Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

GUIDANCE ON CLOUD SERVICE CRYPTOGRAPHY

ITSP.50.106

May 2020

PRACTITIONER SERIES

Canada

FOREWORD

ITSP.50.106 Guidance on Cloud Service Cryptography is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). For more information or suggestions for amendments contact the Canadian Centre for Cyber Security's (Cyber Centre) Client Services team:

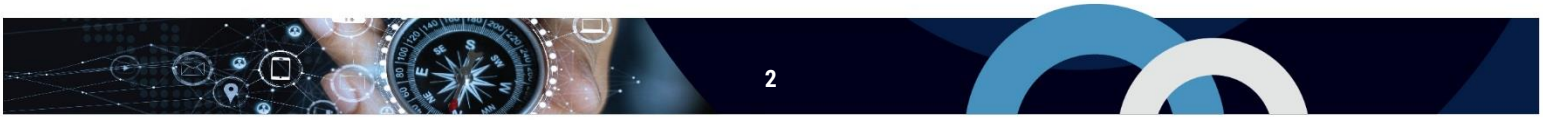
Cyber Centre Contact Centre
contact@cyber.gc.ca
613-949-7048 or 1-833-CYBER-88

EFFECTIVE DATE

This publication takes effect on May 20, 2020.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	May 20, 2020

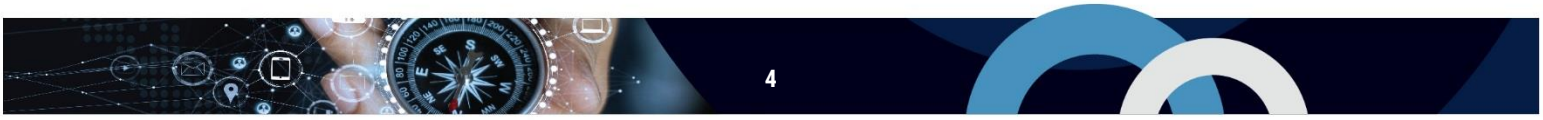


OVERVIEW

Cloud computing has the potential to provide your organization with flexible, on-demand, scalable, and self-service information technology (IT) provisioning. To deliver this potential, it is imperative that we address the security and privacy dimensions of cloud computing. Cryptography is one of the main pillars enabling security and privacy in cloud computing. It plays an essential role in enabling cloud services such as authentication, secure access to cloud workloads, secure data storage, and secure data exchange.

The objective of this security guidance document is to help your organization understand the cryptographic considerations for cloud computing. This document, and its appendices, reviews cryptographic concepts and use cases for cloud computing, provides guidance for key management, and provides cryptographic guidance for database workloads and endpoint devices.

TABLE OF CONTENTS



LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

With the growth of cloud services, the proportion of IT services that are implemented off premises and data that is stored outside of organizational boundaries continues to increase. As IT services and data are migrated to cloud systems, they are deployed based on a shared infrastructure and responsibility model and exposed to public endpoints. At the same time, new cloud-based services are enabling more decentralized capabilities such as the Internet of things, blockchain systems, and edge computing. When adopting cloud computing, your organization should require new approaches and protocols to secure the implementation and operation of business services, virtual entities, and protection of data. Cloud platforms rely heavily on cryptographic measures for secure delivery of cloud services.

While cryptography plays a critical role in cloud security, it can be quite complex to implement. Cloud platforms offer a large number of cryptographic services to cloud consumers. Understanding the various cryptographic service offerings, implementation approaches, protocols, ciphers, and key management options can be overwhelming. However, selecting the right approach and configuration to implement cryptography is important. Poor implementation, configuration, and management of cryptographic services and protocols may lead to serious flaws and ineffective protection of cloud-based services and data.

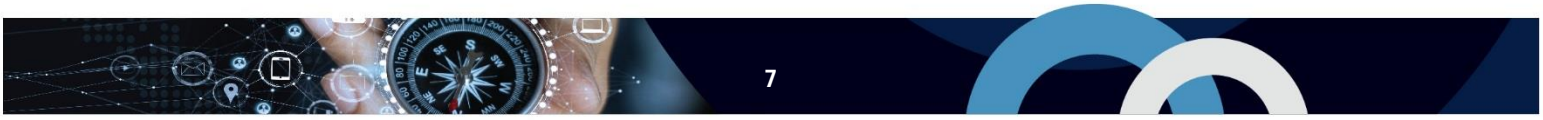
This publication provides guidance for applying and using cryptography in cloud-based services. This document is part of a suite of documents developed by Cyber Centre to help secure cloud-based services and provides your organization with important considerations for using cryptography as an effective measure to protect cloud-based services and data.

1.1 POLICY DRIVERS

The use of cryptography to protect cloud services is required to address several threats. The need for cryptography is normally identified in the security policies, directives, regulations, standards, and guidelines that are applicable to each organization. You can use the publications identified as reference material when incorporating cloud service cryptography in its security program:

- ITSP.40.111 *Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* [1][1];
- ITSP.40.062 *Guidance on Securely Configuring Network Protocols* [2];
- *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)* [3];
- ITSG-33 *IT Security Risk Management: A Lifecycle Approach* [4]; and
- *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5].

[1] Numbers in square brackets refer to resources that are cited in the Supporting Content section of this document.



1.2 APPLICABLE ENVIRONMENTS

The guidance in this document applies to both private and public sector organizations. The guidance can be applied to cloud-based services, regardless of the cloud service and the deployment models chosen.

1.3 RELATIONSHIP TO IT SECURITY AND CLOUD RISK MANAGEMENT

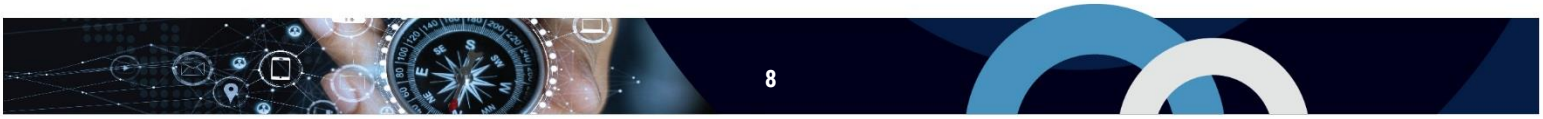
ITSG-33 [4] suggests two levels of IT security risk management activities that you can implement within your organization: the departmental level and the information system level.

You should integrate departmental-level activities[2] into your organization's security program to plan, manage, assess, and improve the management of IT security-related risks. At this level, cloud service cryptography is addressed by the definition of cryptographic security controls that is included in the security control profile.

You should integrate information system-level activities[3] into your information system development lifecycle.
These activities include the execution of information system security engineering, threat and risk assessment, security assessment, and authorization. The Cyber Centre's cloud security risk management approach is aligned with the information system-level activities outlined in ITSG-33 [4]. Figure 1 depicts the relationship of cloud services cryptography to the information system-level activities and the steps of the cloud security risk management approach. As depicted in Figure 1, step 5 of the cloud security risk management approach supports the implementation of cloud service cryptography.
You should establish the need for data encryption in step 1 (perform service categorization) of the cloud security risk management process and through the threat and risk assessment processes.

[2] Annex 1 of ITSG-33 [4] describes departmental-level activities in detail.

[3] Annex 2 of ITSG-33 [4] describes information system-level activities in detail.



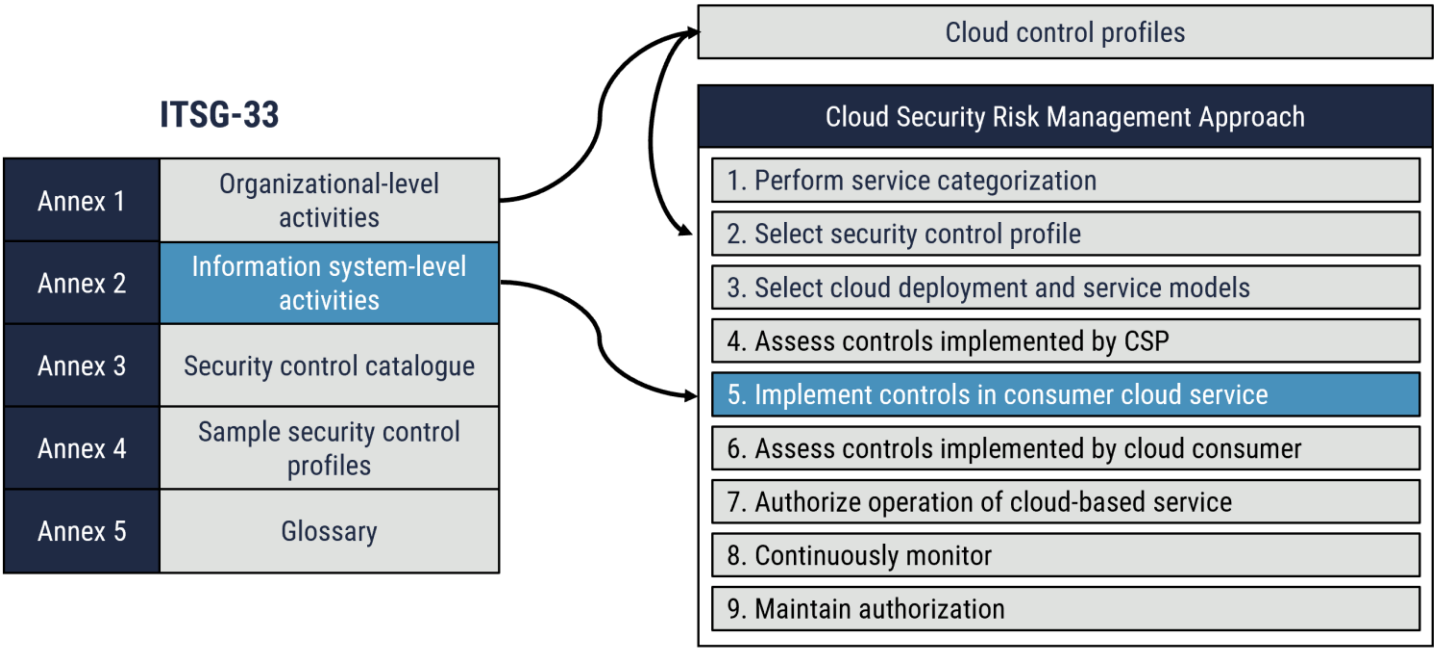


Figure 1: **Relationship of Cloud Service Cryptography to IT Security Risk Management**

