Ontario Health

Cryptography Standard

Version: 1.8

Document ID: 3537

Document Control

Next Review Date: Every two years or otherwise established by the Connecting Security Committee.

Approval History

APPROVER(S)	APPROVED DATE
Connecting Security Committee	2017-02-21
Connecting Security Committee	2018-03-26
Connecting Security Committee	2021-03-18

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.0	2013-12-20	Nov 2013 version adopted from the cGTA PSWG	Mark Carter
1.1	2014-12-04	Updated policy based on feedback from the CSC members. Definitions added for Agent, Data Contribution Endpoint and Identity Provider Services. Max certificate lifespan set to 5 years. TLS 1.1+ added as acceptable cryptographic protocols.	Mark Carter
1.2	2014-12-12	Updated policy based on the Dec 11th CSC meeting. 1.28, 2.47 – key lifespan was set at 7 years to align with infrastructure refresh cycle; 1.33, 2.54 – key custodian responsibilities are to be assign by the CIO or delegate; 1.34, 2.55 – revised accountability for keys are required keys to be handled in a Restricted manner in line with the Information and Asset Management Policy.	Mark Carter
1.3	2015-01-22	Policy tabled at regional privacy and security committees, approved by all CSC members as of Jan 22nd 2015.	Mark Carter
1.4	2015-10-19	Updated policies to note the change in governance. The Steering Committee was replaced by the Applicable Oversight Body. The regional privacy and security committee has been removed from the exemption decision process.	Mark Carter
1.5	2017-02-21	Updated policies to incorporate 2017 refresh changes. Definition of EHR Solution was adjusted. A number of controls were rephrased to note “participating” in the EHR Solution.	Ravi Addepalli
1.6	2018-03-16	Updated standard to include Patient access to the EHR.	Geovanny Diaz

VERSION NO.	DATE	SUMMARY OF CHANGE	CHANGED BY
1.7	2020-03-16	Updated with FIPS 140-3 that supersedes FIPS 140-2. Reviewed and updated the table of approved cryptographic algorithms.	Ana Fukushima
1.8	2021-01-21	Review of the document with minor changes, updated references and the review cycle to biennially.	Ana Fukushima

Cryptography Standard

Purpose

To define the information security controls that are required to implement and manage cryptographic solutions.

Scope

This standard applies to and all [the EHR Solution] components.

For health information custodians (HICs) that use [the EHR Solution] to view, handle or otherwise deal with personal health information (PHI) by provisioning access through:

- **Local identity provider technology** (local IdP), this standard applies to:
    - The HIC's local access control and identity management infrastructure ("identity provider services") that manages the authentication and authorization used to provide access to [the EHR Solution] (e.g., [the EHR Solution] Security Token Service Solution, Microsoft Active Directory Federation Services 2.0, etc.)
    - Direct network connectivity to [the EHR Solution] Provider Portal and administrative functionality, including components in the connection path (firewalls, proxies, etc.)
    - The integration of [the EHR Solution] Provider Portal with the HIC's local health information system (HIS) or electronic medical record (EMR) application(s).

- **Ontario Health's ONE ID service**, this standard applies to:
    - Direct network connectivity to [the EHR Solution] administrative functionality, including components in the connection path (firewalls, proxies, etc.)

In addition to the scope set out for viewing sites, for HICs that create or contribute PHI to [the EHR Solution] Clinical Data Repository ("contributing sites"), this standard also applies to:

- The data contribution endpoints that provide PHI to [the EHR Solution]'s Clinical Data Repository
- The information technology and processes that ensure the quality of the data submitted (e.g., terminology mapping)

This standard does not apply to any HIC, their agents or their Electronic Service Providers who do not have create, contribute, view or access to [the EHR Solution].

