



ENCRYPTION POLICY

Policy #: Cyber_008

Version #: 1.0

Date: December 17, 2021


Office of the Chief Information Security Officer (Office of the CISO)

Encryption Policy

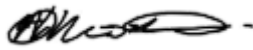
Ownership/Stewardship

Domain	Owner	Steward
Encryption	Director, Threat Management	Technology Services Division

Endorsement

Section	Name/Role	Signature
Technology Services Division	Lawrence Eta Chief Technology Officer	

Approval

Section	Name/Role	Signature	Approval Date
Office of the Chief Information Security Officer	Abiodun Morolari (Chief Information Security Officer)		Dec 17, 2021

Revision History

Version #	Version Date	Reviewed By	Changes in Document
0.1	Apr 16, 2021	KPMG	First draft released
0.2	Apr 23, 2021	Abhinab Chakraborty (Manager Office Of The Chief Information, Corporate Services)	Reviewed and feedback provided
0.3	May 20, 2021	KPMG	Draft updated
0.4	July 30, 2021	Abhinab Chakraborty (Manager Office Of The Chief Information, Corporate Services)	Reviewed and acknowledged
0.5	Aug 19, 2021	Sacha Blasiak-Priestley (Director Office Of The Chief Information, Corporate Services)	Reviewed and acknowledged
0.6	November 19, 2021	Sacha Blasiak-Priestley (Director Office Of The Chief Information, Corporate Services)	Revisions with consideration for feedback from TSD (Andy Kwong and Gary Mak)
0.7	December	Office of the CISO	Minor changes to the

	16, 2021		OC Policy template to reflect the CTO's/TSDs endorsement and role in the OC policies
1.0	Dec 17, 2021	Abiodun Morolari (Chief Information Security Officer)	Approved for publication as a first release

Approval History

Version #	Approval Date	Approved By	Approved with comments	Next Review
1.0	Dec 17, 2021	Abiodun Morolari (Chief Information Security Officer)	Approved for publication as a first release	12/2022

Contact Information

Director, Threat Management

Email: CISO@toronto.ca

Office of the CISO

Table of Contents

Encryption Policy.....	2
Ownership/Stewardship	2
Endorsement.....	2
Approval.....	2
Revision History	2
Approval History	3
Contact Information.....	3
Table of Contents.....	4
1 Purpose	7
2 Application	7
3 Definitions.....	7
4 Policy	10
4.1 Selection and Implementation of Cryptographic Solutions.....	10
4.1.1 Risk Assessment	10
4.1.2 Use of Proprietary Cryptographic Solutions	10
4.1.3 Protecting Sensitive Information	10
4.1.4 Impact on Content Inspection	10
4.1.5 Lifespan of Certificates	10
4.1.6 Applicable Legislative and Regulatory Requirements	10
4.1.7 Authentication of Public Keys.....	11
4.2 Application of Cryptographic Solutions	11
4.2.1 Cryptographic Criteria.....	11
4.3 Acceptable Cryptography	11
4.3.1 Hashes and Digital Signatures.....	11
4.3.2 Annual Reviews.....	11
4.3.3 Restrictions	11
4.4 Key Management.....	12
4.4.1 Key Management Procedures.....	12
4.4.2 Activation and Deactivation.....	12

4.4.3 Time Stamps.....	12
4.4.4 History of Cryptographic Keys.....	12
4.5 Dual Control of Keys.....	13
4.5.1 Dual Control of Keys Principle.....	13
4.5.2 Separate Key Pairs	13
4.6 Cryptographic Solutions and Cloud Service Providers.....	13
4.6.1 Managing the Key Management System.....	13
4.7 Sharing and Communicating Keys	13
4.7.1 Secure Sharing	13
4.7.2 Need-To-Know Basis	13
4.8 Compromised Keys	13
4.8.1 Information Recovery Process	13
4.8.2 Reporting on Compromised Keys	14
4.8.3 Periodic Key Changes	14
4.8.4 Key Disposal	14
4.9 Record Keeping.....	14
4.9.1 Access Control Logs.....	14
4.9.2 Record Keeping Cryptographic Solution Register	14
4.9.3 Key Status Changes	15
4.9.4 List of Application Certificates and Keys.....	15
4.10 Protection of Cryptographic Equipment.....	15
4.10.1 Protection against Unauthorized Access.....	15
4.10.2 Storage Site.....	15
4.10.3 Hardware Security Module.....	15
4.10.4 Transporting Procedures	15
4.10.5 Cryptographic Equipment Serial Numbers.....	15
4.10.6 New Equipment Inspection	15
4.10.7 Inspection Reference Materials.....	16
5 Policy Approval and Review Schedule	16
6 Compliance and Violation	16
7 Exceptions to Compliance.....	17