2 CONTEXT

2.1 TYPICAL CRYPTOGRAPHIC FUNCTIONS

Your organization will face privacy and security challenges when adopting cloud computing. Using a shared pool of resources that are in remote and distributed locations and managed by a third party is not without risks. Cryptography plays a significant role in addressing these risks. It provides critical elements that support the confidentiality, integrity, availability, authentication, non-repudiation, and access control functions required to secure cloud platforms.

2.1.1 CRYPTOGRAPHY AND ENCRYPTION

Cryptography embodies the principles, means, and methods for transforming data to hide its original content, prevent unauthorized use, and prevent undetected modification.[4] Encryption is the cryptographic transformation of data into a form that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called decryption, which restores encrypted data to its original state.[5]

2.1.2 CONFIDENTIALITY

One of the main concerns of organizations when moving operations, services, or data to the cloud is the confidentiality of data. Encryption is a primary mechanism to ensure the confidentiality of data when it is in transit, at rest, and, in some cases, in use. When encryption is used, only authorized users have access to the data. Typical scenarios where encryption is used to ensure confidentiality of data include:

- protection of passwords during the authentication process;
- protection of data in transit when accessing cloud workloads;
- protection of authentication and authorization data between security domains (e.g. in federation of identity);
- protection of sensitive information on cloud storage, virtual disks, and databases;
- protection of cookies and assertion tokens;
- protection of data back-ups;
- sanitization of cloud storage media before it is released to the cloud service provider's (CSP) shared pool of resources;
- destruction of data at the end of life of the cloud storage media; and
- protection of logs.

[4] National Institute of Standards and Technology (NIST) *Computer Security Resource Centre Glossary* [6] entry for cryptography.

[5] NIST *Computer Security Resource Centre Glossary* [6] entry for encryption.

2.1.2.1 ENCRYPTION VS TOKENIZATION

While both encryption and tokenization are common approaches used to ensure confidentiality of data, they differ in several ways. In fact, it is not uncommon for the two approaches to be used together.

Encryption is based on mathematical algorithms that are used along with a secret key to convert clear text data into cipher text. The drawback to this method is that compromised key material may lead to the unauthorized disclosure of data.

Tokenization relies on a process in which sensitive data elements are substituted with non-sensitive equivalents, referred to as tokens, which have no extrinsic or exploitable meaning or value[6]. The resulting tokens and sensitive values are stored in a token database by a tokenization system, separate from the cloud applications. The original values are never stored with the applications, only the tokens. Since the cloud application only has access to tokens and not the sensitive values, it is usually exempt from regulatory audits. This approach contributes to considerable cost savings for organizations that are subject to regulations such as Payment Card Industry Data Security Standard (PCI DSS). Compromise of the tokenization database may lead to the unauthorized disclosure of data.

We have not established best practices and advice for using tokenization in cloud computing. Cloud consumers who want more information on the secure use of tokenization should consult existing guidance from the PCI Security Standard Council.

2.1.3 INTEGRITY

While it is crucial to ensure the confidentiality of information so that your organization can leverage cloud capabilities, information integrity can be equally, or more important. Your organization must ensure that transmission protocols address both the confidentiality and the integrity of data. When using cloud platforms, data transits network infrastructures outside of the cloud consumer's control. This includes data flows between on-premises and cloud environments, as well as data flows between cloud services. The storage infrastructure is also outside of the cloud consumer's control. The data may be subject to modification while in transit or storage, and your organization may not be able to determine if the data has changed. Modifications to data may be caused by system or software malfunction, human error, or unauthorized changes by threat actors. Cryptography provides the means to detect any unauthorized changes to data while it is in transit or storage.

Cryptography provides the data integrity function for digital certificates and the use cases identified in section 2.1.1. Confidentiality and integrity rely on different cryptographic mechanisms to meet their security objectives. The integrity function is generally accomplished via cryptographic hashes and digital signatures.

[6] As defined in the Wikipedia entry for tokenization. https://en.wikipedia.org/wiki/Tokenization_(data_security).

2.1.4 AUTHENTICATION

Cryptography plays an important role in authentication. It supports the authentication function at multiple levels in cloud computing, including the following examples:

- Signing certificates;
- Hashing passwords;
- Establishing a website identity;
- Authenticating application program interfaces (API) using cryptographic keys; and
- Protecting assertion tokens when using federation of identity.

Cloud consumers must ensure that the cryptographic functions and configurations used to support authentication on the CSP's cloud platform, and their cloud workload, is of sufficient strength. Using less secure protocols, hash functions, or ciphers lowers the trust that can be placed on the identity of resources, applications, and users and can severely impact the security of cloud deployments[7].

2.1.5 NON-REPUDIATION

The concept of non-repudiation is useful to prove that a specific transaction was completed by a specific user or cloud service. Non-repudiation is generally implemented via digital signatures and audit logs. For example, cloud computing often relies on the federation of identities. In the federation of identities, a verifier issues an assertion to establish the identity of a claimant to a relying party (RP). Such assertions will be protected against repudiation by the verifier, usually through a digital signature.

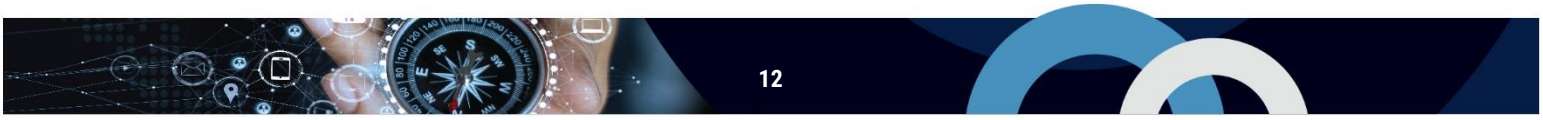
2.2 DATA IN TRANSIT, AT REST, AND IN USE

2.2.1 DATA IN TRANSIT

Data flows to, from, and within cloud environments through network infrastructures that are outside of the control of cloud consumers. Malicious threat actors can intercept this data and compromise its confidentiality and integrity. Your organization should ensure that data in transit is encrypted to secure communications to and from cloud environments.

While organizations control the infrastructure as a service (IaaS) perimeter, the communication patterns are likely to include information exchanges with cloud services outside of the perimeter. In addition, the location of instances involved in data transfers may be unknown. For example, cloud consumer virtual machine (VM) instances might be in different CSP data centres, and communications may flow on network infrastructure that is beyond cloud consumer and CSP control. As such, data communications within a cloud environment should be encrypted if any sensitive information is being exchanged.

[7] For a detailed description of cryptographic considerations for authentication function, readers should review *ITSP.30.031 V3 User Authentication Guidance for Information Technology Systems* [7].



While client-side encryption can be used before a data transfer is performed, we recommend using Hypertext Transfer Protocol Secure (HTTPS) for end-to-end encryption to ensure the integrity of the data[8]. Your organization should:

- configure cloud services to specify that only the HTTPS protocol can be used to access cloud storage services and APIs;
- disable and disallow weak encryption ciphers; and
- allow the use of other encrypted network protocols for application-specific use cases, such as server message block (SMB) for access to file storage.

2.2.2 DATA AT REST

Encryption at rest protects data that is stored on physical or virtual media. It protects data from unauthorized disclosure or modification and supports the overall defence-in-depth approach. While consumers and CSPs may have implemented controls at various levels to protect data, encryption at rest provides an extra layer of defence should other security measures fail.

It is highly recommended that encryption of data at rest is included in your organization's defence in depth strategy. Your organization should update its security policies to address the requirements for encrypting data at rest, and identify the classes of data that require encryption on cloud storage. Your organization should consider encrypting data at rest to protect the confidentiality and the integrity of data, VM images, VM snapshots, core dumps, applications, back-ups, and other important services and information.

In a multi-tenant cloud environment, encrypting data at rest is a way to further isolate data from other tenants and CSP personnel. Your organization may have to encrypt data at rest to meet industry, privacy, and government regulations. It may even be mandatory to meet certain regulatory and compliance requirements. In addition, encrypting data at rest enables your organization to sanitize data before storage resources are returned to the CSP's shared pool of resources (see section 3.4 for more information on crypto-shredding).

