots of Trust (RoT) 70
6.4.3 Access Right Management (ARM) 72
6.4.4 Device Integrity 74
6.4.5 Assertions for Device Integrity 75
6.5 PSG-MD Capabilities 76
6.5.1 Battery Usage 77
6.5.2 GPS Capabilities and location services 77
6.5.3 Network Capabilities 78
6.5.4 Sensor Capabilities 79
6.5.5 Memory 81
6.5.6 Smart cards - Universal Integrated Circuit Card (UICC) 81
6.5.6.1 Universal Subscriber Identity Module [USIM] 82
6.5.6.2 High Capacity USIM (HC-USIM) 84
6.5.6.3 Embedded SIM (eSIM) or embedded UICC (eUICC) 86
7 System Component: Application 88
7.1 Classes of Applications 90
7.1.1 Generic Applications 90
7.1.2 Public Safety Grade Mobile Applications (PSG-MA) 91
7.2 High-level Threats and Vulnerabilities of Applications 92
7.2.1 Lack of Physical Security Controls 92
7.2.2 Use of BYOD 93
7.2.3 Use of Untrusted Communications and Networks 94
7.2.4 Use of untrusted applications 94
7.2.5 Use of Untrusted Permissions 95
7.3 Software quality 97
7.4 Generic Applications Security 98
7.4.1 Clipboard 99

7.4.2 Metadata 99
7.5 Application Vetting Process 100
7.5.1 Public Safety Requirements 101
7.5.2 Testing Limitations and Additional Security mechanisms 103
7.5.3 Application Evaluation and Scoring 104
7.5.4 Application Testing Process 105
7.5.5 Application Approval and Rejection 106
7.5.6 Continuous Monitoring of Applications and Testing Updates 107
7.6 Communicate between PSG-MA and PSG-II 109
7.6.1 Interoperable Application interfaces 109
7.6.2 Applications Information Sharing 111
8 System Component: Information 112
8.1 Information Protection Principles 112
8.1.1 Confidentiality 113
8.1.2 Integrity 113
8.1.3 Availability 113
8.2 Information Security Policies 113
8.3 Information Classification 114
8.3.1 Information Security Levels 115
8.3.2 Protected Information 118
8.3.3 Classified Information: 119
8.4 Layered Information Architecture 119
8.4.1 Information Owner 119
8.4.2 Information Providers 120
8.4.3 Information Custodian 120
8.5 Interoperability of Data between Different Domains 121
8.6 Access Control 122
8.7 Encryption 123
8.7.1 Management of Cryptographic Keys 124
8.8 Record Keeping and Court Admissible Records 125
9 Public Safety User 127
9.1 Policy Determination and situational authentication 128
9.2 Identity, Credential, and Access Management (ICAM) 130

9.2.1 Identity Management 132
9.2.2 Credential Management 132
9.2.3 Access Management 135
9.3 Authentication 136
9.3.1 Authentication Factors 137
9.3.2 Types of Authentication 137
9.3.2.1 User-Device (U-D) authentication 138
9.3.2.2 User-Device-Network (U-D-N) Authentication 139
9.3.2.3 User-Device-Infrastructure (U-D-I) authentication 141
9.3.3 Authentication Process 141
9.3.3.1 Authentication Protocols 143
9.3.3.2 Authentication Assertions 144
References/Bibliography 149
Annex A Mobility Management Mechanisms 158
A.1 Mobile Device Management (MDM) 158
A.2 Mobile Application Management (MAM) 159
A.3 Mobile Content Management (MCM) 156
A.4 Enterprise Mobile Management (EMM) 157
A.5 Requirements for an Extreme Enterprise Mobility Management (EMM) for regulated organizations 158
A.6 Enterprise Mobility Management (EMM) Suites from different vendors 166
Annex B Containerization 176
Annex C Access Right Management (ARM) 179
Annex D High Capacity USIM (HC-USIM) 182
Annex E Mobile Device Extra Capabilities 186
E.1 Battery 186
E.2 GPS & Location Services 186
E.3 Memory 187
Annex F PSG-MAMF open issues 189
F.1 Device open issues: 189
F.2 Applications open issues: 189
F.3 Applications open issues: 189
Annex G List of Abbreviations 190

List of figures

Figure 1 Generic Ecosystem Architecture 6
Figure 2 Main Principles and Security Services of PSG-MAMF 32
Figure 3 PSG-MAMF multi-fencing security principles 34
Figure 4 PSG-MAMF System Components 39
Figure 5 User Interaction 41
Figure 6 Framework Management and administration functions as part of PSG-MAMF 43
Figure 7 Access Right Management Process 50
Figure 8 overall PSG-MAMF Architecture 54
Figure 9 Process of uploading apps to the PSG-AS (steps 1 to 5) 55
Figure 10 the process of downloading apps from the PSG-AS to the PSG-MD 57
Figure 11 the process of requesting information and services from the PSG-II (steps 1 to 7) 58
Figure 12 Mobile Device Architecture and its Layers 63
Figure 13 Secure Boot Chain 66
Figure 14 Measured Boot Chain 67
Figure 15 Transitive chain of trust in mobile device. 69
Figure 16 Root of Trust Security Components Interaction. 71
Figure 17 Access Right Management (ARM) Components 74
Figure 18 ARM-DS architecture using trusted computing components. 74
Figure 19 PSG-MD Attestation to ensure the integrity of the device 75
Figure 20 GSN collecting data from sensors, manage and process data centrally, and redistribute data to applications and services when requested 80
Figure 21 Current Java Card SIM Architecture 84
Figure 22 HC-USIM Architecture 85
Figure 23 Comparison of traditional single-profile SIM and multi-profile eSIM 87
Figure 24 Malicious actions of clipboards 99
Figure 25 Application Vetting Process 101
Figure 26 Public Safety Requirements 102
Figure 27 Mobile Application Monitoring System 108
Figure 28 the Information Ownership and Information Security Management 121
Figure 29 Mapping qualifying attributes to manage access rights, priorities, and QoS 130

Figure 30 Federal identity, credential, and access management (FICAM) complementary architecture 131
Figure 31 the common service components for identity, credential, and access management complementary architecture 131
Figure 32 PSG-MAMF Authentication categories 138
Figure 33 Authentication, Authorization, and Access Control process 143
Figure 34 Extreme Access Control and Policies Enforcement 165
Figure 35 HC-USIM security models 182
Figure 36 Trust Relationship between different Entities for different Security Models 183
Figure 37 Secure Storages' Architecture 184
Figure 38 System's Area Architecture 184
Figure 39 Services' Area Architecture 185
Figure 40 User's Area Architecture 185

List of tables

Table 1 Informed effort toward Authentication, and Identity Management..... 12
Table 2 Security control and basic principles of PSG-MAMF..... 36
Table 3 Advantages of HC-USIM..... 85
Table 4 Equivalent classifications (security levels) in various countries..... 118
Table 5 Classification of Protected Information..... 118
Table 6 Classified Information designation..... 119
Table 7 Comparison of Enterprise Mobility Management Suites from different Vendors. 174
Table 8 list of Organization's Abbreviations..... 190
Table 9 List of Abbreviations..... 191

Acknowledgements

This work was done with a great collaboration from CSSP members, Saskatchewan Ministry of Government Relations, and the Collaborative Center for Justice and Safety out of University of Regina. In addition, contributions from Canadian Advanced Technology Alliance (CATA) and Canadian Interoperability Interest Group (CITIG) have enriched our view.

Overall, the work couldn't have been completed without the contribution of many individuals from the above mentioned organizations. Their selfless and humbled attitude and the developed spirit of collaboration stand out as a great experience and a strong foundation for further work on PSBN as technologies evolve.

We appreciate all contributions and acknowledge the value provided by all individuals.

1 Introduction

Responders and public safety personnel need support to respond to emergency situations as well as day to day operations. To address the growing reliance on information, responders need to migrate into modern technologies and utilize specialized mobile devices, tools, sensors, mobile applications, and access to wide range of information infrastructure and supporting systems. Mobile devices provide tremendous capabilities manifested in handheld devices and advanced mobile technologies that can help public safety personnel in their jobs and assist resolving emergency situations. Therefore, the public safety community is showing a great interest in using mobile smart devices as a productive platform. However, the mobility aspect of smart devices exposes them to different vulnerabilities and threats. The potential for devices to be compromised, stolen or monitored is greater in a mobile environment compared to a fixed infrastructure. Yet, the goal is to maintain, at least, the same levels of security as provided in the current fixed infrastructure. Further, as mobile applications evolve to operate over potentially private wireless cellular networks; the issue of application interoperability presents novel challenges. On one hand, inter-application points of attachments need to be clearly defined. On the other hand, security aspects relevant to opening interfaces between applications need to be well understood and the risks need to be studied, evaluated, and a roadmap to risk mitigation strategies and tactics need to be drafted.

1.1 Purpose and Scope

In addition to providing a review of mobile devices and applications issues, this study provides a framework for identifying the Public Safety Grade Mobile Applications Management Framework (PSG-MAMF hereafter). The framework defines a group of system components that improve the security, interoperability, and assurances provided by mobile devices, applications, and information. The Public Safety Grade – Mobile Applications Management Framework (PSG-MAMF) achieves such objective by relying on available technologies as much as possible and by merging with current and known practices and contributions within Canada and the USA in particular. Where possible, we will include a Canadian contributions and practices, otherwise, we will refer to US standards, either due to lack of Canadian counterpart or reference is unreachable. Furthermore, the document identifies the requirements and capabilities of the mobile devices to be qualified to serve as a Public Safety Grade Mobile Devices (PSG-MD) such as: battery usage, camera, sensors, memory, and network capabilities. The mobile device shall be able to generate integrity assertions to insure that the mobile device is in a trusted state at all times. In addition, this study provides strategies to reduce the risks of the untrusted applications by vetting applications according to well-defined attributes and by providing applications to users only though trusted sources. Public Safety applications on mobile devices shall also be isolated from the generic applications embedded in most mobile devices. The tenet of separation is utilized to limit access to information following a per-need-basis, and limiting the spread of damage in cases of compromised security. The outcome is a solid framework for application operability and interoperability.

The PSG-MAMF study provides security strategies and recommendation when possible. In cases where multiple strategies are possible guidelines are provided to help the process of developing policies, practices, and building multi-security fences. It is anticipated that public safety agencies will utilize and expand current IT personnel to manage and maintain control over devices,

applications, and information on the mobile devices following the same guidelines used to build fixed infrastructure, and by using the guidelines provided here to expand into future smart devices. Typical mobile protection mechanisms include: application-information encryption, user authentication, and the ability to remotely wipe applications and information. Presented security controls fall along the lines of Enterprise Mobility Management (EMM) including known management approaches such as Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Content Management (MCM) platforms. Further, security mechanisms such as "containerizations" can be used to provide a strong separation between different public safety applications. The PSG-MAMF framework supports multi fencing approach to ensure all potential areas of threats are addressed through different layered security, controls, and approaches. Hence, attacks that break through some security fences shall stop at other security fences and may be captured and logged to improve security build up leading to even further secured systems over time.

It is important to acknowledge that the work and research outcome presented throughout this study were used towards the thesis of Mrs. Nesma Keshta, "Secure Mobile Application Management Framework" [1], April 2018, University of Regina, while the publication of the thesis is pending for DRDC Approval.

1.2 Public Safety Grade

The "Public Safety Grade" is a conceptual term that refers to the expectations and needs of public safety organizations that shall be manifested in the system design choices in order for their system to address the reliability, integrity, availability, confidentiality, as well as the performance specification and security requirements during all operational situations including critical missions. Those needs include requirements for each area and component of the system resulting in appropriate implementation techniques that provide desired baseline security level required for public safety environment. Since developing a formal definition of PSG is complex and includes many recommendations for design elements in a variety of areas that form a comprehensive, reliable, secure, and interoperable system, it is prudent to address PSG as a set of, levelled, requirements that shall change over time. It is also important to hint that PSG shall be multi-levels as the needs are different from one organization to another. For example, the requirements for law enforcement defer from requirements for volunteers (e.g. volunteer fire fighter). In this document, we always refer to PSG as the mainstream level of hardened requirements to satisfy the majority of public safety applications and users.

All system components must be relied upon and trusted by public safety community. Thus, system components must follow Public Safety Grade requirements and standards rather than commercial standards in order to be successfully adopted by the public safety community. Mobile devices and applications may use broadband public safety networks and commercial networks that do not have specific security and interoperability considerations commonly encountered. The anticipated Public Safety Broadband Network (PSBN hereafter) shall be composed of Long Term Evolution (LTE) Radio Access Network (RAN) based on commercial bands or based on public safety dedicated 700 MHz RAN. PSBN had been used with slightly different meanings by the community. We adopt the notion that PSBN refers to a public safety communications infrastructure that may utilize commercial LTE, dedicated LTE, WiFi, or other RAN technologies. Regardless of the used RAN technology, PSBN must meet PSG requirements. The National Public Safety Telecommunications Council (NPSTC) defined Public Safety Grade (PSG) in a report to be used as a guide for design and implementation of the PSBN. The NPSTC

report covers considerations and recommendations in terms of applications and other areas to be hardened to PSG. To the best of our knowledge there hasn't been any similar Canadian effort.

This study highlights the requirements and recommendations that must be considered in terms of mobile device capabilities and application conformance in order to comply with Public Safety Grade (PSG) standards. The requirements and recommendations listed hereafter cover mobile devices, mobile application, and information exchange, by describing the elements that, when implemented as a whole, create a framework that meets public safety expectations and meets required reliability, security, and interoperability.

Some of the requirements listed in this document indicate information that is drawn directly from existing standards and relevant studies as recorded by DRDC, CSSP, RCMP, OCIO, NIST, FirstNet, NPSTIC, DHS, and known practices in mobility and security. This document strives to match such requirements to the greatest extent possible to provide a framework that could be employed by public safety organizations as a PSG-framework by establishing the requirements to harden the mobile devices and applications to PSG levels. PSG hereafter, refers to the mainstream requirements acceptable by the majority of public safety operations for each component forming the PSG-MAMF system in order to meet the public safety requirements for reliability, security, and interoperability. The framework is referred to as "Public Safety Grade Mobile Application Management Framework, PSG-MAMF". Accordingly, hereafter mobile devices, applications, and information systems that address the mainstream PSG level requirements will be referred to as Public Safety Grade-Mobile Devices (PSG-MD), Public Safety Grade-Mobile Applications (PSG-MA), and Public Safety Grade-Information Infrastructure (PSG-II).

It is acknowledged that some requirements and recommendations listed hereafter may not meet particular scenarios (e.g. Bring Your Own Device), however, the document also consider highlighting some contribution efforts to deal with such scenarios. It is important to note that different public safety organizations may also have their own requirements and considerations for different scenarios.

1.3 Document Structure:

The remainder of this document is organized into the following major sections:

- Section 2: Summary of Related Work: Discusses the results of our security evaluations of relevant recommendations, standards, best practices in terms of security technologies and security controls. The chapter provides a summary of existing standards and relevant studies recorded by government, non-government, public, and private organizations, as well as studies carried by academic researchers, study groups, and solutions provided by different vendors. The evaluation includes investigation of current mobile device best practices, mobile applications best practices, and evaluation of systems similar to PSG-MAMF. As a result, we summarized the study findings and security gaps identified.
- Section 3: Definitions, Assumptions, and basics Principals of PSG-MAMF: Represent the major definitions, assumptions, and principles that we developed our framework upon. The principles represented were adopted from existing technologies, recommendations, and standards. Some of these principles were adopted in other systems similar to our framework. However, we enhanced and integrated the use of such principles to meet the

requirements of PSG-MAMF and consolidate the adoption of the framework in public safety environments.

- Section 4: Overall System Architecture Framework: Discusses the security framework used to manage the Public Safety Grade mobile devices and applications. It also describes the components of the system and how each component adds a level of security and protection for the system.
- Section 5: Overall Management Framework Architecture: Describes the PSG-MAMF architecture from a high level by illustrating the interaction process between the system components, and highlighting the key role of each component by referring to the security capability added to the framework by such component to reduce a potential risk.
- Section 6 – 8: Describe the major system components including devices (PSG-MD), applications (PSG-MA), and information (PSG-II). For each component, we identified the potential risks to such component, and strategies and recommendations to mitigate such risks.
- Section 9: Describe the interaction of the User with the system accessing application, information, and services on the PSG-II. User access management requires identity management, credential management, and access management, authentication mechanisms, existing rules and policies, and access rights management. In addition, this section discusses the different types of authentication required to access information and services on PSG-II, which include: User-Device authentication, User-Device-Network Authentication, and User-Device-Infrastructure Authentication. Finally, the section discusses the need for a centralized "Identity and Authentication Framework" by referring to efforts that aim to deploy a reliable, secure, interoperable authentication, identity management framework such as: National Institute of Standards and Technology (NIST), Federal Identity, Credential, and Access Management (FICAM), and Global Federated Identity and Privilege Management (GFIPM) initiatives.

2 Summary of Related Work

The built-in mobile protection technologies are not enough to reasonably mitigate the security risks and threats associated with mobile devices mobility nature and remote access to information systems. The security, fidelity, integrity, confidentiality, reliability, resiliency, privacy, and interoperability requirements[1] each influence the sort of security controls, security technologies, and mobility management program that well-suit the needs of organizations and should be adopted by organizations.

The security technologies presented in this document follow stringent evaluation, recommendations, standards, and practices that provide a variety of means across the mobile ecosystem to address the threats and vulnerabilities to mobile devices, applications, and information. Our investigation of security technologies intends to build a semi-closed ecosystem framework that can integrate effectively to provide the security functionalities required for public safety environments. Existing standards and relevant studies included in this document are recorded by DRDC, CSSP, CIO Council, RCMP, NIST, FirstNet, NPSTIC, DHS, DoD, Cloud Security Alliance, OWASP, GlobalPlatform, Trusted Computing Group, NIAP, Silent Circle, Wide Point, MTTT and other known practices in mobility and security.

While there are many recommendations and relevant studies that address different mobile ecosystem components, the lack of integration between different technologies and solutions raises the need for a framework based on existing standards and recommendations that aims to ensure a baseline security level for mobility management within government and public safety organizations. Security approaches taken by mobile device ecosystem vendors are inadequate to provide the desired level of Security and interoperability required to government. The framework requires centralized system components with a group of security functions integrated into one solution, as well as an extra security considerations, technologies, standards, and policies to be taken in consider. Such framework should be implemented to meet as much of the government organization security requirements and operational needs, while other security technologies, standards, and protocols need to be adopted and integrated to ensure the highest level of security, and ensure all the security gaps are taken into consideration. However, there are unique challenges with mobility management and security gaps in existing ecosystems that are worth consideration.

Typically, the mobile architecture consists of the mobile device itself, and other components that connect the device to other devices or information systems. A generic mobile ecosystem consists of the following key components [2] [3]:

- Mobile device stack including the hardware, operating system, firmware, and mobile applications.
- Embedded components including sensors, camera, bootloader, baseband radio, SIM card, and isolated execution environments.

[1] Throughout the study, we would shorten the security, fidelity, integrity, confidentiality, and privacy requirements into “Security requirements”. Thus, each time we mention security, we refer to public safety requirements of security and other requirements that include confidentiality, integrity, availability, etc.

- Networks including cellular, Wi-Fi, Bluetooth, NFC, and services provided by network operators.
- Vendor mobile infrastructure, including mobile app stores, updates and backup services provided by the mobile device vendor or operating-system vendor.
- Enterprise mobile management infrastructure including Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Information Management (MIM), and enterprise mobile app stores.

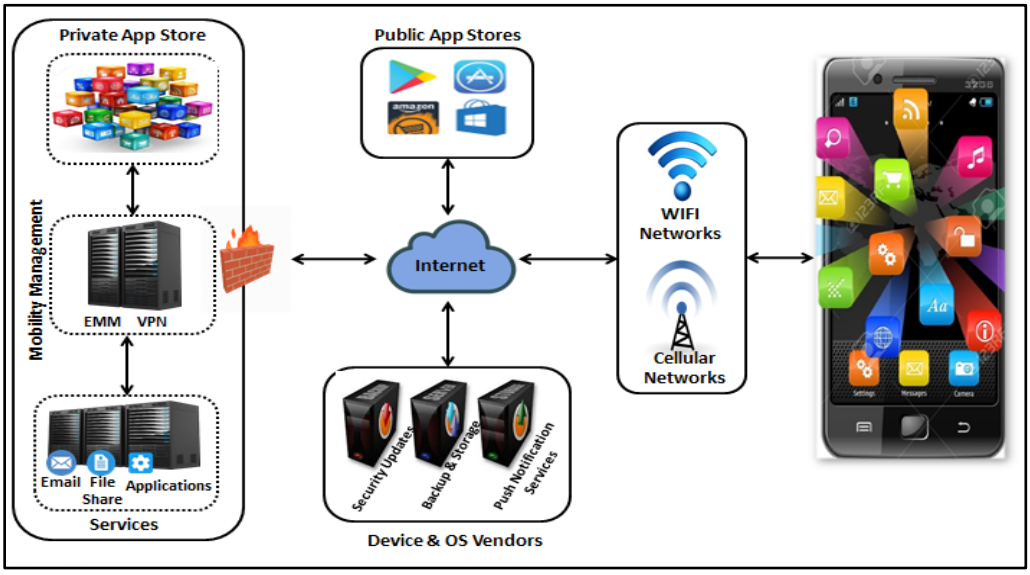

Figure 1 Generic Ecosystem Architecture

Each individual component that interacts directly or indirectly with the mobile device would contribute to the security of the mobile device, the infrastructures accessed by the mobile device, and the information residing the mobile device itself. The following is an overview of several recommendations, standards and protocols, and practices developed by different governmental organizations, industrial organizations, vendors, and study groups to address specific components of mobile architecture. Some of those contributions aim to include basic security measures including encryption, authentication, and integrity checking. Relevant studies of recommendations, standards, and practices to address security gaps of mobile architecture are summarized as follows:

2.1 Mobile Devices Security Best Practices

Mobile devices bring a tremendous amount of capabilities that can be used in different environments to bring information to users' fingertips. In different organization, users may use organization-issued devices or personally-owned devices (known as Bring Your Own Device or BYOD) to access the organization infrastructure to access information and services to perform their duties. However, such capabilities can expose information infrastructure and information residing on the devices to potential security risks. In addition, BYOD increases the challenges to secure a diverse range of computing devices. In general, existing mobile devices are unable to

provide strong security assurance to users and organizations, due to limited of security capabilities on the device. In addition, mobile devices are vulnerable to jail-breaking that results in bypassing security feature and introducing other potential vulnerabilities and security threats.

Much of the security required for mobility relies on the protection provided by the mobile device, and the policies implemented on the device. Thus, mobile devices are critical component in the mobile ecosystem that requires further investigation in terms of recommendations, standards, security controls, and technologies required to mitigate the risks associated with mobility nature. These recommendations, standards, security controls, technologies include requirements to address diverse device types, features, and components by relying on security features including establishing trust in the device, integrity verification of the device and its components, secure booting, containerization and protected storage, real-time monitoring of mobile device activities, Access Rights Management (ARM), policies enforcement, Mobile Device Management (MDM) capabilities, and authentication. A summary of relevant studies of recommendations, standards, security control, and technologies for mobile devices to address their security gaps is described in the following sections:

2.1.1 Guidelines on Hardware-Rooted Security in Mobile Devices

NIST SP 800-164 “Guidelines on Hardware-Rooted Security in Mobile Devices” draft provides guidelines and recommendations to be used as a baseline of security technologies that can be adopted by organizations in order to secure their mobile devices, in both organization-issued and personally-owned devices [4]. The document identifies the security features and capabilities needed to secure mobile devices, and highlights the industry efforts that aim to implement such features and capabilities.

In addition, the document provides a set of security components as key security elements that can be adopted by mobile devices, operating system, and applications. The document focuses on three major security components: Root of Trust (RoT), application programming interface (API), and Policy Enforcement Engine (PEnE) [4]. In PSG-MAMF, we adopt RoT following the NIST approach, but replace PEnE with ARM approach that is proven to require less traffic exchange and provide comprehensive approach to define information policies and rules.

The security requirements recommended by PSG-MAMF are device integrity, isolation, and protected storage. For each security capability (integrity, isolation, protected storage), NIST SP-800-164 covers mobile device security, the threats affecting such capability, considerations to leverage, ways to implement it on the mobile device, and additional security capabilities required to support such security capability.

2.1.2 Guidelines for Managing the Security of Mobile Devices in the Enterprise

NIST SP 800-124 “Guidelines for Managing the Security of Mobile Devices in the Enterprise” draft provides a set of guidelines for mobile device security and recommendations to improve the security of mobile devices in enterprises, including the following recommendations [5]:

- Define security policies to apply on mobile devices including policies relevant to mobile devices’ access to organization’s resources (e.g. types of resources, types of devices, access degree and access rights), and policies related to Mobile Device Management (MDM).

- Develop System threat models to identity the threats and vulnerabilities on mobile devices and the accessed resources, and accordingly identity the security requirements, security controls, and design and implement the solution that best meet such requirements.
- Consider the features provided by each security service, and determines which services are needed for the applied environment. Accordingly, design and implement the solution that provides the necessary services.
- Test the implemented mobile device solution to ensure interoperability of all system components and ensure the solution provide the appropriate protection, authentication, management, monitoring, logging, and performance as expected.
- Ensure all mobile devices are secured and conform to the basic level of trust before issuing it for users to access it. Supplement the mobile devices with additional security controls, if necessary, such as antivirus and malware detection software.
- Maintain mobile device security regularly by adopting the following [5]:
    - Check regularly for patches and updates, acquire, test, and enforce them to mobile devices.
    - Ensure mobile devices' clock and infrastructure components are synchronized with common time source. Such feature is important for monitoring and digital signing.
    - Monitor of mobile devices to detect unauthorized actions and configuration changes to mobile devices.
    - Log all system activities, applications activities, and access to device information and resources.
    - Assess mobile devices conformance periodically to ensure conformance to policies, processes and procedures.

In addition, NIST draft provides an overview of common security threats associated to mobile devices compared to other devices. The draft includes high-level recommendations in order to mitigate the risk facing current mobile devices. The draft also provides overview of the current centralized mobile device management technologies and solutions that are used to manage and control both organizational issued and personally-owned devices. In terms of mobile device management, the draft provide summary of current state of technologies, components, features, and architectures. Finally, the draft explains the interaction of technologies, components, and security services of mobile device management solutions throughout the enterprise mobile device management solution lifecycle in order to provide the security capabilities required to secure the mobile device [5]. PSG-MAMF adapts the same technologies recommended by NIST SP 800-124.

2.1.3 Guidelines on Mobile Device Forensics

NIST SP 800-101 "Guidelines on Mobile Device Forensics" document provides guidelines in terms of recovering and reporting digital evidences from mobile devices by acquiring the information contained in mobile device memory and reporting digital evidences accordingly. Such information would be helpful for the law enforcement community, as it can be used as

evidences. In addition, the document provides guidance for organizations willing to set and apply appropriate policies and procedures in terms of dealing with mobile device [6].

NIST document provides guidelines in terms of types of software tools for mobile device examination. The tools are typically used for mobile device management, testing, and monitoring. Such tools gather information from internal memory and UICCs and calculate the integrity hashes for the collected information. The document provides a classification system that compares different tools for mobile data acquisition. Each type represent different extraction methods including recording information brought up on mobile device screen, extracting and recording an image of physical store, etc.

NIST document describes the forensics process applied to mobile devices in order to collect integrity evidence and other information from the device to be used as evidences in a court of law. Thus, the document provides recommendations and guidelines in terms of protecting and storing of evidences [6]. PSG-MAMF is aligned with NIST SP 800-101 [6].

2.2 Authentication and Identity Management Practices

There are different efforts over the years to deploy a reliable, secure, interoperable access to network and information infrastructures. This requires a comprehensive authentication and identity management framework that is able to provide identity and credential management in order to enable secure access to networks and infrastructures. Typically, such frameworks are designed to provide identity and credential management on the system side, rather than the user side. Table 1 provides a summary of efforts that aim to provide authentication, identity, and access management.

There are also other efforts for establishing standards-based identity management solutions across government agencies. Those efforts include GFIPM, NIEM, and FICAM described in sections 2.2. Such solutions are aim to manage access to resources and provide a secure access to information systems from multiple governmental agencies.

2.2.1 Electronic Authentication Guideline

NIST SP 800-63-2 “Electronic Authentication Guideline” provides technical guidelines and recommendations to assist agencies in implementing electronic authentication [7]. By adopting the technical guidance provided by NIST SP 800-63-2, users can remotely authenticate themselves to federated system and other systems. The “Electronic Authentication Guideline” focuses on common methods of remote authentications, where the user needs to prove his identity by showing that he/she possesses secret information. However, in government systems, credentials and other attributes can be used in the authentication process to provide stronger identity assurance. Credentials and attributes can be provided by different trusted third parties. This requires sophisticated authentication mechanisms that can integrate the authentication factors including identity, credentials, attributes, and any other factors that can assist providing more granular access control based on assurance level.

NIST SP 800-63-2 follows and complements the technical guides of NIST SP 800-63-1 “Electronic Authentication Guideline” and OMB M-04-04 “E-Authentication Guidance for Federal Agencies”. The document defines four levels of assurance, Levels 1 to 4, where 1 is lowest assurance and 4 is highest assurance level. In addition, the document provides a set of specific technical requirements for each level of assurance. The guidance provides assistance to

agencies to determine the level of e-authentication assurance required for their environments, and the appropriate technologies and authentication schemes that at minimum can provide such assurance level [7].

NIST SP 800-63-2 represents an E-authentication architecture model, discusses the various entities complementing the model, and illustrates the interactions of the entities that comprise the e-authentication model. In addition, the document provides the type of tokens used to prove identity during the authentication process, which are *something you know* (e.g. PIN or password), *something you have* (e.g. cryptographic key), and *something you are* (e.g. a fingerprint or other biometric data such as Personal Identity Verification PIV). NIST SP 800-63-2 document discusses how different types of tokens can be integrated forming a multi-factor authentication, assurance level achieved by each type of token, threats and type of attacks on each token, and common strategies to mitigate such threats and attacks. The document also provides brief details in terms of electronic credentials, authentications processes, and assertions. In addition, NIST SP 800-63-2 assists agencies to calculate their overall authentication assurance level.

Finally, NIST SP 800-63-2 discusses the usage of PIV authentication key of a Federal Information Processing Standard (FIPS 201) as an approach that provides level 4 authentication assurance. In addition, the document provides guidelines in terms of mapping Federal Certificate Policies and PIV Credentials to E-authentication Assurance Levels [7]. PASG-MAMF assumes the same federated authentication mechanism and expands the coverage using multiple authentication approaches as highlighted later in section 9.3.

2.2.2 Mobile, PIV, and Authentications

NIST IR 7981 “Mobile, PIV, and Authentication” focus on the challenges of authenticating mobile device remotely [8]. As per NIST SP 800-63-2 discussed in section 2.2.1, federal agencies require strong authentication that represent level 4 assurance level (e.g. Personal Identity Verification Cards, PIV) [8]. PIV is a smart card that uses credential based public keys cryptography, where users need to insert a card into readers attached to computers in order to access government information. However, authenticating from mobile devices using PIV requires further investigation due to lack of integrated smart card readers.

NIST IR 7981 presents different current and near-term options for supporting PIV as an electronic authentication method, aiming to leverage additional security capabilities on the mobile device to address the government flexibility, security, and interoperability requirements. In addition, the document provide recommendations in terms of mobile device ecosystem that integrate credentials and mobile devices authentication schemes and policies [8].

2.2.3 Electronic Credential and Authentication Standard

The “Electronic Credential and Authentication Standard” provides a set of standards recommended to government organizations to leverage a secure system by providing identity assurance for entities attempting to access information systems and applications [9]. The standards provided by OCIO were adopted form (NIST) SP 800-63 and enhanced to meet the requirements of the British Colombia (BC) government. The BC government has central agencies that are responsible for issuing and managing electronic credentials, authenticating electronic credentials. This standard has been made available for other agencies that require the application of electronic credentials and authentication to manage access to their information systems and applications [9].

The standards provided by OCIO include different technologies, security controls, and management processes that are required to assist in implementing of credential and authentication services to manage access to information systems and applications. The document also provides different combination of those technologies, security controls, and processes resulting in different levels of credential and authentication strength and assurance levels. Furthermore, the document lists a set of additional services and information security policies that can assist organizations providing electronic credential and authentication services [9].

The Office of the Chief Information Officer (OCIO) defines the authentication strength in 4 levels, by mapping it to credential strength levels [9]. The use of authentication strength level 4 (very high) is recommended for government agencies in order to ensure a strong authentication process takes place prior to granting access to government information, services, and applications. Authentication strength level 4 includes authentication using multi-factor credentials that use a hardware-based cryptographic token (e.g. a smart card and PIN), through an encrypted communication session.

2.2.4 The Global Federated Identity and Privilege Management (GFIPM) initiative

GFIPM was developed by the U.S. Department of Justice's Global Justice Information Sharing Initiative, which aim to provide a secure, cost effective information sharing architecture based on an electronic credential management [10]. The main aim of GFIPM is to provide a standards-based identity management solution to securely connect law enforcement and public safety Users to applications, information, and services over the Internet. GFIPM assists in access management by mapping identities and other predefined attributes, and securely communicating such information to other parties.

2.2.5 National Information Exchange Model (NIEM)

NIEM is one of the DHS and DOJ initiatives that aim to enhance interoperability, access control, and provide secure information sharing across government organization.

The use of NIEM standards can offer the following benefits for the public safety communities [11]:

- Reduce the total cost of exchanging information among organizations. Accordingly, accurate, real time information can be available to improve decision making.
- NIEM provides tools, methodologies and processes to implement interoperable systems and information exchanges.
- The current systems don't need to be replaced or significantly changed in order to exchange information between existing systems.
- By adapting NIEM standards, MAMF builds on existing frameworks to expand information exchange through mobile applications rather leading to smoother transition into the mobility paradigm powered by the anticipated PSBN evolution.

The goals and objectives of using NIEM align with PSG-MAMF and provide consistency leading to simpler application interoperability and lessen the efforts needed to build the PAS-MAMF. Adapting NIEM leads to more cost efficient systems and fits into the long term view for digital information infrastructure strategy.

2.2.6 Federal Identity, Credential, and Access Management (FICAM)

FICAM represents a comprehensive access management approach that provides formal integration of digital identities, qualifying attributes, credentials, and access control. The ICAM provide major service areas including: "digital Identity, credentialing, privilege management, authentication, authorization, access control, cryptography, and auditing & Reporting" [12]. FICAM Roadmap and Implementation Plan v1.0 provides guidelines to assist federal organizations establishing logical access control architecture that validate the qualifying attributes prior to enable access to governmental organization's resources. FICAM Roadmap and Implementation Plan v2.0 recommends the "Attribute Based Access Control (ABAC)" model for managing access and information sharing between organizations [13].

The primary considerations relative to ICAM were historically the Electronic Authentication (E-Authentication) policy framework [14][15] and HSPD-12 and Federal PKI initiatives [16][17] [8]. However, the desire across Federal Government nowadays is to unify those areas and other identity management initiatives within the government to create a comprehensive and integrated approach, through FICAM. FICAM aims to electronically authenticate entities (e.g. Users, Devices), providing secure electronic transactions at varying assurance levels; and establishing trust and multi-layered security. The FICAM document is limited to two main components: 1) new government wide identity, credential, and access management (ICAM) architecture, and 2) implementation guidance, tested and proven implementation approaches through the incorporation of case studies and learned lessons from programs at selective government agencies.

Table 1 Informed effort toward Authentication, and Identity Management

Document	Author and Resource	Summary
OMB M-04-04: E-Authentication Guidance for Federal Agencies	OMB [15]	Provides guidelines to enable a secure remotely access to government services using the Internet, and guidelines in terms of identity verification and authentication, and implementation of E-authentication process within Federal agencies. NIST SP 800-63-2 provides further technical guidance on the technologies types suitable to support the different level of assurance defined in OMB M-04-04
NIST 800-63-1/2: Electronic Authentication Guideline	NIST [14]	"Provides guidance for electronic authentication, including secure deployment of identity assertions in federated identity deployments. NIST SP 800-63-2 designed to supplement OMB M-04-04 and NIST SP 800-63-1 for selecting a technology based on e-authentication technical guidance including authentication protocols, processes, and assertions used to communicate the result of remote authentication" [14] .
Homeland Security	Executive Office of the President,	"Provides a common identification standard to enhance security, interoperability and efficiency by

Presidential Directive 12	OMB [16]	managing access to federal information systems. The framework was first design to support Personal Identity Verification (PIV) card and its supporting infrastructure to manage physical access to governmental facilities and logical access to federal information system. Afterward, PIV cards enhanced to be used as credentials for mobile devices in several ways. A mobile device could have an integrated smart card reader as part of the device or a separate smart card reader could be attached to the device via a wired or wireless connection" [16].
NIST SP 800-157, "Guidelines for Derived Personal Identity Verification (PIV) Credentials", NIST Interagency Report 7981, "Mobile, PIV, and Authentication"	NIST [17] NIST [8]	Provide requirements for derived PIV, and other considerations for using PIV credentials with mobile devices. Such technology can facilitate different operational scenarios for mobile devices, and manage access from secure PSG-MD or unmanaged BYOD scenarios.
ATIS-1000035: Next Generation Framework (NGN) Identity Management (IDM) Framework ATIS-1000044: ATIS Identity Management: Requirements and Use Cases Standard ATIS-1000045: ATIS Identity Management: Mechanisms and Procedures Standard	ATIS [18], [19], [20]	Provide requirements, use Cases Standard, mechanisms, procedures standard, and ways in which an authentication and identity management solution can confirm to ATIS's identity management requirements.
ATIS-1000030: Authentication and Authorization Requirements for Next Generation Network (NGN)	ATIS [21]	"Provides authentication and authorization requirements for Next Generation Networks (NGN) including requirements for authentication and authorization across the User-to-Network Interface (UNI), the Network-to-Network Interface (NNI) and the application–to–Network Interface (ANI)" [21].
NPSTC: Public Safety Broadband High-Level Launch Requirements	NPSTC [22].	Provides requirements for authentication and identity management framework must conform to meet public safety's needs. NPSTC authentication and identity management framework was built on top of LTE device authentication discussed in section 9.3.2.2.

2.3 Mobile Applications Security Best Practices

Mobile applications have begun to be deployed by organization to increase productivity, and information sharing. In public safety environments, applications will be required to provide enhanced mission capabilities to assist public safety users to perform their duties. However, mobile applications can potentially lead to serious security risks. Applications may contain vulnerabilities that can be exploited by intruders to gain unauthorized access to device resources including sensitive information residing on the mobile device. Thus mobile applications are critical component in the mobile ecosystem that requires further investigation in order to develop recommendations, standards, and security controls required to mitigate risks associated with mobile applications.

The recommendations, standards, and security controls include requirements for establishing an application vetting process, containerization to isolate applications and information, protected execution environment, real-time monitoring of applications, Access Right Management, policies enforcement, and Mobile Application Management (MAM) capabilities. Managing granularities finer than the application level would complicate the security management. Both the application and its information together form reasonable level of containerization granularity. Some of the recommendations, standards, and security controls were established to assist the adoption of mobile applications in Federation agencies, public safety, and health care communities to address their unique mobile challenges. Summary of relevant studies of recommendations, standards, and security control for mobile applications to address their security gaps is as following:

2.3.1 Vetting the Security of Mobile Applications

NIST SP 800-163 “Vetting the Security of Mobile Applications” document defines the application vetting process that consists of group of activities in order to evaluate the mobile applications and assess their compliance with organizational requirements. According to NIST, the application vetting process consists of two main activities: application testing and application approval/rejection. The application testing activity includes testing and evaluating the application for vulnerabilities using automated assessment and human assessment, resulting in risk assessment and evaluation report. The Application approval and rejection include evaluating the risk assessments and reports, as well as determining application conformance with security requirements defined by the organization, then accordingly approve or reject the application [23]. The application vetting program adopted by PSG-MAMF is described in details in section 7.5.

2.3.2 An Overview of Mobile Application Vetting Services for Public Safety

NISTIR 8136 document focuses on mobile application vetting services instead of mobile application vetting techniques, since it targets public safety organizations [24]. Mobile applications vetting techniques and the vetting process are already covered in NIST SP 800-163 “Vetting the Security of Mobile Applications” [23].

Public safety organizations shall evaluate mobile applications security before allowing them to access network or infrastructure. In order to perform application vetting, public safety organizations require expanding their technical expertise to include mobile application testing, or otherwise rely on existing mobile application vetting services to vet applications on behalf of public safety organizations. NISTIR 8136 suggests leveraging the existing mobile application vetting services, and provide an overview of some mobile application vetting services and list of

companies performing application vetting services available at the time the document was developed, in January 2017 [24].

However, public safety should identify the areas of concerns for mobile application security in public safety environment that need to be evaluated through application vetting services. NISTIR 8018 "Public Safety Mobile Application Security Requirements Workshop" identifies six areas of concern for mobile application security in public safety, which is: battery life, network usage, location information, data protection, identity management, and unintentional denial of service [25]. By identifying the areas of concerns, public safety organizations can define the requirements that should be evaluated and the mobile application vetting services that have the ability to evaluate such areas of concerns. NISTIR 8136 provide a set of features offered by existing mobile application vetting services, such information would assist public safety organizations selecting the appropriate mobile application vetting services that match their needs [24].

2.3.3 Adoption of Commercial Mobile Applications within agencies of U.S. Federal Government

"Adoption of commercial mobile applications within Federal Government" document provide a survey of adoption of mobile applications in U.S. federal agencies aiming to assist agencies integrating mobile applications into their daily operations [26]. The document highlights the key findings in terms of adoption of commercial applications into U.S. Federal agencies according to interviews conducted across nine agency of U.S. Federal government including DHS and DOD. Summary of findings are [26]:

(1) Enormous numbers of agencies are already deploying commercial applications to improve agency operations. However, they differ in the way applications are deployed, and the application management process each agency follows.
(2) Most of the agencies are still in the early stages of deploying mobility management solutions for managing devices and applications including mobile device management (MDM) and mobile application management (MAM) solutions. Some agencies use common MDM and MAM products; however, there are still a gaps that call for new solutions, technologies, and products for the Federal government.
(3) Some agencies are in the early stages of using container solutions to isolate agency's approved applications and data from other applications and data residing the mobile device [26]. The container aims to protect the integrity of government applications and data by creating a trusted environment for applications to run inside and protect the data encrypted within the containers. Access to containers is restricted only to authorized entities. However, further investigation is required in terms of solutions and products that can provide such services for federal government.
(4) In general, Applications deployed into Federal agencies are categorized into basic types of applications (90% falls within productive and foundational applications). Those types of application are:
    - Custom Applications: Applications that are developed by government agencies. Such applications are sometimes called Government off the Shelf (GOTS)
    - Mission Specific Applications: Commercial applications that may help the users to perform their duties.

- Enterprise Connected Clients applications: Mobile applications that are connected to the agency enterprise solutions.
- Basic Productivity Applications: Useful applications and tools that help users become more productive (e.g. file sharing)
- Foundational Applications: Applications that provide basic services to support connectivity with agency network.

(5) Federal agencies are taking similar approaches for applications review and approval. The reviewing process includes testing the applications against business needs, security and privacy risks, threats to the infrastructure, and accessibility requirements.

(6) Most of the agencies deploying applications apply policies, rather than technical solutions. Such policies aim to guide user behaviour by requiring the users not to use sensitive information on mobile applications, or requesting the user not to download applications on the government issued devices. In many cases there are no policies enforcement techniques to enforce policies. Relying on users to comply with agencies policies is not enough to ensure security, fidelity, and integrity required in Federal agencies, unless technical solutions are used including policies enforcement techniques, MDM, and MAM solutions [26].

CIO document also provides a list of common challenges when integrating mobile applications into Federal agencies, including [26]:

- Controlling and regulating access to mobile applications. Governmental agencies require mature technologies for controlling application distribution and usage. Existing technologies are not yet mature enough to be adopted by government agencies. This calls for a comprehensive solution that can balance between flexibility and security requirements within government agencies.
- Mobile applications, operating systems and devices are more frequently updated, which require applications updates and distribution of updates through trusted sources. This requires additional security controls including monitoring, managing, and enforcing of mobile devices, applications, and operating systems frequent updates, and trusted application store to distribute applications updates.
- Issues relevant to information storage on public clouds in terms of security, privacy, and records management. Some mobile application use cloud solutions for data storage, as well as mobility management solutions that can take advantage of cloud solutions to implement part of the mobility management solution. Most of the agencies using cloud services are managing and controlling their information by issuing policies that restrict usage of sensitive information in the cloud. Most agencies are relying on issued policies to restrict the use of sensitive information on the public cloud. However there are no policies enforcement mechanisms that guarantee users compliance with those defined policies.
- Issues relevant to data sharing and access to mobile device information and services. Integrating and sharing information on the same mobile device storage raises security risks that must be considered when planning the security of mobile applications. Interaction between applications, access, storing, usage, and sharing of information are

important issues that must be managed in order to provide a regulated controlled mobile applications in Federal agencies.

- Other issues relevant to licensing and agreements on terms of use, in case the agencies are deploying commercial applications from third parties application stores or applications vendors.

In addition, CIO document defined the typical approaches to deploy commercial mobile applications in Federal agencies. In general, the commercial applications life cycle in government agencies consists of several phases, including discovery, review/approval, procurement, distribution/installation, and managing, controlling, and support. Each agency has its own approaches that are applied for activities running through each phase in the lifecycle. Further, government-wide standard policies can be applied through each phase ad government-wide activities could be implemented instead of agencies-level activities [26]. PSG-MAMF presents its take on application vetting later in this document. PSG-MAMF is in-line with the CIO, but presents a more stringent rules and policies for application vetting.

Finally, CIO document provides a set of recommendations, considerations, and best practices that address application adoption challenges including: controlling access to mobile applications, managing frequent updates, public clouds issues including storage services, applications integration, access/storage/usage/sharing of information, and licensing and terms of use issues. The document also includes best practices regarding applications review processes [26].

2.3.4 Open Web Application Security Project (OWASP) – Mobile Security Project

OWASP Mobile security project is a comprehensive guide that aims to provide application developers, testing teams, and security teams the necessary resources to build, test, and maintain security, integrity, fidelity, and privacy in mobile applications. The project provides a set of mobile security risks, and provides recommendations, standards, and security controls to mitigate the risks of exploitation. While the project is still in progress, it has already produced the following deliverables described in the following sections [27]:

2.3.4.1 Mobile App Security Requirements and Verification document:

OWASP document [28] provides standards and guidelines for mobile applications security. The document aims to assist applications developers to develop secure mobile applications, as well as application testers to assess the security of the developed applications and ensure robustness of testing results. The requirements and guidelines were developed for the following objectives [28]:

- To be used as a metric: In order to provide security standards that can be used by applications developers and applications owners as a metric to be compared against, when developing and when assessing applications security.
- To be used as guidance: In order to provide guidance for the development and testing of mobile applications during all phases.
- To be used during procurement: In order to provide a baseline in terms of mobile applications security verification.

2.3.4.2 Mobile Security Testing Guide (MSTG)

Mobile Security Testing Guide is a comprehensive guide for iOS and Android security testers to provide guidance for security testing of mobile applications development lifecycle, basic static and dynamic testing, and assessment of software protections [27]. The MSTG also covers processes, tools, and techniques that could be used by security testers during the security testing process to provide consistent testing processes and ensure robustness of testing results. In addition, the guide provides group of detailed test cases that can assist security testers in their testing processes. The MSTG project is still in progress, while the OWASP announced for the final release in second quarter of 2018 [27] [29].

2.3.4.3 Mobile App Security Checklist

OWASP checklist [30] provide a list of mobile application security requirements for both IOS and Android that can be used during security assessments. The security verification requirements listed in the checklist include: Architecture, design and threat modeling, Data Storage and Privacy, Cryptography, Authentication and Session Management, Network Communication, Environmental Interaction, and Code Quality and Build Settings requirements. Such checklist can be used by security testers as a metric to be compared against, when performing security assessment for mobile applications. For each requirement, the checklist provides the level of confidence that can be assigned for the application by conformance to such requirement [30]. For example, by verifying that application is using proven implementation of cryptographic primitives, the application is assigned a confidence level 2.

2.3.5 Mobile application Security Testing Initiative

The Mobile Application Security Testing Initiative was proposed by Cloud Security Alliance (CSA) to create secure cloud computing ecosystem that aims to address security concerns of mobile applications, by integrating systematic security approaches that aim to address application architecture, design and vetting [31]. Such ecosystem will assist reducing the exposure and security risks associated with mobile application usage.

The Mobile Application Security Testing Initiative highlights the key areas of concerns, and top security challenges and threats facing mobile applications user including third-parties applications security challenges, mobile application development management challenges, and mobile applications security vetting challenges.

The CSA document also provides a mobile application security testing scheme developed by CSA. CSA security testing scheme include testing the applications against mobile applications security vetting requirements defined by OWASP and NIST SP 800-163 [32] [23]. The key identified security requirements include privacy handling (e.g. permission usage, and information disclosure), protection requirements (e.g. information storage, and encryption techniques and strength), and execution environment (e.g. power consumption) [31].

2.4 Preliminary Study on Systems and efforts Closer to PSG-MAMF

Following are efforts aimed at developing a comprehensive mobile application ecosystem to provide secure mobile application environment throughout the applications lifecycle.

2.4.1 Mobile Computing Decision Framework (MCDF)

Mobile Computing Decision Framework (MCDF) was proposed by MTTT and Chief Information Officers (CIOs) in December 2012 as a decision making tool to assist organizations determining which mobility management solution would support their organizational requirements [33][34]. MCDF is a multi-dimensional decision-making process that helps organizations selecting the appropriate mobility management solution, if any exist, according to their missions' requirements. MCDF creates a high-level understanding of the relationships of mobile devices, applications, infrastructure, and mobility management solution. MCDF provides a roadmap by setting up group of questions that can be used as guidance for organizations to determine the mobility management solution that fits their requirements. The framework includes the following 4 stages:

(1) **Mission Requirements Stage:** helps organizations identify their operational and security requirements. At this stage, organizations would build a use cases to identify the following:
- Who need access to information
- What information would be accessed
- Where/when information would be accessed
- Why access to such information is required
- What mission criticality under which the information can be accessed

(2) **Decision Balancing Stage:** once the organizations identify their requirements, the organizations have to trade-off between those identified requirements, taking in consider the following 3 major considerations to balance the decision:
- Capabilities: the capabilities that would be supported by the solution and what an authorized user would be able to do with the information accessed
- Security: how secure the information must be, the security added to the framework by supporting those capabilities, and how information security is addressed following such capabilities and framework.
- Economics: how can organization leverage from existing capabilities and technologies, and whether the organization can afford the desired security and capabilities.

It is important to highlight that PSG-MAMF include technologies and recommendations that support the capability and security considerations, however, PSG-MAMF doesn't include any considerations in terms of cost of implementation or adoption within organization. The economic considerations for PSG-MAMF require further investigation.

(3) **Risk-Based Tailoring Stage:** organizations perform risk tailoring by relying on risk frameworks such as NIST SP 800-37 and SP 800-39 [35][36] to identify the potential risks in terms of 7 considerations, security, privacy, operation, technology, legal, policy, and financial risks. Accordingly, organizations can choose whether to accept those risks and tailor the solution according to the organization risk management strategy, or return to decision balancing stage to modify the trade-off between capabilities, security, and economics resulting in more acceptable risk tailoring. Further iterations may be required to reach to more acceptable risk across all the 7 categories.

(4) **Result Stage:** map the requirements identified in "Mission Requirement Stage", the balanced considerations from "Decision Balancing Stage", and the risks from "Risk-Based Tailoring Stage" together forming the specification of mobility management solution that well fits the organizational needs and missions' requirements.

Using the MCDF, provide organizations with tools to be able to identify the requirements of mobility solution that fits their needs, reach suitable balance between capabilities, security, and economics, determine the potential risks and how to address them, evaluate and compare vendor solutions according to their needs, and finally select the best-fit solution.

2.4.2 Mobile Security Reference Architecture (MSRA)

The Mobile Security Reference Architecture (MSRA) was released by Department of Homeland Security (DHS), Federal CIO Council, and NIST to assist federal agencies to implement secure mobility solutions [37]. MSRA provides a reference architecture for mobile solutions that can be tailored to fit the needs of different agencies according to their security requirements [37]. MSRA document illustrates the components of the architecture and the associated security controls and management services. MSRA provide a flexible architecture design by providing different 4 use cases and 4 implementation strategies to be adopted by organizations according to their needs. Following is a summary of the use cases, implementation strategies provided by MSRA, and our security evaluation for each of them [37].

MSRA Use-Cases:

MSRA document provide four basic use cases for managing mobile devices within agencies varying from fully managed devices to completely unmanaged devices depending on the organizational requirements [37].

(1) Organizational owned - fully managed devices:

Organizational owned - fully managed devices is a use case where the organizations have full control over the hardware, operating system, applications, and other features (GPS, Camera, etc.), storage, and authentication techniques. In such case, the organization is considered the owner of the device, referred to in PSG-MAMF as "Public Safety Owned Devices".

(2) Organizational owned - partially managed devices:

Organizational owned - partially managed device is a use case where the organizations have control over partitioned virtual environment on the mobile device. This can be done by using application and storage virtualization, where the organizational information that requires unique protection, encryption, authentication, and access management can be limited only to the isolated environment. As for fully managed devices, for partially managed devices the organization holds the ownership of the device, allowing it to confiscate the device upon user termination or when deemed necessary, fully wiping of information, and other management and control capabilities.

(3) User owned - partially managed devices:

User owned – partially managed devices is a use case where the user can select the device that match his needs, and can use their own devices for job activities. In this case, the organization has

no control over the mobile service provider, operating system, or additional device services. The device will be partially managed through EMM capabilities (e.g. MDM, MAM, and MCM). However, the organization would specify a set of minimum requirements for the mobile device (e.g. the device should not have been rooted or jail-broken), should be able to enforce their security rules, policies, and requirements over the mobile device, and be able to apply monitoring and auditing services. In addition, organizations should apply applications and storage virtualization, in order to create an isolated environment. This way, organizations can manage information that requires unique protection, encryption, authentication, and apply access rights management only in the isolated environment.

This case provides the user full access to the device, while maintaining the security and integrity of organization applications and information. However, user's actions on the unmanaged portion on the mobile device may still affect security and integrity of the whole system. Hence, users actions should be monitored and appropriate actions should be applied accordingly.

This use case suffers from some challenges. For example, not all devices will comply with the organizational security requirements (e.g. ability to provide two virtualized spaces). In addition, the BYOD requirements must be explicit for such use-case.

(4) User owned – unmanaged devices:

User owned – unmanaged devices is the lowest secure use case, where the user has full ownership and control over the mobile device, while the organization has no control over the device. The mobile device may use managed remote access capabilities that doesn't allow any information to be stored on the mobile device (e.g. prevent the download of attachments using webmail or email). Remote access capabilities may require enhancements to include access from mobile devices. Organizations may require setting additional security standards and technologies to manage such case.

MSRA Possible Implementations:

In addition, [37] provide sample possible implementations strategies for the mobile solution architecture. The implementations can be integrated with other solutions to form more complex solutions. Implementation strategies are as follows [37]:

(1) Public Information Service Implementation

This implementation provides public access to organization resources through organizationally provided mobile application, distributed through third-party application stores. The implementation relies on a Mobile Application Gateway to manage access to organization resources. The access to organization resources through means rather than the Mobile Application Gateway is prohibited. In addition, to provide more assurance, traffic passing though the gateway may be inspected by a security stack. As per our evaluation, we realized that such architecture suffers from several weaknesses, including but not limited to:

- No management and control over the mobile devices, applications, and information.
- Such implementation is not suitable for public safety community since it doesn't require authentication and access control, which are important considerations when providing access to public safety infrastructure.

- Malicious applications could be created and distributed through third-party application stores.

(2) Remote Data Entry Implementation

This implementation requires providing the users with devices to access information and services remotely, while the organization uses a Mobile Device Manager to provision the devices assigned temporarily to users. In addition, all mobile devices can connect to organizational infrastructure through a Virtual Private Network (VPN), to minimize the exposure for public network. Mobile applications connect to organizational infrastructure through the Mobile Application Gateway. The network gateway and security stack allow only the passing of Mobile Application Gateway traffic. As per our evaluation, we realized that such architecture suffers from several weaknesses, including but not limited to:

- Devices are not tied to specific users
- Doesn't require authentication and access control before granting access to information and services.
- No access rights management supported. Although this is acceptable for some information that doesn't require any additional protection on the mobile device, other sensitive information requires access management to provide granular access control.
- Malicious applications could be created and distributed through third-party application stores.
- VPNs raises additional security risks that need to be taken in consider and additional VPN security features need to be applied to mitigate such risks.
- Doesn't consider the occurrence of BYOD scenario

(3) Organizational Owned – Fully Managed Devices Implementation

This implementation requires providing the users with mobile devices to access information and services. Organizational issued devices are configured using Mobile Device Manager. The Mobile Device Manager uses Identity Manager to federate user identities, and in case the mobile device is being used by different users (e.g. during different shifts), user would be identified and validated during the authentication process. This can be done by creating different profiles based on the user's role, and accordingly the user can be identified based on the profile enabled on the mobile device during the time of authentication. Mobile applications are pre-loaded on the mobile devices and managed by MDM. MDM configuration policies can activate device storage encryption, and wipe lost and stolen devices. As per our evaluation, we realized that such architecture suffers from several weaknesses, including but not limited to:

- Pre-loading applications to mobile devices make it harder to distribute new applications and updates to users, compared to distributing applications through an application store. In addition, users may need to download specific application for specific scenario; waiting for the organization to load application may limit the user operational duties.
- Integrating mobile device identity with user identity would be a challenge in case different users may use the same mobile device in different shifts.

- It doesn't support the implementation of federated identity management that allows linkage of multiple users' identities with different Information Providers through a common federated identifier. For example, in public safety environment a group of Information Providers may be connected together through active directory, security policies, trust mechanisms, and protocols. Users should have a unique digital identity in order to authenticate to different Information Providers through common federated identifier
- It doesn't support the authentication schemes that are based on attributes (e.g. location, time, scenario, etc.). According to FICAM Roadmap and Implementation Plan [13], Attribute Based Access Control (ABAC) model is recommended for managing access to information and services among organizations that require a restrictive access control [13].
- Use of VPNs raises additional security risks and attack surfaces that need to be taken in consider and additional VPN security features need to be applied to mitigate such risks.

