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

DEFENCE R&D DÉFENSE

Biometrics for National Security: The Case for a Whole of Government Approach

Pierre Meunier
DRDC Centre for Security Science

Qinghan Xiao
DRDC Ottawa

Tien Vo
Royal Canadian Mounted Police

Defence R&D Canada – Centre for Security Science

Technical Memorandum
DRDC CSS TM 2013-005
June 2013

Canada

Biometrics for National Security: The Case for a Whole of Government Approach

Pierre Meunier
DRDC CSS Centre for Security Science

Qinghan Xiao
DRDC Ottawa

Tien Vo
Royal Canadian Mounted Police

Defence R&D Canada – CSS

Technical Memorandum
DRDC CSS TM 2013-005
June 2013

Principal Author

Original signed by Pierre Meunier

Pierre Meunier

Portfolio Manager, Surveillance, Intelligence and Interdiction

Approved by

Original signed by Dr.Andrew Vallerand

Andrew Vallerand

Director DRDC CSS DSTPS

Approved for release by

Original signed by Dr. Mark Williamson

Dr. Mark Williamson

DRDC Document Review Panel Chair

Abstract

The improvements of the last few years have not only made biometrics more reliable but they have made them also cheaper and more capable of handling high volumes of transaction, and thus more suitable for public safety and security applications. Several governments around the world are now using biometrics as means of verifying the identity of visa applicants and visitors or as a means of expediting the passage of trusted travellers across borders. The sphere of influence of biometric technologies extends well beyond border applications, however, and the prevalence of this technology is likely to increase not just in the public sector, but in the private sector as well.

The objective of this paper is to show the trends surrounding the use of biometrics to improve public safety and security and make the case for taking a holistic view of this capability so as to extract the greatest benefits in the most efficient and effective manner.

Résumé

Les améliorations de ces dernières années ont non seulement rendu la biométrie plus fiable, mais elles ont également réduit son coût tout en augmentant sa capacité de traiter des volumes élevés de transactions, la rendant donc plus adapté aux applications de sécurité et sûreté publique. Plusieurs gouvernements à travers le monde utilisent la biométrie comme moyen de vérifier l'identité des demandeurs de visa et des visiteurs ou comme un moyen d'accélérer le passage des voyageurs dignes de confiance à travers les frontières. La sphère d'influence des technologies biométriques s'étend bien au-delà des applications frontalières, cependant, et la prévalence de cette technologie est susceptible d'augmenter non seulement dans le secteur public mais dans le secteur privé.

L'objectif de ce rapport était de montrer quelques-unes des tendances relatives à l'utilisation de la biométrie pour améliorer la sécurité et sûreté publique et de plaider pour une vue plus globale de cette capacité au sein du gouvernement afin d'en extraire le maximum d'avantages de la manière la plus efficiente et efficace.

Executive summary

Biometrics for National Security: The Case for a Whole of Government Approach:

Pierre Meunier; Qinghan Xiao; Tien Vo; DRDC CSS TM 2013-005; Defence R&D Canada – CSS; June 2013.

Introduction or background: The improvements of biometrics technologies over the last few years have not only made them a more reliable tool, but also cheaper and more capable of handling high transaction volumes, which are all key features for National Security applications. Governments around the world are now using biometrics as means of screening visitors or expediting the passage of trusted travellers across borders. The sphere of influence of biometric technologies extends well beyond border applications, however, and the prevalence of their use over the next decade is likely to increase not just in the public sector, but in the private sector as well.

The objective of this paper was to show some of the trends surrounding the use of biometrics to improve public safety and security and make the case for taking a more holistic view of this capability so as to extract the greatest benefits in the most efficient and effective manner.

Results: What seems to be the case at the moment is that the various biometric programs within government lack an overarching strategy or policy that could lead to the development of a whole of government capability. Before going too far along that road, however, it is necessary to gain an understanding of the current architecture, design an "ideal" architecture that would be able to meet the government requirements, and contrast these two states to define the work that needs to be done and prioritize S&T investments.

With the biometrics expertise in government and through collaboration with academia and industry, it is possible to develop a biometrics road map that could address government requirements.

Significance: Mapping out the National Biometrics Enterprise Architecture, as this report suggests, would help create synergies and economies of scale while improving the sharing of information inter-departmentally as well as internationally, where appropriate. It would also be usefull as a tool to assist in the prioritizing of future S&T investments.

Future plans: The following eight recommendations are proposed as the most important ones to be considered in the road map development:

1. Survey and analysis the current government-wide biometric programs, systems, and future plans in terms of advantages and limitations

2. Study the experience and lessons learned from the others, such as the US and UK government biometric programs, to ensure high-quality, low-cost, and effective solutions

3. Perform gap analysis to help strengthen existing biometric systems

4. Look into current operations and make recommendations to the Executive to get support on further architectural developments

5. Launch inter-agency biometric activities to develop a cross-government policy to guide the biometrics community and practice

6. Identify new areas of opportunity by:

    a. responding to urgent government needs

    b. analyzing national security threats

    c. meeting technology changes

7. Leverage technology to reduce huge amount of time and resources wasted in inspection and re-inspection, and consider scaling, adoptability and interoperability issues

8. Determine the deployment strategy to ensure that all GoC biometrics requirements can be addressed

Sommaire

Biometrics for National Security: The Case for a Whole of Government Approach:

Pierre Meunier; Qinghan Xiao; Tien Vo; 005; R & D pour la défense Canada – CSS; juin 2013.

Introduction ou contexte: Les améliorations des technologies de biométrie au cours des dernières années en ont non seulement fait un outil plus fiable, mais aussi moins cher et plus apte à traiter des volumes de transaction élevés, qui sont tous des éléments clés pour les applications de sécurité nationale. Les gouvernements à travers le monde utilisent la biométrie comme moyen de dépistage de visiteurs ou d'accélérer le passage des voyageurs dignes de confiance à travers les frontières. La sphère d'influence des technologies biométriques s'étend bien au-delà des applications frontalières, cependant, et la prévalence de leur usage au cours de la prochaine décennie est susceptible d'augmenter non seulement dans le secteur public, mais dans le secteur privé.

L'objectif de ce rapport était de montrer quelques-unes des tendances relatives à l'utilisation de la biométrie pour améliorer la sécurité et sûreté publique et de plaider pour une vue plus globale de cette capacité au sein du gouvernement afin d'en extraire le maximum d'avantages de la manière la plus efficiente et efficace.

Résultats: Ce qui semble être le cas en ce moment est que les divers programmes biométriques au sein du gouvernement manquent d'une stratégie ou politique qui pourrait conduire à l'élaboration d'un ensemble de capacités gouvernement. Avant d'aller trop loin dans cette voie, cependant, il est nécessaire d'acquérir une compréhension de l'architecture actuelle, de concevoir une architecture "idéale" qui serait en mesure de répondre aux exigences du gouvernement, et de contraster de ces deux états pour définir le travail qui devrait être fait et pour prioriser les investissements en science et technologie.

Grâce à l'expertise en biométrie dans le gouvernement et à travers la collaboration avec le milieu universitaire et l'industrie, il est possible d'élaborer une feuille de route biométrique qui pourrait répondre aux exigences gouvernementales.

Importance: L'élaboration d'une architecture de l'entreprise biométrique nationale, comme ce rapport l'indique, permettrait de créer des synergies et des économies d'échelle tout en améliorant le partage de l'information entre les ministères et avec nos alliés, le cas échéant. Elle serait également utile comme outil d'aide à l'établissement des priorités pour d'éventuels futurs investissements en science et technologie.

Perspectives: Les huit recommandations suivantes sont proposées:

1. Enquête et analyse des programmes biométriques actuels à l'échelle gouvernementale ainsi que des systèmes biométriques déjà en opération et des plans futurs.

2. Étudier l'expérience de nos alliés, tel que les programmes biométriques des États-Unis et du Royaume-Uni, afin d'en tirer des leçons.

3. Effectuer une analyse des lacunes existantes pour aider à renforcer les systèmes biométriques

4. Observer les opérations en cours et faire des recommandations à l'exécutif au sujet de développements architecturaux.

5. Lancer des activités collaboratives afin d'élaborer une politique pangouvernementale pour guider la communauté de pratique en biométrie.

6. Identifier de nouvelles opportunités pour :

    a. répondre aux besoins urgents du gouvernement

    b. l'analyse des menaces à la sécurité nationale

    c. répondre aux évolutions de la technologie

7. Exploiter la technologie pour réduire la quantité de temps et le gaspillage de ressources en matière d'inspection et de réinspection et d'examiner les questions d'échelle, d'adoptabilité et d'interopérabilité.

