Government of Canada Considerations for the Use of Cryptography in Commercial Cloud Services

Published: 2020-04-28

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT22-254/2020E-PDF
ISBN or ISSN: 978-0-660-34788-2

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Gouvernement du Canada Considérations relatives à l'utilisation de la cryptographie dans les services d'informatique en nuage commerciaux

Government of Canada | Gouvernement du Canada

Government of Canada Considerations for the Use of Cryptography in Commercial Cloud Services

From Treasury Board of Canada Secretariat

Date: September 3, 2019

On this page

1. Introduction

▼ **In this section**

1.1 Background

Cloud computing has introduced a fundamental shift in the way information system services are delivered, and the Government of Canada (GC) is positioning itself to use this alternative service delivery model. Cloud adoption will ensure that the GC can continue to sustain service excellence during a period of increased demand for online services and timely access to accurate information.

The adoption of cloud services will result in GC information being electronically transferred from data stores located on GC premises, where this information resides today, to commercial public cloud environments, where the information will be stored and accessed by users. The protection of information in electronic form will be accomplished through the implementation of data security, which includes the protection of the availability, integrity, and confidentiality of data at rest, in transit and in use.

Cryptographic data protection is a core component of the protection of information in electronic form; however, its implementation in cloud services can be a challenging endeavour. Cloud service providers (CSPs) offer several cryptographic capabilities and options that their consumers need to understand, enable and configure correctly.

Furthermore, when deploying their cloud-based services, GC departments and agencies must ensure that they comply with the cryptographic data protection requirements specified by the Treasury Board of Canada Secretariat (TBS) and the Communications Security Establishment (CSE).

1.2 Document purpose and scope

The purpose of this document is to help GC departments and agencies use cryptography to protect sensitive GC data in their cloud-based deployments.

The guidance provided in this document applies to:

- Protected A and Protected B GC data
- GC data that have a security category of low and medium for integrity

GC organizations must use this document in conjunction with the:

- Direction for Secure Use of Commercial Cloud Services: Security Policy Implementation Notice
- Government of Canada Cloud Risk Management Approach and Procedures
- Guidance on Cloud Service Cryptography (ITSP.50.106)

GC organizations also need to account for other implementation-specific considerations, including the:

- security category of the GC service being implemented
- proper alignment with enterprise architecture and enterprise security architecture
- solution requirements and constraints (for example, performance)
- threat mitigation objectives
- target residual risks

1.3 Audience

This document will be of value to:

- service delivery managers who are responsible for risks to the security of GC information
- chief information officers, other senior IT officials and IT security officials who are responsible for evaluating the suitability of information system products and services for GC use
- information management officers who are responsible for the lifecycle management of GC information
- information system practitioners and information system security practitioners who are responsible for implementing, operating and maintaining cloud-based GC services

2. Baseline requirements

▼ **In this section**

This section identifies the baseline cryptographic data protection requirements that GC organizations must consider for their cloud-based deployments.

2.1 Requirements

The requirements for cryptographic data protection in the GC are specified in Appendix B to the Treasury Board's *Directive on Security Management*. Subsection B.2.3.6.3 of Appendix B states the following:

> Use encryption and network safeguards to protect the confidentiality of sensitive data transmitted across public networks, wireless networks or any other network where the data may be at risk of unauthorized access.

However, these requirements are insufficient to appropriately protect sensitive GC data in commercial cloud services. Sensitive GC data must be encrypted to protect both the data's confidentiality and integrity in the cloud while they are in transit, at rest and in use. These additional data protection requirements are:

- specified in GC cloud security control profiles
- taken into account in this document

At the time of writing, there were no practical implementations for the cryptographic protection of data in use. See Appendix D for more information on the protection of data in use that are stored in cloud services.

2.2 Cryptographic algorithms

GC organizations must use CSE-approved cryptographic algorithms and protocols in their cloud-based deployments, as outlined in:

- CSE's ITSP.40.111 Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information
- CSE'S ITSP.40.062 Guidance on Securely Configuring Network Protocols

For assurance purposes, in ITSP.40.111, CSE recommends using cryptographic modules that have been validated under the Cryptographic Module Validation Program for compliance with the US National Institute of Standards and Technology's (NIST) Security Requirements for Cryptographic Modules (FIPS 140-2).