Definitions

[The EHR Solution]: [The EHR Solution] and supporting systems designed to store and make available specified electronic PHI from the electronic health information systems of HICs.
[The EHR Solution] includes Patient Portals/Applications (HIC or non-HIC affiliated) that facilitate Patient access to the EHR. These applications may be:

- Provider-Gated (Provider facilitates communication with Patient)
- Direct-to-Patients (Patient has direct access to EHR)
- Patient-Gated (Patient delegates access to a Substitute Decision Maker/additional delegates (i.e., family member, physician)

[The EHR Solution] Program: Also known as the Program Office; consists of Agents and Electronic Service Providers who support [the EHR Solution] including privacy and security-related activities, initiatives and processes.

Applicable Oversight Body: The Applicable Oversight Body is comprised of senior-level executives who oversee all aspects of [the EHR Solution]. See the Policy Governance Structure section within the Information Security Policy.

Agent: In relation to a health information custodian, means a person that, with the authorization of the custodian, acts for or on behalf of the custodian in respect of personal health information for the purposes of the custodian, and not the agent's own purposes, whether or not the agent has the authority to bind the custodian, whether or not the agent is employed by the custodian and whether or not the organization is being remunerated. For example, an agent may be an organization, employee or contractor that validates identities of the EHR users on behalf of a HIC; an Agent may perform data correction services for a HIC on their data contribution endpoint.

Data Contribution End Point(s): Technology and related processes that provide data to the Clinical Data Repository or are queried to provide data to a Clinical Viewer. Typically, these systems are the Information System (e.g., Hospital Information System, Laboratory Information System, Clinical Information System, HL7 Interface Engine, etc.) that directly connects to [the EHR Solution] to provide clinical data.

Electronic Service Provider: A person or entity that provides goods or services for the purpose of enabling a HIC to use electronic means to collect, use, modify, disclose, retain or dispose of PHI, and includes a health information network provider.

Information system: A discrete set of information technology organized for the collection, processing, maintenance, use, disclosure, destruction, or disposal of information.

Identity Provider Services: Technology and related supporting services, policies, processes, and procedures that are used to create, maintain, secure, validate, assert and manage electronic identities to [the EHR Solution].

Information technology: Any asset (physical or logical) that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. It includes, but is not limited to, hardware, software, firmware, ancillary equipment, and related resources.

Key Custodian: An agent or Electronic Service Provider who has been authorized to handle all or part of a cryptographic key throughout the key's lifecycle from generation through to destruction.

Message Authentication Code (MAC): A cryptographic checksum on data that uses a session key to detect both accidental and intentional modifications of the data. A MAC uses a message and a secret key to generate a "MAC tag" that is difficult to generate for a given message without knowledge of the key.

Dual control: A control procedure whereby the active involvement of two people is required to complete a specified process.

Split Knowledge: A procedure whereby information is handled as multiple components from the time of generation until they are combined for use. Each component provides no knowledge of the ultimate message.

Shall/Must: Used for absolute requirements, i.e., they are not optional.

Should: Used when valid reasons exist in certain circumstances not to implement the requirement; however, the implementer must understand the implications before choosing a different course and must consider implementing compensating controls.

May: The requirement is only a recommendation, or provided as an implementation example and is not intended on being exhaustive.

Standard Requirements

1. Requirements for Health Information Custodians

1.1. HICs must only use [the EHR Solution]-approved cryptographic algorithms to participate in [the EHR Solution]. A list of approved cryptographic algorithms can be found in Appendix A: Approved Cryptographic Algorithms.

1.2. HICs must assess each proposed implementation of a cryptographic solution on their identity provider services and data contribution endpoints.

1.3. HICs must ensure that cryptographic solutions on their identity provider services and data contribution endpoints fail close (i.e., access is denied if a failure occurs).

1.4. HICs should use hardware cryptography (rather than software cryptography) for their identity provider services and data contribution endpoints.

1.5. Where cryptographic hardware devices are used (e.g., RSA Token) for their identity provider services and data contribution endpoints, HICs must ensure that the cryptographic hardware devices meet or exceed the tamper-resistant enclosure requirements specified in the Federal Information Processing Standards (FIPS) 140-3 standard.