8. Déterminer la stratégie de déploiement pour s'assurer que toutes les exigences du gouvernement du Canada biométriques peuvent être adressées.

Table of contents

List of figures

List of tables

1 Introduction

The Public Security Technical Program (PSTP) was established in March 2006 as an initiative of Defence Research and Development Canada (DRDC). Its aim was to develop a coordinated program to enhance collaboration across government and to deliver science and technology (S&T) advice and solutions across the many dimensions of public security. Biometrics for National Security was established as one of the technical areas of the program to support "science and technology based capabilities to identify and stop terrorist and criminal activity, in the border and transportation security domains, through surveillance, monitoring, disruption, and interdiction"[1].

While it can be argued that biometrics, or biometric identification, has been in existence since the 19th century through the use of fingerprint and other physical traits, it is only recently that the technology has become a viable automated means of identification and authentication. Spurred by the 9/11 attack and ensuing wars, the field of modern biometrics, or automated biometric identification, has grown by leaps and bounds. Such modalities as finger, face, and iris have emerged as indispensable in counterinsurgency operations and have proven their value many times over. Development has been rapid for other biometric modalities, and has resulted in a number of new capabilities.

The improvements of the last few years have not only made biometrics more reliable, but also cheaper and more capable of handling high transaction volumes, which are all key features for National Security applications. Governments around the world are now using biometrics as means of screening visitors or expediting the passage of trusted travellers across borders. The sphere of influence of biometric technologies extends well beyond border applications, however, and the prevalence of their use over the next decade is likely to increase not just in the public sector, but in the private sector as well.

The objective of this paper is to show the trends surrounding the use of biometrics to improve public safety and security and make the case for taking a holistic view of this capability so as to extract the greatest benefits in the most efficient and effective manner.

[1] http://www.css.drdc-rddc.gc.ca/pstp/priorities-priorites/surveillance-eng.asp

2 Range of use of Biometrics for National Security

2.1 Ten years after 9/11

This year marked the tenth year after 9/11. What kind of progress have we witnessed over that period? Where are we heading in the next ten years?

New uses and applications of biometrics technologies will continue to grow because of the increasing need for the positive identification of individuals. Examples of applications that have been successful so far have been partitioned in the categories below.

2.2 Biometrics in law enforcement

Use of fingerprints, of course, but what else is there in the future? Some of the FBI applications should be mentioned; scars, marks and tattoos. What are some of the state police forces doing? Would any of these applications be plausible in Canada at the federal, provincial or municipal levels?

Most of the uses for biometrics are aimed at criminal justice, but should some of it address insider threats? What if a government employee is convicted of a crime, would the information be fed back to the employer? Would there be an assessment of risk? Do we have examples of this type of use elsewhere?

2.3 Biometrics in corrections

Faced with rising costs and rampant overcrowding, correctional facilities need to use computer-based systems in its daily operations. The National Institute of Justice's (NIJ's) Office of Science and Technology (OST) has implemented a correctional technology program that stresses the needs of jails and prisons. Access control is an obvious need because it is a major security concern to identify people entering and leaving correctional facility. In order to assess the potential for application of biometric technology in corrections, NIJ has worked with the DoD Counterdrug Technology Development Program on Facial Recognition 2000 to assess various facial recognition technologies. A second area is the use of biometrics to monitor inmate movement since keeping track of inmates within a prison or jail is a constant challenge. The Federal Bureau of Prisons tested hand geometry system to help prevent escape attempts [1]. The objective is to enhance inmate management and improve staff efficiency. Figure 1 shows an all-in-one Corrections Biometric Management System (CBMS), which features iris and fingerprint biometric technologies, manages electronic key cabinets, secures airlock portals, keeps track of inmate property storage, monitors visitor appointments, conducts criminal record checks, creates key access policies [2].

Figure 1: Corrections Biometric Management System [2].

Some deployments of biometrics have occurred in corrections facilities in recent years. Turner (2003) [3] notes two developments as a result of biometrics being introduced in prisons and jails. The first is that biometrics was found useful to verify the identity of staff and inmates as they enter and exit the facilities and to have an accurate account of who is inside the facility in the event of an emergency. The second is that fingerprint, hand geometry, iris recognition, and face recognition have emerged as the most readily applied [3].

Turner anticipated that while the biometric modalities will likely remain the same, correctional facilities will find more uses as the price point drops. Turner sees the replacement of card passes as feasible and even desirable. "Biometrics will continue to have tremendous impact on corrections" (Turner 2003).

2.4 Biometrics in immigration and border management

Biometric technologies, such as fingerprint identification, iris scan, and facial recognition, are being increasingly used at airports and border crossings to protect the nation from illegal immigrants. Biometrics-based border entry system significantly reduces the chance that a person could pose as or be mistaken for another individual. In addition, the use of biometric technology will provide the law enforcement office's ability to screen criminals applying for Visas. Biometric data, collected by the United States Visitor and Immigrant Status Indicator Technology (US-

VISIT) and linked with specific biographic information, enable a person's identity to be established, and then verified, by the U.S. government. The program checks an individual's biometrics against those associated with the identification document presented to ensure that the document belongs to the same person, as well as against a watch list of known or suspected terrorists, criminals and immigration violators. It is claimed that "Biometrics form the foundation of US-VISIT's identification services because they are reliable, convenient and virtually impossible to forge. Many agencies utilize US-VISIT services to accurately identify people and determine whether they pose a risk to the United States [4]. It is reported that the United Kingdom has required fingerprints and a photograph from all visa applicants to help in the fight against illegal immigration and organized crime since 2007 [5]. The UK Borders Agency has negotiated a biometric contract with IBM to develop an Immigration and Asylum Biometric System (IABS). The system will provide a biometric capability for immigration authorities in monitoring and controlling foreigners entering the United Kingdom. In addition, the system should also make it easier to identify individuals with criminal backgrounds and those who pose a risk to the UK [6]. CARIPASS, a voluntary travel card program, is the first multilateral border crossing program in the world [7]. It is a step towards standardized border control facilities within the Caribbean Community (CARICOM). To participate in CARIPASS, an eligible traveler must register at local immigration or designated offices and has a facial image and two fingerprint images enrolled. Then a card with a 2D barcode is issued, which can be electronically processed through self-service border crossing gates (Figure 2). Since they are connected to the CARIPASS database, the gates will open and allow the traveler to pass through after successfully matching the traveler's biometric data.

Figure 2: CARIPASS gate [7].

2.5 Biometrics in defence

Biometric technologies have been playing more and more important role in the Global War on Terrorism. As a NATO program, the International Security Assistance Force (ISAF) implemented the US biometric systems as part of ISAF force protection and overall security efforts in Afghanistan in February 2007. The system consists of a NATO/ISAF server, and the US biometric devices called Biometric Automated Toolset (BAT) and Handheld Interagency Identification Detection Equipment (HIIDE). It provides the military and intelligence communities with a capability to accurately recognize whether an individual encountered is a friend or foe especially when enemies hide among the civilian populations like the situation in Afghanistan. The objective of the ISAF biometric program is to collect, reference, and analyze biometric data along with associated information to support timely individual verification/identification to enhance Afghanistan mission elements. The key capabilities include the following:

- controlling physical access, identifying an individual encountered during tactical operations,
- locating and tracking a person of interest,
- distinguishing allies with enemy force individuals that were detained by coalition forces, and
- collecting forensic evidence and sharing the information.

Figure 3 shows a nominal operation view of the ISAF biometric program. It is reported that "About 'a dozen or so' ISAF members today would probably be ready to contribute to the database in Afghanistan, including the United States, Canada, Belgium, Holland and Australia" [8].

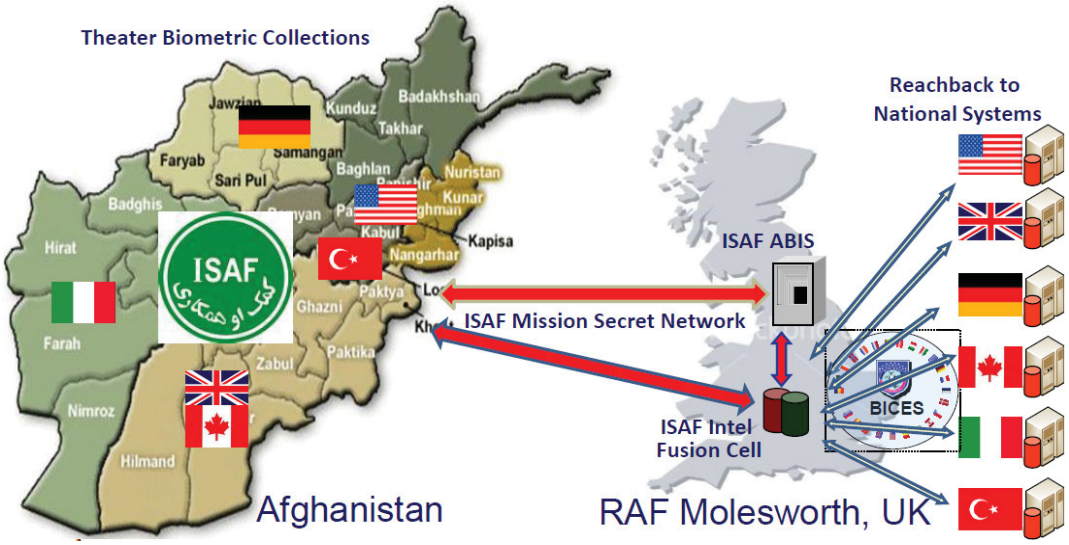

Figure 3: A nominal view of biometric operation [9].