CSPs often enable object and file storage encryption by default. However, default configurations can change over time. Your organization should enforce data-at-rest encryption through baseline security configurations and continuous monitoring. The data encryption options identified in Figure 2 protect the confidentiality and the integrity of data against unauthorized access to physical media. However, not all these options will be effective against platform, operating system, or application compromises. Your organization should consider a number of factors when selecting its data-at-rest encryption strategy, including the type of storage, the environment (platforms, operating system, and application), the volume of information to be protected, and the threats that need to be mitigated. For example, platform as a service (PaaS) encryption options may vary from one platform to the other, while software as a service (SaaS) providers may use any of the options identified in Figure 2.

[8] For more information on cryptographic considerations for use of HTTPS, review ITSP.40.062 [2].

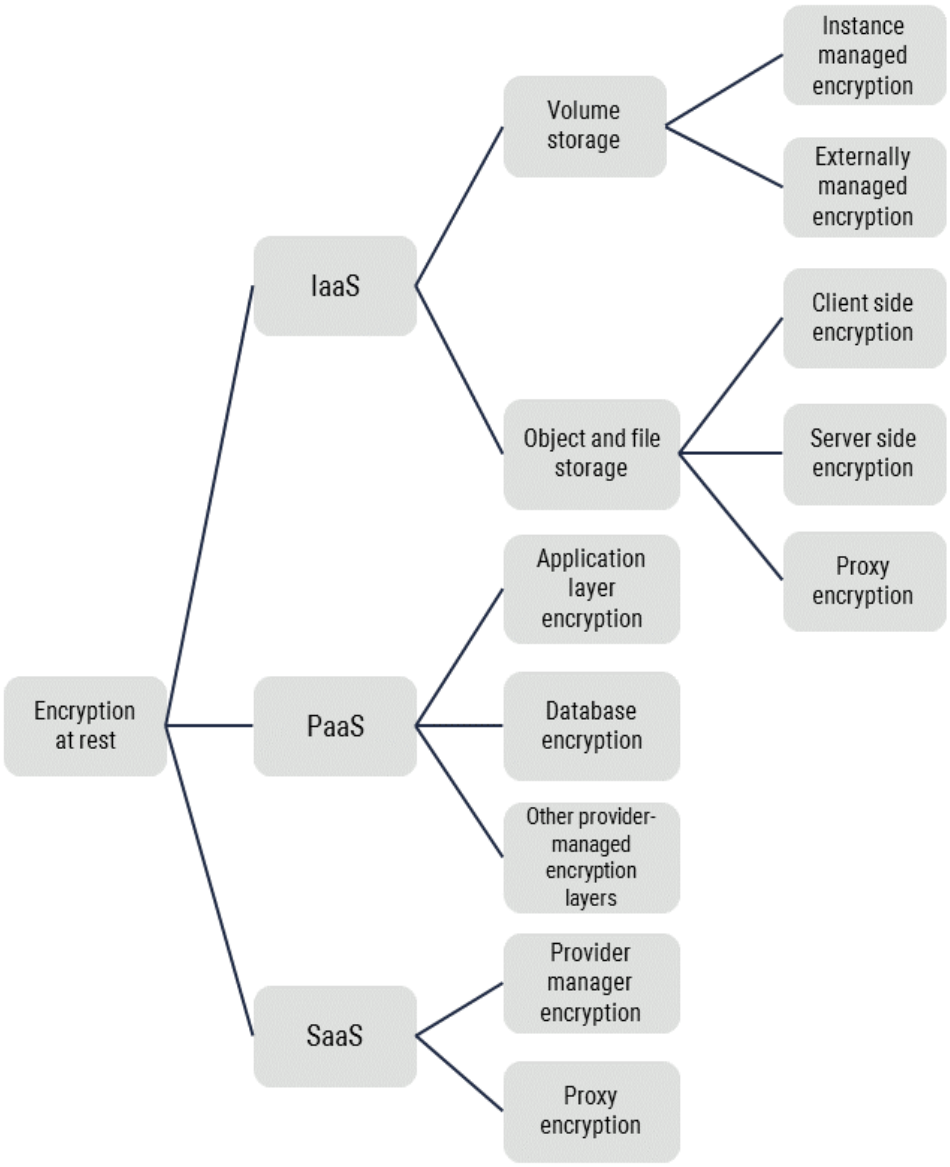


Figure 2: **Encryption Options**[9]

2.2.3 DATA IN USE

Data in use generally refers to data being processed by a computer's central processing unit (CPU) or in random access memory (RAM). While data can be encrypted at rest and in transit, generally, data must be decrypted before it is processed by cloud workloads. Third-party solutions exist, but we have not validated or assessed their implementations, and as such,

[9] These encryption options are based on Cloud Security Alliance's (CSA) *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0* [5].

these solutions may not provide the necessary level of assurance. Approaches used for data-in-use encryption are still considered relatively new technologies. Cloud consumers must carefully analyze the potential benefits (e.g. prevents data visibility), concerns (e.g. data could contain intellectual property), and risks (e.g. data could contain digital certificates) associated with data-in-use encryption before procuring, deploying, or using such solutions.

Since the processing of data in use is usually performed against unencrypted information, which in some cases could include cryptographic material, cloud consumers should ensure that VM snapshots, core dumps, and back-ups are adequately protected at rest. Barring sufficient physical protection in an in-house (on premises), private cloud, the best alternative for protecting VM snapshots is encryption. This can be achieved directly via cloud providers or third-party services.

2.3 SECURITY CONTROLS RELATED TO CLOUD CRYPTOGRAPHY

The Cyber Centre cloud control profiles included in *ITSP.50.103 Guidance on the Security Categorization of Cloud-Based Services* [7] identify several security controls that are related to the use of cryptography in cloud deployments. These related security controls are specified in table 1 below.

Table 1: Security Controls Related to Cloud Cryptography

Security Control ID	Title
AU-2	Audit Events
AU-12	Audit Generation
IA-3	Device Identification and Authentication
IA-3(1)	Device Identification and Authentication | Cryptographic Bidirectional Authentication
IA-5(2)	Authenticator Management | PKI-Based Authentication
IA-5(6)	Authenticator Management | Protection of Authenticators
IA-5(7)	Authenticator Management | No Embedded Unencrypted Static Authenticators
IA-7	Cryptographic Module Authentication
SC-8(1)	Transmission Confidentiality and Integrity
SC-12	Cryptographic Key Establishment and Management
SC-12(1)	Cryptographic Key Establishment and Management | Availability
SC-12(2)	Cryptographic Key Establishment and Management | Symmetric keys
SC-12(3)	Cryptographic Key Establishment and Management | Asymmetric keys
SC-13	Cryptographic Protection
SC-17	Public Key Infrastructure Certificates
SC-23	Session Authenticity
SC-28(1)	Protection of Information at Rest | Cryptographic protection
SI-7(1)	Software, Firmware, and Information Integrity | Integrity Checks

3 CRYPTOGRAPHIC GUIDANCE

3.1 RECOMMENDED CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

To be effective, cloud service cryptography relies on the strength of the keys, algorithms, ciphers, and protocols used throughout the key management lifecycle and operation. ITSP.40.111 [1] describes the approved cryptographic algorithms and the appropriate methods to protect the confidentiality and the integrity of information that is categorized up to the medium injury level.[10] Consumers should ensure that their cloud deployment model complies with the guidance found in ITSP.40.111 [1]. Cloud consumers must assess the CSP's implemented controls to ensure compliance with our guidance.[11] Your organization should carefully assess and set the associated cloud services' configuration settings.

Cloud consumers must also securely configure network protocols. ITSP.40.062 [2] addresses the following topics:

- Measures to securely configure network protocols to protect the confidentiality and the integrity of information to the medium injury level;
- Recommended algorithms for these network protocols; and
- References standards and NIST publications that provide additional information on these network protocols.

By following the guidance found in these two publications, your organization can be assured that your cloud deployments and your information is protected by cryptographic algorithms and protocols that are subjected to threat analysis, tested thoroughly against recognized standards by authoritative organizations, and are monitored for weakness over time. As weaknesses are identified in protocols and algorithms, government security agencies and standards organizations update their guidance to include more secure versions and implementation recommendations.

Brute force attacks against cryptography are not threats that need to be considered when using Cyber Centre-approved cryptographic algorithms. However, the following threats do need to be identified and mitigated in the security risk management process:

- Opportunistic attacks against implementation flaws;
- Unsecure integration of cryptography in applications and protocols;
- Weaknesses in the design, management, and operation of key management systems; and
- Coercion or bribery of trusted personnel who have access to cryptographic key material.

[10] Security categorization is the process of identifying the level of potential injuries that could result from compromises of business processes and related information. See ITSP.50.103 *Guidance on the Security Categorization for Cloud-Based Services* [8].

[11] *ITSP.50.105 Guidance on Cloud Security Assessment and Authorization* [9] describes an approach for assessing controls implemented by CSPs.

3.2 PROPRIETARY CRYPTOGRAPHIC ALGORITHMS AND PROTOCOLS

You should avoid cloud services that use proprietary algorithms and protocols and, as part of your security assessment of the CSP's security controls, your need to verify that these algorithms and protocols are not being used. Your organization should use Cyber Centre-recommended cryptographic algorithms and protocols. You should also use the configuration options for the cloud services to disable and disallow the use of proprietary cryptography.

