Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

GUIDANCE ON USING TOKENIZATION FOR CLOUD-BASED SERVICES

ITSP.50.108

PRACTITIONER

TLP:WHITE

© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed beyond its intended audience, produced, reproduced or published, in whole or in any substantial part thereof, without the express permission of CSE.

Canada

FOREWORD

ITSP.50.108 Guidance on Using Tokenization for Cloud-Based Services is an UNCLASSIFIED publication issued under the authority of the Head of Canadian Centre for Cyber Security (Cyber Centre).

This document is part of a suite of documents developed by the Cyber Centre to help secure cloud-based services. This document supports the cloud security risk management approach defined in *ITSM.50.062 Cloud Security Risk Management* [1][1].

For more information or suggestions for amendments to this document, you can email or phone our Contact Centre:

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

EFFECTIVE DATE

This publication takes effect on October 6, 2021.

REVISION HISTORY

Revision	Amendments	Date
1	First release.	October 6, 2021

ISBN 978-0-660-40518-6
CAT D97-3/50-108-2021E-PDF

[1] Numbers in square brackets refer to reference material listed in the Supporting Content section of this document.

OVERVIEW

The information provided in this security guidance document applies to private and public sector organizations. Your organization can apply the guidance in this document for all cloud-based services, independently of the cloud service and the deployment models. For an overview of cloud services and deployment models, see *ITSAP.50.111 Models of Cloud Computing* [2].

TABLE OF CONTENTS

1 Introduction 6
1.1 Applicable Regulations and Policies 6
1.2 Cloud Risk Management 7
1.3 Defence in Depth for Cloud-based Services 7
2 Tokenization 8
2.1 The Tokenization Process 8
2.2 Token Generation Schemes 9
2.3 Tokenization Servers 10
3 Considerations for Tokenization Solutions 11
3.1 Governance and Risk management 11
3.2 Network Security 12
3.3 Compute 12
3.4 Data Security 12
3.5 Identity and Access Management 14
3.6 Application 15
3.7 Monitoring and Incident Response 15
3.8 Endpoint Security 15
4 Summary 16
4.1 Contacts and Assistance 16
5 Supporting Content 17
5.1 List of Abbreviations 17
5.2 Glossary 18
5.3 References 20

LIST OF FIGURES

Figure 1: Basic Tokenization Service for Cloud-Based Services 9

Figure 2: Defence in Depth for Cloud-Based Services 11

1 INTRODUCTION

This document describes how your organization can use tokenization to reduce the residual risks incurred when using cloud-based services to transmit, process, or store sensitive information (i.e. information that requires protection against unauthorized disclosure). When using cloud-based services, your organization still has legal responsibility for its systems and data. You are accountable for protecting the confidentiality, integrity, and availability of the information systems and information that are hosted by a cloud service provider (CSP).

To protect sensitive information and minimize the risk of compromises, your organization can use tokenization as part of its defence-in-depth security architecture. Tokenization is the process by which a surrogate value (called a token) is generated and used in place of the original data or information. Widely used in finance and healthcare organizations, tokenization is designed to protect discreet data fields in information systems.

1.1 APPLICABLE REGULATIONS AND POLICIES

When using cloud-based services, it can be challenging to ensure compliance with applicable policies and regulations; your organization and the CSP share direct control over many aspects of security and privacy. However, your organization must ensure that it meets the requirements of all applicable policies and regulations, provincial and territorial privacy laws, and sector-specific regulations and standards. Policies and regulations such as the *Privacy Act* [3] and the *Personal Information Protection and Electronic Documents Act* (PIPEDA) [4] dictate how Canadian organizations store, transmit, and process personal information. For Government of Canada (GC) departments and agencies, sensitive information is also marked with security classifications, which denote the level of injury that would result if that information is compromised.

You can refer to the following resources for additional information on requirements for protecting sensitive information:

- Treasury Board of Canada Secretariat, *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice* [5]; and
- Office of the Privacy Commissioner of Canada, *Cloud Computing for Small and Medium-Sized Enterprises* [6].