2.3 Baseline security controls

Table 1 lists the security controls and security control enhancements for the cryptographic protection of GC data that are selected in the Government of Canada Cloud Security Control Profile for Cloud-based GC Services. These security controls and security control enhancements form the baseline for the protection of GC data up to and including Protected B, medium integrity and medium availability (PBMM).

Table 1: baseline security controls and security control enhancements for the cryptographic protection of GC PBMM data

Security control ID	Title	Related recommended values
AU-2	Audit events	(D) Auditable events (or a subset thereof) with the frequency of auditing or for the reason for auditing to be defined as part of the tailoring process
AU-12	Audit generation	(A) Components are all information system and network components where audit capability is deployed or available (B) Personnel or roles are to be defined as part of the tailoring process
IA-7	Cryptographic module authentication	This security control has no organizational parameters. Recommended values not applicable.
SC-8(1)	Transmission confidentiality and integrity	Prevent unauthorized disclosure of information and detect changes to information

Security control ID	Title	Related recommended values
SC-12	Cryptographic key establishment and management	CSE-approved cryptography
SC-12(1)	Cryptographic key establishment and management: Availability	This security control has no organizational parameters. Recommended values not applicable.
SC-12(2)	Cryptographic key establishment and management: Symmetric keys	CSE-compliant
SC-12(3)	Cryptographic key establishment and management: Asymmetric keys	CSE-approved key management technology and processes
SC-13	Cryptographic protection	CSE-compliant cryptography according to the CSE's cryptographic algorithms for unclassified, Protected A and Protected B information (ITSP.40.111)
SC-17	Public key infrastructure certificates	Medium assurance policy
SC-28(1)	Protection of information at rest: Cryptographic protection	As defined for deployment, but the security category is not to exceed medium for confidentiality and integrity

3. Key management

▼ **In this section**

3.1 Key management system

GC organizations must implement a key management system for the cryptographic protection used in their cloud-based services. Failure to adequately manage encryption keys can lead to a range of administrative and security problems including the loss of critical data. Considerations for the management of encryption keys include:

- where and how keys are generated and stored
- how keys are distributed and protected
- how keys and data are recovered if they become lost
- when and how keys are destroyed

CSE recommends that GC organizations follow the guidance and recommendations in the following publications to implement key management systems:

- Guidance on Cloud Service Cryptography (ITSP.50.106)
- NIST Special Publication 800-57, Part 1, Revision 4, *Recommendation for Key Management*, Part 1: General
- NIST Special Publication 800-57, Part 2, Revision 1, *Recommendation for Key Management*, Part 2: Best Practices for Key Management Organizations
- NIST Special Publication 800-57, Part 3, Revision 1, *Recommendation for Key Management*, Part 3: Application-Specific Key Management Guidance
- NIST Special Publication 800-130, *A Framework for Designing Cryptographic Key Management Systems*

- NIST Special Publication 800-152, *A Profile for US Federal Cryptographic Key Management Systems*

Related controls: SC-12, SC-12(1), SC-12(2), SC-12(3).

3.2 Key management models

Table 2 describes 3 key management models and some considerations when determining which model to select. GC organizations should consult ITSP.50.106 to determine which key management model is best suited for their cloud-based deployments.

Table 2: key management models

Identifier	Key management model	Description	Considerations
KM-1	Model 1: keys controlled by the CSP	Under this model, the CSP is responsible for all key management operations using its own equipment. GC organizations would typically select a data protection service or options and the CSP would do the rest.	• GC organizations must use the cryptographic capabilities of the cloud service. • The CSP has the ability to access the cryptographic keys and decrypt the data. • Any copy of the encrypted data made by the CSP for replication or backup purposes must also be encrypted. • Protecting data integrity requires specific cryptographic modes of operation (for example, cipher block chaining (CBC) and galois/counter mode (GCM)).
KM-2	Model 2: keys managed by the GC organization	Under this model, GC organizations would use a CSP's cryptographic data protection capabilities, but the organizations would be responsible for managing their own keys.	• GC organizations must manage their own keys. • GC organizations must ensure a secure process to transfer existing keys to the CSP's environment. • The CSP has the ability to access the cryptographic keys and decrypt the data. • Protecting data integrity requires specific cryptographic modes of operation (for example, CBC-GCM). • Any copy of the data made for replication or backup purposes must also be encrypted. • This model may limit the CSP's ability to provide data management services (for example, data migration).