(4) Organizational Owned and Managed – Personal Use Enabled Implementation

In this implementation, mobiles belong to organizations and are issued to users. Such an implementation is similar to fully managed implementation; however, it required the use of Mobile Application Manager to manage the isolated protected space (i.e. container) on the mobile device. Applications are installed and managed on the mobile device by the MDM. MDM can also blacklist specific applications, wipe the protected container, or wipe the whole device, if deemed necessary. In this implementation, applications are protected and running within isolated environment. Thus, the usage of applications downloaded from third-party application store is enabled, providing more convenience for users. As per our evaluation, we realized that such architecture suffers from several weaknesses, including but not limited to:

- Most of the security controls are applied through MDM. Thus the implementation is dependent on the specific implementation of the MDM.
- It doesn't support the authentication schemes and access control based on based on attributes (e.g. location, time, scenario, etc.).
- Requires enhanced integration of EMM/MDM solutions with mobile threat intelligence services.
- Typically, MDM doesn't have the ability identify vulnerable mobile devices or vulnerable components.
- Doesn't support integrity measurements capabilities
- Stronger mechanisms for information security, authentication, and authorization need to be considered. For example, Sensor data and integrity measurements of the mobile device could be integrated to support the authentication process and provide more granular access control based on assurance conditions.

The MSRA implementations do not explicitly reflect their use cases. It is also important to highlight that Canadian use-cases are much more extensive than MSRA use cases. The Canadian use cases are not published yet, so they are not accommodated in this document.

2.4.3 Federal Mobile Computing Security Baseline

Federal The Federal Mobile Computing Security [38] baseline was issued by Department of Homeland Security (DHS), the Department of Defense (DoD), and the National Institute of Standards and Technology (NIST) to develop a mobile security baseline based on the Reference architecture described in section 2.4.2, and Mobile Computing Decision Framework (MCDF) described in section 2.4.1. Federal Mobile Computing Security Baseline document also includes an overview of the MCDF and Reference Architecture [33] [37]. The mobile security baseline was developed by cooperative efforts of experts from NIST, DHS, DoD, Department of Justice, GSA, and MTTT [38].

The primary goal of the Federal mobile computing baseline is to map MCDF, reference architecture, and security baseline into a comprehensive guide. This guide could be used to define organizational requirements, select appropriate mobile architecture, and then applying security controls defined in the mobile security baseline [39].

The Federal Mobile Computing Security baseline identifies four key security services that require improvements to assist in the adoption of secure mobile technologies into federal environment, which include the following controls: Mobile Device Management (MDM), Mobile Application Management (MAM), Identity and Access Management (IAM), and Data Management. Federal Mobile Computing Security baseline follows NIST standard and guidelines, and focuses exclusively on Federal employee use cases, referred to as "Federal Employee Operating Agency-Controlled Mobile Device to access moderate impact systems on a federal network" [38] by relying on MDM, MAM, IAM, and data management as the core security controls. MDM is used to address the risks from the mobile device itself. MAM and IAM security controls are used to address risks from malware, untrusted/compromised mobile applications, and to set requirements for user and device identification, and access control. Although the federal mobile computing security baseline for federal use case covers some important security controls, this baseline suffers from several weaknesses, including:

- Lack a comprehensive architecture that clarifies the core architecture components, the role of each component, which controls apply to which elements, how each component utilizes the controls to reduce potential risks, and the formal interaction process between the system components forming a barrier to mitigate risks against the system.
- Lacks of vulnerability management processes for mobile operating system including version updates, integrity measurements, etc., leaving the operating system layer a potential attack surface.
- BYOD scenario is not taken into consideration
- Stronger mechanisms for data security, authentication, authorization decisions, and access management need to be considered.

2.4.4 The Definitive Guide To Enterprise Mobile Security

The Definitive Guide to Enterprise Mobile Security issued by BlackBerry in 2015 [40], provide a strategic overview of potential security risks organization are facing today in the mobility environment. The guide tailored for business, government, and IT decision makers. It provides recommendations for security architecture planning, as well as recovery strategies in case breaches occur. The guide also provides a number of case studies from private and regulated sectors (e.g. government, financial institutes, etc.), highlight their security gaps, and discuss

BlackBerry security technologies and solutions used to address security weaknesses within those organizations. In addition, the guide provides recommendations, guidelines, and best practices for mobility management in regulated sectors including government and financial institutes.

The guide focuses on the security requirements that should be included in mobility management solutions to qualify them to be used in government sectors. The requirements are classified into Extreme Mobile Device Management, Extreme Mobile Application and Content Management, Extreme Access Control and Policy Enforcement. According to the guide, Extreme Mobile Device Management should include the following capabilities: authentication controls, encryption technologies, containerization, and device wiping capabilities, remote locate/lock capabilities, whitelisting, blacklisting, and over-the-air management and configuration. Extreme Mobile Application and Content Management should include the following capabilities: strict usage policies, private application store, secure middleware or cloud, monitoring console, and auditing and reporting functionalities.

The BlackBerry Enterprise Mobility Management (EMM) suite combines MDM, MAM, MCM, IAM, mobile security and containerization. Although the BlackBerry EMM suite combines major security capabilities, BlackBerry EMM has limited support for third-party services such as Identity and Access Management (e.g. FICAM). Such limitation makes it hard to integrate with other security services and EMM solutions in order to enable effective response and recovery capabilities. In addition, BlackBerry did not provide a comprehensive framework that addresses all the ecosystem components; however, the Blackberry EMM suite addresses only the Enterprise mobile management infrastructure component within the environment. As such, while PSG-MAMF is influenced by the guide, it does not adopt the technologies recommended in the guide. As a result, the PSG-MAMF remains an open architecture.

2.4.5 Enterprise Mobility Management (EMM) Suites – (Different Vendors)

There are many vendor approaches for enterprise mobility management (EMM) that focus on identity and access management, and content security. According to the Gartner Report “Magic Quadrant for Enterprise Mobility Management Suites” in June 2017 [41], mobility management approaches should utilize MDM, MAM, and at least one of MCM or IAM functionalities to be considered an EMM suite [42].

The National Information Assurance Partnership (NIAP) has invested in developing technology-specific security requirements that recommend technologies and security controls for mobile devices, applications, and mobility management solutions. The NIAP requirements were adopted by different vendors including Apple, Microsoft, MobileIron, and Samsung. Their aim was to develop mobility products with enhanced security and mobility management functionalities.

The Gartner report [42] highlighted the leading vendors in the Enterprise Mobility Management technology, which are: BlackBerry, IBM, MobileIron, and VMware. Although some of those vendors are leaders in mobility management industry, the lack of integration capability raises the need for comprehensive framework that covers as much of the ecosystem components as possible while integrating effective security features in mobile devices stack (hardware, firmware, software, and applications).

2.4.6 Practice Guide – Mobile Device Security

The NIST SP 1800-4 Cybersecurity Practice Guide addresses the challenges of securely deploying and managing mobile devices in enterprises. The project was implemented by National Cybersecurity Center of Excellence (NCCoE) at NIST, along with other partners and vendors that are leaders in mobility management industry, including: Intel, Lookout, Microsoft, and Symantec.

The proposed architecture uses standards-based, commercially available products from vendors, which considered an early effort of integration between different solutions and products provided by different vendors. The architecture would be helpful for organizations and aiming to implement an enterprise mobility management (EMM) solution, while moving part of their mobility management solution into a public cloud [43] [44].

NIST practice guide provides two different architecture, cloud and hybrid. The cloud architecture uses public cloud for data storage and mobile devices management services, while the hybrid architecture place potion of the data, management services, and physical equipment within the enterprise infrastructure.

Although NIST Guide doesn't focus on regulated sectors (e.g. government), and doesn't address organizationally owned devices and BYOD scenarios directly, it covers security controls and standards that may be integrated with existing infrastructure within government organizations to mitigate intrusion risks.

NIST project support three major security capabilities that are required for mobile device security and trustworthy, which are: device integrity, isolation, and protected storage [4]. NIST SP 800-164 provides deep insight into integrity, isolation, and protected storage requirements [4]. In addition, the project adopts other standards and recommendations built upon principles creating a comprehensive list of security functionalities and capabilities, including: protected storage, protected communication, containerization, device integrity checks, automatic and regular device integrity and compliance checks, automated alerts for policy violations, asset management, authentication of users, and auditing and logging capabilities [44].

In order to address such security functionalities and capabilities, NIST project adopts a set of security technologies by integrating solutions from different vendors, including: "Microsoft" (i.e. EMM, cloud platform, configuration management, and Outlook & Community Portal Mobile Applications), "Intel" mobile device, "Symantic" digital certificates, and "Lookout" malware and OS integrity detection [43][44]. Integrating such solutions would result in better understanding of the risks tied to mobility management and mitigation strategies. The main goal of the framework is that mobile devices, operating system, and applications storing, sharing, and processing information to be configured and implemented securely, mainly via EMM. NIST SP 1800-4 Draft describes the system components for both cloud architecture and hybrid architecture. In addition, the NIST SP 1800-4 Draft discusses also the benefit of both hybrid and cloud architecture and the set of security capabilities supported by each of them.

NIST project is considered one of the early efforts toward developing a framework that integrates different security technologies from different vendors, and applying existing security principles, standards, and recommendations [43][44]. Such efforts shows that the world is starting to realize the importance of secure mobile application management framework and the need for comprehensive framework that supports as much of the security requirements listed in this document. However, the NIST framework suffers from the following weaknesses:

- The architecture is not focused on government organizations security requirements. Additional security controls and principles need to be further investigated.
- The NIST project is focused on enterprises that are considering the use of cloud services and the security implications.
- The architecture does not address organizationally owned devices and BYOD explicitly.
- Stronger mechanisms for authentication, authorization decisions, and access management need to be investigated (e.g. FICAM). Sensor data and integrity measurements of the mobile device could be integrated to support the authentication process.
- It does not support authentication schemes that are based on attributes (e.g. location, time, scenario, etc.). According to FICAM Roadmap and Implementation Plan v2.0 [FEDCIO2] (2011), Attribute Based Access Control (ABAC) model is recommended for managing access to information and services in organizations that require a restrictive access control [13]

2.4.7 Mobile Device Security for Enterprises (MDSE) project

The Mobile Device Security for Enterprise (MDSE) project is still under way. NIST announced the MDSE project in February 2018 [45], as mobile device security project develop mobile architectures that can be tailored and adopted by organizations to deploy mobility management programs in their organizations.

As announced by NIST, the project should result in practice guides that explain the commercially available management technologies that can be integrated into single solutions that manage and secure mobile devices in different usage scenarios [45]. MDSE develops different architectures based on enterprise services and mobility management requirements. Each instantiation will include the following services [46]:

- A network confidentiality protection mechanism (e.g. Virtual Private Network, VPN)
- Device-side security technologies including secure containers and malware detection.
- A variety of mobile security technologies including EMM, application vetting, virtual mobile infrastructure, and mobile threat intelligence system.
- A set of security controls based on industry and government standards (e.g. NIST, NIAP, Cloud Security Alliance, and ISO).

Collaborators for this effort include: MobileIron, Lookout, Kryptowire, Appthority, and Qualcomm [46].

2.5 Summary of security threats and identified Gaps

Threats and vulnerabilities associated to government deployed mobile devices and application exist across all segments of the mobility ecosystem. As discussed throughout this document, they were identified from “Mobile Threat Catalogue” draft by NIST, NIST IR8144 “Assessing Threats to Mobile Devices & Infrastructure”, and “Top Threats to Mobile Computing” by Cloud Security Alliance (CSA). The threats reviewed include those due to lack of defensive mechanisms and technologies, or the constantly evolving technologies.

The United States Government Accountability Office (GAO) provided a detailed list of threats and vulnerabilities that exist and their impact on the security of mobile devices. GAO also identified the security controls and practices currently available for devices, applications, and user security controls which mitigate the risks associated with them, including: user authentication, application vetting, encrypting information stored on mobile device, and mobile device integrity validation. The GAO document recommends guidelines in terms of mobile device adherence to minimum security requirements, cryptographic modules that may include both hardware and software components, and managing and monitoring devices, In additions GAO document include guidelines for establishing policies to regulate the usage of mobile device, applications, and user behaviour and activities [47].

NIST SP 800-124 and ITSG .80.001 provided an overview of the major security concerns and threats associated with mobility, and recommendations for mobile device security management by providing mobility control guidelines to mitigate the security concerns [5] [3].

The Federal Chief Information Officer Council (CIO) also discussed some of the common mobile threats and mitigation strategies. CIO divided the threats into 4 areas based on threat: mobile device, mobile applications, agencies infrastructure, and access networks. The mitigation strategies include operational, technical, and security controls applied to address common security threats and attacks against different components of the mobile architecture [38].

Despite the existing standards, security controls, security technologies, EMM products provided by different vendors, security gaps still exist. The recommendations and relevant studies already exist are addressing specific components of the mobile ecosystem, leaving other components a potential attack surface. This requires a comprehensive framework with an integrating security functionalities and technologies that aim to improve mobility management architecture, mobile device security, applications security, by addressing as much of the security gaps existing in mobile ecosystems.

Highlighted gaps in terms of mobile device security include:

- Inability to monitor mobile device activities and identifying exploitable vulnerabilities.
- Inability to verify integrity of mobile device and applications. In addition, other lower-level components require such verification including baseband, software, and firmware.
- Inability to extend organizational access rights and enforces security policies on the mobile device framework.
- More attention needs to be given to mobile device booting to ensure that the mobile device never boot in malicious or unexpected state, and detect device compromise.
- Lack of protected storage and containerization approaches.
- Lack of strong authentication mechanisms including local and remote authentication.
- Inability to use existing authentication mechanisms on mobile devices (e.g. Personal Identity Verification, PIV)
- Limited attention to Bring Your Own Device (BYOD)

Highlighted gaps in terms of mobile applications security include:

- Lack of recommendations, standards and guidelines for mobile applications development lifecycle for developers.
- Lack of defined metrics that can be used by application developers and security testers.

- Limited adoption of rigorous application vetting processes
- Lack of application stores security criteria.
- Limited attention to well-defined vetting tools and services for government organizations.
- Lack of adoption of trusted execution environments for organization specific applications.
- Lack of access rights management and policy enforcement.
- Lack of real-time monitoring for applications to monitor all applications activities, performance, and timely notification of applications affected by vulnerabilities.
- Limited authentication capabilities
- Lack of security controls that define how applications handle information for access, storage, usage, and sharing on mobile devices.
- Lack of encryption keys management strategies.

Highlighted gaps in terms of mobility management solutions include:

- Limited attention is given to government requirements and needs for mobility solutions.
- Most of the existing security controls are applied through EMM solutions or products provided by vendors. Vendor lock-in makes the controls dependent on the specific implementation and limited to supported functionalities. While in most cases, the available products are not enough to fully address the security requirements for government organizations.
- Implement industry standard mobile security controls and existing security technologies in order to reduce long term costs and decreasing the risk of vendor lock-in by integrating solutions provided by different vendors.
- Limited focus on government organizations security requirements.
- Limited integration of different solutions provided by different vendors and their integration with mobile threat intelligence services.
- Limited ability of current mobility solutions to identify vulnerable mobile devices or vulnerable components.
- Limited ability of current solutions to detect attacks against mobile devices.
- Limited support of integrity measurement capabilities.
- Limited ability of verifying mobile operating system version, and insurance that the mobile device always running the most recent operating system version to ensure that the device is benefiting from security improvements that provide resilience against unknown vulnerabilities.
- Most of the current mobility solutions do not support strong authentication and authorization mechanisms.
- Only few existing solutions support authentication schemes that are based on attributes (e.g. role, location, time, scenario, etc.). As per our evaluation, the “Attribute Based Access Control (ABAC) model” proposed by NIST is the only schemes providing a restrictive access control based on attributes [13].

- Lack of sensor data and integrity measurements integration to provide stronger authentication and granular access control based on assurance conditions
- Lack of implementation of federated identity management. This doesn't only involve modernization of IT systems, it also includes tidies effort to change IT culture.
- Lack of integration between EMM solutions with other security systems and frameworks to enable enhanced security functions and recovery capabilities.

In summary, the identified threats and security gaps raises the need for a single comprehensive framework based on existing standards and recommendations that can provide recommendations for the integration of different mobility solutions and security technologies in order to ensure a baseline security level for mobility management within government organizations and public safety community.

The PSG-MAMF proposed in this study, proposes a level of integration that is not available in other frameworks identified in other research studies (e.g. NIST) or products supported by vendors (e.g. Blackberry, AirWatch, etc.). PSG-MAMF attempts to fill the gaps listed above by presenting an integrated solution that explores security and management features for mobility management. PSG-MAMF basic principles are discussed in details in section 3.

3 Definitions, Assumptions, and Basics Principals of PSG-MAMF

PSG-MAMF attempts to define public safety grade requirements and considerations. The PSG-MAMF and public safety security requirements have been developed based mainly on a set of assumptions and principals. The PSG-MAMF presents detailed analysis and design of the following assumptions and principals:

3.1 PSG-MAMF assumptions

PSG-MAMF was developed upon the following assumptions:

(1) The availability of reliable high-speed data applications access to information and real-time content.
(2) The availability of access to shared services such as records management and Computer Aided Dispatching (CAD).
(3) A communication backbone across the nation without interruption, via permanent or temporary infrastructure, being commercial or private, LTE, WIFI or other forms of access
(4) Communications may take place across PSBN or commercial network services (CNS), thus, communication between PG-MD and PSG-II cannot be trusted since there is no guaranteed control over the security of the commercial CNS. Thus, potential communications over un-secure channels is a basic assumption to be considered when planning the security of PSG-MD and PSG-MA.
(5) PSG-MAMF builds on existing and/or evolving policies, where the Information Providers defined their own policies, rules, and terms of use to be enforced on users accessing their information.
(6) Mobility management solutions available by different vendors are inadequate for public safety mobility management and security requirements. Public safety organizations require fairly comprehensive multi-fencing approach that can address all the security threats in all system levels.

3.2 PSG-MAMF principals

PSG-MAMF has been developed based on principals that are shared by most individuals and organizations involved in the technical aspects of the PSBN development. The two main principles of PSG-MAMF are shown in We list the relevant principals hereafter to provide the reader with the proper meaning of technical terms, technologies, and approaches. Table 2 summarizes the key security controls and basic principles of PSG-MAMF.

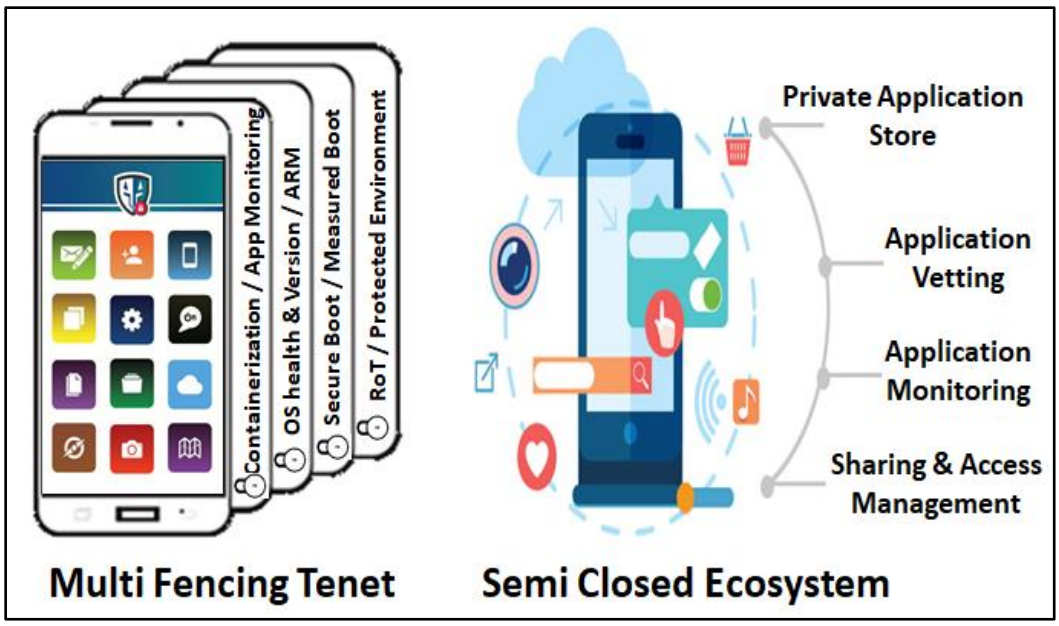

Figure 2 Main Principles and Security Services of PSG-MAMF

3.2.1 Public Safety Broadband Network (PSBN):

The wireless access network that is used to reach the public safety network infrastructure has been called Public Safety Broadband Network (PSBN) by most involved Canadian organization. PSBN represent the entire national infrastructure that might utilize different wireless access technologies at different situations. Therefore, PSBN is not limited to private LTE, instead, private LTE represent only one form of RAN accessibility. Typically, Radio Access Network (RAN) is used as a last-mile to reach mobile responder in the field, but the PSBN itself is a much larger network.

3.2.2 Opportunistic RAN Connectivity

Current technologies projected to build-up RANs include, commercial cellular service (at multiple spectrums), private cellular (the 700 MHz), unlicensed cellular (LTE-U), WiFi (802.11 series and beyond), DSRC (connected Vehicle 5.9 GHz), Ultra-Wide-Band (UWB), etc. PSBN hand-held equipment shall use combinations of available wireless access media based on availability and security. For instance, a responder to an incident inside a university campus might use his/her cellular connectivity outdoors, but the device could maintain a secured connectivity using pre-set WiFi access as soon as the responder moves indoor. Hence, hand-held devices are typically opportunistic in picking the best wireless access medium as long as security and privacy requirements are fulfilled.

3.2.3 Interoperability

Considering the wide scope of applications, devices, services, and information, PSG-MAMF, defines interoperability as:

> "Interoperability is the ability of an entity or technology (device, application, or service) to share itself or its asset(s) by making itself or its asset(s) (re)usable to another trusted entity or technology, typically, through secured means."

For example, Agencies must ensure the following:

- Creating policies, procedures, and standards for interoperable emergency communications requirements (e.g. use of existing nationwide interoperability frequencies, and incident management).
- Maintaining network interoperability across the PSBN
- Ensuring all network components (hardware/firmware/software) are in compliance with the network interoperability requirements
- Managing nationwide interoperability requirements for deployed applications
- Defining interoperability requirements for mobile devices
- Enabling smooth migration of public safety information to maximize interoperability. In addition, interoperability between different classifications systems must be taken in considers when information migrate between countries or between different jurisdictional domains

3.2.4 Multi fencing Tenet:

PSG-MAMF uses a multi fencing approach to enhance security. The multi-fencing approach provides sequence of security layers to capture any vulnerability that passed through early fences, results in improved risk mitigation, as shown in Figure 3. In a multi-fence approach failure of one security mechanism is localized and does not compromise the fidelity and operability of the entire system. The multi-fencing approach includes mobility management, compartmentalization, Roots of Trust, Access Right Management, and application vetting approaches.

3.2.5 Mobility Management Frameworks

PSG-MAMF support mobility management security technologies such as Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Information Management (MIM) solutions to address addition security requirements and provide a real time management and monitoring for the device, applications and information residing the mobile device.

3.2.6 Containerization Approach

Containerization is the concept of partitioning applications, information storage, access, and providing encryption in a way that limit the access to information to only the intended user/application/device for the intended period of time only. Containerization is used by PSG-MAMF to mitigate the risk of hostile information exposure.

Simply, each application and its related information are kept secured and isolated from other applications on the mobile device. The containers are usually secured using cryptographic techniques where the PSG-MA and information will be encrypted and processed only within the container. Separation ensures that public safety information is separated from user's personal

information on the same device. The tenet of containerization is highly adopted through this document and it provides the following advantages:

- Separation of information from application allows Information Providers to set the access rules without any worries about validating application use of information.
- In the case of compromised security, information being exposed is limited to the container being compromised limiting the impact of security attacks.
- Malicious applications that are initially undetected still cannot impact more than the information it had already accessed

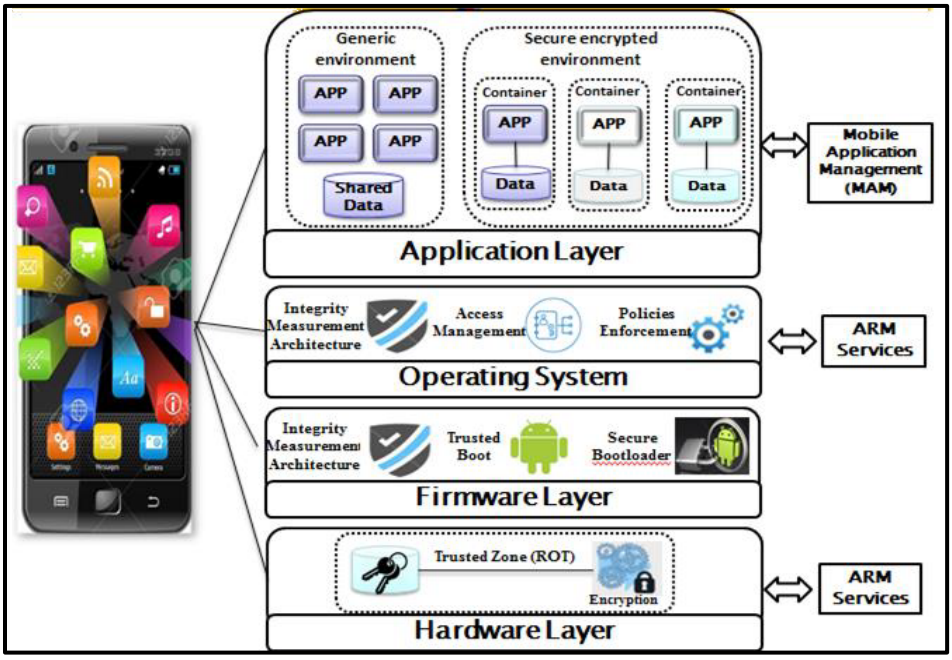

Figure 3 PSG-MAMF multi-fencing security principles

3.2.7 Root of Trust

Root-of-Trust (ROT) is used to confirm and guarantee fidelity of system elements from smaller pieces to larger ones by establishing a chain of trust. ROT is typically used to ensure the trustworthiness of hardware, firmware, and software that will result in a secure and trustworthy device. In general, ROT provides the following services:

- Establish a chain of trust beginning with a Root of Trust implemented and stored secure by hardware, software, or firmware.
- Provide the device with the ability to provide assurance by issuing device state assertions
- Provide a set of security services including storing cryptographic keys, authentication credentials, and other sensitive information.

3.2.8 Semi-closed Ecosystem

PSG-MAMF controls public safety applications system by controlling the entry-exit points through a semi-closed ecosystem. The ecosystem includes set of capabilities and processes to provide a full lifecycle management of application. Same solution has been followed by FirstNet [48]. The PSG-MAMF ecosystem supports the following key services:

3.2.8.1 Public Safety Grade-Application Store (PSG-AS)

PSG-MAMF supports a public safety application store that can provide secure vetted applications from trusted source. The PSG-AS provide public safety users with a way to discover, download, update, rate, and manage applications. The ecosystem locks the accessibility to a Public Safety Application Store. FirstNet has also launched an application store to serve as a home for public safety applications [49].

3.2.8.2 Application vetting

PSG-MAMF provide a framework for application vetting before making them available on the PSG-AS as a necessary step to improve system security and guarantee reasonable levels of applications coherence with the applied public safety policies. PSG-MAMF increases the robustness of the application testing process by relying on different testing strategies including automated assessment and human assessment.

3.2.8.3 Management and Monitoring of Applications

PSG-MAMF supports Mobile Application Management (MAM) approach to provide a real time management and monitoring for mobile applications and its related information residing the mobile device. MAM provides the agencies with tools and interfaces to remotely control their applications and information on the mobile asset.

3.2.8.4 Applications sharing and access management

Applications can be shared between different agencies by being distributed from public safety application store (PSG-AS) as a source. Access to applications can be then managed dynamically based on user role, agency, location, scenario, and other qualifying attributes.

3.2.9 Federation of identity and authentication management

Federation is a centralized organization formed by the link of government and federal agencies, where each agency sets and retains the control of its own users and assets. Public safety organizations need to properly identify, authenticate, and authorize users before granting them access to application, information, and services. Federation can provide such capabilities resulting in improvement of availability, interoperability, confidentiality, integrity, and sharing of information. The centralized organization in the PSG-MAMF responsible for managing information and services of group of agencies is referred to as Public Safety Grade – Information Infrastructure (PSG-II), while the centralized source responsible for managing and distribution of applications is referred to as Public Safety Grade – Application Store (PSG-AS). Access to both

PSG-II and PSG-AS is managed and controlled by the centralized federation of identity and authentication.

3.2.10 Access Right Management (ARM)

PSG-MAMF facilitates information access and sharing following an Access Rights Management (ARM) mechanism. As information move from its origin to destination, PSG-MAMF maintains tight monitoring of the information to ensure information is kept secured, policies are extended to mobile framework, and information usage complies with the handling requirements. Therefore, information can only be used as intended by the information custodian. Assertions and certificates are exchanged to monitor and guarantee adherence to set policies. ARM can also apply policies such as Time-To-Live and self-destructive.

The main objective of the ARM is that security rules and policies are defined by the Information Providers, managed on a central system, and transferred with the information in such a way that rules and policies can still be applied even when the server is not accessible or where there is not network connectivity at all.

3.2.11 Court Admissible Logging and Record Keeping

PSG-MAMF should support court admissible logging and record keeping features in order to ensure that audit logs are used to record all user and system activities, and information security and operational events including activities on networks, applications, information, and systems. Law enforcement agencies, for example, may likely require logs and records to be used as evidence admitted in a court. PSG-MAMF shall store logs and records encrypted in protected storage, restrict access to them with need-to-know privileged access, and apply the proper controls to be protected from unauthorized access, alteration, disposal of logs without proper privilege in order to preserve integrity of logs and records.

Table 2 Security control and basic principles of PSG-MAMF

Security Principles	Security Capabilities	Capabilities Examples
Data Protection	Protect data at rest: "Protected Storage"	• Device encryption • User-Device authentication • Containerization • Trusted key storage • Remote Lock/wipe • Access Right Management
	Protect data in motion: "Protected Communications"	• Virtual private network (VPN) including per-app VPN is recommended. • Encrypted information distribution.
	Protect data in process "Protected execution"	• Encrypted memory space • Protected execution environments

		• Access Right Management
Data Isolation	Isolating Public Safety Information from User private information	• Virtualization • Sandboxing • Containerization • Protected execution • Data tagging/Metadata • Baseband isolation
Device Integrity	Device Integrity measurement checks	• Boot validation: Secure Boot, and Measured Boot • Verified Applications • Verified application and OS updates • Verified OS health • Continuous Integrity Monitoring • Policies compliance integrity verification • Baseband integrity checks
	Device Integrity Evidence Reports	• Trusted integrity evidence Reports • Attestation
Monitoring	Monitor, Detect, Report	• Compliance verification • Applications life cycle monitoring (e.g. downloads, updates, usage, services usage, permissions usage, application behaviours, and performance monitoring) • Malicious behaviours detection • Root and jailbreak detection • Real-time monitoring • Auditing and logging
Policies Enforcement	Access Right Management Enterprise Mobility Management	• Access Rights enforcement on information (storage, access, usage, and sharing) • Enforce appropriate actions on applications (updating, freezing, deleting, event management, remote selective wipe of information)
Logging and Reporting	Record all Activities, Protect logs	• Record user and system activities, and information security and operational events. • Log activities on networks, applications, information, and systems.

		• Integrity of logs and records using protected storage, multi-factor authentication, digital signatures, backup of logs, and logging access to logs. • Logs and reports usage as evidence admitted in a court
Identity and Authentication	Authenticate each single entity in the system Enhanced Authentication mechanisms	• User-Device Authentication • SIM-Network Authentication • User-Device-Network Authentication • User-Device-Infrastructure Authentication • Authentication schemes based on attributes "Attribute Based Access Control (ABAC)" (e.g. role, agency, location, time, scenario, etc.). • Authentication schemes based on Sensor data and integrity measurements of the mobile device. • Credentials secure storage and usage

4 PSG-MAMF Architectural Components

Architectural components of the PSG-MAMF can be viewed in the following major System Components illustrated through this section. The System Components consists of human actors involved in the system either directly or indirectly, and hardware and software components that complement the system architecture by interacting together to perform security services. Each entity in the system architecture plays a key role by adding a security capability to the framework to reduce a potential risk and mitigate security vulnerabilities. The overall objective of the PSG-MAMF system components is to ensure the same levels of security and confidence in information use on wired-protected infrastructure apply to the mobile infrastructure as well.

The PSG-MAMF system components include physical entities involved in the system either directly or indirectly. Each entity represents a vital aspect in the overall system architecture and has specific roles and responsibilities which support information sharing and the security framework. Physical entities involved in the PSG-MAMF include: Application Developer, User, Framework Management and Administration, and Information Provider. Figure 4 represents the PSG-MAMF system components, including the physical entities of PSG-MAMF architecture.

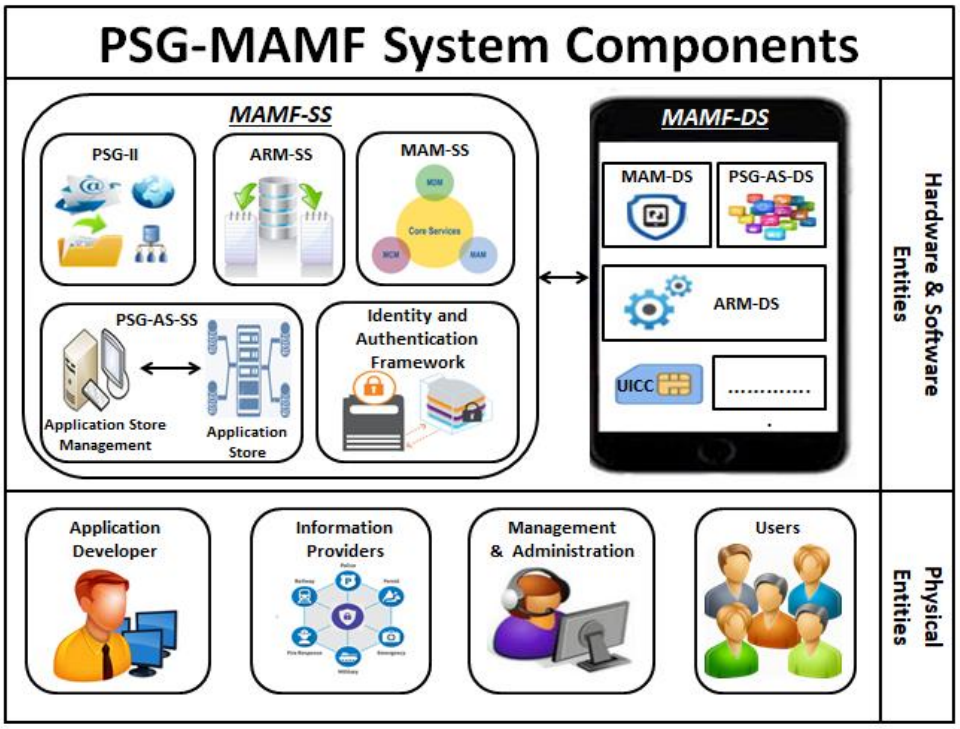

Figure 4 PSG-MAMF System Components

The PSG-MAMF system components include also hardware and software components that complement the proposed system architecture. PSG-MAMF system components can be divided into MAMF Support System (MAMF-SS) and MAMF Device System (MAMF-DS), as shown in Figure 4. The MAMF-SS could be viewed as a part of the public safety infrastructure that supports the Public Safety Grade-Mobile Application Management Framework (PSG-MAMF).

MAMF-SS can be a platform implementation on server farm, cloud service, or other form of data center management. MAMF-SS consists of the Public Safety Grade-Application-Store-Support System (PSG-AS-SS), Mobile Application Monitoring Support System (MAM-SS), the Access Rights Management Support System (DRM-SS), Identity and Authentication Framework, and Public Safety Grade Information Infrastructure (PSG-II). The MAMF-DS, on the other hand, is implemented on the Public Safety Grade Mobile Device (PSG-MD). The MAMF-DS consists of the Public Safety Grade Mobile Device (PSG-MD) itself, the Public Safety Grade-Application-Store-Device System (PSG-AS-DS), the Mobile Application Monitoring-Device System (MAM-DS), Sensors, UICC (e.g. USIM, HC-USIM, or eSIM), and other essential parts as discussed later in sections 6.4 and 6.5.

4.1 Application Developer

Application Developer is an entity or individual developing Public Safety Grade mobile applications (PSG-MA) as referred throughout this study. The Application Developer could be an employee of an agency, a non-profit organization, a Small-to-Medium Enterprise (SME) or any other entity or individual developing public safety applications. Naturally, and Application Developer is interested in publishing his applications in the Public Safety Grade Application Store (PSG-AS). The Application Developer has to maintain a high level of security, fidelity, and integrity in published applications to be qualified as a PSG-MA. Typically, the Application Developer is responsible for the following:

- Uploading the applications to be evaluated and scored before going through a Security Assessment and Authorization (SA&A) process that can take advantage of priori tested applications. Application will also be vetted and reviewed by the Application Store Management System, and then published to the PSG-AS to be available for public safety users from trusted sources.
- Improving the applications to be accepted by the PSG-AS according to predefined requirements, and known policies and regulations defined by public safety organizations.
- Updating the applications as needed in order to provide the Users with effective application functionalities and to mitigate and resolve potential issues that arise over time due to operational use.

4.2 User

Users are referred to public safety users that may use PSG-MD to perform public safety day to day operations. Users may use PSG-MD in form of Public Safety Owned Device (PSOD) or Bring Your Own Device (BYOD) within the public safety community to assist them in their jobs and emergency situations. Users can use PSG-MD to access the Public Safety Grade – Application Store (PSG-AS) to download applications as needed to perform their duties. In addition, users may use Public Safety Grade – Mobile Applications (PSG-MA) to access information and services in Public Safety Grade-Information Infrastructure (PSG-II). Thus, user, PSG-MD, and PSG-MA need to be authenticated before granted access to network and PSG-II. The authentication process is done by another system component, namely, “Identity and Authentication Framework”. Further, it is necessary to manage user’s access to PSG-II by relevant policies, access rights, and predefined attributes. The access management process takes

place by another system component, namely, "Access Right Management". User access to PSG-II takes place over secure communications regardless of the wireless medium.

The Public Safety Grade-Information Infrastructure (PSG-II) provides responders with a formal way to access the needed information by remaining in compliance with policies and regulations set by Information Providers as described in section 4.3. Users are required to present their identity, credentials, and qualifying attributes to gain access to needed information and services. In other words, the Information Providers will grant access only to users who have the appropriate identity, qualifications, and credentials.

The "Mobile Application Monitoring" system component provide tools such as mobility management frameworks that are supported by Mobile Device Management (MDM), Mobile Application Management (MAM), and Mobile Content Management (MCM) platforms to manage users access to Public Safety Grade Information Infrastructure (PSG-II), and monitor user's activities on PSG-MD at all times as described in section 4.10.1. In addition, real time monitoring maintains guarantees of fidelity and integrity of the user, PSG-MD, and PSG-MA, and support situational awareness and contextual access decisions. Figure 5 represents the user direct and indirect interaction with system components in order to download applications, and access information and services within the PSG-II. The user interaction process including user authentication and user access management are discussed in details in section 5.2 and 5.3.

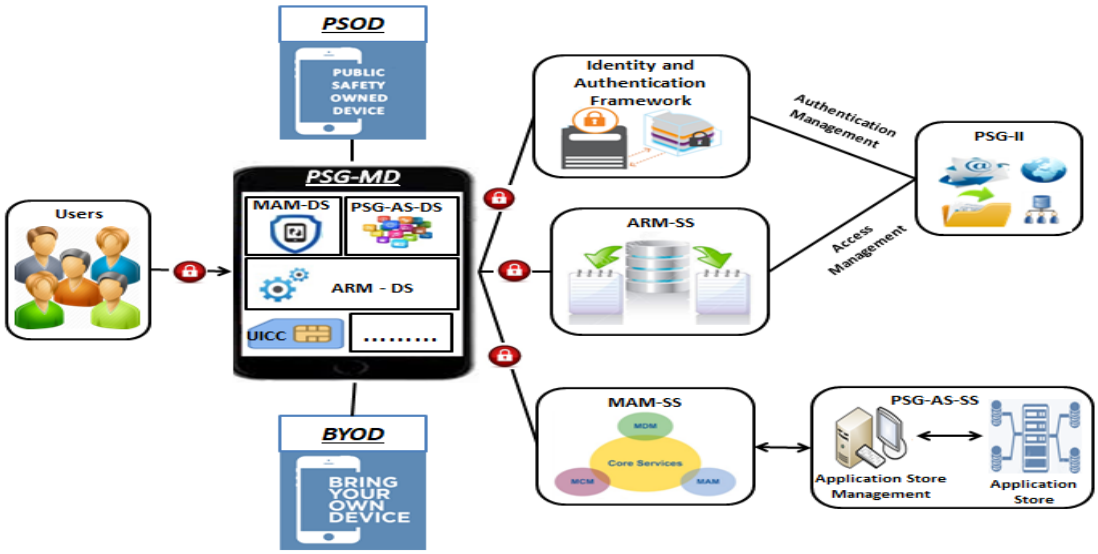

Figure 5 User Interaction

4.3 Information Provider

Information Providers are the organizations, including government agencies, law enforcement agencies, and other organizations; that are responsible for granting access to information and service. Information Provider is any entity that holds the responsibility and decision making authority of handling information throughout its life-cycle including creating, classifying, restricting and managing (e.g. access, usage, storing, and sharing), maintenance, and housekeeping of the information asset. Information Providers hold the legal authority to set the rules and policies on handling its information. The responsibility of the Information Provider

expands beyond the access and sharing rules imposed on the Public Safety Grade Information Infrastructure (PSG-II) and covers the information use within the mobile infrastructure and temporary information access and storage with all its elements. As an example, an Information Provider shall grant the use of its information to device, users, and application, of particular privilege and request that information be used only in granular forms. The Information Provider may grant only temporary storage or impose other rules the Information Provider deem necessary to maintain its legitimate control over information.

PSG-MAMF aims to provide the guarantees to the Information Providers that the rules and policies set are extended to the mobile framework. The Access Right Management (ARM) system component provide and maintain the handling of information and policies enforcement within the PSG-MD as discussed in section 4.9 and 6.4.3. ARM may rely on Roots of Trust to verify the integrity of the PSG-MD, PSG-MA, or any element of the device. ROT may use assertions to communicate the state of the PSG-MD with the Information Providers and inform them about the policies enforcement status.

4.4 Framework Management and Administration

The Framework Management and Administration is responsible for managing, monitoring, and ensuring compliance of the overall system as shown in Figure 6. The most critical requirement for management and administration of the PSG-MAMF is the ability to manage and configure the device, application, and information over the air from a central system (e.g. console windows) by administrators. Most of the mobility management requirements and security features supported by MDM, MAM, and MCM require over-the-air management capability in order to be applied. Over-the-air management allow administrators to manage devices by providing configuration manage, real-time monitoring, locking/wiping, push applications or updates, manage policy settings, and ensure device integrity of both PSOD and BYOD. Hence, over-the-air capability should be a fundamental tool for management and administration. The Management and Administration has three major roles in PSG-MAMF as following:

4.4.1 Compliance Management and Administration:

Information Providers have a set of defined regulations and security policies to manage users, devices, and applications access to information and services. The PSG-MAMF should support a strong automated, comprehensive process to control the devices, applications, and users access to PSG-II. Compliance Management and Administration may use features provided by other system components such as MAM-SS tools including MDM, MAM, and MCM management platforms as well as Access Rights Management (ARM) capabilities to perform the following compliance management services:

- Compliance Management and Administration verifies whether the security policies are defined, in place, processed, configured, effective, and not being bypassed.
- Compliance Management and Administration monitors PSG-MD, PSG-MA, and ensure information handling is done properly and policies are enforced in a proper way according to the policies and access rights defined by public safety organizations.
- Compliance Management and Administration should be able to detect any deviations and violations of regulations and policies, detect jail breaking, and identify potential security vulnerabilities. Accordingly, Compliance Management and Administration would take

appropriate actions including revoke, lock, or wipe PSG-MD, or may wipe all public safety information stored on the PSG-MD (e.g. revoke, wipe) in such cases.

- Compliance Management and Administration performs over-the-air management through management console, to control the devices, applications, and information by having remote access to devices to enforce corrective measures such as whitelisting and blacklisting for users and devices, monitoring the device behaviour, and ensure the MAM-DS receives and implements the commands coming from MAM-SS.

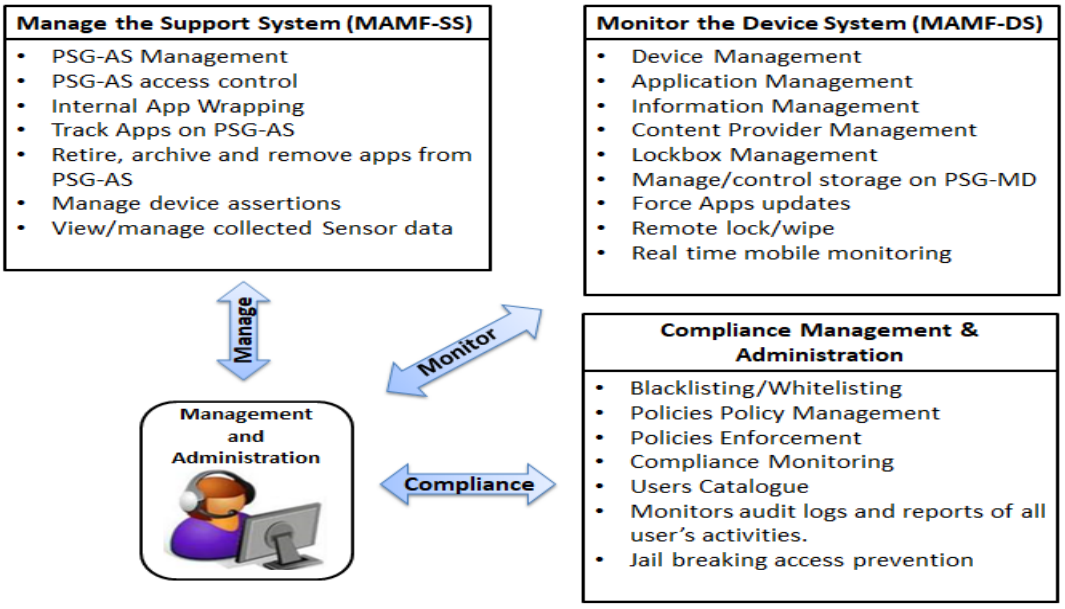

Figure 6 Framework Management and administration functions as part of PSG-MAMF

4.4.2 Application Management and Administration

Application Management and Administration manage applications throughout its lifecycle. Application Management and Administration utilize features supported by MDM, MAM, and MCM platform to perform the following application management services:

- Application Management and Administration manages the application throughout testing, evaluating, uploading, redistribution, updating, and review application performance throughout its lifecycle. During application testing and evaluation, Application Management and Administration need to ensure that appropriate requirements are defined and validating applications compliance to the predefined set of rules and policies. Applications violating known rules and policies are denied redistribution through the PSG-AS; a report to the Application Developer can highlight the reason for such denial. Accepted applications are uploaded to the PSG-AS in order to be accessible for responders.
- Application Management and Administration manages and controls applications running on the PSG-MD by providing a visibility over applications behavior and performance throughout their life cycle. This way Application Management and Administration can

provide maintenance to easily retire, archive and remove applications from PSG-AS when necessary (e.g. obsolescence Applications).

- Application Management and Administration must review Apps updates provided by the Application Developers before allowing applications to be updated. Application Management and Administration can also push updates to responders as deemed necessary.
- Application Management and Administration can enforce policies to enforce users to use PSG-MA effectively and in a secure manner. Consequently, Application Management and Administration is provided by sufficient tools to provision, control, monitor, update, and remove PSG-MA from PSG-MD as deemed necessary.
- Application Management and Administration ensure that applications are isolated using containerization or application wrapping, ensure applications are handling information access, usage, storage, and sharing in compliance with the defined access rights and policies. For example, application cannot access information unless the policy attached to the information grant access to that application, an application cannot leave cache RAM or temp files vulnerable in shared storage or temporary RAM, etc. Application Management and Administration takes the appropriate actions over applications violating such rules and policies.
- Application Management and Administration can take the responsibility of remote power management by adjusting the behaviour of applications running on the PSG-MD according to the current user's context.

4.4.3 Information Management and Administration

Information Management and Administration may use features provided by MDM, MAM, and MCM platforms as well as Access Rights Management (ARM) capabilities to perform the following information management services:

- Provision, manage, and control information access, usage, storing, and sharing on the PSG-MD, as well as information accessibility by other applications.
- Information Management and Administration ensures that PSG-MAs are isolated from other generic applications on the same PSG-MD using code-based approaches such as containerization or application wrapping [50]. The containerization and application wrapping approaches are discussed in details in Annex B, as capabilities of EMM platforms2. Containerization and application wrapping provide granular control and isolations capabilities that support application and information management process.

[2] The containerization approach requires the application's code to integrate with the SDK published by the MDM or MAM vendor. The SDK lets developers build containerization directly into their applications, tying them into the management platform. Thus, applications should be updated to in order to incorporate an SDK. On the other hand, in application wrapping approach, dynamic libraries provided by the MDM or MAM vendor are layered over the application's native binary files after the application is compiled. Thus, application wrapping requires no development

- Information Management and Administration ensures that application wrapping and/or containerization approaches are applied properly, such that applications and their related information are isolated and encrypted, and only shared only among authorized users and defined set of PSG-MA according to valid license.
- Information Management and Administration ensures that information sharing between applications is prohibited and only the intended granular level of information is shared.
- Information Management and Administration ensure information handling and access management takes place according to the access rights and policies defined by public safety organizations and accompany the information throughout its lifecycle. This way, Information Management and Administration guarantees that rules and policies set for handling information are extended to the mobile asset and enforced in a proper way.
- Information Management and administration ensure that information asset imposing Time-to-Live policy is self-destructed and wiped out from application space, memory space, and from each location it reside on the PSG-MD by that time .
- Information Management and administration may have other potential enforcement capabilities to enforce when deemed necessary (e.g. cache clearing).

4.5 Public Safety Grade – Mobile Device (PSG-MD)

The Public Safety Grade Mobile Devices (PSG-MD) can be any intelligent device that can be used on the move while remaining connected to public safety information infrastructure by direct or indirect means. Responders might use either Public Safety Owned Device (PSOD) mobile devices or Bring Your Own Device (BYOD), as described later in section 6.1. In general, BYOD devices require more security scrutiny compared to PSOD.

A device should have a wide range of components and capabilities that qualify it to serve as a Public Safety Grade Mobile Device (PSG-MD), as described in section 6.3 and section 6.5. The PSG-MD can use sensors to collect wide range of data required to assist public safety users in their missions. Further, the PSG-MD contains a Universal Integrated Circuit Card (UICC) that support USIM application or eSIM to connect to network and also can be used as a protected storage on the PSG-MD. Further, a PSG-MD should be able to generate assertions about the state of the device to the MAM-DS to ensure the integrity of the device.

PSG-MD can access PSG-AS in order to download and install applications from trusted source. In addition, PSG-MD can access PSG-II in order to request information and services to assist public safety users in their missions. This requires the PSG-MD to be authenticated before granted access to network, PSG-AS, and PSG-II. The authentication process within the PSG-MAMF takes place through a system component referred to it as “Identity and Authentication Management Framework”, as described in section 4.6. The authentication process is described in details per section 9.2 and 9.3.

---

work, since the application’s codes don’t have to be integrated with the MDM or MAM SDK. This way, the Management and Administration can provide security and control capabilities over applications using management console, without needing to access the source code [50].

Furthermore, additional functions are required to provide security management for a PSG-MD. These functions may include remote management, remote lock, remote wipe, policy enforcement, data tracking and certification, and assertions to ensure device integrity. PSG-MD capabilities and security features are described later in section 6.

4.6 Identity and Authentication Management Framework

PSG-MAMF requires comprehensive method for authentication that consider authenticating each single entity within the PSG-MAMF including the device itself and the user before granting them access to network and PSG-II. In public safety environments, PSG-MD could be shared between different users, and Bring Your Own Device (BYOD) scenario may occur. Hence, an authentication process must consider authenticating both the device and user before granting them access to network and PSG-II.

Identity and Authentication Management Framework is a PSG-MAMF system component that builds on top of LTE to enable a secure User-Device access to network and PSG-II. The framework could be standards based, and can use assertions to exchange User and PSG-MD authentication information during the authentication process. The framework provide a reliable, secure, and interoperable authentication and identity management that aims to identify User-Device access to network and assure appropriate information access. The Identity and Authentication Management Framework supports an authentication process that take place completely on the public safety system side.

The authentication and identity management framework manages User-Device access by managing the identities, credentials, and qualifying attributes on behalf of public safety organizations, and simplifies applications development by standardizing on the mechanics of User-Device authentication and identities management.

Public safety organizations need to join the authentication and identity management framework so that User and PSG-MD can be authenticated, federated, and trusted to other organizations. This requires the framework to handle the security policies defined by different public safety organizations. However, to enable interoperable use of the identity information available from the authentication and identity framework, a set of attributes and their corresponding format must be agreed upon by the public safety community. PSG-MAMF would follow the precedent efforts and initiatives that aim to deploy a reliable, secure, interoperable authentication management framework including National Institute of Standards and Technology (NIST), Federal Identity, Credential, and Access Management (FICAM), and Global Federated Identity and Privilege Management (GFIPM) initiatives. The Identity and Authentication Framework, authentication process, authentication protocols, and assertions are described in details in section 9.3.

4.7 Public Safety Grade - Information Infrastructure (PSG-II)

Public Safety Grade Information Infrastructure (PSG-II) is a system component resides the MAMF-support system and represents the set of information resources made available by different levels of governmental stakeholders, and public safety entities. The PSG-II corresponds to the heterogeneous collection of information resources managed by different domains administrators following wide range of rules and policies. In this study, we rely on each Information Provider to define the policies, rules, and terms of use to be enforced on users accessing the information managed by each Information Provider. As PSG-MAMF builds on top

of existing policies, it works as a way to simplify the complex public safety information infrastructure by honouring the set of policies imposed by Information Providers.

Furthermore, sharing information between different governmental stakeholders, public safety entities, and responders is a challenge. Organizations and Users shall share information by relying on the PSG-MAMF to handle efficiency, security, and maintain records of actual information exchange. PSG-MAMF shall provide guarantees of fidelity, integrity, availability, and scalability to all information exchange parties. Further, PSG-MAMF shall provide guarantees of the imposition of the Information Providers rules and policies over shared information throughout the information lifetime. In order to achieve the set PSG-MAMF lofty goals, and to maintain consistency with current and evolving public safety systems, we recommend to follow the National Information Exchange Model (NIEM) approach for information and data exchange among different organizations [51] [11], as described in section 2.2.5

Section 8, provides more details on dealing with information exchange, and interoperability. Further, section 8 provides security considerations required to keep information secured at rest, in motion, in temporary storage, while being processed by applications, and during information exchanging between different domains and different Information Providers.

4.8 Public Safety Grade-Application Store (PSG-AS)

PSG-AS is a locked private application store that serve as a home for applications developed or deployed by Application Developers specifically for public safety organizations, and in some cases developed by public safety community to enhance their missions. PSG-AS is a way to offer public safety users the applications they need, and allow download and install of PSG-MAs developed for public safety community in a manner similar to the consumer application stores, however, from trusted source and under administration control. Public safety users are not allowed to download applications through means other than PSG-AS. PSG-AS provides the convenience of a public application store with added security features of a secured private application store including:

- **Access control:** to control user access to the PSG-AS through the identity access management that verify the users' access privileges before granting them access to PSG-MA.
- **Private connections:** Applications downloads should only be allowed over private connections (e.g. HTTPS) or through VPN tunnels.
- **Centralized management & Administration console:** to provide additional security features and monitoring applications throughout its lifecycle.
- **Applications vetting:** to ensure applications are incompliance with public safety security policies and controls before distributing applications among users.

The PSG-AS can be viewed as two main elements, namely, the Public Safety Grade – Application Store – Support System (PSG-AS-SS) that is part of the PSG-MAMF support system; and the Public Safety Grade – Application Store – Device System (PSG-AS-DS) that is part of the device system, as shown in Figure 4.

4.8.1 Public Safety Grade – Application Store – Support System (PSG-AS-SS)

PSG-AS-SS is the support system component of the PSG-AS that reside the public safety infrastructure. PSG-AS-SS is mainly responsible for housekeeping and managing of PSG-MA. PSG-AS-SS consists of the following two components:

A. Application Store System

The Public Safety Grade Application Store (PSG-AS) stores applications and makes them available on the PSG-AS along with related information on the PSG-AS support servers. Those support servers are referred to as "Application Store System" throughout this document. Application Store System holds the full responsibility of housekeeping and redistribution of PSG-MA. Thus, Application Store System is responsible for two major roles:

- Receive and process a request from the Application Developer to upload Applications.
- Receive and process a request from users to download Applications

B. Application Store Management System

Application Store Management System holds the responsibility of testing and managing of PSG-MA on the PSG-AS. The Application Store Management System provides a testing process to ensure only secures applications are available for the public safety Users. The testing process provide key services such as threat modeling, security requirements analysis, security architecture and design review, and application security code reviews & penetration testing. Typically, application should pass a Security Assessment and Authorization (SA&A) process that consists of four phases as provided by National Institute of Standards and Technology (NIST) [52][53][54], namely, initiation, certification, accreditation, and continuous monitoring [55]. It is also recommended to follow NIST and ITSG mechanisms for testing applications in order to provide software assurance for applications [23][56]. NIST provided a formal testing process, where they referred to this process as "Vetting Process". An application vetting process is a sequence of activities that aims to determine if an application conforms to the organization's security requirements. This process is performed on an application after the application has been developed by the Application Developer and released for distribution but prior to its deployment on an organization's mobile device.

Application Store Management System follows the Security Assessment and Authorization (SA&A) process and NIST testing mechanisms to grantees all security gabs and vulnerabilities are tested and covered. PSG-MAs have to go through a rigorous application testing process to assess their compliance with public safety security requirements. For example, how data used by an application should be secured, the environment in which an application will be deployed, and the acceptable level of risk for an app, permissions required by applications, sensitivity of applications, and impact that would occur if the Confidentiality, Integrity, or Availability were compromised, specific cryptography requirements, and other predefined attributes [57]. Accordingly, Application Store Management system grants accreditations to applications that meet the PSG-AS criteria. The vetting process is described in details per section 7.5.

In addition, the Application Store Management System provide a process for rating applications (e.g. star rating) in order to allow the public safety organizations to understand the security level of the application, and accordingly allow or deny their members to install applications from the application store (PSG-AS).

Furthermore, Application Store Management System verify the users access rights before forwarding a download request to the Application Store System to process the download request. This way, PSG-MAs are available only for authorized users.