1.6. HICs should only use software cryptography solutions on their identity provider services and data contribution endpoints for:

1.6.1. One-way (or non-reversible) cryptographic functions;

1.6.2. Client-side software for remote access;

1.6.3. Client-side storage encryption such as full-disk encryption; or

1.6.4. Client-side or server-side digital certificates.

1.7. Where software-based cryptography is implemented, HICs must ensure that the password is not stored in a program, batch file, or script file, with the exemption of server-based TLS digital certificates, which must have strict access control placed on the file that contains the password.

Digital Certificates on identity provider services and data contribution endpoints

1.8. HICs must ensure that all digital certificates are revocable with a cryptographically secured certificate revocation list (CRL) system.

1.9. HICs must ensure that a digital certificate is only trusted once it has been cryptographically validated and does not appear on a trusted CRL.

Key Management

1.10. HICs must protect their cryptographic keys for their identity provider services and data contribution endpoints against unauthorized access (in the case of secret and private keys), modification, loss, and accidental or intentional destruction.

1.11. HICs must ensure that equipment used to generate, load, store and archive cryptographic keys for their identity provider services and data contribution endpoints are physically protected against unauthorized access or modification.

1.12. HICs should establish a process for managing cryptographic keys for their identity provider services and data contribution endpoints, which covers:

1.12.1. The secure generation, distribution, loading, storage, recovery, replacement, revocation and destruction of cryptographic keys; and

1.12.2. The secure back-up and archive of cryptographic keys.

1.13. HICs must maintain an inventory of their cryptographic keys and key components associated with their identity provider services and data contribution endpoints. The inventory should contain the following:

1.13.1. Key name and purpose/usage.

1.13.2. Key type.

1.13.3. Key generation date.

1.13.4. Component number, including the total number of components.

1.13.5. Storage location(s).

1.13.6. All key custodians since generation, including the dates of custodial changes.

1.13.7. The date the key was destroyed, and proof of destruction.

1.14. HICs should review the inventory of keys associated with their identity provider services and data contribution endpoints annually.

1.15. HICs should maintain logs to record any instance in which keys, key components, or related materials for their identity provider services and data contribution endpoints are generated, removed from storage or loaded to a cryptographic device. Logs may include:

1.15.1. Key name and purpose/usage.

1.15.2. Date and time.

1.15.3. Component identifier.

1.15.4. Purpose of access.

1.15.5. Name and signature of custodian accessing the component.

1.15.6. Tamper evident package number pre and prior to removal (if applicable).

1.16. HICs must restrict access to cryptographic keys or key components, and key devices for their identity provider services and data contribution endpoints to the designated key custodians and their backups.

1.17. HICs should store keys for their identity provider services and data contribution endpoints in the fewest possible locations and forms.

Key Generation

1.18. HICs must ensure that all keys and key components for their identity provider services and data contribution endpoints are generated using a random number generator or a pseudo-random number generator that passes all the basic tests for statistical randomness as defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-22 Revision 1a.

1.19. To ensure the confidentiality of secret keys for their identity provider services and data contribution endpoints, HICs must ensure that secret keys only exist in the following forms:

1.19.1. As cleartext inside the protected memory of a tamper-resistant security module (TRSM);

1.19.2. As ciphertext outside the protected memory of a TRSM; or

1.19.3. As two or more components, held under split knowledge and dual control.

1.20. HICs should require the output of the key generation process for their identity provider services and data contribution endpoints to be monitored by at least two authorized agents or Electronic Service Providers.

1.21. HICs must ensure that multi-use or multi-purpose computing systems are not used for a key generation where any clear-text secret key or key component may appear in unprotected memory.

Key Loading

1.22. HICs must ensure that keys or key components for identity provider services and data contribution endpoints are never loaded (or reloaded) when there is any suspicion that either the key, key components or the cryptographic device have been compromised.

