Communications Security Establishment Canada | Centre de la sécurité des télécommunications Canada

CANADIAN CENTRE FOR CYBER SECURITY

Cryptographic algorithms for UNCLASSIFIED, PROTECTED A and PROTECTED B information

Practitioner

TLP:CLEAR

Canada

Foreword

Cryptographic algorithms for UNCLASSIFIED, PROTECTED A and PROTECTED B information is an UNCLASSIFIED publication issued by the Head, Canadian Centre for Cyber Security (Cyber Centre) and provides an update to and supersedes the previously published version.

For more information, contact the Cyber Centre:

- email: contact@cyber.gc.ca
- phone: (613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on May 29, 2026.

Revision history

Revision	Amendments	Date
1	First release	August 2, 2016
2	Version 2	August 17, 2022
3	Version 3	March 19, 2024
4	Version 4	March 5, 2025
5	Version 5	May 29, 2026

D97-3/40-111-2026E-PDF
ISBN: 978-0-660-99820-6

Overview

This publication identifies and describes recommended cryptographic algorithms and appropriate methods of use that organizations can implement to protect sensitive information. For Government of Canada (GC) departments and agencies, the guidance in this publication applies to UNCLASSIFIED, PROTECTED A and PROTECTED B information.

Your organization's ability to protect sensitive data and information is fundamental to the delivery of programs and services. Properly configured cryptography provides security mechanisms which can be used to protect the authenticity, confidentiality and integrity of information. Several algorithms may be required to satisfy your organization's security requirements, and each algorithm should be selected and implemented to meet those requirements.

Table of contents

List of figures

List of annexes

1 Introduction

Organizations rely on information technology (IT) systems to achieve business objectives. These interconnected systems can be the targets of serious threats and cyber attacks that threaten the availability, authenticity, confidentiality and integrity of the information assets. Compromised networks, systems or information can negatively affect business activities and may result in data breaches and financial loss.

This publication helps IT practitioners choose and appropriately use cryptographic algorithms. When used with valid domain parameters and specific key lengths, the cryptographic algorithms listed in this publication are recommended cryptographic mechanisms for protecting the authenticity, confidentiality and integrity of sensitive UNCLASSIFIED, PROTECTED A and PROTECTED B information to the medium injury level, as defined in the Cyber Centre's Cyber security and privacy risk management: A lifecycle approach (ITSP.10.033). For requirements on the use of Cyber Centre-approved cryptography to protect PROTECTED C and classified information, email the Cyber Centre at contact@cyber.gc.ca.

This publication complements the Treasury Board of Canada Secretariat (TBS) Guideline on Defining Authentication Requirements. Organizations are responsible for determining their security objectives and requirements as part of their risk management framework.

1.1 Practitioner notes

In this publication, the Cyber Centre makes recommendations for cryptographic algorithms and parameters. We also list algorithms that should be phased out. New applications should not use these algorithms. Where these algorithms are used in existing applications, they should be replaced with the recommended algorithms in this publication. For certain algorithms, we specify a date by which organizations should replace these algorithms. In other instances, organizations should replace these algorithms as soon as possible.

When an algorithm requires a primitive, organizations should choose 1 of the algorithms recommended in this publication, unless otherwise specified. For example, a hash function from section 7.2 Secure Hash Algorithm-2 should be used when using the Keyed-Hash Message Authentication Code (HMAC) from section 9.1 Keyed-Hash Message Authentication Code. When an algorithm requires a parameter, organizations should select 1 of the recommended parameters in the given reference for the algorithm, unless otherwise specified.