Identifier	Key management model	Description	Considerations
KM-3	Model 3: keys controlled by the GC organization	Under this model, GC organizations would manage their own keys using their own cryptographic capabilities conducted on their own premises. The organizations would upload keys to their cloud service environments.	• GC organizations must have cryptographic capabilities on their premises. • GC organizations must manage their own keys. • The CSP has no access to the cryptographic keys. • Protecting data integrity requires specific cryptographic modes of operation (for example, CBC-GCM). • Any copy of the data made for replication or backup purposes must also be encrypted. • This model may limit the CSP's ability to provide data management services (for example, data migration). • This model may limit the functionality of a cloud service (for example, with O365, no search, no web viewers, no pivoted views, no anti-malware, no anti-spam, no eDiscovery). • Depending on the organization's network bandwidth capacity, this model may reduce performance.

3.3 Hardware security module

A hardware security module (HSM) is a hardware device that protects and manages cryptographic keys for strong authentication. The functions of an HSM that are relevant to this document are secure cryptographic key generation, key storage and key management.

The use of HSMs enhances the security aspects of key management, enabling the effective protection of cryptographic keys throughout their lifecycle.

3.4 Key management responsibilities

Whether the CSP or the GC organization is responsible for key management depends on which key management model is selected. GC organizations must be aware of the distribution of responsibilities under each model to ensure that they correctly satisfy the security controls of the GC PBMM cloud profile.

Under models 1 and 2, a GC organization relinquishes all or some control over key management operations to the CSP. Model 1 requires no investment on the GC side because the CSP controls all key management operations in the cloud service environment and model 2 requires some investment on the GC side.

Under model 3, a GC organization has full control of key management operations except during use, which occurs in the public cloud environment. Model 3 requires an investment in people, processes and technology on the GC side in order to implement and maintain the key management capability.

When selecting an underlying CSP for a specific cloud-based GC service, GC organizations must consider:

- the key management models that are available
- the advantages, disadvantages and risks associated with each model

GC organizations must also ensure that they correctly implement the key management operations that they are responsible for.

The key management operations that GC organizations may be responsible for are described in Table 3. For full coverage of a key's lifecycle, key management operations were selected from the following sources:

- NIST Special Publication 800-57
- CSE ITSP.40.111
- Open Web Application Security Project (OWASP) Key Management Cheat Sheet

The distribution of key management responsibilities for each of the key management models are provided in Appendix B.

Table 3: key management operations

Name	Description	Tracing to sources		
		NIST SP 800-57	**ITSP.40.111**	**OWASP**
Generation	No definition provided in NIST SP 800- 57, ITSP.40.111 or OWASP. NIST identifies this operation as a component of key establishment.	Generation	Generation	Generation
Distribution	Transport of a key and other keying material from an entity that either owns or generates the key to another entity that intends to use the key (source: NIST SP 800-57).	Distribution	Dissemination	Distribution
Storage	No definition provided in NIST 800-57, ITSP.40.111 or OWASP.	Storage	Storage	Storage
Use	No definition provided in NIST 800-57, ITSP.40.111 or OWASP.	Usage	Not explicitly stated	Usage
Change	No definition provided in NIST 800-57, ITSP.40.111 or OWASP.	Change	Replacement	Not explicitly stated
Backup	A copy of information to facilitate recovery during the crypto-period of the key, if necessary (source: NIST SP 800-57).	Backup	Not explicitly stated	Escrow and backup
Recovery	Mechanisms and processes that allow authorized entities to retrieve or reconstruct keying material from key backup or archive (source: NIST SP 800-57).	Recovery	Not explicitly stated	Recovery
Accountability and audit	A property that ensures that the actions of an entity may be traced uniquely to that entity (source: NIST SP 800-57).	Accountability and audit	Not explicitly stated	Accountability and audit
Archive	To place information into long-term storage (source: NIST SP 800-57).	Archive	Archival	Not explicitly defined
Destruction	To remove all traces of keying material so that it cannot be recovered by either physical or electronic means (source: NIST SP 800-57).	Destruction	Destruction	Destruction

3.5 Related security controls and mechanisms

Using the tables in Appendix B and Appendix C, GC organizations can identify the security controls and mechanisms that are related to key management that they need to implement.