8	Applicable Legislation and Regulations	17
9	Related Documents.....	17
10	Responsibilities	18
10.1.1	Assign Responsibilities.....	18
10.1.2	Key Custodians.....	18
10.1.3	Key Users	19

1 Purpose

The Encryption Policy document defines the policies and standards that all employees, contractors, vendors and/or service providers are obligated to adhere to for protecting the confidentiality, integrity and availability of the technology and information assets of the City of Toronto.

This policy is intended to provide direction on the types of processes and procedures that should be carried out in a consistent manner to ensure that the City's information technology (IT) assets and operational technology (OT) assets are adequately protected.

Any changes to be made within this policy must be made in adherence with the City's [policy excellence practices](#).

This policy defines the City's commitment to cyber security, specifically with:

- The criteria to adhere to when selecting and implementing cryptographic solutions.
- The specific instances in when cryptographic solutions should be applied.
- The necessary procedures and requirements to manage and protect keys against modification and loss throughout their lifecycle.
- The defined principles that should be applied to exist to minimize the risk of keys being compromised or used inappropriately during their lifecycle.
- The means to protect cryptographic equipment during storage and transportation from unauthorized use and tampering.
- The defined requirements and responsibilities of the individuals that have access to cryptographic keys.

2 Application

This policy is applicable to all authorized individuals using IT and OT provided by the City and for authorized individuals accessing the City of Toronto infrastructure, IT assets, OT and information to fulfill their duties and the City's business goals. All City information and technology assets are subject to these policies and standards, regardless of their use or physical location. Every individual is required to read and attest to complying with the requirements associated within their role. Additional roles and responsibilities will be specified within the policy, as required.

3 Definitions

Accountability: Refers to the ability to hold individuals liable for the consequences of their actions. Individuals could be responsible for their actions but may not be held accountable.

Authentication: The ability to corroborate the identity of a person or system based on the presentment of credentials.

Authorization: The ability to grant access to a person or system.

Authorized Users: All individuals who have been granted access to the City's IT Assets. This includes, but is not limited to, employees, consultants, contractors, subcontractors, vendors, and business partners, individuals on secondment to the City, students and volunteers at the City of Toronto.

Availability: Defined as ensuring timely and reliable access to and use of information by authorized users and systems. A loss of availability is the disruption of access to or use of information or an information system.

Confidentiality: Defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and property information. A loss of confidentiality is the unauthorized disclosure of information.

Cryptography: The enciphering and deciphering of messages into code or cipher.

Cyber Security: Defined as the practice of defending computers, servers, mobile devices, electronic systems, networks, information and data from malicious attacks, compromise or theft. It can also be known as IT security, electronic information security or information security. Cyber security is defined in terms of confidentiality, integrity, availability, identification, authentication, authorization, and non-repudiation.

Digital Signature: The method of verifying the authenticity of digital messages or documents.

Dual Control: The practice of requiring two or more individuals to perform a function. A single individual is unable to retrieve the output independently.

Encryption: The process of converting information or data into a code to prevent unauthorized access (see *Cryptography*).

Hardware Security Module (HSM): The device that protects and manages digital keys in addition to performing cryptographic functions, such as encryption and decryption for digital signatures.

Hash Function: The methodology of transforming the input value into a fixed-length output which can be easily referenced and is unique.

Hypertext Transfer Protocol Secure (HTTPS): Protocol used for secure communication over the network.

Identification: The presentment of credentials or identifiers that uniquely distinguish a person or system.

Information Assets: Information is what both the corporation and authorized individuals know, manage, and use, both collectively and individually. Information is inclusive of all data and knowledge that is applied to the business context and forms the basis upon which decisions are made. Information assets are both intangible: represented as raw data in repositories such as computer files and databases; and tangible: represented in printed, hard-copy reports or other physical media. Appropriate due care of the City information assets extends to both formats so that they are safeguarded against security breaches that could adversely affect their confidentiality, integrity and availability.