Key Use

1.23. HICs must only use cryptographic keys on their identity provider services and data contribution endpoints for a single intended purpose and must never share these keys between production and non-production environments.

Key Lifespan and Destruction

1.24. A certificate key lifespan must be no longer than 7 years.

1.25. HICs must replace an uncompromised key used for their identity provider services and data contribution endpoints on or before its stipulated lifespan.

1.26. If a key or key component for a HIC's identity provider services and data contribution endpoints has been compromised or is suspected of being compromised, the HIC must:

1.26.1. Replace the compromised or suspected compromised key as soon as possible. The replacement key must not be a variant of the original key.

1.26.2. Inspect the cryptographic device for any form of unauthorized modification before installing the new key or key component.

1.27. HICs must promptly revoke all keys or key components for their identity provider services and data contribution endpoints when no longer required and ensure that the key or key components are securely destroyed.

1.28. HICs should require the destruction of their keys or key components for their identity provider services and data contribution endpoints to be witnessed by the key custodians and the details of the destruction recorded for audit purposes. The record may include:

1.28.1. The date and time of the keying material destruction.

1.28.2. The reason for destroying the keying material.

1.28.3. The full name and signature of the individual authorizing the destruction.

1.28.4. The full name and signature of the individual destroying the keying material.

1.28.5. The full name and signature of all persons witnessing the destruction.

Key Custodians

1.29. The Chief Information Officer or their delegate must assign the Key Custodian(s) responsible for each key.

1.30. HICs must ensure that key custodians for their identity provider services and data contribution endpoints handle the key or key component in their custody in a Restricted manner as described in the Information and Asset Management Policy.

1.31. HICs must ensure that each cryptographic key or key component has the fewest number of key custodians necessary.

1.32. HICs must ensure that key custodians understand their responsibility to never disclose the key or key component in their custody to anyone, not even to a manager or an auditor, except to another authorized key custodian for that specific key or key component.

2. Requirements for [the EHR Solution]

2.1. Only [the EHR Solution]-approved cryptographic algorithms shall be implemented on [the EHR Solution]. A list of approved cryptographic algorithms can be found in Appendix A: Approved Cryptographic Algorithms.

2.2. [The EHR Solution] Program must ensure that each proposed implementation of a cryptographic solution on [the EHR Solution] is assessed by an information security specialist.

2.3. [The EHR Solution] Program must only implement cryptographic solutions that fail close (i.e., access is denied if a failure occurs).

2.4. [The EHR Solution] Program must ensure that all implementations of cryptography have documented contingency procedures prior to production implementation. These procedures must be made available to all relevant stakeholders.

2.5. [The EHR Solution] Program should use hardware cryptography (rather than software cryptography such as an RSA Token) in environments that store or process PHI.

2.6. Where cryptographic hardware devices are used, [the EHR Solution] Program must ensure that these devices meet or exceed the tamper-resistant enclosure requirements specified in the Federal Information Processing Standards (FIPS) 140- 3 standard.

2.7. [The EHR Solution] Program must only permit software cryptography solution to only be permitted for:

2.7.1. One-way (or non-reversible) cryptographic functions;

2.7.2. Client-side software for remote access;

2.7.3. Client-side storage encryption such as full-disk encryption;

2.7.4. Client-side or server-side digital certificates; or

2.7.5. Data storage in data centres.

2.8. Where software-based cryptography is implemented, [the EHR Solution] Program must ensure that the password is not be stored in a program, batch file, or script file, with the exemption of server-based TLS digital certificates, which must have strict access control placed on the file that contains the password.

2.9. [The EHR Solution] Program must cryptographically protect the integrity of their cryptographic keys, especially when their cryptographic keys are located in a publicly accessible location (e.g., Internet-facing webserver).

Digital Certificates

2.10. [The EHR Solution] Program must ensure that all digital certificates are revocable.

2.11. [The EHR Solution] Program must ensure that a digital certificate is only trusted once it has been cryptographically validated and does not appear on a trusted CRL.