3 The state of Biometrics in the US and Canada

Canada and the US share a common culture and have common interests, not the least of which is in ensuring the prosperity of both nations.

Canada's involvement in the counter-insurgency operations in Afghanistan spurred it to rapidly ramp up a biometrics capability for the first time. Supported by the US, Canada collected biometrics from insurgents and shared the information with the International Security Assistance Force (ISAF).

3.1 US

Various US federal agencies are engaged in the use of biometrics within an operational environment, be it for criminal justice purposes, military operations in theatre and or United States internal administrative purposes such as civil screening and immigration applications and enforcement. There are three main U.S. federal departments with large operating systems that are biometric specific; Department of Homeland Security, Department of Justice and Department of Defence. Although there is an overarching mission; that of securing the defence of U.S. citizens in a variety of roles external to the United States and homeland security within the United States, each agency is responsible for the delivery of services and programs to a particular client for specific purposes.

Historically, these three departments operated for the most part within their own swimming lanes, or silos, and the sharing of information was guarded at best. The events of September 11th, 2001 changed the political landscape and the 9/11 Commission Report highlighted cultural practices such as over classification of information that led to a failure to share between agencies efficiently and effectively.

> Current security requirements nurture over classification and excessive compartmentalization of information among agencies. Each agency's incentive structure opposes sharing, with risks (criminal, civil, and internal administrative sanctions) but few rewards for sharing information. No one has to pay the long-term costs of over-classifying information, though these costs-even in literal financial terms- are substantial. There are no punishments for *not* sharing information. Agencies uphold a "need-to-know" culture of information protection rather than promoting a "need-to-share" culture of integration.[2]

Subsequently, various regulatory directives were put in place and specifically the Homeland Security Presidential Directive 24[3] called for federal agencies to "... use mutually compatible methods and procedures in the collection, storage, use, analysis and sharing of biometric and associated biographic and contextual information of individuals". The various vested interest

[2] http://govinfo.library.unt.edu/911/report/911Report_Ch13.htm

[3] http://www.dhs.gov/xabout/laws/gc_1219257118875.shtm

departments then took the directive as a starting point in the development of strategic partnerships between the three main biometrics stakeholders:

- Department of Homeland Security – US VISIT manages the IDENT biometric repository for a series of client groups;
- Department of Justice – Federal Bureau of Investigation (FBI), Criminal Justice Information Services manages the Automated Fingerprint Identification System (AFIS) servicing the broad criminal justice community at the federal, state, local and tribal level and is directly linked to other independent state biometric systems; and,
- Department of Defence – Automated Biometric/Biographic Identification System (ABIS) serving military specific requirements both of an operational and administrative purpose.

Department of Homeland Security U.S. VISIT Program

US VISIT, as a program, is the youngest of the three agencies and was established in 2003 as one of many originating programs within the then newly formed Department of Homeland Security. Since 2007 it has been a sub-group of the National Protection and Programs Directorate. As its mission[4], the US VISIT is "*...to protect our nation by providing biometric identification services to federal, state and local government decision makers to help them accurately identify the people they encounter and determine whether those people pose a risk to the United States"*. Through the integrated use of biometrics the US VISIT contributes to the overall objective of government to enhance the security of citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of the immigration system and adhere to privacy principles as it relates to *bona fide* visitors. US VISIT perceives its role as one that contributes to defense, intelligence, credentialing, law enforcement and immigration and border management.

The biometrics of choice in the US VISIT program is fingerprints. In 2004 US VISIT deployed a 'two finger' biometric system at air and sea ports of entry with the same process for land, in 2005. The system was simply used for verification and authentication purposes at points of entry against visas that had been previously granted using only two fingers. The early system was a closed system as there was no ability to search against other biometric data bases due to the use of a two finger capture policy, nor was there a desire to query criminal databases such as that of the FBI, which uses ten fingerprints.

In 2005, DHS started the move away from two-fingers to ten fingerprints in order to achieve interoperability with the Department of Justice's IAFIS (Integrated Automated Fingerprint Identification System)[5]; the transition was completed in 2009 with the deployment of the system. The switch to ten-prints was a key step forward in interoperability, but it came at a price: significant costs in data conversions.

---

[4] http://www.dhs.gov/files/programs/usv.shtm

[5] http://www.biometrics.org/bc2005/Presentations/Conference/2%20Tuesday%20September%2020/Tue_%20Ballroom%20E/Wheelock%20-%209.15.05-FINAL.pdf

The US VISIT IDENT (Automated Biometric **Ident**ification System) serves as the authoritative repository for both biometric and biographic data along with travel document information. A sub-system, the Arrival and Departure Information System (ADIS), contains basic biographic data and connection identifiers to the IDENT data base in addition to operational data relating to the visitor. The current IDENT system contains in excess of 130 million records (unique individuals); it is the largest biometric data base within the federal government. The following agencies or departments house or share biometric data stored within IDENT system:

- ✓ US Department of State (DOS) for enrolment of Visa applications and verifications,
- ✓ US Customs and Border Protection (CBP) – Operations for international visitors identity verifications and or enrolments at ports of entry,
- ✓ US Citizenship and Immigration Services (USCIS)
- ✓ Immigration and Customs Enforcement (ICE)
- ✓ US Coast Guard (USCG)
- ✓ Transportation Security Administration (TSA)
- ✓ National Protection and Programs Directorate components
- ✓ Key federal partner agencies
    - Department of Justice - FBI
    - State and Municipal Law Enforcement
    - Department of Defense (DoD)
    - Intelligence community

The following statistics provide an idea of the breadth and depth of the biometrics enterprise and the volume of transactions that DHS needs to accommodate:

- It is estimated that the Department of State (DOS) processes between 20,000 and 40,000 visa applications every day from its 220 or so consulates and embassies around the world. The collected fingerprints are searched against both the IDENT and IAFIS databases for matches. The responses are usually returned to the DOS within 15 minutes for adjudication.

- CBP process between 80,000 and 140,000 travelers per day at the points of entry. The fingerprints are searched in 10 seconds against the IDENT watch list. This process results in more than 1000 individuals per day being referred to Secondary Inspection due to either a mismatch of biometrics against previously submitted biometrics or to a hit against the watch list.

- Every day, USCIS processes more than 10,000 applications for immigration benefits – including asylum, refugee, Lawful Permanent Residence (LPR) and naturalization requests. Every applicant is fingerprinted and searched against IDENT and many subsequent processes incorporate verification of prints against previously collected prints to confirm applicant identity throughout the adjudication process.

- The Border Patrol interdicts 3,000-5,000 individuals per day trying to enter the U.S. illegally between the POE. Every one of these individuals is fingerprinted to be enrolled in IDENT and about 80% are determined through an IDENT search.

- Through interoperability with DOJ's IAFIS, some 23,000 State and local law enforcement searches are processed through IDENT daily. Another 5,000+ searches against IDENT are received from the Office of Personnel Management, as part of the process of conducting background investigations for the Executive Branch.

- Other agencies, including USCG and DoD, conduct more limited searches against IDENT. These organizations are working to improve their capabilities in order to conduct more searches against IDENT. And others have expressed Interest in IDENT searches, including the Federal Protective Service, U.S. Secret Service and the Social Security Administration. The breadth of business processes that can be supported by conducting searches against IDENT for derogatory information or to verify identity is still in the early stages of being considered.

- In addition, US-VISIT has a Biometric Support Center (BSC) that is responsible for making final determinations on potential biometric matches that cannot be resolved by IDENT without human intervention. On a daily basis, the BSC conducts 400-600 urgent verifications (within 10 minutes), and an additional 1,000-1,200 non-urgent verifications for other customers. The BSC also reviews thousands of latent fingerprints a day to determine matches to known prints, resulting in several matches in an average week, which supports terrorist investigations, helps solve crimes, and identifies otherwise unknown individuals (namely unknown deceased).