Information Technology (IT) Assets: Any system, service, hardware, software and network assets that are owned by or supplied to Authorized Users by the City. This includes, but is not limited to, desktop computers, monitors, printers, notebooks, mobile devices, digital projectors, scanners, storage devices, networks and network devices, software, cloud based software or platforms, internet access, email, communication and business applications, telephones and voice mail, facsimile machines, and photocopiers.

Integrity: Defined as guarding against improper addition, modification, or destruction of information. Enforcing integrity to preserve the timeliness, accuracy, and completeness of information.

Key Custodian: The assigned individual responsible for managing keys throughout their lifecycle.

Management: A team of individuals that are responsible for overseeing, coordinating, and managing activities at the City to ensure that objectives and compliance with requirements are met.

May: The item is an optional requirement.

Must: An absolute requirement of the specification.

Non-repudiation: The ability to irrefutably associate a person or system with a transaction, process or event.

Office of the CISO: The central group within the City that provides cyber security services across all City divisions.

Operational Technology (OT) Assets: Any device or system that monitors, manages or automates operational processes and supports industrial equipment. This includes, but is not limited to, any hardware, software or equipment that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Responsibility: Refers to the obligations and general behaviour of an individual. It implies a proactive stance on the part of the responsible party and a causal relationship between the responsible party and a given outcome.

Risk Assessment: The overall process of risk identification, risk analysis and risk evaluation.

Secure Sockets Layer (SSL): The standard that permits encrypted communication between a web browser and a web server.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS): The cryptographic protocols to ensure communications over the network is secure.

Sensitive Information: Includes, but is not limited to, privileged information, draft by-laws or staff reports, third party information, personal information, technical or financial or scientific information and any other information collected, obtained or derived for or from City records that must or may be kept confidential under the Municipal Freedom of Information of Privacy Act, the Personal Health Information Protection Act, 2004 or the City of Toronto Act, 2006.

Shall: Means an absolute requirement of the specification. See "MUST"

Should: Means there may be valid reasons in particular circumstances to ignore a particular item,

but the full implication must be understood and carefully considered before choosing a different course.

Split Knowledge: The method in which two or more individuals have their own key components and the individual key component does not convey the original cryptographic key.

Technology Services Division (TSD): The central group within the City that provides IT services across all City divisions.

4 Policy

4.1 Selection and Implementation of Cryptographic Solutions

4.1.1 Risk Assessment

A risk assessment via CISO intake process shall be performed to determine the required level of protection, such as the type of algorithm that should be used to protect the confidentiality, integrity and availability of information. The application of cryptographic solutions must be documented and communicated via prescribed standards across the organization for consistency.

4.1.2 Use of Proprietary Cryptographic Solutions

The use of proprietary cryptographic solutions is not allowed for any purpose, unless reviewed and approved by the Office of the CISO. Due diligence must be performed by the Office of the CISO by conducting appropriate risk assessments during any selection, approval and implementation process of cryptographic solutions.

4.1.3 Protecting Sensitive Information

Assets that store, process or transmit sensitive information must be protected using approved encryption algorithms with key lengths equal to or above industry standards (e.g. Advanced Encryption Standard (AES) 128-bit, 192-bit or 256-bit).

4.1.4 Impact on Content Inspection

The selection of a cryptographic solution must consider the impact it has on controls that rely on content inspection (e.g. malware detection or content filtering). Compensating controls should be considered such as endpoint agents to minimize the risk that may arise from data not being scanned as a result of the encryption.

4.1.5 Lifespan of Certificates

The lifespan of Secure Sockets Layer (SSL) certificates must be maintained and HTTPS (SSL/TLS) is enabled on a site-wide basis.

4.1.6 Applicable Legislative and Regulatory Requirements

All cryptographic solutions must comply with applicable legislative and regulatory requirements.

Discretionary methods to provide authorities with access to the encrypted information must be defined and documented.

4.1.7 Authentication of Public Keys

The authentication of public keys shall be accomplished using public key certificates, which may be issued by a certification authority. This authority must be a reputable organization with the appropriate controls and procedures in place.