Proprietary cryptography is defined as the use of algorithms, ciphers, and protocols that are kept secret. Vendors may use proprietary cryptography for different reasons. However, the rationale for using proprietary cryptography often includes the need for lightweight protocols, improved performance, and even improved security.

Usually, vendors do publicly release the details related to implementing proprietary cryptographic algorithms and protocols, or submit them to acknowledged authorities for evaluation. These details are not reviewed independently so the vendors do not benefit from feedback from the scientific community, standards organizations, or the worldwide community of IT security experts. If there are no independent reviews available, cloud consumers cannot be assured that the implemented protocols provide the required strength, are free of weaknesses, and do not contain any back doors. Threat actors can use these weaknesses, which may not be known to the vendor, to compromise the confidentiality, integrity, and availability of cloud-based services and data.

3.3 KEY MANAGEMENT OPTIONS FOR CLOUD SERVICES

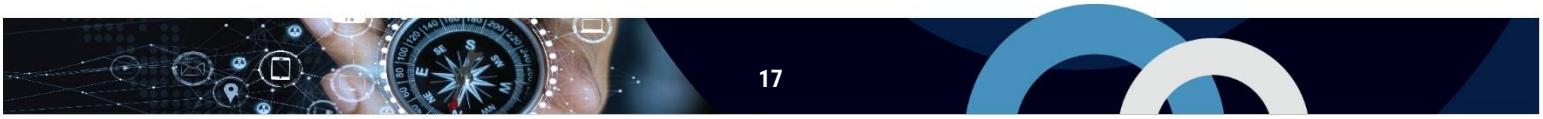
Key management is an important consideration in cloud service cryptography. It is a complex undertaking and should not be underestimated. Key management can be performed by the CSP or the cloud consumer. Key lifecycle management activities include generating, distributing, storing, revoking, recovering, and destroying encryption keys. An ineffective key management process puts the confidentiality, integrity, and availability of data at risk. Cloud consumers can refer to NIST *Special Publication 800-57 Recommendation for Key Management, Part 1: General (Revision 4*) [10] for guidance on developing an effective key management program.

Before assessing key management options and developing a key management strategy for cloud deployments, cloud consumers should consider the following:

- **Regulatory requirements and implications**: This may include requiring that a CSP key management solution meets PCI DSS compliance requirements[12] and privacy regulation requirements;
- **Data sovereignty and residency requirements and implications**: Cloud consumer data may be subject to the laws of other countries regardless of where the data is located. In such situations, a CSP with foreign operations could be required to comply with a warrant, court order, or subpoena request from a foreign law enforcement agency that is trying to obtain cloud consumer data.[13] When data is encrypted with keys that are managed by the CSP, the CSP may have to comply with a lawful order to provide access to client encryption keys and your organization's data;

[12] Organizations requiring PCI compliance should consult the *PCI DSS Cloud Computing Guidelines* [11].

[13] See Treasury Board of Canada Secretariat's (TBS) *Government of Canada White Paper: Data Sovereignty and Public Cloud* [12].



- **Protocols, interfaces and API requirements (e.g. Key Management Interoperability Protocol [KMIP])**: Cloud consumers may be using IT solutions that use KMIP to manage an application key and that may not support the API that was provided by the CSP for their key management service (KMS); and
- **Cloud service model**: Some cloud key management offerings only work with IaaS-based solutions, while others will work with all service models.

The right key management solution varies between organizations and depends on the criteria that is most important to the organization. There are three approaches to key management in cloud computing:

- Keys controlled and managed by the CSP;
- Keys controlled by the CSP and managed by the cloud consumer; and
- Keys controlled and managed by the cloud consumer.

If the keys are controlled by the CSP, it has access to the keys, even in situations where the keys are managed by the cloud consumer. For example, it is common for CSPs to provide their clients with a cloud KMS. In this example, the CSP has control over the KMS and can potentially access the keys to respond to requests from a foreign law enforcement agency.

Cloud consumers can use multiple key management models. Your organization may decide to secure most of its data using keys controlled by the CSP and then use keys that it controls and manages to protect highly sensitive data.

3.3.1 KEYS CONTROLLED AND MANAGED BY A CSP

If your organization has rigid compliance and regulatory requirements, we do not recommend this key management model, as it may not comply with the requirements identified by applicable oversight bodies.

Under this model, the CSP is responsible for all aspects of key management. These aspects include physical security, key management infrastructure and software, secure key storage, isolation from other tenants, and implementation of key management functions (e.g. access control and encryption). The CSP is also responsible for implementing the key management process. Typically, when subscribing to a cloud service, your organization configures the data protection options (e.g. storage, virtual disk, and database encryption), and the CSP takes care of key management.

For some SaaS and PaaS offerings, this key management model is the only option available. For example, a PaaS database offering may include configuration settings to encrypt data at rest and in transit, but it may not offer any means for the cloud consumer to manage the keys. Cloud consumers who require control or management of the keys should verify that the CSP offers these options.

This key management model is the easiest to implement. No additional configurations are needed, and the cloud consumer does not need to plan for the solution's capacity, performance, or scalability. However, the cloud consumer does not have control as to how and where the keys are stored and does not have visibility of the audit logs related to key access and operations.

3.3.2 KEYS CONTROLLED BY THE CSP AND MANAGED BY THE CLOUD CONSUMER

Under this model, consumers subscribe to the CSP's KMS, which is usually offered as part of their service offerings. The CSP KMS is implemented as a multi-tenant service. Access to the keys is generally provided through a web portal, command line interface, or API. A CSP KMS is integrated with the CSP Identity and Access Management system, as well as the auditing function and allows cloud consumers to manage and monitor access to key material.

A CSP-managed KMS is a convenient and inexpensive way for your organization to manage keys, secrets, and certificates. With this model, the cloud consumer controls the geographic locations where the keys are created and can meet data residency requirements. Note that the KMS and Hardware Security Module (HSM) services offered by many CSPs are not located in Canada.

Your organization shares responsibility with the CSP when using this key management model. The CSP is responsible for physical security, key management infrastructure, secure key storage, isolation from other tenants, and implementation of key management functions (e.g. access control and encryption). Your organization is responsible for implementing the key management process, as well as configuring the cloud services and applications to use the KMS to access the necessary keys. This key management model is more difficult to implement. If your organization wants to implement this key management model, ensure that you:

- have well-designed, documented, and tested key management processes;
- enable CSP-provided audit log functions for all access and actions taken on keys;
- restrict operations on keys according to the principle of least privilege; and
- use the CSP KMS to simplify its key management processes.[14]

Under this key management model, you have more control over the key management lifecycle. For example, if you suspect any unauthorized access or disclosure of information, you can revoke the keys you manage to prevent further data exfiltration.

In this key management model, the CSP controls the KMS and potentially has access to the keys that your organization manages. If the CSP has access to both the keys and the data, the CSP has the ability to decrypt data. Your organization can review and verify the processes and controls that the CSP has in place to prevent this possibility; however, the keys and the data could be exposed if the CSP must comply with a warrant, court order, or subpoena request from a foreign law enforcement agency.

This key management model can be applied to all service and deployment models. However, it is not supported by all PaaS or SaaS offerings.

[14] A CSP's KMS may not be available in all countries. Cloud consumers with data residency requirements should verify that the KMS is available and hosted in Canada.

3.3.2.1 BRING YOUR OWN KEYS (BYOK)

With BYOK, cloud consumers generate their own keys using on-premises key generation services or a third-party provider. The generated keys are typically stored on an on-premises HSM that is controlled by the cloud consumer. Once generated, the keys can be securely exported to a cloud KMS. The KMS can protect the keys using an HSM.

By implementing key usage policies, your organization can prevent a CSP from further exporting client encryption keys and using them outside of the cloud KMS. However, a CSP can access the keys that your organization has exported to the cloud KMS. While BYOK allows your organization to retain control of the keys that are stored on premises, once you export the keys to a cloud KMS, they are accessible by the CSP. For example, for the CSP storage service to be able to encrypt and decrypt data, the CSP must have access to the keys.

Compared to CSP generated keys, your organization may benefit in the following ways by using BYOK:

- Full control of key generation;
- More control of key lifecycle;
- Capability to revoke keys and prevent anyone from decrypting data that is encrypted with the key; and
- Protection from vendor lock-in, as they retain a copy of the key, and your organization can easily transition to another service provider.