Policies and standards for the use of tokenization to help secure payment and other financial transactions include:

- Payment Card Industry Security Standards Council, *Payment Card Industry Data Security Standard (PCI DSS) Information Supplement: PCI DSS Tokenization Guidelines* [7]; and
- American National Standards Institute (ANSI), ASC/X9 – *ANSI X9.119-2 Requirements for Protection of Sensitive Payment Card Data – Part 2: Implementing Post-Authorization Tokenization Systems* [8].

Refer to these resources and other applicable policies, standards, and guidance for recommendations on using tokenization to secure payment transactions.

1.2 CLOUD RISK MANAGEMENT

By applying IT security risk management practices, including defence-in-depth strategies for cloud services, your organization can mitigate the risks introduced by using cloud services to store, transmit, and process sensitive information. The Cyber Centre's *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [9] defines two levels of risk management activities: organizational-level (or departmental) activities and information system-level activities. You can integrate organizational-level activities into your organization's security program to plan, assess, and improve the management of IT security risks. At this level, tokenization supports organizational risk management by defining the security approaches of your organization's security control profiles. The Cyber Centre has developed security control profiles for cloud-based services, which are derived from the baseline profiles in Annex 4 of ITSG-33 [9].

You can integrate information system-level activities into your information system development lifecycle (SDLC). 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 aligns with the information system-level activities. Tokenization may be implemented to support step five of the cloud security risk management approach. Tokenization supports a defence-in-depth security architecture, which can be used in the design and implementation of cloud security controls.

1.3 DEFENCE IN DEPTH FOR CLOUD-BASED SERVICES

As described in *ITSP.50.104 Guidance on Defence in Depth for Cloud-Based Services* [10], using tokenization technologies to protect sensitive systems and information is part of the third defensive layer (data security). Your organization needs to consider how sensitive information is protected while in transit to, from, and within cloud environments. You must also ensure that sensitive information is protected when it is at rest in the cloud and while it is being processed in all data replication repositories. You must also ensure that this information is protected after the subject information systems are decommissioned. Tokenization is one of the technologies that you can use to meet these protection requirements.

2 TOKENIZATION

Tokenization is the process by which a surrogate value (a token) is generated and used in place of the original data or information. Many tokenization systems also enable the reverse process (de-tokenization) by which the token is replaced with the original data or information.

The token can act as an identifier that is mapped back to the original data. Appropriately generated tokens do not contain sensitive information and can be transmitted, stored, and processed in place of the original data. The residual risks to the confidentiality and the integrity of the original information are reduced because only approved information systems, including the tokenization system, have access to the original sensitive information.

Tokenization is like encryption in that both techniques can be used to mask sensitive information. Both tokenization and encryption have advantages for protecting information, and they are commonly used together. While encryption uses reversible coding processes and encryption keys, tokens are not mathematically correlated to the original data (except for tokenization systems that use reversible encryption schemes to generate tokens). Decryption reverses the encryption process to revert ciphertext back to its plaintext form. The original information represented by a token is stored and mapped in the de-tokenization database. One of the advantages of using tokenization systems is that tokenization methodologies can be designed to enable you to process, search for, and sort the original data while only using the associated tokens.

2.1 THE TOKENIZATION PROCESS

Tokenization solutions can vary significantly depending on the vendor, the operational requirements, and the architecture of the supported information systems. As part of your organizational cloud security risk management process, you need to assess the available deployment models, the tokenization and de-tokenization methods, and the tokenization processes to determine which solution meets your organization's needs.

2.1.1 TOKENIZATION PROCESS ACTIVITIES

The following is a description of a basic tokenization service that could be used to help protect sensitive information in a system using cloud-based services.

There are six core activities in a cloud-based system that uses tokenization to protect sensitive information (see Figure 1):

1. Sensitive information is collected, generated, or retrieved from existing data sources and sent to the tokenization server.
2. Applications in the tokenization server identify sensitive information fields based on pre-defined rules and policies and generate random or semi-random tokens for those fields. The original information, the associated token(s), and the mapping data is stored in the tokenization database.
3. The tokens are sent to and stored in your organization's cloud-based services.
4. The tokenized information can be integrated with other information sources, processed, distributed, and stored in other locations based on your organization's operational requirements.
5. When required by authorized users and applications, aggregate and/or processed information containing the tokenized information is pulled from the cloud services.