4. Implementation considerations

▼ **In this section**

4.1 Use cases

One of the key security considerations when planning the implementation of a cloud-based GC service will come from the cryptographic use cases. The more common of these use cases include:

- protect data at rest in the cloud
- protect data at rest on a virtual disk
- protect data in transit between a cloud-based GC service and external users (for example, citizens)
- protect data in transit using a private, dedicated connection
- protect cloud service management data in transit using a private, dedicated connection
- process encrypted data in the cloud

Appendix D provides implementation considerations for each of these cryptographic use cases along with deployment examples and a list of the prescribed security controls.

4.2 Security control dependencies

While this document covers the set of security controls that are prescribed for the cryptographic protection of sensitive GC data, cryptography alone is insufficient to appropriately protect data while it is in transit, at rest and in use in information systems. GC organizations therefore need to rely on the correct implementation of other prescribed security controls to ensure appropriate protection. These security controls include without limitations:

- the security categorization of GC data
- the identification and authentication of users and processes
- the enforcement of access authorizations based on separation of duties and least privilege
- the protection of storage media
- the capability to respond to data breaches and other data-related incidents
- the capability to restore data in support of availability
- the logging, monitoring, and auditing of data access and use

4.3 System development lifecycle

GC organizations need to implement cryptography in commercial cloud services according to their departmental system development lifecycle (SDLC) process. CSE provides guidance on the SDLC process in Annex 2 of ITSG-33.

4.4 Encryption keys in shared resources

The distribution of responsibility matrix in Appendix B shows that, within cloud environments, the use of encryption keys remains under the control of CSPs in all 3 key management models. While in use in public cloud environments, encryption keys are exposed to compromise in shared hardware resources through various attack methods. The risks associated with these threats were assessed in the TBS position paper entitled *GC Cloud*

Initiative: Rationale for the Protection Against Exploits of Shared Resources (accessible only on the Government of Canada network). The results show that the expected residual risks from these types of threats fall within the threat protection objectives of the GC PBMM cloud profile.

4.5 Crypto-shredding attacks

Having GC data encrypted at rest in public cloud environments exposes the data to crypto-shredding attacks. In a crypto-shredding attack, a threat actor deletes data by deleting or overwriting the encryption keys under which the data is encrypted. Regardless of the key management model, GC organizations need to consider this threat and, if it is relevant to their cloud-based GC deployment, they need to ensure that the CSP or the GC organization maintains appropriate backup copies of the encryption keys to enable recovery.

4.6 Multi-cloud deployments

At the time of writing, it was not entirely clear whether data encrypted with keys managed by CSPs can be ported from one cloud environment to another cloud environment. GC organizations should consider the portability of encrypted data in their multi-cloud GC service deployments.

Appendix A: definitions

accountability and audit
Accountability refers to a property that ensures that the actions of an entity may be traced uniquely to that entity (source: US National Institute of Standards and Technology (NIST) SP 800-57).

Note: A definition of audit in the context of cryptography could not be found. In the International Standards for the Professional Practice of Internal Auditing, the Institute of Internal Auditors defines **internal audit activity** as an activity that "helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and control processes." Based on that definition, audit in the context of cryptography can be defined as an evaluation of the effectiveness of cryptographic procedures, especially key management procedures.

archive
To place information into long-term storage (source: NIST SP 800-57).

cloud-based GC service
An application or IT service that a GC department implements and operates using a cloud service (source: SPIN 2017-01).

cloud service provider (CSP)
A non-federal government organization that offers cloud services to the public and/or to the government as part of a business venture, typically for a fee with the intent to make a profit (source: SPIN 2017-01).

commercial cloud service
A CSP's product or service offering (source: SPIN 2017-01).

consumer-controlled keys
Encryption keys that are generated and managed by the consumer using capabilities that they have on their premises or a combination of capabilities that they have in the cloud and on their premises.

consumer-managed keys
Encryption keys that are generated and managed by the consumer using CSP capabilities.

cryptographic algorithm

A well-defined computational procedure that takes variable inputs, including a cryptographic key, and produces an output (source: NIST SP 800-57).

cryptographic module
The set of hardware, software and firmware that:
- implements cryptographic security functions (including cryptographic algorithms and key generation)
- is contained within the cryptographic boundary (source: ITSP.40.111)

cryptography
The discipline that treats the principles, means and methods for making plain information unintelligible. It also means reconverting the unintelligible information into intelligible form (source: ITSP.40.111).