The US VISIT is now focusing its efforts in the development, through partnerships of multi-modal biometric opportunities with specific efforts to move to a 13-set biometric: a full set of ten prints, both irises and face. Since US VISIT does not possess a research component, it relies on the efforts of others to progress.

While the US VISIT operates seamlessly with the FBI AFIS, there is currently no direct connection to the DoD ABIS. Dependent upon the nature of query, protocols are in place that will allow a US VISIT set of fingerprints to be queried in the FBI AFIS followed by a second step whereby the FBI AFIS performs a secondary query to the DoD ABIS. Responses are routed back via the FBI AFIS and DoD treats the request as though it were a primary FBI AFIS request. Efforts are underway to secure a direct pathway between the US VISIT and the DoD.

Department of Justice, FBI Criminal Justice Information Services

The Criminal Justice Information Services (CJIS) is the division within the FBI that serves as the national biometrics and criminal history repository for law enforcement. The FBI has operated within a biometric environment since 1910 with the collection of rolled and flats fingerprints. In 2003, left and right writer's palm prints were added.

Fingerprints are submitted by various FBI investigation offices and all other police services at State, local and tribal levels. These fingerprints are obtained from persons who have been charged with having committed crimes within categories regardless of outcome in criminal proceedings and as such criminal records supported by fingerprints may or may not have an outcome registered. Police Services in the US were never required by statute to obtain nor forward fingerprints to the FBI for a broader police use. With the passing of presidential

directives that were federal agency specific the FBI has now seen an increase in the number of fingerprints submitted annually. It should be noted that a majority of police services within the United States possess their own AFIS capacity and historically these systems service State and local needs without consideration for the FBI repository. The State of California has an AFIS biometric data base that exceeds that of Canada.

The Integrated Automated Fingerprint Identification System (IAFIS) collection currently holds approximately 100 million records. There are annex systems attached to the repository much like the systems attached to the Canadian AFIS and criminal history compilation. These systems provide name-based search capability as well. Some examples of annex systems include:

- National Instant Criminal Background Check (NICS) system – firearms applications;
- National Crime Information Center (NCIC) – system of wanted/missing persons, stolen and or lost articles and "persons of interest". Note that Canada has direct access to this system through the Canadian Police Information Centre (CPIC) and each police officer is able to directly query this database from a police car. The CPIC is virtually identical to the NCIC;
- Law Enforcement National Data Exchange (N-Dex) operational file exchange;
- Law Enforcement Online (LEO) Secure delivery system for unclassified and sensitive data;
- RCMP Canadian Criminal Real Time Identification Services (CCRTIS) a sister agency to the FBI CJIS participates in LEO;
- Sexual Offender Registry.

Through CJIS, the FBI has engaged in information sharing domestically, internationally and with Interpol for over 50 years; information sharing is part of their service delivery culture. There are over ten thousand different client groups contributing to and sharing information through appropriate protocols, Memoranda of Understanding and law. Canada has been able to electronically search the IAFIS since 2007 and has been sharing information with the FBI and through the FBI to other law enforcement communities for over 50 years. The FBI is also able to query CPIC. IAFIS is designed to process 130 000 queries per day; peak workdays can reach up to 300 000.

As a very mature operation, the FBI has been an agency lead in assisting other federal agencies to become interoperable. Searches are conducted in real-time between IDENT and IAFIS - since US VISIT IDENT migrated to a ten print system – and between DoD ABIS and IAFIS in a "lights out" (automated) fashion. Query searches between IDENT and ABIS are managed through IAFIS and search results are determined by protocol and agreement.

With the rapid advances in technology and the growing demand for services, the FBI initiated the Next Generation Identification (NGI) program to go beyond fingerprints. NGI program was conceived as a mechanism for the progressive replacement of IAFIS capabilities and the addition of new ones[6]. The NGI system will, among other things, allow the receipt of photographs (mug

[6] http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi

shots, scars, marks, and tattoos) with ten-print submissions, and it will support the inevitable move toward multimodal biometrics (i.e. voice, iris, face, etc).

The NGI system, which started implementing advances in 2010, has completed three of seven phases. The most recent was the standing up of the Repository for Individuals of Specific concern (RISC). RISC is designed to provide law enforcement and partnering agencies with rapid/mobile identification services to quickly assess the level of threat that an encountered individual poses. The database contains a subset of the "worst of the worst" from the main database, to achieve the quickest turn-around time possible. It contains data on wanted persons, sex offenders, known or suspected terrorists, and other persons of special interest.

In 2007, the FBI created a Biometric Center of Excellence (BCOE) in an effort to foster collaboration and improve information sharing across law enforcement and national security communities through the application of biometrics and identity management solutions. By grouping under one roof agencies such as Department of Defense (DoD) Biometrics Identity Management Agency (BIMA), the Department of Homeland Security (DHS), the Department of State (DoS), the National Institute of Justice (NIJ), the National National Institute of Standards and Technology (NIST), State and local law enforcement, and Academia, the FBI hopes to achieve synergies and the leveraging required for the advancement of biometrics.

Department of Defense

The US Department of Defense has been engaged in the use of biometrics since the early 1990s but it was not until July of 2000 that a formal biometric service was instituted. At that time, the Army was designated as the executive responsibility for the coordination, lead and consolidation of biometric efforts for the Department of Defense. At that point a Biometrics Fusion Center (BFC) was established in Clarksburg West Virginia for the purposes of research, tool development and systems management for biometric applications. The FBI assisted in the program development at the outset. Research was focused on latent applications while fingerprint capture devices were developed for field use. With the theatre implications in Iraq and domestic requirements as a result of the September 11th events, a Biometric Task Force (BTF) was formed. In 2009 the two biometric services were brought together and the Biometric Identity Management Agency (BIMA) was created. As a mission, BIMA "leads all Department of Defense (DoD) activities to program, integrate and synchronize all biometric technologies and capabilities and operate and maintain the authoritative biometrics data base", i.e. Automated Biometrics Identification System (ABIS).

The ABIS holdings include fingerprints of Foreign Nationals accessing US installations external to the continental US, latent theatre/crime scene fingerprints, military enemy combatants and all military detainees. There are presently 6 million sets of fingerprints in the repository and 120 000 Unknown Latents with approximately 4 000 transactions received daily although the system is rated for 8 000 transactions per day. Current physical and behavioural biometric modalities include fingerprints, iris, face, palm (includes left and right writer`s palms), DNA and voice. DNA is housed within a Combined **DNA** Index System (**CODIS**) and functions as a separate entity. Iris and facial images exist on a separate data base as do voice recognition data. Fingerprints and palm- prints as well as latents reside on ABIS.

As was the case for US VISIT, BIMA adheres to and supports the presidential directives that were borne out of the 9/11 Commission and the Markle Foundation Report requiring a concerted effort to integrate to the extent possible and concentrate efforts in information sharing between all federal agencies. Key partners were the Department of Homeland Security (US VISIT) and the Department of Justice (FBI). It is to be noted that DoD had been sharing limited information with the FBI CJIS Division since the early 1990s, but there had not been a formal link or accord established. It was not until 2009 that a Memorandum of Understanding was developed with the FBI.

The current information exchange is electronic between the DoD and the FBI CJIS based on law and established protocols. There is not yet a direct electronic link to transfer, request or otherwise vehicle biometric data between DOD ABIS and US VISIT. As previously mentioned, the FBI CJIS serves as the conduit between DoD ABIS and US VISIT. Agreements and protocols exist with international partners as well with the same operating principles as used by US VISIT. That is to say that the contributor of the information is the determiner of its usage, retention and destruction cycle. DoD is a high volume user of the FBI IAFIS as all ten print submissions are submitted whether it is for an administrative or an operational requirement.

BIMA is managed via a robust governance structure with participation by a range of strategic partners. The current client structure is:

- DoD Theatres of Operation
- DoD Defense Manpower Data Center (DMDC) – houses all employee and veteran prints
- Naval Criminal Investigative Service (NCIS)
- DoD Defense Intelligence Agency (DIA)
- North Atlantic Treaty Organization (NATO)
- Department of State
- National Ground Intelligence Center (NGIC)
- Intelligence community
- State and local law enforcement agencies
- Key partners;
    - Department of Justice – FBI
    - Department of Homeland Security – US VISIT

3.2 Canada

Implementing biometrics will bring Canada in line with other countries, such as the United States, the United Kingdom and Australia, which already use biometrics for immigration, border security and defence purposes. Currently, Government of Canada (GoC) is involved in various biometric activities, including research and development, pilot project and requests for proposals (RFPs), which deal with the issues such as legislative, policy-related, technical, interface-related, interoperability, physical, support and user acceptance requirements.