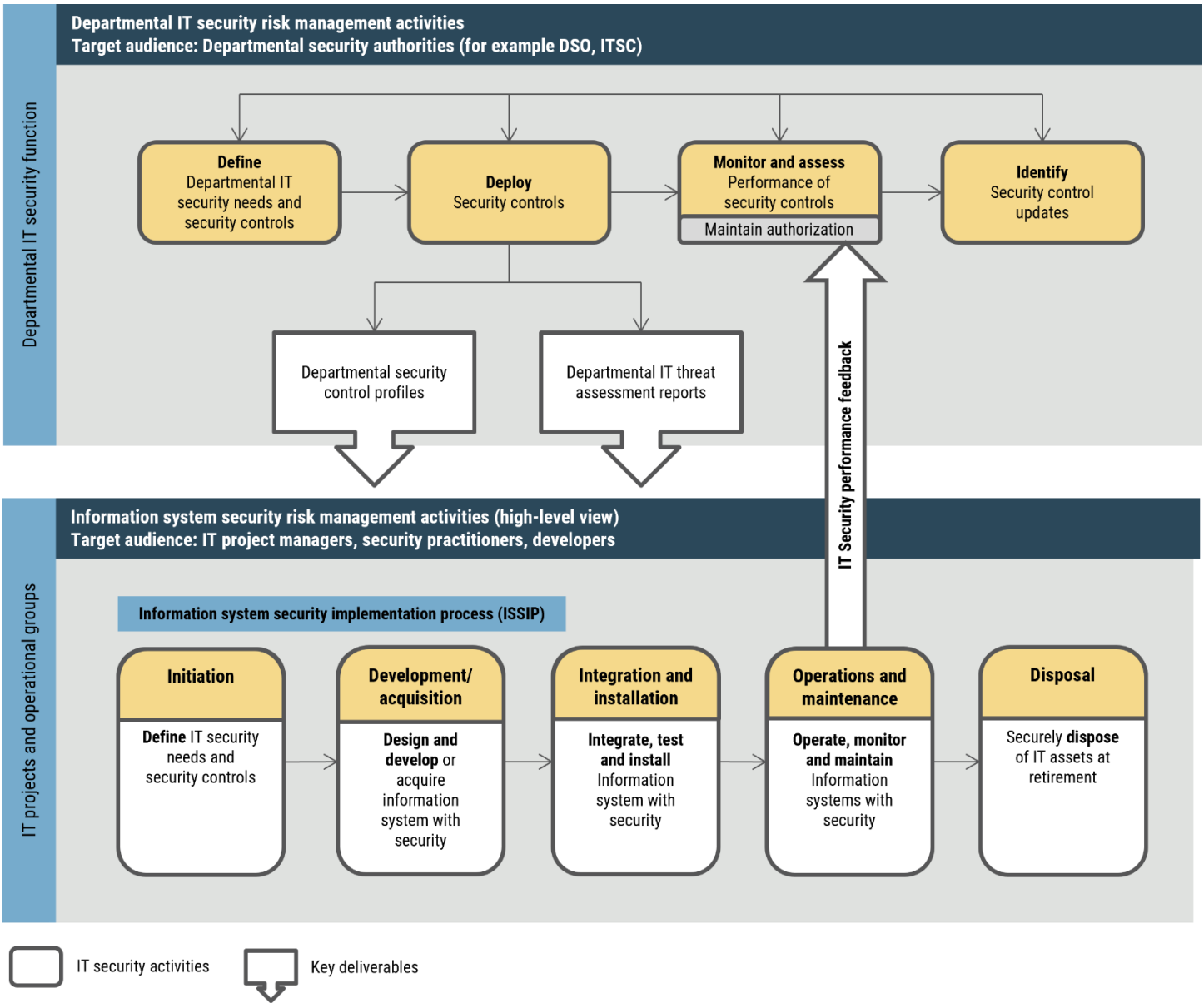
1.2 Policy drivers

Addressing and countering cyber threats and network vulnerabilities are crucial steps in securing networks, data and assets. GC departments must implement IT security policies and procedures in accordance with the TBS Policy on Government Security.

1.3 Relationship to the IT risk management process

The Cyber Centre's Cyber security and privacy risk management: A lifecycle approach (ITSP.10.033) recommend that organizations undertake activities at 2 levels: the departmental level and the information system level.

Figure 1: Cyber security risk management process



Long description – Figure 1: IT security risk management process

This figure describes the high-level departmental IT security risk management process and associated activities, as well as the information system security risk management activities. It also highlights how the IT security risk management activities at both levels act together in a continuous cycle to efficiently maintain and improve the security posture of departmental information systems.

At the departmental level, the IT security risk management activities conducted by the departmental security authorities (for example, CSO, ITSC) include:

- define departmental IT security needs and security controls

- deploy security controls
- monitor and assess performance of security controls - maintain authorization
- identify security control updates

The key deliverables of the deploy security controls activity are departmental control profiles and departmental IT threat assessment reports. These deliverables are key inputs into the security risk management activities at the information system level.

At the information system level, the IT security risk management activities conducted by IT project managers, security practitioners and developers include:

- define IT security needs and security controls
- design and develop or acquire information system with security
- integrate, test, and install information system with security
- operate, monitor, and maintain information systems with security
- securely dispose of IT assets at retirement

Information from the operations and maintenance activities provide feed back into the monitor and assess activity at the departmental level. The IT security performance feedback supports the maintain authorization activity under the monitor and assess.