4.8.2 Public Safety Grade Application Store – Device System (PSG-AS-DS)

PSG-AS-DS runs on the PSG-MD where users can access it to download applications published on PSG-AS. The PSG-AS-DS may allow users to download applications that were created specifically for public safety services or other publicly available applications such as browser(s), email applications, and similar general purpose applications. PSG-MAs and Generic Applications provided by the PSG-AS or run on the PSG-MD are discussed later in section 7. PSG-AS-DS is also responsible for processing the pushed updates coming from the Application Management and Administration, as described in section 4.4.2.

Applications running on PSG-MD may raise common security concerns due to their access to PSG-II, where the information is stored on the device, and whether the information stored on the device is accessible by other apps. Applications security vulnerabilities, concerns, and mitigation strategies are discussed in details in section 7. Users may need to be authenticated before granting access to the PSG-AS in which identities, credentials, and tokens may need to be provided and verified in order to have assurance in the User's identity. The results from the authentication process and the user's attributes are then shared with the Application Store Management System, so that Users granted access to applications according to their access privileges.

PSG-MAs must handle information incompliance with the organizational security policies for accessing, storing and sharing of information. This capability can be achieved via Access Right Management (ARM). This requires PSG-MA available on PSG-AS to be ARM-enabled, in order to be able to understand and translate the license and management files attached to information that assist information handling including access, usage, storing and sharing. In addition, PSG-MA running on the PSG-MD should be monitored and managed all the time so that Application Management and Administration could be able to remotely invoke and wipe PSG-MA and its related information from the PSG-MD when deemed necessary.

4.9 Access Rights Management (ARM)

PSG-MAMF builds on top of existing policies, where the Information Providers are responsible for defining their own policies, rules, and terms of use to be enforced on users accessing the information managed by particular Information Provider. Consequently, PSG-MAMF should support a secure information management at the device and application layer, and provide the guarantees to the Information Providers that their information will kept secured as it were secured on their infrastructure, and the rules and policies set of handling information are extended to the mobile framework. To achieve this, PSG-MAMF requires to supports a privilege management and a secure access management mechanism, which referred to hereafter as "Access Right Management (ARM). ARM manages access to information and services on PSG-II, as well as access, storing, and sharing of information on the PSG-MD.

The main advantage of the ARM is that security rules and policies are defined by the Information Providers, managed on a central system, and encapsulated and migrates with information in such a way that rules and policies can still be applied even on the PSG-MD even when the server is not

accessible or where there is not network connectivity at all. Thus, ARM allows the Management and Administration to control information even after it shared and reside the PSG-MD.

Access Rights Management (ARM) consists of two major components: ARM-support system (ARM-SS) that is part of the PSG-MAMF support system, and ARM-device system (DRM-DS) that is part of the PSG-MAMF device system, as shown in Figure 4.

4.9.1 Access Rights Management Support System (ARM-SS)

ARM support system (ARM-SS) is part of the PSG-MAMF support system that represents the administrative central point for ARM and provides the guarantees to the Information Provider that their rules and policies set are extended to the mobile framework as shown in Figure 7. ARM-SS can be considered as the license provider which is responsible for the following:

- Creating licenses according to the management files provided by the Information Providers. The licenses contain the rules, policies, and organizational requirements that should be applied on the information according the Users access privileges.
- Encapsulates the license to the information, creates packaged information, encrypt the packaged information, and distribute packaged encrypted information among PSG-MD, PSG-MA, or Users
- ARM-SS is considered a part of authentication and authorization process.

Consequently, the ARM needs to have another component running on the PSG-MD (referred to it later as ARM-DS) in order to work with the ARM-SS in processing the received packaged information, interpret the information, requests the licenses of handling information, and enforce the rules and policies provided in the license encapsulated with the information.

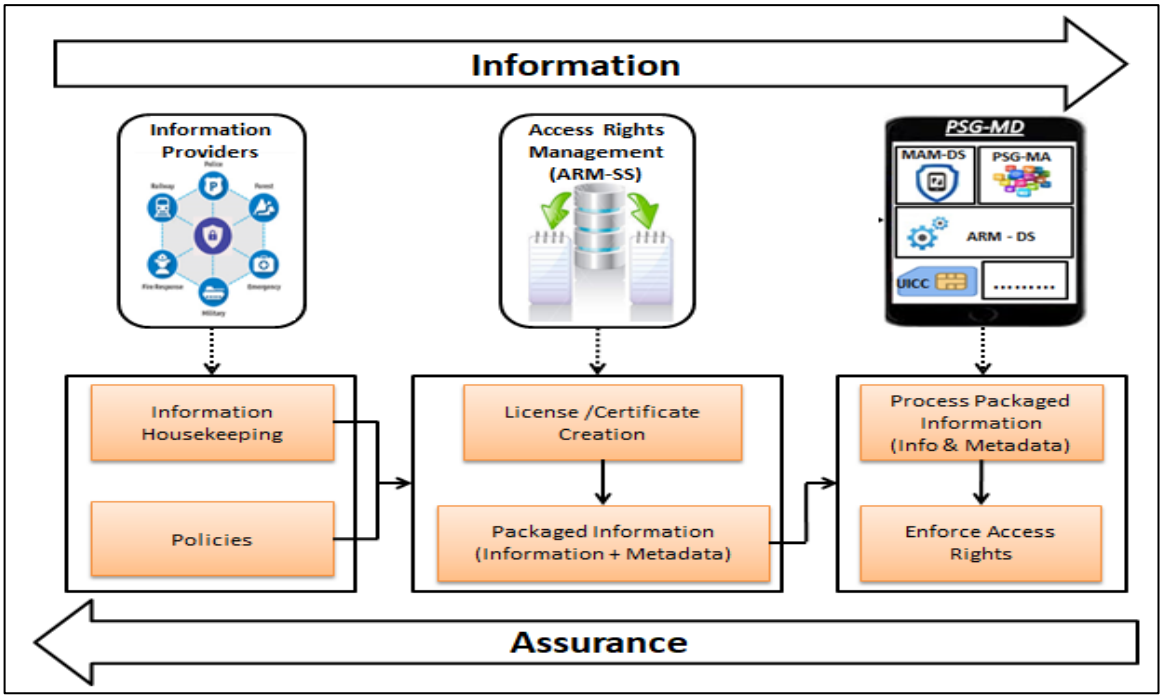

Figure 7 Access Right Management Process

4.9.2 Access Rights Management Device System (ARM-DS)

ARM device system (ARM-DS) is part of the PSG-MAMF device system that is running on the PSG-MD and communicates with the DRM-SS. ARM-DS is responsible for performing information handling and policies enforcement on the PSG-MD. DRM-DS is responsible for processing the received packaged information, decrypt information, interpret the information, requests the licenses of handling information, and enforce the rules and policies provided in the license encapsulated with the information.

There are different ways to implement the ARM-DS depending on the way it interpret the information and the management files on the PSG-MD. The interpretation of information takes place either by the application requesting the information itself, by adding a support security layer as a thin interpretation layer between the application and the management file, or by a hybrid of both applications and the additional security layer. PSG-MAMF considers extending the PSG-MD operating system to add an extension security layer that aims to support the ARM functionalities. The extension layer provided in the PSG-MAMF can be implemented using trusted computing components as the core blocks of embedded ARM and security mechanisms as discussed in section 6.4.3. ARM-DS components are described in details in section 6.4.3 and further in Annex C.

4.10 Mobile Application Monitoring (MAM)

The Mobile Application Monitoring (MAM) is a PSG-MAMF system component that aims to provide and maintain secure environment by implementing secure controls to manage, monitor, and control PSG-MD, PSG-MA, information, and Users activities. MAM consists of hardware and software elements that utilize known management tools including MDM, MAM, and MCM platforms to provide management and monitoring features.

MAM manages and deploys PSG-MA on PSG-AS as well as the PSG-MD. MAM allow the public safety organizations to distribute, manage, and upgrade applications on PSG-MD, where applications can be pushed onto the PSG-MD directly from the PSG-AS. MDM, MAM, and MCM platforms provide information management services to secure the information at rest, in motion, in temporary storage, while being processed by applications, and during information exchanging between different domains. Thus, MAM can provide the needed separation between applications and information as well as managing smaller granularity of data sharing. Further, MAM provide an option to deploy devices in Kiosk Mode or Lock-Down Mode. PSG-MAMF may rely on mobility management platforms supported by top vendors (e.g. New Technology, BlackBerry, etc.) to complement the system architecture. Such mobility management solutions can provide additional security features and mobile protection mechanisms (e.g. containerization, locking/wiping, blacklisting and whitelisting, management console, etc.) that can be used to assist the management and monitoring services required by PSG-MAMF

The Mobile Application Monitoring (MAM) is composed of two major components, namely, the Mobile Application Monitoring Support System (MAM-SS) and Mobile Application Monitoring Device System (MAM-DS).

4.10.1 Mobile Application Monitoring Support System (MAM-SS)

MAM- support system (MAM-SS) is part of the PSG-MAMF support system that represents the central remote management within the PSG-MAMF support system. MAM-SS can be

implemented either on server farms, on-premises, or as a cloud-based service. MAM-SS exchanges commands with MAM-DS within PSG-MD to perform the following management services:

- An administrator can use an administrative console within the MAM-SS to manage, monitor, configure, update or alter PSG-MD behaviour.
- Provide assurance to the Information Provider by support the authentication process through exchanging commands with MAM-DS to collect information about the device, user, and application, and to insure integrity of the device. Such information is to be used as an input in the authentication process that assist the authentication decision making to whether grant access to PSG-II and network or not. NIST SP 800-63-2 provided a guidance for remote authentication process [14].
- MAM-SS also provide security and control capabilities by providing the Management and Administration with the ability to manage users' options, device configurations, and device behaviour.
- MAM-SS provide application management capabilities including application wrapping or containerization, application configuration management, and application performance monitoring.
- MAM-SS role extend to control long term and temporal information storage, information usage, and information sharing between mobile applications on the same PGS-MD following management technologies (e.g. containerization) and ensuring compliance with predefined rules and policies. MAM-SS supports the containerization concept to ensure that when an application is running on a memory space, other applications cannot access the memory being used. This way, applications and related information are enforced to stay within their assigned memory areas and cannot be interfere with other applications in different memory areas. Applications should have a license with a proper access rights in order to access information. It is important to know that containerization can also be applied physically using HC-USIM that aims to support the idea of containerization and separated memory areas as discussed in section 6.5.6.2 and Annex D

4.10.2 Mobile Application Monitoring Device System (MAM-DS)

MAM- device system (MAM-DS) is part of the PSG-MAMF device system that runs on the PSG-MD and receives and implements the management commands coming from MAM-SS. MAM-DS interact with MAM-SS to manage, monitor, and control PSG-MD, PSG-MA, information, and user activities by performing the following management services:

- MAM-DS have the ability to provision and de-provision PSG-MA on the PSG-MD by collecting information about the PSG-MD and reports to MAM-SS.
- MAM-DS monitors and collects information about the mobile devices which include: mobile device status, compliance status, OS health, etc. Such information can support the authentication process by reporting it to the MAM-SS. The “Identity and Authentication Framework” system component typically queries the status information collected by MAM-DS to use it as input in the authentication process.

- MAM-DS monitors and reports the application download, usage, and services usage to MAM-SS. This allows the Management and Administration to push applications remotely to the devices for instant install, push remote updates and also remote removal of applications.
- MAM-DS monitor behaviours of PSG-MD, PSG-MA, and user's activities, and accordingly enforces implementation commands and corrective measures coming from MAM-SS such as white-listing, black-listing, remote locking/wiping, etc.
- MAM-DS support the application configuration management, where applications can be remotely configured for different reasons such as adjusting their power consumption in order to provide real time remote control to meet situational demands.
- MAM-DS provides mobile application visibility, testing, and performance monitoring. Such capabilities can be used to track applications usage (e.g. each time a User opens an app, brings an application from the background to the foreground, or returns to an application from the lock screen, applications performance, applications access to network, etc.)
- MAM-DS provide application reporting, usage analysis, and provides statistics in an analytic dashboard for MAM-SS and Management & Administration. MAM-DS can report the state of the application to the MAM-SS such as, application crash log reporting and application battery drainage reporting. Accordingly, MAM-SS can take the appropriate actions, for example, event management, application updating, application freezing, application deleting, or remotely wipe information from certain application, etc.

5 Overall Management Framework Architecture

The PSG-MAMF architecture can be viewed in terms of a group of system components that interact together to provide a comprehensive security services. Each component of the system framework provides secure capabilities that contribute to reducing the potential risks imposed by the nature of mobility. Figure 8 illustrates the PSG-MAMF architecture from high level.

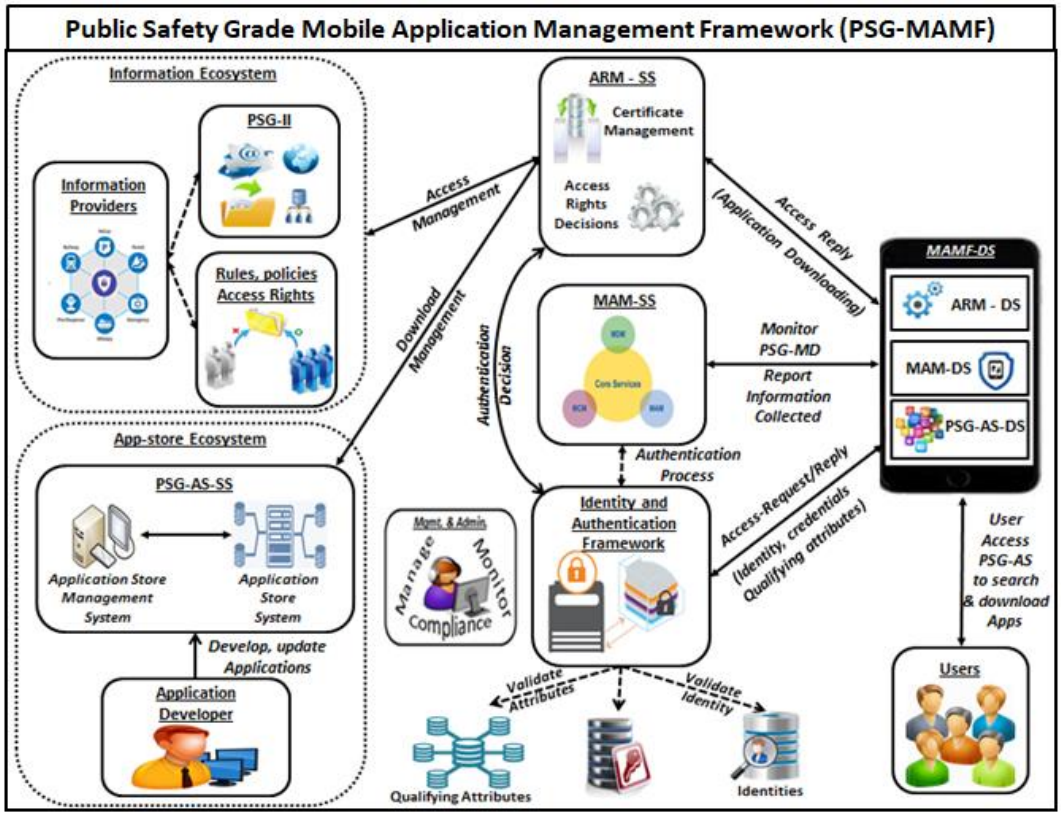

Figure 8 overall PSG-MAMF Architecture

The PSG-MAMF consists of three main processes; each process consists of set of considerations, which add secure capabilities to the framework.

5.1 Adding and updating mobile applications on PSG-AS

The procedural steps for adding mobile applications to PSG-AS are as following:

(1) The Application Developer develops a potentially, Public Safety Grade Mobile Application (PSG-MA) and is interested in publishing the application on the Public Safety Grade Application Store (PSG-AS). The Application Developer has to improve the applications according to organization security requirements, responders operational requirements and set of well-defined attributes to maintain high level of security, fidelity,

and integrity in published applications, so that the PSG-MA can provide high levels of security and integrity for users, devices, and information.

(2) Application Developer sends a request to the PSG-AS-SS to publish an application, where the application is then uploaded to be reviewed and vetted.

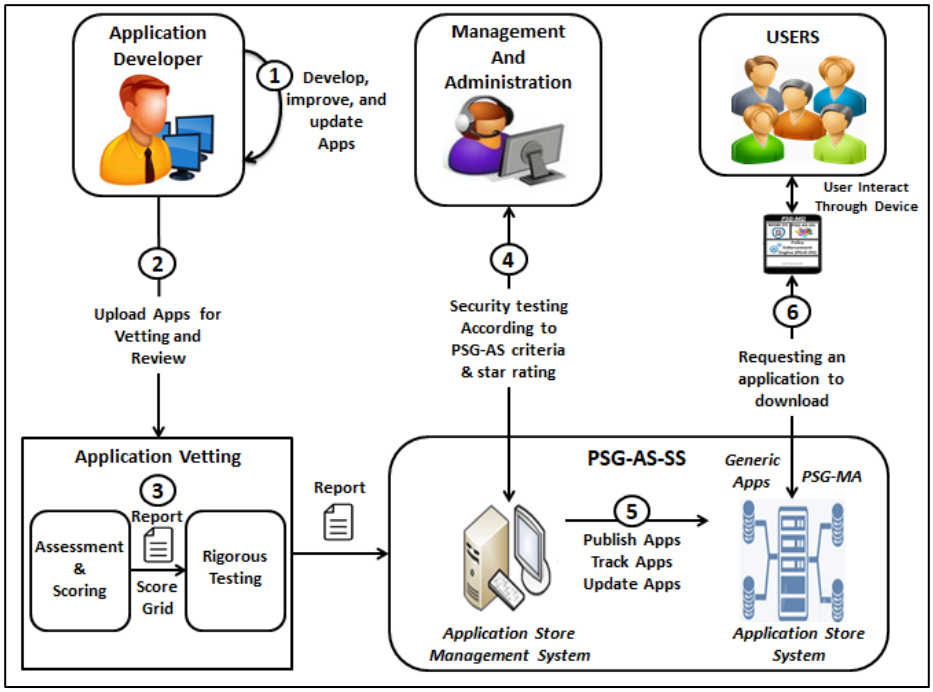

Figure 9 Process of uploading apps to the PSG-AS (steps 1 to 5)

(3) The applications must be evaluated through risk assessment, where the application is then assigned a score/metric (e.g. high, moderate, or low) that can be then used as input for Security Assessment and Authorization (SA&A) process that can take advantage of priori tested applications. Thus, it is required to identify approved common criteria for assessment and scoring that are recognized by public safety organizations. The application has to undergo a rigorous application testing process that may include software assurance, security assurance, look and feel, and behavior types. The testing process should also ensure the application compliance with public safety requirements, operational requirements, and any and predefined attributes [52][53][54][23]. The applications vetting process is discussed in details in section 7.5. Accordingly, a report of assessment, scoring, and testing process is generated, and then reviewed by the responsible parties which may include public safety security testers and approvers, followed by a decision of approval or rejection.

(4) The application store management system along with the Management and Administration take appropriate action based on approval/rejection. The application has also to be tested according to the PSG-AS security criteria. If the application is rejected, procedures for generating a rejection report that contain a rejection list of the identified

software or security vulnerabilities and the steps needed to resolve detected vulnerabilities have to be sent to Application Developer to remediate the risks and improve the application accordingly. If the application approved, procedures of hosting and posting the PSG-MA on the PSG-AS shall be followed. This include statistics on the performance and star ratings, such rating can somehow assist PS organizations with whether to allow or deny their members to install such PSG-MA from the PSG-AS.

(5) Once the application vetted, assessed, and approved, the Application Store Management System uploads the application to the Application Store System to be available for public safety User to download through PSG-AS. PSG-MA will be available for users only through PSG-AS. (Figure 9 describes the uploading process through step 1 to 5).

(6) Public Safety Users download PSG-MA or updates through PSG-AS. The process of downloading or updating of PSG-MA is described in details in section 5.2.

5.2 Downloading mobile applications to PSG-MD

The procedural steps for downloading applications from PSG-AS-SS are as following:

(1) Users access the PSG-AS-DS within the PSG-MD in order to search and download vetted approved applications from trusted source. Since Users have access only to certain applications according to their access privileges and the rules and policies imposed by their organization. Users have to represent their identity, credentials that prove their own identity, and other qualifying attributes to be validated. Such information along with Download-Request is forwarded to the "Identity and Authentication framework".

(2) The MAM-DS running on the PSG-MD validates and executes management commands received from the MAM-SS, and collects information about the PSG-MD that defines the integrity status of the PSG-MD and reports such information to the MAM-SS to assist the authentication process. In addition, MAM-SS simplifies the User interaction with Identity and Authentication framework to form the User authentication process. The MAM-SS is supported by the MDM, MAM, and MCM platforms to manage and deploy downloading of PSG-MA to the PSG-MD.

(3) The "Identity and Authentication Framework" system component queries the status information collected by MAM-DS to use it as input in the authentication process. In addition, Identity and Authentication Framework validates the digital identity, credentials, and qualifying attributes in order to limit the user's options according to their needs and permissions defined in organizational policies.

(4) Once the User has been authenticated to the network via the Identity and Authentication framework, the authentication result is forwarded to Access Rights Management (ARM) that state the Authentication-Decision, and other information that support the Download-Request.

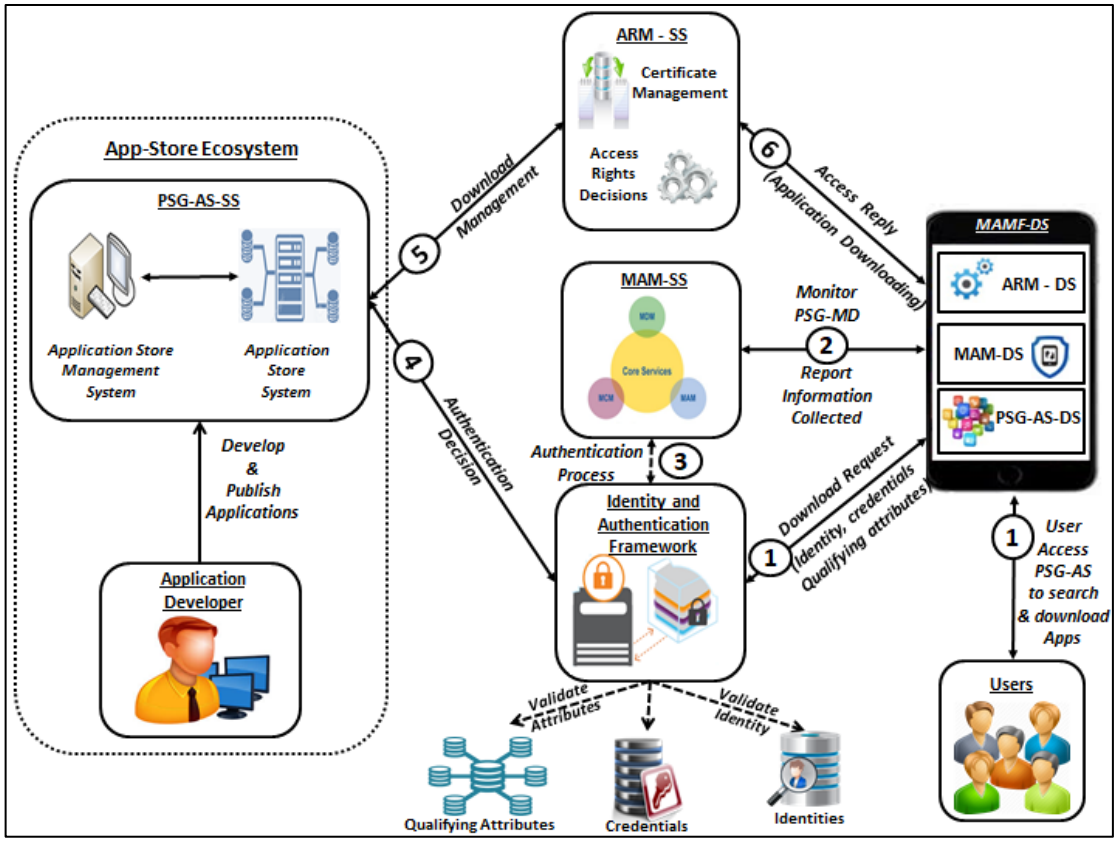

Figure 10 the process of downloading apps from the PSG-AS to the PSG-MD

(5) ARM manages User's access to PSG-AS-SS. According to the User identity, access rights, and current qualifying attributes, User provided access only to appropriate applications. Accordingly, a Download-Request forwarded to PSG-AS-SS to start the downloading process.

(6) The Users granted access to download PSG-MA from the PSG-AS to the PSG-MD according to their access rights. Figure 10 describes the process of downloading PSG-MA from PSG-AS-SS through steps 1 to 6.

5.3 The Requesting of information and services process

The process of requesting information and services from the PSG-II is typically the same as the process of downloading applications from the PSG-AS-SS discussed in part 2. After the vetted applications downloaded to the PSG-MD, the Users, PSG-MD, and PSG-MA may request access to information and services from the PSG-II. The procedural steps for of accessing information and services from PSG-II are as following:

(1) The User requests access to information and services in the PSG-II by sending Access-Request and representing his/her identity, credentials, and qualifying attributes to be validated to obtain access to the needed information and services according to their access privileges. Such process requires authenticating both User and device to the

network, and then to the PSG-II. The requirements for User-device authentication to the network and PSG-II is described in details in subsections 9.3.2.2 and 9.3.2.3.

(2) The MAM-DS running on the mobile device collects information about the PSG-MD which may include: device status, compliance status, OS health, and other factors that define the integrity status of the PSG-MD and reports such information to the MAM-SS to assist the authentication process.

(3) The "Identity and Authentication Framework" system component queries the status information collected by MAM-DS to use it as input in the authentication process. In addition, Identity and Authentication Framework validates the digital identity, credentials, and qualifying attributes using the appropriate authentication techniques and protocols. The identity, credentials, qualifying attributes, authentication process, and access management within the PSG-MAMF are described in details in section 9.

(4) Once the User has been authenticated to the network via the authentication and identity framework, the authentication result is forwarded to Access Rights Management (ARM) that state the Access-Decision, user identity, and the qualifying attributes associated to this unique user's digital identity.

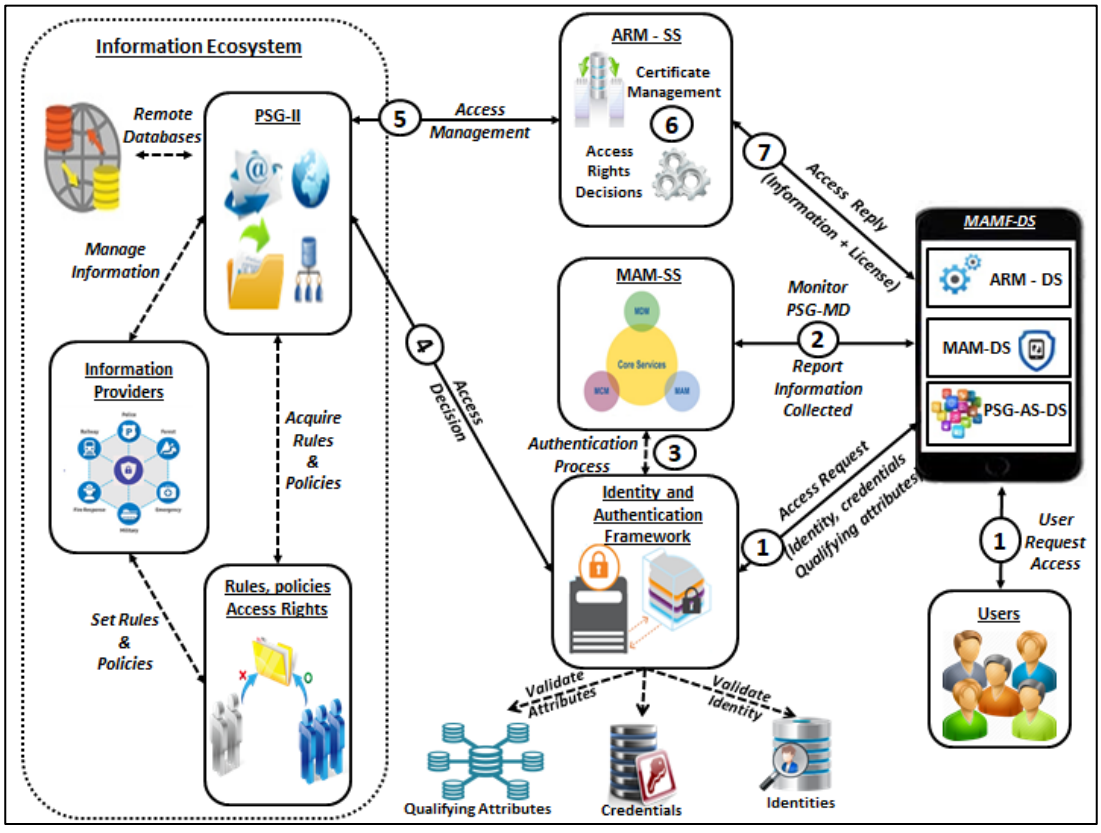

Figure 11 the process of requesting information and services from the PSG-II (steps 1 to 7)

(5) The Access Right Management (ARM) manages the access to information and services on behalf of PSG-II by verifying the User‘s access rights based on the rules, policies, access privileges, and the current qualifying attributes. Following successful verification of accessibility rights, the User shall be granted access to the required information and services according to their access rights.
(6) The Access Right Management (ARM) creates a license file that contains the rules and policies that should be applied to information to manage information handling process, according to the User access Rights. Such license is encapsulated to information forming packaged, encrypted information.
(7) An Access-Reply is forwarded to the User, along with the information and license that manage information handling on the PSG-MD. Such license should be encapsulated and accompany the information throughout its lifecycle including usage, storing, and sharing.

The communication between the PSG-MD along with PSG-AS-SS and PSG-II in order to download PSG-MA or accessing information and services is performed using secure control communication. The PSG-MAMF relies on set of technologies to provide end to end multi-fencing security system. Such technologies include mobility management solutions such as MDM, MAM, MCM, and mechanisms to enforce the concept of applications and information separation such as application wrapping or containerization. As mentioned earlier, each component of the system framework provides security capabilities that aim to mitigate the potential security risks on the system. The following sections discuss each system component in details by identifying the potential risk on such component, and the technologies, strategies, recommendations, and best practices to mitigate such risks.

It is important to highlight that information and services available through the PSG-II shall be managed by Information Providers. The role of PSG-MAMF shall be limited to securing the information exchange and to providing the necessary guarantees of legitimate use and handling of provided information.

6 System Component : Public Safety Grade-Mobile Device (PSG-MD)

As mentioned earlier, PSG-MAMF consists of major system components which include hardware and software components along with physical entities that form the proposed system architecture and interact together to provide security capabilities that aim to mitigate the potential security risks on the system. This section focused on Public Safety Grade Mobile Device (PSG-MD) system component.

A PSG-MD could be any mobile device such as smart phone, tablet, modem, dongle, or any other wearable device as long as it can connect to the PSBN without a proxy and has the capabilities and technologies that qualify it as Public Safety Grade (PSG), as mentioned in section 1.2. Smart phones bring a tremendous amount of capabilities to the public safety responders. PSG-MAMF provides insight on the policies and requirements of PSG-MD and PSG-MA in order to provide the responders with the capabilities needed to securely connect to the PSBN, access PSG-II, while maintaining sufficient levels of assurances to involved stakeholders in terms of security, availability, confidentiality, fidelity, and integrity of the entire system. Whereas an example, responders and public safety Users can gain access to criminal history, vehicle registration records, dispatch information, and other information using their devices, when needed. PSG-MAMF maintains logs of all activities happening in the system at all times. PSG-MD capabilities and technologies help responders to bring mission critical information at their fingertips at the right time. However, PSG-MD and new technologies expose the PSG-II and information residing the PSG-MD to potential security risks. Further, with the increased pressure to support Bring Your Own Device (BYOD) trend, public safety agencies are facing increasing challenges to secure a diverse range of computing devices. Thus, potential security risks need to be addressed using well-defined strategies in order to keep mobile devices and their access to PSG-II secured and protected at all times.

Much of the security required for PSG-MAMF relies on the protection provided by the mobile device, and the policies implemented on the device. Thus, the selection of the device is critical issue since it affects the security features supported by the framework. For example, some mobile devices may support some form of secure boot started with a code rooted in hardware or firmware (e.g. root of trust), while other devices support no secure boot integrity check at all. Another mobile devices supports secure key storage, while other devices not. Thus, public safety organizations should ensure that PSG-MD supports the desirable hardware, firmware, and operating system capabilities.

Public safety agencies require integrity verification of a PSG-MD and its components prior to access granting to the PSG-II. This verification is essential to guarantee the safe guarding of information and other services. PSG-MD must hold essential security capabilities to provide higher degrees of assurance that the device can be trusted. PSG-MAMF assumed that the PSG-II and the PSG-MD cannot trust each other until sufficient security credentials are exchanged initially and on-going through strategies such as assertions are maintained during operations. It is important to highlight here that user role and credentials, and device information (known later as 6 qualifying attributes) are required to identify the level of trust that can be awarded to informational transaction. Access to particular atomic information requires authenticating user credentials and other attributes but may be denied if the device in use is known to have been compromised or if the device is lacking the capabilities required to secure and manage the

required information following policies set by Information Providers. Thus, both user and device need to be authenticated prior to granting access to network and PSG-II. The authentication process is described in details per section 9.3.3.

6.1 Classes of PSG-MD

There are two fundamentally different classes of PSG-MD relevant to security challenges and the required PSG-MD capabilities, namely, a Public Safety Owned Devices (PSOD) and a Bring Your Own Device (BYOD). In this document, the risks arise due to the inherently different nature of the two PSG-MD classes are addressed through different potential security mechanisms provided in section 6.4. The two mobile devices classes described in the PSG-MAMF are:

6.1.1 Public Safety Owned Devices (PSOD)

Public safety agencies shall supply their users with mobile devices that have specific capabilities in order to be qualified to serve as public safety grade mobile device (PSG-MD). Public Safety Owned Devices (PSOD) are expected to have as many functionalities and capabilities as a regular commercial mobile devices. However, PSOD must undergo a Security Assessment and Authorization (SA&A) process for evaluating, testing, and authorizing the device to ensure compliance with the public safety security requirements. Further, PSG-MD, PSG-MA, and the stored information can be centrally managed using mobility management technologies including MDM, MAM, and MCM platforms as discussed in Annex A. This way, the public safety agency is considered the device owner and the Information Provider as well. Consequently, relevant public safety agency control the PSOD, thus, public safety agencies can enforce their policies to PSOD or users and has the ability to remotely wipe its information from PSOD when deemed necessary.

6.1.2 Bring Your Own Device (BYOD)

BYOD trend is a concept that allows users to bring their own devices and use it in public safety environments, where the user can use his mobile device to access PSG-II as well as the normal use of the BYOD to provide the user with access to his/her personal information. This way, the user is considered the device owner and the public safety agency is considered the Information Provider. It is easy envision the comparatively, higher security risk and vulnerability when BYOD class is used. However, if the BYOD doesn't have the required capabilities to qualify and serve in public safety communities, it can't be considered as a PSG-MD.

Information Providers need more sophisticated strategies to protect its own information. Since users will require their public safety organization approval to allow the use of their BYOD, organizations bear the responsibility to set the proper policies for adapting BYOD use by carefully considering operational needs as well as potential risks and vulnerabilities. Consequently, BYODs approved by different organizations shall go through different vetting policies to gain access to the PSBN. Essentially, BYOD of different security grades may be able to access PSBN. However, since Users' access to information follow the policies set by the Information Provider, a lower security grade BYOD cannot access information that require high security grade BYOD. Further, due to the policies set to require device status updates, any changes in BYOD configuration and any tampering with a BYOD can be remotely detected. Potential actions on compromised BYOD follows the set of policies defined by the relevant public safety agency and the Management and Administration ensures the device remains in

incompliance with the organizational security requirements, otherwise, Management and Administration shall detect any violence and accordingly take the proper actions.

Furthermore, we recommend that organizations identify different classes for the BYOD. BYOD can have different policies from one organization to another depending on the concerns, risks, and level of information security required by the organization. BYOD policies can differ in the level of flexibility given to the Users depending on credentials and device type. For example, some policies may narrow the range of the devices, while other policies may allow wider versions of devices. Furthermore, BYOD policies may include how to authorize use, prohibit use, perform management, handle policy violations, and handle liabilities. BYOD policies shall be integrated with the existing organization known policies. Following are potential strategies to address BYOD security concerns and protect PSG-II from potential risks involved in using BYOD:

- Provide a way to separate personal information from public safety information on the same BYOD device. This can be achieved by adopting mechanisms that have the ability to separate and information on the mobile devices such as idea of containerization described in Annex B, or using HC-USIM described in section 6.5.6. Further, such mechanisms support the ability to encrypt and lock public safety information on the BYOD device and the user's personal information as well. Hence Information Providers are able to control their information (e.g. access, revoke, or wipe) if the BYOD is believed to have been compromised. This way, in case of device lost/theft, information Providers have confidence that their information is protected from disclosure.
- Information Providers can rely on Access Right Management (ARM) and policy enforcement techniques to limit access to PSG-II according to access rights, pre-defined security policies and qualifying attributes. For example, an Information Provider can control access of multiple users sharing a device by managing access control of entities to information such that only approved users can access an Information Provider's information while policies enforcement is still applied on the mobile asset. This may also require storage encryption and authenticating access to device using PIN following particular rules. Another way for controlling access to information may include forcing the BYOD user to use a generic browser to access non-public safety information, while use a specific browser to access PSG-II.
- Use Root of trust to establish a chain of trust and provide the device with the ability to send device state assertions to the Management and Administration, then to Information Provider.

The provided list of strategies aims at providing Information Providers with the needed confidence in their information protection by use of combination of encrypted storage, information isolation, and device integrity through assertions.

6.2 Finding a Root-of-Trust

In general, to establish a trust in a device, the device is broken into well-known layered boundaries which typically are: application software; operating systems, boot code, firmware, and hardware. Systemically, the interfaces between device layers can be defined. Following, the trust in each layer can be independently, and incrementally, be defined. Finally, as a consequence of

the trust developed in each layer, the entire device can be trusted. Each layer of the device provide a service to a lower layer or an interface to the higher layers, and since the higher layers have limited insight into the exact implementation of lower layers, lower layers may expose the device to possible potential security risks that can alter the behaviour of the device. Thus, higher layers of the device shall validate the trustworthiness of the lower layers before concluding the availability of to be trustworthy environment. On the way down, each layer needs to be examined in more detail in order to assure a high level of trustworthiness of the device. For example, a trust in the operating system (OS) needs to be developed and validated before processing any trust relation in a mobile application. The reason is simple, there shall be no trust developed in a mobile application running on top of an infected compromised OS. To do that, one must trust that there is no pernicious code in the boot loader (firmware) that could have corrupted the OS, and keep building incremental trust in device layers until the whole device is trusted [58]. This process is typically known as “Finding a Root of Trust”.

6.3 Device Components

Device architecture consists of hardware, firmware, and software layers that complement each other. Generally, each layer of the stack provides services to a lower layer and interfaces for the higher layers of the stack. Following the Root-of-Trust concept, each layer should trust the lower layer, until the whole device can be trusted [4]. Figure 12 shows the device architecture different layers.

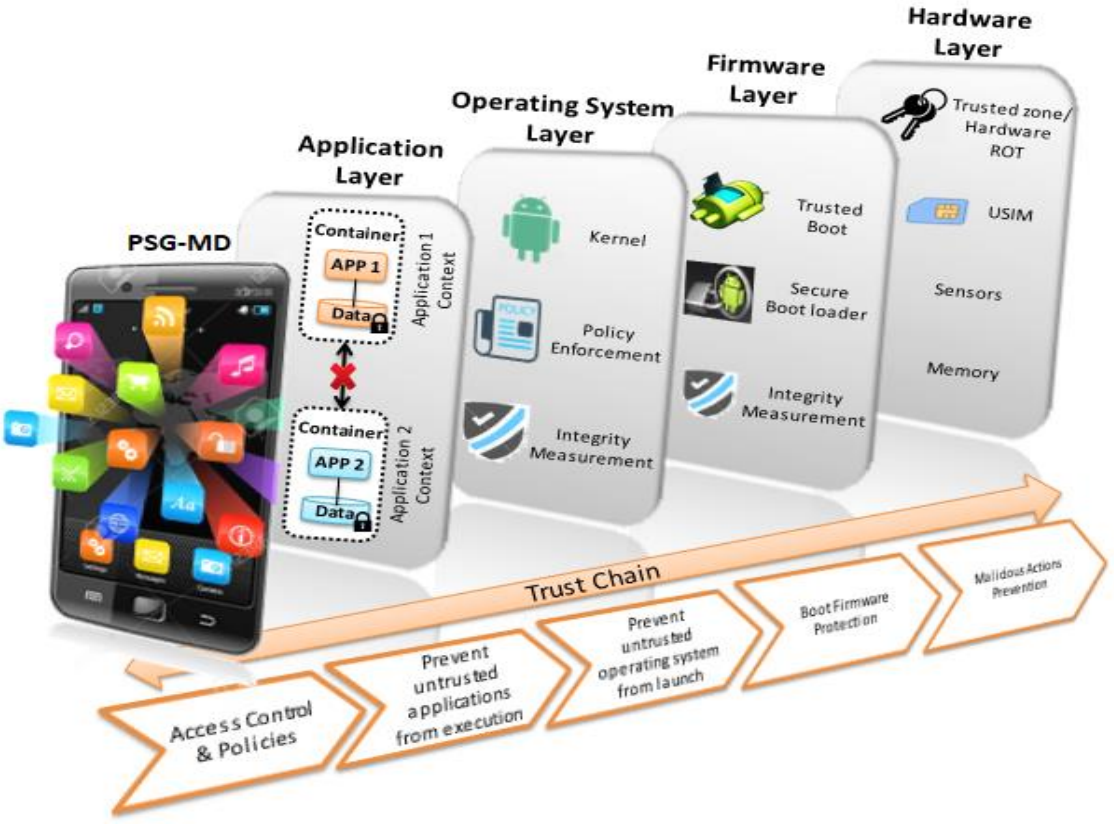

Figure 12 Mobile Device Architecture and its Layers [4].

6.3.1 Hardware Layer

The hardware layer is the lowest layer of the stack. A mobile device could be any device such as smart phone, tablet, modem, dongle, or any other wearable device as long as it can connect to the PSBN without a proxy. Typically, mobile devices have common hardware components such as: battery powered computing capabilities, cameras, various sensors (GPS, accelerometer, gyroscope, proximity, compass), and support multiple connectivity methods such Bluetooth, WIFI, NFC, LTE, and IEEE 802.11 WLANs.

In order to ensure that the mobile device has secure capabilities that can build the trustworthiness in the device, the device shall support some security capabilities including Root-of-Trust (RoTs), Secure boot, Access Right Management (ARM) mechanisms, Device security and integrity vetting, Device ability to communicate its state (e.g. through assertions) [4]. Such security capabilities shall be employed to improve mobile device security and present a basic component in defining the Public Safety Grade Mobile Device (PSG-MD).

Device integrity can be referred to as ensuring the lack of any means of corruption of the device components and layers, including hardware, firmware, and software of the mobile device. PSG-MAMF assumes that a PSG-MD with assured integrity should have the ability to communicate its state to the Mobile Application Monitoring Support System (MAM-SS). It is important to highlight here that once a device provides assurances of compliance to the set of required security policies, the user identity and qualifying attributes are used to request the release of information as per the policies set by the Information Providers. The process of handling information and enforcing policies is managed by access right management (ARM) mechanisms. This way MAM-SS can ensure safe user's access to PSG-II according to the integrity evidences asserted by the PSG-MD, and policies enforcement performed on the mobile asset. Device integrity and assertions are described in details in section 6.4.4 and section 6.4.5, while access right management (ARM) is described in section 6.4.3.

6.3.2 Firmware Layer

Firmware layer is the next layer of the stack following the hardware layer. In general, firmware is "Protected set of special code that interacts closely with device hardware, and responsible for setting up the configuration of the hardware of the device, measuring and launching itself, any other ROM code that runs before the OS, launch the OS boot loader, which in turns launch the main OS and a series of OS components" [4].

Typically, firmware codes provide two core services, where "boot firmware" is responsible for loading the OS to the memory during boot time, and launch the hardware layer, while other firmware sub-components control other hardware components (e.g. baseband processor). Such process exploits vulnerabilities for the mobile device. Most commonly, a malware can be inserted into a system that results in a platform booting in a compromised state. This requires more sophisticated technologies to address such threats. Secure Boot and Measured Boot are technologies that provide assurance that platform boot is running a code that hasn't been compromised [59]. Secure Boot and Measured Boot provide the device with the required protection against pre-boot malware and rootkits [4].

In order to provide a secure firmware layer, PSG-MD shall have the capabilities required for "Boot firmware protections" and "Secure measurement of firmware". Secure Boot and Measured Boot capabilities can be achieved using ROT (Root-of-Trust) that provides a security services for the device, as described in section 6.4.2. A root-of-trust is a "hardware, firmware, and/or software

component that is inherently trusted to perform security services on a device" [60]. However, ROT should be planned in a secure way, in order to be trusted to perform security tasks. In addition, RoT should be protected from malicious actions. Ideally, secure RoT and protection requirements can be achieved by implementing RoT in dedicated hardware, or protected through hardware mechanism (e.g. code stored in the ROM) [60].

Secure Booting Mechanisms:

Secure Boot is a mechanism that aims to ensure mobile device integrity, by verifying each software image during the boot cycle prior to execution. Such process provide device compromise detection and ensure that the device never execute in unexpected or malicious state. Secure Boot ensures verification of all the codes that were initialized prior to establishing functionalities of the mobile device. Secure Boot starts by running well-known trusted code stored at a fixed trusted location on the mobile device (typically in on-chip ROM that server as hardware root of trust). This code is considered as the RoT of the chain of trust for the mobile device, thus, it must be trustworthy to enforce Secure Boot. Typically, two types of Secure Boot are used to trust mobile devices, namely: Secure Boot and Measured Boot.

Both Secure Boot and Measured Boot rely on a Root of Trust (ROT), which can be a piece of code or hardware that is hardened enough that it can't be compromised, modified, or can only be modified through cryptographic credentials. In some cases, the ROT can be provided as a code that takes place of BIOS stored in a secure flash memory that can't be modified without cryptographic authority [59].

Both Secure and Measured Boot start with the Root of Trust (ROT) that extends a chain of trust starting at the ROT, and going through each component that launch by the boot, to the Operating System, and sometimes to the applications itself. However, the process of Secure Boot and Measured Boot is different once a (ROT) is established. The different between Secure Boot and Measured Boot are as following [59]:

6.3.2.1 Secure Boot

The Secure Boot chain starts with a ROT, which can be an executing immutable code stored in a fixed location, usually ROM. In each step of the secure boot process each module of code has to verify the integrity of the subsequent module of code prior to loading it for execution [60]. Thus, prior to the launch of the next step a cryptographic signature of next step is checked first. Hence, the BIOS will check the signature on the boot loader, the loader will check the signature on the kernel, and the kernel will check the signature of each object it loads, and so on until the whole chain can be trusted. During the boot chain, if any of the software modules have been compromised, modified, or hacked, the signature of such module will not match, and accordingly the device will not boot the image.

Hence, the Secure Boot is an automated process. If the signed objects have been modified, the signature is no longer valid, and accordingly the platform will not boot and re-installation is required. On the other hand, if the signed object and signatures are matched, the platform will boot and the secure process is done successfully. It is important to know that secure boot doesn't store any integrity evidence on the device; however, Measured Boot does store such evidences for future integrity reports. The Secure Boot Process is shown in Figure 13.

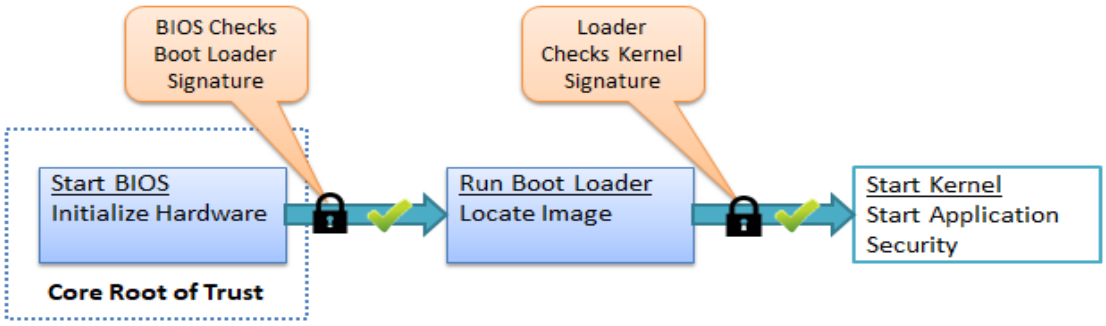

Figure 13 Secure Boot Chain [59].

6.3.2.2 Measured Boot

The Measured Boot chain starts with a ROT, where in each step of the Measured Boot process, prior to launching the next step, the current step running object measures and stores the hash of the next step object in the chain. Such stored hashes must be stored securely allowing a future retrieval figure out which objects were encountered [59]. The process of Measured Boot is illustrated in Figure 14.

It is important to know that Measured Boot doesn't stop the platform from running, Measured Boot compute the object hashes for future checks. Measured boot verify the OS image and other software stack, and compute and store all kinds of platform configuration information (e.g. boot device identity, loader configuration files, or any other information that can be used later to ensure integrity of the device state) [60]. Measured Boot may extend integrity measurements to other parts such as applications.

Measured Boot requires a way to securely store the measured hashes, and a way to report such information to the central Management and Administration. The process of reporting such information is commonly known as "Attestation", as discussed in section 6.4.4. Since the Measured Boot will allow the platform to boot in whatever state, the launched OS can't be trusted to be relied upon to report such hashes. Hence, In the case of Measure Boot, hardware Root of Trust (ROT) (e.g. TPM, Trusted Platform Module) can be the best way to provide such protected storage required for storing hashes measured during the Measured Boot. However, such ROT should be bared to the device OS in order to establish the chain of trust, then be able to report such hashes using assertions during the attestation process [59].

PSG-MAMF requires both Secure Boot and Measured Boot at the same time to provide the security required for PSG-MA and information. In this case, Secure Boot ensures that the system only runs authentic trustworthy software, while the Measured Boot gives a much more detailed picture of how the platform is configured, and reports such information to assist the PSG-MAMF processes. The Management and Administration can review the reported logs to determine if the platform is running an acceptable image. In addition, the "Identity and Authentication Framework" relies on the reported information to assist the authentication process, while the Access Rights Management (ARM) use such information to determine the access rights associated to such platform state.

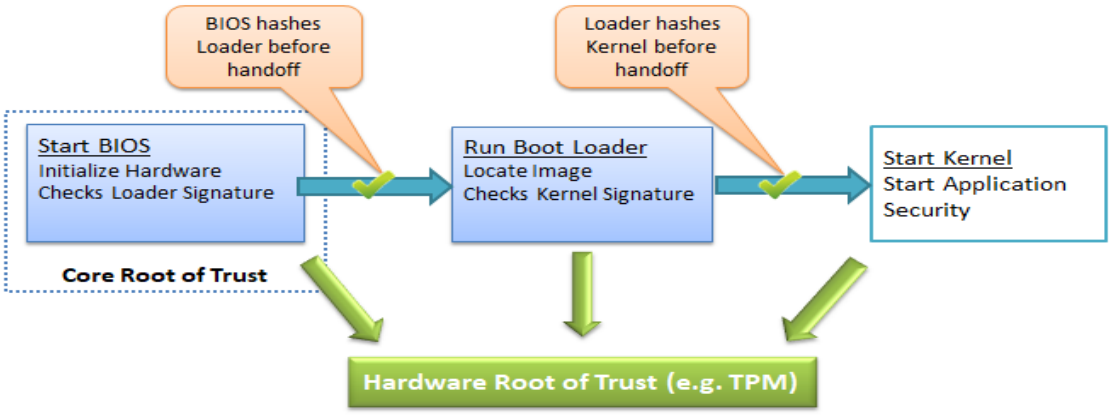

Figure 14 Measured Boot Chain [59]

6.3.3 Operating System Layer

The Operating System layer consists of the OS kernel, components of system service including their configuration data. Typically, the operating system components offer main services including setting up environments for applications, provided access to device hardware using interfaces, policies management and enforcement capabilities, and additional services for the device and its components [4].

The operating system layer provides basic level of security to the device by protecting the device and its contents from exploitation, including applications and its related information. The OS kernel shall provide application isolation capabilities required to protect applications and information from malicious behaviours. Such isolation controls the interaction between applications, as well as the interaction between an application and device components (e.g. access to sensor information). Typically, application should obtain user permission to access the device capabilities (e.g. GPS, camera, etc.), and to access information stored on the mobile device. The application isolation ensures that even if an application is compromised, other applications and its related information would not be affected. The OS application management capabilities provide the control required over applications installed on mobile device. The OS also ensures applications and their updates are installed only from trusted authorized sources.

The compromise of mobile device operating system can result in bypassing the security protection capabilities provided by the operating system, including application isolations and management capabilities. The bypassing of such capabilities resulting in access to mobile device capabilities (e.g. GPS, Camera, etc.) or access to information stored on the device.

In addition, software updates or new operating system versions are usually includes new patches developed by operating system vendors to fix new issues and bring security improvements against potential weaknesses and vulnerabilities in operating system. Leaving the mobile device unpatched or failure to upgrade to the latest software version could result in exploitation risk. Public safety organizations need to ensure that PSG-MDs are continuously patched and running the most recent OS version. In addition, access to network and resources should be managed based on OS version and health. PSG-MAMF considers verifying such information as an integrity evidence of PSG-MD. Following each access

request, integrity evidences would be queried and validated during the authentication process before access decision is made. Such process is later referred to as "Attestation", as described in section 6.4.4. Attestation process may follow existing efforts and well known attestation capabilities provided by different contributions, such as Google's SafetyNet and Samsung KNOX [61].

However, the OS may require the cooperation of hardware and firmware components to perform and enforce security and protection services including device integrity verification, Access Rights Management, isolated secure execution environment and protected storage. However, OS and additional components with interaction with the OS to provide the application and information isolation required to separate personal information from public safety information on the same device, support the containerization concept, provide protected storage space, and provide device integrity measurements.

Recently, monitoring capabilities are introduced to mobile devices that allow the measurement of integrity and security state of the device. For example, Google introduced "Android security path level" indicator on the Android devices (e.g. Nexus and Pixel) that allow users or their organizations to assess the security state of the android devices. In addition, some android vendors improved their security architecture through additional security capabilities such as Real-time Kernel Protection (RKP) feature and TrustZone-based Integrity Measurement Architecture (TIMA) [61] to detect and respond to device compromise detected through measurements reports.

Real-time kernel protection (RKP) is a solution provided by "Samsung Knox" to ensure the security of kernel which results in security of the whole system. As mentioned in section 6.3.2, Trusted Boot measurements are used to determine the kernel state that was loaded and run when the device was started. However, the integrity of kernel after the system runs and start interacting with potential risks is also worth consideration. Thus, real-time monitoring of kernel is required to detect and prevent modifications to kernel code. RKP provides the required protection and monitoring of kernel capabilities using secure monitor located in isolated secure execution environment [61].

TrustZone-based Integrity Measurement Architecture (TIMA) is a solution that provide attestation process to enable the device to attest its state based on a Trusted Boot that maintain trusted measurements of loaded images within secure memory space. The attestation provide integrity measurements to remote server that indicate that the device has performed a Trusted Boot sequence and loaded only approved images during the boot time. TIMA typically works with Knox security features including RKP to guarantee the integrity of mobile devices [62]. TIMA Attestation is similar to Trusted Boot; however, attestation can be requested and reported to server via Enterprise Mobility Management (EMM) solutions. Attestation provides an ability to check integrity of mobile device remotely as deemed necessary. PSG-MAMF supports an attestation process to check if the PSG-MD performed trusted boot sequence by authenticating all the images loaded during boot time, authenticate bootloader and kernel, and collects other information and reports it back for EMM system components, which in turns report such information to Identity and Authentication framework to perform the authentication process. The attestation process within PSG-MAMF is described in details in section 6.4.4.

6.4 PSG-MD Security Components

PSG-MD requires leveraging of a set of security components that can be implemented, interacted, managed, and adopted by hardware, OS, firmware, and applications, in order to be able to provide the security capabilities required for the device to be qualified as Public Safety Grade-Mobile Device (PSG-MD) and to enable the framework provided in section 5. The following sub-sections provide the overview of essential security components to qualify PSG-MD, namely: Chain of Trust, Root of Trust (RoT), Access Right Management (ARM), Device Integrity and Assertions.

6.4.1 Chain of Trust

Transitive chain-of-trust is the process of establishing trustworthiness of specific layer of the mobile device through establishing trustworthiness of other layers. Each entity requires measuring and verifying by another trusted entity, starting from a Root of Trust (ROT) to subsequent entities, in order to expand the transitive chain-of-trust to each entity and the whole device. Figure 15 provides an example of chain-of-trust in a mobile device. The transitive trust begins with a root-of-trust protected by hardware. The root-of-trust could be a code stored securely within the ROM that measure and verify subsequent piece of code in the boot cycle, such as operating system. The device is only allowed to execute if the OS verification approved to be in a trusted state. Then the base file contents are verified, and then its contents are loaded. Once the file system is available, the system can initialize and execute additional system services (e.g. application). This process is typically called "measure–verify–execute" [60]. Hence, “This sequence continues as each code module measures and verifies the next code module before passing execution” [60]. Another example of chain of trust is the process of secure boot and measured boot described in section 6.3.2.

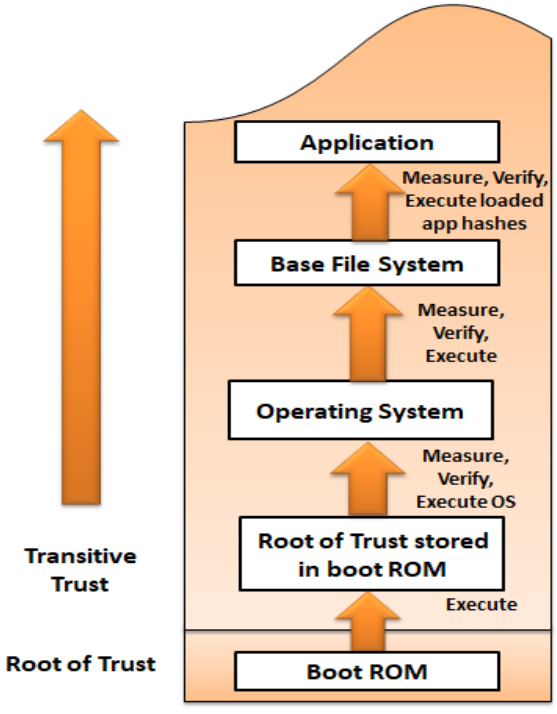

Figure 15 Transitive chain of trust in mobile device [60].