3.2.1 Real Time Identification (RTID)

Real Time Identification (RTID) [10] is a National Police Services (NPS) Project under the stewardship of the RCMP designed to improve the efficiency of Canada's national fingerprint and criminal record repository. Outdated paper processes and legacy systems will be replaced by modern technology, re-engineered workflows and automation to support interoperability with all users of the NPS Canadian Criminal Real Time Identification Services (CCRTIS) fingerprint and criminal records services.

RTID efficiencies are directly related to reducing the number of paper-based fingerprint submissions and, in turn, increasing the number of electronic fingerprint submissions. Agencies will be supported by CCRTIS during the transition to, and implementation of the new system.

The RTID system is RCMP's solution to address challenges in the legacy fingerprint identification and criminal record system by re-engineering and automating legacy processes. Transforming the current paper-based infrastructure into a seamless paperless electronic system will allow RCMP's Canadian Criminal Real Time Identification Services (CCRTIS) to complete work in only hours and days that previously took weeks and months. Preliminary service delivery targets for RTID are listed in Table 1.

Table 1: Target response time

Service	Current average Processing Time	Targeted Processing Time
Criminal ten print searches	10 weeks	2 hours
Criminal record updates	Several months	24 hours
Civil ten print services	Several months	72 hours
Latent crime scene searches	6 weeks	24 hours

National Police Services - National Institute of Standards and Technology - Interface Control Document (NPS-NIST-ICD version 1.7.7) is to provide law enforcement and other agencies a specification for interfacing electronically with the RCMP National Police Services (NPS) and it implements the ANSI/NIST-ITL-2000 specification.

RTID will supply a new Automated Fingerprint Identification System (AFIS) and an NPS National Institute of Standards and Technology (NIST) Server that allows for rapid fingerprint identification and supports the immediate update of the associated criminal record (Figure 4). The criminal records workflow component will manage:

- 4 M criminal records

- 540,000 annual transactions
- 35 M supporting documents

Figure 4: RTID system [11].

The RTID system will enhance the ability of Canadian police services, government departments and international law enforcement agencies to meet their mandates for public safety, national security and economic prosperity.

3.2.2 Canadian Passenger Accelerated Service System (CANPASS) Air

It is a Canada Border Services Agency (CBSA) program that allows pre-approved, low-risk air travelers to clear customs and immigration quickly and securely by using iris recognition technology [12]. It has been claimed that the benefits of CANPASS program include:

- Reducing the waiting time at busy airports
- Avoiding interacting with inspection officers
- Improving airports' ability to process increasing passenger volumes
- Allowing CBSA to focus on potentially unknown travelers
- Leveraging the technology to provide improved customer service

Figure 5 shows a man leaning in to scan his iris at a CANPASS kiosk.

Figure 5: CANPASS Air iris recognition system [13].

3.2.3 Electronic Passport (E-Passport)

Passport Canada has studied biometric passport for several years. It launched a pilot project to investigate the potential of facial recognition solution (FRS) in the prevention of passport fraud in December 2002. A feasibility study on the applicability of the technology was conducted in the summer 2003. A privacy assessment study and a business case are being developed. In September 2005, a spokesperson for the Passport Office announced that Canada would begin issuing biometric passports in the summer or fall 2006 [14]. However, that did not happen because the FRS is a big project and Passport Canada requires accurate, high volume FRS including scanning, storage and retrieval for verified, processed digital images of passport pictures [15]. Since January 2009, Passport Canada has been issuing most Official Travel passports (special and diplomatic passports) as e-passports. This pilot project is expected to lead to full implementation of e-passports for the public before the end of 2012 [16]. It will look like a traditional passport, but contain an electronic chip that is encoded with the same information found on page 2 of the passport, as well as a digital picture of the bearer's face (Figure 6).

Figure 6: E-Passport [17].

3.2.4 Temporary Residents Biometrics Project (TRBP)

Citizenship and Immigration Canada is leading the Temporary Resident Biometrics Project, announced in Budget 2008, in partnership with the Canada Border Services Agency (CBSA) and the Royal Canadian Mounted Police (RCMP). This major Crown project oversees the introduction of biometrics into the temporary resident stream of Canada's immigration program. Beginning in 2013, certain foreign nationals seeking visas to enter Canada will be required to give their fingerprints and have their photograph taken as part of their application.

In the fall of 2007, Citizenship and Immigration Canada (CIC) completed a field trial in partnership with CBSA to use fingerprint and facial recognition technologies to effectively assess and test the impact of using multiple biometrics in the CIC and CBSA operations. The field trial took place at Canadian visa offices in Hong Kong and Seattle, and at the Vancouver International Airport, the Douglas/Pacific Highway land ports of entry, and the Etobicoke refugee processing centre [18]. At the visa office ten fingerprints and a digital photograph are taken from the temporary resident visa applicants and refugee claimants. These data will be sent to a standalone database at CIC National Headquarter. When visa applicants arrived at a port of entry, they were asked to provide two fingerprints for verification purposes while the matching and analysis were performed in Ottawa (Figure 7). Multiple biometric modalities were captured to evaluate their usefulness in detecting fraud and facilitating legitimate travel. By 2013, biometric identifiers will be collected from all visitor visa, study permit and work permit applicants [16]. Canada intends to participate in a planned biometric data-sharing initiative involving the United States, Australia, the United Kingdom and New Zealand [19].

Figure 7: A setup of the field trial equipment [20].

3.2.5 Biometrics research

Since 2002, DRDC Ottawa has been working on different biometric R&D projects and providing S&T support to DPM Secure, CDI and SJS. Different from the other GoC biometric projects that focus on criminal forensic or physical access control, DRDC intends to use biometrics to enhance force protection in the war against terrorism.

3.2.5.1 Client-server facial recognition system

A client-server facial recognition system with watch list name search function has been deployed in the Canadian Navy [21]. Different from the other facial recognition algorithms that have many restrictions, such as both eyes having to be open, no smile and no glasses, uniform lighting, the algorithm is able to recognize a "fuzzy face", such as with one eye covered, with open mouth either smiling or singing a song, and even wearing dark glasses. Ongoing research efforts are focusing on detecting dark coloured faces and faces captured under poor illumination. The objective is to improve the performance of face detection on the face images taken in Africa or in low light situations [22].

3.2.5.2 Multi-biometric fusion

Multi-biometric fusion is a research area that aims to improve biometric system accuracy, robustness, and fault tolerance by combining multiple sensors, multiple acquisitions, multiple instances, multiple algorithms, or multiple modalities [23]. Unlike previously published adaptive methods that pre-assign a weight to each biometric trait, a novel approach to fuse multiple

biometric modalities has been proposed that adjusts the weights dynamically based on feedback received from the rejection cause, working environment, and the estimated noise level [24]. Research has been conducted that uses a fuzzy approach to fuse the outputs of multiple face detectors to dynamically generate the weights [25]. The objective is to improve the face detection rate under uncontrolled environment. Figure 8 presents an example when all the lights are turned off and the illumination comes only from a computer monitor. Figure 8 (a) shows the background, Figures 8 (b) and 8 (c) present the results of face detection when the user is close to the monitor and is about 1 meter away from the monitor, respectively.

(a) Background *(b) User is close to the monitor* *(c) User is about 1 meter away*

Figure 8: Example of face detection in a near dark room.

3.2.5.3 Spoofing and anti-spoofing

Like the other information systems, biometric authentication systems are also vulnerable to attack and can be compromised at various stages. Biometric systems are vulnerable to some common attacks such as denial of service, spoofing, and man in the middle. Spoofing is an attack where a malicious individual pretends to be someone else. In biometrics, spoofing is a process that defeats a biometric system by providing a forged biometric of a legitimate user. Although techniques for spoofing are different for each biometric technology, they all present forged biometric samples to the sensor. It includes three stages: first, capturing biometric sample belonging to the enrolled user; then, creating a copy of the captured sample by means of an artefact, and finally using the artefact to attack the physiological biometric technologies while mimicry is often used to spoof behavioral biometric technologies [26].

3.2.5.4 Public Security Technical Program (PSTP)

The PSTP, operated by the DRDC Centre for Security Science (CSS), is a joint endeavour of Defence Research and Development Canada and Public Safety Canada. One of its main missions is to understand threats to national security, which includes evaluating biometric technologies that could be used to improve border security. The PSTP provides funding for collaborative research projects with various levels of government, industry, international allies and academia [27].