4.2 Application of Cryptographic Solutions

4.2.1 Cryptographic Criteria

Cryptographic solutions are necessary when:

- Sending sensitive files, attachments or messages, via email or other end-user messaging methods, electronic meetings and/or collaborative tool services, both internally and externally.
- Using methods of communication between clients, business partners or other parties whereby the communications lines are deemed insecure.
- Any files or information that must be stored, transported, distributed or archived in non-secure or non-bonded environments.
- Any files or information that can be potentially accessed by unauthorized persons or mechanisms.
- Removable devices, such as USBs, are used.
- Required by industry regulations or by law.
- Digital signatures or message authentication codes are used to verify the authenticity or integrity of the transmitted information.
- Confirmation that the data has been received by the intended party is required.

4.3 Acceptable Cryptography

4.3.1 Hashes and Digital Signatures

Hash functions or digital signatures should be used to protect sensitive or critical information. Standard hashing and cryptographic solutions with best practice entropy effectiveness must be used for all cryptographic operations.

4.3.2 Annual Reviews

The approved algorithms and key length requirements must be reviewed annually and upgraded as technology allows.

4.3.3 Restrictions

As there are countries that do not allow the import of encrypted files, permission to send an

encrypted file to a specific country must be determined in advance, in consultation with the Office of the CISO via CISO intake process.

4.4 Key Management

4.4.1 Key Management Procedures

The procedures to manage and protect keys against modification and loss throughout their lifecycle must be defined and documented. Secret and private keys must be carefully protected against unauthorized use and disclosure.

The key management system shall be based on an agreed set of procedures and secure methods for:

- Generating keys using the approved key lengths.
- Generating and obtaining public key certificates.
- Distributing keys to intended users, including how keys must be activated when received.
- Storing keys, including how authorized users obtain access to keys.
- Changing or updating keys, including rules on when keys must be changed and how this must be done.
- Handling compromised keys.
- Revoking keys, including how keys must be withdrawn or deactivated (e.g. when keys have been compromised or when a user leaves the organization, in which case the keys must also be archived).
- Recovering keys that are lost, corrupted or have expired.
- Archiving keys.
- Destroying keys.
- Logging and auditing of key management related activities.

4.4.2 Activation and Deactivation

Activation and deactivation dates for keys shall be defined and the keys can only be used for the defined period.

4.4.3 Time Stamps

A time source shall be defined (e.g. Network Time Protocol (NTP)) to ensure that the key custodian is using accurate time stamps.

4.4.4 History of Cryptographic Keys

Keys must be archived for as long as any enterprise information is encrypted or signed with this key and exist either on live systems or on backup media. If system capabilities permit, keys may have to be kept available for the lifetime of the key management solution to ensure no data loss. At minimum, keys need to be available for the longest data retention period needed for system

records encrypted with them, or for 7 years, whichever is longer. The history of cryptographic keys must be maintained.

4.5 Dual Control of Keys

4.5.1 Dual Control of Keys Principle

Dual control and split knowledge principles shall be utilized throughout the key life cycle (creation, transmission, loading and administration) to ensure that sufficient controls exist to minimize the risk of keys being compromised or used inappropriately during their lifecycle.

4.5.2 Separate Key Pairs

Separate key pairs shall be generated for encrypting and decrypting information or producing and validating digital signatures. Separating the cryptographic key pairs for encryption and digital signatures allows one pair to be deactivated or replaced while the other key pair remains valid.

4.6 Cryptographic Solutions and Cloud Service Providers

4.6.1 Managing the Key Management System

When sensitive information is handled in a public or service provider cloud environment, the cloud service provider shall establish policies and procedures for the management of cryptographic keys in the service's cryptosystem (e.g. lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, the provider shall inform the City of Toronto of changes within the cryptosystem, especially if the City of Toronto information is used as part of the service, and/or the City of Toronto has some shared responsibility over implementation of the control.

4.7 Sharing and Communicating Keys

4.7.1 Secure Sharing

The process of securely sharing cryptographic keys must be established and documented.

4.7.2 Need-To-Know Basis

Cryptographic keys shall be used and distributed on a need-to-know basis to authorized individuals and be stored in the fewest possible locations.

4.8 Compromised Keys

4.8.1 Information Recovery Process

The process for recovering the encrypted information if the key is lost, compromised or

damaged must be defined and documented. This process require review by OC, TSD, and Divisional IT to prevent unauthorized access to data during recovery.

4.8.2 Reporting on Compromised Keys

Any compromises to keys or potential compromises must be immediately reported to Office of the CISO.