6.4.2 Roots of Trust (RoT)

Root of Trust (RoT) is essential for ensuring the trustworthiness of a device by providing unique security services. RoT provide a high degree of assurance to perform trusted functions and in turns the whole device can be trusted while performing the needed functions. RoT can be implemented in hardware, firmware, and/or software that aim to provide a series of security services for the device. However, hardware RoT is usually preferred over software due to their more reliable and more secure behaviour, or at least protected by hardware mechanism (e.g. code stored in the ROM) [60]. The hardware is usually isolated from other parts of the device, and typically can only be used by specific entities on the device. On the other hand, software RoTs signifies in terms of rapid deployment to varieties of platform. Most commonly, "Roots of trust can be implemented as a combination of hardware and software to provide the best balance of cost of hardware against the security provided (e.g. combine TPM or USIM with BIOS capabilities)" [4] [60]. However, in order to start the chain of trust required to establish confidence in each entity, RoT must securely exposed to the mobile device and interact closely with the operating system to provide set of security services (e.g. assertions).

ROT is typically used to ensure the trustworthiness of hardware, firmware, and software that will result in a secure and trustworthy device, as described in section 6.3.2. The security capabilities required for PSG-MD can be achieved using the RoT which may consists of the following ROT components that interact to achieve the security requirements provided by the ROT [4] [60]:

- Root of Trust for Confidentiality (RTC): The RTC furnishes a location for securing and protecting sensitive information (e.g. cryptographic keys).
- Root of Trust for Integrity (RTI): RTI provides a "protected storage" to protect integrity measurement and "protected interface" to manage assertions and other integrity parameters. Usually, RTC and RTI are combined to form "Root of Trust for Storage (RTS)" [4].
- Root of Trust for Reporting (RTR): RTR supports the integrity, authenticity, and nonrepudiation services for the device integrity reports. RTR is used for identity management and assertions signing for the aim of device integrity generation [4] [60].
- Root of Trust for Measurements (RTM): RTM implement the integrity measurements on the mobile device utilized by assertions. RTM ensures that integrity measurements protection via RTI and attestation with RTR [4].
- Root of Trust for Verification (RTV): RTV typically verifies the integrity of all software, firmware, and storage by checking the measurements against their reference values. After verifying the integrity, the device creates assertions based on the result of the verification [4] [60].
- Root of Trust for Update (RTU): RTU is essential to authenticate device update, successful verification, and to initiate the update process. In addition, RTU can be used to protect the other ROT components [60].
- Root-of-Trust-for-Enforcement (RTE): "a trusted entity that builds any of the RoT components that are based on allocated resources (e.g. operating system or function implemented in software application). Typically, the RTE is the trusted code that is stored

in ROM and executed on platform reset to begin secure boot. If all RoT components are provided as dedicated resources, the RTE is not required" [60].

Figure 16 represents an example of the interaction between the Roots of Trust components that provide security services for the mobile device. The interaction between RoT components is as following [60]:

(1) The RTM performs an integrity measurements for pieces of firmware, software, or storage on the device. Such measurements could occur during the boot cycle or any time after booting as requested.
(2) The RTM stores the integrity measurements securely in the RTI.
(3) During the device attestation, a report of integrity measurements can be requested by any entity on the device (e.g. application).
(4) The RTR restore the integrity measurement from the RTI.
(5) The RTR match the identity stored in RTC with the integrity measurements restored forming a signed integrity measurement report.
(6) The RTR forwards the signed measurement report to the requesting entity (e.g. application) in order to be used in the attestation process.

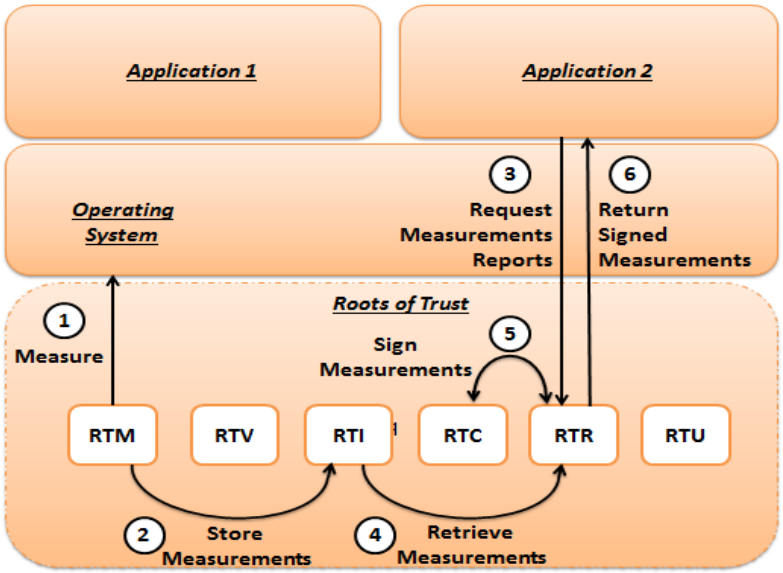

Figure 16 Root of Trust Security Components Interaction [60].

Since the public safety Users use PSG-MA to access information and services in PSG-II provided by various Information Providers, PSG-MA require utilizing RoT services discussed earlier, in order to perform security services and securely store sensitive information including cryptographic keys and authentication credential. PSG-MD may implement ROT in order to allow PSG-MA to provide assurance that information handling requirements are satisfied. Furthermore, Information Providers can rely on assertions based on RoTs to ensure integrity of the PSG-MD before granting access to PSG-II. In addition, Access Right Management (ARM) could use the results of integrity measurements to assign the access rights associated to PSG-MD current state [63].

6.4.3 Access Right Management (ARM)

PSG-MAMF should support a secure information management mechanisms at the device and application layer, and provide the guarantees to the Information Provider that their information will kept secured, and the rules and policies set of handling information are extended to the mobile framework. Access Right Management (ARM) mechanisms can be used to manage access, usage, storing, and sharing of information on the PSG-MD.

ARM extends the enforcement of usage rights and security policies to the users, devices, and the applications running on the device by issuing a license or management file that accompanies the information. Further, ARM can apply policies such as Time-To-Live on information such that, after a period of time the information is self-destructed and can't be accessed by any User or application. In addition, ARM hooks into the mobile device operating system to prevent protected information from being hijacked out. Furthermore, ARM can provide a trusted record of actions performed on the information within the PSG-MD.

Requirements of Access Right Management (ARM) in the PSG-MAMF:

(1) The PSG-MD should be able to enforce the management rights included in the management files or license encapsulated with the Information.
(2) Information should be interpreted by a trusted component on the PSG-MD that has the ability to decode the license that accompanies the information.
(3) Information should be protected from disclosure by encrypting the information before distributing it among different Users. This way, the Information would be protected at rest, and in motion.
(4) There must be a mechanism that assures the integrity of the ARM components, PSG-MD components, PSG-MA, storage, or the integrity of the information itself. For example, Root of Trust can be applied which may use assertions to ensure integrity of different components on the PSG-MD an report such information to ARM to assist in assigning the appropriate access rights according to the PSG-MD state as indicated in the integrity measurement report. Such process is discussed in sections 6.4.2, 6.4.4, and 6.4.5.
(5) ARM-DS should have a part that can be trusted to be responsible for storing protected information, License, and cryptographic keys. In addition, it should be responsible for requesting information interpretation, monitoring the interpreting process, and ensure that information interpretation is done incompliance with the specified license.
(6) Interoperability of ARM; The ARM should be able to operate under different types of devices, since the BYOD will be supported. In addition, different Information Providers may use different ARM mechanisms; under such cases the framework must still consistently functioning including access and security, such that information can be handled according to the usage rights in the way that it intended to function.
(7) Information Providers must be informed and reported about the license enforcement status in the PSG-MD. In addition, any access, usage, storage, sharing of information must be recorded, monitored, and reported.

The simplest way to perform access rights management is to use the applications itself as policy enforcement point, where access right management relies on the application to interpret the management file and enforce the set of rules, policies, and access rights on the information. However, this option has a significant weakness, since trusting applications to enforce usage rights is inefficient. For example, if an application receives information with different security levels, when verifying the User access privileges, the User can granted access only to part of the received information. Under such case, the application would be the enforcement point to deny access to the part of information that is not permitted to the User according to his access privileges. However, all the information requested by the application was encrypted using single key, thus, all the information has to be decrypted in the memory space or the content provider of that application, including information in which the User is not authorized to access. This means that, if the PSG-MD or PSG-MA tampered or compromised, the information within the space memory of the application could be compromised. Even if the applications went through SA&A process, vetted applications still can be compromised which may put all information accessible by such application at risk. Thus, applications can't be completely trusted to enforce the policies of Information Provider.

Another way is to use trusted computing components to perform access rights management. Trusted computing components can act as a an additional security layer between the applications and the management files and can be used as the core blocks of the embedded ARM and security mechanisms in the PSG-MD. These components are referred to as trusted, since they are part of the privileged OS layer and some techniques are used to verify their integrity and authenticity to detect any unusual modification (e.g. hacker's modifications) [64].

The proposed Access Rights Management (ARM) architecture shown in Figure 17, consists of the following components: ARM support system (ARM-SS), ARM device system (DRM-DS), and ARM enabled applications and SDKs. (1) The ARM-SS: is the administrative central point for ARM, which is responsible for creating the license files, packaging and encrypting information, and distribute packaged encrypted information among applications or Users. (2) The ARM-DS: is running on the mobile device and works with the ARM-SS as illustrated in sections 4.9.1 and 4.9.2. The ARM-DS components are responsible for performing information handling and policies enforcement on the PSG-MD, shown in Figure 17. (3) The ARM enabled applications: are applications enabled to ARM by using the Access Rights Management SDKs [65]. The ARM enabled applications can use the functions provided by the ARM-DS in order to encrypt and decrypt information, acquire licenses and certificates from ARM-SS, and accordingly performs security tasks.

The proposed ARM architecture considers extending the OS to support the Access Right Management (ARM) functionalities as shown in Figure 18. ARM-DS shall be extension to the operating system in order to has the necessary privileges to access the mobile devices resources (e.g. sensors outputs), and to be able to perform policies enforcement accordingly. The ARM-DS components are described in details in Annex C.

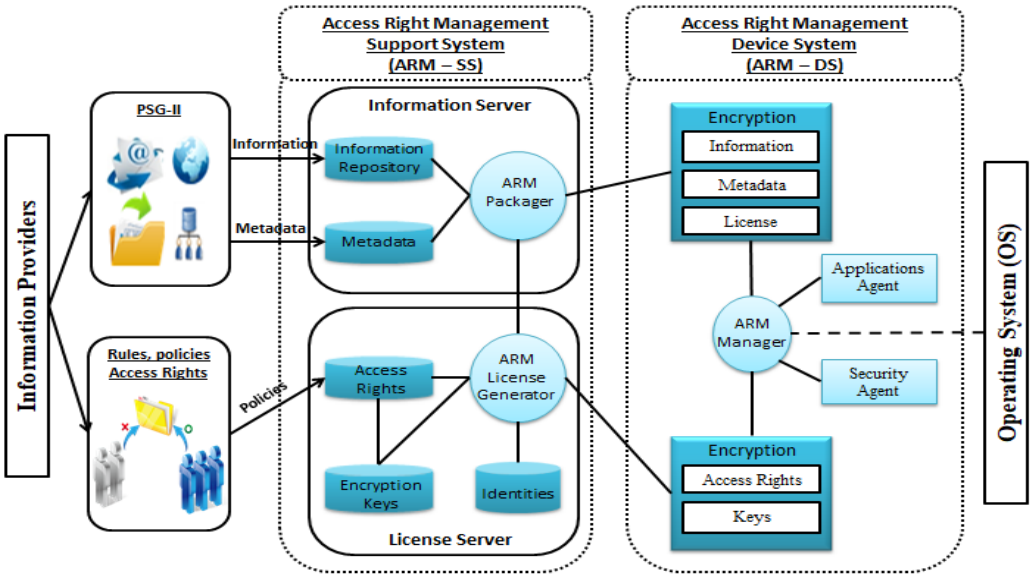

Figure 17 Access Right Management (ARM) Components

6.4.4 Device Integrity

Device integrity guarantees the lack of any means of corruption or vulnerabilities in the hardware, firmware, and software of the mobile device. A device has integrity if it can provide evidences that the device's hardware, firmware, and software are in the expected state that is trusted for the Information Providers that provide access to PSG-II. PSG-MD should has the ability to report its integrity measurements through asserting particular claims showing its state (e.g. configuration, health, or operating status) in such a way that Information Providers can trust and depend on such assertions to take decisions and appropriate actions (e.g. whether grant/reject access to network/PSG-II, revoke/wipe/lock) [4]. Information Providers relies on ARM to control the access to its information and services based on the organizational policies and regulation which may require integrity evidences of trustworthiness to be asserted by PSG-MD. Thus, state of the PSG-MD must be updated, measured, monitored, and reported using mechanisms such as ROT and assertions mechanisms. The process of measuring and reporting integrity evidence of PSG-MD is referred to as “Device Attestation”.

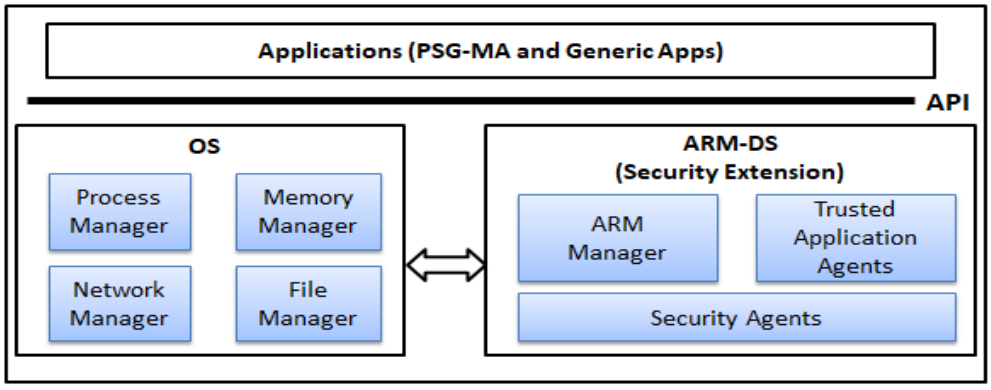

Figure 18 ARM-DS architecture using trusted computing components [64].

Device Attestation:

An attestation is a formal process to ensure the trustworthiness and integrity of the device. An attestation is made by the device to provide integrity evidence in order to gain access to protected resources. Public safety organizations should define a trust metric that must be achieved prior to allow entities to access its information and services. If the device does not achieve the trust metric threshold, the required access shall be denied; otherwise, access to required information and services is granted. Trust metrics may be granted based on ROT that uses assertions to report integrity evidences. However, access to information requires also a set of qualifying attributes to be challenged before granting access (e.g. credentials, role, location, and context), as described in section 9.1. Device attestation requires that the PSG-MD as well as the User to be authenticated to the device, network, and PSG-II, as described in section 9.3. The authentication, assertions, and authorization process is described in details in sections 9.3.3. In general, the overall idea of the PSG-MD attestation in PSG-MAMF is illustrated in Figure 19.

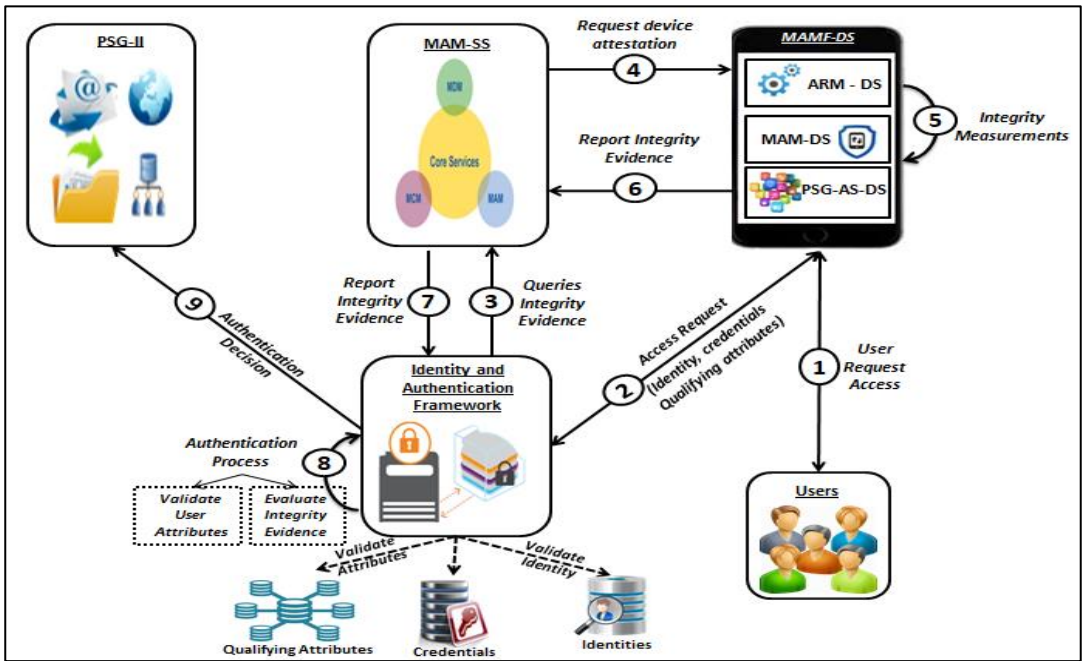

Figure 19 PSG-MD Attestation to ensure the integrity of the device

6.4.5 Assertions for Device Integrity

An Assertion can be defined as "a set of one or more attributes that represents the state of entity in a transaction locally (e.g. between two different information domains on the same device) or remotely (e.g. online through network). That entity can be a person, an object, a process, or a service" [4].

Assertions allow information providers to verify the state of the mobile devices, detect malicious activities on the device and malicious corruption of security components, and reveal if the device state have been intentionally or unintentionally changed in a way that may expose their information and services to potential risk [63]. This way, information providers can request

integrity measurements that illustrate the mobile device current state, accordingly take appropriate actions to protect their information and services, and make informed decisions based on the assurance level. Informed decisions include granting or rejecting access to network and PSG-II. Informed actions include electing to invoke locking the device or selective wipe for their information that already reside the device.

Typically, device assertions can be used to "represent the state of firmware as either verified or unverified, represent the state of an OS as either validated or not, represent the state of file encryption as either on or off, represent the state of the microphone as either on or off, represent the state of the GPS as either on or off, or to represent any state using the mobile device sensor's events, etc." [4]. The MAM-DS is responsible for collecting such assertions from the devices and determines whether the device is in compliance with specific policies [4], and enforce actions accordingly, as shown in Figure 19.

In order to assert device state with cryptographic primitives, PSG-MD requires signing keys that represent the identity of known entity such as device, user, Information Provider, or relevant application running on the device, as discussed in section 6.4.2. NIST provides guide that include principles of the implementation and usage of such identities represented by the signing keys [4]. Furthermore, NIST described the overall assertions lifecycle which consists of: "establishing identities, generating, maintaining, sharing, collecting, and processing of assertions" [4][63]. Examples of integrity assertions are as following [63]:

- Are the device and firmware used been modified?
- What is the configuration, health, or operating system status?
- Who are you and are you trusted? (The Who)
- Are you authorized to perform this process?
- Whether the code or application can be trusted?
- Do the information exchanged been tampered, was such tempering authoritative?
- Do you need to perform this process? (The need to know)
- Can the infrastructure and communication network be trusted?
- Is the situation or context you are involved require and can be trusted to access to such information?

To address such assertions, a set of qualifying attributes have to be challenged to provide evidence that support the access request and the authentication process. Such attributes are described in details in section 9.1. The assertion creation process is described in details in "Assertions Framework for BYOD" [63].

Information Providers may use integrity assertions by relying on Root of Trust (RoT). Thus, RoTs capabilities should be supported by the PSG-MD in order to manage assertions, and to act as the core block for the chain of trust to measure trustworthiness of PSG-MD components. Furthermore, PSG-MA may use the capabilities provided by RoT to store sensitive information including cryptographic keys, authentication credentials, and other record keeping [63].

6.5 PSG-MD Capabilities

Public Safety Grade Mobile Device (PSG-MD) which can be either Public Safety Owned Device (PSOD) or Bring Your Own Device (BYOD) should have wide range of capabilities. As indicated

earlier, this study is focused on devices (PSOD or BYOD) that connect to Public Safety Broadband Networks (PSBN). The potential of devices to connect to wearable and sensors is highly anticipated and will lead to larger list of device capabilities. In the following subsections we investigate basic capabilities known to exist in current devices, and other capabilities that require to be adopted in PSG-MD that connect to PSBN.

6.5.1 Battery Usage

Communication and information in public safety environment are critical, since real time information is important in public safety missions. Public safety environment require much more battery capabilities than normal devices, due to mission-criticality. Right information at the right time can make difference and save lives. Understanding the hardware capabilities, the battery capabilities, and the battery usage on PSG-MD is important to review the required capabilities of batteries in PSG-MD. Following are some essential capabilities for batteries in PSG-MD that are being used in public safety environment:

- Device battery should remain maximally available during and exceeding the time required for public safety activity, and should powerfully run on the PSG-MD nonstop.
- Device battery must be able to sustain continuous use for an amount of time well exceeding a single shift for a responder.
- Device battery should be easily replaceable and easily rechargeable in a quick manner as the need arise.
- Device battery must be able to operate in extreme hot and cold temperature, so that the PSG-MD can serve efficiently in different environments.

In addition, the power consumption of an application on a PSG-MD is critical and must be taken in consider when selecting desired Public Safety Grade Mobile Applications (PSG-MA). Although PSG-MA impact on battery can be mitigated by battery hardware improvements or through the use of supplementary power solutions. Yet, the issue of battery use remains relevant. For example, BYOD trend raises other challenges relevant to battery. Thus, battery technology remains a challenging factor in BYOD scenarios [25].

Furthermore, differences in responder's needs and utilization of devices make the requirements vary between agencies, leading to different power consumption. Some agencies may focus on high-definition resolution while others focus on heat resistance or the need for simultaneous multiple video streaming [25]. In general, the availability of potential live data streams adds more stress on battery consumption. The different roles and operational scenarios of responders influence their demands and choice of battery. According to public safety community, "Field agents may require up to twelve or more hours of battery life, while incident responders may be tethered to a power source. Some responders may require constant usage of their device's screen whereas others may use their devices as simple radios" [25]. Thus, the Users role, agency, and operational scenarios must be taken in consider when identifying the battery requirements and capabilities, and when selecting the applications that to be used on the PSG-MD. In addition, applications are also a major source of batteries drainage.

6.5.2 GPS Capabilities and location services

PSG-MD with GPS capabilities typically runs location services. Locations services, typically, map a GPS location to the entities close to such location. Location services are heavily used in

different areas including mobile application, web browsers, social media, and navigation programs [5].

Location information generated by the GPS and location services are required for enabling location-aware policies and policy enforcement. PSG-MD, PSG-MA, and User require access permissions in order to be able to access PSG-II and information stored on the PSG-MD. The Access Right Management (ARM) should support location-driven policies, and runtime enforcement of security policies. For example, an application can have access to camera according User location and scenario. In order to enable location-driven policies, location information should be accessible to identify the location of the device mapping it to the security policies, and accordingly, the access rights and privileges are adapted based on the security policies associate to the identified location [66].

However, enabled location services on the devices increase the risk of attacks which may expose the device security and personal privacy to potential risk. For example, the attacker can easily determine the location of the device and User, and the sorts of actions performed in specific location. Thus, location information generated by the PSG-MD should be stored in specific secured memory storage on the PSG-MD, and secure location information architecture is needed in order to manage transferring, processing, storing, and sharing of location information in a secure way. Public safety organizations could support standards that organize how PSG-MAs transmit, process, and store location information, and how different organizations and different Information Providers can collaborate by sharing their information in a secure manner.

NIST provided some mechanisms to digitally exchange locations information in a secure manner. However, such mechanisms have to be reviewed and evaluated in terms of their applicability to public safety environment [25]. In addition, Open Mobile Alliance (OMA) provided “user plane location protocol”, “secure user plane location requirements”, and “secure user plane location architecture” for carrying location information using user plane architectures and access methods [67][68][69]. Using user plane location architecture, location information can be locally acquired, and pushed into server side databases where it can be processed and kept secured, and contexts a and accordingly processed in a form of addresses, maps, relevant zones or routes. Location information can be accessed and distributed to desktops, webs, and other mobile devices, with support of automated decision processes. Furthermore, user plane can provide generating-content applications with the ability to capture information using GPS, camera, or sensors, push collected information to server, processes the information at server side, manage the flow of information, and offer access to information from other devices.

Furthermore, the accuracy and freshness of location information are also important considerations. According to the operational needs, it is important to identify what is considered “real time” for location information (e.g. 1 minute, 5 minutes, or best available). Applications should be developed with a capability to refresh location information in specified rate to suit operational needs [25]. Further guidelines in terms of location information handling are provided in Annex E, E.2.

6.5.3 Network Capabilities

PSG-MD should support all wide-area wireless communications such as Commercial Network Services (CNS), Public Safety Broadband Networks (PSBN), and WiFi. Furthermore, PSG-MD should support other network services such as Global Positioning System (GPS) and PAN interfaces (e.g. Bluetooth or NFC). PSG-MD shall use a combination of available wireless access

networks based on availability, security, and QoS. PSG-MD should be able to pick up the best wireless communication as long as the security and privacy requirements defined by their organizations are fulfilled

PSG-MD may use PSBN or CNS networks. Since there is no control over the security of the commercial CNS, public safety organizations should plan the security of PSG-MD on presumption that communication networks between the PSG-MD and the organizations are insecure. The National Public Safety Telecommunications Council (NPSTC) provided a guidance report for design and implementation of the PSBN according to Public Safety Grade (PSG) security requirements.

6.5.4 Sensor Capabilities

Sensors are capable of providing high precision and accurate information that can be used by different PSG-MA. Sensor information is useful in monitoring device movement and changes in the environment around the device. Sensors embedded to the PSG-MD allows it to work as data-generating devices that have the ability to create a stream of data for public safety to improve their situation awareness as well as their decision making. PSG-MD requires to features new, specific, and more sophisticated sensors for public safety tasks in order to assist Users in their critical missions. For example, PSG-MD may have attached environmental sensors that can detect humidity, atmospheric pressure, temperature and ambient sound. Further, public safety Users may need gas sensors that can test air quality and levels of carbon monoxide, propane, and other gases during fire rescue. Such sensors will enable the device to passively monitor and evaluate the surrounding environment [70]. PSG-MD requires sensors to capture biometric and meteorological data in the short-term. Additionally, Public safety community needs to harness industry advances in device sensors such as more precise gyroscopes, accelerometers, and magnometers.

In addition, the sensor's capabilities need to meet PSG requirements. PSG-MD's sensors need to meet such requirements in order to be useful and efficiently serve in the public safety environments. Characteristics need to be taken in consider include accuracy, power consumption, and collected data management including processing, storing, and sharing.

The public safety environment needs to improve the capabilities of PSG-MD, and the quality of the PSG-MD sensors. Using external sensing unit as an extension to the PSG-MD that can be physically or remotely connected, can provide more accurate data stream, and add more capabilities to the PSG-MD. The sensing unit should be able to collect, store, process, and share data with PSG-MA and PSG-MD. "Sensordrone" is an example of an open platform for all kinds of sensors and Bluetooth peripheral device apps that can be connected to different applications on the mobile device. Hence, sensors information can be integrated with PSG-MA so that the PSG-MD can be used as carbon monoxide detector, non-contact thermometer, lux meter, or proximity sensor. Sensordrone is packing more than 11 sensors into one tiny package which are: precision gas sensor, reducing gas sensor, oxidizing gas sensor, non-contact thermometer, humidity sensor, temperature sensor, light sensor, color sensor, pressure sensor, and proximity sensor [71] [72].

The PSG-MD should serve to create, collect, store, process, and transmit sensor's information more effectively. Sensor information must be protected such that PSG-MA and Users must be authenticated before authorized access to such information. Sensor information needs to be stored in specific secured memory storage on the PSG-MD. In addition, sensor information probed from the PSG-MD or from any connected or remotely connected device shall be managed by a

Middleware. 3GPP defined the SCEF [3] network element to provide such a function as described in 3GPP TR 23.708, and TS 23.682 [73][74]. The "Global Sensor Data middleware" [75] may use the LTE Service Capability Extension Function (SCEF) in order to manage transferring, processing, storing, and sharing of sensor information in a secure way. However, using such function in case of the device is connected via WiFi, commercial LTE, or other means that does not have SCEF, is still an open issue that need further investigation.

Another contribution designed "Global Sensor Data Middleware (GSDM)" platform that provide a flexible middleware that aims to address the challenges of integration and distribution of sensor data. GSDM collect sensor data from devices and other external sensors, then organize them according to a standard data model and share data with applications or services when requested as shown in Figure 20 [75]. However, authentication is required in order to gain access to sensor data. GSDM can provide the capabilities required to collect, integrate, process, query, and filter sensor data through a declarative XML-based language. Typically, the sensor can be any type of sensor such as: a real sensor, a wireless camera, a desktop computer, a mobile device, or external sensor unit physically or remotely connected to PSG-MD, or any combination of virtual sensors. Connecting PSG-MD to processing engine allow the integration of sensor data collected by different sources connected to the engine. The combination of different sensor's data can create complex outputs that support context-aware applications with enhanced levels of privacy and security.

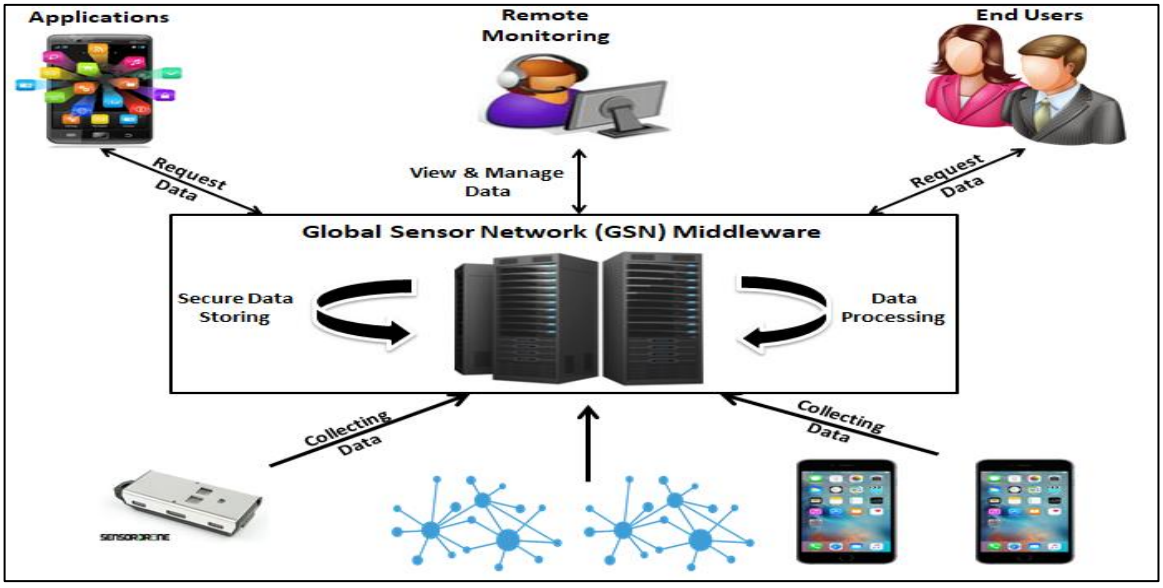

Figure 20 GSN collecting data from sensors, manage and process data centrally, and redistribute data to applications and services when requested [75].

[3] SCEF is a Core Network node that was introduced in 3GPP R13. The Service Capability Exposure Function (SCEF) provides a means to securely expose the services and capabilities provided by 3GPP network interfaces. The SCEF provides a means for the discovery of the exposed service capabilities. The SCEF provides access to network capabilities through homogenous network application programming interfaces (e.g. Network API) defined by OMA, GSMA, and possibly other standardisation bodies. The SCEF abstracts the services from the underlying 3GPP network interfaces and protocols.

6.5.5 Memory

PSG-MD requires continuous working even in catastrophic situations and for extended period of time, thus, PSG-MD's memory needs attention. PSG-MA stores their related information in the PSG-MD's memory. Hence, memory architecture, management, and security must be considered. PSG-MA information needs to be protected from other malicious applications by providing potential solutions to address such concerns.

PSG-MD requires integrity check in order to enhance its security. Thus, it is necessary to protect the system during the initial boot stage. A "secure boot" is sometimes supported by chipsets having specific secure hardware features, however in many cases, the boot procedures rely on a code stored in memory, as provided in section 6.3.2. Hence, proper memory security features can provide the most benefit and first line of defence to enhance PSG-MD security [76].

In addition, PSG-MD requires proper technologies and solutions to overcome memory corruption and unauthorized use of memory. To ensure the non-volatile flash memories integrity, hardware, software and combination solutions are required to protect information stored in memory.

PSG-MD may be subjected to normal/abnormal shut down, or physical tamper (e.g. unusual reboot procedure) which could lead to memory corruption and stored information could become irretrievable. To ensure the PSG-MD storage integrity, it is essential to understand the kinds of storage corruption an unexpected power failure can cause [77]. Therefore, public safety community should consider proper policies to apply in the case of abrupt shut down or physical tamper (e.g. unusual reboot procedure).

Furthermore, PSG-MD can have additional security functionalities in terms of storage either by hardwired security logic such as memory smart cards (e.g. USIM, high capacity USIM and eSIM) which provide flexibility of doing reprogramming over air, or using a chip circuit (e.g. TPMs – Trusted Platform Modules) which provide possibility to perform computations and implement cryptographic algorithms. TPM can act as hardware Root of Trust (RoT) that is required to support some security functionalities required by PSG-MD. RoT can also be implemented as firmware, software, or at least a code protected by hardware [78].

6.5.6 Smart cards - Universal Integrated Circuit Card (UICC)

Mobile devices are partitioned into two separated components: the Mobile Equipment (ME) and the Universal Integrated Circuit Card (UICC). The UICC is a removable component that usually contains important information about the User and is the only way to connect to network, and can sometime referred to it as "identity module". The UICC is the physical smart card and different mobile network applications can contain and run the following applications: Global System for Mobile Communications [GSM], Subscriber Identity Module [SIM], Universal Subscriber Identity Module [USIM], CDMA Subscriber Identity Module [CSIM], IP Multimedia Services Identity Module [ISIM], etc. USIM application is the application used nowadays and runs on the UICC in LTE network.

UICC typically consists of "processor, Electronically Erasable, Programmable Read Only Memory (EEPROM), RAM for program execution, ROM for the OS processes, Algorithms for authenticating users and encrypting information, and other applications" [6]. The UICC plays three important roles on the mobile device:

- Store network parameters and subscriber identifier securely and identify to the network
- Authenticate the device user to the network to allow access to subscribed services.

- Provide an extra storage for user personal information, such as phonebook entries, text messages, and last numbers dialled. Such storage is usually more secure than the mobile device memory.

The UICC OS controls access to elements of the file system. According to the application, UICC operating system can be categorically permit or deny actions (e.g. reading or updating), or provisionally permitted according to specified access rights. Access is permitted to users through authenticating using Personal Identification Number (PIN), such authentication is referred to later as user-device authentications, and is essential to ensure information security and integrity [6].

Furthermore, UICC authenticate the mobile device to the network securely. Such process requires the use of algorithms (e.g. LTE standards), protocols (e.g. Authentication and Key Agreement (AKA) protocol), and Cryptographic keys to securely authenticate the device to network without exposing keys and other sensitive information that may expose the UICC to potential attack that can gain access to information and services [79] [80]. Cryptographic keys support cyber encryption capabilities that protect from eavesdropping on the air interface [6]. Furthermore, UICC can store multiple profiles (e.g. work and private) that could be selected and used by the user. This capability supports the public safety need to isolate the public safety information and user's private information in a BYOD configuration.

Over the past few years, great efforts were given to improve the security features of the mobile device storage including credential storage by taking the advantage of UICC. In general, storage security features of the mobile devices can be improved by adding some form of Secure Element (SE) that has the ability to perform storage security tasks. However, UICC (more specifically, USIM) used today are programmable, and are flexible for reprogramming over air. Such capability grabs attention to the USIM to be used as a Secure Element (SE) to enhance the security of the mobile devices, and most commonly mobile applications.

6.5.6.1 Universal Subscriber Identity Module [USIM]

USIM is a smart card with an embedded integrated circuit. The smart card is kind of Universal IC Card (UICC) and USIM is an application running on top of UICC. A SIM card have a microprocessor and consists of Central Processing Unit (CPU), working memory, RAM, program memory, ROM, EEPROM, and serial communication module. Typically, the SIM operating system is stored on the ROM, while the application and information are stored on EEPROM.

USIM works on UMTS and LTE. USIM offers more security compared to SIM due to the use of "Milenage algorithm"[4] for mutual authentication. Furthermore, USIM offers a larger storage compared to SIM. USIM could also have applications written on to it including java applications.

Dynamic modification of the user subscription and setting can be done over the network using (OTA) management capabilities. USIM cards are supporting applications management features including Over-the-Air (OTA) updates via binary SMS (e.g. enable downloading of application OTA) and enable interoperability across card manufactures for installing and loading of Java-

[4] Milenage algorithm: is 3rd Generation Partnership Project confidentiality algorithm that is used for authentication and key generation. Milenage algorithm is typically used by most network operators specially for LTE to generate authentication keys, and a secure communications between mobile subscribers and their associated operator networks using mutual authentication

based applets onto the SIM card from any source. In general, the only way to load applets on the USIM is to implement OTA by wrapping card commands (APDUs) in SMS, which the mobile device forwards to the SIM. Thus, some tools that support SIM OTA (e.g. SIMalliance loader [81], or implement APDU wrapping/unwrapping) are required, including the necessary encryption and integrity algorithms needed for such process. The major use of OTA functionality is to install and maintain SIM Toolkit (STK) applications, which provide mechanisms for the applications existing in the UICC to interact with mobile devices which support specific mechanisms required by the application. In general, android devices supports the STK applications which make it internally support the communication with the USIM, hence, android devices could have internal interaction with USIM.

The USIM card runs a separate operating system from the device's operating system, that provides more secure communication between the USIM and device, and hence, the USIM act as a firewall between the device and the information on the USIM memory, consequently adding secure capabilities to the PSG-MD. However, the operating system explicitly doesn't allow low level access of third party applications to SIM cards. This was usually being a great challenge that stands upon using the SIM card as a Security Element (SE). Some efforts were given to implement an Open Mobile API that aims to provide a unified interface (e.g. SIMalliance Open Mobile API [81]) for accessing Security Element (SE) on Android, include the USIM. SIMalliance provided more details about how the Open Mobile API implemented and works, and how access to the SIM card can then be implemented in android [81] [82].

By connecting the mobile device to the SIM card, mobile applications can be then connected to the SIM card. PSG-MA can leverage UICC access and use it as a Secure Element (SE) to perform security tasks. PSG-MA may leverage UICC applets to provide security capabilities like storing data and keys securely and performing cryptographic operations without keys having to leave the card. PSG-MA can benefit from using the SIM card and a Secure Element (SE) to store authentication keys and other sensitive information. Some applications rely on SE to store encrypted passwords, where Users may need to provide a passphrase to derive a symmetric key, which is in turn used to encrypt stored passwords. This way, it is hard to recover stored passwords without knowing the passphrase. However, OS platforms should provide access to UICC applets by supporting an existing third party API (e.g. SIMalliance Open Mobile API) [81]. This API will enable the interaction between mobile applications and the applets running in the UICC.

For an ideal key management and encryption solution, all key management and encryption logic should be done inside the Secure Element (SE), and the PSG-MA would only provide input and retrieve encrypted information. The SE applet should provide encryption as well as guarantee the integrity of the encrypted information (e.g. by using an algorithm that can provide authenticated encryption).

In addition, all the recent SIM cards are based on Java Card technology; Figure 21 illustrates the current java card SIM architecture. The Java cards capabilities make it possible to develop and install an applet that has access to OTA keys. However, such capability is not naturally available for commercial SIMs, thus, public safety organizations would need to consider providing a programmable SIM to the Users that allows applets loading without authentication, or otherwise the SIMs come strapped with the required keys. This way, applets can be automatically loaded using OTA mechanism and PSG-MA can take advantage of such applets and then be distributed through PSG-AS. Public safety organizations may rely on existing guidelines and implementations to implement such technology [81] [82]. In addition, public safety organizations may rely on any existing applets that offer a key management interface. SIMalliance provided a

set of mandatory requirements for API that manage access to UICC applets. The idea is to set up the PSG-MD to use the SIM card as a secure element.

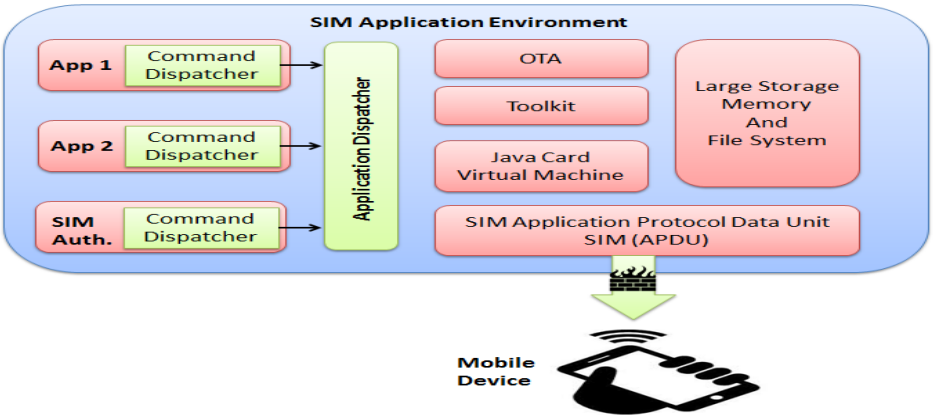

Figure 21 Current Java Card SIM Architecture

Although USIM can support the idea of isolation, protected storage, and can be used as a Secure Element (SE), USIM still has limited resources and limited storage. Recently, more advanced type of USIM with higher capacity has been introduced under the name "High Capacity USIM". By having a USIM architecture that supports larger memory storage, PSG-MD can take advantage of such USIM to provide protected storage and protected execution functionality for PSG-MA.

6.5.6.2 High Capacity USIM (HC-USIM)

HC-USIM is enhanced category of USIM, with higher CPU performance, mass storage, and higher speed interfaces. A HC-USIM card has an integrated card and a flash memory embedded together, to provide an internal USIM storage using a flash memory. Compared to traditional SIM cards, HC-USIM can have 10-100 Megabytes of non-volatile flash memory, while the traditional USIM have only 10-100 Kilobytes of non-volatile ROM and EEPROM memory [83]. However, since flash memories don't provide security, an encryption algorithms need to be used to encrypt flash stored information. Furthermore, the HC-USIM can provide the PSG-MD with management features for public safety information, while separating PS information from user's personal private information. HC-USIM is designed to include "CPU, EEPROM, RAM, memory controller, and flash memory. It also provides interfaces to International Standards Organization (ISO), Multi Media Card MPEG (MMC), and Universal Serial Bus (USB) to communicate with the host application" [84], as shown in Figure 22. Table 3 provides the features of HC-USIM compared to traditional USIM and flash memory. In general, HC-USIM can provide the public safety environment with the following capabilities [84]:

- HC-USIM provides secured trusted environment that can protect information securely during storage and execution. Further, it contains cryptographic co-processor to perform arithmetic operations efficiently.
- In a BYOD configuration, HC-USIM enables users to manage their information using the HC-USIM isolation mechanism.

- HC-USIM can be used along with Access Right Management (ARM) to enforce relevant organizational and information policies on the PSG-MD. PSG-MAMF may rely on ARM to enforce policies and ensure that information is consumed on the PSG-MD according to the rights. PSG-MD must contain ARM agents that executes all security functions and manages the access rights enforcement. In order that ARM scheme to be truly robust, the ARM agent should reside in a trusted tamper-resistant environment. Obviously, HC-USIM can provide such an environment [83].

Table 3 Advantages of HC-USIM [84]

	USIM	**Flash Memory**	**High capacity USIM**
Advantage	• Securable • Controllable	• Large storage • Support multimedia services • Support high speed interfaces • Multimedia-based GUI	• Compatible • Large storage • Support high speed interfaces • Securable
Disadvantage	• Slow interface • Limited storage • Text-based GUI	• Not secure • No control	

Information Security Solutions Europe (ISSE)/SECURE 2007 Conference included a document that discussed the security aspects of HC-USIM by comparing it to traditional USIM, and proposed architecture for the new generation of USIM by referring to it as “High Density USIM”. In addition, the (ISSE)/SECURE 2007 document discussed the security features of HC-USIM and the enhanced security applications including the Access Right Management (ARM) functionalities on the mobile device considering the use of HC-USIM.

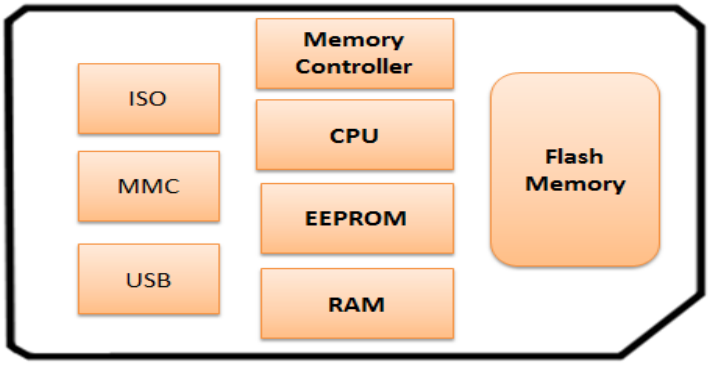

Figure 22 HC-USIM Architecture[84]

Annex D provide another HC-USIM architecture that was proposed by researchers at KOREA University. Such HC-USIM architecture was examined in terms of its applicability to environments that require sophisticated security (e.g. public safety environment), and the enhanced security features of the PSG-MD as HC-USIM new generation introduced to the real world. The proposed architecture also illustrates the HC-USIM secure storage area, where Users and applications need to be authenticated in order to have access to the information stored in the secure storage area. Within such storage area, the smartcard performs encryption and decryption, while providing encoded and decoded information without disclosing the keys. Encrypted information stored in the secure storage area can be accessed only by authorized entities. The architecture discusses the security schemes of the HC-USIM internal storage considering the areas that worth protection. Such scheme considers dividing the internal storage into Secure System Area (e.g. key storage, applications), Secure Service Area (used by services and content providers of applications to store information), and Secure User Area (e.g. User private information that can be accessed only by the User) [84].

HC-USIM represents an innovative solution for a secure, large storage capacity, and sophisticated cryptographic functionalities co-exist on the same ship with such new generation of SIM cards. Although HC-USIM technology doesn't exist yet in the market, however, introducing HC-USIM would represent a leap in the SIM cards and security technologies. However, such new architecture introduces new challenges in terms of security that requires further investigations [83][84][85]. Furthermore, additional encryptions algorithms need to be taken in consider for encrypting information stored in the flash memory.

6.5.6.3 Embedded SIM (eSIM) or embedded UICC (eUICC)

The eUICC is a reprogrammable SIM which can be defined as a small trusted hardware component that can be embedded in the mobile device to run the SIM application. The eSIM is embedded into the device; it must be reprogrammed Over the Air (OTA). The eSIM runs secure network access applications, securely changing subscription data and identity, and also performs the role of traditional UICC, provide more protected storage due to the embedded capability, and provide other security services. The eSIM is a combination of traditional SIM, additional features, and an ecosystem. One of the additional features is the support of remote management of operator credentials, set of interfaces and standards to allow those credentials to be transmitted securely between the operator and the UICC. The ecosystem provides the integrity and trust needed to protect users during the transport of information [86]. To provide the level of security required for eSIM, all entities involved in the platform and profile management have to be mutually authenticated [86]. The GSM Association provided a document that discuss in details the remote provisioning architecture of eSIM [87].

Advantages of eSIM over the traditional SIM:

(1) In traditional removable SIM, users can change SIMs by physically remove the SIM and replace it with another. However, in embedded SIM (eSIM), users rely on the Subscription Manager (SM) to do the switch.
(2) eSIM provide a flexible connectivity by supporting several connectivity profiles, but only the profile being used will be activated. While in the traditional SIM, only 1 profile is loaded when manufacture of the SIM card.
(3) eSIM support swapping between profiles rather than switching as shown in Figure 23 SIM swapping change the profile temporarily and the user can return back to the previous

profile when needed. In addition, swapping can be done nationally or internationally. The idea of swapping in real time can provide the public safety with the following additional functionalities:

- Swapping profiles facilitates an easy way for PSG-MD to hop between public safety private LTE networks and multiple network carriers.
- Responders can swap profiles to different operators to improve coverage and quality of service when needed.
- Swapping can be done automatically without User interaction; such capability can enable the selection of best mobile network operator and connect to it automatically and faster to improve the quality of service during emergency situations. In addition, there will be less potential for loss of connectivity to occur, since each device is self-managing.
- Coverage management provides the PSG-MD with further capabilities.

(4) An advantage of eSIM is to be able to change service provider for fleets of users. For example, an agency may change provider for hundreds or thousands of users would not need to re-issue new SIMs to all users. However, eSIMs can be reconfigured by reprogramming it Over-the-Air (OTA).

(5) eSIM can support cypher security services by act as a Secure Element (SE) to provide a firewall that detect threats and attacks during data transmission, and also can be used to ensure device integrity.

(6) eSIM also provide a security benefits due the virtual SIM card nature and the lack of physical SIM that can be removed from the device. In case of the device lost/stolen, the eSIM can't be removed from the device, thus, there will be benefits from a tracking perspective.

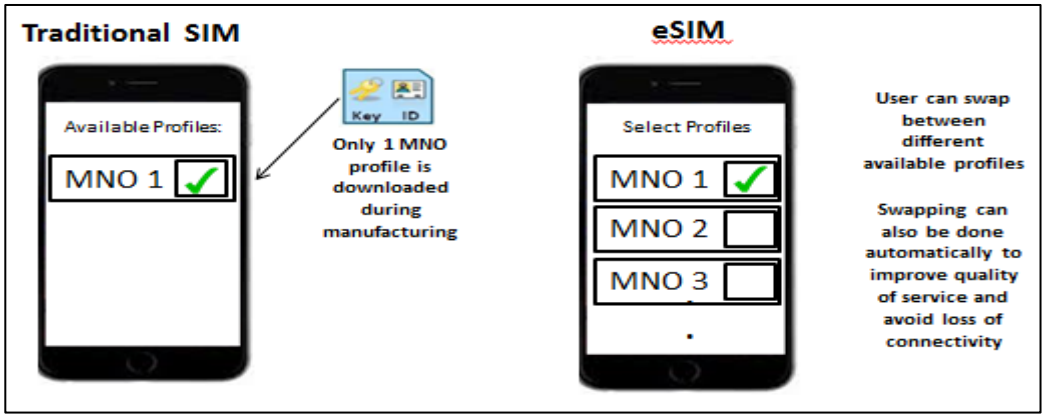

Figure 23 Comparison of traditional single-profile SIM and multi-profile eSIM [86].

Public safety organizations need to consider that eSIM requires suitable mobile devices that support suitable capabilities. The eSIM requires further investigation in terms of additional policies and requirements of PSG-MD to leverage the capabilities required to securely connect to network, provides more secure communication between the eSIM and device, and to be used a Secure Element (SE).

7 System Component: Application

Mobile applications can potentially lead to serious security risks, since applications may expose the PSG-MD to potential threats and vulnerabilities that are liable to attack. An attacker can exploit such threats and vulnerabilities in order to gain unauthorized access to public safety information and services, or private information.

Public Safety organizations should be aware of the potential security risks of mobile applications and their effect on PSG-II, information residing the PSG-MD, and Users. Such awareness will help public safety organizations plan for application's risk mitigation strategies and adopt the appropriate security technologies. In addition, the potential of "zero-day vulnerabilities" [5] should also be taken in consider when planning the security of mobile applications.

Public safety organizations must state their operational and security requirements in such a way that application behaviour and security can be assessed. The security requirements are mainly to address the integrity, confidentiality, or availability of information, and then applications should be assessed against the risk of compromising either integrity, confidentiality, or both. In order to apply mitigation strategies that can address most significant risks and threats, public safety organizations may follow NIST recommendations and guidance, as following:

- Public Safety organizations should first define their operational and security requirements that address overall mission's requirements [5].
- Apply decision balancing approach in order to select the mitigation strategies and technologies that balance between operational capabilities requirements, security requirements, and cost requirements [5].
- Apply a risk management framework in order to leverage mitigation strategies and technologies according to risk-based tailoring approach. The risk-based tailoring approach should identify, assess, and prioritize the potential risks on mobile applications, and determine their prospect and impact. This way, the mitigation strategies and technologies address most significant facets of risk which expand operational, security, privacy, technology, policy, etc. [35] [36].
- Select the appropriate security controls, technologies, and solutions that according to mission requirements, balancing and trade-off between requirements, and tailoring of risk approach.

Depending on the risk assessment, public safety organizations may define a set of general requirements that include predefined application capabilities and limitations. For example, public safety organizations may define the security requirements associated with applications such as sensitivity of applications, the acceptable level of impact for an application that would occur if the confidentiality, integrity, or availability were compromised, specific cryptography requirements, and other predefined attributes [23][57]. In addition, there may be also requirements that control some of the PSG-MD functions (e.g. only certain applications may

[5] Zero-day Vulnerabilities are known as "vulnerabilities that are not yet known to the vendor and hence have not yet been patched" [2].

access the camera). The public safety organizations may also define a set of security policies in terms of dealing with resources and information, and control access rights. For example, an application can have access to device resources (e.g. camera) according User location or scenario. The Application Store Management shall define the PSG-MA access scope; hence, the PSG-MA can't access information out of its intended scope. For example, if the application access scope is health care information, application can't access different database outside of its scope using the User access permission. The application is only allowed to access resources and information within its predefined scope.

Security Assessment and Authorization (SA&A) must take place to provide end to end assessment. To ensure that developed applications are incompliance with the predefined security policies and attributes, an assessment should be carried out to evaluate the applications. The assessment process assesses the SA&A process by providing testing evidence in terms of application compliance with the public safety security controls. The software assurance process refers to "the assessment to be carried out to determine the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and the software functions in the intended manner" [23]. In addition, the software should comply with the public safety security controls. The assessment must produce a risk metric by assigning a score to the application that the operational authority can rely on to decide whether to accept or reject the application. In addition, whenever a new version or a new application becomes available, the assessment process has to be carried out from scratch.

There are some existing mobile application security standards that can be used to provide a standard software assurance processes to evaluate applications [28]. Public safety organizations may use similar standards to provide them with baselines for security requirements and policies, and helps them to express their security requirements and policies. The standards can also provide Application Developers with a list of requirements for developing secure PSG-MA, and can provide a basis for testing application security controls, as well as any security controls required in the public safety environment. Thus, the need for security standards is important for the following objectives:

- Metrics: standards can provide the public safety organizations and Application Developers with a metrics that can be used as a yardstick to assess the degree of trust that can be placed in the developed PSG-MA.
- Guidance: standards can be used as a guidance to provide the Application Developer with guidance into what to build into the security controls of the application in order to satisfy the application security requirements.
- Verification: standards can provide an idea of the type of application security verification requirements for the testing process.

The software assurance process may follow common criteria to perform evaluating for the applications against their compliance with set of controls [23][25][56]. If the application passes the test against the security controls, it can assess a protection profile level. This allows the SA&A process to take advantage of priori tested applications. Hence, protection profiles would have to be developed to test applications for the vetting process. It is recommended that the applications going to the PSG-AS be tested in the same manner. The process of vetting applications referred to process of evaluating applications that include a sequence of activities or

processes that aim to verify the applications incompliance with public safety requirements and security controls.

An application vetting criteria supported by PSG-MAMF consists of: (1) public safety organizations define their security requirements with the help of existing mobile application security standards and metrics, as described in section 7.5.1. (2) Application Evaluation and Scoring, involve evaluating the security of applications, and ensure the application conformance to the security requirements developed by the public safety organizations. The evaluation process may follow common criteria that assess applications and determine their performance against a set of security controls. The evaluation results in a score that specify the sensitivity of application and level of impact associate with such risks. The evaluation and scoring process is described in section 7.5.3. (3) Application testing, this involves risk assessment to identify the system vulnerabilities and produce risk metric that can assess the SA&A process. Then sensitivity assessment have to carried out to test applications against such software vulnerabilities, and verifying the application compliance with the pre-defined security verification requirements. The testing process may also verify the set of permissions required and how permissions are processed by the application. The testing process is described in section 7.5.4. (4) Application approval or rejection according to the evaluation results, and providing a report of scope verification, a summary of verification finding, and clear instructions of how to resolve the failed test that is forwarded to the Application Developer, as described in section 7.5.5. (5) Continuous monitoring, in which any applications updates or new versions must be tested again and approved, as described in section 7.5.6.

7.1 Classes of Applications

There are two fundamentally different classes of applications that provide the PSG-MD with the required capabilities to support public safety Users in performing necessary duties, first; Generic Applications, and second; Public Safety Grade Mobile Applications (PSG-MA).

7.1.1 Generic Applications

A Generic Application is an application developed for the general public, such as word processing applications or browsers. Vendors of Generic Applications are unlikely to release different versions of Generic Applications to accommodate public safety particular needs. Yet, public safety Users have legitimate and valid reasons to rely on Generic Applications. Generic Applications shall include: browser, email, chat, camera, social apps, and navigation, among wider range of applications.

Generic Applications may be used by public safety users for personal purposes as well as accessing PSG-II, especially in the case of BYOD scenarios. As an example, Public safety Users may use browser to access information residing on the PSG-II, email, text services, camera, and many other commonly known applications.

Generic Applications raise potential security risks and vulnerabilities that may be exploited. Thus, Generic Applications require special considerations as they deal with information sharing in a more relaxed way. However, most risks pertaining to Generic Applications are well understood and there have been great efforts over the years to identify and develop policies and regulations to manage and control the security risks of Generic Applications.

7.1.2 Public Safety Grade Mobile Applications (PSG-MA)

Public Safety Grade Mobile Applications (PSG-MA) are applications developed or deployed specifically for public safety organizations to enable access to PSG-II and can be used by public safety Users to provide field support and enhanced situational awareness. By integrating variety of public safety tools and situation awareness capabilities, mobile apps can allow public safety Users to have enhanced operational awareness, including real-time information sharing.