4 Enterprise Architecture/ Holistic approach

Biometric Enterprise Architecture (BCA) in the Canadian government agencies is a blueprint that will provide a holistic view of mission functions, which systematically defines government biometrics community's vision, mission and standards with guiding principles in both business and technology terms including policy, operation model, system development and service delivery. This blueprint will also facilitate collaboration among government agencies by examining the linkages of enterprise architecture with existing and undergoing biometric initiatives. Enterprise architecture creates a complete action plan that links government long-term strategy to the day-to-day biometric operations in different government agencies.

4.1 Biometric enterprise architecture

At the moment biometric systems are generally inflexible and are not optimized for use within an enterprise. Most biometric systems don't have the ability to interface with enterprise information systems. Although some biometric applications do offer interoperability and integration points, there is a lack of robust architectural support within the policy, technical and practice domains when using biometrics in national security contexts. Canadian government stakeholders primarily consist of agencies that require biometric capabilities to support their internal business processes while in a networked environment need to expose portions of their business processes to partner organizations in resolving identity management issues. Currently these agencies collect and distribute biometric information internally but are reluctant to share biometric data with partner organizations because of such issues as security, privacy, and lack of policy cover. Therefore it is necessary to spend some effort to incorporate biometric systems into enterprise applications. It was pointed out that "The FEA (Federal Enterprise Architecture) is composed of five reference models: Performance, Business, Service, Data, and Technical. Each of the models represents specific aspects of the FEA, and provides a framework, or a shared language, for departments and agencies to develop technology solutions that can be used by the federal government collectively. The reference models are updated as needed to reflect changes in applications and services [28]. They describe the mission processes and functions, measuring the performance and outcomes, identifying the means of service delivery, clarifying information and data definitions, and indicating technology standards. It states that "There are principles that govern the EA process and principles that govern the implementation of the architecture. Architectural principles for the EA process affect development, maintenance, and use of the EA. Architectural principles for EA implementation establish the first tenets and related decision-making guidance for designing and developing information systems" [29]. The architectural principles should represent fundamental requirements and practices and ensure that policies, strategic plans, and business needs be addressed (Figure 9).

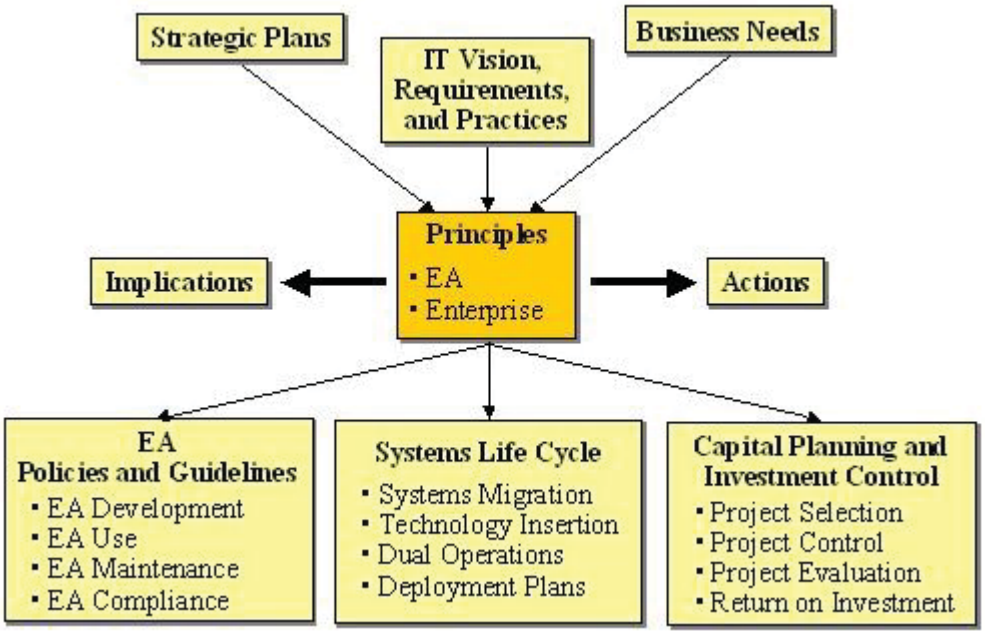

Figure 9: Role of architecture principles [29].

4.2 Case studies

4.2.1 Information sharing between United States government biometric systems

There are three major automated biometric systems within the US government: Integrated Automated Fingerprint Identification System (IAFIS), Automated Biometric Identification System (ABIS), and Automated Biometric Identification System (IDENT). They are operated by the FBI, DoD, and DHS, respectively. IAFIS is the largest biometric database in the world and is the National Repository for all automated criminal and civil records, which became operational in July 1999 to support the paperless submission of fingerprint search. DHS operates the US-VISIT program that collects fingerprints from nearly all international visitors to the US, which contains searchable fingerprint records for over 130 million people and processes about 25,000 fingerprints per day. Although both are developed by the US Department of Justice (DOJ), IAFIS and IDENT use different fingerprint standards — IAFIS based on rolled fingerprints and IDENT based on flat fingerprints. ABIS was put into operation with fingerprints in July 2004, and is managed by BIMA. The current ABIS, v1.0, deployed in early 2009, is a multi-modal biometric system that stores over six million fingerprint, face, iris and palm biometric records on persons of interest and has a daily throughput of between 8,000 and 10,000 transactions. Interoperability and information sharing issues were not considered when these systems were developed. However, in order to enhance cooperation in preventing and combating serious crime and terrorist attack, a great deal of effort has been taken to allow the DoD ABIS and DHS IDENT to exchange information (Figure 10).

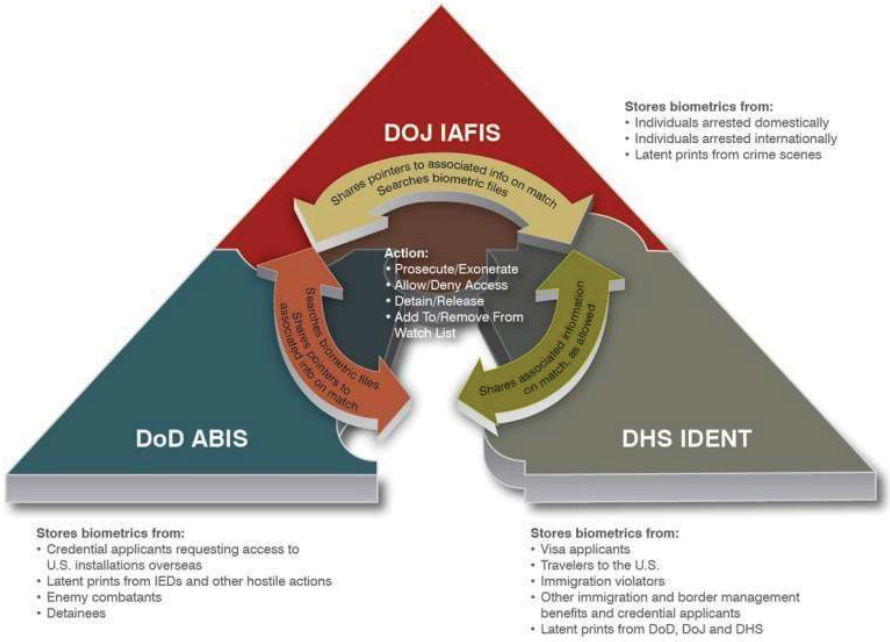

Figure 10: Interagency information sharing [30].

4.2.2 Large-scale biometrics deployment in Europe

EU Member States have been working together to strengthen their border controls, law enforcement activities and policies by introducing biometric technology into passports that comply with both EU and US policy requirements. In the last few years, EU has launched several major projects to deploy large-scale biometric systems on both national and EU levels. It was reported that there are numerous issues that require cooperation among the major stakeholders including data interchange, system interoperability, scalability, testing and evaluation, conformance to existing standards, data protection and privacy [31]. Currently, international database use both centralized and decentralized structures. The forms of cooperation are as the following [32]:

- Each party establishes a national central DNA database and a national central AFIS database for the investigation of criminal offences
- Separation of reference data (stain and reference) from other data (personal data, case information) index data
- Member States have direct access to the databases of another Member State (decentralized database network) automated search functionality within defined deadlines
- Two-step cooperation:
  - 1st step: automated searching or comparison (hit/no hit)
  - 2nd step: supply of personal data /case data and other information through police or judicial legal assistance

Figure 11 shows a vision of the future international database structure.