6. Authorized users and applications submit requests to the tokenization server, identifying the tokens for which they need to know the original information. The tokenization server returns the original information values to the authorized users and applications.

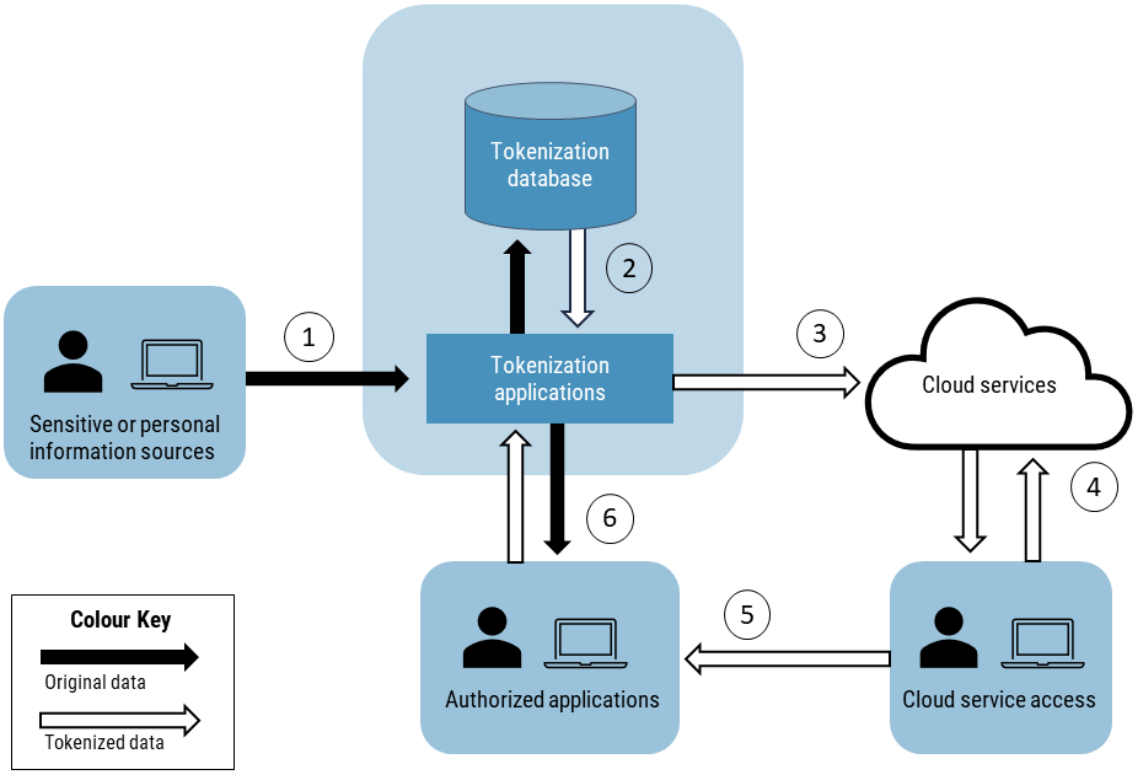

Figure 1: Basic Tokenization Service for Cloud-Based Services

2.2 TOKEN GENERATION SCHEMES

Except in the payment industry, there are few international tokenization standards. The methods and technologies used to produce, store, and manage tokens vary significantly between vendors. Generally, tokenization systems that are designed to protect sensitive information generate tokens that match the format of the original data. The tokens can be more easily processed, searched, and sorted. Applications and databases use the format-matched tokens as direct substitutes for the original values without having to adapt their applications.

There are three common token generation schemes:

- **On-demand random assignment**: A random number or alphanumeric sequence is produced by a random number generator (RNG) for each information field or value.
- **Static table-driven tokenization**: An RNG or a pseudo-random number generator (PRNG) is used to populate a table from which tokens are subsequently selected.