Departmental-level activities are integrated into the organization's security program to plan, manage, assess and improve the management of IT security-related risks faced by the organization. Cryptographic algorithms should be considered during the define, deploy, and monitor and assess stages of the risk management process. These activities are described in detail in Annex 1 - Departmental IT security risk management activities (ITSG-33).

Information system-level activities are integrated into an information system lifecycle to ensure:

- IT security needs of supported business activities are met
- appropriate security controls are implemented and operating as intended
- continued performance of the implemented security controls is assessed, reported back and acted upon to address any issues

Cryptographic algorithms should be considered during all information system-level activities. These activities are described in detail in Annex 2 - Information system security risk management activities (ITSG-33).

2 Post-quantum cryptography

In August 2024, the U.S. National Institute of Standards and Technology (NIST) published standards for 3 post-quantum algorithms which are secure against known attacks from a quantum computer:

- Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) (see section 5.4 Module-Lattice-Based Key-Encapsulation Mechanism)
- Module-Lattice-Based Digital Signature Algorithm (ML-DSA) (see section 6.5 Module-Lattice-Based Digital Signature Algorithm)
- Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) (see section 6.6 Stateless Hash-Based Digital Signature Algorithm)

ML-KEM establishes shared key material between 2 parties over a public channel. It will replace the key establishment schemes in sections 5.1 Rivest Shamir-Adleman, 5.2 Finite Field Cryptography Diffie-Hellman and Menezes-Qu-Vanstone, and 5.3 Elliptic Curve Cryptography Cofactor Diffie-Hellman and Menezes-Qu-Vanstone for most use cases.

ML-DSA and SLH-DSA are digital signature schemes. ML-DSA is a general-purpose, lattice-based signature scheme and will replace the signature schemes in sections 6.1 Rivest-Shamir-Adelman to 6.4 Edwards-Curve Digital Signature Algorithm for most use cases. Hash-based signatures, including post-quantum stateful hash-based signature schemes and SLH-DSA, rely on a different mathematical problem than ML-DSA. Stateful hash-based signature schemes have the additional complexity that signature generation implementations must carefully manage an internal state. Mismanagement can result in a complete loss of security. SLH-DSA does not require state management but has inferior performance and larger signatures than ML-DSA and the stateful hash-based signature schemes.

International standards bodies are incorporating these new post-quantum algorithms into network protocols. As new protocol standards become available, the Cyber Centre's Guidance on securely configuring network protocols (ITSP.40.062) will be updated to include post-quantum configurations. For more detailed information on how to prepare, read Preparing your organization for the quantum threat to cryptography (ITSAP.00.017).

This version of ITSP.40.111 includes new phase-out dates for quantum-vulnerable key establishment schemes and digital signature schemes.

Organizations should only use post-quantum public-key encryption and signature schemes that comply with the final, published standards (as referenced in this publication) to protect information or systems.

3 Encryption algorithms

The following section outlines the recommended encryption algorithms for protecting the confidentiality of UNCLASSIFIED, PROTECTED A and PROTECTED B information.

3.1 Advanced Encryption Standard algorithm

We recommend the Advanced Encryption Standard (AES) algorithm, as specified in NIST Federal Information Processing Standard (FIPS) 197: Advanced Encryption Standard, with key lengths of 128, 192, and 256 bits.

4 Encryption algorithm modes of operation

The following section outlines the encryption algorithm modes of operation that we recommend for use with the AES algorithm specified in section 3.1 Advanced Encryption Standard Algorithm.

4.1 Protecting the confidentiality of information

We recommend the following block cipher modes of operation for protecting the confidentiality of UNCLASSIFIED, PROTECTED A and PROTECTED B information, as specified in NIST Special Publication (SP) 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques:

- Electronic Codebook (ECB) mode is only suitable for situations in which a single block of data is being encrypted, or as specified in derived algorithms such as key wrapping (see section 11 Key wrap modes of operation). It should not be used for bulk data encryption
- Cipher Feedback (CFB)
- Output Feedback (OFB)
- Counter (CTR)
- Cipher Block Chaining (CBC)
    - When using CBC mode with a plaintext input of bit length greater than or equal to the block size, a padding method must be used as described in Appendix A of NIST SP 800-38A. Protocols typically specify particular padding methods that may be used
    - If no padding method is specified, we recommend the following modes from NIST SP 800-38A Addendum: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode
        - CBC-CS1
        - CBC-CS2
        - CBC-CS3

NIST SP 800-38A lists several important requirements:

- CBC and CFB modes require unpredictable Initialization Vectors (IVs)
- For OFB mode, the IV must be a nonce that is unique to each execution of the encryption operation. It does not need to be unpredictable
- CTR mode requires a unique counter block for each block of plaintext ever encrypted under a given key, across all messages

For protecting data on storage devices, we recommend XTS-AES mode as specified in NIST SP 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices.