CSP-controlled keys
Encryption keys that are generated and managed entirely by CSP capabilities.

data at rest
Data that is stored in persistent storage.

data in transit
Data that is being transferred over a private or public network.

data in use
Data that is stored in non-persistent storage, such as random access memory (RAM) and central processing unit (CPU) caches and registries.

infrastructure as a service (IaaS)
The capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications (source: NIST SP 500-292).

key backup
A copy of information to facilitate recovery during the crypto-period of the key, if necessary (source: NIST SP 800-57).

key destruction
The removal of all traces of keying material so that it cannot be recovered by either physical or electronic means (source: NIST SP 800-57).

key distribution
The transport of a key and other keying material from an entity that either owns or generates the key to another entity that is intended to use the key (source: NIST SP 800-57).

key establishment
The process by which cryptographic keys are securely established among cryptographic modules using manual transport methods (for example, key loaders), automated methods (for example, key-transport and/or key-agreement protocols), or a combination of automated and manual methods (source: NIST SP 800-57).

key generation
NIST identifies this operation as a component of key establishment.

key management
1) The set of mechanisms and procedures for generating, disseminating, replacing, storing, archiving and destroying keys that control encryption processes (source: ITSP.40.111).
2) The activities involving the handling of cryptographic keys and other related security parameters (for example, initialization vectors) during the entire lifecycle of the keys, including their generation, storage, establishment, entry and output, use and destruction (source: NIST SP 800-57).

key recovery
The set of mechanisms and processes that allows authorized entities to retrieve or reconstruct keying material from the key backup or archive (source: NIST SP 800-57).

platform as a service (PaaS)
The capability provided to the consumer to deploy onto the cloud infrastructure applications that are consumer created or acquired using programming languages and tools supported by the provider (source: NIST SP 500-292).

software as a service (SaaS)
The capability provided to the consumer to use the CSP's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface, such as a web browser (for example, web-based email) (source: NIST SP 500-292).

Appendix B: distribution of responsibility matrix for key management operations

The distribution of responsibilities in the matrix below is structured according to the following process areas:

- Capability: The processes of implementing and maintaining the key management operation capability. The capability may be implemented by the cloud service provider (CSP) in the cloud service environment or on the premises by the consumer.
- Management: The processes of configuring the key management capability (where applicable) and manually invoking the key management operation. If the key management operation is invoked automatically, then it falls under the capability process area.
- Assessment: The process of assessing the implementation of the capability or the management process as part of security assessment and authorization.

The consumer is the GC organization that uses or relies on the cloud service.

The matrix refers to 2 types of security assessment:

- the Canadian Centre for Cyber Security (CCCS) security assessment, which the CCCS conducts as part of the GC cloud risk management procedures according to ITSP.50.100
- security assessments conducted by GC organizations according to their departmental security assessment and authorization process

Table B1: distribution of responsibility matrix for key management operations

Key management operation	Key management responsibilities								
	Model 1 (CSP-controlled keys)			Model 2 (consumer-managed keys)			Model 3 (consumer-controlle		
	Capability	Management	Assessment	Capability	Management	Assessment	Capability	Management	Ass
Generation	CSP	CSP	CCCS	CSP	Consumer	Capability: CCCS Management: Consumer	Consumer	Consumer	Con
Distribution	CSP	CSP	CCCS	CSP	CSP	CCCS	Consumer	Consumer	Con
Storage	CSP	CSP	CCCS	CSP	CSP	CCCS	Consumer	Consumer	Con

1 The consumer may have the ability to view audit records for cryptographic operations that are related to their subscription.

Key management operation	Key management responsibilities								
	Model 1 (CSP-controlled keys)			Model 2 (consumer-managed keys)			Model 3 (consumer-controlle		
	Capability	Management	Assessment	Capability	Management	Assessment	Capability	Management	Ass
Use	CSP	CSP	CCCS	CSP	CSP	CCCS	CSP	CSP	CCC
Change	CSP	CSP	CCCS	CSP	Consumer	Capability: CCCS Management: Consumer	Consumer	Consumer	Con
Backup	CSP	CSP	CCCS	CSP	Consumer	Capability: CCCS Management: Consumer	Consumer	Consumer	Con
Recovery	CSP	CSP	CCCS	CSP	Consumer	Capability: CCCS Management: Consumer	Consumer	Consumer	Con
Accountability and audit	CSP	CSP [1]	CCCS	CSP	Consumer	Capability: CCCS Management: Consumer	Consumer	Consumer	Con
Archive	CSP	CSP	CCCS	CSP	Consumer	Capability: CCCS Management: Consumer	Consumer	Consumer	Con
Destruction	CSP	CSP	CCCS	CSP	Consumer	Capability: CCCS Management: Consumer	Consumer	Consumer	Con

1 The consumer may have the ability to view audit records for cryptographic operations that are related to their subscription.