- **Encryption-based tokenization**: Encryption methods, including the use of symmetric key with message authentication code algorithms, are used to generate tokens. Encryption-based tokenization schemes can be used to produce tokens that can be decrypted to restore the original values or one-way tokens that cannot be decrypted. The tokens generated by encryption techniques may also match the format of the original values if format-preserving encryption (FPE) algorithms are used.
  - See National Institute of Standards and Technology (NIST) *Special Publication 800-38G Recommendation for Block Cypher Modes of Operation: Methods for Format-Preserving Encryption* [11] for more information.

For more information on these three methods, see ASC/X9 – ANSI X9 119-2 [8].

2.3 TOKENIZATION SERVERS

Tokenization servers are the foundation of most tokenization systems. Not only do they create and store tokens, but they also support the security functions that protect the sensitive information that they store, process, and transmit. These security functions include authentication of the applications and the users accessing the tokenization server, data encryption, and monitoring.

As tokenization servers manage most of the security functions that protect the sensitive information stored in these servers, they may have one of the highest security categories of all the sub-systems in your information system architecture. Your organization should carefully assess and maintain the security categorization and the security control profile assigned to the tokenization server(s). See *ITSP.50.103 Security Categorization for Cloud-Based Services* [12] for more information about security categories.

Some applications and databases have integrated tokenization capabilities. Tokenization-as-a-service (TaaS) has become a popular cloud service offering. One advantage of these solutions is that your organization does not need to establish, operate, and maintain a tokenization server. Depending on your operational requirements, IT support capabilities, and security requirements, these solutions may best meet your operational requirements. However, it can be more difficult to assess the effectiveness of the security controls and functions of tokenization solutions that do not have dedicated tokenization servers. We recommend that you complete the first three steps of the cloud security risk management process found in ITSM.50.062 [1]:

1. Perform a security categorization;
2. Select a security control profile; and
3. Select a cloud service and a deployment model.

You should complete these steps before you choose the tokenization architecture that best meets your organization's operational and security needs.

3 CONSIDERATIONS FOR TOKENIZATION SOLUTIONS

Our cloud security guidance is based on defence-in-depth strategies, which are described in ITSP.50.104 [10]. When you determine your organization's security requirements for the tokenization system(s) that support your cloud-based services, you should also consider these requirements in the context of defence in depth.

The considerations presented in this section are grouped based on the defensive layers described in ITSP.50.104 [10] and shown in Figure 2.