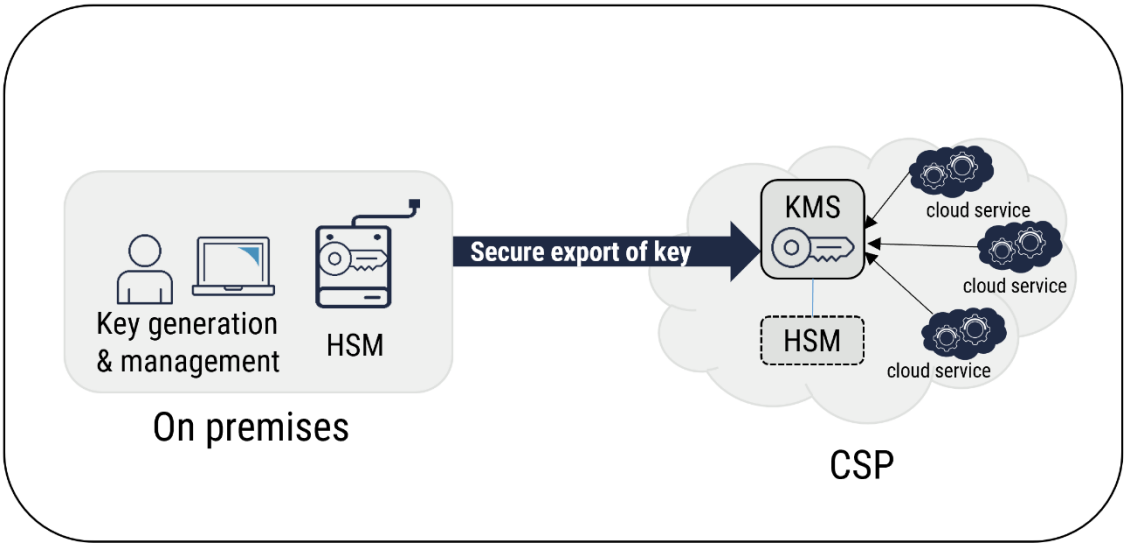


Figure 3: **BYOK Concept**

3.3.3 KEYS CONTROLLED AND MANAGED BY A CLOUD CONSUMER

If your organization has increased security requirements or is highly regulated, you may need to store data in the cloud while ensuring that it remains indecipherable to the CSP. In such scenarios, your organization must control and manage the keys. Approaches supporting this key management use case include the following:

- Subscription to dedicated cloud HSM services;
- Use of dedicated third-party gateways or a Cloud Access Security Broker (CASB); and
- Use of a third-party KMS.

This key management model provides the following advantages:

- Allows your organization to control who has access to data;
- Meets data residency requirements;
- Protects your organization from vendor lock-in; and
- Ensures consumer-controlled destruction of data by destroying the encryption keys.

The disadvantage of this key management approach is that some cloud services such as indexing, search, and data loss prevention are ineffective over encrypted data. Your organization is still subject to court orders and subpoenas, and you may have to provide data in such situations.

3.3.3.1 DEDICATED CLOUD HSM

An HSM is a physical computing device that safeguards and manages digital keys for strong authentication. An HSM also provides crypto-processing. The key material is stored in tamper-resistant and tamper-evident hardware modules, and applications are required to be authenticated and authorized before they can access the key material. The key material never leaves the HSM protection boundary.

Cloud HSM services generally provide a dedicated HSM to the cloud consumer[15]. The cloud consumer controls and manages all key operations on that HSM. Cloud HSMs are generally restricted to the IaaS mode, meaning that cloud consumers cannot use key material from cloud HSMs when using PaaS and SaaS offerings.

Some CSPs provide consumers with the capabilities to authorize the KMS to access a dedicated cloud consumer HSM[16]. The benefit of this approach is that cloud consumers can use PaaS and SaaS offerings while using a dedicated HSM for key storage. While this approach provides a cloud consumer with the flexibility to use PaaS and SaaS offerings, it is very similar to the BYOK. CSPs with foreign operations may access the keys to comply with a request from a foreign law enforcement agency who is trying to obtain cloud consumer data. As such, if your organization must maintain control of the keys, you should refrain from authorizing the CSP KMS to access your dedicated cloud HSM.

---

[15] Some dedicated HSMs are hosted on physical devices that are shared with other tenants.

[16] CSP HSMs may not be available in all countries. Cloud consumers with data residency requirements should verify that the CSP HSM is available and hosted in Canada.

3.3.3.2 CLOUD ENCRYPTION GATEWAYS (CEG) AND CASB

CEGs and CASBs act as proxies between a cloud consumer's on-premises networks and the cloud services. They are typically deployed on premises. CEGs and CASBs can intercept sensitive data and use tokenization and encryption techniques to obfuscate sensitive information before it is forwarded to the cloud for storage or processing. CEGs and CASBs can be integrated with cloud services by using secure APIs. With this integration, cloud consumers can control and manage the keys, encryption, and information protection policies. Sensitive data is obfuscated before it is passed on to cloud services.

You must ensure that your organization's data residency requirements are met. Unlike other approaches, your organization may have to disclose sensitive information to comply with court orders or subpoenas. Your organization should evaluate its requirements carefully before selecting a CEG-based solution. This approach is dependent on the following:

- Network structure;
- Locations;
- Available third-party integrations; and
- Volume of data.

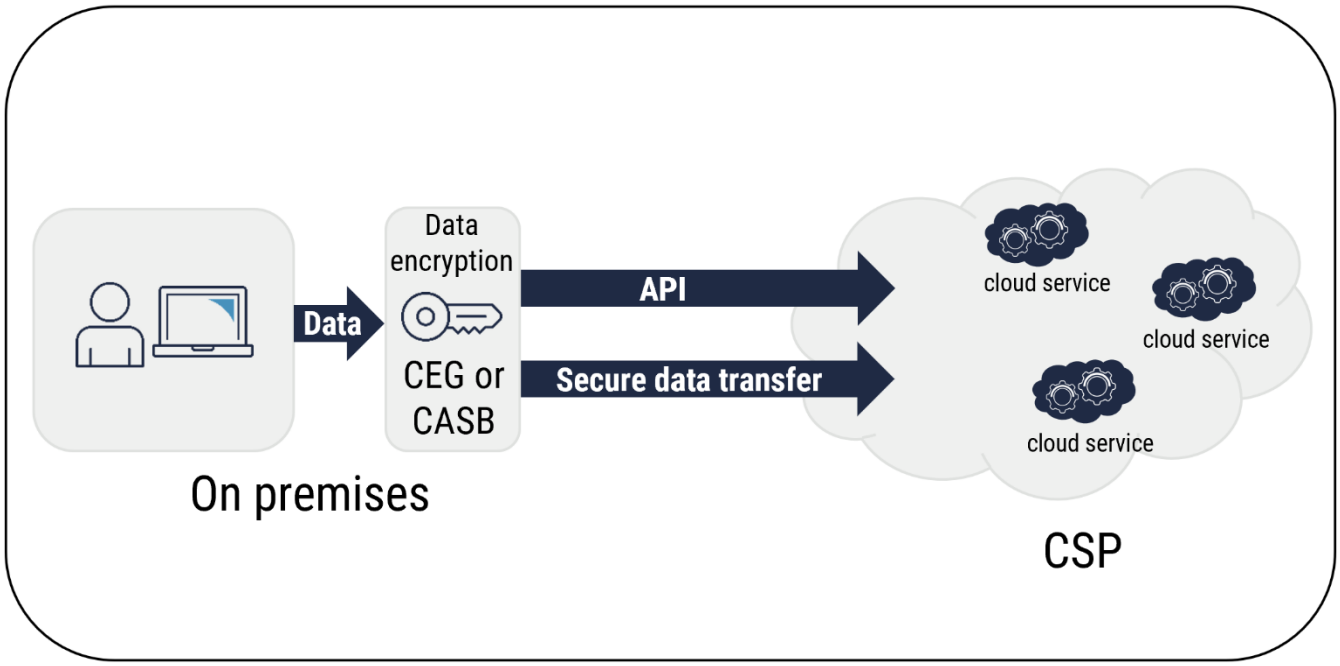


Figure 4: **Data Encryption Using a CEG or a CASB**

3.3.3.3 THIRD-PARTY KEY MANAGEMENT SERVICE

When service providers have access to keys and data, the potential for unauthorized access exists. One way to prevent unauthorized access is to separate the control of the data and the keys. You can use a third-party key management service to separate the control of key material from the control of data, which allows you to control and monitor access to key material and use the key management service in hybrid cloud scenarios.

3.3.4 SERVICE MOBILITY

There are a variety of CSP services, which have both their pros and cons, that you can choose from when designing and deploying your business services. To stay competitive as an organization, you must be able to react quickly to both market demands and your client's requirements. You need to adapt your IT strategy to use the cloud services that best address your business needs, and as a result, you might use a hybrid, multi-cloud strategy.

Cryptography is one of the foundations for CSP cloud platforms. If your organization wants to use multiple cloud platforms, you must avoid vendor lock-in. You need a key management strategy that can be used across multiple cloud platforms. Your organization's key management strategy must address the cloud service mobility that is required for multi-cloud environments.

You can use key management approaches such as BYOK and HSM to address service mobility requirements. With BYOK, your organization can generate and manage its keys on premises. You can export the keys to multiple CSP KMSs, which provides flexibility when migrating services and data from one cloud to another. For highly regulated environments, BYOK may not be an acceptable approach because, once the keys are exported to the cloud platforms, the CSPs have control over those keys. Highly regulated environments may need to use HSMs and separate the control of data from the control of keys. With a third-party provider hosting the HSM, your organization can avoid the complexity of deploying an HSM, and benefit from the agility offered by self-provisioning HSM as a service. You must ensure that adequate connectivity is in place for each cloud environment.