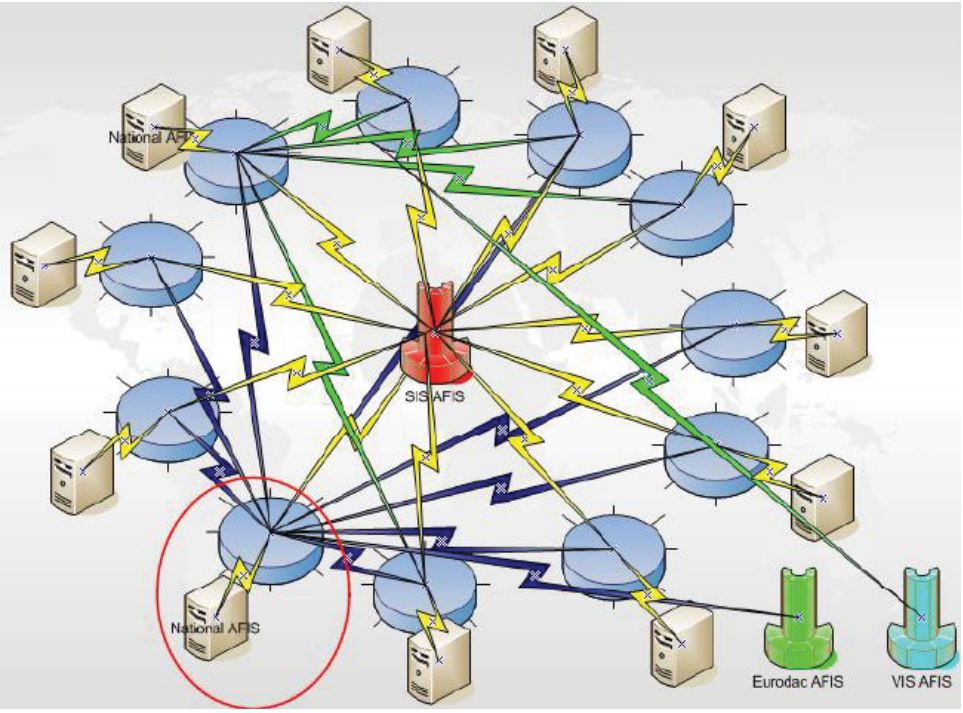

Figure 11: Vision of the future international database structure [32].

4.3 Holistic approach to biometrics

Biometrics systems are sophisticated and advanced compared to other identification methods since they verify a claimed identity base on an individual's unique physiological or behavioral attribute. BCA promotes biometric-based information sharing and enhances mission critical collaboration among and across government agencies, such as law enforcement, homeland security, national defense, and civil service organizations, not only for high-security applications, but also for high-volume services that have a strong identity requirement. The success of any technology depends on various factors that relate to its implementation in the wider context. The holistic approach enables the integration of business intelligence, process management, activity monitoring, and corporate performance management to achieve a single view of enterprise with a better fit between them [33, 34]. It is necessary to focus GoC biometric efforts into a common architecture to create a more unified cross-government biometric capability. A holistic approach to biometrics will enable government agencies to meet the following challenges:

9. Improving public safety

   Anonymity provides insurgents or terrorists with protection and operational advantage. It has been successfully proved that the use of biometrics strips away this anonymity. Using biometric data to screen entrants to our country will reduce the risk of unknown individuals, who have been involved in criminal or terrorist activities. Biometric matching will bring us the added value under a new and deeply interconnected national security

environment. Enterprise solution will enhance the government capability to collect, store, analyze, and share biometrics to identify and screen persons who may pose a threat to national security.

10. Safeguarding borders while encouraging travel and trade

    Around the world, more and more governments are using biometrics to improve their border security by deterring or detecting the passenger travelling with a false identity. Combined with airline and airport processes to streamline aviation operations, biometrics can help governments enhance border security and facilitate the lives of ordinary business travelers and tourists. In addition, using biometric technologies can free up valuable and skilled resources to focus on more strategic border control tasks. The use of biometric technology has changed the focus of border security management from merely processing people to higher-value, intelligence based activities focused on persons of interest.

11. Reducing identity theft

    Identity theft refers to all types of crime in which a stolen identity is used to commit certain criminal acts, typically for economic gain. To address this challenge, several governments are starting to develop national electronic identification (National e-ID) systems. Integrated identity management through e-ID offers a variety of benefits for individuals, businesses and governments. Not only can systems help reduce identity theft, but also enable individuals to use online applications more securely [35].

12. Enabling the secure delivery of government services to citizens

    When sharing biometric data across government departments, it will also make a profound impact on social benefits and government services, such as welfare payments, working compensation benefits, driver's licenses. It was reported that “benefits going to individuals who are not entitled to receive them are a significant cost to governments and ultimately to the people of Canada and the United States [36].

The purpose of the Biometrics Enterprise Architecture is to establish the foundation from which evolution of the Biometrics Enterprise can be explicitly understood and modeled. But in order to build a common architecture for a unified GoC biometric capability, there is a need to establish a biometrics working group in which each stakeholder is represented. There is a need to achieve strategic realignment of GoC biometric projects, provide biometric capabilities across the government departments, and deal with system interoperability and biometric information sharing issues through programmatic efforts, policy, and standards.

In general, an Enterprise Architecture (EA) should connect with the GoC’s strategic plan through program and system solutions by providing the operational and technical information needed to guide and constrain implementable investments in a consistent, coordinated, and integrated fashion.

5 Conclusions and recommendations

From law enforcement to national security, biometrics is gradually making its way into society. Recognizing the benefits of biometric technology, federal government departments, such as CBSA, CIC, DND, the RCMP, and others have initiated internal procedures to develop biometric systems to address national security and force protection requirements. What seems to be the case at the moment is that the various biometric programs within government lack an overarching strategy or policy that could lead to the development of a whole of government capability and bring synergy to the table. Before going too far along that road, however, it is necessary to gain an understanding of the current architecture, design an "ideal" architecture that would be able to meet the requirements for national security, and use the difference between these two states to define the work that needs to be done so that S&T investments can be prioritized.

With biometrics expertise in government and through collaboration with academia and industry, it is possible to develop a biometrics road map that could address the government requirements. We propose the following eight recommendations as the most important ones to be considered in the road map development:

13. Survey and analysis the current government-wide biometric programs, systems, and future plans in terms of advantages and limitations

14. Study the experience and lessons learned from the others, such as the US and UK government biometric programs, to ensure high-quality, low-cost, and effective solutions

15. Perform gap analysis to help strengthen existing biometric systems

16. Look into current operations and make recommendations to the Executive to get support on further architectural developments

17. Launch inter-agency biometric activities to develop a cross-government policy to guide the biometrics community and practice

18. Identify new areas of opportunity by:

    d. responding to urgent government needs

    e. analyzing national security threats

    f. meeting technology changes

19. Leverage technology to reduce huge amount of time and resources wasted in inspection and re-inspection, and consider scaling, adoptability and interoperability issues

20. Determine the deployment strategy to ensure that all GoC biometrics requirements can be addressed

References

[1] "Biometrics in Corrections," *TechBeat*, http://www.justnet.org/Pages/TechBeatIssue.aspx?issue=Fall+2000, Fall 2000.

[2] "Corrections Biometric Management System," *Biometrics Newsletter 48*, Page 9, 3 December 2010.

[3] Turner, A. (2003). "Biometrics in Corrections: Current and Future Deployment." Corrections Today **65**(4): 62-64.

[4] "US-VISIT Biometric Identification Services," Homeland Security, http://www.dhs.gov/files/programs/gc_1208531081211.shtm, Modified on 18 March 2011.

[5] "International Use of Biometrics," *Citizenship and Immigration Canada*, http://www.cic.gc.ca/english/department/biometrics-international.asp, Modified: 2011-11-02.

[6] "U.K. Borders Agency in Immigration Biometrics Deal with IBM," *Homeland Security News Wire*, http://www.homelandsecuritynewswire.com/uk-borders-agency-immigration-biometrics-deal-ibm, 14 September 2010.

[7] "Caribbean Nations Share Biometric Border System," *Planet Biometrics*, http://www.planetbiometrics.com/article-details/i/475/, 27 January 2011.

[8] Fawzia Sheikh, "U.S. preparing to solicit bids on biometrics database in Afghanistan", *Inside the Pentagon*, http://www.biometrics.dod.mil/PublicAffairs/media.aspx, April 15, 2010, (Access date: 8 Sept. 2011).

[9] "Counter-trafficking scenario", *EUCOM Workshop*, http://www.paxpartnership.org/Knowledgebase/Attach/15-08%20-%20EUCOM%20Workshop%20Intro.pdf, June 21, 2010, (Access date: 7 Sept. 2011).