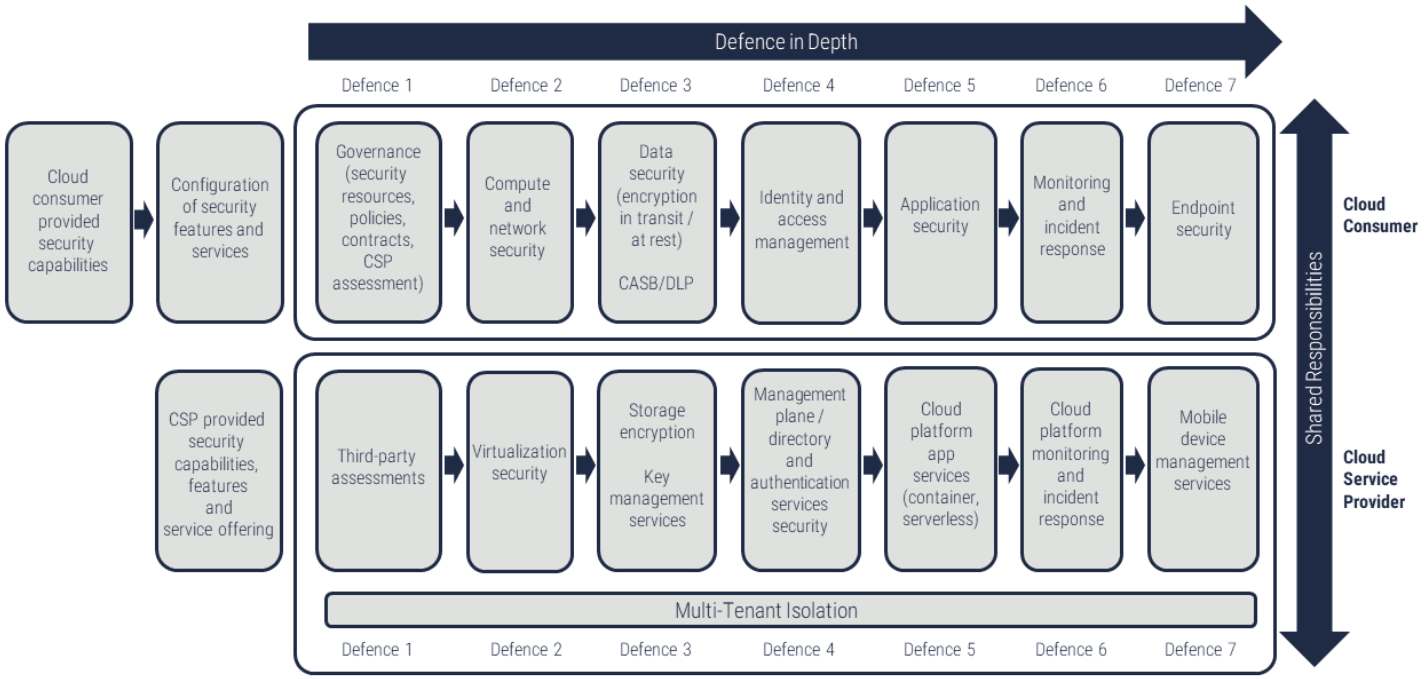

Figure 2: Defence in Depth for Cloud-Based Services

3.1 GOVERNANCE AND RISK MANAGEMENT

The foundation of your organization's defence-in-depth strategy for your tokenization service is your policies, directives, contract requirements, and allocation of security resources (i.e. your governance framework). With proper governance, your organization can ensure it conforms with legal and compliance requirements and establishes clear roles and responsibilities. Your governance framework provides the guiding principles for protecting sensitive information entrusted to your organization.

The first step in the cloud risk management process is to perform a security categorization. As part of this process, your organization needs to determine which laws, regulations, and standards apply to its activities and which information it uses for those activities. Your organization can use this assessment to determine the following:

- The security measures required to protect that information; and
- The specific information values and data fields that should be tokenized within your cloud-based services.

However, the lack of international standards can result in challenges with using tokenization to protect sensitive information. In the absence of standards to accredit tokenization systems, your organization needs to assess the security measures for its selected tokenization systems annually, at least. Your initial and subsequent security assessments can help you understand the overall effectiveness of these security controls and determine and manage residual risks.

3.2 NETWORK SECURITY

Regardless of the tokenization solution and cloud service models you choose, sensitive information transits your networks as it is collected, sent to the tokenization service, and retrieved by authorized applications and users (activities 1, 2, and 6 in Figure 1). To protect information in transit, you need to secure the network connections to and from your tokenization and cloud services. You also need to protect the network connections used to access, administer, and monitor the tokenization and supporting security services.

To achieve an effective defence-in-depth security architecture, you need to appropriately segment the networks that are used in and that connect to the tokenization server. Network segmentation improves access control, monitoring, and containment of any compromise. We recommend that you ensure the tokenization server can only be reached by external information services, including your cloud-based systems, through a security gateway. You should isolate the tokenization server from Internet access.

See ITSP.40.062 *Guidance on Securely Configuring Network Protocols* [13] and ITSP.40.111 *Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* [14] for additional guidance on securing the networks that are in and that connect to your tokenization system(s).

3.3 COMPUTE

This defensive layer includes protecting the physical hosts, processors, hypervisors, virtual machines, and platforms that support your tokenization service. To reduce the risks to the sensitive information processed by these systems, your organization should implement security best practices such as patching, security baseline configurations, and monitoring.