Appendix C: implementation responsibility matrix for related security controls and mechanisms

Notes:

1) A loose mapping of key management operations is included to help GC organizations link security controls and mechanisms to the distribution of responsibility matrix in Appendix B. Not applicable indicates that the security control may not extend to the key management operation because, for example, it is fully automated.

Table C1: implementation responsibility matrix

Related security controls		Security mechanisms to implement	Related key management operations							
Identifier	Title		Generation	Distribution	Storage	Use	Change	Backup	Recovery	A

Related security controls		Security mechanisms to implement	Related key management operations							
Identifier	**Title**		**Generation**	**Distribution**	**Storage**	**Use**	**Change**	**Backup**	**Recovery**	**A**
AC-5	Separation of duties	Configure access privileges for encryption key operations to enforce separation of duties	Applicable	Not applicable	Not applicable	Not applicable	Applicable	Applicable	Applicable	A
AC-6	Least privilege	Configure access privileges for encryption key operations to enforce least privilege	Applicable	Not applicable	Not applicable	Not applicable	Applicable	Applicable	Applicable	A
AU-2	Audit events	Configure audit events to include key management operations	Applicable	Applicable	Applicable	Not applicable	Applicable	Applicable	Applicable	N
AU-6	Audit review, analysis and reporting	Conduct periodic audits of key management operations	Applicable	Not applicable	Not applicable	Not applicable	Applicable	Applicable	Applicable	A
CM-2	Baseline configuration	Add the configuration items related to key management to the configuration database of the cloud-based GC service	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	A
CM-6	Configuration settings	Establish and document the configuration settings in accordance with the most restrictive mode	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	A

Related security controls		Security mechanisms to implement	Related key management operations							
Identifier	Title		Generation	Distribution	Storage	Use	Change	Backup	Recovery	A
IA-7	Cryptographic module authentication	Configure the authentication mechanism that meets the requirements of applicable GC legislation and TBS policies, directives and standards	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	A
SC-12	Cryptographic key establishment and management	Draw up a key management plan that addresses the key management operations according to the distribution of responsibility matrix Draw up key management procedures for those key management operations	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	A
SC-13	Cryptographic protection	Configure key management operations in accordance with applicable GC legislation and TBS policies, directives and standards	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	Applicable	A

Appendix D: implementation considerations for generic use case

The table below provides implementation considerations that are structured around a set of generic use cases for cryptographic data protection in cloud services.

Table D1: implementation considerations for generic use cases

Identifier	Title	Description	Implementation considerations	Deployment examples	Applicable security controls

Identifier	Title	Description	Implementation considerations	Deployment examples	Applicable security controls
UC-1	Protect data at rest in the cloud	A Government of Canada (GC) organization: • requires cryptography to protect the confidentiality and/or integrity of data stored in the cloud service • makes use of a commercial cloud service where data can be stored	• Applicable to infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) • Address data residency requirements as outlined in the Direction for Electronic Data Residency (IT Policy Implementation Notice (ITPIN 2017-02)) • Ensure that the cryptographic capabilities are enabled in the cloud service • Ensure that the cryptography is correctly and compliantly implemented, in alignment with the Communications Security Establishment's (CSE) ITSP.40.111 and ITSP.40.062 • Select an appropriate key management model as outlined in section 3.3 of this document • Review the cloud service provider's (CSP) operational procedures for any manually implemented key management operations as part of the GC cloud security assessment process • Establish operational procedures for all consumer-facing manual key management operations (as appropriate • Establish operational procedures for all manual key management operations (as appropriate)	• Documents stored in the cloud for access by or sharing with GC users or external users (for example, citizens) • Backups stored in the cloud • Cloud-based GC service (commercial off the shelf, government off the shelf, custom) where data will be stored in a database and accessible to GC users, external users or both • Cloud-based service where data will be stored outside Canada and accessed or used by GC users, external users or both • A GC service delivered on premises that will store data in the cloud • Import and export operations between components that are stored on premises and in the cloud • Data protection for physical transfer between CSPs or between a CSP and the consumer	AU-2, AU-12, IA-7, SC-12, SC-12(1), SC-12(2), SC-13, SC-28(1) If asymmetric cryptography is used:SC-12(3) and SC-17