[10] "Real Time Identification (RTID)," *RCMP Fact Sheets*, http://www.rcmp-grc.gc.ca/factsheets/fact_rtid_e.htm, Content Revised: 2008-01-09.

[11] "Canadian Criminal Real Time Identification Services Newsletter," *CCRTIS Report*, Volume 2, Issue 1 - Winter 2010-2011, **http://www.rcmp-grc.gc.ca/cr-cj/report-rapport/2010-2011-eng.htm**.

[12] "CANPASS Air," *Canada Border Services Agency*, http://cbsa-asfc.gc.ca/publications/pub/bsf5017-eng.html, Date Modified: 16 April 2007.

[13] Helen Lee, "Iris recognition", http://imps.mcmaster.ca/courses/SE-4C03-07/wiki/leehk5/Iris_recognition.html, Modified: 4 April 2007.

[14] Allan Swift, "Canada Joins Move to Electronic Passports to Improve Security," http://www.airportbusiness.com/article/article.jsp?id=3721&siteSection=5, 30 September 2005.

[15] Richard Bray, "It's A Match," *Bnet*, http://findarticles.com/p/articles/mi_qa3993/is_200610/ai_n17194493, Oct. 2006.

[16] Lalita Acharya and Tomasz Kasprzycki, "Biometrics and Government," http://www.parl.gc.ca/Content/LOP/ResearchPublications/06-30-e.htm, 16 April 2010.

[17] E-Passport Coming in 2012," http://www.todayswindsor.com/4181, *Today's Windsor*, 23 September 2011.

[18] "Citizenship and Immigration Canada Begins Biometrics Field Trial," *Citizenship and Immigration Canada Notice*, http://www.cic.gc.ca/EnGLIsh/department/media/notices/notice-trial.asp, Date Modified: 2007-05-31.

[19] Biometric Information Sharing Under the High Value Data Sharing Protocol," *Citizenship and Immigration Canada Operational Bulletin 226*, http://www.cic.gc.ca/english/resources/manuals/bulletins/2010/ob226.asp, 25 August 2010.

[20] "Biometrics Field Trial Evaluation Report," *Citizenship and Immigration Canada*, http://www.cic.gc.ca/english/resources/publications/biometrics-eval/section12.asp, Date Modified: 2011-04-26.

[21] Qinghan Xiao, "Multi-modal biometric system with web-based name search: User manual", *DRDC Ottawa TM 2010-226*, December 2010, (50 pages).

[22] Patrick Laytner, Chrisford Ling, and Qinghan Xiao, "A robust approach to detect faces from still images," will be submitted to *SIAM Conference on Imageing Science*.

[23] Sahnoune Dahel and Qinghan Xiao, "Accuracy performance analysis of multimodal biometrics", *Proc. of the 2003 IEEE Workshop on Information Assurance and Security*, pp.170-173, June 2003.

[24] Qinghan Xiao, "An approach to adaptive multimodal biometric fusion," in *Engineering Applications and Computational Algorithms*, Edited by Xinzhi Liu, Waterloo, Watam Press, pp.133-136, May 2003.

[25] Qinghan Xiao, "Using Fuzzy Adaptive Fusion in Face Detection," *Proc. of 2011 IEEE Workshop on Computational Intelligence in Biometrics and Identity Management*, pp. 157-162, 2011.

[26] Qinghan Xiao, "Fingerprints: Spoofing and Anti-Spoofing," *Proc. of the 4th International DCDIS Conference on Engineering Applications and Computational Algorithms*, pp. 652-657, July 2005.

[27] "Government of Canada Invests $2 Million to Bolster Canada's Safety and Security," *National Defence and the Canadian Forces*, http://www.forces.gc.ca/site/news-nouvelles/news-nouvelles-eng.asp?cat=00&id=2941, 6 April 2009.

[28] Jeffrey W. Seifert, "Federal Enterprise Architecture and E-Government: Issues for Information Technology Management," CRS Report for Congress, http://www.fas.org/sgp/crs/secrecy/RL33417.pdf, Updated 10 April 2008.

[29] "A Practical Guide to Federal Enterprise Architecture", *CIO Council*, February 2001.

[30] "Biometric Interoperability," *Facial Recognition Forum*, https://www.fbibiospecs.org/FacialRecogForum/Forum2/_Uploads/facial%20recog%20forum%20110211_1.pdf, 2 November 2011.

[31] James Goldstein, Rina Angeletti, Manfred Holzbach, Daniel Konrad, Max Snijder, "Biometrics Deployment Study: Identifying challenges and threats facing large-scale biometrics deployment in Europe," *EUR 23564 EN*, 2008.

[32] Reinhard Schmid, "International Biometrics Data Exchange: Prüm Solution as European Perspective and Beyond," *CIBRA 11*, http://www.biometria.gov.ar/media/71560/international_biometric_data_exchange_cibra_2011_11_final.pdf, 14-16 November 2011.

[33] Itiel Dror, "A Holistic-cognitive Approach for Success," *Biometric Technology Today*, July/August 2006.

[34] Pugna Irina Bogdana, Albescu Felicia, and Babeanu Delia "The Role of Business Intelligence in Business Performance Management," *Annals of Faculty of Economics*, Volume 4, Issue 1, pp. 1025-1029, 2009.

[35] Daniel Castro, "Explaining International Leadership: Electronic Identification Systems," *Information and Innovation Foundation*, http://www.itif.org/files/2011-e-id-report.pdf, September 2011.

[36] "Report on Identity Theft," *Public Safety Canada*, http://www.publicsafety.gc.ca/prg/le/bs/report-eng.aspx#back15, Date Modified: 2011-11-28.

List of symbols/abbreviations/acronyms/initialisms

BAT	Biometric Automated Toolset
CARICOM	Caribbean Community
CBMS	Corrections Biometric Management System
DND	Department of National Defence
DRDC	Defence Research & Development Canada
DRDKIM	Director Research and Development Knowledge and Information Management
FBI	Federal Bureau of Investigation
HIIDE	Handheld Interagency Identification Detection Equipment
ISAF	International Security Assistance Force
NIJ	National Institute of Justice
OST	Office of Science and Technology
PSTP	Public Security Technical Program
R&D	Research & Development
UK	United Kingdom
US-VISIT	United States Visitor and Immigrant Status Indicator Technology

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.)	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.)
Centre for Security Science, Defence R&D Canada, 222 Nepean St. 11th Floor, Ottawa, ON Canada K1A 0K2	UNCLASSIFIED NON-CONTROLLED GOODS DMC-A REVIEW:GCEC JUNE 2010

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Biometrics for National Security: The Case for a Whole of Government Approach:

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Meunier, Pierre; Xiao, Qinghan; Vo, Tien

5. DATE OF PUBLICATION (Month and year of publication of document.)	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.)	6b. NO. OF REFS (Total cited in document.)
June2013	28	36

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Centre for Security Science

Defence R&D Canada, 222 Nepean St. 11th Floor, Ottawa, ON Canada K1A 0K2

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.)

10a. ORIGINATOR'S DOCUMENT 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 CSS TM 2013-005	

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable
that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

The improvements of the last few years have not only made biometrics more reliable but they have made them also cheaper and more capable of handling high volumes of transaction, and thus more suitable for public safety and security applications. Several governments around the world are now using biometrics as means of verifying the identity of visa applicants and visitors or as a means of expediting the passage of trusted travellers across borders. The sphere of influence of biometric technologies extends well beyond border applications, however, and the prevalence of this technology is likely to increase not just in the public sector, but in the private sector as well.

The objective of this paper is to show the trends surrounding the use of biometrics to improve public safety and security and make the case for taking a holistic view of this capability so as to extract the greatest benefits in the most efficient and effective manner.

Les améliorations de ces dernières années ont non seulement rendu la biométrie plus fiable, mais elles ont également réduit son coût tout en augmentant sa capacité de traiter des volumes élevés de transactions, la rendant donc plus adapté aux applications de sécurité et sûreté publique. Plusieurs gouvernements à travers le monde utilisent la biométrie comme moyen de vérifier l'identité des demandeurs de visa et des visiteurs ou comme un moyen d'accélérer le passage des voyageurs dignes de confiance à travers les frontières. La sphère d'influence des technologies biométriques s'étend bien au-delà des applications frontalières, cependant, et la prévalence de cette technologie est susceptible d'augmenter non seulement dans le secteur public mais dans le secteur privé.

L'objectif de ce rapport était de montrer quelques-unes des tendances relatives à l'utilisation de la biométrie pour améliorer la sécurité et sûreté publique et de plaider pour une vue plus globale de cette capacité au sein du gouvernement afin d'en extraire le maximum d'avantages de la manière la plus efficiente et efficace.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Biometrics; identity management