4.8.3 Periodic Key Changes

Keys shall be changed periodically as defined in the appropriate key management process, or when the integrity has been suspected to be compromised or weakened.

4.8.4 Key Disposal

Keys and any respective components that are no longer in use due to compromise or being replaced by a new key, must be destroyed. The means of disposal must ensure that the content is made unrecoverable.

4.9 Record Keeping

4.9.1 Access Control Logs

An Access Control Log should be established and maintained for access to key management systems, certificate authorities, and other public key infrastructure. This log must contain the following information:

- Custodian Names (primary and secondary).
- Access / Replacement / Removal Date Timestamp.
- Name of component accessed or removed.
- Reason for access / removal.
- Encryption technique(s) (e.g. software, hardware, firmware, or any combination thereof).

4.9.2 Record Keeping Cryptographic Solution Register

A register of approved cryptographic solutions must be created, maintained and regularly reviewed. At a minimum, this inventory and audit trail must contain details of:

- Key name and purpose/usage.
- Key type.
- Activation and deactivation dates.
- Number of components.
- Storage location(s).
- Custodians (all dates since generation).
- Information related to licensing requirements.

- Dates of any changes (e.g. replacement, rotation, destruction).
- Inventory of any Hardware Security Module (HSM) and other Secure Cryptographic Device (SCD) used for key management and performing cryptographic functions.

4.9.3 Key Status Changes

Any changes to the status of a key must be performed in a formally defined change management procedure. All cryptographic key management activities must be logged, and the inventory of cryptographic keys must be updated.

4.9.4 List of Application Certificates and Keys

The Office of the CISO shall maintain a list of applications for which issued certificates and/or identified key types are suitable for, restricted and prohibited.

4.10 Protection of Cryptographic Equipment

4.10.1 Protection against Unauthorized Access

Equipment used to generate, store and archive keys must be physically and logically protected against access by unauthorized individuals, tampering and modification. Audit log should be in place for tracking physical or logical access. A hardening standard must be defined to ensure that all known vulnerabilities are patched, and unnecessary services are disabled.

4.10.2 Storage Site

The storage site of cryptographic equipment must only be accessed by authorized personnel.

4.10.3 Hardware Security Module

Keys shall be stored in an HSM which should be safeguarded with strong physical and logical controls and should be properly maintained. The HSM is designed to encrypt and decrypt information and to manage digital keys.

4.10.4 Transporting Procedures

Proper transporting procedures must be developed and followed when cryptographic equipment is moved to or from City of Toronto premises. These procedures are in place to prevent or detect access by unauthorized personnel from the time of manufacture or removal from service to the time that the key is in transit from the manufacturer to or from City of Toronto premises. The equipment must be transported via a bonded courier and packaged securely to preserve the integrity of the device.

4.10.5 Cryptographic Equipment Serial Numbers

The serial number on the cryptographic equipment must match the serial number provided by the manufacturer either in a written format or communicated verbally.

4.10.6 New Equipment Inspection

All new cryptographic equipment must be inspected during the commissioning process. The equipment must be inspected for signs of tampering or modification on a quarterly basis.

4.10.7 Inspection Reference Materials

The inspector must use vendor supplied drawings or photographs as a reference during the inspection. Any variances must be brought immediately to the attention of the Office of the CISO.

5 Policy Approval and Review Schedule

The Office of the CISO has developed this policy in alignment with cybersecurity best practices and framework (NIST and ISO 27001/ISO 27002).

This policy is submitted to the Accountable Director within the Office of the CISO's Senior Management Team for final approval and the Chief Technology Officer for Endorsement.

This policy is reviewed annually and updated as necessary. Review and re-issuance ensure that the Policy direction and content remain current with changes to the City's cyber security risk profile that include, but are not limited to:

- Security incidents.
- New vulnerabilities.
- Technology advancements.
- Changes in organizational design.
- High-risk, high-profile business transformation initiatives.
- Changes in regulatory or legislative requirements.
- Privacy breaches.

6 Compliance and Violation

Authorized users of IT resources or access to City of Toronto assets or information must comply with this policy.

Non-compliance with this policy may result in disciplinary action up to and including termination of employment, privileges and/or contract relationship. Investigations of non-compliance will be undertaken with due consideration of the rights of the individual under investigation. Depending on the nature and gravity of the violation, it may constitute an offence and result in related penalties under applicable legislations.