Identifier	Title	Description	Implementation considerations	Deployment examples	Applicable security controls
UC-2	Protect data at rest in a virtual disk	A GC organization: • requires cryptography to protect the confidentiality and/or integrity of data stored in a virtual machine's (VM) virtual disk • makes use of a commercial cloud service where the organization can create and configure its own VMs	• Applicable to IaaS • Refer to UC-1 implementation considerations • Data is exposed in clear text outside of the virtual disk when the VM is running • Protecting data integrity requires specific cryptographic modes of operation (for example, CBC-GCM) • Data moved outside of the VM is not cryptographically protected	• Cloud-based GC service where data will be stored in a VM	AU-2, AU-12, IA-7, SC-12, SC-12(1), SC-12(2), SC-13, SC-28(1)
UC-3	Protect data in transit between a cloud-based GC service and external users (for example, citizens)	A GC organization: • requires cryptography to protect the confidentiality and/or integrity of data collected from or exchanged with external users (for example, citizens) • allows users to connect to the cloud-based GC service via public networks	• Applicable to IaaS, PaaS, SaaS • Ensure that the cryptography is correctly and compliantly implemented in alignment with CSE's ITSP.40.111 and ITSP.40.062 • Review the CSP's operational procedures for any manually implemented key management operations as part of the GC security assessment process for cloud • Establish operational procedures for consumer-facing manual key management operations	• Cloud-based GC service that will be accessed by external users	AU-2, AU-12, IA-7, SC-8(1), SC-12, SC-12(2), SC-12(3), SC-13, SC-17
UC-4	Protect data in transit using a private, dedicated connection	A GC organization: • requires cryptography to protect the confidentiality and/or integrity of data exchanged between the cloud service and GC users • makes use of a commercial cloud service where consumers can connect via a private connection	• Applicable to IaaS, PaaS, SaaS • Refer to UC-3 implementation considerations • Avoid deploying many site-to-site connections • Implement a dedicated, encrypted connection point for accessing the solution, or leverage centrally provided, dedicated connections, such as the GC Trusted Interconnection Points (GC-TIPs) or GC Cloud Access Points (GC-CAPs).	• Cloud-based GC service that will be accessed by GC users	AU-2, AU-12, IA-7, SC-8(1), SC-12, SC-12(2), SC-12(3), SC-13, SC-17

Identifier	Title	Description	Implementation considerations	Deployment examples	Applicable security controls
UC-5	Protect cloud service management data in transit using a private, dedicated connection	A GC organization: • requires cryptography to protect the confidentiality and/or integrity of management data exchanged between the cloud service, internal components, operators and administrators • makes use of a commercial cloud service where consumers can connect via a private connection	• Applicable to IaaS, PaaS, SaaS • Refer to UC-3 implementation considerations • Avoid deploying many site-to-site connections • Implement a dedicated, encrypted connection point for accessing the solution or use centrally provided, dedicated connections, such as GC-TIPs and GC-CAPs	• Cloud-based GC service accessed by GC cloud operators and administrators	AU-2, AU-12, IA-7, SC-8(1), SC-12, SC-12(2), SC-12(3), SC-13, SC-17
UC-6	Process encrypted data in the cloud	A GC organization requires cryptography to protect the confidentiality and/or integrity of data while it is being processed in the cloud.	• Applicable to IaaS, PaaS, SaaS • At the time of writing there are no practical implementations to protect data-in-use using cryptography, such as an implementation of a fully homomorphic encryption (FHE) scheme • Investigate options that are offered by the CSP (for example, data anonymization, data tokenization, hardware-level isolation) that could act as compensating measures • Review the security mechanisms implemented by the CSP to satisfy security control SC-4 (information in shared resources) as part of the GC process for assessing cloud security	n/a	To be defined

Date modified:
2019-12-06