4.2 Protecting the confidentiality and authenticity of information

We recommend the following modes of operation for protecting the confidentiality and authenticity of UNCLASSIFIED, PROTECTED A and PROTECTED B information:

- Counter with Cipher Block Chaining-Message Authentication Code (CCM) as specified in NIST SP 800–38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality
- Galois/Counter Mode (GCM) as specified in NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC

5 Key establishment schemes

A key establishment scheme is a procedure by which multiple participants create or obtain shared secrets, such as cryptographic keys. The following section outlines the key establishment schemes that we recommend for use with cryptographic algorithms for protecting UNCLASSIFIED, PROTECTED A and PROTECTED B information.

5.1 Rivest Shamir-Adleman

We recommend the Rivest-Shamir-Adleman (RSA)-based key-transport and key-agreement schemes, as specified in NIST SP 800-56B Rev. 2: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, with an RSA modulus length of at least 2048 bits.

The RSA modulus length should be increased to at least 3072 bits by the end of 2030.

The use of RSA without a post-quantum key establishment scheme should be phased out by the end of 2035.

5.2 Finite Field Cryptography Diffie-Hellman and Menezes-Qu-Vanstone

We recommend the Finite Field Cryptography (FFC) Diffie-Hellman (DH) and FFC Menezes-Qu-Vanstone (MQV)-based key-agreement schemes with valid domain parameters, as specified in NIST SP 800-56A Rev. 3: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. The field size (prime modulus parameter) should be at least 2048 bits.

The FFC field size should be increased to at least 3072 bits by the end of 2030.

The use of FFC DH and FFC MQV without a post-quantum key establishment scheme should be phased out by the end of 2035.

5.3 Elliptic Curve Cryptography Cofactor Diffie-Hellman and Menezes-Qu-Vanstone

We recommend the Elliptic Curve Cryptography (ECC) Cofactor Diffie-Hellman (ECC CDH) and ECC MQV-based key-agreement schemes as specified in NIST SP 800-56A Rev. 3: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography. We recommend the following elliptic curves specified in NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters:

- Curve P-224
- Curve P-256
- Curve P-384
- Curve P-521

Curve P-224 should be phased out by the end of 2030. We no longer recommend binary curves specified in Appendix D of NIST FIPS 186-4: Digital Signature Standard.

All binary curves should be phased out by the end of 2030. A list of the curves to be phased out can be found in section 3.3 of NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters**.**

The use of ECC CDH and ECC MQV without a post-quantum key establishment scheme should be phased out by the end of 2035.

5.4 Module-Lattice-Based Key-Encapsulation Mechanism

We recommend the Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) as a general-purpose, post-quantum key establishment scheme, as specified in NIST FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard, with the following parameters:

- ML-KEM-512
- ML-KEM-768
- ML-KEM-1024

6 Digital signature schemes

The following section outlines the algorithms that we recommend for digital signature applications providing data integrity and data origin authentication of UNCLASSIFIED, PROTECTED A and PROTECTED B information. We also specify a digital signature scheme that was recommended in a previous version of this publication but should be phased out by the end of 2030.

6.1 Rivest-Shamir-Adelman

We recommend the Rivest-Shamir-Adleman (RSA) digital signature algorithm, using RSASSA-PKCS1-v1.5 or RSASSA-PSS, as specified in NIST FIPS 186-5: Digital Signature Standard with an RSA modulus length of at least 2048 bits.

The RSA modulus length should be increased to at least 3072 bits by the end of 2030.

The use of RSA without a post-quantum digital signature scheme should be phased out by the end of 2035.

6.2 Digital Signature Algorithm

The use of Digital Signature Algorithm (DSA) should be phased out by the end of 2030.

We no longer recommend the DSA as specified in NIST FIPS 186-4: Digital Signature Standard for new applications. Existing applications must use valid domain parameters for a field size (prime modulus parameter) of at least 2048 bits.