PSG-MA can satisfy a higher level of reliability, security, and policy compliance compared to Generic applications. Since the OS is linked tightly to the PSG-AS, downloading applications through means other than the PSG-AS in not allowed. In addition, PSG-MA must satisfy high levels of security at the vetting stage and throughout the application life cycle. Even in closed ecosystem application stores, it has been observed that malware-infected applications may exist. Compromised or malicious applications present a major threat to the security of public safety information and ultimately to the safety and security of public safety Users and emergency responders as well as the public at large. PSG-MA has to be vetted before being uploaded to the PSG-AS. The vetting processes have to be performed on PSG-MA after the PSG-MA has been developed by the Application Developers and released for distribution through PSG-AS, but prior to its deployment on PSG-MD. The vetting process aims to provide a software assurance process to evaluate the PSG-MAs incompliance with the public safety organizational policies, security requirements, and set of controls. It is recommended to follow common criteria for testing applications such as NIST and ITSG mechanisms to provide software assurance for applications [23][25][56]. The assessment assigns a score to each application that the operational authority can rely on during the SA&A process to decide whether to accept or reject the application.

The accepted PSG-MAs will be available for Users only from PSG-AS, and also can be pushed to the User's devices by the Management and Administration. PSG-MA could be managed and monitored on the PSG-MD using mechanisms such as Mobile Application Management (MAM) platform.

In addition, Access Rights Management (ARM) can provide a solution to enforce information and application handling requirements. DRM system can provide the guarantees that public safety rules and policies are extended to the PSG-MA and information on the mobile framework, and enforce handling requirements. The access to information can be controlled by handling the metadata tied to application or information asset using the right management capabilities on the PSG-MD. If the handling requirements are tied to the application, the metadata reside within the application, however, if the handling requirements are tied to the information asset, the metadata must always travel with the information asset. The right access management capabilities can be provided by the applications, the operating system, or both. However, in order for the application to handle requirements, PSG-MA has to be ARM enabled by using ARM SDKs[6]. This way, the PSG-MA can use the functions and capabilities provided by the ARM system in order to encrypt

[6] Software Development Kit (SDK) is "a set of software development tools that allow the creation of applications software framework, hardware platform, computer system, video game console, operating system, or similar development platform. To enrich applications with advanced functionalities, application developers implement specific software development kits (SDK) that provide the applications with these functionalities" [129]. ARM SDK is a specific SDK to build applications that have the ability to apply access right management features including management files interpretation, policies enforcement, and ARM-protected files mechanisms [130] [131]

and decrypt information, acquire licenses and certificates from ARM, and then perform security tasks [65]. The proposed ARM system is discussed in more details in section 6.4.3.

The communications between the PSG-MA and the PSG-II, PSG-MA and PSG-MD operating system follows the communications rules that require end-to-end encryption at all times. Interoperability is important issue that must be taken in consider due to its impact on applications several levels such as between applications and user device operating systems, user device-generated data, and network-generated data. It is important to continue the efforts of enforcing NIEM standards on the growing PSG-MAMF efforts.

7.2 High-level Threats and Vulnerabilities of Applications

Applications usually pose threats relevant to security. Mobile devices are typically exposed to the same threats as desktop devices, and additional security threats. Mobile devices are exposed to additional threats compared to desktops due to their mobility nature, size, portability, access to wide range of network services including short-range data connectivity (e.g. Bluetooth and NFC, WIFI, and 4G/Long Term Evolution (LTE)), sensors (e.g., camera) and location services and GPS. Mobile applications may have access to location information, sensor information, personal health information, photos storage, and audio, which expose them to various security challenges and subject information to risk in terms integrity, confidentiality, and availability [38]. In case of PSG-MA, applications may also have access to PSG-II. All these capabilities can be used by malicious means to forward information outside of the mobile device.

In general, mobile devices attacks typically take place among four various activities which are: software downloads, using browsers to visit a malicious website, direct attack through the communication networks, and physical attacks. All security controls already exist and applied to desktop applications need to be applied to mobile applications. However, mobile applications require additional security controls in order to mitigate the additional security concerns due to mobile device nature in terms of untrusted nature of device, mobility, using vulnerable wireless communication, using vulnerable permissions, and vulnerabilities related to security policies, as discussed in section 2.5.

Most of mobile device vulnerabilities are relevant to mobility and physical unauthorized access to the device itself. Section 2.5 summarizes the common efforts over the years to identify the threats and vulnerabilities of mobile device. This subsection provide an overview of the most common vulnerabilities and security concerns in terms of applications running on the mobile device compared to desktop applications [23][5].

7.2.1 Lack of Physical Security Controls

Mobile devices are most likely to be lost or stolen due to their size and mobility nature. Losing control over the physical device raises vulnerabilities in terms of applications and information compromise. Thus, public safety organizations should consider that mobile devices could be accessed by unauthorized parties aiming to gain unauthorized access to information stored on mobile device or use PSG-MA to access PSG-II. Hence, appropriate security policies and security controls should exist in order to lower the impact of such compromise to lowest damage.

To mitigate the lack of physical security controls, more additional security controls are required to mitigate the risk of mobile applications compromise and protect their information. One way involve requiring authentication before gaining access to PSG-MD, PSG-MA, and public safety

organizations information and resources stored on the device or accessing PSG-II through the device. However, PSG-MD requires more robust forms of authentications to provide more security controls. NIST SP 800-63-2 “Electronic Authentication Guidelines” provided guidelines for implementing e-authentication process. Public safety organizations shall consider appropriate authentications technologies that meet the required level of assurance [14]. PSG-MAMF provide different types of authentications aiming to authenticate each single entity within the system, as described in section 9.3

Another form of mitigation involves protecting public safety information from being recovered by unauthorized parties, by isolating public safety information from other information stored on the mobile device, and encrypting the mobile device’s storage used to store public safety information. In addition, control access to information using capabilities provided by Access Right Management to guarantees that public safety organization security policies are extended to the PSG-MA on the mobile framework, and security policies are enforced on the PSG-MA. Finally, mitigation may involve awareness and training, to aware public safety users of potential security risks and common practices that may reduce the risk of physical compromise.

7.2.2 Use of BYOD

Typically, mobile devices are untrustworthy due to the lack of any form root of trust security features that already exist in desktop devices (e.g. trusted platform modules, TPMs). The built-in security controls are usually not enough to fully mitigate the security risks associated with mobile devices and application, and to provide the security requirements that well-suit the need of public safety organizations. Mobile devices are frequently suffer from rooting or jail-breaking that can allow users or other unauthorized entities to that may that results in bypassing security feature and introducing of other potential vulnerabilities and security threats In addition, Bring Your Own Device (BYOD) raise additional security concerns in terms of information storage, access, and sharing.

To mitigate the risk associated with untrusted devices including BYOD usage, mobile devices shall undergo different vetting processes to provide higher degrees of assurance of the trustworthiness of PSG-MD and ensure they have the security capabilities required to be qualified as PSG-MD. Section 6.4 provides the essential security components to qualify PSG-MD. In addition, BYOD should be tested to insure compliance with public safety security controls and BYOD security policies, to ensure they are fully secured and qualified before deploying PSG-MA on them, and allowing them to access PSG-II. If the BYOD device satisfy the security controls and policies, it approved by the public safety organizations allowing them to be used in public safety environment. Otherwise, restrict or prohibit the use of BYOD device, and favours Public Safety Owned Device (PSOD). Further, any changes in BYOD configuration, any tampering, or jail-breaking with a BYOD should be remotely detected to ensure the device remain incompliance with the public safety security requirements and policies. Section 6.1 discusses further considerations and policies for the use of BYOD in public safety environment.

Furthermore, PSG-MA shall run in secure isolated containers on the PSG-MD to protect their processes and related information. There are some technical solutions can be used to ensure the integrity and trustworthiness of PSG-MD, PSG-MA, and any part of the mobile device, and deviations from trusted state can be identified, monitored, and addressed.

7.2.3 Use of Untrusted Communications and Networks

The application communication can be internally or externally. Internal communication protocols are the means by which the application communicates to pass information within the device, either to itself or to other applications. While external communication protocols are the means by which the application communicates to pass information outside the device. Vulnerable communication present potential security risks to the device and the information residing the device.

Internal vulnerable communications of PSG-MA are addressed using DRM and containerization solutions, while Generic Applications are following current safe policies and regulations to manage and control their security risks.

While external communications allow the application to communication via network. PSG-MD may use wide range of communicate networks to access PSG-II including WIFI and LTE, thus, there is no security controls over all the communication networks a PSG-MD may use. These communications systems may be eavesdropped, which may place public safety information transmitted through network at risk of compromise.

Risk of external communications and untrusted networks can be mitigated by providing secure encrypted end-to-end communication channels, and encrypt distributed information. Encrypting communication channels and technologies (e.g. VPN) can protect distributed information against compromise. In addition, authentication mechanisms can be used to verify identities before granting access to network and PSG-II.

Consequently, internal and external communications are secured in the PSG-MAMF and access to information and services is controlled efficiently as shown in Figure 8. In addition, network permissions shall be verified during the vetting process to ensure the application is using network permissions in a proper way.

7.2.4 Use of untrusted applications

Mobile Applications poses obvious security relevant weaknesses that leave the PSG-MD, PSG-MA, and information vulnerable to exploitation by attackers. Public safety organizations should plan their security requirements and policies on the assumption that applications are untrustworthy. Threats and risks of mobile applications can be mitigated in different means, including:

- Prohibiting applications download from other means rather than PSG-AS
- Application should undergo a risk assessment and vetting process before permitting its publish on PSG-AS and distribution to use on PSG-MD
- Implementing containerization in order to isolate the PSG-MA and its related information from all other applications and information on the PSG-MD.
- Control applications access to information using capabilities provided by Access Right Management. Such mechanism can provide the guarantees that public safety rules and policies are extended to the PSG-MA on the mobile framework, and enforce rules and policies on the PSG-MA.

Public safety organizations should also consider that even security controls and mitigation strategies may not address security threats due to accessing web-based applications through

browsers built into PSG-MD. The security controls over the web browsers are limited, which may raise additional security vulnerabilities. Such challenges need to be addressed by the application itself, and other additional security controls. One way to mitigate the risk of using generic browser is directing mobile device traffic to PSG-II through secure gateways or other intermediate devices to assess URLs before granting user's access to such URLs. Providing encrypted end-to-end communication using encrypting technologies (e.g. VPN) to minimize the exposure for public network and protect distributed information and services from compromise. Another mitigation strategy is using a separate browser within a secure execution environment. Users are enforced to use such protected browser for all browser-based access related to the public safety organizations, while using mobile device's built-in browser for other uses. Accessing web-based application using generic browsers requires more investigation and further work to identify the common risks associate with using such browsers, and to identify potential mitigation strategies to address such risks. In addition, browser cache raises security risks in terms of information storage that need additional security controls to be mitigated.

In addition, all mobile devices can connect to organization infrastructure through a Virtual Private Network (VPN), to minimize the exposure for public network. Mobile applications connect to organization infrastructure through the Mobile Application Gateway. The network gateway and security stack allow only the passing of Mobile Application Gateway traffic.

7.2.5 Use of Untrusted Permissions

Desktop operating system built around a multi-user security model, by isolating users to ensure that one user could not attack another user on the same device. However, for the mobile devices, the main threats are malicious attacks from different malicious means (e.g. malicious application). Thus, mobile operating systems are designed in such a way to provide much more fine-grained permissions to address such threats. The existing mechanisms (e.g. application containerization, permission systems, app store) help make the device generally pretty safe. Thus, the mobile operating systems focus on protecting device from malicious applications actions and isolate applications from each other, rather than isolating users from each other.

Mobile devices require much more privacy and security considerations due to mobility, wide range of sensors, permanent network connection, and frequent software downloading. Mobile devices have variety of sensors that can capture a lot of valuable information such as photos, videos, location information, temperature, motion, etc. Mobile applications may request permissions to access functionalities on the mobile device, so that the application can perform the intended functions. Applications must declare the permissions that allow access to controlled functionalities such as using camera, GPS and location services, internet access, reading or writing to SD cards, or any function required on the mobile device. In addition, since permissions are vulnerable to being hijacked by an intruder, permissions requested by applications shall represent the application and User needs without exceeding or lowering the legitimate demands set by policy makers.

Thus, mobile operating systems have fine-grained permissions compared to desktop operating systems. However, current permission systems in mobile devices are following approach that can't be applied in public safety environment. PSG-MD requires more fine-grained permission systems to support a rights management and access control approach. Thus, policy-based, location-based, and context-based permissions are required to control the access of PSG-MA to functionalities, information, and resources after handling the public safety requirements and

access rights. For example, an RCMP policy may states that only RCMP approved applications may access the GPS functionalities on the PSG-MD.

Challenges of Current Mobile Devices Permissions

Current mobile operating systems (iOS and Android) use all-or-nothing approach to assigning permissions to applications. The operating system, usually, requires users to review and grant a set of permissions for the application only once, then the application can use that permission whenever it executes thereafter without the user permission. Permissions are granted in different ways based on the OS. For example, Androids require users to approve permissions prior to installation, while IOS requires such approval during the application first usage. However, both approaches suffer from two major limitations:

- Both approaches lack the capabilities to support location-based, situation-based, and context-based policies.
- Both approaches grant applications the permissions to access resources or information even when no access is needed to perform the expected functions. Once an application is permitted access, it can access to information, resource, or services in the absence of user interaction. For example, an application may request access to storage space to store photos, hence, the same application gains access, inadvertently, to other photos.

However, in public safety environment, permissions could be fairly more complex. Each organization shall set its own access permissions to resources, services, and storage access on the PSG-MD. Permissions granted to PSG-MA must be controlled and limited according to the PSG-MA itself, PSG-MD either PSOD or BYOD; User credentials, agency, role, location, context, and applied policies.

Mitigation Strategies for the challenges of PSG-MD Permissions

In PSG-MD, permissions can't be granted according to all-or-nothing approach, however, context specific access control approach should be applied to enforce only permissions with appropriate privileges [88]. To do this, limiting Permissions granted to PSG-MA by providing a rights management and access control approach (e.g. DRM).

In PSG-MAMF, the Access Rights Management (ARM) ensures that security rules, policies, organizational requirements can be handled. Also ARM can manage applications' access to different device resources including sensors such as camera or GPS, location information, or public safety information stored on the PSG-MD. The interpretation layer hooks into the device operating system in order to be able to perform management and security tasks such as managing direct access to device resources and preventing applications from misusing assigned permissions. The interpretation layer in the proposed ARM framework is called "ARM Manager", as described in section 6.4.3. The ARM Manager can support context-driven policies, and runtime enforcement of security policies. Hence, the application can be granted permissions, while public safety organizations can still apply their rules, policies, and security requirements. For example, the public safety organizations may define context-driven policy such as "the application can have access to the camera only during emergency context or specific scenario according to the User location, context, and scenario, and the pictures captured with the camera during emergency responses should only be shared with the public safety organizations and should be stored in specific secured memory storage".

To enable context-aware policies, the ARM Manager should be able to analyze the device/application context at real-time while application is requesting access to device resource (e.g. camera); accordingly, the analyzed context lead to adaptation of permissions. For example, for location-driven policies, the ARM Manager shall be able to access the location information in real-time to recover the device location. The location information is then used to determine the associated security policies, and assign the appropriate permissions based on the security policies associate to the identified location [66]. Note that, the ARM Manager must be trusted and the integrity verification should be done regularly to ensure that the fidelity of ARM Manager.

In addition, the process of vetting applications shall identify the level of risk a particular application presents based on a metric utilizing the severity of the demanded permissions. The vetting process shall distinguish between low risk applications and high risks applications that may have a potential to compromise information. Further, the application monitoring process detects any changes in the application behaviour and permissions usage. The applications behaviour on the PSG-MD can be monitored and managed using mechanisms such as Mobile Application Management (MAM).

Furthermore, secure containers can be used to isolate PSG-MA and protect information from unauthorized access. Containerization can be used along with Mobile Application Management (MAM), along with security policies to balance between the security required for application and its information secured by the containers and the access permissions to such information according to security policies [89] [40].

7.3 Software quality

PSG-MAs used by public safety Users should run in a high quality and optimal performance that meets the public safety requirements in order to be able to serve Users efficiently and effectively. Since PSG-MA requires access to information and service from PSG-II, it is important that the communications and access granting be performed in real time. PSG-MAs should be able to access, decrypt, process the information, and enforce the rules and policies on information as fast as possible.

PSG-MAs shall undergo all testing processes to ensure the quality and performance of the PSG-MA. PSG-MAs shall prove that they are working as intended. In addition, PSG-MAs may need to undergo other kinds of tests as required by different agencies. For example, public safety agency may require that application be tested for response time and resource consumption (e.g. CPU, memory, data transfer, render, database, battery, etc.). Other agencies may require testing the application for compatibility across different kinds of devices or networks.

In addition, PSG-MAs shall be tested rigorously for quality and performance before being uploaded to PSG-AS and distributed to User's devices. Furthermore PSG-MAs shall be monitored frequently while it is running on the PSG-MD. Mobile Application Management (MAM) platform can provide the application monitoring on the mobile device, and provide reporting, tracking, and usage analysis of PSG-MAs to the Management and Administration. Monitoring PSG-MA helps detecting and diagnosing the deep level PSG-MA performance problems such as PSG-MA crashing and excessive power consumption, which are important factors in public safety environments and emergency situations.

7.4 Generic Applications Security

Generic Applications require special considerations as they deal with information sharing in a more relaxed way. It is required to control the access of Generic Applications to information that are irrelevant to the application intended functionalities and information stored in a secure memory locations.

Generic Applications and the use of BYOD may present different types of vulnerabilities. However, most risks pertaining to Generic Applications are well understood and there have been great efforts over the years to identify and develop policies and regulations to manage and control the security risks of Generic Applications. PSG-MAMF would follow the existing policies and regulations developed to mitigate the Generic application vulnerabilities, while the framework is more involved in threats related to security policies. BYOD shall be discussed in more details as part of the open issues.

PSG-MAMF is working with the assumption that all email services are secure and encrypted end-to-end. However, information can be compromised by User's careless handling of email attachments that cannot be detected or protected. In addition, very little knowledge on the data protection level of the attachment or information storage received by email. Public safety organizations should be aware of such issues to accept or require further investigation to deal with security concerns due to using generic email services.

Public safety Users can also use the public browsers to access to the PSG-II that have vulnerabilities that can be exploited exposing the public safety information to the risk of malware browser attacks. Public safety Users can use untrusted web browsers built into PSG-MD to access web applications, which may collect User input and reaches out to services to retrieve information. The use of HTTPs servers and common web based interfaces to access applications provide more flexibility of running over multiple platforms, however, in terms of security they present more vulnerabilities and security risks that need to be considered. Public safety community should be aware of such vulnerabilities and security risks in order to determine the appropriate security policies with regard to the use of such browsers. In addition, public safety information requires end-to-end security during transmission and while it is temporarily stored on the PSG-MD. Providing encrypted end-to-end communication using encrypting technologies (e.g. VPN) between the PSG-MD and the web-application can protect the confidentiality and integrity of communications. In addition, to mitigate the risk of using generic browsers consider directing mobile device traffic to PSG-II through secure web gateways or other intermediate devices to assess URLs before granting access to such URLs. Another mitigation strategy is using a separate browser within a secure execution environment. Users are enforced to use such protected browser for all browser-based access related to the public safety organizations, while using mobile device's built-in browser for other personal usage.

The browser cache can used to store information that can be used to track public safety Users such as location information and credentials. One way to provide a secure web caching is to control cached information based on policy triggers. For example, data cannot be siphoned from the cache, and the cache can be purged as the result of a trigger, such as jailbreak.

Cookies may also be used to remember arbitrary pieces of information about the User. Thus, cookies raise a potential security risk, since the information stored can be compromised. An attacker can impersonate a user to gain unauthorized access to cookies and perform malicious actions. Hence, public safety organizations may require supporting well-known strategies and security controls that aim to mitigate the risks associated with cookies.

7.4.1 Clipboard

The PSG-MD clipboard raises security challenge. Typically, the clipboard stores a block of text in the (RAM) memory until it is replaced by a newer copied item. However, all applications have access to clipboard contents, and thus, clipboard contents are considered a globally under-guarded information. Globally here refers to all applications on the same PSG-MD. A malicious application can gain access to information in the clipboard.

Clipboards can be misused by malicious processes using different means. Information stored on the clipboard can either be manipulated or stolen.

- Manipulation: is the action where a malicious process can interfere with legitimate applications execution by manipulating the information on the clipboard. The malicious process can keeps monitoring the information change on the clipboard. Once the copying operation is performed either by some other applications or by the User, the malicious process can selectively manipulate the clipboard information.
- Stealing: is the action where a malicious process steals and leak clipboard's information and send the stolen information to a hostile entity. The malicious actions of clipboards are shown in Figure 24.

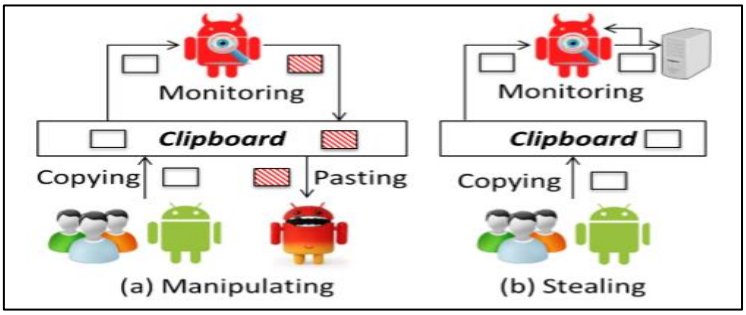

Figure 24 Malicious actions of clipboards

7.4.2 Metadata

Metadata can be found in almost every type of digital files, such as pictures, audio, video files, documents, and text messages. Mobile device embed metadata in digital files they create by default. Metadata may include: The date and time the file was created and last modified, the username and organization of the creator of the file, information of the device and its configuration which creates the file; GPS coordinates where the file was created, etc. The classification of the information itself can be considered metadata.

Metadata is used for multiple purposes including providing application level usage information, security and confidentiality information, and handling requirements information. Metadata can be considered essential for the security control issues. Access control policies depend on the metadata that may include identities and credentials, location, context and scenarios of User attempting to access a protected resource. ITSG-33 provided guideline in terms of information access control policies and enforcement mechanism [56]. Information sharing between the PSG-MA and the PSG-II, as well as access management can be done through DRM system or similar access management mechanisms. The DRM system depends on the metadata tied to information or application in order to apply the security requirements, control device functionalities, and

enforce policies on the PSG-MD. The ARM support system (ARM-SS) is responsible for processing public safety information metadata and creating licenses according to available metadata.

For security reasons, it is important to know the types of metadata associated with public safety information. Trustworthiness of metadata is important issue that worth considerations in terms of metadata generation process, data accuracy (e.g. metadata values are accurate with respect to data), and data integrity (e.g. protecting data and metadata against unauthorized access and modification). Metadata shall have the same level of security, and trust as data. In addition, public safety organizations need to establish a trust method in information, so that when using information captured by the PSG-MD such information and metadata have to be validated to ensure that they can be trusted and did not altered or changed by any malicious means. One way to build trust in information is to use certification and digital signatures.

However, in some cases the information is created by the PSG-MD or the application running on the PSG-MD. Thus, PSG-MD must be able to add metadata to files and information created by any application. For example, public safety User capturing images or videos using PSG-MD's camera, or input text messages during an emergency situation, files will be stored with relevant metadata based on in order to facilitate certification that can be admitted in a court. In addition, information created by the PSG-MD along with its relevant metadata should be stored encrypted and should be stored only in a proper folder hierarchy following the containerization architecture.

Thus, it is important to provide a way to digitally sign the information once it created by the PSG-MD and before uploading it to PSG-II (e.g. add signature to the data, username, MD5, etc.). Information captured by public safety Users are likely to be used as evidence in court. Thus, the technique used by PSG-MD to digitally sign information should provide proper certification that is court admissible. The certification shall require a stamp that prevents any alteration or amendment to information.

7.5 Application Vetting Process

Vetting process is a part of Security Assessment and Authorization (SA&A) process to provide trust in applications developed for the public safety Users. The vetting process is composed of a set of activities that provide software assurance and determine application conformance to the organizational policies and security requirements [52][53][54][23].

Application vetting process shown in Figure 25 usually consists of two main activities: Application testing described in section 7.5.4, and application approval/rejection described in section 7.5.5. However, before implementing the vetting process, public safety organizations need a risk assessment and scoring grid that can be considered as an acceptable metric that can help public safety organizations understand what kind of risks accompany the applications, and the risk impact level. This can help public safety organizations identify and define the public safety acceptance policies and security requirements, what kind of tests are need to be carried, and assist the organizations to take the decision whether to approve or reject the application. In PSG-MAMF, we refer to such process as application evaluation and scoring, as described in section 7.5.3. The score can then be used as an input that assist the SA&A process that can take advantage of priori tested applications. Public safety organizations also need to understand the

limitations of vetting process in order to help them identify any additional security requirements needed to overcome such limitations of the vetting process.

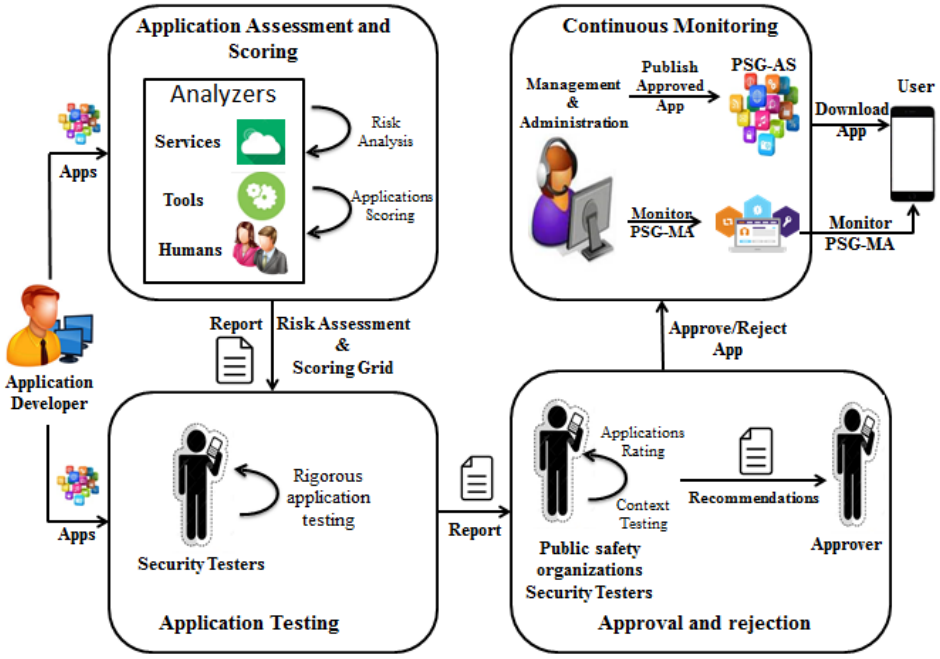

Figure 25 Application Vetting Process

7.5.1 Public Safety Requirements

Public safety requirements are requirements that state the expectations of public safety organizations for application software and application security. The defined public safety requirements shall drive the evaluation process of application, and guide the evaluators to whether approve the application or not. This way, the application is tailored to the public safety mission requirements, security measurements, rules, policies, and risk tolerance. Organizations may depend on current standard metrics to assist and guide them identifying the security requirements, perform a risk analysis, define the potential risks, and determining the level of impact associate with such risks. This way, the assessment could minimize exploiting behaviours results from malicious attacks which were not identified through vetting process.

The assessment and scoring process described in section 7.5.3, aims to evaluate applications against a set of standards and security controls [52] [56] , which may include risk analysis and identifying risks impact level according to the sensitivity of application. The applications passes the evaluation would then assigned a score that can help public safety organizations to understand what kind of risks accompany the applications, the risk impact level, define their security requirements and policies, identify the tests that need to be carried to test applications incompliance with their defined requirements, and assist them taking the decision whether to approve or reject the application.

NIST provided a questionnaire that can be used by organizations as a guidance to identify their security needs in order to define the appropriate security requirements and security controls required by the organization [23]. NIST highlighted a set of general requirements that specify the

software behaviours and the required application characteristics that need to be tested to verify the application integrity including, enabling authorized functionalities, prevent unauthorized functionalities, limiting permissions, and usage of secure information storage [23]. NIST also provided list of specific Android and iOS application vulnerabilities in terms of security. According to NIST SP 800-163, public safety requirements may include two types of requirements: general requirements, and security requirements. General requirements are software characteristics and behaviours that an application should adopt to be trustworthy. During the testing activity, applications should be tested for software vulnerabilities and against their conformance with defined general requirements. If the application has any software vulnerability, the application is considered violating the general requirements; otherwise, the application is satisfying the general requirements and the testing process continues to verify the security requirements. Examples of general requirements may include preventing unauthorized functionality, secure information storage, and limiting permissions [23].

Security requirements are requirements that specify how the application should be used by the organization and the rules and policies that should be enforced through the application to ensure the security of PSG-II. The satisfaction and violation of security requirements is not based on the general requirements and the absence and presence of software vulnerabilities, however, it depends how the rules and policies are satisfied by the process of enforcement. Examples of security requirements may include: set of applications that are allowed to record audio/video are only to be used by classified Users, applications that access the network must not be used in defined situations, etc.

Public safety tailored security requirements and context requirements are additional security controls that may tailored to address specific threats according to each public safety organization requirements. For example, an organization may require additional security controls and policies for BYOD in order to allow deploying of the application on BYOD. Context security requirements may include policy requirements (e.g. information handling), targeted users, targeted hardware (e.g. platform, configuration, or class), and targeted context. The incompliance of application with public safety tailored security requirements and context requirements must be verified by specific administrators and public safety security testers with organization specific testing criteria and application store security before the application approval/rejection activity of the application vetting process.

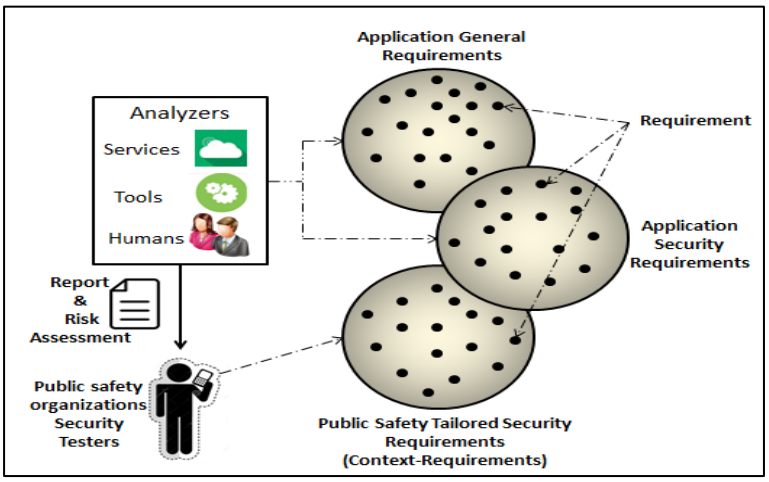

Figure 26 Public Safety Requirements

During the application approval/rejection activity, reports and risk assessments generated for the violation and satisfaction of security controls and security requirements are reviewed to determine whether the application would be approved or rejected.

It is also important to know that some public safety needs and expectations may not be addressed through the vetting process and may need additional security mechanisms to address them as provided in section 7.5.2.

7.5.2 Testing Limitations and Additional Security mechanisms

The Testing process has limitations in terms of its ability to detect deeply hidden vulnerabilities. Some types of application vulnerabilities or weaknesses in applications (e.g. permissions usage) may not be detected during the Testing process. Thus, additional security controls and mechanisms may be required.

Before designing and deploying mobile device security mechanisms, it is recommended that public safety organizations consider developing threat models for the PSG-MD and the resources that are exposed to potential risk as accessed through PSG-MD. Such process would assist organizations identifying the system security limitations and the additional security requirement needed. According to NIST, threat modeling involves identifying the vulnerabilities and threats associated with PSG-MD and resources accessed in specific environment considering operational scenarios. Accordingly, organizations can determine the likelihood of potential attacks and considering their impacts on system components. Such threat modeling assist organizations defining their security requirements by determining the areas and the gaps that require additional security controls, and then define the set of security controls applied to each area to improve its security level. In addition, organizations can then identify the kind of mobile device security mechanisms required to incorporate the security controls required to meet their predefined security requirements.

PSG-MAMF follows a multi-fence security concept that provides sequence of security layers to capture any vulnerability that passed through early fences, as shown in Figure 3. Further, PSG-MAMF follows a compartmentalization approach to isolate information and applications. The compartmentalization provides risk mitigation by limiting the exposure and limits the size of damage in case of unforeseen successful attack. Following the PSG-MAMF; we highlight the use of ROTs and Access Rights Management (ARM) capabilities as discussed in section 6.4. In addition, mobile management security technologies such as MDM, MAM, and MIM solutions may be used to address addition security requirements and provide a real time management and monitoring for the device, applications and information residing the mobile device.

Furthermore, since the testing process may not address all the security assessments required to verify that applications are in compliance with public safety organizational policies and security requirements, the security assessment must include human aspects. The PSG-MAMF includes both the automated assessment and human assessment in the evaluation and scoring, and testing processes. The human aspects assessment carried out by special human analyzers, administrators and security testers from public safety organizations, and the Framework Management and Administration described in section 4.4. This way, the PSG-MAMF increases the robustness of the application testing process by relying on different testing strategies.

7.5.3 Application Evaluation and Scoring

The application evaluation and scoring refers to the process of evaluating the security of applications, and ensure the application conforms to the security requirements developed by the public safety organizations. The evaluation process may follow common criteria that assess applications and determine their performance against a set of security controls [56]. The evaluation may include risk analysis, defining the potential risks of application, and the evaluation should results in a score that specify the sensitivity of application, and level of impact associate with such risks. The applications passes the evaluation would then assigned a protection profile level (score). The scoring grid can be considered as an acceptable metric that can help public safety organizations to understand what kind of risks accompany the applications, the risk impact level and how secure the application is. Hence, process of evaluation and scoring should be trusted by the public safety organizations in order to assist the organization to take the decision whether to approve or reject the application. The score can then be used as an input that assist the SA&A process that can take advantage of priori tested applications. Hence, the application score would have to be developed to assist testing applications during the vetting process.

ITSG 33 and NIST SP 800-53 provided a set of security controls to be used as guidance during the process of evaluation to determine whether the applications satisfy those security controls and the defined security requirements. Security controls are “the safeguards/countermeasures prescribed for organizations to evaluate applications against protection level of the confidentiality, integrity, and availability of information that is processed, stored, and transmitted by those applications” [52]. Hence, organizations can determine assurance level satisfied by the applications once those security controls are applied. Accordingly, each application is assigned a protection profile level (score) that indicate their conformance with such security controls [56] [52]. The score can then be used as an input for the SA&A process.

A formal approach for testing and scoring applications may follow efforts similar to MITRE project designed by Open Web Application Security Project OWASP [28]. In MITRE framework, a detailed quantitative evaluation of the application risk and security level are driven from Architecture, Design and Threat Model, Data privacy and storage approach, Cryptography mechanisms, Authentication and Session Management, Network Communication, environment Interaction, Code Quality and configuration Setting, Specific organizational tailored requirements. OWASP provided a checklist than can help public safety organization express their security requirements and policies [29]. Each security verification requirement set consists of a list of security requirements that have to be verified in order to determine the level of assurance that the application satisfy by determining if the application is incompliance with each requirement [28] [29].

The OWASP security models “Mobile Application Security Verification Standard (MASVS) model” define two basic verification levels (L1 and L2), and a specific tailored requirements (MASVS-R) that is defined according to specific environment or organizational security requirements. MASVS-L1 and MASVS-L2 define generic security requirements, where L1 is recommended for all mobile applications, L2 for applications that handle highly sensitive information (e.g. public safety information), while MASVS-R provides additional security controls that can be applied to enforce specific security policies and mitigate specific threats according to each organization requirements. The application evaluation process starts with the applications uploaded by the Application Developer to be evaluated and assigned a score by the analyzers which may include tool, services, and human aspects. Once the application is received, the application must be stored on a secured database or respiratory to prevent any unauthorized

access to the application leading to potential integrity issues (e.g. application modification), or violations of intellectual property by accessing source code or decompiled code of application. After the analyzer process the application, application will be tested for software vulnerabilities that may results in violation of some of the security controls and security requirements. In case that analyzer is a third party organization or any exterior personnel to the public safety organizations, then the analyzer is responsible for ensuring the security, confidentiality, and integrity of the application files in terms of storing, sharing, and processing, while complying with defined agreements. This way, the process of evaluation and scoring can be trusted by the public safety organizations and considered to assist the organizations to take the decision whether to approve or reject the applications. As per PSG-MAMF, the analyzer is considered a part of the framework which is "Application Store Management". The Application Store Management is part of the PSG-AS-SS which is responsible for testing applications before being uploaded to the PSG-AS to be distributed to Users as shown in Figure 9. The Management and Administration is a member or organization or a group of members from different public safety organizations responsible for managing, monitoring, and securing the PSG-MD. In addition, Management and Administration is responsible for ensuring PSG-MD and PSG-MA are incompliance with public safety's security requirements.

Then the analyzer conducts a report and risk assessment in order to assist the SA&A process. The report generated identifies the detected software vulnerabilities and identified risks. In addition, the risk assessment estimates a score which indicate the probability that the identified software vulnerabilities and risks may be exploited and the impact on other applications, device, information, and PSG-II. The risk assessment indicate the impact of the risk as for example, NIST indicate the risk impact level as low-risk, moderate-risk, and high-risk. While OWASP define different impact levels according to the compliance with the two basic verification levels (L1 and L2), and a specific tailored requirements level (MASVS-R) [23]. The report and risk assessment assist the administrators or security testers in their verification against specific security controls and requirements, and assist approvers in whether to approve or reject application.

7.5.4 Application Testing Process

Public safety mobile applications (PSG-MA) have to go through a rigorous application testing process to assess their compliance with public safety security requirements. In addition, the application store security must include a process for rating applications (e.g. star rating) in order to allow the public safety organizations to understand the security level of the application, and accordingly allow or deny their members to install applications from the application store (PSG-AS).

NIST provided recommendations in terms of mobile application testing which include guidelines related to the application testing activities, testing approaches that assist the SA&A process, and assessment tools and techniques used during application testing process [23]. During the testing process, the application is rigorously tested for software vulnerabilities and security risks to verify that the application satisfies the public safety security requirements. The testing process shall ensure the integrity of the applications under test in terms of applications protection of accessed information, required permissions, and information storage [23].The Open Web Application Security Project (OWASP) proposed a "Mobile Security Project" that aim to help provide organizations with standards in terms of mobile application testing and standardize applications testing mechanisms that can be tailored to meet the security requirements of any organization. The project aims to provide guidelines for both Application Developers and organizations

security testers. According to OWASP, the guidelines provide "a mobile assessment that combines dynamic analysis, static analysis, and forensic analysis to ensure that the majority of the mobile application attack surfaces are covered. The static analysis covers the mobile source code, decompiled or disassembled code testing. The dynamic analysis covers the assessment of application's local inter process, forensic analysis of the local file system, and remote service dependencies" [90].

7.5.5 Application Approval and Rejection

After the application has been through the evaluation and scoring process, and application testing process, a final report that specify the identified software vulnerabilities along with risk assessment that determine the impact level associated with each risk. The evaluation and scoring process, and the application testing process may follow a common criteria as described in section 7.5.3 and 7.5.5, also the methods must be trusted and approved by public safety organizations so that the assessment, scoring, and testing reports can be recognized by the organizations and assist them in the approval and rejection process. The report shall be used by the approvers to assist them to take the decision to whether approve or reject the applications. NIST provided recommendations and guidelines in terms of the application approval and rejection that can assist approvers while taking their decision [23].

The report must be analyzed to ensure that the application meets the public safety general and security requirements. In addition, the application must be assessed with respect to any context security requirements, if any available using specific vetting criteria. Context security requirements are requirements that specify how the application should be used by the Users to ensure that public safety security requirements are enforced.

After assessing, scoring and testing the application's compliance to security controls and public safety security requirements, recommendations for approving or rejecting the application may also be available to the approvers to assist them taking the decision. In addition, the application scoring and rating can help public safety organization to decide to allow or deny their users to install applications, or specify the scope of Users that can have access to such applications. After the decision is made, the process of handling the approval or rejection of the application can be done as following:

- If the application is approved, procedures that identify the scope and limitations of hosting and posting the PSG-MA on the PSG-AS shall be followed. This include the scope of the User that gain access to download the newly approved PSG-MA, the list of Users using the PSG-MA, statistics on the performance and star ratings, and many other attributes relevant to monitoring the PSG-MA. Application downloading from PSG-AS follows common approaches of digital signature to protect against potential tampering during downloading. Modifications to the PSG-MA invalidates prior digital signature [91]. In addition, since the PSG-MAMF supports Access Right Management (ARM) to manage information handling on the device framework, applications would have to be ARM enabled before being uploaded to the PSG-AS. The applications can be enabled to ARM by using the Access Rights Management SDKs [65]. The ARM enabled applications can use the functions provided by the Access Right Management in order to encrypt and decrypt information, acquire licenses and certificates from ARM-SS, and then perform security tasks.

- If the application rejected, procedures for generating a rejection report that contain a rejection list of the identified software or security vulnerabilities and the steps needed to resolve detected vulnerabilities have to be sent to Application Developer to modify the application.

Once the application vetted, assessed, and approved, the PSG-MA shall be made available on the PSG-AS for public safety Users. In addition, any updates or new releases of applications shall go through the same process until it approved.

7.5.6 Continuous Monitoring of Applications and Testing Updates

Ideally, applications and their updates should be vetted before allowing installation of updates even by the user, automatically, or by pushing it to the PSG-MD. Applications updates and new versions must be evaluated, scored, tested and approved before being uploaded to the PSG-AS to identify any new weaknesses and to verify that updates or new versions are usually incompliance with the predefined acceptable security level.

In addition, PSG-MD can be configured automatically in order to enforce updates, and enforce additional security options including: preventing the use of any application store rather than PSG-AS, disabling automatic updates, and enabling mobile management solutions such as MDM, MAM, and MCM that can provide additional security features and applications monitoring.

To provide long-term assurances of PSG-MA fidelity and integrity throughout its life cycle, all PSG-MAs may be monitored to detect potential unforeseen threats or malicious behaviour [23]. PSG-MA may be monitored on the PSG-MD to prevent any unauthorized changes to the compliance baseline, and configuration changes or compromises (e.g. data exfiltration performed by malware).

In PSG-MAMF, Mobile Application Monitoring support system (MAM-SS) and device system (MAM-DS) illustrated in sections 4.10.1 and 4.10.2 is responsible for the applications monitoring process as shown in Figure 27 . MAM-DS has the ability to provision the PSG-MAs running on the PSG-MD by collecting information and report to MAM-SS. Mobile Application Monitoring monitors the PSG-MA downloads, updates, usage, services usage, permissions usage, application behaviours, and performance monitoring. Monitoring allows the Management and Administration to push downloads/install/delete of PSG-MAs remotely, and enforce remote updates. Performance monitoring may include PSG-MA crash log, and battery consumption. Accordingly, MAM-SS shall take the appropriate actions that may include, event management, application updating, application freezing, application deleting, or remote selective information wiping.

Real-time monitoring of mobile applications can support context-aware applications, as well as ensuring integrity of application throughout its life cycle. However, the capabilities of real-time monitoring and assessment of applications raises a trade-off between the performance requirements, user experience, and risk management. There are great efforts over the years to manage real-time monitoring while maintaining good performance. One of the existing monitoring frameworks called “CIMON”, designed to monitor mobile applications by providing middle layer between the operating system and applications, and providing an easy-to-use API, which supports a comprehensive and configurable monitoring services. The framework was designed in such a way that ensure minimum battery consumption, and that the load on the CPU is not too high. In order to evaluate the framework, it was implemented on android mobile operating system while a periodic monitor of the CPU utilization was performed by increasing the

number of applications on the mobile device, while the CPU utilization and energy usage of the Android device was measured. According to the evaluation results, the framework could handle the mobile applications monitoring processes on an android device efficiently, experiencing minimal additional energy consumption and CPU utilization as the number of mobile applications increase. Hence, real-time monitoring of applications can be done today without significantly affecting the performance of the mobile device [92].

Another framework developed to support real-time mobile applications monitoring called "AntMonitor". The framework aims to monitor mobile applications behaviours in real-time, and detect and prevent leakage of information through the mobile device in real-time. The AntMonitor framework is compatible with Android OS versions 4.0+, allowing it to works with most of Android devices available nowadays. The AntMonitor framework was designed in such a way that provide efficient real-time monitoring, maximum user experience by running seamlessly in the background, and humble CPU and battery usage, and high performance. The AntMonitor framework consider user experience by following VPN based approach for data collection, which is compatible with most of mobile devices. The AntMonitor framework consists of three components a client-side Android application runs on android devices, and two server applications. In order to evaluate the framework, a prototype of Ant-Monitor was developed, and deployed on mobile devices to users and activities. Accordingly, 20 GB of mobile data was collected, logged, and analyzed from 151 applications. As a result, the log files arrived the LogServer was observed, demonstrating real-time measurements with high performance and low battery consumption of the mobile device [93].

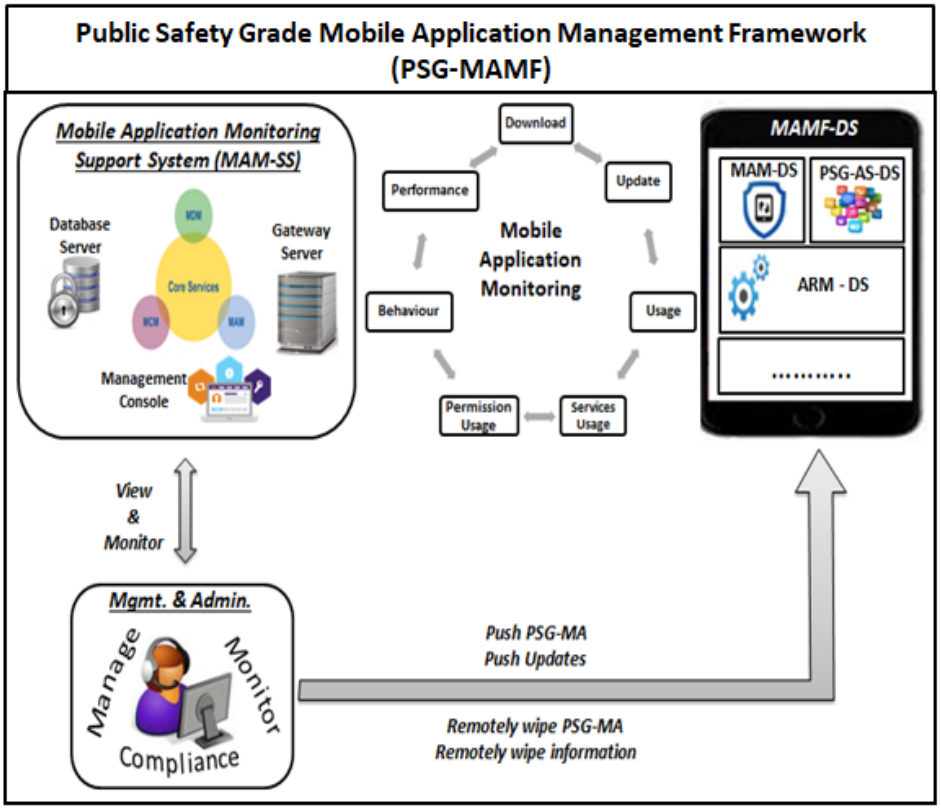

Figure 27 Mobile Application Monitoring System

7.6 Communicate between PSG-MA and PSG-II

Communication between PSG-MA and PSG-II is a challenging issue. PSG-MAMF provides a group of mechanisms to ensure interoperability during communication between PSG-MAs and operating system, and between PSG-MA and PSG-II. In this study, standards are being reviewed to provide interoperable communication over several levels. Access Rights Management (ARM) framework and similar access management mechanisms can provide a solution to supports a privilege management and provide secure access management including storage and information sharing.

7.6.1 Interoperable Application interfaces

Interoperability impacts applications at several levels such as between PSG-MA and user device operating systems, user device-generated data, and network-generated data. There are different models that use a suite of standards to facilitate interoperability. For example, there are several standards for application programming interfaces APIs and data models. Thus, it is important to select the suite of standards that can ensure interoperability throughout the PSG-MAMF.

In public safety environment, sharing information between different governmental stakeholders, public safety organizations, and responders is a challenge. PSG-MAMF shall provide guarantees of fidelity, integrity, availability, and scalability to all information exchanging parties. In order to achieve the PSG-MAMF goals, and to maintain consistency with current and evolving public safety systems, we recommend the use of interoperability standard models such as National Information Exchange Model (NIEM) framework as a platform for information and data exchange [51][11]. By adapting NIEM framework, PSG-MAMF shall provide interoperable information sharing. NIEM interoperability framework builds on existing frameworks and expands information exchange through PSG-MA. Consequently, adapting NIEM framework leads to smoother transition into the mobility paradigm powered by the anticipated PSBN evolution.

Also it is recommended to use interoperable application interface for the communication between PSG-MA and PSG-II that may include an API, to provide a uniform interaction between the PSG-MA and PSG-II. This interoperable interface can be used by the DRM system or any similar access management mechanisms to perform the security tasks needed as shown in Figure 18.

PSG-MAMF builds on top of existing rules, policies, and organizational requirements as described in section 7.5.1. The Information Providers are responsible for defining their own policies, rules, and terms of use to be enforced on users accessing the information. Consequently, PSG-MAMF shall provide guarantees of the imposition of the Information Providers rules and policies over shared information throughout the information lifetime. PSG-MAMF should support a secure information management at the device and application layer, and provide the guarantees to the Information Providers that information use shall comply with the defined rules and policies, and that information shall be kept as secured as it could’ve been on the Information Provider infrastructure. In essence, PSG-MAMF will rely on Access Right Management (ARM) capabilities built into PSG-MA in order to provide a way to deliver information to mobile asset and extend the rules and policies established for information handling into the mobile framework.

To extend information handling policies into the mobile framework; PSG-MD is required to support privilege management, secure access management mechanisms, information storing and sharing mechanisms, as well as PSG-II access capabilities. Access Right Management (ARM) can provide such capabilities.

Using ARM, management files, including rules and policies descriptors, shall be managed on a central system, and encapsulated with the information in such a way that rules and policies can still be handled and enforced on the PSG-MD even if the central system is inaccessible. Consequently, the Management and Administration shall continue to enforce information rules and policies even on the remote PSG-MD.

The communication between the PSG-MA and the PSG-II, and the process of handling rules and policies on the PSG-MD takes place through the ARM system components as shown in Figure 11 The process takes place as following:

(1) Public safety Users interacts with the PSG-MA in order to request information and services from the PSG-II.
(2) PSG-MA interacts with the ARM device system (ARM-DS) running on the PSG-MD in order to communicate with the ARM Support System (ARM-SS) and authenticate the PSG-MA, User, and PSG-MD to the Information Provider prior accessing information and services provided by targeted Information Providers.
(3) The DRM Support System communicates with the identity access control, where PSG-MA, User, and PSG-MD are authenticated to access the targeted Information Providers through a common federated identifier following "Identity Access Control". The identity access control is responsible for managing the authentication process as described in section 9.3.3.2.
(4) Once the User and PSG-MA are authenticated and granted access to the information, the information and the management files shall be forwarded from the PSG-II to the ARM-SS information server and shall be stored temporary in a secure storage space.
(5) The ARM-SS shall process the information coming from the PSG-II, and shall prepare the information to be forwarded distributed to the PSG-MA. The ARM-SS License Server creates licenses according to the management files and access rights provided by the Information Providers with the information. The licenses contain the rules, policies, and organizational requirements that should be applied on the information according to the given access privileges. Then, the ARM-SS packager encapsulates the license to the information and creates packaged information. The DRM-SS is also responsible for encrypting information by a public key, and forwarding encrypted information to the PSG-MD.
(6) The ARM device system (ARM-DS) is responsible for processing the packaged information and interpreting the meta-information. The Security agents within ARM-DS handle all the security functions needed, which include: memory management, secure storage, key management, and executes the basic cryptographic operations.
(7) The ARM Manager within the ARM-DS authenticates the license and information, decrypts information, enforces policies and requirements, solves conflicts between requirements, and provides decrypted information to the intended trusted PSG-MA agent. Trusted PSG-MA agent is responsible for supporting the applications access to the decrypted information.

PSG-MA may also need to access outputs from parts of the PSG-MD components (e.g. sensors events). PSG-MA access to sensors data shall be managed by the PSG-MD based on the User

credentials, role, agency, location, context, and applied policies. Thus, the ARM Manager shall be part of the OS extension to have the necessary privileges to query mobile device state, and access its resources including sensor data. The ARM Manager may apply enforcement mechanisms to control applications' access to device resources including camera and GPS. Essentially, the ARM System prevents PSG-MAs from having direct access to the PSG-MD resources and stored information [66].

In addition, any PSG-MA requires to access public safety information, shall first communicate with ARM Manager, to handle information and policies enforcement. This approach necessarily requires PSG-MAs to be ARM enabled.

7.6.2 Applications Information Sharing

Applications may require the same information from PSG-II; however, within PSG-MAMF sharing information between applications is prohibited. Containerization would ensure that applications are isolated and information is encrypted inside the containers. Access management mechanisms (e.g. DRM system) can be used to provide an access and control management, where each application requires a certification or license through DRM in order to access information. The License contains the rules and policies that shall be applied to the information. DRM provide guarantees that rules and policies set for handling information are extended to the mobile applications.

Using NIEM, ensure that there is no sharing of storage space, while the actual information moves from one application to another. This way, one application can't access data container of other application, and only the intended granular level of data is shared.

8 System Component: Information

Public safety Users may interact with PSG-MD and PSG-MA in order to access PSG-II. A basic tenet of PSG-MAMF is that the information must receive the same level of processing and handling protection by every entity throughout the system and that level of processing and handling protection must match the policy set by the Information Provider. Public safety organizations shall utilize secure mobile computing architecture to manage access to Public Safety Grade Information Infrastructure (PSG-II) and relevant services. Mobile computing architecture shall include Access Rights Management mechanisms to manage access to information and to enforce applied policies on the mobile device framework; secure development and lifecycle management of mobile applications. The PSG-MAMF provides information management principles including application vetting, PSG-AS vetting criteria; strong and enhanced authentication mechanisms; information tagging to enable secure interoperable information sharing; cryptographic mechanisms (e.g. NIST-validated cryptography); and protected encrypted storage on the mobile device.

In general, information management consists of two aspects:

- Data classification and tagging to manage information sharing and safeguarding
- Encrypting information at rest and in motion to provide protection against unauthorized access or disclosure, this can be done by:
    - Encrypting information storage on the mobile device
    - Encrypting information shared across access networks
    - Encryption Key Management as described in section 8.7

Information categorization and tagging require data governance policies and establishment of common standards, which include guidance on interoperable tags and metadata for access control to manage information. In addition, since the loss of mobile devices puts public safety information stored on the mobile device at potential risk, information shall be stored encrypted. Furthermore, access right management techniques are required to protect and prevent unauthorized access to information.

8.1 Information Protection Principles

Confidentiality, integrity, and availability are three essential principles for information security. The security and protection level required to accomplish these principles differ from one environment to other, since each environment employs its own combination of security tools, controls, and mechanisms. In general, all security controls, mechanisms, and safeguards are implemented to provide one or more of these principles. Within the public safety environment, the three principles are essential to provide environment protected from unauthorized actions.

The lack of confidentiality, integrity, or availability may present immediate security breach. According to federal information processing standards publication (FIPS Publication 199) [94], the potential impact of associate risks could range from low, moderate, to high. FIPS [94] define the following types of potential impact on compromised systems:

- Low impact: "loss of confidentiality, integrity, or availability expected to have a limited adverse effect on organizational operations, organizational assets, or individuals" [94].

- Moderate impact: "loss of confidentiality, integrity, or availability expected to have a serious adverse effect on organizational operations, organizational assets, or individuals" [94].
- High impact is "loss of confidentiality, integrity, or availability expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals" [94].

Consequently, two factors qualify to measure the level of a breach impact; first is the level of protection of the data exposed to potential compromise. The PSG-MAMF follows the Canadian system for information protection classification to quantify the potential risk. Second is the spread or breadth of the information potentially exposed by the breach, the spread may use the number of data grains or simple byte count to quantify the level of impact.

8.1.1 Confidentiality

Confidentiality measures the requirements required for each level of protection that needs to be enforced according to information classification, in order to prevent exposure or disclosure of information. This level of confidentiality shall be granted while information at rest (resides on infrastructure and devices), in motion (while being transmitted on network) and while in processing. Lack of confidentiality means unauthorized access or information disclosure. The common mechanisms and measures used to ensure confidentiality are encrypting information as it is stored and transmitted, authentication, and strict access control mechanisms [94] [5].

8.1.2 Integrity

Integrity manages the consistency, accuracy, and trustworthiness of information over its entire life cycle. Integrity can be achieved by ensuring information “non-repudiation and authenticity”. Lack of integrity means unauthorized modification or information destruction. The common mechanisms and measures used to ensure integrity are hashing, and digital signature [94] [5].

8.1.3 Availability

Availability measures the reliability and timely access to information to authorized individuals, while ensure that information continues to be available at a required level of performance. Reliability is required to support information availability. The common mechanisms and measures used to ensure availability are redundancy, high platform resiliency, and clouds. In addition, to ensure availability safeguards against data loss or interruptions in connections are required to ensure available, adequate, and secure communication channels by providing firewalls and proxy servers, and monitoring activities [94] [5].

8.2 Information Security Policies

Information Security Policies include “operational policies, standards, guidelines and metrics intended to establish minimum requirements for management, protection, and secure delivery of information and services” [95]. Guidelines and standards include specifications, technologies, approaches and mechanisms required to ensure information and services security. Procedures include set of sequenced steps required to perform specific security tasks. Procedures are typically used to ensure compliance with predefined requirements, rules, standards, and security

policies [95]. Security policies must express the security requirements in terms of protection against unauthorized disclosure (confidentiality) and unauthorized modification (integrity).

Information security requires security controls that include operational, management, and technical controls set to ensure information assets meets the fundamental information protection principles, described in section 8.1. NIST SP 800-53 rev4 provides information assurance controls that could be applied to the mobile infrastructure components [96]. Information security can be achieved by classification of information, defining security requirements for each classification, establish security policies required for each classification, information labeling and establishing metadata, handling information based on security policies attached to information in metadata, and monitoring compliance. Security policies express how information to be handled by considering level of protection to be given to stored information, who can access information, whether operations on the information or service are to be logged and audited, whether the information transmitted needs to be encrypted, and whether digital signatures are required to authenticate information.

Information security policies may include specific policies to address relevant concerns to an organization. New technologies may require new risk assessment to be accepted or rejected; the risk assessment may result in new policies to be considered. Hence, any technological modifications within organizations should followed by reviews of security policies to ensure that current policies are addressing any potential threats and security concerns resulted from new technologies. Specific policies may need to be issued to include security controls that regulate the use of BYOD. BYOD policies may have specific considerations and requirements for the mobile device, users, and rules of behaviour that must be satisfied to gain access to organizational resources using BYOD [95].