Key Management

2.12. [The EHR Solution] Program must protect their cryptographic keys against unauthorized access (in the case of secret and private keys), modification, loss, and accidental or intentional destruction.

2.13. [The EHR Solution] Program must ensure that equipment used to generate, load, store and archive cryptographic keys are physically protected against unauthorized access or modification.

2.14. [The EHR Solution] Program must establish a process for managing cryptographic keys, which covers:

2.14.1. The secure generation, distribution, loading, storage, recovery, replacement, revocation and destruction of cryptographic keys, and

2.14.2. The secure back-up and archive of cryptographic keys.

These processes and procedures must be made available to all relevant stakeholders.

2.15. [The EHR Solution] Program must maintain an inventory for all their cryptographic keys and key components. The inventory should include the following:

2.15.1. Key name and purpose/usage.

2.15.2. Key type.

2.15.3. Key generation date.

2.15.4. Component number, including the total number of components.

2.15.5. Storage location(s).

2.15.6. All key custodians since generation, including the dates of custodial changes.

2.15.7. Date the key was destroyed, and proof of destruction.

2.16. [The EHR Solution] Program should review the inventory of their cryptographic keys annually.

2.17. [The EHR Solution] Program must maintain logs to record any instance in which keys, key components, or related materials are generated, removed from storage or loaded to a cryptographic device. The logs should include:

2.17.1. Key name and purpose/usage.

2.17.2. Date and time.

2.17.3. Component identifier.

2.17.4. Purpose of access.

2.17.5. Name and signature of custodian accessing the component.

2.17.6. Tamper evident package number pre and prior to removal (if applicable).

2.18. [The EHR Solution] Program should review the audit logs of their keys annually.

2.19. [The EHR Solution] Program must restrict access to secret keys or key components, key devices and key materials to key custodians and their backups. Generally, the designation of a primary and a backup key custodian for each key or key component is sufficient.

2.20. [The EHR Solution] Program must store keys in the fewest possible locations and forms.

2.21. [The EHR Solution] Program must ensure that backup copies of secret keys exist only for the purpose of reinstating keys that are accidentally destroyed or are otherwise inaccessible. The backups must exist only in one of the allowed storage forms for that key.

2.22. [The EHR Solution] Program must ensure that the backup copies of secret keys are stored with strict access controls, under dual control, and subject to at least the same level of control as operational keys.

2.23. [The EHR Solution] Program must ensure that the creation of backup copies (including cloning) requires at least two authorized persons to enable the process. All requirements applicable for the original keys must also apply to any backup copies of keys and their components.

2.24. [The EHR Solution] Program must ensure that secret keys and key components that are no longer used or have been replaced are securely revoked and destroyed.

Key Generation

2.25. [The EHR Solution] Program must only permit a key generation process to be initiated by the key custodian.

2.26. [The EHR Solution] Program must ensure that all keys and key components are generated using a random number generator or a pseudo-random number generator that passes all the basic tests for statistical randomness as defined in the NIST Special Publication (SP) 800-22 Revision 1a.

2.27. To ensure the confidentiality of their secret keys, [the EHR Solution] Program must ensure that a secret key only exists in the following forms:

2.27.1. As cleartext inside the protected memory of a tamper-resistant security module (TRSM);

2.27.2. As cyphertext outside the protected memory of a TRSM; or

2.27.3. As two or more components, held under split knowledge and dual control.

2.28. [The EHR Solution] Program should ensure that the output of the key generation process is monitored by at least two authorized agents or Electronic Service Providers.

2.29. [The EHR Solution] Program must ensure that multi-use or multi-purpose computing systems are not used for a key generation where any clear-text secret key or key component thereof appears in unprotected memory.

Key Distribution

2.30. [The EHR Solution] Program must ensure that a key-encryption key (KEK) is transferred by physically forwarding the separate components of the key using different communication channels or is transmitted electronically in cipher-text form.