One of the primary security considerations for tokenization systems is maintaining the isolation between the tokenization service and the applications accessing the tokenized information. The risk of unauthorized access to the sensitive information is significantly increased if this isolation is not maintained (see subsection 7.2.4 of ANSI X9.119-2 [8]). The most direct method to establish this isolation is to host the tokenization service and applications on separate physical systems. If the tokenization service and the connected applications are hosted in the same computing environment, you can achieve this isolation by using process isolation (e.g. separate operating systems), environment isolation (e.g. separate virtual machines), or physical process separation (e.g. separate processors).

3.4 DATA SECURITY

One of the primary reasons to use a tokenization service is to protect sensitive information. As such, implementing appropriate data security defensive layer mechanisms in your tokenization system is essential to minimizing the residual risks to that information.

Although the other identified defensive layers play a role in protecting sensitive information, there are several considerations unique to the tokenization storage and databases that you need to address:

- Storage;
- Availability;
- Replication and backup;
- Disposal and data remanence; and
- Encryption.

3.4.1 STORAGE

The token vault is the system that stores the tokens, the original values, and the token mapping information. One of the first security architecture decisions that your organization needs to make is where the token vault may be located. Depending on the policies, regulations, and standards that apply to your organization, there may be geographical (e.g. data residency) or architectural limitations on where the token vault (and the information it contains) may reside. If you use third-party tokenization systems or store your token vault in off-premises facilities, you do not have direct control over the sensitive information that is being processed and stored.

Token vaults likely contain an aggregate of most or all of your organization's sensitive information; these vaults may have a higher security category than other portions of your information system architecture. See ITSP.50.104 [10], subsection 4.3.3.1, for additional information on aggregation.

As part of your security risk management process, you choose a storage location for the token vault based on these considerations and the residual risks of each architectural option.

3.4.2 AVAILABILITY

If your organization has an operational requirement for continuous, uninterrupted access to the tokenization services or the information in the token vaults, your security architecture needs to support high availability or failover capabilities. You can accomplish high availability and failover capabilities by using dispersed and/or redundant systems.

If your organization has outsourced a portion of or all the tokenization services, you should specify your availability requirements in your contracts and service level agreements. Ensure that the tokenization system or service you use meets your operational requirements for availability.

3.4.3 REPLICATION AND BACKUP

Your organization may need multiple tokenization systems to meet its operational requirements for processing, access, or availability. You may need to synchronize, manage, and secure the multiple tokenization servers, token vaults, and backups in different locations. Regardless of the security architecture you organization choose or designs, you must ensure that

sensitive information transmitted between and stored in each of these locations remains secure throughout the information lifecycle.

3.4.4 DISPOSAL AND DATA REMANENCE

Your organization is responsible for protecting sensitive information throughout its lifecycle – when it is collected, stored, in use, transmitted, and disposed of when no longer required. When you replace or reuse the media that supports the tokenization servers, token vaults, and backups, it may still be possible to recover the remnants of sensitive information that was stored on that media. You should establish policies, procedures, and resources for securely sanitizing and disposing of this media.

For more information on data remanence, see ITSP.50.104 [10], subsection 4.5.4.5. For more information on media sanitization see *ITSP.40.006 V2 IT Media Sanitization* [15].

3.4.5 ENCRYPTION

To effectively protect sensitive information throughout its lifecycle, you should encrypt sensitive information when it is in transit and when it is stored. We recommend that you routinely encrypt all networks and storage media according to the guidance in ITSP.40.111 [14] and *ITSP.50.106 Cloud Service Cryptography* [16], as applicable. When procuring a tokenization system, your organization should confirm that the encryption and key management services used by that system also meet the recommendations in these documents.

3.5 IDENTITY AND ACCESS MANAGEMENT

Effective identification, authentication, and access controls are critical to the security of your tokenization system and the protection of the services and information contained in the system. These controls include measures such as logical or physical segregation of the storage, separation of duties, and role-based permissions. See *ITSP.30.031* V3 *User Authentication Guidance for Information Technology Systems* [17] for additional recommendations on choosing the appropriate security controls when you are designing a user authentication system.