Information security policies are often automated through the use of access controls, as described in section 8.6. However, establishing security policies require defining the security policies that yet to be applied on different information classification according to the information label or metadata. Access controls are then used to implement or enforce those security policies.

NIST SP 800-53 addressed the selection, establishment and implementation of security controls, as well as recommended procedures for ideal implementation of security controls [52]. Such security controls are countermeasures assigned to safeguard information systems as well as information storing, sharing, or processing by applying the information protection principles described in section 8.1. Implementing the selected security controls should result in the desired level of assurance required by the organization to protect information assets.

8.3 Information Classification

Information classification determines the sensitivity of information, and appropriate information usage according to its value. Information classification involves categorizing information into different security levels, as described in section 8.3.1. Information is classified based on information content, and accordingly relative value of information including the impact that information being available for unauthorized persons, impact to health, life or personal safety, effects of data aggregation, and changes to information sensitivity over time. PSG-MAMF follows the Canadian system for information classification and security levels as described in section 8.3.1.

Information sharing requires agreements and guidelines that inform the value of information exchanged between government in consistent manner in order to simplify interoperability and prescribe information handling requirements.

8.3.1 Information Security Levels

Public safety information can be classified into levels based on value and sensitivity of the information and associated risks that may lead to information exposure. According to the Government of Canada designations for information classification and security policies, information is classified into:

- "Information that can be freely disclosed to the public, don't need any type of encryptions, and can be transferred and move freely through networks and between applications" is classified as public information. As an example, some published emergency and weather information;
- "Information that could cause harm to an individual or an agency" is classified as protected information. Protected information itself is classified into protected A, protected B, and protected C based on the impact of information exposure;
- "Information that could cause harm to the country" is classified as classified information. Classified information can be further classified into top secret, secret, and confidential.

Those classifications are not necessarily applied to the information of provincial, municipal or non-government organizations, but those organizations may adopt the Government of Canada classification as a matter of convenience and to simplify information portability. Each organization may use other phrases to mean the same thing.

The United States government has classification that is similar to Canadian classification, namely, "Top Secret, Secret, Confidential, Public trust, and Unclassified" [97]. On the other hand, North Atlantic Treaty Organization (NATO) has four levels of security classification, namely, "Top Secret, Secret, Confidential, Restricted" including protected (A, B, C), and NATO unclassified that includes information that requires NATO permissions in order to be public. The European commission has five classification levels, namely, "top secret, secret, confidential, restricted, and council//commission" [97].

Table 4 represents the parallel equivalent classification or security levels for Canada, U.S., NATO, and Europe.

Interoperability between different classifications must be taken into consideration. While

Table 4 might suggest particular parallel between information residing on a USA, NATO, or Europe, it must be noted actual information migration follows strict notation. When information migrate from one system (for instance, USA) to another system (for instance Canadian), the information metadata and classification are reorganized based on individual agreements governing the domain that resulted in the information migration. Once a copy of the information arrive into the PSG-II along with its proper metadata and information classification, that information will be handled and processed only in compliance to the set of metadata and information classification that followed the information migration.

Table 4 Equivalent classifications (security levels) in various countries

Country Classification	Classified			Restricted		
Canadian System	Top Secret	Secret	Confidential	Protected A	Protected B	Protected C
NATO	Top Secret	Secret	Confidential	Protected A	Protected B	Protected C
United States	Top Secret	Secret	Confidential	"The U.S. previously had a Restricted level, but no longer does. U.S. regulations state that information received from other countries at the Restricted level should be handled as Confidential" [97].		
Europe	Top Secret	Secret	Confidential	Restricted		

8.3.2 Protected Information

Protected information refers to "information that is not classified, not related to the national interest, and cannot be disclosed under the access and privacy legislation". The compromise of protected information may cause harm to private or other non-national interests. Protected information can be classified into protected C, protected B, and protected A, starting from most sensitive information [97].

Table 5 Classification of Protected Information

Protected C	Protected B	Protected A
Protected C is a protection level that used to protect extremely sensitive "information that if compromised, could reasonably be expected to cause extremely grave injury outside the national interest and could result in loss of life" [97] Example: Disclosure of the identity of a Royal Canadian Mounted Police informant, or	Protected B is a protection level used to protect particular sensitive "information that if compromised, could reasonably be expected to cause serious injury outside the national interest and often include information, which if released, would reasonably compromise individual privacy. In addition, the compromise of such information may result in loss of	Protected A is a protection level applied to low sensitive "information that if compromised could reasonably be expected to cause injury or embarrassment outside the national interest. Such information should not be disclosed to the public without authorization" [97]. Examples: home addresses, dates of birth, SIN numbers, banking

disclosure of information that may cause serious financial harm (e.g. bankruptcy).	reputation or competitive advantage." [97] Example: Law enforcement and medical records, personnel evaluations and investigations, financial records, solicitor-client confidence	information, salaries, other personal information

8.3.3 Classified Information:

Classified information refers to information that if compromised, may cause harm to the national interest including social, political, or economic order of Canada. Classified information can be designated Top Secret, Secret or Confidential [97].

Table 6 Classified Information designation

Top Secret	Secret	Confidential
Applied to "information that if compromised would cause grave damage to the national interest. Top Secret documents could be expected to deal with issues of national defence and international treaties or agreements" [97]. It also may include extremely sensitive information related to international affairs, law enforcement investigations and intelligence matters".	Applied to "information that if compromised would endanger national security, cause serious injury to the interests or prestige of the nation, or give substantial advantage to a foreign power. Secret documents may include records of Cabinet discussions, proposed legislation, documents or material pertaining to important government plans, and documents pertaining to national security" [97].	Applied to "information that if compromised, cause injury to the national interest including social, political, or economic order of Canada. Confidential documents include those whose premature disclosure would be detrimental to government plans or intentions, such as negotiations, international affairs, administrative plans; and Private views of officials on public events" [97].

8.4 Layered Information Architecture

Public safety organizations are responsible for developing and maintaining information infrastructure (PSG-II) that enables information and services access to provide field support, enhanced situational awareness, and enable real-time information sharing. The information ownership involves three parties as shown in Figure 28, namely, Information Owner, Information Provider, and Information Custodian.

8.4.1 Information Owner

Information Owners are, typically, the individuals (e.g. Canadian Citizens) or organization originating the information. Information Owner expects public safety organizations collecting the information to honour the agreement in effect for fair use of information. In the context of public safety, information may be shared with other organizations to provide services or to protect the

public. Information Owners trust the public safety organizations to handle and process the information in accordance with the agreement in effect. The rules of information storage, sharing, access, handling, and processing policies are identified as a set of metadata attached to the information. The PSG-MAMF framework defines ways to ensure, guarantee, and monitor compliance of information usage throughout the infrastructure system components.

8.4.2 Information Providers

Information Providers can be defined as the entity that have the responsibility and decision making authority for information throughout its life-cycle, including creating, classifying, restricting, regulating, administering its use or disclosure, managing, and defining rules and policies that accompany information to asses information handling [98].

Information Providers are the organizations, including government agencies, law enforcement agencies, and other organizations; that are responsible for granting access to information and service. . As an example, in an ambulance operator may collect information on an individual citizen injured in an accident. In this instance, the injured citizen is an Information Owner. The EMS collects the Information Owner information and shall provide it to, potentially, an investigating officer in accordance with the information sharing in effect. Hence, the EMS acts as an Information Provider.

Information providers have to guarantee compliance to the agreement in effect with the Information Owner and compliance with the rules and regulations in place. In addition, Information Provider responsibilities may include:

- Determine public safety requirements including information security requirements per classification.
- Ensure security threat and risk assessments are performed to identify and minimize the potential risks to information and its impact on the organization
- Ensure that the necessary security controls are in place, proper access rights are being used
- Ensure information is protected commensurate with their information classification.
- Define requirements for authorization decision, and define User access criteria.
- Approve and regularly review access privileges for Users, devices, and applications.
- Approve or reject access requests according to policies and access privileges
- Implement processes and awareness trainings to ensure Users awareness and fulfilling of security responsibilities.
- Information Providers may delegate responsibility of the information protection and information management to the Information custodian.

8.4.3 Information Custodian

An Information Provider may delegate the operational aspects of record keeping to an Information Custodian. An Information Custodian is responsible for maintaining or administering information on behalf of the Information Owner, but actually operates, serves, and is contracted by the Information Provider. Custodianship typically includes accountability of managing, accessing, handling, disposing and providing information in accordance with the set rules and regulations.

Information Custodian responsibilities may include:

- Maintaining and protecting information by fulfilling the requirements specified in the organization's security policies, standards, and guidelines that pertain to information security and protection.
- Managing and ensuring information security throughout its life-cycle, at rest, in motion, and during processing;
- Maintaining and operating the security infrastructure protecting the information
- Periodically validating the integrity of information
- Ensuring that the identified security controls are implemented
- Identifying and minimizing risks to information by regularly assessing the effectiveness of the security controls, and threats to the information and information systems.

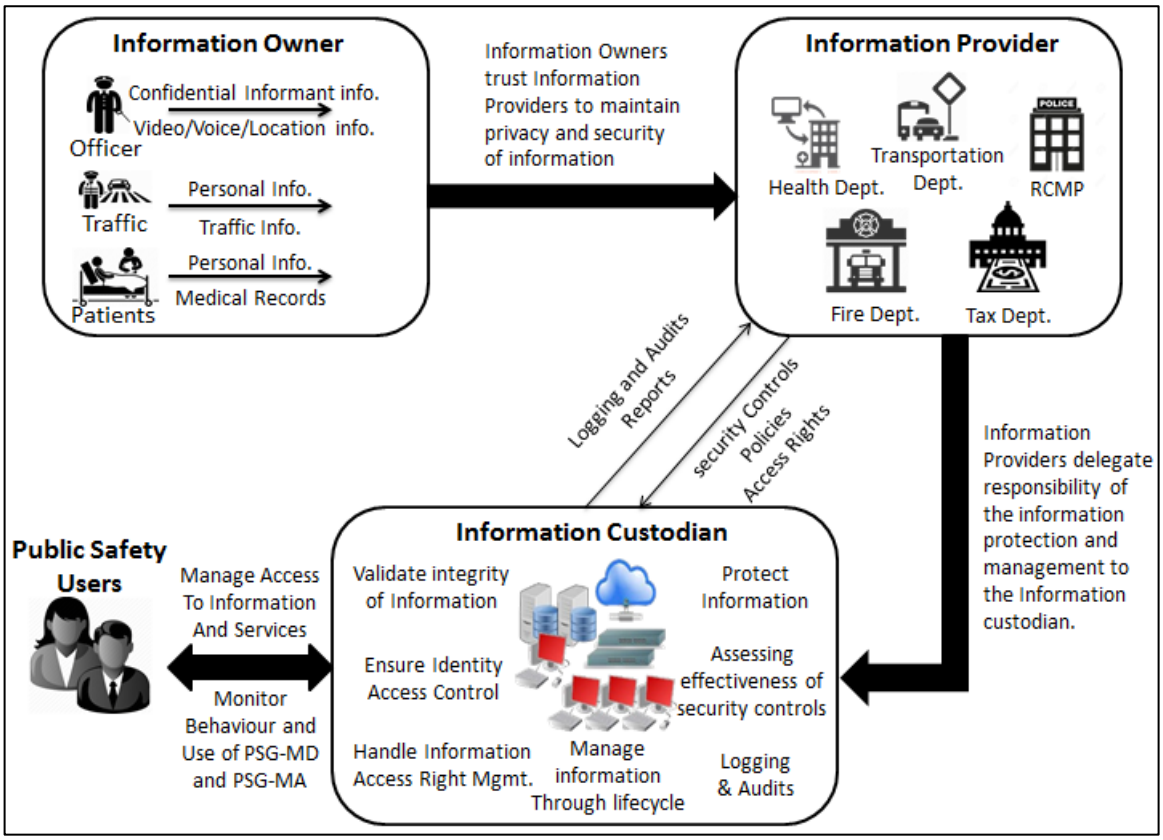

Figure 28 the Information Ownership and Information Security Management

8.5 Interoperability of Data between Different Domains

Public safety organizations including governmental, non-governmental, and international parties may share information between each other. Most countries and even organizations employ their own sort of information classification. For example, SBU (Sensitive but Unclassified) information classification in U.S. system would mapped and classified as "Protected" information

in a Canadian system, and can be subcategorized further into levels A, B, and C. Interoperability between different classifications systems must be taken in considers when information migrate between countries or between different jurisdictional domains, otherwise, a special preapproved cross mapping scheme must be honoured. For example, the United Kingdom uses “Most Secret”, which changed later to match the United States' classification “Top Secret” in order to simplify interoperability.

In order to manage interoperability between different countries, organizations, or groups, establishing and monitoring security policies is required. Security policies state how information is to be handled during storage, processing and transmission to maintain its security. Furthermore, information must classified and assigned labels which indicate, in conjunction with a security policy, how information should be handled. In public safety environment, more granular access control is required. Using metadata as guidance to an access control system is essential to meet the security and interoperability requirements. Metadata will be assigned to each information asset to indicate how the information to be handled with reference to the security policies, and metadata must always travel with information to assist information handling. Metadata has to be usually stored, processed, and transmitted with information to assist information handling process. Metadata can be examined to make security decisions such as access control, storage, processing, and transmitting security requirements [99].

The actual information migration between different classifications follows strict notation. Secure interoperable communication requires additional information security policies, standards and guidelines, and agreements, and the use of parallel metadata [99]. When information migrate from one system (for instance, USA) to another system (for instance Canadian), the information metadata and classification are reorganized based on individual agreements governing the domain that resulted in the information migration. Such agreement often includes guidelines on how to reorganize the information metadata mapping it into proper policies that include information labeling and Time-to-Live that form the parallel metadata that have to accompany the information in the new system. Once a copy of the information arrive into the PSG-II along with its proper metadata and information classification, that information will be handled and processed only in compliance to the set of metadata and information classification that followed the information migration.

8.6 Access Control

Access control is essential to ensure that information is protected from unauthorized access and security threats including internal and external intrusions. Encryption and authentication, information management, access rights, and policies enforcement are the primary security controls required to provide restricted information access [100]. Users require authenticating themselves in order to gain access to information stored in encrypted storage locations. Authentication mechanisms include passwords, PINs, cryptographic tokens, and smart cards. Two-factors authentication mechanisms Thus, combining encryption and authentication form more granular access control, that manage access to stored information based on assurance level [101].

Access Control policies combined with information metadata manages access to information based on user’s identity credentials, role, agency, location, context, and need-to-know and privileges principles [102]. Additionally, access control policies should consider access through unique identity access control system to ensure that all access actions are auditable and court

admissible. NIST SP 800-12 provides guidance in terms of standards, security policies and procedures required to provide granular access control, as described in section 8.2 [95].

Information Provider and Information Custodian shall provide comprehensive multi-layered solution for safeguarding information beyond the use of a simple access control. Access Right Management (ARM) provides better access control by managing access, storing, and sharing of information. ARM ensures that information is protected and temper-resistant throughout the life-cycle of information use. ARM secures information access management at the PSG-MD and PSG-MA that can provide the necessary guarantees to the Information Providers. ARM extends the enforcement of usage rights and security policies to the users, devices, and the applications running on the device by issuing a license or management file that accompanies the information to manage information access, storage, sharing, and time-to-live. The management files that include rules and policies descriptors are managed on a central system, and encapsulated with the information in such a way that rules and policies can still be handled and enforced on the PSG-MD even if the central system is, temporarily, inaccessible.

ARM can also protect and secure information by allowing the use of cryptographic keys. Encrypted information can yet be decrypted based by PSG-MA, role, location, context and scenario, and authorization in the usage right policies resulting from the enforcement of specific Access Right Management files. Consequently, ARM can provide the multi-layer of security and governance technologies, operational practices, and compliance policies that combine to ensure confidentiality, integrity, and privacy of information at a very granular level [102].

In the past few years following the ICAM evolution, there had been discussions on access management that provide comprehensive solutions for the modern complexities of network and applications. As an example, accessing PSBN Radio Access Network (PSBN-RAN) is typically dependent on the PSG-MD and SIM credentials. Simple user credentials may be used to give a user access to a device, but those credentials fall short of providing guarantees of fidelity and authenticity of a user rights to access information. Therefore, and using this really simplified example, access to the PSBN network, access to the PSG-MD, and access to the PSG-II are different things.

In realization of the need to address growing complexity, NIST developed two frameworks following the ICAM. The first framework is the "Federal Identity, Credential, and Access Management (FICAM)"; the second is the "Attribute Based Access Control (ABAC)".

PSG-MD access to the PSBN-RAN is different from user access to resources information. In addition, device hardware, firmware, SIM, and operating system all require authentication following a successful use of a chain of trust system.

In short, the PSBN RAN (Radio Access Network) authentication may be served by common ICAM as a basic approach; however, access to PSG-II requires a more comprehensive framework to authentication and manages access.

8.7 Encryption

Encryption is essential requirement to protect confidentiality and integrity of public safety information. Public safety organizations shall establish encryption policy, cryptography controls, and provide a clear strategic direction on the use of encryption across the organization and its related information. According to OCIO, “cryptographic controls must be based on a security threat and risk assessment, and include consideration in terms of confidentiality requirements,

according to information classification; labeling, metadata and handling requirements; Integrity requirements; Authentication requirements; Legislation, regulations or policies requiring the use of cryptography; and other security measures" [98]. Encrypted storage technologies shall also consider setting encryption policies that may involves choosing the appropriate standards for encryption and integrity protection algorithms, cryptographic algorithms, key lengths, key generation, key storage, and key management.

Information Provider and Information Custodian shall rely on federal information processing standards (FIPS Publication 199), including FIPS-approved algorithms within validated cryptographic modules. NIST SP 800-21 provides guidelines that assist federal government implementing cryptography in their organizations. The guidelines define the process of selecting and implementing cryptographic technologies including authentication and key management [100] [103]. Furthermore, a key management system based on policies, procedures and approved methods shall be used to support and protect the use of cryptographic controls throughout their life-cycle [98].

8.7.1 Management of Cryptographic Keys

Encrypted storage technologies may use cryptographic keys to encrypt and decrypt information. Such keys may be used to decrypt other key(s), which in turn decrypt information. For example, a PIN can be used to retrieve a key from a smart card; which in turn can then be used to decrypt the storage encryption key that is finally used to decrypt information. If a key is lost or damaged, it may not be possible to recover the encrypted data. If a key is compromised, it may result in compromise of information or unauthorized access to encrypted information [101]. Encryption policies may include rules that disallow storing cryptographic keys on the same device that store the encrypted information.

Therefore, public safety organizations need to ensure that all keys used for encrypting information are managed and secured properly. Key management processes, procedures, and technologies are important considerations that need extensive planning by public safety organizations before implementing encryption to ensure healthy key management. Key generation, usage, storage, recovery, and destruction are important considerations that must be taken in consider.

Public safety organizations need to ensure that access to keys is properly restricted. Keys could be secured logically (e.g. encrypted) or physically (e.g. stored in tamper-resistant cryptographic token). Using a combination of authentication mechanisms used to decrypt encryption keys (e.g. passwords and smart cards) may be required to provide the appropriate security for cryptographic keys. Otherwise, unauthorized access to storage encryption keys may take place.

The storage location of local keys is also an important aspect. For some mobile device encryption technologies, there are different means for storing keys, including the smart cards (e.g. USIM, high capacity USIM, and e-SIM), a cryptographic token, or chip circuit which provide possibility to perform computations and to implement cryptographic algorithms (e.g. TPMs [7] – Trusted Platform Modules). In addition, Roots of Trust may be required to support such security

[7] A *TPM chip* is "a tamper-resistant integrated circuit that can be built into end devices and mobile devices to perform cryptographic operations (including key generation) and protect small amounts of sensitive information, such as passwords and cryptographic keys" [132].

functionalities. Other encryption technologies permit keys to be stored on a centralized server and retrieved automatically after the user authenticates successfully. On the other hand, some encryption technologies do not store a key; instead, they retrieve the password entered by the user, perform cryptographic hash function on the password, and then use such hash as the key [104].

NIST SP 800-57 provides recommendations for proper cryptographic key management [105]. NIST SP 800-57 part 1, provides basic key management guidance that includes best practices associated with key management. Such practices can help public safety organizations identify the key management characteristics associated with different algorithms and gain further understanding of security services associated with such algorithms. Using NIST SP 800-57 part 1, public safety organization could identify the following [105]:

- Types of keys, and security services associated in different cryptographic mechanisms.
- Assign protection level required for each information type, security controls and techniques that provide such protection level, and the type of keys required to satisfy such protection.
- Information regarding cryptographic algorithms, cryptographic period length, selecting appropriate keys size, key storage and usage, keys auditing and logging, and other issues relevant to key management.

NIST SP 800-57 part 1 provides a framework that include guidelines to support establishing cryptographic key management within a governmental organizations and planning security policies for federal government organizations in terms of key management. Furthermore, NIST SP 800-57 part 1 provides unique key management implementation guide that aim to address current challenges of existing key management implementations [105].

NIST SP 800-57 part 2 of the "Recommendation for Key Management" provides guidelines that aim to assist the implementation and management of key management system. First, the guidelines identify the common elements associated to effective key management systems; second, identifies the requirements and practices in terms of policies and security controls to provide effective key management; and finally, provide recommendations in terms of key management policies and procedures [106].

Furthermore, NIST SP 800-53 "Recommended Security Controls for Federal Information Systems" identifies the key management controls required for federal systems [96]. NIST SP 800-53 rev4 provides information assurance controls that could be applied to the mobile infrastructure components. In order to provide key management system that supports protection of sensitive federal government information, NIST SP 800-37 "Federal Guidelines for Security Certification and Accreditation of Information Systems" recommends guidelines for security certification and accreditation to the overall system including the system components responsible for performing key management for the federal government organizations [107]. Public safety organizations may follow NIST guidance and recommendations in order to establish appropriate cryptographic operations and proper cryptographic keys management.

8.8 Record Keeping and Court Admissible Records

To ensure integrity of information, audit logs must be used to record user and system activities, and operational events including activities on networks, applications and systems. According to

the information sensitivity, information system criticality, authorized activities, and operational need, the degree of detail to be logged is determined. Audit logs may include, User identity, location, role, scenario and context; Logon method, location, network address; records of successful and unsuccessful system logon attempts; records of successful and unsuccessful information access and other resource access attempts; Dates, times and details of key events; Changes to configuration; Use of privileges; Use of applications and mobile device resources (e.g. camera, GPS, etc.); Network addresses, protocols, and transferred network data traffic flow; Alarms raised by the access control system [98].

Logs and records must be reviewed and analyzed periodically and independently. Since logs and records may contain confidential information that likely to be used as evidence admitted in a court, access to logs and records must be restricted with need-to-know privileged access and be protected accordingly. Logs and records shall be protected against tampering and unauthorized access. Hence, logs and records should be encrypted and stored in a proper protected storage. Information Custodians must implement the proper controls in order to prevent modification, amendment, access, or disposal of logs without proper privilege to preserve integrity of logs and records.

In order to protect log files from tampering or modification, Information Custodians must apply appropriate controls which may include: multi-factor authentication, digitally signing information for detecting alteration or corruption, automatic archiving of logs within protected storage, backup of logs, and access to logs should also be logged [98]. Digitally signed information can keep the integrity of logged information and provide proper certification that is court admissible. Redundant copy of information can be stored in undisclosed, untraceable location that can only by unlocked by a combination of keys generated by multiple authorities.

9 Public Safety User

Public Safety Users shall use PSG-MD and PSG-MA to access PSG-II to perform day-to-day operations. Public safety organizations and Information Providers employ known identity management mechanisms to control and manage access to services and information on the PSG-II. A robust approach to identity management and control access ensures only authorized can access PSG-II. Therefore, public safety organizations shall be able to verify the identity of the PSG-MD and PSG-MD user if it is being used by multiple users. Accurate secured logs keep track of information access and may be used for system audits, court records, and event review or investigations.

PSG-MAMF builds on top of existing rules and policies defined by Information Providers in order to manage access to information and services managed by different Information Providers. Thus, PSG-MD, user identity, and other qualifying attributes described in section 9.1 needs to be verified before granting access to PSG-II. Further, IP addresses may be used to identify devices as well as credentials to control access to information and services. Authentication mechanisms are required to authenticate PSG-MD and user before authorized to access the PSG-II [25].The authentication mechanisms shall provide the management layers required, without distracting the public safety highly dynamic operational environment. Authentication mechanisms in all its forms, passwords or bio-metrics, shall not be distracting and shall complement the necessities of responder's operational environment. Situational authentication may provide well-defined design to control data sharing and "who can see what". Situational authentication refers to the change in information accessibility based on the use-case the responders are handling [25].

PSG-MAMF supports more comprehensive authentication processes that consider authenticating each single entity within the PSG-MAMF before granting access to network and PSG-II. Such process requires different types of authentications, including local and remote authentications. Within the PSG-MAMF, the user needs to authenticate himself to the PSG-MD before granted access to PSG-MD and its resources. User access to PSG-MD follows an authentication form defined by the user's organization. Then, both PSG-MD and user need to be authenticated to the network, being commercial or private, LTE or other forms of network access. In order to access PSBN-RAN, a User must be registered in his organization as well as the federal registry. Once access to the network is authorized, PSG-MD and User shall be authenticated to the PSG-II. In order to access PSG-II, 6 qualifying attributes described in section 9.1 need to be challenged to fit and match the policy set by the public safety organization. Accordingly, PSG-MAMF requires 3 types of authentication: User-Device authentication, User-Device-Network authentication, and User-Device-Infrastructure authentication. Different types of authentications used in PSG-MAMF are described in details in section 9.3.

However, PSG-MAMF requires a comprehensive identity and access management approach to validate any access request to network and PSG-II. Access shall be granted only to entities providing appropriate identity, credentials, and other qualifying attributes as per subsection 9.1. Accordingly, PSG-MAMF shall support a reliable, secure, and interoperable authentication and identity management framework to identify User-Device access to network and assure appropriate information access, while all the authentication process takes place on the system side. The authentication and identity management framework is described in details in section 9.3.2.2 and 9.3.2.3.

9.1 Policy Determination and situational authentication

Situational awareness may call for a situational authentication. Responders may be granted access to information that may not be permitted in other situations. A situational authentication follows the set of organizational policies defined by the Information providers. The anticipated situational access to information may require limited time-to-live on PSG-MD. A situational access to information can be handled through the PSG-MAMF by policy determination of defined relevant organizational policies. Situational authentication provides responders with the needed security without compromising the User's access to needed information following a "need-to-know" approach. Factors influencing the decision to grant access to information are referred to hereafter as "6 qualifying attributes", which are a group of attributes uniquely describing entity (e.g. device, application, or user) within a given context. The 6 qualifying attributes are included hereafter:

User Role: User role is the actual functionality of a user during particular situation. User role is affected by the active organization they belong to and his duties in each situation.

User Organization: User Organization is the public safety organization or agency the User belongs to. Each User belongs to at least one organization or agency. User organization defines the set of policies and User access rights to the PSG-II. Further, the User's role may be different from one organization/agency to another. Thus, User organization, User role within the organization, and the current situational scenario have to all match relevant policy requirements in order to assign the appropriate access rights and privileges to the User.

The term "public safety organizations" includes a wide range and different levels of governmental, community groups and private agencies that are performing day-to-day operations and are responding to incidents and emergency situations. The "first responders" are law enforcement (e.g. police), Fire and Protection Services, Emergency Medical Services, rescue groups, and other responders according to the operational scenario. The "Emergency responders" include transit, search-and-rescue, hospitals, the Red Cross, and many others. Stakeholders may include public safety partner agencies, public safety review bodies, small organizations or community groups that serve their communities in case of emergency, and individual volunteers.

User Location: According to the User location, User will be granted appropriate access rights. For example, using criteria such as "postal code", a User in Canada may have access to different information and services compared to Users in United States. In addition, access to network would be determined according to the User location.

Scenarios & Context: Represent the current event or operational situation on the ground. Responders need dynamic configuration to insure privileged services, and particular situational awareness that may lead to prioritized access. Prioritized access can be controlled by User emergency situation, and immediate Peril.

According to the User's scenario and context, the User may be assigned a temporary permission set. Temporary permission sets are useful for providing a specific set of functionality to a User in addition to the typical access rights. For example, we may want to grant only a few of police officers the ability to manage specific information in emergency situation. In this case, rather than changing the User role, it is easier to create a temporary permission set with the new access privileges based on the situation and context, and assign such privileges to those Users temporarily. Once the Users finish their assigned mission, the temporary permission set will be revoked automatically. Using mechanisms such as MDM, MAM, and MCM may provide the

Management and Administration with the ability to assign temporary permission sets with additional access privileges to User as illustrated in Annex A.

Temporary permission sets can define what applications, information, and services the Users may have access to. Also it may be required to assign multiple temporary permission sets to a single User, or the same temporary permission set to different Users [108]. The PSG-MAMF would accommodate the temporal permissions by defining the relevant policy in the Information Provider framework, and then the Access Rights Management (ARM) would enforce them.

User Device: Represent the class of the PSG-MD that can be either Public Safety Owned Device (PSOD), or Bring Your Own Device (BYOD). Also the mobile devices platform may affect the policies being enforced. Also the type and model of the device and its capability can limit access to particular information if the device model is known to have lower security capabilities.

Date/Time: the User credentials may change when the User is on vacation or either s/he is in work assignment. During a vacation, User credentials are temporally invalid, or paused. Thus, the date and time should be taken into consider when determining the applied policies.

The six qualifying attributes described above can be considered as the qualifying attributes that have to be challenged to influence whether User requesting to access information or services shall be granted access to PSG-II. The qualifying attributes can be divided into static qualifying attributes, and dynamic qualifying attributes.

Static qualifying attributes are pre-configured by public safety organizations, which are then used to derive the access privileges. Those attributes can be used to manage access and derive the default priorities when information and services are requested from the PSG-II. User role, organization, and device can be considered as static qualifying attributes. Dynamic qualifying attributes are impossible to be statically pre-configured, since public safety operations are situational, and there are no set values to address different operational needs. Scenario/context, Location, Date/Time, and temporary roles assigned according to the situation are considered dynamic qualifying attributes. Dynamic qualifying attributes are ultimately influence access privileges, priorities, and QoS. It is also important to know that dynamic qualifying attributes manage access to resources during heavy NPSBN congestion according to their dynamic priority [22].

Static and dynamic qualifying attributes should be mapped together to support the mission with real-time incident services and information, and manage access rights, dynamic priorities, and QoS as shown in Figure 29. Further, real-time access to appropriate information and services facilitates situational awareness and increase coordination of response. Thus, PSG-II shall be kept secured, while information and services shall be shared with Users as needed. Furthermore, we recommend the use of National Information Exchange Model (NIEM) standards for information and data exchange between different organizations, and Users in order to provide multi-agency collaboration, and providing Users with information to support effective decision making in real-time [109].

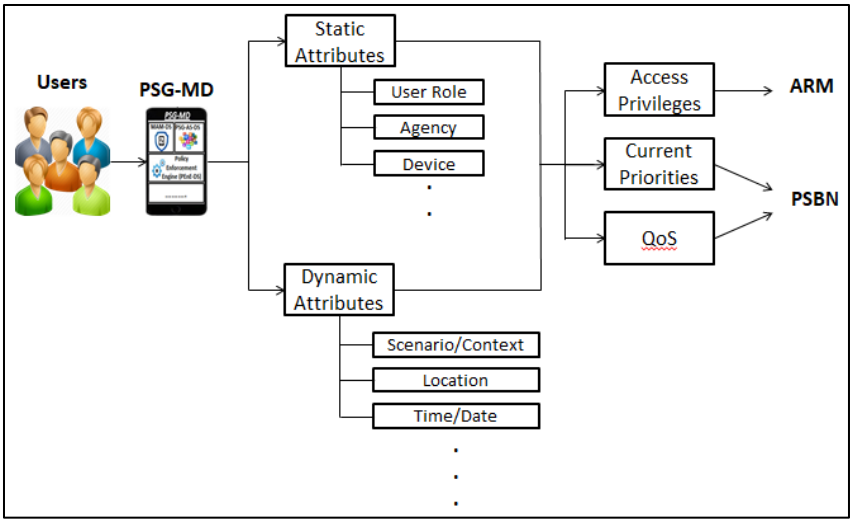

Figure 29 Mapping qualifying attributes to manage access rights, priorities, and QoS

9.2 Identity, Credential, and Access Management (ICAM)

PSG-MAMF relies on security disciplines such as: Access Management, Credential Management, and Identity Management (ICAM), as well as key exchange mechanisms to guarantee policy enforcement and secure information handling at all times. Such security disciplines have to be integrated together to provide a complementary architecture that aims to manage access to governmental agency's resources. "Federal identity, credential, and access management (FICAM) Roadmap and Implementation Plan v2.0" [13] provides a high level overview of the complementary architecture by cutting across numerous systems within the government agencies as shown in Figure 30, which are typically directed and managed separately [13].

FICAM also simplifies the mobility of responders along geographic areas out of their normal jurisdictional boundaries. As an example, a Saskatchewan EMS may respond to emergency call in Manitoba due to its relative proximity to the incident. The FICAM manages the mobility of the User and PSG-MD into the area of the incident without any need for Saskatchewan-Manitoba solution. The use of FICAM lends itself to be managed through a national Canadian technical entity that manage FICAM alongside other aspects of PSBN management and control layer.

The architecture involves 3 key services, including identity management, credential management, and access management. Typically, in order to provide granular access control to access information and services, digital identity need to be established associated with a credential to enable different authentication levels. Identity Lifecycle management of the digital identity and credential lifecycle management of credentials ensure integrity of identity and credential, and provide trustworthiness in identity when being used to make granular access control decisions.

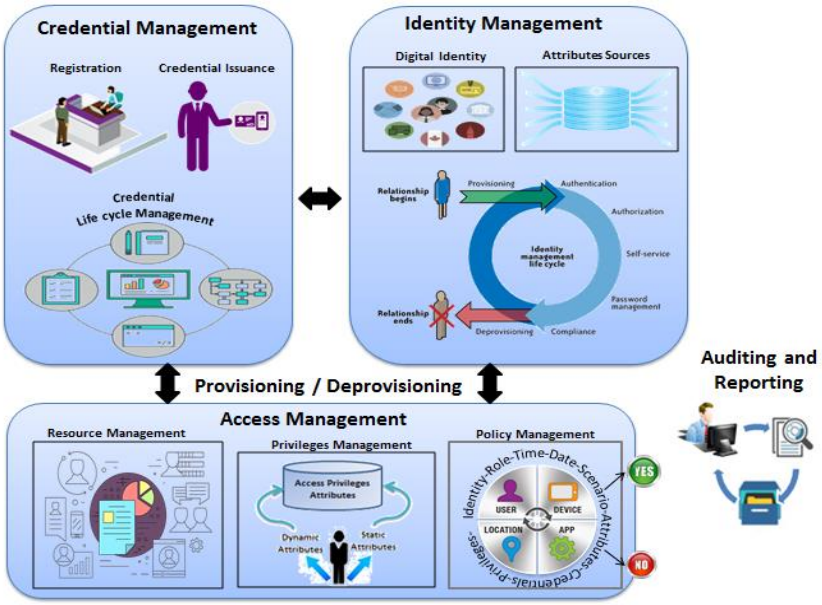

Figure 30 Federal identity, credential, and access management (FICAM) complementary architecture

However, such architecture requires not only technologies or solutions to be deployed, but also trust models across agencies, uniform authentications assurance levels, defining security policies that would manage the authorization and access management decisions. Since many public safety organizations cannot manage and maintain its own ICAM, a Canadian National Technical Entity may manage a FICAM and provide smaller agencies with a front end to add/remove users. Figure 31 illustrates the common service components for "Identity, Credential, and Access Management Complementary Architecture [13]. "Federal identity, credential, and access management (FICAM) Roadmap and Implementation Plan v2.0" provides a brief description for each service component of the architecture [13].

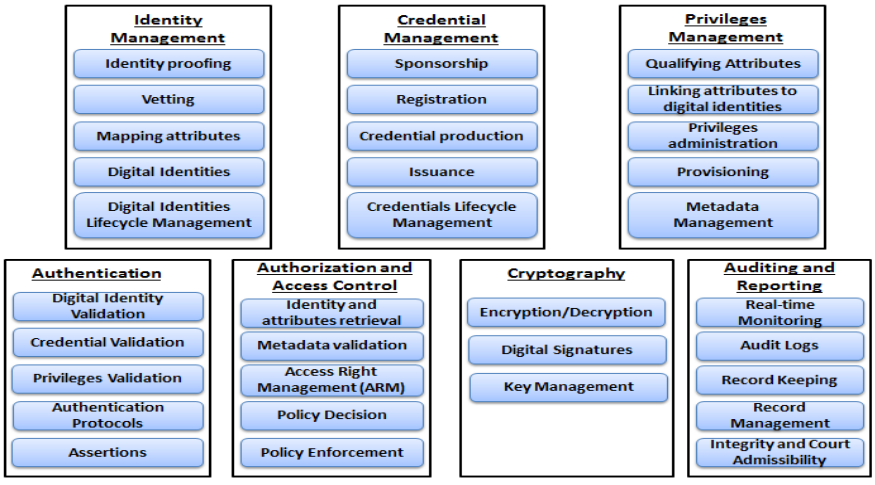

Figure 31 the common service components for identity, credential, and access management complementary architecture

9.2.1 Identity Management

In In order to manage access to PSG-II, the User requires appropriate **role**, **clearance** and **need to know** requirements, in addition to the provided 6 qualifying attributes as listed in subsection 9.1. User Clearance is a status or permission set granted to Users allowing them access to specific information and services. However, User role and clearance is normally not sufficient to gain access; the organization must also determine that the user needs to know this specific information. The need to know could be implemented as part of the organizational policies, and can also be assigned to User as a temporary permission set for specific task. Need to know is the reason behind the user needs to grant access to this specific information. The "need-to-know" is defined by the Information Providers as part of the organizational policies, and must be relative to the prospective User's mission.

According to NISTIR 8014, identity management can be defined as “the process of managing the identification, authentication, and authorization associated with an access request”. The identity management process typically considers identity proofing, selecting tokens, authentication and authorization process [80].

PSG-MAMF control user access to PSG-II based on the User identity, credentials, as well as the 6 relevant qualifying attributes of an entity as per subsection 9.1. User identity, credentials, and 6 qualifying attributes need to be challenged during the authentication process leading to granting access. FICAM recommends the use of digital identities as a single digital representation of entities that can be leveraged across different governmental agencies for multiple reasons, including access control and interoperability requirements. The process of establishing a digital identity is described in details in FICAM Roadmap and Implementation Plan v2.0 and NIST SP 800-63-3 [13] [110]. Digital identity include a set of attributes mapped together to uniquely identify and define an entity within a system. The qualifying attributes in various agencies have to be linked together forming digital identity. Such digital identities have to be provisioned into Access Management to support access decisions, and de-provisioned when access is no longer required.

Digital identities are beneficial in different situations. Typically, public safety scenarios, operational, and security requirements, require both the User and PSG-MD to be validated. For example, in BYOD scenarios, users typically use their devices to access information and services on PSG-II to support their mission. Hence, PSG-MD should be provisioned with a strong device identity, as well as the user identity. Such identities shall be unique and shared among different public safety organizations to simplify interoperability and access control. Thus, digital identities could support the following situations. Users and devices need to go through authentication and authorization processes to prove their access privileges (Access-Request), and then granted access to information and services according to their access privileges and access rights (Access-Grant). Such authentication scheme would ensure only authorized entities can access network and PSG-II with granular access control based on assurance level.

9.2.2 Credential Management

According to NIST SP 800-63 [14], a credential is an object or information issued to individual and padded to his/her identity (and additional attributes) to enable future authentication of identity and privileges determination associated to an Access-Request to provide a secure access to information and services. Typically, identity credentials are used as part of the authentication process where an Access-Request is submitted that include known credentials such as security

clearance, username, password, keys, and smart cards. Authentication may also use tokens, biometrics, or a set of challenging questions that the User must answer [14]. Identity credential can be categorized as "something you know" (e.g. passwords, PINs), "something you have" (cryptographic based tokens such as smart cards, etc.), or "something you are" (biometrics such as fingerprint, retina, etc.).

"Federal Information Processing Standards Publication 201 (FIPS 201)" [111], NIST SP 800-73 [112], and "Federal PKI Common Policy" documents provide PIV standards for federal specific credential implementations [113]. The process of establishing credentials is described in details in FICAM Roadmap and Implementation Plan v2.0 [13]. In addition, FICAM v2.0 provides an overview of different types of credentials, and the architectural analysis and procedural steps associated with each credential types, especially credentials used within the Federal Government. Such analysis is being carried through analyzing different case studies within government agencies and highlighting some learning lessons from each case study [13].

PSG-MAMF supports identity credentials following the authentication form and applied policies of the agency that the user belongs to. The requirements of credentials for each organization are different from another, based on the level of credential strength. Typically, the most common credentials used in Federal Governments are smart cards, private/public cryptographic keys, and digital certificates. The strength of a credential depends basically on [9]:

- The credential life cycle management strength, including credential issuance, management and authentication processes.
- The security measurements adopted by the organization in charge of credential issuance, management and authentication.
- The integrity and reliability of security controls, technologies, and standards associated with the credential itself.

The Office of the Chief Information Officer (OCIO) divided the credential strength into 4 levels [9]:

- Level 1 – Low: This level includes "single-factor electronic credentials" with low security requirements (e.g. simple a user ID or password). This level also includes electronic credentials that do not meet the requirements of level 2 for any reason (e.g. a password that does not meet the password strength requirements).
- Level 2 – Medium: This level includes "single-factor electronic credential" with security requirements stronger than level 1 (e.g. user ID and strong password). This level also includes electronic credentials that do not meet the requirements of level 3 for any reason (e.g. multi-factor credential issued for a device that doesn't meet the cryptographic module validation requirements, resulting in a credential that does not meet the high level strength requirements).
- Level 3 – High: This level includes "multi-factor electronic credential" with any sort of software-based, hardware-based, and cryptographic tokens (e.g. digital certificate combined with password).
- Level 4 - Very High: This level include a "multi-factor credential", however, it must use a hardware-based cryptographic tokens (e.g. smart card that uses PKI). It may also include biometrics such as finger prints and digital imaging.

Credential management includes the process of supporting the credential life cycle. The difference between the credential lifecycle management vs. identity life cycle management is that credentials may expire. In general, the qualifying attributes forming the digital identities may change over time, leading in changes in the digital identity; however, the digital identity itself doesn't terminate. On the other hand, credentials are typically valid for only specific period of time as specified during issuance. For instance, the issuance of digital to individuals may expire based on policies and attribute associated to such individual and new certificates may be issued, while the identity remains unchanged. Hence, credentials are effective tool for authentication that may set different levels of assurances based on the credential strength.

The credential life cycle management, technology requirements, and the security and technical features for each credential level should match the strength of such level. For example, credential strength level 4 requires very powerful credential issuance and management processes, and more strict security controls for credential services. The Office of the Chief Information Officer (OCIO) "electronic credential and authentication standard" report provides a standards sets that recommend the lifecycle management of electronic credentials, technology requirements, and security features that are acceptable for each credential strength level described above [9].

PSG-MAMF recommends the use of credential strength level 4 (very high), to ensure a strong credential is challenged in the authentication process, resulting in a strong authentication process prior to granting access to an entity accessing information and services within the PSG-II. PSG-MAMF requirements for credential management include requirements for the following [9]:

- Digital Identity requirements: include requirements for issuing digital identities with a unique single digital representation across different governmental agencies for the purpose of access control and interoperability. For example, a digital identity issued to a user by his organization should be the same digital identity representing the user in all other organizations.
- Credential creation, renewal, replacement, deactivation, and revocation requirements.
- Credential state requirements: include requirements for maintaining the status of the credential, and requirements for the process of checking the status and validity of credentials during the authentication event
- Cryptographic key requirements: this includes requirements for key generation algorithms, key length, and key management (e.g. key usage, storage, recovery, and destruction)
- Credential records management requirements: include requirements for producing auditable records of all events including credential issuing, changing, and revocation. It also includes requirements for recording evidence of keys and certifications generation. In addition, it may include requirements for management and securing the audit records itself.

Credential policies requirements: include policies for issuing and management of credentials. This include security policies to ensure integrity of credentials, since it affect the level of trust given to a credential. The credential management security requirements should consider protecting the credential throughout its life cycle.

9.2.3 Access Management

Access Management is the process of managing and controlling the methods by which entities (e.g. User, Device, applications, etc.) are granted or denied access (Access-Grant or Access-Deny) to resources (e.g. information or services). The main goal of the access management is to control entities attempting to access resources, in order to ensure authorized access according to trust given to entities, and proper verification and authentication take place prior to authorization decisions.

PSG-MAMF uses identity and access management to validate and challenge the requests attempting to access PSG-II. Public safety Users requesting access to PSG-II will not granted access to requested resources, unless proper verification and authentication take place. In other words, the Information Providers shall grant access only to entities providing appropriate identity, credentials, and other qualifying attributes as per subsection 9.1. After the authentication process, a decision can be made as to whether grant/deny access to the resources.

Information Providers need guarantee a level of assurance in the entities attempting to access information and services. The access management provides such assurance by aiming to meet the following objectives [13]:

(1) Ensure the validation of all entities (including identities and credentials) attempting to access information/services (Authentication)
(2) Ensure only authorized entities have access to information/services (Confidentiality)
(3) Protecting information against unauthorized creation, modification, or deletion (Integrity)
(4) Ensure that required information is available for authorized entities at right time (Availability, Reliability, and Maintainability)
(5) Performing auditing and reporting to ensure the responsibility and liability of entities by logging each single activity taking place (e.g. access to resources and actions such as creating, modification, and deletion) (Nonrepudiation)

In addition, access management should provide additional functionalities over the traditional access control paradigms. The access management should be able to verify that all entities attempting to access information/services possess appropriate “need to know”. In addition, enhanced authentication schemes (e.g. Attribute Based Access Control ABAC) should take place prior to access decisions. Thus, in addition to the authentication and authorization, policies and access rights are required to manage the access control process.

According to FICAM Roadmap and Implementation Plan v2.0 [13], a successful access management should support the following three areas:

- Resource Management: is the process of establishing and maintaining information, including information classification, rules, credential requirements for access, sharing, and storing of information that require an access control.
- Privilege Management: is the process of establishing and maintaining the privilege and qualifying attributes associated to each individual. Such attributes clarify the current features of an entity that can be used as an input for authentication and access control processes to determine the appropriate access decisions based on assurance level, as per subsection 9.1. Individual identity, privileges, and qualifying attributes are to be linked to

form digital identities, which in turn is used to determine access decisions, and access rights.

- Policy Management: is the process of establishing and maintaining policies which usually based on privileges and qualifying attributes (e.g. role, agency, location, etc.). Such policies are included in the metadata that always accompany the information to support the information handling process.

PSG-MAMF supports an Access Right Management (ARM) framework that include an automated mechanisms for verifying identities, credentials, and qualifying attributes resulting in informed access decisions and more granular access control. ARM ensures that access controls, access decisions, and policies enforcement are compliant with public safety security requirements and risk-based analyses. PSG-II relies on the Access right Management (ARM) to guarantee User's compliance with the applicable policies in the given context.

9.3 Authentication

Authentication usually includes verification of user identity by presenting of credentials that prove user possession of such identity. PSG-MAMF defines the authentication as "the process of establishing confidence in a digital identity claiming PSG-II or network with an Access-Request and providing a credentials as an authenticator (e.g., password, PIN, smartcard, biometric), and other predefined qualifying attributes as a proof of access privilege". Authentication takes place both locally and remotely. NIST SP 800-63-2 document presents guidelines relevant to remote authentication process which include Users registration, identity proofing, authentication using tokens (e.g. cryptographic keys), access management, authentication protocols, and assertions to ensure integrity and communicate the results of remote authentication [80].

The strength of authentication process is a complex task. Evidently, some authentication processes provide greater assurance than others based on how securely can the authentication protocol communicate with user, how users can securely present credentials. Thus, the authentication process strength depend mainly the credential strength level, as discussed in section 9.2.2, and the process and protocols by which the authentication conducted.

The Office of the Chief Information Officer (OCIO) divided the authentication strength into 4 levels, by mapping it with the credential strength levels described in section 9.2.2 [9]. PSG-MAMF recommends the use of authentication strength level 4 (very high) to ensure a strong authentication process takes place prior to granting access to PSG-II. Authentication strength level 4 includes "authentication of multi-factor credential than uses a hardware-based cryptographic token (e.g. a smart card and PIN), through an encrypted communication sessions, may also include high-quality biometrics, and usage of very strong processes and protocols for verifying very high level strength credentials, and more rigorous security requirements for authentication services " [9].

Authentication mechanisms and technologies shall be verified against their applicability and reliability to public safety environments, including operational contexts, communication networks (especially, PSBN based on LTE technology), available security controls, and applicable policies that can regulate the use of such technologies. In the public safety environment, the delay and complexity of the authentication process may lead to dangerous situations. On the other hand, in terms of security, the public safety requires more comprehensive authentication processes that

consider authenticating each single entity within the PSG-MAMF before granting access to network and PSG-II. Defining, maintaining, and implementing of security controls and policies for different scenarios are the responsibility of public safety organizations and agencies.

9.3.1 Authentication Factors

PSG-MAMF supports authentication process that verifies different authentication factors during the authentication process as shown in Figure 33. The authentication forms supported by PSG-MAMF are summarized as following:

- Digital Identities: Digital identity is the user unique identity among government organizations, and a group of attributes associated to such user, mapped together to form unique entity identifier within a system. The identity and qualifying attributes of an entity are to be linked together forming such unique digital identity that is common between all agencies to support interoperability and access control decisions, as described in section 9.2.1.
- Credentials: credential is an object or information issued to enable future authentication of identity or privileges. Credential can be categorized as “something you know” (e.g. passwords, PINs), “something you have” (cryptographic based tokens such as smart cards, etc.), or “something you” are (biometrics such as fingerprint, retina, etc.), as described in section 9.2.2.
- Qualifying Attributes: Include contextual information, including location of the entity authenticating, time/date, or the scenario the user involved in. It also includes user’s role, agency, and device. The 6 qualifying attributes consider by the PSG-MAMF are described in details in section 9.1. Such attributes are used for policy determination and attributed access control decisions.
- Sensors data and mobile device integrity measurements could be integrated to provide stronger authentication scheme with more granular access control based on assurance condition.
- Other network security controls, risk-based approaches, and behavioural patterns may further restrict authentication to increase the confidence in the authentication process [9]

9.3.2 Types of Authentication

PSG-MAMF supports authentication process that provide different types of authentications in order to authenticate each single entity within the PSG-MAMF before granting access to network and PSG-II, as shown in Figure 32. The types of authentications supporting by PSG-MAMF are namely, User-Device authentication, SIM-Network Authentication, User-Device-Network authentication, and User-Device-Infrastructure authentication.

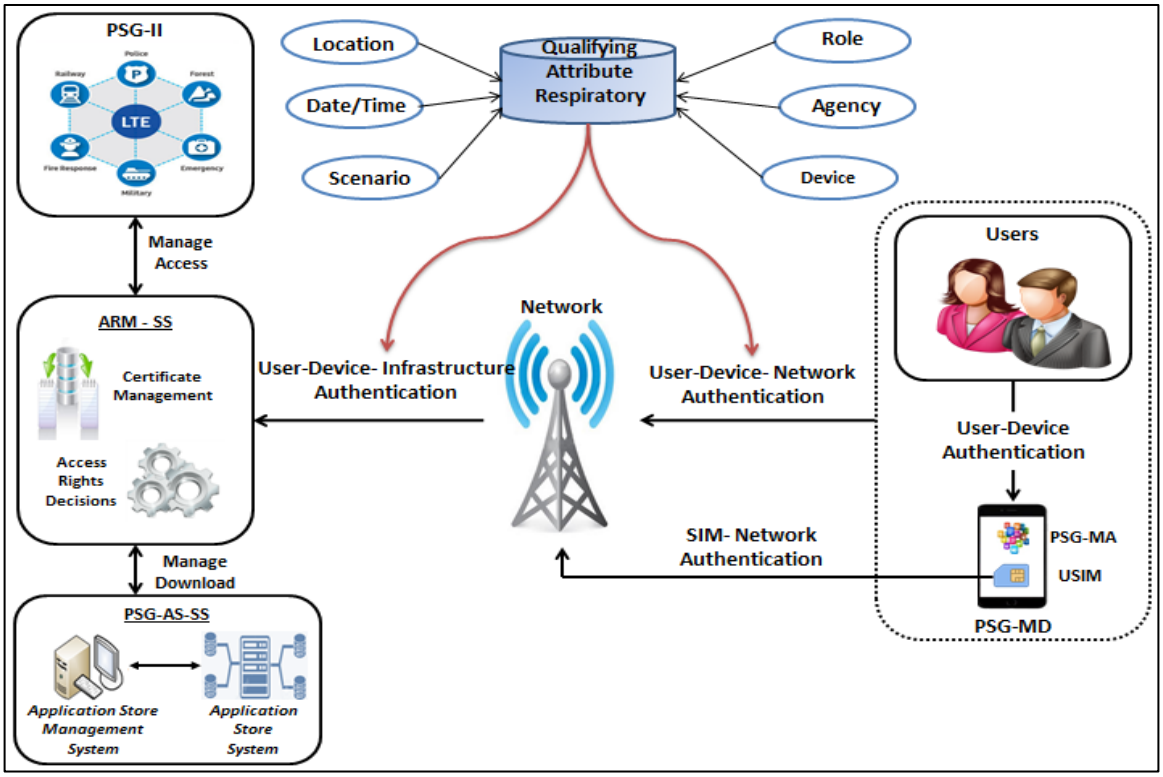

Figure 32 PSG-MAMF Authentication categories

9.3.2.1 User-Device (U-D) authentication

User-Device authentication is a local authentication, where the public safety User needs authenticate to the PSG-MD. Local authentication takes place before granting access past a lock screen. Local authentication mechanisms may consider *something you know, something you have*, and *something you are* categories of authentication, and may also consider combining different forms of authentication. The form of U-D authentication within the PSG-MAMF shall follow the policy of the agency that own the PSG-MD or the agency that the user belongs to.

The most common forms of local authentication to support U-D authentication are PINs, passwords, gestures, fingerprint scanners. In addition, Iris scanning, speaker authentication, and other forms of biometric reading can support the U-D authentication process. The U-D authentication is considered the first line of defence against malicious attempts to access the PSG-MD's information and functionalities.

Public Safety organizations are responsible for defining their own authentications forms based on the operational and security requirements within such organizations. The operational requirements affect the form of authentications used in public safety environments, since it may constrain the user's ability to authenticate the device. For example, operational requirements that require the user to wear gloves or masks could constrain the use of some forms of authentications (e.g. passwords, finger prints, and Iris scanning). The security requirements for each organization is different based on the level of assurance required.

There are some forms of authentications that started to be used as strong forms of authentications. For example, Universal Integrated Circuit Card (UICC) including the USIM can be used for local

authentication, where the user can authenticate locally to lock screen separated from the mobile OS, which in turn communicate with the USIM to perform the verification required. There are great efforts over the years to enhance the security capabilities of UICC. NIST IR 8014 provides further guidelines in terms of local authentication [80]

9.3.2.2 User-Device-Network (U-D-N) Authentication

PSG-MD's SIM logging to network infrastructure follow the LTE system technologies. Authentication between the PSG-MD' SIM and the cellular network are achieved via LTE authentication mechanisms. The major authentication mechanism used by mobile devices to authenticate to LTE network is known as "Authentication and Key Agreement (AKA) protocol" [79]. The SIM – Network authentication via AKA protocol is described in details by NISTIR 8014 [80]. In general, the authentication process takes place between the UICC on the mobile device and the network by evaluating a secret key K, then sequence of cryptographic functions take place. If the authentication process is completed successfully, the UE is granted access to the network.

However, the authentication process supported by LTE authenticates only the UICC to the network. Such authentication is not enough to meet public safety's operational and security requirements for authentication, since neither the PSG-MD nor the User is authenticated yet. Both PSG-MD and User authentication are required in case PSG-MD is to be shared between multiple Users. In addition, the authentication process should consider the occurrence of BYOD scenarios. In such case, the PSG-MD and the User identity and attributes need to be authenticated to allow enhanced functionalities, and grant access to the PSG-II according to appropriate privileges. Thus, PSG-MAMF requires more comprehensive methods for authentication that consider authenticating each single entity within the PSG-MAMF including the device itself and the user before granting them access to network and PSG-II. To support user and device authentication, the LTE standards need to support additions of LTE standards and capabilities, or a separate authentication framework is required to be built on the top of LTE.

A. Expanding LTE standards:

In terms of expanding the LTE standards to support more authentication capabilities, NISTIR 8014 suggests a supplementary context that enhance leveraging of IMSI and IMEI identifiers used by LTE for authentication services [80], however, such technique is not suitable for public safety environments for the following reasons:

- The IMSI (International Mobile Subscriber Identity) is a long term identity stored on UICC and used to identify the user. Typically, UICC is removable, which can be removed intentionally or stolen and used to perform unauthorized actions by impersonating the user. This makes the IMSI unsuitable to verify the user identity in public safety scenarios. However, on the long term, considering using eSIM described in section 6.5.6.3 would provide a solution for such problem, since the eSIM is embedded and can't be removed and exchanged between different Users.
- On the other hand, the IMEI (International Mobile Equipment Identifier) is a unique number used to identify mobile devices to the network. In addition, it can be used in the "blacklisting" process to prevent some Users from connecting to networks, which helps prohibiting stolen phones from assessing the network. Typically, IMEI is stored on the

device flash memory, or UICC, which make it possible to be altered or modified by user or attackers. Some countries prohibit the alteration of IMEI. However, due to the lack of long terms integrity of the IMEI, IMEI can't provide high level of assurance in User identity. This makes IMEI inadequate verification of user identity in public safety scenarios.

Hence, public safety requires a separate authentication framework that can be built on top of the LTE standards. The authentication framework shall provide a comprehensive vetting and authentication process for PSG-MD and Users identities, credentials, and other qualifying attributes as per subsection 9.1.

B. Identity and Authentication Framework:

In order to enable a secure User-Device access to network and PSG-II, public safety organizations require a reliable, secure, and interoperable authentication and identity management framework to identify User-Device access to network and assure appropriate information access. The framework must not require any identity and credential management on the Users side; however, the authentication process must take place completely on the system side. The authentication process shall be part of the system components within the PSG-MAMF as described in the architecture components in section 4.

The authentication and identity management framework can manage User-Device network access by managing the identities, credentials, and qualifying attributes on behalf of public safety organizations, and simplify and standardizing User-Device authentication and federated identities management across government and public safety organizations.