6.3 Elliptic Curve Digital Signature Algorithm

We recommend the Elliptic Curve Digital Signature Algorithm (ECDSA) and deterministic ECDSA[1] as specified in NIST FIPS 186-5: Digital Signature Standard. We recommend the following elliptic curves specified in NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters:

- Curve P-224
- Curve P-256
- Curve P-384
- Curve P-521

Curve P-224 should be phased out by the end of 2030.

We no longer recommend binary curves specified in Appendix D of NIST FIPS 186-4: Digital Signature Standard.

All binary curves should be phased out by the end of 2030. A list of the curves to be phased out can be found in section 3.3 of NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters.

[1] From NIST SP 800-186, Deterministic ECDSA "is a variant of ECDSA, where a per-message secret number is a function of the message that is signed, thereby resulting in a deterministic mapping of messages to signatures". Signature verification in deterministic ECDSA is unchanged from ECDSA.

The use of ECDSA without a post-quantum digital signature scheme should be phased out by the end of 2035.

6.4 Edwards-Curve Digital Signature Algorithm

We recommend the Edwards-Curve Digital Signature Algorithm (EdDSA) as specified in NIST FIPS 186-5: Digital Signature Standard with the following elliptic curves specified in NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters:

- Edwards25519
- Edwards448

We do not recommend the prehash version HashEdDSA.

The use of EdDSA without a post-quantum digital signature scheme should be phased out by the end of 2035.

6.5 Module-Lattice-Based Digital Signature Algorithm

We recommend the Module-Lattice-Based Digital Signature scheme Algorithm (ML-DSA) as a general-purpose, post-quantum digital signature scheme as specified in NIST FIPS 204: Module-Lattice-Based Digital Signature Standard with the following parameters:

- ML-DSA-44
- ML-DSA-65
- ML-DSA-87

6.6 Stateless Hash-Based Digital Signature Algorithm

We recommend the Stateless Hash-Based Digital Signature Algorithm (SLH-DSA) as a post-quantum digital signature scheme as specified in NIST FIPS 205: Stateless Hash-Based Digital Signature Standard with the following parameters:

- SLH-DSA-SHA2-128s
- SLH-DSA-SHAKE-128s
- SLH-DSA-SHA2-128f
- SLH-DSA-SHAKE-128f
- SLH-DSA-SHA2-192s
- SLH-DSA-SHAKE-192s
- SLH-DSA-SHA2-192f
- SLH-DSA-SHAKE-192f
- SLH-DSA-SHA2-256s
- SLH-DSA-SHAKE-256s
- SLH-DSA-SHA2-256f
- SLH-DSA-SHAKE-256f

6.7 Stateful hash-based signature schemes

Stateful hash-based signature schemes are another family of post-quantum digital signature schemes. Implementations of signature generation for stateful hash-based signature schemes must carefully manage an internal state. This is an additional complexity in comparison to other types of digital signature schemes. Mismanagement of the internal state can result in a complete loss of security. Previously, we recommended stateful hash-based signatures when certain conditions applied, including when a post-quantum signature scheme must be implemented before general-purpose, post-quantum signature schemes were standardized. Although stateful hash-based signature schemes can still be used, the newly standardized post-quantum digital signature schemes ML-DSA and SLH-DSA do not require state management (sections 6.5 Module-Lattice-Based Digital Signature Algorithm and 6.6 Stateless Hash-Based Digital Signature Algorithm) and can be used in most situations where a digital signature scheme is needed. Stateful hash-based signatures should only be used when the signer is not required to rapidly produce signatures and is able to protect and manage private key state.

If you are using stateful hash-based signatures, we recommend the following post-quantum digital signature schemes, as specified in NIST SP 800-208: Recommendation for Stateful Hash-based Signatures Scheme, using one of the hash functions SHA-256, SHA-256/192, SHAKE256/256, or SHAKE256/192 specified in section 2.3 of NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes.

- Leighton-Micali Signature (LMS)
- Hierarchical Signature System (HSS)
- eXtended Merkle Signature Scheme (XMSS)
- Multi-tree eXtended Merkle Signature Scheme (XMSS^{MT})

7 Hash functions

A hash function is a procedure to transform a message of arbitrary length into an output, called a "digest", of fixed length. A secure (cryptographic) hash function should satisfy additional properties, such as "collision resistance", whereby it is infeasible to find distinct messages with the same digest. The following section outlines the recommended hash functions for use with the cryptographic algorithms specified in this publication for protecting UNCLASSIFIED, PROTECTED A and PROTECTED B information.