2.31. [The EHR Solution] Program must ensure that any sign of package tampering results in the destruction and replacement of the set of key components, as well as any keys encrypted under this (combined) key.

2.32. [The EHR Solution] Program must ensure that mechanisms exist to ensure that only authorized key custodians place key components into tamper-evident packaging for transmittal and that only authorized key custodians open tamper-evident packaging containing key components upon receipt.

Key Loading

2.33. [The EHR Solution] Program must ensure that keys or key components are never loaded (or reloaded) when there is any suspicion that either the key, key components or the cryptographic device have been compromised.

2.34. [The EHR Solution] Program must ensure that unencrypted secret keys are entered into cryptographic devices using the principles of dual control and split knowledge. In instances where a secure key loading device is used, only dual control is required.

2.35. [The EHR Solution] Program must ensure that any hardware used in the key-loading function is controlled and maintained in a secure environment under dual control.

2.36. [The EHR Solution] Program should require key custodians to examine all cable attachments before each key loading activity to ensure they have not been tampered with or compromised.

Key Use

2.37. [The EHR Solution] Program must define and implement procedures to prevent or detect the unauthorized substitution (unauthorized key replacement and key misuse) of one key or key component for another, or the operation of any cryptographic device without legitimate keys or key components.

2.38. [The EHR Solution] Program must ensure that cryptographic keys are only used for a single intended purpose and must never be shared between production and non-production environments.

2.39. [The EHR Solution] Program must ensure that all secret keys used for any function are unique (except by chance) to that device.

Key Lifespan and Destruction

2.40. A certificate key lifespan must be no longer than 7 years.

2.41. [The EHR Solution] Program must ensure that an uncompromised key is replaced on or before its stipulated lifespan.

2.42. If a key or key component has been compromised or is suspected of being compromised, [the EHR Solution] Program must:

2.42.1. Replace the compromised or suspected compromised key as soon as possible. The replacement key must not be a variant of the original key.

2.42.2. Inspect the cryptographic device for any form of unauthorized modification before installing the new key or key component.

2.43. [The EHR Solution] Program must ensure that their keys are promptly revoked when no longer required and ensure that the key is destroyed in accordance with [the EHR Solution] Information and Asset Management Policy.

2.44. [The EHR Solution] Program must ensure that the destruction of a key is witnessed by the key custodians with the appropriate records retained for audit purposes. Each key or key component destruction should record the following:

2.44.1. The date and time of the keying material destruction.

2.44.2. The reason for destroying the keying material.

2.44.3. The full name and signature of the individual authorizing the destruction.

2.44.4. The full name and signature of the individual destroying the keying material.

2.44.5. The full name and signature of the persons witnessing the destruction.

Key Custodians

2.45. The Chief Information Officer or their delegate must assign the Key Custodian(s) responsible for each key.

2.46. [The EHR Solution] Program must ensure that Key Custodians handle the key or key component in their custody in a Restricted manner as described in the Information and Asset Management Policy.

2.47. [The EHR Solution] Program must ensure that Key Custodians assigned to cryptographic keys are limited to the fewest number of key custodians necessary.

2.48. [The EHR Solution] Program must ensure that Key Custodians understand their responsibility to never disclose the key in their custody to anyone, not even to a manager or an auditor, except to another authorized Key Custodian for that specific key.

2.49. [The EHR Solution] Program must never permit a Key Custodian to be the custodian for more than one key component for the same key, even if the custodianship applies to the key components at different times.

Exemptions Any exemptions to this Policy must be approved by the Applicable Oversight Body, who will authorize exemptions only where there is clear justification to do so and only to the minimum extent necessary to meet the justified need.

Enforcement All instances of non-compliance will be reviewed by the Applicable Oversight Body.

The Applicable Oversight Body has the authority to impose appropriate penalties, up to and including termination of Agreements with the HIC, Electronic Service Provider or termination of the access privileges of agents, and to require the implementation of remedial actions.