In public safety environment, it is likely that PSG-MDs are sharable between different responders during different shifts (e.g., shift-by-shift) or incidents, and BYOD scenarios are considered. Thus, public safety requires that access to information and services to be managed and controlled based on the device identity even PSOD or BYOD, User identity, qualifying attributes, sensor and integrity measurements, and other parameters as required by each organization. Hence, an "authentication and identity management framework" that extends beyond the LTE device authentication and support authentication process that perform such verifications is essential.

The authentication and identity management framework should be trusted to be utilized by public safety organizations to securely authenticate Users and PSG-MD on the network. The framework could be standards based, and can use cryptographically protected assertions to exchange User and PSG-MD identities, credentials, and qualifying attributes during the authentication process. Different public safety organizations have different requirements for User and PSG-MD identities, and different security policies. Public safety agencies possess the major responsibility for setting their own security policies and access rights that will be leveraged by the framework to manage and control access to information and services, and authorizing access according to those security policies. Hence, the framework should be able to handle the security policies defined by public safety organizations. Public safety organizations need to join the "authentication and identity management framework" so that Users and PSG-MDs from different organizations can be authenticated and federated through unique framework, and in turns trusted to other organizations.

However, to enable interoperable services through the usage of "authentication and identity management framework", public safety organizations should have an agreement upon the identity

information, and the set of attributes and their corresponding structure, as described in section 9.1. For example, "attributes that describe a user's name, organization or agency are fairly straightforward. Attributes that describe a user's role (e.g., chief, incident command, patrol officer, utility electrician, etc.) and a user's accreditations (e.g., EMS, paramedic, incident commander, SWAT team sharp shooter, etc.) will require common attribute value definition to ensure that identity information and attributes can interpreted in a common way" [80]. This agreement simplifies the authentication process, access control, and interoperability requirements.

9.3.2.3 User-Device-Infrastructure (U-D-I) authentication

Once a User-Device has been authenticated to the network via an authentication and identity management framework described in section 9.3.2.2, an access management mechanism should take place to control user access to resources within home network, jurisdiction network, and regionally based on their identity information combined with the 6 qualifying attributes listed in subsection 9.1. Users and Devices shall be authenticated and authorized to access information based on PSG-MD identity, User identity, role, agency, and other attributes listed in subsection 9.1, based on policies and access privileges defined by public safety organization.

PSG-MAMF follows the FICAM Roadmap implementation guidance for implementing identity, credential, and access management framework in public safety organizations. FICAM can be applied across variety of environments, and can be easily tailored to meet the operational requirements for public safety environment. This include environments associated with emerging IT advancements such as cloud computing, identity-as-a-service, and software-as-a-service. In addition, FICAM recommends the use of Personal Identity Verification (PIV) certificates as per "Homeland Security Presidential Directive 12" to provide enhanced processes (e.g. strong authentication, standardized processes, and digital signatures) [17] [8][13].

In addition, PSG-MAMF support Access Right Management (ARM) framework that aims to manage access to information on PSG-II and PSG-MD according to access rights and policies defined by public safety organizations. The ARM issues certificates that encapsulated and migrate with information to support information handling process.

9.3.3 Authentication Process

The authentication process supported by PSG-MAMF involves authenticating devices, Users, and applications before granting access to network and PSG-II. In order to ensure PSG-MD and Users gain according to their access privileges and access rights, Information Providers need to authenticate the requested entity in order to establish trustworthiness by verifying their identities, credentials, and qualifying attributes. The authentication process uses identities, credentials, tokens, and other qualifying attributes to provide assurance in an entity's access requests and access privileges. Typically, authentication involves two parties: an entity asserting an Access-Request (e.g. User, device, and application) and an entity verifying the request, determining the level of assurance, and asserting an Access-Reply (e.g. Information Provider).

PSG-MAMF supports an additional management framework as a third party involved in the authentication process as a proxy between the authentications parties. In this document, the management framework responsible for authentication is referred to as identity and authentication framework. The identity and authentication framework aims manage the authentication process and supplement the authentication protocol by authenticating the identities, credentials, and qualifying attributes on behalf of public safety organizations to provide enhanced assurance to

Information Providers. The identity and authentication framework may follow the precedents efforts and guidelines discussed in sections 9.3.2.2 and 9.3.2.3.

The authentication process uses authentication protocols as a way to provide assurance to the Information Provider through exchanging authentication protocol messages, in order to take an authentication decision to whether grant access or not. The authentication process may results in authentication success/failure, and the access decision should be included in the access-reply. After the authentication process, the result of the authentication process needs to be communicated to the PSG-II that the user was attempting to access. The communication takes place in the form of assertions, which states the Access-Decision, and user identity and attributes. The authentication protocol and assertion mechanism involves secure communications by exchanging messages and assertions through protected secure session, and setting a Time-to-Live for the assertion in order to expire after a period of time. By the time assertion expire, any access to PSG-II require the authentication process to be held from scratch [14].

The authentication, authorization, and access control process is described in Figure 33, and can be summarized as following:

(1) A User requests access to network or PSG-II by sending an Access-Request and presenting digital identity, credentials, privileges, and 6 qualifying attributes in order to authenticate themselves. Such process requires both the user and device to be authenticated, using "User-Device-Network authentication" described in section 9.3.2.2, and "User-Device-Infrastructure authentication" described in section 9.3.2.3.
(2) The identity and authentication framework validates the digital identity, credentials, and qualifying attributes using the appropriate authentication techniques and protocols. The authentication protocols and techniques typically require the user to prove that they are in control or have possession of the credential. This may take place in form of entering a user ID and password, inserting a smart card into a device and activating it with a password, or other form of credentials as described in section 9.2.2.
(3) Once the User has been authenticated to the network via the authentication and identity framework, the result of authentication is forwarded to PSG-II in form of assertion that state the Access-Decision, user identity, and the 6 qualifying attributes associated to this unique user's digital identity. The PSG-II grant the user access to information and services according to their privileges, access rights, and the 6 qualifying attributes received via the assertion.
(4) The Access Right Management (ARM) manages access to information and services on behalf of PSG-II by verifying the User's access rights based on the rules, policies, and access privileges defined by public safety organizations.
(5) The Access Right Management (ARM) creates a license file that contains the rules, policies, and organizational requirements that should be applied to information according to the User access Rights. Such license should be encapsulated with the information to manage information handling process.
(6) The Audit and Reporting records the access event to be used as court admissible record.

Accordingly, the authentication and authorization process requires techniques, services, and protocols to manage such process including: identity validation, credential validation,

authentication protocols, session management, data exchange, assertions, access authorization, policy management, policy decision, and, policy enforcement.

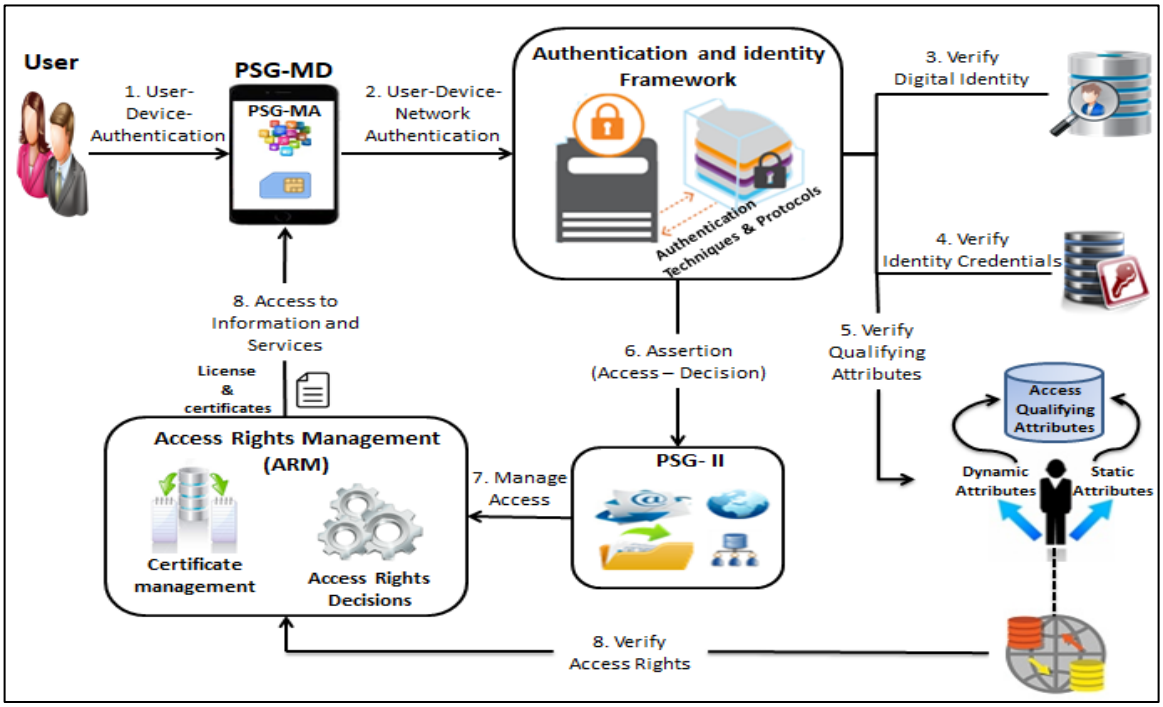

Figure 33 Authentication, Authorization, and Access Control process

9.3.3.1 Authentication Protocols

Authentication protocols are protocols used during authentication process that use a set of messages between two authentication parties to establish confidence in an entity. The authentication protocols ensure the device, user, or application possess valid digital identity, credential, and qualifying attributes before granting access to network, information, and services. Authentication process uses the authentication protocols also to verify the entity claiming an access request have a valid credential key that is not revoked, suspended, or expired, by securely communicating the policy under which the credential was issued. Hence, mapping the digital identities, credentials, and qualifying attributes with the policies provide an effective tool for higher levels of assurance when authenticating an entity [80].

The levels of assurance that can be placed in entities typically depend on the strength of authentication processes and protocols used. The strength of an authentication protocol depends heavily on the way the protocol was designed and the types of risk the protocol can mitigate. NIST SP 800-63-2 provides a list of level of assurance of used protocols based on different types of threats [7]. However, threats that can't be mitigated by an authentication protocol can be mitigated by other parts of the authentication process, and additional security controls and technologies. Authentication protocols are typically designed for particular situations, whereas protocols used for device authentication may be different from protocols used for User authentication depending on the type of threats that protocol need to protect against. An example of authentication protocol and standards is LTE AKA, the primary LTE authentication protocol used to authenticate the mobile device's SIM to LTE network [79].

9.3.3.2 Authentication Assertions

The assertions are existing technologies that can be used as part of the authentication process to establish confidence through authentication protocols. Assertions enables access to information and services by exchanging statements between Information Provider and the entity requiring access to information and services. Such statements can describe the state of the entity requiring access, identity, and access privileges to establish a confidence in such entity (e.g. PSG-MD, PSG-MA, or User) and ensure that integrity and confidentiality are addressed. According to the assertions received, the appropriate privileges and access rights are assigned to the particular User or PSG-MD. SAML token is a common example of security token assertion. Assertions are discussed in details in NIST SP 800-63-2 [14].

Assertion-based authentication has different models, known as: direct model, indirect model, and proxy model [14]. PSG-MAMF would rely on the proxy model for assertion based authentication. In the proxy model, a verifier acts as a proxy or intermediary between the entities requesting access (e.g. User, PSG-MD or PSG-MA) and Information Provider to manage the authentication process. The advantage of the proxy is managing access to multiple Information Providers at the same time, and enabling network monitoring and filtering. As mentioned earlier, the authentication process within the PSG-MAMF would follow the LTE standards along with the identity and authentication framework that act as a proxy between the PSG-MD and the Information Provider to manage the authentication process. Typically, the User, PSG-MD, or PSG-MA authenticate to the identity and authentication framework. After a successful authentication, the identity and authentication framework creates an assertion, and then the assertion can be forwarded to the Access Right Management (ARM) framework to create the access licenses according to the management files provided by the Information Providers and assertions received from the identity and authentication framework. The ARM would control access to information based on User and device identity, location, integrity measurements, sensors information, and other qualifying attributes used to determine access rights. The licenses created by the ARM contain the rules, policies, and organizational requirements that should be applied on the information according the Users access privileges. Therefore, the identity and authentication framework and the ARM shall collaborate in order to provide the capabilities required for authentication, authorization, and access control as described in Figure 33.

Assertion-based authentication provide the following advantages [14]**:**

- Support the process of Single-Sign-On (SSO) for User, which allow Users to authenticate once and then gain access to information and services from multiple Information Providers, without the need of further authentication. Typically, the authentication process use assertions to communicate the result of authentication, which may have a Time-to-Live. After such time, the authentication process has to be carried out from scratch.
- Support the implementation of federated identity management required by PSG-MAMF. This allows linkage of multiple users' identities with different Information Providers through a common federated identifier, which in this document referred to as "Identity and Authentication Framework". In PSG-MAMF, a federation is a group of Information Providers connected together through active directory, security policies, trust mechanisms, and protocols. Users authenticate to different Information Providers through

identity and authentication framework that manages authentication process between the User and the Information Provider. Figure 33 illustrate the process of assertion-based authentication, authorization and access control.

- Support enhanced authentication schemes that are based on attributes, and digital identity of the User, PSG-MD, and PSG-MA. These attributes are usually used to determine access privileges in form of Attributes Based Access Control (ABAC) or Role Based Access Control (RBAC). According to FICAM Roadmap and Implementation Plan v2.0 [FEDCIO2] (2011), Attribute Based Access Control (ABAC) model is recommended for managing access to information and services among organizations that require a restrictive access control [13]. NIST SP 800-162 provides guidance for Attribute Based Access Control (ABAC) model for managing access to information and services based on defined qualifying attributes [114].

Assertions can be implemented using various technologies such as “cookies, Security Assertion Markup Language (SAML), Kerberos tickets, and other assertion technologies” [14]. Assertions are usually a potential target for attackers, since they enable access to information and services. Thus, assertions need to be protected against different threats through additional security controls that shall be satisfied. NIST SP 800-63-2 provided more details to the authentication process, authentication protocols, and assertions [14].

10 Conclusion

The "Public Safety Grade - Mobile Application Management Framework" is focused on providing a framework for mobile device and mobile application management in public safety organizations. Government organizations and public safety communities are expressing great interest and reliance on mobile devices as a platform that can increase productivity and assist first responders in their day-to-day operations, as well as responding effectively to emergency situation. Adoption of mobile application management in organizations increases productivity, real-time information sharing. In addition, modern mobile device capabilities (e.g. sensors) have the potential to provide enhanced mission capabilities, support situational awareness and contextual decision making.

However, mobile devices and applications raise concerns regarding vulnerabilities and threats to the security and integrity of information due to the nature of mobility and sophistication of attacks. The potential for mobile devices to be compromised, stolen or monitored is greater in a mobile environment compared to a fixed infrastructure. In addition, some organizations may allow Bring Your Own Device (BYOD), a decision that increases the challenges of providing a secure environment. In general, existing mobile devices are unable to provide string security assurance to users and organizations, due to lack of security capabilities in current mobile devices. Current mobile security technologies are insufficient to mitigate the risks and threats associated. Further, mobile application can potentially lead to serious security risks, as it may contain vulnerabilities that can be exploited by intruders to gain unauthorized access to device resources including sensitive information residing the mobile device. Furthermore, Access to organizational infrastructure to exchange information and services can expose information infrastructure and information residing the devices to potential security risks.

The reliance on mobile devices and applications is growing at a tremendous rate. This introducers the potential for more security threats, and has led to increasing demand in the government and public safety community for a safer mobile application framework. The security, fidelity, integrity, reliability, resiliency, privacy, and interoperability requirements each influence the need for standards, best practices, security controls and security technologies that well-suit the need of organizations, to be developed and implemented to leverage mobile device security and mobile application security tailored for government and public safety environments.

In this thesis we made the following contributions:

- We investigated the current security controls, technologies, best practices in terms of mobile devices security and mobile applications security. We reviewed the standards, and relevant studies recorded by NIST, FirstNet, NPSTIC, DHS, DoD, DRDC, CSSP, RCMP, Cloud Security Alliance, CIO Council, OWASP, GlobalPlatform, Trusted Computing Group, NIAP, Silent Circle, Wide Point, MTTT and other known practices in mobility and security.
- We expanded our investigation to cover security technologies intended to build semi-closed ecosystem components that can be integrated effectively to provide the security required for public safety environments, as well as the current efforts towards implementing mobile application ecosystem to provide the security required for mobile devices and applications adoptions by organizations. As a result, we realized the lack of integration between different technologies and solutions that raises that need for single,

integrated, comprehensive framework based on the investigated standards, recommendations, practices, security technologies and controls that can ensure the proper baseline security level for government and public safety community. In addition, we highlighted a group of identified threats and security gaps in terms of mobile device security, mobile application security, and current ecosystems, as discussed per sections 2.1, 2.2, and 2.3.

- We proposed a framework, the Public Safety Grade-Mobile Application Management Framework (PSG-MAMF), that provide a unique level of integration which is missing from other frameworks. The framework components are discussed in details in Chapter 3, while the interaction between components to provide the security capabilities required by the proposed framework are discussed in Chapter 4. We developed our framework based on security principles aiming to provide the desired level of security and interoperability requirements that meet the needs of the public safety community. PSG-MAMF allows security requirements to be met by relying on available technologies as much as possible and by bringing to bear best practices from Canada and the US. PSG-MAMF was designed to meet the following security principles:

(1) Data Protection at rest, in motion, and in use, by creating the following:
   - Protected storage supported by security capabilities, including containerization, encryption, authentication, and Access Right Management (ARM)
   - Protected communication supported by information encryption and use of secure communication channels (e.g. VPN)
   - Protected execution supported by protected execution environment, encrypted memory space, and ARM.

(2) Data isolation through containerization, virtualization, sandboxing, data tagging, and baseband isolation.

(3) Device Integrity Verification, continuous monitoring, and integrity measurements reporting through attestation.

(4) Continuous monitoring, detecting, and reporting of all system activities and applications.

(5) Policies Enforcement including:
   - Information access management, information usage, information storage, and information sharing.
   - Enforcement of handling requirements (e.g. selective wipe)

(6) Auditing, Logging, and Reporting.

(7) Authenticating each single entity in the system using enhanced authentication mechanisms including:
   - Authentication schemes based on attributes “Attribute Based Access Control (ABAC)” (e.g. role, agency, location, time, scenario, etc.).
   - Authentication schemes based on Sensor data and integrity measurements of the mobile device.

- We highlighted a set of requirements that include security gaps c for mobile devices to be qualified to serve as a Public Safety Grade Mobile Devices (PSG-MD) and to enable the framework proposed. Mobile device basic capabilities include: battery usage, camera, sensors, memory, and network capabilities. While mobile device security components include essential security components to qualify PSG-MD, namely: Chain of Trust, Root

of Trust (RoT), Access Right Management (ARM), Device Integrity and Assertions to insure that the mobile device is in a trusted state.

- We provided an overview of mobile applications vulnerabilities, strategies to reduce the risks of untrusted applications, and recommended an ecosystem that includes a set of capabilities and processes to provide a full lifecycle management of applications which include:
  - Supporting a private application store: Public Safety Grade-Application Store.
  - Supporting application vetting processes.
  - Performing Management and Monitoring of Applications
  - Applications sharing and access management
- Finally, we covered the different types of authentication supported by the PSG-MAMF authentication process. The objective is to authenticate each single entity within the PSG-MAMF environment before granting access to information, infrastructure and network. We also the current efforts in deploying reliable, secure, interoperable authentication and identity management framework, resulting in a comprehensive framework that supports federated identity and authentication management.

References/Bibliography

[1] N. Keshta, "Secure Mobile Application Management Framework," *Univ. Regina*, 2018.

[2] DHS and NIST, "DHS Study on Mobile Device Security - April 2017 - FINAL," no. April, 2017.

[3] ITSG, "INFORMATION TECHNOLOGY SECURITY GUIDANCE - SECURING THE ENTERPRISE FOR MOBILITY," no. July, pp. 1–11, 2016.

[4] NIST, "Guidelines on Hardware-Rooted Security in Mobile Devices (Draft)," vol. 164, no. SP 800-164, pp. 1–33, 2012.

[5] NIST, "NIST Special Publication 800-124 Guidelines for Managing the Security of Mobile Devices in the Enterprise," *NIST Spec. Publ.*, p. 30, 2013.

[6] NIST, "Guidelines on Mobile Device Forensics (Draft)," vol. 1, 2014.

[7] NIST, "Electronic Authentication Guideline (Special Publication 800-63-2)," 2013.

[8] NIST, "Draft NISTIR 7981 Mobile , PIV , and Authentication," pp. 1–14, 2014.

[9] OCIO, "ELECTRONIC CREDENTIAL AND AUTHENTICATION STANDARD," 2010.

[10] The U.S. Department of Justice; The U.S department of homeland Security, "The Global Federated Identity and Privilege Management (GFIPM)," 2014.

[11] NIEM, "NIEM Background and Benefits." [Online]. Available: https://www.publicsafety.gc.ca/cnt/bt/niem/bk-bnft-en.aspx.

[12] K. Icam, S. Areas, T. Federal, I. Roadmap, E. Branch, and F. Government, "Identity , Credential , and Access Management Segment Architecture What is Identity , Credential , and Access Management (ICAM)? The Roadmap."

[13] ICAMSC, "Federal Identity , Credential , and Access Management (FICAM) Roadmap and Implementation Guidance V2.0," *Management*, 2011.

[14] NIST, "Electronic Authentication Guideline," *NIST Spec. Publ.*, vol. 800, p. 112, 2013.

[15] OMB, "E-Authentication Guidance for Federal Agencies," *Director*, no. 202, pp. 1–17, 2003.

[16] Executive Office of the President, "Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors," 2004. [Online]. Available: https://www.dhs.gov/homeland-security-presidential-directive-12.

[17] NIST, “Guidelines for Derived Personal Identity Verification (PIV) Credentials,” *NIST Spec. Publ.*, pp. 800–157, 2014.

[18] ATIS, “ATIS-1000035.2009: Next Generation Framework (NGN) Identity Management (IDM) Framework,” 2009.

[19] ATIS, “ATIS-1000044.2011: ATIS Identity Management: Requirements and Use Cases Standard,” 2011.

[20] ATIS, “ATIS-1000045.2012: ATIS Identity Management: Mechanisms and Procedures Standard,” 2012.

[21] ATIS, “ATIS-1000030.2008: Authentication and Authorization Requirements for Next Generation Network (NGN),” 2008.

[22] NPSTC, “Public Safety Broadband High-Level Launch Requirements,” 2012.

[23] NIST, “Vetting the Security of Mobile Applications (NIST Special Publication 800-163),” 2015.

[24] NIST, “An Overview of Mobile Application Vetting Services for Public Safety,” 2017.

[25] NIST, “Public Safety Mobile Application Security Requirements Workshop Summary,” 2015.

[26] CIO, “Adoption of Commercial Mobile Applications within the Federal Government,” 2013.

[27] Open Web Application Security Project (OWASP), “OWASP Mobile Security Testing Guide.” [Online]. Available: https://www.owasp.org/index.php/OWASP_Mobile_Security_Testing_Guide.

[28] OWASP, “Mobile AppSec Verification,” 2017.

[29] OWASP, “Mobile App Security Testing,” 2017.

[30] OWASP, “Mobile App Security Checklist.” OWASP, 2017.

[31] Cloud Security Alliance (CSA), “Mobile Application Security Testing,” *Foundstone Whitepaper*, no. June, pp. 1–27, 2016.

[32] Open Web Application Security Project (OWASP), “OWASP Mobile Security Project.” [Online]. Available: https://www.owasp.org/index.php/OWASP_Mobile_Security_Project.

[33] MTTT and CIO, “Mobile Computing Decision Framework,” pp. 1–23, 2013.

[34] MTTT and CIO, “Mobile Computing Decision Framework - Appendix,” 2013.

[35] NIST, "NIST Special Publication 800-37 Guide for Applying the Risk Management Framework to Federal Information Systems," p. 102, 2010.

[36] NIST, "Managing Information Security Risk," *NIST Spec. Publ. 800-39*, no. March, p. 88, 2011.

[37] CIO, "Mobile Security Reference Architecture," p. 103, 2013.

[38] Federal Chief Information Officer Council (CIO), "Government Mobile and Wireless Security Baseline," 2013.

[39] DHS, DoD, and NIST, "Federal-Mobile-Security-Baseline-Appendix-A-11." 2013.

[40] BlackBerry, *The Definitive Guide to Enterprise Mobile Security*. 2015.

[41] R. Smith, B. Taylor, M. Bhat, C. Silva, and T. Cosgrove, "Magic Quadrant for Enterprise Mobility Management Suites," no. Mdm, pp. 1–40, 2017.

[42] Garnet, "Magic Quadrant for Enterprise Mobility Management Suites," 2017.

[43] NIST, "NIST SP 1800-4 - Draft: Practice Guide – Mobile Device Security," 2017.

[44] National Institute of Standards and Technology (NIST), "BUILDING BLOCK MOBILE DEVICE SECURITY : CLOUD & HYBRID BUILDS," 2017.

[45] National Institute of Standards and Technology (NIST), "Mobile Device Security: Enterprise Builds," 2018. [Online]. Available: https://nccoe.nist.gov/projects/building-blocks/mobile-device-security/enterprise.

[46] NIST, "Mobile device security For Enterprise (MDSE)," 2014.

[47] GAO, "INFORMATION Better Implementation of Controls for Mobile Devices Should Be Encouraged," no. September, 2012.

[48] Mark Golaszewski and First Responder Network Authority (FirstNet), "What is an Applications Ecosystem?," 2015. [Online]. Available: http://www.firstnet.gov/newsroom/blog/what-applications-ecosystem.

[49] First Responder Network Authority (FirstNet), "Advanced, customized apps developed for public safety's sake," 2017. [Online]. Available: https://www.firstnet.com/apps/app-store.

[50] R. Sheldon, "Mobile application management comparison: App wrapping vs. containerization," *Search Mob. Comput.*, 2014.

[51] J. D. Averill, D. Holmberg, A. Vinh, and W. Davis, "Building Information Exchange for First Responders Workshop :," no. June, 2009.

[52] NIST, "Security and Privacy Controls for Federal Information Systems and Organizations," 2013.

[53] NIST, “Guide for Developing Security Plans for Federal Information Systems,” no. February, 2006.

[54] NIST, “Guide for Applying the Risk Management Framework to Federal Information Systems,” vol. 1, 2016.

[55] “The Four Phases of the Certification and Accreditation Process,” 2013. [Online]. Available: http://www.qtsdatacenters.com/resources/blog/2013/09/13/the-four-phases-of-the-certification-and-accreditation-process.

[56] ITSG, “Information Technology Security Guidance IT Security Risk Management : A Lifecycle Approach,” no. December, 2014.

[57] I. Liccardi, J. Pato, and D. J. Weitzner, “Improving Mobile App Selection through Transparency and Better Permission Analysis,” no. 2, pp. 1–55, 2013.

[58] Ron Wilson, “Secure Embedded Systems: Digging for the Roots of Trust,” 2015.

[59] Gfedorkow and Juniper Networks, “What’s the Difference between Secure Boot and Measured Boot?,” 2015.

[60] K. N. McGill, “Trusted mobile devices: Requirements for a mobile Trusted Platform Module,” *Johns Hopkins APL Tech. Dig. (Applied Phys. Lab.*, vol. 32, no. 2, pp. 544–554, 2013.

[61] Samsung Knox, “Real-time Kernel Protection (RKP),” 2016. .

[62] Samsung Knox, “TIMA attestation.” [Online]. Available: https://seap.samsung.com/html-docs/android-premium/Content/about-tima-attestation.htm.

[63] C. Daly, “Assertion Framework for BYOD,” pp. 1–29.

[64] T. S. Messerges and E. A. Dabbish, “Digital Rights Management in a 3G Mobile Phone and Beyond.” 2003.

[65] R. Muller, “How IT Works Windows Rights Management Services,” 2006.

[66] K. Singh and IBM, “Practical Context-Aware Permission Control for Hybrid Mobile Applications,” 2013.

[67] OMA, “User Plane Location Protocol,” 2011.

[68] OMA, “Secure User Plane Requirements,” no. May, pp. 1–22, 2012.

[69] OMA, “Secure User Plane Location Architecture,” 2008.

[70] M. Campbell, “Future Apple devices may boast environmental sensor suite with built-in thermometer,” *Apple Insid.*, 2014.

[71] R. Felts and R. Felts, “Public Safety Analytics R & D Roadmap NIST Technical Note 1917 Public Safety Analytics R & D Roadmap,” 1917.

[72] S. Social, “Sensordrone - 11 Sensors For Your Smartphone.”

[73] 3GPP Organizational Partners, “3GPP TR 23.708,” 2015.

[74] 3GPP Organizational Partners, “3GPP TS 23.682,” vol. 0, no. Release 13, 2016.

[75] C. Perera, A. Zaslavsky, P. Christen, A. Salehi, and D. Georgakopoulos, “Capturing Sensor Data from Mobile Phones using Global Sensor Network Middleware,” 2013.

[76] E. B. Protection, A. Type, and S. Memory, “Enhancing System Security with Macronix Flash,” pp. 1–12, 2014.

[77] H.-W. Tseng, L. Grupp, and S. Swanson, “Understanding the Impact of Power Loss on Flash Memory,” *Proc. 48th Des. Autom. Conf.*, pp. 35–40, 2011.

[78] H. Handschuh and E. Trichina, “Secure Integrated Circuits and Systems,” 2010.

[79] D. Forsberg, G. Horn, W.-D. Moeller, and V. Niemi, *LTE Security*. WILEY, 2012.

[80] NIST, “Considerations for Identity Management in Public Safety Mobile Networks (NISTIR 8014),” 2015.

[81] SIMalliance, “Device Implementation Guidelines,” no. June, 2013.

[82] N. Elenkov, “Using the SIM card as a secure element in Android,” 2013. [Online]. Available: https://nelenkov.blogspot.ca/2013/09/using-sim-card-as-secure-element.html.

[83] N. Pohlmann, H. Reimer, and W. Schneider, *ISSE/SECURE 2007 Securing Electronic Business Processes - Highlights of the Information Security Solutions Europe/SECURE 2007 Conference*. 2007.

[84] E. S. Jeong, B. H. Kim, and D. H. Lee, “Security scheme for high capacity USIM-based services,” *Int. J. Secur. its Appl.*, vol. 7, no. 4, pp. 433–444, 2013.

[85] K. E. Mayes and K. Markantonakis, “On the potential of high density smart cards,” *Inf. Secur. Tech. Rep.*, vol. 11, no. 3, pp. 147–153, 2006.

[86] E. Vahidian, “Evolution of the SIM to eSIM,” 2013.

[87] C. Notice and A. Notice, “Embedded SIM Remote Provisioning Architecture,” pp. 1–84, 2014.

[88] A. Rahmati, “Context-Specific Access Control : Conforming Permissions With User Expectations,” 2015.

[89] Mkhalili2, “Four Reasons Why Mobile Containerization Now Matters More Than Ever,”

Blackberry Bus. Blog, 2016.

[90] OWASP, "Mobile Security Project Archive," 2016.

[91] Microsoft TechNet, "Digitally Signed Software."

[92] C. Miller and C. Poellabauer, "Configurable integrated monitoring system for mobile devices," *Procedia - Procedia Comput. Sci.*, vol. 34, pp. 410–417, 2014.

[93] A. Shuba, U. C. Irvine, S. Langhoff, U. C. Irvine, U. C. Irvine, and U. C. Irvine, "Demo : AntMonitor - a System for Mobile Traffic Monitoring and Real-Time Prevention of Privacy Leaks Categories and Subject Descriptors."

[94] F. Information and P. Standards, "Standards for Security Categorization of Federal Information and Information Systems," no. February, 2004.

[95] NIST, "An Introduction to Information Security," vol. 12, 2017.

[96] NIST, "Recommendations for security controls for Federal Information Systems," 2005.

[97] Wikipedia, "Classified Information," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Classified_information#NATO_classifications.

[98] OCIO, "Information Security Policy," no. July, 2016.

[99] The Open Group Security Program Group, "INFORMATION SECURITY LABELLING Requirements Statement," no. September, 1997.

[100] NIST and Federal Information Processing Standards, "ADVANCED ENCRYPTION STANDARD (AES)," 2001.

[101] NIST, "Guide to Storage Encryption Technologies for End User Devices Recommendations of the National Institute of Standards and Technology," 2007.

[102] Philippe Beraud; Microsoft, "Protect-your-key-assets-through-information-classification." 2014.

[103] NIST and Federal Information Processing Standards, "SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES," 2002.

[104] NIST and Federal Information Processing Standards, "SECURE HASH STANDARD," vol. 2, 2008.

[105] NIST, "Recommendation for Key Management – Part 1," vol. 3, 2015.

[106] NIST, "Recommendation for Key Management – Part 2 : Best Practices for Key Management Organization," 2015.

[107] NIST, "Guide for the Security Certification and Accreditation," vol. 1, 2015.

[108] Salesforce, "Salesforce Security Guide," 2017.

[109] CISCO, "Broadband Revolution: Roadmap for Safety and Security Mobile Communication Services." 2012.

[110] NIST, "Digital identity guidelines: revision 3," 2017.

[111] NIST, "FIPS PUB - Personal Identity Verification (PIV) of Federal Employees and Contractors," *Nist-Fips Pub 201-2*, no. August, pp. 1–87, 2013.

[112] NIST, "Interfaces for Personal Identity Verification – NIST Special Publication 800-73-4," vol. 4, 2015.

[113] Federal Public Key Infrastructure Policy Authority (FPKIPA), "The U.S. Federal PKI Common Policy Framework," 2014.

[114] NIST, "Guide to attribute based access control (abac) definition and considerations," *NIST Spec. Publ.*, vol. 800, p. 162, 2014.

[115] L. Flw and X. H. G. X. Kn, "Mobility Management For Enterprises In BYOD Deployment," vol. 76, 2016.

[116] Blackberry, "The CIO ' s Guide to UEM," 2015.

[117] C. Smulders and P. DeBeasi, "Mobile Enterprise Strategy Key Initiative Overview," *Gartner.Com*, 2014. [Online]. Available: https://www.gartner.com/doc/2700917?ref=SiteSearch&sthkw=mobile&fnl=search&srcId=1-3478922254.

[118] D. D. Visibility and D. A. Control, "Mobile Device Management and Enterprise Mobility Management Integrations with Cisco Identity Services Engine," 2017.

[119] AirWatch, "Transform Business with Comprehensive Enterprise Mobility Management (EMM)." [Online]. Available: https://www.air-watch.com/en/solutions/enterprise-mobility-management/.

[120] K. Hess, "10 Enterprise Mobility Management Solutions: Beyond MDM."

[121] CITRIX, "Enterprise Mobility Management (EMM)." [Online]. Available: https://www.citrix.com/enterprise-mobility-management/.

[122] IBM, "Introducing IBM MaaS360 with Watson 'A cognitive approach to unified endpoint management.'" [Online]. Available: https://www.ibm.com/security/mobile/maas360.html.

[123] MobileIron, "Enable business transformation with MobileIron's Enterprise Mobility Management (EMM) platform." [Online]. Available: https://www.mobileiron.com/en/solutions/enterprise-mobile-management-emm.

[124] Symantec Corporation, "Enterprise Mobility Management | Symantec Mobility,"

Symantec Corp., p. 3, 2012.

[125] BlackBerry, "BlackBerry Enterprise Mobility Suite." [Online]. Available: https://us.blackberry.com/enterprise/blackberry-enterprise-mobility-suite.

[126] Microsoft, "Keep pace with security challenges." [Online]. Available: https://www.microsoft.com/en-ca/cloud-platform/enterprise-mobility-security.

[127] S. Date, "Non-Functional Requirements in Mobile Applications," 2013.

[128] T. Schiesser, "Guide to smartphone hardware (3/7): Memory and Storage," 2012.

[129] Wikipedia, "Software Development Kit," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Software_development_kit.

[130] Microsoft, "Enabling DRM Support," 2017. [Online]. Available: https://msdn.microsoft.com/en-us/library/windows/desktop/dd798059(v=vs.85).aspx.

[131] Serdar Yegulalp and TechNet, "Microsoft Rights Management Services: An introduction," *TechTarget*, 2006.

[132] Wikipedia, "Trusted Platform Module," 2017. [Online]. Available: https://en.wikipedia.org/wiki/Trusted_Platform_Module.

[133] Wikipedia, "Active Directory." [Online]. Available: https://en.wikipedia.org/wiki/Active_Directory.

This page intentionally left blank.

Annex A Mobility Management Mechanisms

Mobile devices used in enterprises or regulated sectors poses tremendous security challenges for organizations that have to abide strict rules and policies to mitigate such risks. For example, banks, credit unions and other financial services organizations require strict access control policies, formal information security strategies, and other security controls that aim to protect integrity, confidentiality, and privacy of financial information. Regulated organizations including law enforcement (e.g. police), Fire and Protection Services, Emergency Medical Services, rescue groups, and emergency responders and many others need to access infrastructure to gain information that enhance their situation awareness and help them to effectively perform their duties. However, any access to the infrastructure has to comply with the strict rules, policies and regulations. In addition, the BYOD "Bring Your Own Device" introduces additional security challenges that require a set of policies to regulate the use of BYOD and deal with the threats and security risks it bring to the organization. In regulated and governmental agencies, IT administrators should assume that mobile devices either organization owned devices, or BYOD are inherently insecure. Such cases require comprehensive cyber security approaches that include different monitoring and management tools that have the ability to provide a set of security compliance requirements. The set of security compliance requirements are aim to ensure the confidentiality, integrity, and Availability of information during storage, transit, and process across multiple organizations, users, devices, and applications. Hence, organizations require a comprehensive mobility management solution that can offer board range of security functionalities including:

- Containerization and isolation of private information from enterprise/governmental information on organization-owned or BYOD devices.
- Management functions and services including locking and wiping of the device
- Encryption and decryption of information
- Authentication and access control
- Auditing and reporting
- Private application store as a trusted source to distribute applications

The primary enterprise mobility management solutions fall into three categories: Mobile Device Management (MDM), Mobile Application Management (MAM) and Mobile Content Management (MCM). However, today many vendors are blurring the lines between these solutions by providing comprehensive solutions that addresses devices, applications and content in a single solution. Although the management approaches offered by different vendors cover much of the security concerns, some enterprises and governmental environments require adding additional security technologies, standards, and policies to address their security requirements.

A.1 Mobile Device Management (MDM)

MDM refers to "Mobile Device Management" which is a mobility management solution that is used as a main tool for managing mobile devices security at the device level. MDM is an effective approach for setting up mobile devices, managing mobile email, and access points for devices. MDM system can remotely monitor the mobile devices status and control their functions.

MDM is a key requirement for organizational owned devices, although MDM is pushed back because of the concerns relevant to privacy and legal concerns.

MDM solutions offer software-based enforcement of security policies that manage the whole device or a segregated virtual portion of it that includes remote lock and wipe capability, policy enforcement, and data tracking. MDM enables IT to deploy, configure, manage, support and secure mobile devices. Usually MDM management system is used for devices which are owned by corporate to make them better secure and keep all confidential information protected.

MDM system infrastructure consists of two main components: MDM agent and MDM server, along with gateway server, and MDM console. MDM server side has all the controlling capabilities over the MDM agent side, by triggering commands to the managed mobile device, MDM server can control, lockdown, remotely wipe, encrypt, and enforce policies on the mobile devices. MDM agent is an application installed on mobile devices to keep the device synchronized with the MDM server. The MDM agents is responsible for exchanging mobile device status information and user information to MDM server, act according to the push and pull commands from management server, and apply the relevant policies and administrative operations (e.g. remote wipe). MDM primary features are as following [115]:

- Remote wiping of mobile devices
- Remote locking of mobile devices
- Monitor and track mobile devices
- Profile management
- Detecting malware
- Protect information by storing it in encrypted spaces
- Access control using authentication and authorization

MDM solutions suffer from several limitations. First, MDM requires a profile to be installed on the mobile devices in order to be able to manage it. Thus, it is not the ideal solution in case of BYOD scenario. Second, if a federal agency needs to share an application with government and first responders, most commonly, those user's devices are controlled by variety of different MDM systems from different vendors. Thus, distributing the application becomes a real challenge. This requires all the organizations to enrol their users in the same MDM system. Third, the MDM has a security gap around the applications and information on the devices being managed by MDM.

However, when it comes to mobile applications and information within the enterprise or governmental organization, a management mobility solution is required at higher level than device level. Applications and information require more fine-grained security policies where a higher level of security and management is required at the application level and information level. Nowadays, MDM has changed from being a stand-alone product into a required feature along with MAM, and MCM features within the enterprise mobility management (EMM) suites.

A.2 Mobile Application Management (MAM)

MAM refers to "Mobile Application Management" is a mobility management approach that works at the application level by managing a list of applications rather than the entire device. MAM aims to provide more granular control by facilitating the deployment and operational life cycles management of mobile application including administrative management, install and update of application, and license management. The idea of MAM is to distribute policy-enabled mobile applications that allow the administrators manage applications and information on a

device with security and management policies, and selectively wipe applications and its related information remotely. MAM solutions enable policies to applications by wrapping the application with policies such as app-level security policies, app-level VPN, copy/paste restrictions, data wipe controls, encryption, application expiration, etc.

MAM solutions apply policies to enterprise applications include security policies, by providing the following services [115]:

- Per-app VPN connection
- Selectively wipe applications and information remotely
- Whitelisting and blacklisting of applications
- Enrolling certification for application
- Encrypting enterprise applications information at rest, in motion, and while processing, which may include stronger encryption than OS encryption.
- Restricting actions including cut, copy, and paste.
- Requiring conditional launch or access (e.g. device in approved state, no jailbreak or rooting detected).
- Enterprise Application store, application distribution
- Applying applications policies by leveraging on native OS MAM APIs (however, native APIs hard to be accessed), Application wrappers (code injection into the binary post development), or SDKs compiled into applications during development.

MAM nowadays is a required feature along within the enterprise mobility management (EMM) suites. MAM provide application extensions tools that allow the mobile applications to be managed via EMM by leverage controls built into applications. SDKs and/or applications wrappers are required for use cases that managed application delivered to devices that are not enrolled in EMM. Otherwise, EMM vendor's SDK has to be used. SDK's provide libraries that compiled with mobile applications by organizations to enable policies to be applied to them. Wrappers on the other hand, use a code that is injected into the binaries of mobile devices to enable policies to be applied.

A.3 Mobile Content Management (MCM)

MCM refers to "Mobile Content Management" which is a mobility management approach that works at the content level by providing a way to encrypt, store, deliver and manage information and services securely on the mobile devices. Mobile devices, applications, and users can access corporate information and services at any place. The IT needs to protect confidential information at rest, in motion, and while processing on mobile device. Most commonly, separating corporate information from personal information on the mobile device can leverage such protection. MCM system can restrict information to certain containers to safeguard this information from unauthorized actions. In addition, MCM solution can remotely wipe certain information or containers from the mobile device when deemed necessary. MCM system is also capable of providing a multi-channel content delivery, content access controlling, and location based content delivery. MDM primary features are as following [115]:

- Control access to information according to defined policies and rights.
- File level Authentication and content integration

- Secure content storage on-premises using containerisation or wrapping approach, or on cloud (public, private, or hybrid) according to organizational requirements.
- Provide Encrypted containers to secure information
- Remote wiping and locking of information or containers
- Event reporting and real-time monitoring of information, allow IT to monitor utility rate of information, Information expiration, and any action done on information while analyzing users behaviours.

A.4 Enterprise Mobile Management (EMM)

Enterprise mobile management is an approach to manage and monitor mobile devices by handling the security and access to information. EMM solutions expand the security and management capabilities to application and information level. EMM features are best integrated from MDM, MAM, MIM, and MCM functionalities. Mobile Application Management (MAM) manages devices from application level, by providing capabilities such as application wrapping, and managing applications access to information, configuring. Mobile Identity Management (MIM) provide management of identities by providing functions such as role-based access-control to manage access to information according to roles and other defined attributes. Mobile Content Management (MCM) provides management and control at a content level, which may include copy and paste restriction.

EMM solution usually provides appropriate Software Development Kits (SDKs) that can be used to integrate security libraries directly into applications source code before compilation to provide additional functionalities. Such capability is essential to provide a containerization solution to safeguard applications and its related information on the mobile device [116]. Several EMM vendors support containerization approach at the device operating system level.

The EMM solution highlights the potential for multilayer approach implemented in a centralized management solution. According to Gartner Report “Magic Quadrant for Enterprise Mobility Management Suites”, Gartner requires the inclusion of MDM, MAM, and at least one of MCM or IAM to consider the solution as an EMM suite. The most advanced suites may include all these technologies [42]. The aim of EMM is to provide the security capabilities including manage devices (e.g. remote wipe), manage applications (e.g. blacklist app), authentication controls, and manage content

However, choosing a solution that meets the security needs for an organization is critical. The organization should identify their mobility objectives, accordingly identify the requirements for a mobility management solution, and then select technologies and providers. Gartner recommend that each organization should collaborate with the vendor to agree on the mobility objectives, security requirements, and mobility management functionalities required to achieve such goals before implementing any mobility management architecture [117]. This document identified the public safety or governmental organization’s needs, by highlighting security requirements for each level including device, application and information to provide a comprehensive mobility management solution that address such requirements. Although the EMM centralized a lot of security functions integrated into one solution, Public safety environment may require more comprehensive considerations. As such, the EMM solution may meet a set of security requirements for public safety, while other security technologies, standards, and protocols need to be adopted to ensure the highest level of security, and ensure all the security gaps are taken in

consider. For example, organization should consider access control and authentication requirements to manage access to network and infrastructure. In addition, access right management and policies enforcement should also be taken in consider.

A.5 Requirements for an Extreme Enterprise Mobility Management (EMM) for regulated organizations

As mentioned earlier, regulated or governmental organizations require more comprehensive mobility management solutions that can address the security and compliance requirements for such environments. Governmental organizations require a centralized EMM with a group of security functions integrated into one solution. In addition, an extra security considerations, technologies, standards, and policies should be taken in consider. As such, the EMM suit may be implemented to meet as much of the government organization security requirements, while other security technologies, standards, and protocols need to be adopted and integrated to ensure the highest level of security, and ensure all the security gaps are taken in considered.

Governmental sectors and public safety organizations are more likely to be dealing with sensitive and classified information as discussed in section 8.3. Such information will be used to enhance situation awareness and operational decision making. Access to accurate, timely and reliable information is essential to maintain national security. Accessing and sharing of classified information require extreme mobility management functionalities and security technologies. This appendix discusses the extreme mobility management functionalities that must exist in an EMM suite to be qualified to be implemented and used in government sectors.

A. Extreme Mobile Device Management:

For organizations in regulated sectors, device level controls, rules, and policies are required to ensure that mobile devices accessing the infrastructure requesting information and services can be trusted and managed in a secure manner. Since users in regulated organizations may use organization owned devices or BYOD, the organization need a way to identify the mobile device, authenticate users and devices, and ensure only authorized devices and users are accessing the network and infrastructure, and using applications and information as per access rights. In addition, organizations need to ensure that once information moved from infrastructure to the mobile devices, the same level of protection is applied to information during storing, sharing, and processing on the mobile device. In summary, regulated organizations require at a minimum the following device level controls:

(1) Authentication Controls:

A mobile device without a strong authentication may put the organization information stored on the mobile device at the risk of compromise and unauthorized access. A strong authentication should be the minimum requirements for user want to access a mobile device including its application and information, and to connect to network and request access to infrastructure as a way to access information and services. Accordingly, two types of authentication are required, which are local authentication and remote authentication. Local authentication and remote authentication are discussed in details in section 9.3. Local authentication requires a user to authenticate to the device before granted access to the device and its resources. According to NIST SP 800-63-2, local authentication may consider *something you know (e.g.* PINs, passwords, and gestures)*, something you have (e.g.* Physical tokens), and *something you are (e.g.* Biometric

tokens) categories of authentication, and may also consider combining different forms of authentication [14].

Remote authentication requires the user and the device to be authenticated to the network and infrastructure. In order to authenticate the user and the device, a reliable, secure, and interoperable authentication and identity management framework need to be deployed to authenticate user-device access to the network-infrastructure. Section 9.3 discussed the efforts over the years to deploy a reliable, secure, interoperable authentication and identity management framework.

In addition, organizations should consider appropriate policy controls that aim to support the authentication process. Such policies may include locking the device out after a specific number of failed login attempts, wiping the whole device or segregated part of the device (e.g. container) as a result of multiple login failures, and enforcing other authentication requirements.

(2) Encryption technologies:

To provide high level of security and protection for information stored on the mobile device, encryptions technologies must be taken in consider. Encryption would ensure that organizational information is protected even if the device is compromised, lost, or stolen. Mobile device's operating system offer a native encryption support, and additional policies can be enforced to ensure that encryption is enabled.

However, in regulated environments, organizations require more sophisticated encryption technologies that can provide highest level of protection and ensuring confidentiality and integrity of information. Regulated organizations should consider authentication technologies that can be used to encrypt specific information on the device, not the whole device. Such approaches should be supported by a technology that can separate organizational information from personal information on the mobile device (e.g. containerization). In addition to Encryption technologies, organizations shall also consider establishing encryption policies, cryptographic controls, and standards (e.g. federal information processing standards, FIPS Publication 199) for encryption and integrity protection algorithms [94], cryptographic algorithms, key lengths, key generation, key storage, and key management [100] [98] [103]. Section 8.7 provides further details for encryption requirements on mobile devices used in regulated organizations.

(3) Containerization

In order to protect information stored on the mobile device, organizations should consider separating their applications and information from personal applications and information on mobile device. Containerization approach ensures applications are separated into containers (software–defined zones) to mitigate the risk of compromise. Containerizations also provide the administration a full control over applications and information in the containers without affecting the user personal information. In addition, containerization provides an easier way to encrypt organizational information stored in containers instead of encrypting all information on the device. Furthermore, containerizations enable administration to wipe organizational information stored in containers when deemed necessary, while user personal information would not be affected. Several vendors of Mobile Device Management (MDM) products support containerization approach at the device operating system level, as described in A.6.

(4) Device Wiping

Lost, stolen, and compromised devices put the organizational information at risk. Regulated organizations should have the capability of remote wiping devices that access or store organizational information. In general, remote wipe ensures that in case of compromise, all applications and information on the device are permanently removed and the device returned to its original factory setting. However, there are other cases that organization may need to wipe their information only, while keeping the user's personal information. Separating organizational information from personal information using approaches such as containerization provides a way to wipe only specific information or container. Most Mobile Device Management (MDM) tools support containerization capability.

(5) Remote Locate and Remote Lock

Regulated organizations should have a way to remotely lock and locate lost or stolen devices. Many smart devices already have features that enable them to be tracked or locked completely in case of lost or stolen. Administration should enforce users to enable such features, and take the appropriate actions to quickly lock, wipe, and track as soon as possible.

(6) Application Whitelisting and Blacklisting

Application whitelisting and blacklisting restrict the applications on the mobile devices that could access the organizational information. Whitelisting approach set a list of applications that are only approved to be used on the mobile device, where users are only allowed to download such application. This way, organizations can ensure that only properly vetted applications can be downloaded and used on mobile devices. Blacklisting is less restrictive than whitelisting since it allows users to download any application of their choice as long as avoiding known bad applications (blacklisted applications). However, blacklisting require the administration to update it regularly to include all latest malicious applications, thus, it is not an effective way to mitigate all security threats and risks.

Regulated organizations should consider whitelisting approach, where users are allowed to use only specific properly vetted application. Applications should go through a rigorous application to ensure they satisfy a high level of reliability, security, and policy compliance. Testing process should test application among software vulnerabilities, security risks, and compliance with the organization security requirements. NIST, ITSG, and OWASP provided recommendations and guidelines in terms of mobile application testing that can assist organizations in the SA&A process [23][25][56][90]. Section 7.5 provides further details regarding the application vetting process.

Whitelisting could be implemented using private application store, where organizations can distribute their applications to users from their private trusted source. Users are not allowed to download applications through means other than the private application store. In addition, the application store should also consider a vetting process, applications should satisfy high level of security that can be accordingly somehow rated in order to enable organisations to allow or deny their members to install applications from the store.

Furthermore, whitelisting of applications should be managed by device and user assigned policies. For example, some applications may be restricted to be used only on organization issued devices, and prohibited from BYOD. User roles, agency, and other qualifying attributes may also be used to support the decision of application whitelisting for different users. However, such

functionalities should be supported by a well-defined access control policies, and strong policy enforcement mechanisms.

(7) Over-the-Air Management and Configuration

The most critical requirement for mobile device management is the ability to manage and configure the device over the air from a central system (e.g. console windows) by administrators. Most of the requirements listed above require over-the-air management capability in order to be applied. Over-the-air management allow administrators to manage devices by wipe/lock device, monitor mobile device, push applications or updates, manage device configuration, manage policy settings, and on ensure device integrity of both organization issued devices and BYOD. Hence, over-the-air capability should be a fundamental component of any enterprise mobility management (EMM) solution.

(8) Additional Controls:

Each regulated organization may require its own additional controls to protect and manage the use of the mobile device according to their environment requirements. For example, some MDM tools allow administrators to restrict the camera usage, screenshots, and copy/paste to clipboard. Other controls may restrict storing information on removable media (e.g. SD cards). In addition, some functionality may be granted or restricted according to user role, location, situation, device, or other defined qualifying attributes. For example, camera may be restricted according to the location; storage of information may follow the metadata attached to information, etc.

B. Extreme Mobile Application and Content Management:

For organizations in regulated sectors, application level controls, rules, and policies are required to have control over mobile applications deployment and management. Mobile Applications management (MAM) tools are required to manage application life cycle from development to distribution and application usage on the mobile device. MAM tools give the administrators the ability to securely provision, push, update, monitor applications and applications usage and access rights on organizational issued devices and BYOD. Mobile Application Management (MAM) tools should be focussed on application distribution, management, and usage according to qualifying factors including: device type (organizational issued or BYOD), device platform, operating system, user role, and other access rights mapped from the organization's attributes and access rights respiratory. This way, MAM can restrict applications and services to specific devices and users based on access rights and applied policies. MAM tools provide a way to control mobile applications without needing to control the whole device. Since users in regulated organizations may use mobile applications to access information in infrastructure or information stored on the mobile device, the organization need a way to ensure that information access and handling is following the rules and policies attached to information. Thus, MAM should give a way to administrators to have insight on such process to ensure applications are handling and accessing information according to access rights and that policies enforcement process is being done properly. In summary, regulated organizations should support an MAM that support at a minimum the following application level controls and capabilities:

(1) Usage Policies:

Mobile Application Management (MAM) should has a clear defined policies for usage rights, and access qualifying attributes including device, role, agency/sector, location, date/time, scenario/context, and other qualifying attributes as deemed necessary by each organization. Some

mobility management solutions handle the policies management component as a part of the application management strategy, while other approaches address it as a part of the device management strategy. However, regulated organizations require much more fine-grained rules and policies that can be extended into the mobile framework in real time. Such rules and policies should be able to control access to infrastructure as well as access to information stored on the mobile device. Access Right Management (ARM) solution can provide such capabilities. Access control and policies enforcement capabilities requirements for enterprise mobility management (EMM) solutions in regulated sectors are described A.5 C.

(2) Private Application Store

Regulated organizations should support a private application store that provide a secure way to distribute the vetted approved organization-developed applications and other third-party applications to their users from a unified trusted source. Applications can be pushed to user's devices by administrators and could also be downloaded according to user's requests on as-needed basis according to user's roles and duties. In addition, applications downloading should be controlled based on access privileges and qualifying attributes imposed by the organization. For example, some users may be able to download an application while others are prohibited based on their role. Thus, the private application store would limit the user's options based on their needs, policies and permissions.

Furthermore, the applications pushing process should be controlled based on the situation or context. For example, an application or its update can't be pushed to user's device in the middle of serious situation. Thus, real time monitoring for mobile devices and mobile applications can support location-based and context-aware applications and can also support the push and update process of mobile applications.

In addition, the private application store should support a well-defined vetting process, to ensure that all applications uploaded to the application store are in compliance with the organization requirements. NIST and ITSG 33 provides guidelines and recommendations for regulated sectors in terms of mobile applications testing and continuous monitoring to provide software assurance of mobile applications [23][56].

(3) Secure Middleware or Cloud:

In some organization, employee may require to share and collaborate with information which they may rely on a consumer services such as "Dropbox". However, using the public sync and sharing services posed the organization's information to risks of exposure. Regulated organizations should prohibit the use of such public services and exchange it with alternative for storing, accessing, and sharing of organizational contents securely. In addition, regulated organization should ensure that only users with proper permissions could access such contents, which is a capability that is not supported by public sync and sharing services.

Regulated organizations should implement a secure private middleware or cloud that allow users to push contents to secure flexible central location that can integrate and redistribute collected information with a proper access control permissions. As such, mobile applications, users, or mobile device resources (e.g. sensors) can create, collect, store, process, and transmit such information more effectively and securely. Such information must be protected and managed by the middleware or cloud in such a way that require users or other applications to be authenticated before authorized access to such information. 3GPP defined the SCEF network element to provide such a function as described in 3GPP TR 23.708, and TS 23.682 [73][74]. The

middleware or the cloud can use the LTE Service Capability Extension Function (SCEF) in order to manage transfer, process, store, and share information in a secure way. Information may be organized according to standard data model and then be shared with applications or users as requested, taking in consider their access privileges. Such organization can combine and integrate different information to create complex outputs that can also support the context-aware applications.

(4) Monitoring Console:

Administrators require a monitoring console in order to manage and monitor mobile applications running on the mobile devices. Monitoring console gives the administrator a centralized view over applications and ability to manage usage by device and users. Monitoring Console allows the following services:

- Unified view over all enrolled devices on the network.
- Managing user privileges
- Apply specific device policies including lock and wipe capabilities
- Enforce security policies
- Pushing applications and updates
- Monitor and troubleshoot applications performance issues
- Set priorities for network usage and access to infrastructure. Optimizing the network usage and access to infrastructure should be based on user, application, context, and other attributes.
- Enable view over unauthorized actions (e.g. access to restricted application or information), and provide a way to monitor and audit such actions.

(5) Auditing and Reporting:

Regulated organizations require an EMM solution that can be configured to collect and store detailed information about the devices, applications, and user's actions. The EMM solution may rely on the device operating system, where a time and a date stamp could be captured for each single event including: application usage, information access, web browsing, text and messaging, disabling of security, jailbreaking or rooting of devices, downloads, copy/paste, and external sharing of information. In addition, the network used and the location of the device based on GPS and cell-site coordinates could be used to track the device, and report the exact location, time and action. It is also important to provide a way to digitally sign information created by mobile devices, applications, or user, as well as the audit logs collected from the mobile devices. Digital signatures could provide certifications that may require a stamp to prevent alteration of information or audit logs.