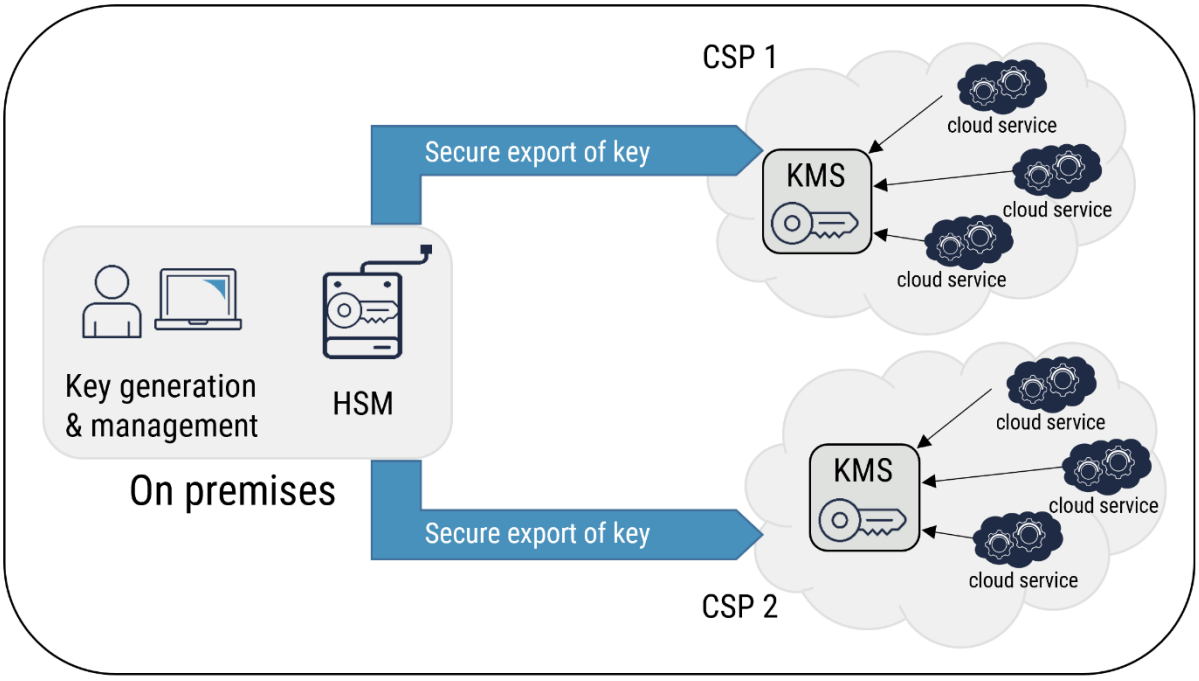


Figure 5: **Service Mobility with BYOK**

3.4 CRYPTO-SHREDDING

Data remanence is the lingering representation of data that remains on a storage device even though efforts have been made to eliminate the data (e.g. overwriting, deleting, erasing). After data is eliminated, there are techniques that can be used to recover that data. Data remanence can make the unintentional release of sensitive information possible if the storage device is released, lost, or accessed without authorization. Your organization should protect the confidentiality of any residual data on storage media by ensuring it is disposed of properly. However, you must also comply with legislation (e.g. privacy laws), government and industry regulations, and organizational security policies.

NIST's *Special Publication 800-88 Guidelines for Media Sanitization* [13] defines media sanitization as a process that renders access to target data on the media infeasible for a given level of effort. This ensures the continuing confidentiality of residual data on the media and minimizes the threat of unauthorized disclosure. In a multi-tenant cloud environment, cloud consumers do not have control of the physical storage media. As such, cloud consumers cannot use media sanitization methods that require access to physical media, and a different approach is required. Crypto-erase (CE) is a method that can be used to sanitize cloud storage media before it is released to the CSP shared pool of resources. *ITSP.40.006 v2 IT Media Sanitization* [14] defines CE as a sanitization process to erase the encryption key that is used on encrypted media, making the data unreadable.

Using encryption throughout the life cycle of the storage media makes sanitization faster and more effective. Encryption also eases the destruction requirements at the end of the media's life. Your organization should routinely encrypt storage media throughout its life cycle to protect the ongoing confidentiality of data after media decommissioning and disposal. This ensures the continuing confidentiality of residual data on the media and minimizes the threat of unauthorized disclosure.

3.5 CLOUD STORAGE CRYPTOGRAPHY

Cloud storage is provided by allocating a logical and virtual pool of storage to cloud consumers from a shared pool of physical resources. The CSP who is responsible for allocating storage resources also controls and manages this pool of physical resources. CSPs provide cloud consumers with configuration and deployment options to ensure the security of their data when using cloud storage services.

Your organization is responsible for selecting and configuring the various cloud storage security features. You should understand the benefits of each approach, including the risks that these approaches help mitigate.

3.5.1 STORAGE SERVICE ENCRYPTION

With storage service encryption, all data written to the storage service is encrypted. The CSP controls the encryption engine and access to the encryption key material. In cases where the CSP offers BYOK capabilities, the cloud consumer can manage the keys; however, the keys are still controlled by the CSP because they must access the keys to encrypt and decrypt information on cloud storage.

This approach provides crypto-shredding capabilities and protects data from unauthorized physical access or access by other cloud tenants. It also provides additional protection if physical disks are stolen, lost, or accessed by unauthorized users. However, storage service encryption does not protect data after it is backed up using cloud back-up services; your organization must ensure that the cloud back-up service provides data encryption.

3.5.2 INSTANCE-LEVEL ENCRYPTION

Instance-level encryption encrypts all files on operating systems or data virtual disks. Your organization is responsible for configuring and managing instance-level encryption. You have more control over which virtual disks you encrypt, and you can use different encryption keys for different disks. While your storage administrators usually manage the storage service encryption, the VM instance system administrators manage the instance-level encryption. When implemented, instance-level encryption has a minimal impact on performance. Similar to storage service encryption, the CSP still controls the encryption keys because they need to access the keys to encrypt and decrypt information as VMs are started.

In addition, instance-level encryption adds protection in scenarios where virtual disks are backed up or unauthorized copies of virtual disks are taken for offline analysis. This approach can be used with pre-boot protection capabilities to prevent unauthorized instantiation of a VM.

Instance-level encryption does not protect individual file back-up or access to data if the VM instance is compromised.

Instance-level encryption can be used with storage service encryption. Since each approach can be managed by different roles and addresses different threats, using both can contribute to your organization's defence-in-depth strategy.

3.5.3 DATA IN TRANSIT

Network access to cloud storage is not always encrypted by default. You should ensure that cloud storage services are configured to specify that only secure protocols (e.g. HTTPS and SMB 3.0) can be used to access cloud storage services and APIs.

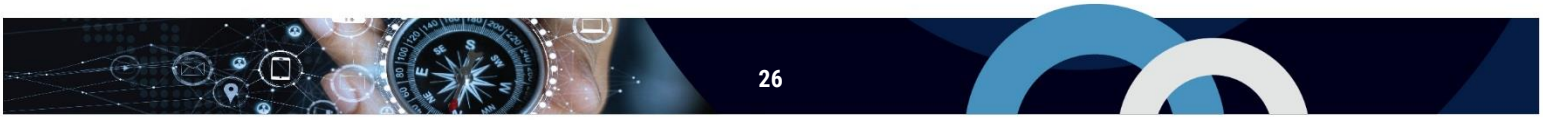
3.5.4 KEY MANAGEMENT

Cloud storage services are accessed via access keys. Cloud consumers obtain the storage keys via the management portal for each CSP.

Your organization should have a documented key management and key rotation process to prevent unauthorized disclosure of storage access keys and data. Some cloud storage services provide you with the capability to issue storage keys that are valid only if they are used in a specific time period, use secure protocols, and are from specific IP addresses. You should understand the cloud storage key options that are provided by your CSP. Always use the key management options that best address your organization's information protection requirements.

3.6 DATABASE CRYPTOGRAPHY

Your organization may have a significant amount of sensitive information stored in databases. This information is a high-value target for threat actors. You should ensure that these databases have security measures in place. When deploying database structures on cloud platforms, you give up control on components of the underlying infrastructure that support these databases. A security incident involving your database can be disastrous. These factors must be considered when developing and authorizing design patterns for use in deployment of cloud workloads.



Cryptography plays a crucial role in preventing unauthorized access to, and disclosure of, information contained in databases. It also supports the authentication of the end systems and the users involved in database transactions and ensures the confidentiality and the integrity of data while it is in transit and while at rest.

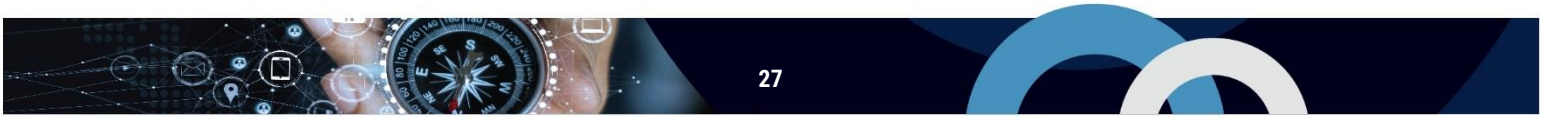
3.6.1 AUTHENTICATION

In cloud deployments, network traffic between applications and database servers flow on network infrastructure that your organization does not control. Failure to authenticate each end of the connection between an application server and a database server can expose the data flow to threat actors. These threat actors can intercept, relay network connections, and attempt to spoof the identity of a source system or user. Common cryptographic approaches to prevent man-in-the-middle attacks include public and private key pair-based authentication to determine the identity of the end systems involved in database transactions. Mutual authentication of these end systems is implemented with public key infrastructure (PKI) certificates to authenticate the database servers to client applications and users. PKIs use client certificates, connection strings, tokens, or database credentials to authenticate the client system or the user to the database. In a cloud environment, where cloud consumers are not in control of the network infrastructure, end systems must authenticate each other to prevent man-in-the-middle attacks.