To ensure only authorized individuals, applications, and systems can access your tokenization system, you should determine the access requirements (e.g. the entities that require access, the types of access the entities require, the information and the services that the entities need to access). For example, you should identify who is authorized to submit data for tokenization, request de-tokenization, and access the management plane of the tokenization system. If possible, we recommend integrating the identification and authentication (I&A) systems used to control access to your tokenization system with the other I&A systems used by your organization. Your organization should use role-based access (RBAC) to control all management plane services, including any cryptographic functions provided by the tokenization server.

3.6 APPLICATION

The application defensive layer security considerations for tokenization include the following:

- Secure application development;
- Source code analysis;
- Security and vulnerability testing;
- Secure deployment;
- Runtime vulnerability management; and
- Threat protection.

One of the primary concerns for tokenization applications is the method used to generate tokens. It should not be possible to conduct de-tokenization or determine the original value of a token outside of your tokenization system(s). De-tokenization should only be conducted when requested by authorized users, applications, or systems. As such, independent testing agencies should prove and validate the RNG or encryption methods used to generate the tokens, reducing the risks of unauthorized de-tokenization and exposure of the associated sensitive information.

3.7 MONITORING AND INCIDENT RESPONSE

Your organization should use security monitoring and incident response capabilities to maintain and adapt your information security architecture and practices as threats evolve. We recommend that you consider an “assume breach” security model. You should allocate sufficient security resources to detect, define, and respond to malicious actors and vulnerabilities discovered in your information systems. The costs of mitigating a breach and the exposure of sensitive information often greatly exceed the costs of effective information security monitoring and threat response capabilities.

Your tokenization system should permit and facilitate tracking, monitoring, and logging of all access to and actions in that system and the supporting security services. The monitoring services should detect and alert management and security personnel of any malfunctions, anomalies, and suspicious behaviour. Your management and security personnel can use these alerts and analyze the associated logs to proactively detect and mitigate any problems, vulnerabilities, and compromises of your tokenization systems.

3.8 ENDPOINT SECURITY

In addition to implementing security controls and measures to protect the tokenization system and the networks connected to that system, your organization should also protect all systems and devices that have authorized access to the original sensitive information. If these systems or devices are compromised, threat actors can use them to gain unauthorized access to the tokenization system. Threat actors can also use the information stored in these devices to build unauthorized rainbow tables and attempt brute force and replay attacks. Threat actors use these types of attack vectors to de-tokenize and access the tokenized sensitive information that is stored in less secure or open information systems.

4 SUMMARY

This document provides guidance on defense in depth and security architecture considerations for effectively implementing, operating, and managing your organization's tokenization system.

Your organization can use tokenization as a method to protect the confidentiality and integrity of sensitive information that is transmitted, stored, or processed by cloud-based systems. You can also use tokenization to help your organization comply with the policies, regulations, and standards that govern your activities. However, you should only use tokenization as part of a defence-in-depth security architecture. You should ensure that tokenization is supported by other security technologies, such as encryption.

4.1CONTACTS AND ASSISTANCE

For more information on using tokenization to protect sensitive or personal information, you can contact our Contact Centre:

Contact Centre
contact@cyber.gc.ca
613-949-7048

5 SUPPORTING CONTENT

5.1 LIST OF ABBREVIATIONS

Term	Definition
ANSI	American National Standards Institute
CSP	Cloud service provider
FPE	Format-preserving encryption
GC	Government of Canada
I&A	Identification and authentication
IT	Information technology
NIST	National Institute of Standards and Technology
PCI DSS	Payment Card Industry Data Security Standard
PIPEDA	Personal Information Protection and Electronic Documents Act
PRNG	Pseudo-random number generator
RNG	Random number generator
SDLC	System development lifecycle
TaaS	Tokenization as a service
TLP	Traffic Light Protocol