Auditing, logging and reporting is useful in different situations that require data analysis including: investigations that require evidence, troubleshooting device problems, disasters recovery scenarios, risk management, and compliance monitoring. In addition, regulated organizations may require the use of audit logs collected as evidence in courts. Thus, audit logs must be protected in such a way that prevents any damage or alteration to ensure its integrity and court admissibility.

C. Extreme Access Control and Policy Enforcement

Access control and policy enforcement within regulated organizations should comply with strict rules, policies, and organizations security standards. Mobile devices mobility nature places them at higher risks than desktop devices. In addition, access to wide range of network services including Bluetooth, Wifi, 4G/LTE, and location services raise additional security threats [38]. Further, in regulated sectors, users would require access to sensitive information and services that require more granular access controls. Hence, traditional security controls and policy enforcement mechanisms are not enough. Yet, all security controls already exist and applied to desktop applications need to be applied to mobile applications as well as additional security controls to address such challenges. Mobile applications in regulated sectors require extreme access control and policies enforcement mechanisms in order to mitigate concerns due to mobile device nature and to be able to trust devices enough to authorize them access to organization infrastructure.

In traditional mechanisms, authentication and access control depend on identity, device status, and user profile information. However, such information is not enough to enable security policies in regulated sectors that require strict access control. For effective access control and policy enforcement approaches, organizations need some qualifying attributes to be challenged during access control decision as well as context awareness. In other words, access control and policy enforcement decisions have to be based on the physical attributes including the device, location, date/time, user's role, agency, as well as the context or situation the mobile device and user is involved in. This requires information on device type either organization issued or BYOD, device platform, and operating system health. In addition, the type of application and information being accessed, security policies and access privileges attached to information are also major factors in access control and policies enforcement decisions. Such information and qualifying attributes shall be mapped and integrated together forming more complex access privileges that support real-time incidence services, situational awareness, access right management, dynamic priorities, etc. [109] Thus, the enterprise mobility management (EMM) solution should provide the organization with the ability to analyze collected information, forming complex access rights, ensuring users compliance, and supporting policies enforcement decisions.

The best way to provide such extreme access control and mobility management is to provide greater visibility into mobile devices accessing the infrastructure and aggressive dynamic control to identify and challenge devices to ensure devices and users get right access to information and services. The aim is to ensure that mobile devices comply with the security policies before granting them access to the network and infrastructure. This can be done by integrating the enterprise mobility management (EMM) solution with an identity and authentication framework that serve as a crucial bridge between mobile devices and infrastructure by managing the authentication process to provide secure access to network and infrastructure [118]. The identity and authentication framework may follow the precedents efforts and guidelines discussed in section 9.3. The identity and authentication framework aims to authenticate devices and users, and take an authentication decision to whether grant access or not [14]. In addition, the enterprise mobility management (EMM) solution requires integration with an Access Right Management (ARM) mechanism that aim to supplement the authentication process and manage access to information and services according to access privileges. As such, organizations may use such integration to gain insight into the posture of mobile devices, authenticate mobile devices and users, and enforce appropriate security policies and access rights. The requirements for extreme access control and policies enforcement mechanism can be addressed by integration of EMM, identity and authentication management, and ARM is illustrated in Figure 34.

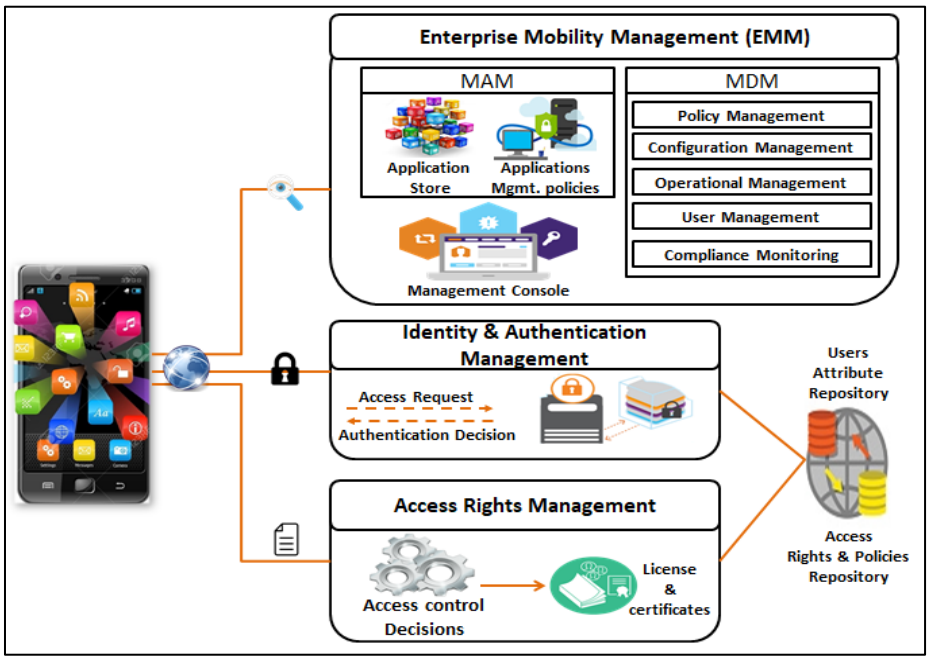

Figure 34 Extreme Access Control and Policies Enforcement

The integration described in Figure 34 manages the authentication, authorization, and access control process as following [118]:

(1) The EMM platform monitors and collects information about the mobile devices which include: mobile device status, compliance status, OS health, etc.

(2) The identity and authentication management framework receive an Access-Request. Accordingly, it queries the status information collected by the EMM platform. Then it validates the identities, and qualifying attributes using the appropriate authentication techniques and protocols, and generates an authentication decision.

(3) The Access Right Management delivers the authentication status and decision. Once the User and device are successfully authenticated (Access-Approve), an authentication decision is sent to the Access Right Management (ARM) to manage access to information and services. The ARM collects information about the qualifying attributes and contextual information including the following:

- User: identity, role, agency, IP address, authentication status, and location.
- Device: Type (organizational issued or BYOD), platform, OS, OS version, network connection method, and location.
- Context: situation the user and device are involved in.

(4) The Access Right Management (ARM) framework accordingly map the collected information in order to verifies the access rights based on the rules, policies, and access privileges defined by the organizations. ARM creates a license file that contains the rules, policies, and

organizational requirements that should be applied to information according to the User access Rights. Such license encapsulated with the information to manage information handling process on the mobile device asset.

In addition to policies enforcement at the information level, regulated organizations require also automating and centralized policy enforcement at the application and device level to maintain an overall awareness and control over the mobile device environment. This requires a policy enforcement component that can automatically enforce strict policies and security controls on the device and application level. Policy enforcement component can be used to reset, lock, or wipe device or information in case of mobile device compromise. As such, the enterprise mobility management (EMM) solution should have a policy enforcement component that can provide such strict policies and regulations.

A.6 Enterprise Mobility Management (EMM) Suites from different vendors

(1) AirWatch

AirWatch started with Mobile Device Management (MDM), and then expanded to support applications and contents [119]. AirWatch supports a comprehensive enterprise mobility management (EMM) suite that helps companies manage mobile devices, applications, content, email, browsers, and network [119]. AirWatch provides the following capabilities [120]:

- AirWatch provide flexible platform choices, it supports all major mobile platforms including Android, iOS, Blackberry, Symbian, and Windows.
- AirWatch solution includes also an automated device vetting and enrolment process.
- AirWatch authenticate users, and then grant profiles, applications, and contents based on the user, his device, and device ownership (company owned, and BYOD)
- AirWatch solution offers on premise or a cloud service, where organizations can switch between the two solutions according to their needs changes.
- AirWatch provides AD/LDAP[8] integration.
- AirWatch uses policy-based security, whitelists, and blacklists.
- AirWatch provides information security using strong encryption, remote wipe, and a secure container known as “AirWatch Content Locker”.

(2) Citrix

Citrix provides virtualization technologies, SaaS solutions, cloud computing, and mobility management solutions to organizations. Citrix has enterprise mobility management solution “XenMobile” that delivers device and application management services. Citrix XenMobile is a

[8] AD/LDAP: AD (Active Directory) is a database based system or directory service that provides directory, management and storage of information, security policies, policies enforcement, authentication, authorization, Certificate Services, Federated Services, Rights Management Services, and other services in a Windows environment. LDAP is a protocol that communicates with AD for querying and modifying items in directory service [133].

comprehensive Enterprise Mobility Management (EMM) solution that delivers Mobile Device Management (MDM), Mobile Application Management (MAM), and distributes applications to mobile devices [121]. Citrix XenMobile provides the following capabilities [120]:

- XenMobile is EMM solution that secures devices, applications, and information.
- XenMobile Distributes applications to various platforms and devices
- XenMobile bypass the need for layered, multi-vendor solutions to mobile management.
- XenMobile Provide security services including ShareFile sync, share content management, and secure application distribution.
- ShareFile product provides secure cloud storage, and secure connections between users and your information.
- ShareFile provide information security using encryption, remote wipe, and information expiration capabilities.
- ShareFile also monitors, audits, and reports all user activities.

(3) Good Technology

Good Technology specializes in mobility security solutions for general business, financial institutions, and government organizations. Good Technology provides EMM solution that integrates Mobile Device Management (MDM), Mobile Application Management (MAM), Mobile Content Management (MCM), and a customizable enterprise application store. Good's focus is on securing apps, data, and mobile devices. Good Technology's EMM solution offers an on-premise and a cloud-hosted solution. Good Technology solution provides the following capabilities [120]:

- Good Technology solution protects corporate information as well as the device, applications, and the information residing the device.
- Good Technology invented mobile application containerization. Containerization encrypts the application sandbox and logically separates personal information from corporate information.
- Good Technology secures the corporate applications by containerizing applications, although applications are separated, Good Technology provides a capability that allows sharing information between containerized applications securely if needed.
- Good Technology provides the following security services [120]:
    - App-level encryption
    - Application authentication
    - Application authorization
    - Single sign-on
    - Strong password enforcement
    - Remote lock/wipe
    - Data loss prevention (integrity)
    - Secure access to corporate information and services behind firewalls

Good Technology seems to be an ideal mobility management solution, however, it has several limitations including the lacks of usage policies, policies enforcement, user access rights, and

role/attributes based access control. Such capabilities are essential for mobility management in governmental organizations.

(4) IBM

IBM provides "MobileFirst", a comprehensive mobility management solution for enterprises that provide a security-rich Mobile Device Management solution for IOS, Android, Blackberry, and windows mobile devices [122]. IBM's MobileFirst provide the following capabilities [120]:

- MobileFirst provide a secure cloud-based mobility management solution for devices, applications, and Information.
- MobileFirst provide extreme security services and granular policies for enrolled devices.
- MobileFirst provide a sort of privacy settings, secure document sharing, certificate management, and email access controls
- MobileFirst provide AD/LDAP[9] integration.

(5) MobileIron

MobileIron provides an enterprise mobility management (EMM) solution since 2007. MobileIron's EMM management suite is composed of MDM, MAM, and MCM products and services that help organizations secure devices, applications, and information regardless of the mobile device platform or type [123]. MobileIron's EMM solution provides the following capabilities [120]:

- MobileIron's EMM is available as a cloud-based or on premise solution
- MobileIron provide flexible support to all major devices, but focuses most on iOS, Android, and Windows.
- MobileIron provide group of services that are mapped to organizational need including security and policy management.
- MobileIron provides an automated configuration client, and an intelligent security gateway.
- MobileIron's MAM provides an enterprise application store that secures applications and distribute them to users from trusted source.
- MobileIron's secures applications on mobile devices by containerizes and separated them and their related information from personal applications and information
- MobileIron's MCM solution provides an email attachment security application known as, Docs@Work.

[9] AD/LDAP: AD (Active Directory) is a database based system or directory service that provides directory, management and storage of information, security policies, policies enforcement, authentication, authorization, Certificate Services, Federated Services, Rights Management Services, and other services in a Windows environment. LDAP is a protocol that communicates with AD for querying and modifying items in directory service [133].

- MobileIron's supports a securely browsing environment (known as, Web@Work) that allows users to securely browse and access the organization intranet resources without the need of device-wide VPN.
- MobileIron's supports additional security services including data encryption, enforcing passwords, and strong authentication.
- MobileIron's derives security wrapper that includes per-App VPN, App-level data loss prevention, and a secure Application ecosystem through "AppConnect" and "AppTunnel".

(6) SAP

SAP also provides an enterprise mobility management solution that aims to provide a secure environment for both applications and information. SAP's EMM solution "Afaria" provide security for devices, applications and information on mobile devices. SAP "Afaria" support the following capabilities [120]:

- SAP "Afaria" provides flexible support for iOS, Android, Windows phone, Blackberry, Windows desktop and server operating systems.
- SAP "Afaria" provide AD/LDAP integration for user authentication
- SAP "Afaria" provide the users with a selectable list of SAP or third-party applications to install. Such list in the only way to get the organization applications
- SAP "Afaria" manage and secure applications once it installed on the mobile devices including: update, remove, install new features, monitor of applications
- SAP "Afaria" provides security services that include[120]:
    - Strong user authentications using directory authenticated username, password, and enrolment code. Users need to be authenticated before granted access to listed applications within the Afaria application on the mobile device.
    - Containerization by separating personal information from encrypted organizational information
    - Afaria is the only gateway to access the organizational resources

(7) Sophos

Sophos began as a security company that produced security products including anti-virus and encryption products. Nowadays, Sophos provides products that secure every end point of a network including laptops, virtual desktops, servers, email, web browsing, and mobile devices. Sophos also provide mobile management solution (known as, Mobile Control) which is flexible to manage and control iOS, Android, Windows, and other device types. Sophos Mobile Control provides security services including [120]:

- Device loss and theft protection
- Device policies configurations, building group-based compliance policies, and ability to deploy such policies over-the-air
- Enforcement of built-in security features including passwords and device encryption

- Sophos MAM also provide email management, and integrated anti-virus and web protection for Android devices
- Sophos also provide a "Mobile Security application" [10] that scans all newly installed applications for malware infections, infected devices are reported, revoked, and/or wiped. Applications may also be scanned in real time.
- Sophos supports encryption products for both Android and iOS devices
- Sophos provide protected cloud security to encrypt and secure information. The cloud is integrated with tools such as Dropbox, iTunes, and SD cards.

(8) SOTI

SOTI provides major mobile security products including enterprise mobility management (EMM) solutions. SOTI's EMM solution "MobiControl" is an award winning solution that supports organizations with security capabilities to securely manage mobile devices, applications, information, and email. SOTI's EMM solution provides the following capabilities [120]:

- SOTI's MobiControl provide flexible support to iOS, Android, Windows Phone and PCs, and Mac OS.
- SOTI's MobiControl provide integration with AD/LDAP, Office 365, and Microsoft Exchange Server.
- SOTI's provide a MobiControl's Android+ Technology, which is integrated with more than 36 Android OEM partners that extends a secure mobile management to a wide range of Android devices.
- MobiControl provide security services including anti-virus and anti-malware software, and blocking application that weren't specifically requested from Google Play Store to protect users and devices from malicious or infected applications.

(9) Tangoe

Tangoe is a global provider of Lifecycle Management software and security services products for enterprises and service providers. Tangoe provides an enterprise mobility management (EMM) solution "MatrixMobile" that support MDM, and other mobility services. Tangoe's MDM solution provides flexible support for iOS, Android, Blackberry, and Windows Phone. MatrixMobile MDM is a comprehensive mobile management and monitoring suite for mobile devices in the enterprise. MatrixMobile's support the following features:

- Single console management
- Secure access management of enterprise resources
- Role-based policies
- Applications distribution over-the-air software

[10] Mobile Security app is a free scan application that is available for all Android users with no ads.

- Containers to separate organization and personal information on the mobile device, encryption of information, prevent information leakage and unauthorized access, and remotely wipe information.
- MatrixMobile's can focus user on using single portal, enforce VPN and wifi rules.

MatrixMobile's also support unique services including: "mobile device logistics, telecom expense management, real-time expense management, and mobile advisory services" [124].

(10) Symantec

Symantec is one of the first software companies to provide security solutions to personal computer at the 1980s. Symantec provides security products including anti-virus, encryption, and secure backup solutions for individuals, small businesses, and large enterprises. Symantec provide mobility management solution that integrates MDM, MAM, and mobile threat protection into single unified console solution [120]. Symantec's solution provide flexible suite that supports Android, iOS, and Windows phone, either organizational owned devices or BYOD. Symantec Mobility key features and security services are derived from three products [124]:

A. Symantec Mobile Management:

Symantec Mobile Management is Mobile Device Management (MDM) Solution that provides the following services [124]:

- Enterprise User Activation
- Configuration Management
- Policy Management
- Compliance Enforcement
- Asset Management
- Application Distribution
- Information access management
- Selective Wipe
- Secure Email

B. Symantec App Center:

Symantec App Center is a Mobile Application Management (MAM) solution that provides distribution, protection, and management for mobile applications and information on iOS and android devices. Symantec App Center provides the following capabilities [124]:

- Enterprise applications distribution
- Application security policies
- Enterprise information Distribution
- Information security policies
- Selective Wipe of applications and its related information

C. Symantec Mobile Security:

Symantec Mobile Security is a threat protection product that provides antivirus technologies, firewall and other security services for mobile devices, including [124]:

- Antimalware
- Web Protection and safe browsing
- Anti-theft
- Enterprise security Policies Management
- Applications whitelisting and blacklisting
- Visibility, monitoring & Compliance

(11) Blackberry

Blackberry provides a unified complete Enterprise Mobility Management (EMM) solution that provide a flexible support for iOS, Android, Window 10, and mac OS. Blackberry EMM solution provides a range products for device management, application management, information management, and identity and access management.

In 2016, blackberry integrated with Good Technology, which now called "BlackBerry Unified Endpoint Manager (UEM)". UEM expand the existing capabilities of management of mobile devices, PCs, Macs, and Internet of Things (IoT) devices. The successful integration gained BlackBerry immediate credibility as a multiplatform mobility management tool in 2016. As per Gartner, the combination of security capabilities of BlackBerry, WatchDox and GoodTechnology make BlackBerry a very strong effective choice for regulated organizations that require comprehensive security requirements (e.g. governmental organizations). BlackBerry EMM provides general purpose SDK for securing organizations internally developed applications and third party applications.

BlackBerry EMM delivers security capabilities that support enterprises security and business needs, by providing a comprehensive EMM solution by relying on Mobile Device Management (MDM), Mobile Application management (MAM), in addition to the following solutions:

A. Mobile Content Management (MCM):

BlackBerry EMM tools use MCM solution to protect and manage access to information on the mobile device. MCM tools provide a secure access to organization resources, manages the access rules for information on the mobile device, and ensure access rights are enforced on the mobile device. The MCM tools offer also additional features including advanced policies management. MCM tools can enforce policies to information including encryption keys, authentication, and rules for restricting actions (e.g. copy/paste, Time-To-Live), and provide conditional access to information. In addition, beyond the basic access policies, MCM tools are compatible with third-party rights management systems, and Access Right Management (ARM) infrastructures [125].

B. Identity and Access Management (IAM):

BlackBerry identity and Access Management is a unified approach to facilitate and manage access to information and services by offering authentication policies and access controls, integration with active directory, PKI, and supporting assertions using protocols such as Kerberos and SAML. In addition, BlackBerry identity and Access Management provide secure application access using token-based two-factor authentication [125].

EMM tools ensure that only trusted devices and users can access enterprise applications using identity and access management (IAM) functions including: user and device certificates, authentication and single sign-on (SSO). In addition, IAM functions may rely on contextual information (such as location and time) to evaluate access decisions and assist policies enforcement.

C. Mobile Security and Containerization

BlackBerry mobile security and containerization is an end-to-end approach that aims to protect information by safeguarding the three Cs of mobile security, which are: content, credentials, and configuration [125].

BlackBerry Enterprise Mobility Management (EMM) Suite offer five different editions that meet the enterprises mobility needs by supporting variety of advanced capabilities. BlackBerry Whitepaper "The CIO's Guide to UEM" provides further information for BlackBerry EMM and the five editions capabilities [125][116]. The BlackBerry EMM suites editions are as following [116]:

- BlackBerry Enterprise Mobility Management (EMM) Suite – Management Edition
- BlackBerry Enterprise Mobility Management (EMM) Suite – Enterprise Edition
- BlackBerry Enterprise Mobility Management (EMM) Suite – Collaboration Edition
- BlackBerry Enterprise Mobility Management (EMM) Suite – Application Edition
- BlackBerry Enterprise Mobility Management (EMM) Suite – Content Edition

In general, BlackBerry Enterprise Mobility Management (EMM) Suite supports the following unique functionalities:

- BlackBerry EMM suite provide containerization and security policies across operating systems in order to separate corporate information from personal information, safeguard information using encrypted containers, and manage access to information by enforcing security policies.
- BlackBerry EMM suite Provides tools, APIs, and software development kits (SDKs) for applications development to ensure consistent security across devices and operating systems.
- BlackBerry EMM suite can manage actions over information by embedding Access Rights Management (ARM) protection to information to stay secure and manageable all the time during access, sharing, storing, and processing on the mobile device.

BlackBerry EMM suite is commonly used by organizations that require high level of security requirements and regulatory compliance. According to BlackBerry whitepaper "The CIO's Guide to UEM" [116], BlackBerry EEM suite currently supports:

- 16 of the G20 governments
- 10 of the largest law firms
- 5 of the largest oil and gas businesses
- Over half of the Fortune 100 (including banks)

BlackBerry report "The Definitive Guide to Enterprise Mobile Security" provide a group of case studies where enterprises, organizations, and regulated sectors relied on BlackBerry EMM suites to enable mobility within their organizations, and provide a secure remote access to information and resources to users and devices, while applying the organization security policies and regulatory compliance [40].

(12) Other vendors

There are other diverse vendor approaches for enterprise mobility management (EMM) that focus on identity and access management, and content security. However, according to Gartner Report "Magic Quadrant for Enterprise Mobility Management Suites", the approach must utilize MDM, MAM, and at least one of MCM or IAM functionalities to consider it as an EMM suite [42].

According to Gartner qualitative analysis of market research report in 2016, current EMM vendors were divided into a magic quadrant of leaders, visionaries, challengers and niche players for mobility management market. Gartner report highlighted the vendors that lead the Enterprise Mobility Management technology, namely, BlackBerry, IBM, MobileIron, and VMware. Other visionary vendors include: Ivanti, SOTI, SOPHOS, CITRIX, Airwatch, and Microsoft [42]. Table 7 provides a summary of vendors supporting EMM, and the different key features of their Enterprise Mobility Management (EMM) suites.

Table 7 Comparison of Enterprise Mobility Management Suites from different Vendors [119] [121][122][123][125][116][42][126].

	Airwatch	**Black Berry**	**MobileIron**	**Citrix**	**IBM**	**Microsoft**
Deployment	Cloud/On premises	Cloud/On premises	Cloud/On premises	Cloud/On premises	Cloud/On premises	Cloud/On premises
Compatibility	Multiplatform (All versions)	Multiplatform (limited versions)	Multiplatform (limited versions)	Multiplatform (limited versions especially for Mac OS)	Multiplatform (including all versions)	Multiplatform (limited versions)
Password protection	Yes	Yes	Yes	Yes	Yes	Yes
Single Sign-on	Yes	Yes	Yes	Yes	Yes	Yes
Remote wipe	Yes	Yes	Yes	Yes	Yes	Yes
Remote lock	Yes	Yes	Yes	Yes	Yes	Yes
Jailbreak detection	Yes	Yes	Yes	Yes	Yes	Yes
Policy Configuration	Yes	Yes	Yes	Yes	Yes	Yes
Network Configuration	Yes	Yes	Yes	Yes	Yes	Yes (Via system center configuration manager)
VPN/Proxy Gateway	Yes	Yes	Yes	Yes	Yes	Yes
Device encryption	Yes	Yes	Yes	Yes	Yes	Yes

Email Encryption	Yes	Yes	Yes	Yes	Yes	Yes
Multifactor authentication	Yes	Yes	Yes	Yes	Yes	Yes
Malware detection	Yes	Yes	Yes (with partner integration)	Yes	Yes	Yes
Firewall	No	Yes	Yes (with partner integration)	No	Yes	Yes
Data isolation	Yes	Yes	Yes	Yes	Yes	Yes
OS updates	Yes	No	No	No	Yes	No
Alerts reporting	Yes	Yes	Yes	Yes	Yes	Yes
Web-based console	Yes	Yes	Yes	Yes	Yes	Yes
Maintain Logs	Yes	Yes	Yes	Yes	Yes	Yes
3rd party integration	Yes	Yes	Limited	Yes	Yes	Yes

Annex B Containerization

Containerization provides more fine-grained control by segregating each application and its own information into dedicated encrypted storage area. Containers are authenticated, encrypted storage area on the mobile device that can be used to separate and secure a portion of device's storage from the rest of the device. The goal of containerization is to isolate applications and its related information to prevent malware, intruders, system resources, or any other applications from interacting with the application and any of its information secured by the container without permission. Since generic applications are isolated from corporate applications, they are restricted from accessing corporate information in the corporate application containers. In addition to isolation, containerization allows the Management and Administration to disable certain functions of applications and wipe information within the container remotely without affecting User's personal information, and provide a capability to apply different usage rules and policies to each container. Such capabilities are important features for BYOD scenario. Containerization limits the risk of exposure in case other security measures are compromise.

Containerization is not only encrypting the applications and its information, but also secures the interactions between different applications. This way, containerization provides a trusted end-to-end security approach by safeguarding the three Cs of mobile application security: content (e.g. applications and its information), credentials (e.g. pins, passwords, tokens, and certificates), and configurations (e.g. information on backend systems and resources) [40].

Containerization is different from application wrapping. Application wrapping use a code that is injected into the binaries of mobile device to enable policies to be applied. Policies and restriction are then be set or wrapped around application defining the usage rights such as authentication requirement, information storage and other access requirements. On the other hand, containerization requires SDK that usually offered by the EEM solution, in order to integrate the security libraries directly into the application source code before compilation to enable policies to be applied to applications. Although containerization requires access to the source code and developer to do the coding, SDK's provide more security and business benefits to organizations than wrapping. Several EMM vendors support containerization approach at the device operating system level.

Containerization allows a set of applications to run in their own dedicated encrypted container on the mobile devices. This provides the following functionalities:

- It provides applications and its related information with an extra layer of security, by providing additional protection against malware, intruders, unauthorized access.
- It separates corporate applications and its information from user personal information.
- It enables organizations to remotely wipe their corporate information in case of compromise, lost or stolen without affecting the user personal information.
- It enable security policies to be applied on applications and information including encryption, data storage and sharing, and other set of usage and access rule to be applied to a set of applications and information.

Application wrapping is different from containerization in two ways. First, application wrapping is specific to each application, where each application is wrapped with its own set of rules and policies. Second, it provides a separate management layer to be applied directly to the application

without changing application or doing any coding. This way, application wrapping provides the following objectives:

- It enables specific policies to be applied per application including encryption, data sharing between application, and other security/compliance controls.
- It provides a flexibility of updating and modifying security policies over the time, thus, it enables more granular remote management.
- It provides more applications portability over multiple operating systems (e.g. Apple iOS, Android and Windows Phone).
- It simplifies implementation of single sign-on for applications.
- It also provides a rapid secure reinstallation of applications in case recovery is required.

A mentioned above, containerization and application wrapping can complement each other. Such capabilities achieved by implementing containerization and application wrapping can provide better mobility management and achieve the security and compliance objectives required by organizations to secure their applications and information.

According to BlackBerry whitepaper "The CIO's Guide to UEM" [116], in order to meet the security and regulatory requirements, any containerization solution should at minimum provide the following:

- App-level encryption: Application level encryption provides a safeguard for application and its related information independently from device level encryption, which is essential to protect information in case the device is compromised.
- Application authentication: Application authentication requires app-level password authentication, and may include other forms of authentications such as two-factor authentication.
- Application authorization: Application authorization manages provisioning of applications only to authorized devices and users. In addition, manage access to applications and information on mobile devices only to authorized users.
- Single sign on: Single sign on allow users to log in to one containerized application and gain access to all containerized apps. Although this capability provide more smother user experience, it is not suitable for regulated and governmental organizations that require mobility management to secure their applications and information. In such environment, applications and its related information should be separated, and sharing of information between applications is prohibited
- Security policies and compliance control: Security policies should be applied on applications and its related information to regulate the usage, which include access rights and content management that applied on information when storing, accessing, sharing, and processing of information on the mobile device. Compliance controls allow the IT to remotely manage and monitor applications and information including remote lock/wipe, detect jailbroken/rooted devices, enforce OS version, enforce policies, enforce updates, etc.
- Access Rights Management (ARM): ARM enable applying of information level security policies to protect corporate information at rest, in motion, while processing, and as it

moves across application, mobile devices, systems and clouds. The containerization approach should be supported by ARM solution that has the ability to enforce security policies on applications and information on the mobile device.

Annex C Access Right Management (ARM)

Access Right Management (ARM) is a secure information management at the device and application layer, that provide the guarantees to the Information Providers that their information will kept secured as it were secured on their infrastructure, and the rules and policies set of handling information are extended to the mobile framework. ARM manages access to information and services on PSG-II, as well as access, storing, and sharing of information on the PSG-MD.

The main advantage of the ARM is that security rules and policies are defined by the Information Providers, managed on a central system, and encapsulated and migrates with information in such a way that rules and policies can still be applied even on the PSG-MD even when the server is not accessible or where there is not network connectivity at all.

Access Rights Management (ARM) consists of two major components: ARM-support system (ARM-SS) that is part of the PSG-MAMF support system, and ARM-device system (DRM-DS) that is part of the PSG-MAMF device system. In this annex, ARM-DS components are illustrated.

ARM-DS is responsible for performing information handling and policies enforcement on the mobile device. DRM-DS is responsible for processing the received packaged information, decrypt information, interpret the information, requests the licenses of handling information, and enforce the rules and policies provided in the license encapsulated with the information.

ARM-DS can be implemented as an extension to the operating system in order to has the necessary privileges to access the mobile devices resources (e.g. sensors outputs), and to be able to perform policies enforcement accordingly, as shown in Figure 17 and Figure 18. The ARM-DS components are as following:

A. ARM Manager

ARM Manager is responsible for authentication of license and information, policies and access rights enforcement, information decryption, and provides decrypted information to a trusted application agent [64].

The ARM Manager is also responsible for processing different policies and requirements defined by different Information Providers and prevent one Information Provider's requirement from adversely affecting another's. ARM Manager should be able to solve conflicts between requirements, for example, ARM Manager shall enforce the policy with the strictest requirement, otherwise, enforce a default policy. In addition, if ARM Manager finds a management file that it cannot understand, the access should fail in a secure manner. This way, ARM Manager can prevent unauthorized access, storage, sharing of information until conflicts are resolved or the management file could be interpreted. Furthermore, one way to fool the ARM Manager is to supply older versions of the management files, thus, ARM Manager should be able to recognize the versions of the management files and interpret them in a proper way.

Since ARM Manager is part of the OS it has the necessary privileges to query and access the device state, access the outputs from parts of the device (e.g. sensors events), and accordingly enforce policies. For example, the device sensors can be used in order to enhance the context awareness and their events and outputs will be considered as a part of policies to be enforced, thus, ARM Manager needs to access those sensor's outputs in order to enforce policies.

B. Security Agents:

Security agents are responsible for handling all the security functions required by the ARM functionalities, which include: (1) Memory management and secure storage. (2) Key management. (3) Implement the basic cryptographic operations. Sometime embedded hardware is used to enhance the security of the ARM (e.g. Hardware Root of Trust, RoT), where the security agents work closely with the secure hardware to provide enhanced security features.

(1) Memory Management and Secure Storage

To provide secure ARM functionalities, access to memory and system files must be controlled. There are 3 basics functions required in order to provide memory management and secure storage, which are access control file system, secure memory system, and memory separation system.

Access control file system is important to provide a secure storage for information that is not encrypted. It may be inefficient to always keep applications and its related information in encrypted state. Some applications may require that the information be decrypted, but still stored securely. This way the application and its related information are decrypted and kept securely in files that are only accessed by trusted agents. In addition, the ARM may records of all events and actions may need to be tracked and stored in a secure database for monitoring purposes. Access controlled file system can be used to store a secure database. For example, a policy may state that particular information can be accessed by an application only once. Thus, when the information is accessed by an application the access action should be logged into the database. Thus, when the application requires access to such information again, the database should be verified in case that there is any logged action that prevents the access for such information. Access control file system can be implemented using the device's memory or smartcards (e.g. USIM) as discussed in section 6.5.6. However, memory separation between tasks needs to be maintained.

To provide the application separation required by the ARM, lockbox mechanism can be used to enforce the concept of containerization. The concept of containerization is to ensure that when an application is running on a memory space, other applications cannot access the memory being used. This way, applications and related information are enforced to stay within their assigned memory areas and cannot be interfere with other applications in different memory areas. HC-USIM can also support the idea of containerization and separated memory areas as discussed in section 6.5.6.2.

ARM operations has critical information that must be protected in a secure location in the mobile device such as the cryptographic keys, since compromising cryptographic keys enable the attacker to access encrypted information and decrypt it. Thus, ARM mechanism requires a secure memory to protect sensitive information. ARM may use the capabilities provided by the ROT to store cryptographic keys, authentication credentials, and other sensitive information. Furthermore, smartcards (e.g. USIM, HC-USIM) can provide a secure memory for sensitive information as discussed in section 6.5.6.2.

(2) Key Management

To provide a secure key management, DRM system should be able to handle a database of credentials such as private keys, public keys, and certificates that represents the state of the device, application, or any other peripheral or software element. DRM system may rely on ROT in which a root certificate is used to verify the integrity of device, application, or any other peripheral or software element. The verification process may require establishing a transitive

chain-of-trust as described in section 6.4.1. Furthermore, DRM system must be able to control the use of private keys. These keys must be used only by trusted components of the OS. These keys must be decrypted only to secure temporary memory, thus, they can be easily cleared if any tempering is detected.

C. Trusted Application Agent:

Trusted application agent is responsible for supporting the applications to access and manipulate decrypted information. The trusted application agent provides the applications with the ability to interpret the DRM protected information. The trusted application agents are trusted to handle the decrypted information. An agent called application loader is responsible for enforcing the usage rules and policies before executing previously installed applications, and ensure that the access rights and privileges assigned to an application are enforced during the application is running.

Annex D High Capacity USIM (HC-USIM)

HC-USIM is enhanced category of USIM, with higher CPU performance, mass storage, and higher speed interfaces. HC-USIM can provide the PSG-MD with management features for public safety information, while separating PS information from user's personal private information. HC-USIM is designed to include "CPU, EEPROM, RAM, memory controller, and flash memory, as shown in Figure 22.

In order to use the HC-USIM in environments that require sophisticated security requirements (e.g. public safety environment), it is required to identify the proper security technologies to be applied between different entities in public safety environment (e.g. Information Providers, Network Operators, Users, and Device). This requires a well-defined security models and policies to define the purpose and function of each entity and establishes the trusted relationships between entities [84]. Typically, the security models consist of security models for service domain and smartcard domain as shown in Figure 35. The security model of service domain defines the roles, purposes, and trusted relationships between participants, namely, service (e.g. Information Providers and Service/Network operator), PSG-MD, and Smartcard. On the other hand, the security model of smart card domain defines the security functions and roles between smartcard (including platform, processor, EEPROM, COS), and flash memory.

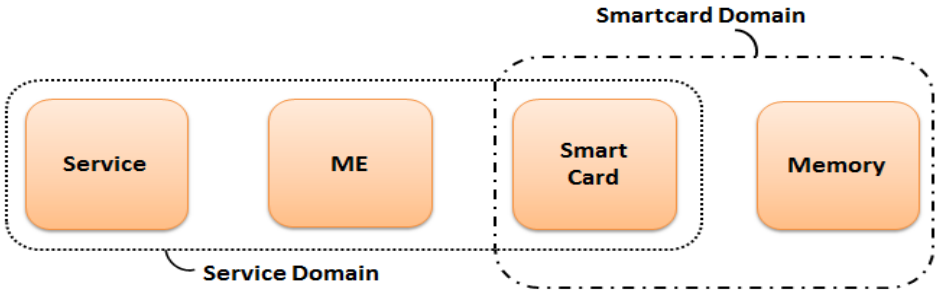

Figure 35 HC-USIM security models[84]

The purpose of this structure is to store information securely and to define the trust relationships between entities. In general, the models can be divided into (a) basics security model, (b) external security model, (c) asymmetric security model, and (d) public security model as shown in Figure 36.

The basic security model (a) applies to internal services in the mobile operator. This model is based on secret key, where the USIM card stores its secret key after subscription, and encryption. This is similar to the HC-USIM applications that authenticate users and perform key exchange and encryption in the mobile zone. The external security model (b) has the same characteristics of the basic security model. However, in the external security model, the Information Provider generates the secret key, and the keys management must be done in a proper way for the confidentiality of information, even the Information Provider must not know the secret keys. This provides the required assurance for Information Providers of the integrity and enforcement of its information policy.

The asymmetric security model (c) and the public security model (d) are based on public key cryptography algorithm utilizing a common Trusted Authority TA mechanism. The common TA generates verification certificates of the public keys. Since the public safety environment has multiple Information Providers, the certificate issuance is made by multiple certificate authorities. However, if all the agencies follow a common TA or tree of TA, a unique verifiable certificate can be used for information and services. Consequently, a public security model can be efficiently used in the public safety environment [84].

Considering the public safety environment, there are several areas that need to be protected. Secure space can be created on the HC-USIM for protecting information on PSG-MD including PSOD and BYOD devices. Inserting a HC-USIM that is configured with secure storage partition may replace the need for containerization solutions to perform the isolation required for public safety information.

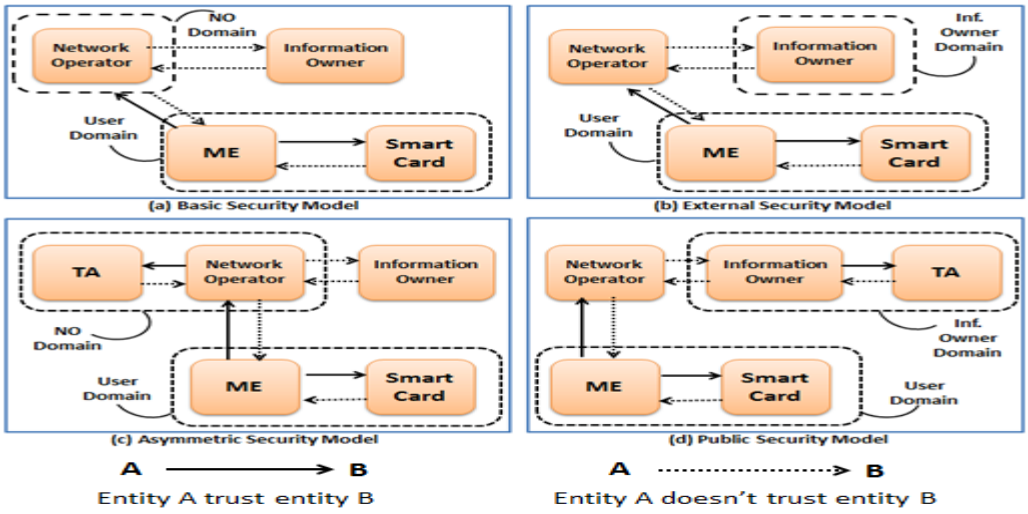

Figure 36 Trust Relationship between different Entities for different Security Models

Secure Storage Area on PSG-MD is required because the device can't be trusted. HC-USIM can provide such secure storage area, where the device, User, application can't access information and services on the smartcard without permission. Thus, the smartcard must verify whether the connected PSG-MD has the privilege to access the smartcard. The user needs an authentication key to authenticate and access the content of the smartcard. In general, smartcards have two keys, namely, Master Session Key (MSK) and MMSK. MSK is the master key of the card that is stored on the smartcard during card issuance. While MMSK is a unique master key of the smartcard that is embedded so even the HC-USIM issuer doesn't know this key. MSK is known only by the card issuer and can't be accessed by the user, Information Providers, or any other entity. However, MMSK can't be accessed by any user, Information Providers, or card issuer. The smartcard performs encryption and decryption using these two keys, while providing encoded and decoded information without disclosing the keys. Since information is stored only after encryption, storage can be accessed by privilege entities using authentication keys as shown in Figure 37. The Secure Storage Area in the HC-USIM can be partitioned as following:

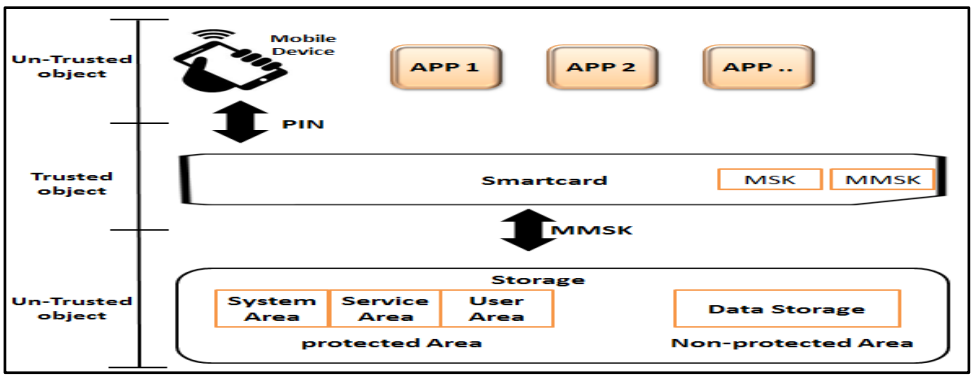

Figure 37 Secure Storages' Architecture

(1) Secure System Area

The system area of the HC-USIM consists of key storage that store all the keys, and the application area that store various applications as shown in Figure 38. The key storage area stores keys including service key for service area, and various encrypted keys. Each folder is encoded, and a unique key for the folder is generated. Therefore, information can be stored securely by encrypting each folder [84] and satisfy the requirements for isolating information access and storage.

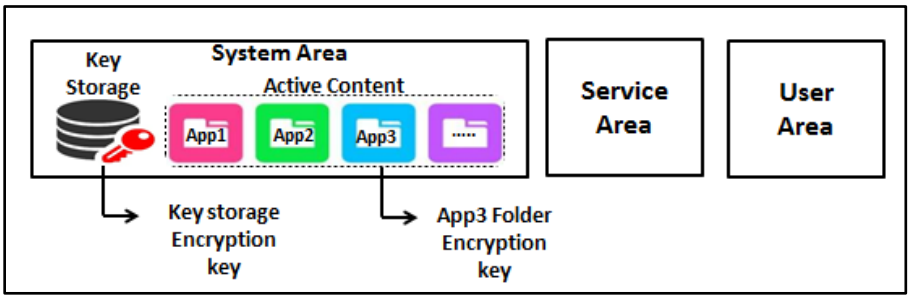

Figure 38 System's Area Architecture

(2) Secure Service Area

The service area of the HC-USIM is a secure storage that can be used by any service or content provider of any application to store information/services securely in the HC-USIM of the PSG-MD. Even if the user has a valid PIN, he can't access the service area. As shown in Figure 39, each content provider can have a unique area defined by Service ID (SID), and a unique secret key (SK) corresponding to each SID, that is not disclosed to the user. Therefore, the PSG-MA can operate on both PSBN and a commercial carrier and keep its contents stored in a protected storage within the HC-USIM. In addition, each content provider service area must be encrypted and the secret key (SK) should be stored securely in the system area of the HC-USIM. This can be done, for instance, using a service registration protocol described in [84].

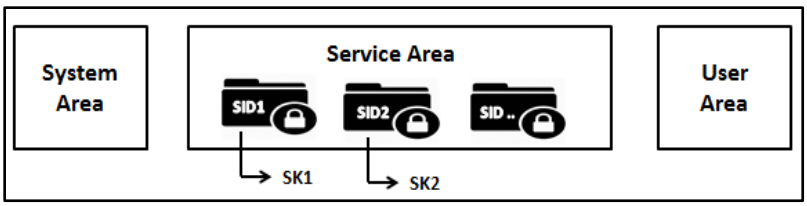

Figure 39 Services' Area Architecture

(3) Secure User Area

The user area of the HC-USIM is a protected area within the USIM that can be accessed only by the user. This area is not accessible by the Information Providers or the Management and Administration. The user area should be encrypted, and only the user can access it using unique encryption key. Users can store their private information (e.g. SMS, addresses), and personal information. User can divide the user area within the HC-USIM into different folders, where each folder is encrypted using unique encryption key. This way, if a key of one folder is disclosed, other folders remain secured. Typically, the encryption key is calculated and generated based on the user own PIN for index number and the folder name as shown in Figure 40. The process of generating encryption keys of the user area is described in [84].

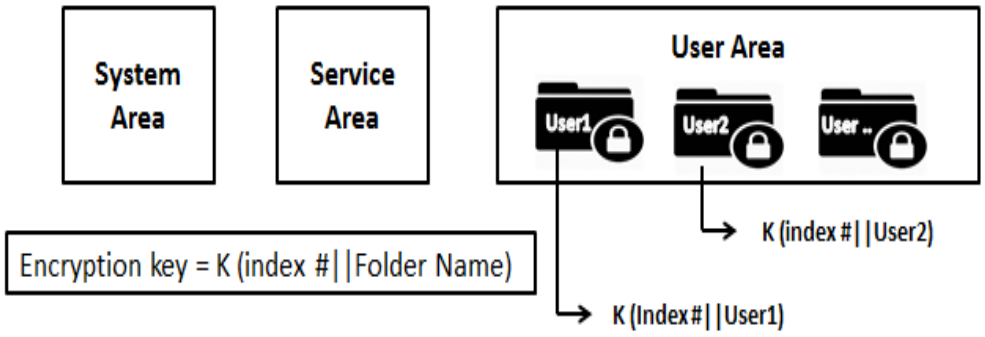

Figure 40 User's Area Architecture

Annex E Mobile Device Extra Capabilities

E.1 Battery

There are many major sources of batteries to drain such as: main processor, the device's screen (and therefore also the Graphics Processor, the GPU), the communications processors (cellular network, WiFi, GPS and Bluetooth), and the applications used on the device [127]. Further, the range of what consume 'too much' may vary depending on the nature of the application and the hardware capabilities of the platform it is running on.

When selecting the applications for use by PS Users, further work is needed to evaluate the appropriateness and effectiveness of applications to be used in public safety. Various tools, methodologies, and metrics must be used to measure the application battery impact which include [25]:

- Analytic techniques that attempt to address application inefficiencies and comparing them to the maximum predefined battery consumption. Such inefficiencies have to be improved by developers before uploading the application to the PSG-AS.
- Techniques that attempt to assign quantitative consumption scores to applications.

Furthermore, public safety applications should allow remote configuration of their power consumption. This configuration can come from two primary sources as mentioned by NIST [25]:

(1) **Role/mission based power management profiles:** Power management profile tailored for responder's specific needs (For example, a firefighter may have very different power needs from a police officer). Power management profiles for a User's specific needs can be applied before the device enters the field. Applications should be able to adjust their behaviour by changing their network interactions, processing requirements, or shutting themselves off completely when being used by a profile of specific needs according to the requirements defined in such profile.

(2) **Real time remote control to meet situational demands:** Remote power management takes the form of an on-demand control made by a centralized authority which can remotely adjust the behaviour of applications in use on the PSG-MD according to the circumstances and the User's scenario.

The requirements mentioned above add extra capabilities for battery in PSG-MD. Using such capabilities we can establish suitable metrics for battery usage where applications can report their battery usage and its impact using analytical and quantitative metrics. Furthermore, applications can be dynamically configurable in order to adjust their power needs by either manually where the user can control the application usage and adjust the power consumption, or automatically using power management profiles, or remote power management to provide real time remote control to meet situational demands.

E.2 GPS & Location Services

PSG-MAMF encourages policies that enforce the configuration of location services to be disabled by default. Malicious applications can detect device location by sensing nearby networks or based

on the given IP address range, thus, PSG-MA access to location services should be on a per need basis. Adopting location restriction policy limits the risks of compromising the device and its holder [5]. There are different techniques that can be used by the device or mobile application to derive location information. Each technique has different accuracy that enables it to work in a specific range. For example, Global Position System (GPS) provide accuracy within 3 meters, location based service providers provide different accuracy levels depending on the technique being used, and the communications network provide accuracy within 1200 meters using triangular techniques, while LTE proximity services can provide more enhanced accuracy location derivation [25].

NIST.IR.8080 [25] provided guidelines, considerations and requirements for using location services on PSG-MD. In addition, NIST considerations provide guidelines to PSG-MA usage of locations services, guidelines to configure location services as enabled/disabled according to specific situational scenarios, and guidelines to location service information sharing between PSG-MA and PSG-MD. A snapshot of NIST guidelines are as follows:

- When considering the requirements for location services, there are three factors that must be considered, namely, accuracy, integrity, and confidentiality.
    - Accuracy: Accuracy must be taken in consider when choosing the appropriate source for deriving location information. As mentioned earlier, location information can be derived using different sources and techniques that may result in varying levels of information accuracy.
    - Integrity: Location information integrity should be taken in consider, so that inaccurate location information is not provided during a real time situation. Location information created by PSG-MD should be digitally signed so that any alteration can be detected.
    - Confidentiality: The location information generated by the PSG-MD need to be protected in a secure storage space, and access to such information should be managed
- Location sharing must remain protected (integrity and confidentiality) in order to maintain trust in location information and make use of it in a secure manner [25].
- Location services must be configurable either by user control, remote management, and/or location/mission-based profiles.
- Location services must be reconfigurable remotely. The administration should be able to turn the location services on/off. This capability will allow the administration to remotely support the Users while they are involved in other duties.
- It must be consider who will have control over location services, what kind of control they will have, and who will have access to location information. The entity responsible for policies enforcement should have access to the location information. This should occur while protecting the confidentiality and integrity of location information as well.

E.3 Memory

PSG-MD has both Volatile Memory (VM) and Non-Volatile Memories (NVM). VM (i.e., RAM) is used for dynamic storage and its contents are lost when power is drained from the device.

NVM is persistent as its contents are not affected by loss of power or overwriting information upon reboot. Most recent devices use solid state technology to maintain robust use of NVM.

The devices typically contain one volatile flash memory (e.g. RAM), and one or two different types of non-volatile flash memory such as NAND and NOR. RAM is the most difficult to capture accurately and more secured due to its volatile nature. However, device RAM capture tools are just beginning to become available. RAM is considered a middle man between the file-system stored on the ROM, and the processing cores. RAM is typically used for program execution, thus, it contain valuable information (e.g., configuration files, passwords, etc.). Critical files that are needed by the processor are stored in the RAM, waiting to be accessed. These files could be things such as operating system components, application data and game graphics; or generally anything that needs to be accessed at speed faster than other storage can provide [128]. When running an application, the application is loaded from device memory into the RAM, due to the RAM faster access speed. The RAM lose its contents whenever the power is drained or the user clear it, however, this clear the RAM but most background applications will automatically be loaded back into the RAM. The automatic loading of application into the RAM raises a security risk for the PSG-MD, which need further consideration.

On the other hand, flash memories are easier to capture due to their non-volatile nature and is much slower than RAM. Flash memories can be an internal memory storage or external memory storage. The external memory (removable storage) is SD Card which can switch and swap with a variety of different sizes. PSG-MD should include external memory slot as a method for expanding storage. However, the SD cards used with PSG-MD must have a heavy security features activated (e.g. the card can't be read in other devices), while a management software can be used to change what is on the device [128].

The internal memory is a built in memory just like SD Card, however, it can't be swapped or taken out of the phone and has better performance than external SD cards. The internal memory holds the operating system and critical files that make the device work. These files are read only, and can't be edited by the user unless the device is rooted. The applications and its related files are stored on the internal memory. Whenever the application opened to be used, it loaded (or part) into RAM and starts running. This is because the access speed is far greater in RAM. There are multiple storage chips inside the device. These chips may then be partitioned into several areas for different purposes, such as application storage, cache and system files. Normally the chip that stores the system files is called the ROM (read only memory) [128].

Annex F PSG-MAMF open issues

F.1 Device open issues:

- Public safety agencies need to develop rules for battery exchange (LMR battery life is 9-16).
- Sensor authentication and securing sensing feed. Particularly managing sensors that are not on device.
- Need for sensor data probing, logging and archiving techniques.
- Issues relevant to memory corruption and unauthorized use of flash memory

F.2 Applications open issues:

- Key storage and exchange need to be discussed.
- Does the DRM system supported by Android or IOS?
- The creation of security policies would be per app, device, or user?
- Minimum security requirements/policies which public safety grade maps to?

F.3 Applications open issues:

- Identity proofing mechanisms that is acceptable for public safety.
- Types of credentials/mechanisms that is acceptable for public safety
- How about SIM cards? Does it always go with same Device?

Annex G List of Abbreviations

Selected abbreviations of governmental organizations, industrial organizations, vendors, and study groups used in this study are defined below:

Table 8 list of Organization's Abbreviations

Abbreviation	Definition
ATIS	Alliance for Telecommunications Industry Solutions (ATIS)
APCO	Association of Public Safety Communications Officials
CSSP	Canadian Safety and Security Program
CSA	Cloud Security Alliance
CIO Council	Chief Information Officers Council
CITIG	Canadian Interoperability Technology Interest Group
CIRTEC	Communications Interoperability Research, Test and Evaluation Centre
DHS	Department of Homeland Security
DoD	Department of Defence
DRDC	Defence Research and Development Canada
FirstNet	First Responder Network Authority
GP	GlobalPlatform
ISO	International Organization for Standardization
MTTT	Mobile Technology Tiger Team
NATO	North Atlantic Treaty Organization

NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NPSTC	National Public Safety Telecommunications Council
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OWASP	Open Web Application Security Project
RCMP	Royal Canadian Mounted Police
TCP	Trusted Computing Group

Selected abbreviations used in the report are defined below:

Table 9 List of Abbreviations

Abbreviation	Definition
API	Application Program Interface
ARM	Access Rights Management
ARM-SS	Access Rights Management Support System
ARM-DS	Access Rights Management Device System
BYOD	Bring Your Own Device
HC-USIM	High Capacity-Universal Subscriber Identity Module
LTE	Long Term Evolution
MDM	Mobile Device Management

MAM	Mobile Application Management
MCM	Mobile Content Management
MIM	Mobile Information Management
MAM-SS	Mobile App Monitoring Support System
MAM-DS	Mobile App Monitoring Device System
MAMF-SS	Mobile Application Management Framework – Support System
MAMF-DS	Mobile Application Management Framework – Device System
MCDF	Mobile Computing Decision Framework
MSRA	Mobile Security Reference Architecture
PSBN	Public Safety Broadband Network
PSG	Public Safety Grade
PSG-MD	Public Safety Grade – Mobile Device
PSG-MA	Public Safety Grade – Mobile Application
PSG-II	Public Safety Grade – Information Infrastructure
PSG-AS	Public Safety Grade – Application Store
PSG-AS-SS	Public Safety Grade – Application Store – Support System
PSG-AS-DS	Public Safety Grade – Application Store – Device System
PSG-MAMF	Public Safety Grade – Mobile Application Management Framework
PSOD	Public Safety Owned Device

PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-I	PIV-Interoperability
PKI	Public Key Infrastructure
RKP	Real-time kernel protection
SIM	Subscriber Identity Module
SE	Secure Element
SDK	Software Development Kit
TPM	Trusted Platform Module
TIMA	Trust-Zone based Integrity Measurement Architecture
UE	User Equipment
UICC	Universal Integrated Circuit Card

DOCUMENT CONTROL DATA

*Security markings for the title, authors, abstract and keywords must be entered when the document is sensitive

1. ORIGINATOR (Name and address of the organization preparing the document. A DRDC Centre sponsoring a contractor's report, or tasking agency, is entered in Section 8.)

University of Regina
3737 Wascana Parkway
Regina, SK Canada S4S 0A2

2a. SECURITY MARKING (Overall security marking of the document including special supplemental markings if applicable.)

CAN UNCLASSIFIED

2b. CONTROLLED GOODS

NON-CONTROLLED GOODS
DMC A

3. TITLE (The document title and sub-title as indicated on the title page.)

Public Safety Grade Mobile Application Management Framework (PSG-MAMF)

4. AUTHORS (Last name, followed by initials – ranks, titles, etc., not to be used)

Keshta, N.; Morgan, Y.

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total pages, including Annexes, excluding DCD, covering and verso pages.)	6b. NO. OF REFS (Total references cited.)
March 2018	213	133

7. DOCUMENT CATEGORY (e.g., Scientific Report, Contract Report, Scientific Letter.)

Contract Report

8. SPONSORING CENTRE (The name and address of the department project office or laboratory sponsoring the research and development.)

DRDC – Centre for Security Science
NDHQ (Carling), 60 Moodie Drive, Building 7
Ottawa, Ontario K1A 0K2 Canada

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.)	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
CSSP-2015-CP-2103	W7714-166169/001/SV

10a. DRDC PUBLICATION NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.)	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)
DRDC-RDDC-2018-C203	

11a. FUTURE DISTRIBUTION WITHIN CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

Public release

11b. FUTURE DISTRIBUTION OUTSIDE CANADA (Approval for further dissemination of the document. Security classification must also be considered.)

12. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Use semi-colon as a delimiter.)

Public Safety Broadband Network (PSBN); Android, phone, mobile, ad ahoc; Mobile Networks; Software Security; Software Engineering; Information Management; Information System Technology

13. ABSTRACT/RÉSUMÉ (When available in the document, the French version of the abstract must be included here.)

This study covers in details the Public Safety Grade Mobile Application Management Framework, which is a system that includes a group of trusted components with integral security functions into a single framework, as well as extra security considerations, technologies, standards, and policies. PSG-MAMF is intended to provide semi-closed ecosystem components that can integrate effectively to provide the security functionalities required to address the threats and vulnerabilities of mobile devices, applications, and information in public safety environments. PSG-MAMF improves the security of mobile devices and applications use by the government and public safety, and provides safer ways to access information infrastructure while adhering to organizational policies. The study identifies approaches to monitor, detect, and sense potential attacks taking place from within or outside mobile applications. The study also provides comprehensive ways to identify and mitigate security risks by applying separation of data, applications, algorithms, and keys.
Compared to other advanced security solutions available for mobility management, PSG-MAMF provides a level of integration that is not available in other ecosystems provided by other research studies (e.g. NIST ecosystem) and other existing products supported by different vendors (e.g. Blackberry, AirWatch, etc.).

Cette étude couvre en détail le cadre du Cadre de gestion des applications mobiles de niveau sécurité publique. Il définit des moyens sûrs d'accéder à l'infrastructure et à l'information tout en respectant les politiques organisationnelles. L'étude identifie également des approches pour surveiller, détecter et détecter les attaques potentielles qui se produisent à l'intérieur ou à l'extérieur des applications mobiles. L'étude fournit également des moyens complets d'identifier et de mesurer les risques de sécurité en appliquant la séparation des données, des applications, des algorithmes et des clés.