References

Legislative

- PHIPA, ss. 12, 13 and Part V.1
- O. Reg. 329/04, s. 6

International Standards

- ISO/IEC 27001:2013, Information Technology – Security Techniques – Information Security Management Systems – Requirements
- ISO/IEC 27002:2013, Information Technology – Security Techniques – Code of Practice for Information Security Management
- ISO/IEC 27005: 2018 Information Technology – Security Techniques – Information Security Risk Management
- ISO 27799:2016 Health Informatics – Information security management in health using ISO/IEC 27002
- NIST SP 800-22 Revision 1a - A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- FIPS 140-3 - Security Requirements for Cryptographic Modules

Ontario Health EHR Policy Documents

- Information Security Policy
- Acceptable Use of Information and Information Technology Standard
- Access Control and Identity Management Standard for System Level Access
- Local Registration Authority Procedures Standard
- Identity Federation Standard
- Business Continuity Standard
- Cryptography Standard
- Electronic Service Providers Standard
- Information Security Incident Management Standard
- Information and Asset Management Standard
- Network and Operations Standard
- Security Logging and Monitoring Standard
- Systems Development Lifecycle Standard
- Physical Security Standard
- Threat Risk Management Standard

Appendix A: Approved Cryptographic Algorithms

Algorithm	Minimum Key Length	Appropriate Usage	
Symmetric Key Algorithms			
AES	AES 256	Data encryption: • Session • Storage ○ Backup ○ Archival	Key encryption: • Session • Storage ○ Backup ○ Archival
Skipjack	80-bits, with 32 iterations	Data encryption: Disallowed Decryption: Allowed Legacy Systems	
Triple DES	112-bits (Disallowed less than 112-bits)	Data encryption: • Session • Storage ○ Backup ○ Archival	Key encryption: • Session • Storage ○ Backup ○ Archival
		3DES will be disallowed in 2023. AES will be the replacement.	
Scrypt (Non-FIPS Approved)	256-bits	Data encryption: • Session • Storage ○ Backup ○ Archival	
Asymmetric Key Algorithms			
Elliptic Curve	160-bits decrypt only / 224-bits recommended	Data encryption: • Session • Storage ○ Backup ○ Archival Digital Signature	Key encryption: • Session • Storage ○ Backup ○ Archival Session key establishment
RSA	2048-bits	Data encryption: • Session • Storage ○ Backup ○ Archival Digital Signature	Key encryption: • Session • Storage ○ Backup ○ Archival Session key establishment

MACs and Hashes			
AES MAC	128-bits	Message authentication	
MD5 (Non-FIPS Approved)	128-bits, with 16 iterations	Message authentication and message digest. MD5 hashes are no longer considered cryptographically secure and should not be used for cryptographic authentication.	
SHA-1	Not applicable	Message authentication and message digest. SHA-1 no longer useful for cryptographic signing protection although still strong; SHA-2 will be the replacement.	
SHA-2	Not applicable	Message authentication and message digest	
TDES (Triple DES) MAC	112-bits	Message authentication	
Argon2 (Non-FIPS Approved)	128-bits	Message authentication	
Digital Signatures			
DSA (Digital Signature Algorithm)	1024-bits verification only/ L=2048, N=224 recommended	Digital Signature	
Elliptic Curve DSA	160-bits signature verification only / 224-bits recommended	Digital Signature	
RSA DSA	2048-bits	Digital Signature	
Digital Certificates			
X.509 v3 compliant	N/A	Binds a public key with a specific identity.	
Key Transport/Agreement Algorithms			
Diffie-Hellman (Non-FIPS Approved less than 2048-bits)	1024-bits / 2048-bits recommended	Digital Session key establishment	
Elliptic Curve Diffie-Hellman (Non-FIPS Approved less than 224-bits)	160-bits verification only / 224-bits recommended	Digital Session key establishment	
Cryptographic Protocols			
TLS 1.2 and higher	N/A	Protocol to authenticate and encrypt communication between authenticated parties.	