3.6.2 DATA-IN-TRANSIT ENCRYPTION

While authenticating endpoints involved in database transactions is paramount, ensuring the confidentiality and the integrity of database flow between endpoints is equally important. Data flowing on network infrastructure between on-premises and cloud environments and between cloud services can be modified or intercepted, which may lead to serious impacts on your organization if it is not protected by the appropriate cryptographic measures.

Your organization should enforce the use of the network encryption protocols, ciphers, and algorithms identified in ITSP.40.111 [1] for all data flows between application and database servers. Management traffic between system administration servers and database instances must also be protected by cryptographic measures that include multi-factor authentication.



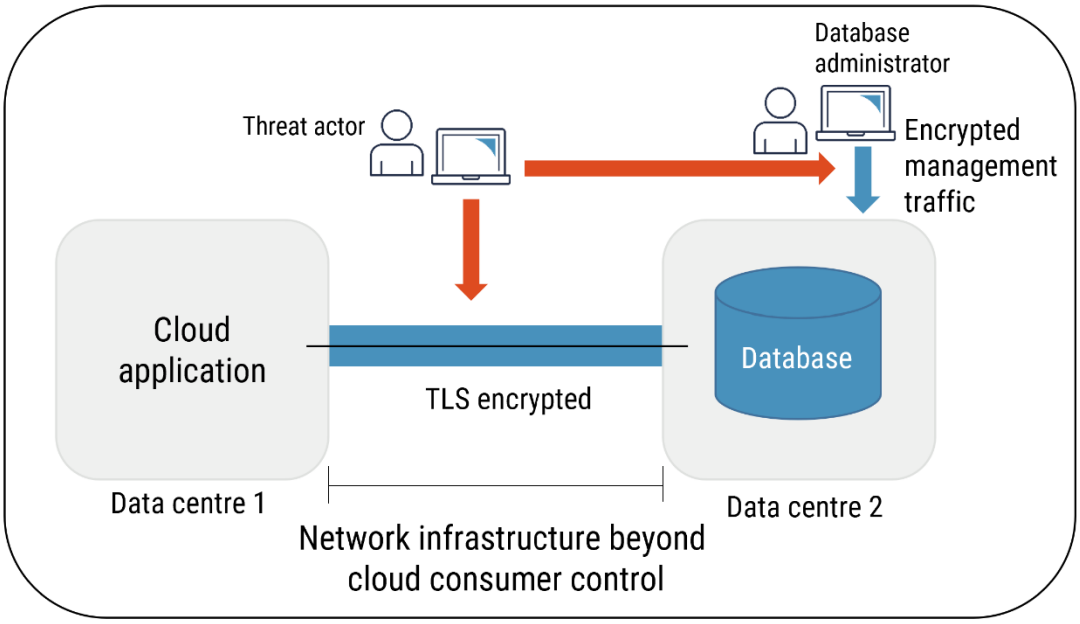


Figure 6: **Encryption of Data in Transit**

3.6.3 TRANSPARENT DATA AND EXTERNAL DATABASE ENCRYPTION

Transparent data encryption (TDE) performs input/output-level encryption and decryption of data, back-ups, and log files. It provides confidentiality and integrity of data at rest, but it does not protect data in transit or in use. With TDE, the database server is responsible for encrypting all data that is written to the disk. TDE does not require any modifications to the applications or the database schema. Data is encrypted using a single data encryption key (DEK), which is protected by other means (e.g. a key encryption key stored within the database file structure, an HSM, or a KMS).

TDE can be used with disk or storage encryption. TDE protects data in scenarios where the database files, back-up files, and physical or virtual media are lost, copied, stolen, or modified. However, disk and storage encryption only protects physical or virtual media.

TDE does not protect against malware or unauthorized access or modification of data by database administrators. In cases where cloud consumers subscribe to a PaaS database from their CSP, the CSP personnel who are responsible for database instance administration can potentially access the data stored on that database. If your organization wants to protect its data from unauthorized access by malware or CSP personnel, then consider alternative approaches to protect its databases.

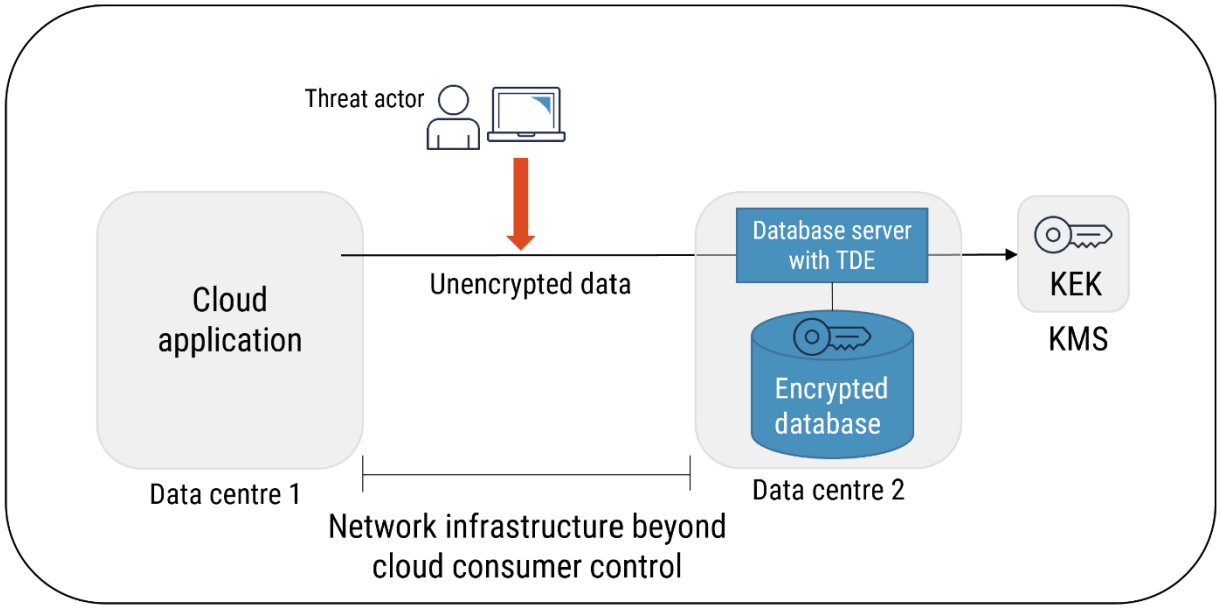


Figure 7: **TDE without Encryption of Data in Transit**

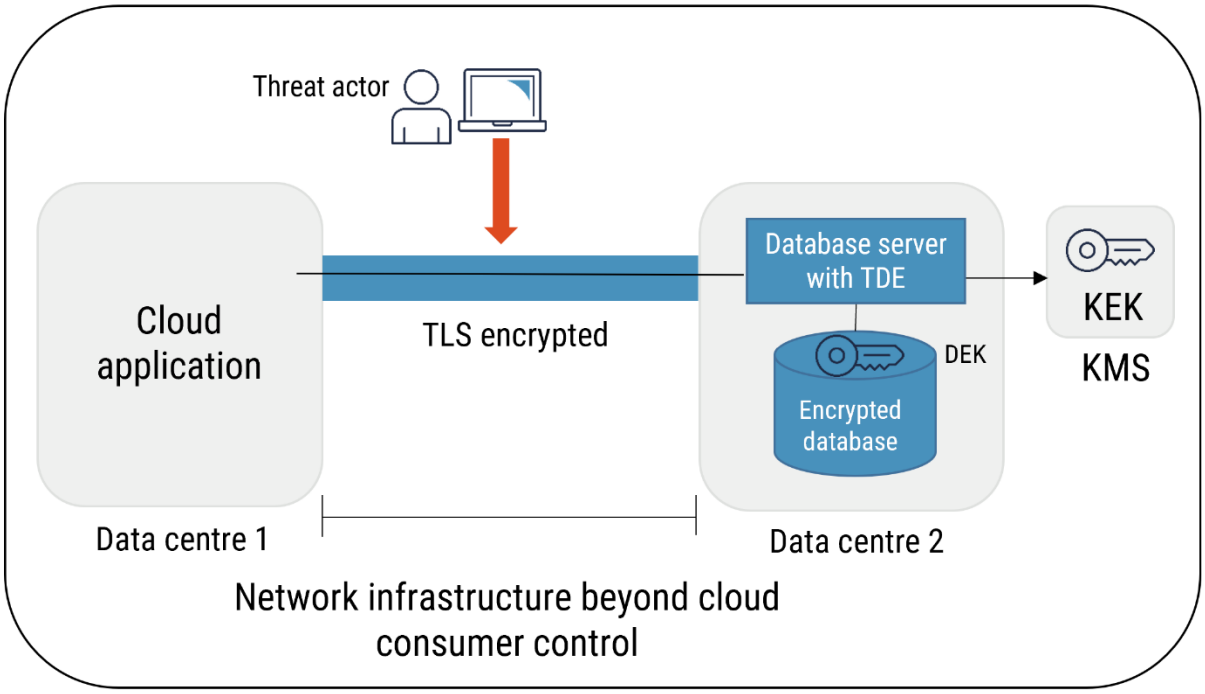


Figure 8: **TDE Used with Encryption of Data in Transit**

3.6.4 COLUMN-LEVEL ENCRYPTION

Column-level encryption helps provide segregation of duties. It ensures that personnel (e.g. CSP employees) who are responsible for managing the data that is held in large repositories (e.g. databases) can manage them without having access to the actual data. Column-level encryption also ensures that personnel who require access to the data do not have access to manage data repositories. With column-level encryption, the application manages which column is to be encrypted. This approach requires changes to the applications. Different DEKs can be used to encrypt each column, and each column DEK is then protected by other means, such as a KMS.