5.2GLOSSARY

Term	Definition
Assume breach security model	An information security strategy where it is assumed that information systems are already compromised but the compromise has yet to be discovered.
Availability	The ability for the right people to access the right information or systems when required.
Cloud service provider	Any commercial provider of cloud services that wishes to offer its services to consumers.
Confidentiality	The ability to protect sensitive information from access by unauthorized people.
Data residency	Data residency refers to the physical or geographical location of an organization's digital information while at rest.
Decryption	The process of reverting ciphertext to plaintext.
Defence in depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization.
De-tokenization	The reverse process of tokenization through which the original data or information that has been mapped to a token is restored.
Encryption	Converting information from plaintext to ciphertext to hide its contents and prevent unauthorized access.
Format-preserving Encryption	An encryption method that puts out information in the same format as the original information.
Identification and authentication	The process of establishing the identity of an entity interacting with a system.
Integrity	The ability to protect information from unauthorized modification or deletion.
Personal information	Any factual or subjective information, recorded or not, about an identifiable individual.
Pseudo-random number generator	A process that is invoked to generate sequences of numbers approximating the properties of random numbers.
Random number generator	A process that is invoked to generate a random sequence of values (usually a sequence of bits) or an individual random value.
Residual risk	The likelihood and impact of a threat that remains after security controls are implemented.
Risk management	A systematic approach to setting the best course of action under uncertainty by identifying, assessing, understanding, making decisions, and communicating risk issues.
Sanitization	Sanitization is the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before sanitizing.
Security categorization	The process of identifying potential injuries that could result from compromises of business processes and related information and determining their security category.

Term	Definition
Security control profile	A security control profile specifies a set of controls and enhancements. When applied appropriately with your specific technical and threat context in mind, these controls and enhancements protect the confidentiality, integrity, and availability of information systems that are used to support business activities.
Sensitive information	Information that requires protection against unauthorized disclosure.
Tokenization	The process by which a surrogate value (called a token) is generated and used in place of the original data or information.
Token vault	The system that stores the tokens, the original values, and the token mapping information.

5.3REFERENCES

Number	Reference
1	Canadian Centre for Cyber Security. ITSM.50.062 Cloud Security Risk Management. March 2019.
2	Canadian Centre for Cyber Security. *ITSAP.50.111 Models of Cloud Computing*. November 2018.
3	Department of Justice Canada. *Privacy Act*. 1985
4	Department of Justice Canada. *Personal Information Protection and Electronic Documents Act*. 2000.
5	Treasury Board of Canada Secretariat. *Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN).* 1 November 2017.
6	Office of the Privacy Commissioner of Canada. *Cloud Computing for Small and Medium-sized Enterprises*. June 2012.
7	Payment Card Industry. *Payment Card Industry Data Security Standard*. Version 3.2.1. May 2018.
8	American National Standards Institute. ASC/X9 – *ANSI X9.119-2 - Requirements for Protection of Sensitive Payment Card Data - Part 2: Implementing Post-Authorization Tokenization Systems*. 3 August 2017.
9	Canadian Centre for Cyber Security. *ITSG-33 IT Security Risk Management: A Lifecycle Approach*. November 2012.
10	Canadian Centre for Cyber Security. *ITSP.50.104* Guidance on Defence-in-Depth for Cloud-based Services. May 2020.
11	National Institute of Standards and Technology (NIST). *Special Publication 800-38G* Recommendation for Block Cypher Modes of Operation: Methods for Format-Preserving Encryption. March 2016.
12	Canadian Centre for Cyber Security. *ITSP.50.103* Categorization for Cloud-based Services. May 2020.
13	Canadian Centre for Cyber Security. *ITSP.40.062* Guidance on Securely Configuring Network Protocols. August 2020.
14	Canadian Centre for Cyber Security. *ITSP.40.111* Cryptographic Algorithms for Unclassified, Protected A, and Protected B Information. August 2016.
15	Canadian Centre for Cyber Security. *ITSP.40.006 V2* IT Media Sanitization. July 2017.
16	Canadian Centre for Cyber Security. ITSP.50.106 Guidance on Cloud Service Cryptography. May 2020.
17	Canadian Centre for Cyber Security. ITSP.30.031 V3 User Authentication Guidance for Information Technology Systems. April 2018.