Prior to using any infrastructure, IT assets and/or information, authorized users should request a clarification through their supervisor if they have any concerns regarding compliance with this policy. A privacy breach may be reported to the appropriate regulatory body, such as the Information and Privacy Commissioner, where applicable.

Security breaches or incidents must be reported to the Office of CISO and Chief Technology Officer Intake Process.

7 Exceptions to Compliance

Where compliance is not immediately possible, a request for an exemption must be submitted for review by the Office of the CISO Director or the appropriate Division Head. The process and required stakeholders to manage contingencies to exceptions shall be aligned to the Office of the CISO and Chief Technology Officer Intake process. This request must contain a plan to become compliant as well as a contingency plan to reduce risk during the non-compliance period. If the exception is approved by the Office of the CISO, the risk owner must sign off and own the exception. All exemptions with supporting details must be documented and reported to the Office of the CISO's Senior Leadership. All exceptions to this policy will be tracked and monitored by the Office of the CISO.

8 Applicable Legislation and Regulations

In addition to adhering to this document, the following laws and regulations shall be complied with.

Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) provide individuals with a right of access to certain records and personal information under the custody or control of institutions covered for the Acts. The purpose of the MFIPPA is as follows:

- To provide a right of access to information under the control of institutions in accordance with the principles that:
 - Information should be available to the public,
 - Necessary exemptions from the right of access should be limited and specific,
 - Decisions on the disclosure of information should be reviewed independently of the institution controlling the information.
- To protect the privacy of individuals with respect to personal information about themselves held by institutions and to provide individuals with a right of access to that information.

The **Personal Health Information Protection Act (PHIPA)** sets out rules for the collection, use and disclosure of personal health information. These rules will apply to all health information custodians operating within the province of Ontario and to individuals and organizations that receive personal health information from health information custodians.

The **Freedom of Information and Protection of Privacy Act (FIPPA)** legislates access to information held by public institutions in Ontario subject to specific requirements to safeguard the personal information of individuals.

9 Related Documents

- [Policy Excellence Practices](#)
- Cyber Risk Management Framework*

- Cyber Security Policy
- Governance, Risk, and Compliance Policy
- Third Party Risk Policy

* This document to be finalized.

10 Responsibilities

The City of Toronto shall ensure compliance with this policy across the organization, with assistance of the Office of the CISO, by providing direction on individual responsibilities and the specific procedures to be followed. The division should have a reporting cadence with the management of each division to confirm that their employees are compliant.

Please see the Cyber Security Policy [REFERENCE NUMBER] for a detailed description of cyber security responsibilities across City roles.

Specific roles and responsibilities for this policy are defined as follows:

10.1.1 Assign Responsibilities

The following responsibilities shall be defined and assigned individual accountability for key management responsibilities:

- Central oversight authority.
- Oversight for relationships with certification authorities.
- Oversight for relationships with registration authorities.
- Compliance auditor.
- Resolving conflicting laws and regulations related to the use of cryptographic solutions.
- Overseeing and approving key management operations.

10.1.2 Key Custodians

A key custodian who is responsible for managing keys (e.g. generation, distribution, archiving, updating, rotating, revocation, destruction) must be assigned in agreement by the TSD and Office of the CISO. Due diligence must be performed during the hiring process.

The key custodian shall be responsible for archiving public key certificates and certificate revocation lists in an archive database.

In addition to the City's hiring process, the requirements of the key custodian must include the following:

- Have at least one-year satisfactory service with the City of Toronto and be full-time employee (no contractors, or part-time employees).
- Be selected from different City of Toronto divisions, where possible.
- Neither of the key custodians can report to another key custodian on the organization

chart.

- Not have a family relationship (by blood or marriage) with any other custodian for a key or related key.
- Not be involved in the application development for which the key is to be used (e.g. no programmers or system administrators with intimate technical knowledge).
- Renew their role every two years.

Custodians must protect their keys against disclosure and misuse. Keys must not be disclosed to anyone, including their manager or an auditor. Prior to issuing keys, the custodian must be able to successfully verify that the individual is authorized to receive the key.

10.1.3 Key Users

Users of the cryptographic keys must be aware of the purpose and function of the key, their responsibilities to protect the key, and how to use the key (e.g. using encryption and digital signatures).