Despite requiring changes to the applications, column-level encryption provides significant security benefits in cloud computing. It provides protection under the following threat scenarios:

- CSP personnel who have elevated privileges and who are attempting to run unauthorized queries on or modify databases containing sensitive information;
- CSP personnel who have elevated privileges and who are attempting to gain unauthorized access to or modify data in use on database server memory or dump files;
- Malware that is running on database servers and that is attempting to access or modify database files, memory, or dump files; and
- Interception or modification of data that is in transit between the application and the database servers.

Cloud consumers subscribing to PaaS databases can benefit from the additional security offered by column-level encryption. This additional security comes with a slight performance impact and additional complexity.

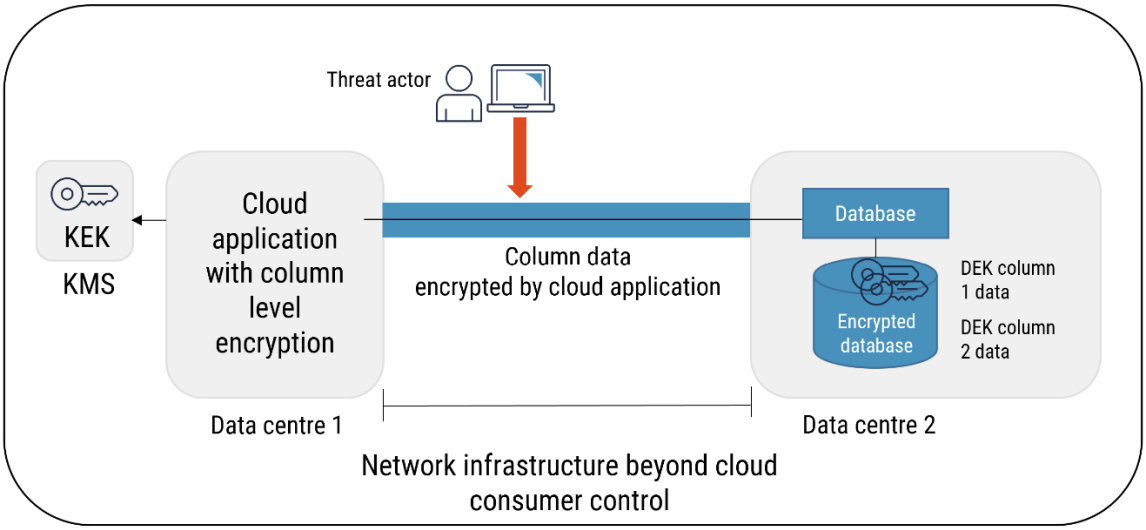


Figure 9: **Column-Level Data Encryption**

3.6.5 KEY MANAGEMENT

When using any of the database cryptography approaches outlined above, cloud consumers should be careful not to manage the keys on the same system that is using the keys. It is highly recommended that cloud consumers make use of KMS or HSM services to ensure secure storage of cryptographic key material.

3.7 ENDPOINT CRYPTOGRAPHY

Cloud consumers rely on an increasingly mobile workforce to deliver their business objectives. Today's users use a variety of devices (e.g. smart phones, tablets, and laptops) to access cloud applications remotely. Along with large data repositories, mobile endpoints are one of the primary assets that are targeted by threat actors. If compromised, endpoint devices and credentials offer an ideal point of entry into your organization's information.

Cloud consumers remain responsible for the security of endpoints used to access workloads and data in the cloud. Endpoint devices require a variety of security controls that work together to ensure endpoints and the data and credentials that they contain, are adequately protected. Cryptography plays an increasing role in securing endpoint devices, and cloud consumers must ensure that configuration of cryptographic capabilities on mobile endpoints is managed effectively, including:

- ensuring approved cryptographic algorithms, ciphers, and protocols are configured and enforced;
- ensuring endpoint agents and mobile device management data flows are authenticated and encrypted; and
- ensuring protection of data at rest by encrypting disks, files, and removable storage devices (e.g. thumb drives).

Your organization should ensure that the confidentiality and integrity of its data is maintained by using applications that are configured to use approved protocols and algorithms.

4 SUMMARY

This document can be used to help you understand the cloud service cryptography considerations that are needed to support an effective cloud security management program.

To effectively implement cloud service cryptography, your organization must understand the various cryptographic service offerings, implementation approaches, protocols, ciphers, and key management models that are available. Poorly selecting, implementing, configuring, and managing cryptographic services and protocols may lead to serious flaws and ineffectively protect cloud-based services and data.

Your organization should analyze the key management and the database cryptography options that are available and select the approaches that best address your cloud deployment strategy, risk tolerance, and compliance requirements.

4.1 CONTACTS AND ASSISTANCE

If you would like more information on security assessments and authorizations for cloud-based services, please contact the Cyber Centre Contact Centre:

Cyber Centre Contact Centre
contact@cyber.gc.ca
613-949-7048 or 1-833-CYBER-88

5 SUPPORTING CONTENT

5.1 LIST OF ABBREVIATIONS

Term	Definition
API	Application program interface
BYOK	Bring your own key
CASB	Cloud access security broker
Cyber Centre	Canadian Center for Cyber Security
CE	Crypto-erase
CEG	Cloud encryption gateways
CSA	Cloud Security Alliance
CSE	Communications Security Establishment
CSP	Cloud service provider
DEK	Data encryption key
HSM	Hardware security module
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a service
IoT	Internet of things
IP	Internet Protocol
IT	Information technology
KMIP	Key Management Interoperability Protocol
KMS	Key management system
NIST	National Institute of Standards and Technology
PaaS	Platform as a service
PCI DSS	Payment Card Industry Data Security Standard
PKI	Public key infrastructure
RP	Relying party
SaaS	Software as a service
SMB	Server message block
TBS	Treasury Board of Canada Secretariat
TDE	Transparent data encryption
VM	Virtual Machine

5.2 GLOSSARY

Term	Definition
Assertion	A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes.
Availability	The state of being accessible and usable in a timely and reliable manner.
Authentication	A measure designed to provide protection against fraudulent transmissions or imitations by establishing the validity of a transmission, message, or originator.
Authenticity	The state of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
Confidentiality	The state of being disclosed only to authorized principals.
Cryptography	The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.
Encryption	The transformation of data into a form that conceals the data's original meaning to prevent it from being known or used. If the transformation is reversible, the corresponding reversal process is called "decryption," which is a transformation that restores encrypted data to its original state.
Decryption	A process that converts encrypted voice or data information into plain form by reversing the encryption process.
Integrity	The accuracy and completeness of information and assets and the authenticity of transactions.
Internet of things	The concept of extending Internet connectivity beyond conventional computing platforms such as personal computers and mobile devices, and into any range of traditionally "dumb" or non-internet-enabled physical devices and everyday objects.
Key management	Procedures and mechanisms for generating, disseminating, replacing, storing, archiving, and destroying keys which control encryption or authentication processes.
KMIP	Enables communication between key management systems and cryptographically-enabled applications, including email, databases, and storage devices. As defined by OASIS, KMIP is a communication "protocol used for the communication between clients and servers to perform certain management operations on objects stored and maintained by a key management system".

5.3 REFERENCES

Number	Reference
[1]	Cyber Centre. ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B, August 2016.
[2]	Cyber Centre. ITSP.40.062 Guidance on Securely Configuring Network Protocols, August 2016.
[3]	TBS. Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN), 1 November 2017.
[4]	Cyber Centre. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*, December 2014.
[5]	CSA. Security Guidance for Critical Areas of Focus in Cloud Computing v4.0, 2017.
[6]	NIST. *Computer Security Resource Centre Glossary,* N.D.
[7]	Cyber Centre. ITSP.30.031 V3 User Authentication Guidance for Information Technology Systems, April 2018.
[8]	Cyber Centre. *ITSP.50.103 Guidance on the Security Categorization of Cloud-Based Services ,* May 2020.
[9]	Cyber Centre. *ITSP.50.105 Guidance on Cloud Security Assessment and Authorization*, May 2020.
[10]	NIST. *Special Publication 800-57* Recommendation for Key Management, Part 1: General (Revision 4), 28 January 2016.
[11]	PCI Security Standards Council. PCI DSS Cloud Computing Guidelines, April 2018.
[12]	TBS. *Government of Canada White Paper: Data Sovereignty and Public Cloud*, N.D.
[13]	NIST. Special Publication 800-88 *Guidelines for Media Sanitization (Revision 1),* 18 December 2014.
[14]	Cyber Centre. ITSP.40.006 v2 IT Media Sanitization, July 2017.