7.1 Secure Hash Algorithm-1

We no longer recommend the use of Secure Hash Algorithm-1 (SHA-1), as specified in NIST FIPS 180-4: Secure Hash Standard, which was previously approved for use with keyed-hash message authentication codes, key derivation functions (KDFs) and random bit generators (RBGs).

SHA-1 must not be used with digital signature schemes or with any applications that require collision resistance. SHA-1 should be phased out for use in keyed-hash message authentication codes, KDFs, and RBGs.

7.2 Secure Hash Algorithm-2

We recommend SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224, and SHA-512/256, as specified in NIST FIPS 180-4: Secure Hash Standard, for use with digital signature schemes, keyed-hash message authentication codes, KDFs and RBGs. The truncated hash function SHA-256/192 specified in NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes is only recommended for use with the stateful hash-based signature schemes listed in section 6.7 Stateful hash-based signature schemes.

SHA-224 should be phased out by the end of 2030.

7.3 Secure Hash Algorithm-3

We recommend SHA3-224, SHA3-256, SHA3-384, and SHA3-512, as specified in NIST FIPS 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, for use with digital signature schemes, keyed-hash message authentication codes, KDFs and RBGs.

SHA3-224 should be phased out by the end of 2030.

8 Extendable output functions

An extendable-output function (XOF) is a procedure to transform a message of arbitrary length into an output that can be extended to any desired length. A secure XOF should satisfy additional properties, such as “collision resistance”, whereby it is infeasible to find distinct messages with the same output. The following section outlines 2 XOFs that we recommend for use with select cryptographic algorithms specified in this publication for protecting UNCLASSIFIED, PROTECTED A and PROTECTED B information.

8.1 SHAKE

We recommend SHAKE128, as specified in NIST FIPS 202: SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions, for use in the following:

- ML-KEM (section 5.4 Module-Lattice-Based Key-Encapsulation Mechanism)
- The digital signature schemes
  - RSA (section 6.1 Rivest-Shamir-Adelman)
  - ECDSA (section 6.3 Elliptic Curve Digital Signature Algorithm)
  - ML-DSA (section 6.5 Module-Lattice-Based Digital Signature Algorithm)
- KECCAK Message Authentication Code (KMAC) (section 9.4 KECCAK Message Authentication Code)

We recommend SHAKE256, as specified in NIST FIPS 202: SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions, for use in the following:

- ML-KEM (section 5.4 Module-Lattice-Based Key-Encapsulation Mechanism)
- The digital signature schemes
  - RSA (section 6.1 Rivest-Shamir-Adelman)
  - ECDSA (section 6.3 Elliptic Curve Digital Signature Algorithm)
  - EdDSA (section 6.4 Edwards Curve Digital Signature Algorithm) with curve Edwards448
  - ML-DSA (section 6.5 Module-Lattice-Based Digital Signature Algorithm)
  - SLH-DSA (section 6.6 Stateless Hash-Based Digital Signature Algorithm)
  - Stateful hash-based digital signature schemes (section 6.7 Stateful hash-based signature schemes)
- KMAC (section 9.4 KECCAK Message Authentication Code)

9 Message authentication codes

A message authentication code (MAC) is a fixed-length tag used to verify the authenticity and integrity of a message. The following sections outline the MAC algorithms that we recommend for data integrity and data origin authentication of UNCLASSIFIED, PROTECTED A and PROTECTED B information.

9.1 Keyed-Hash Message Authentication Code

We recommend Keyed-Hash Message Authentication Code (HMAC), as specified in NIST FIPS 198-1: The Keyed-Hash Message Authentication Code, with a key length of at least 112 bits.

The key length should be increased to at least 128 bits by the end of 2030.

9.2 Cipher-based Message Authentication Code

We recommend Cipher-based Message Authentication Code (CMAC), as specified in NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. CMAC is only recommended for use with the AES algorithm as specified in section 3.1 Advanced Encryption Standard algorithm.

9.3 Galois/Counter Mode Message Authentication Code

We recommend Galois/Counter Mode Message Authentication Code (GMAC), as specified in NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. GMAC is only recommended for use with the AES algorithm as specified in section 3.1 Advanced Encryption Standard algorithm.

9.4 KECCAK Message Authentication Code

We recommend KECCAK message authentication code (KMAC)128 and KMAC256 as specified in NIST SP 800-185: SHA3-Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash with a key length of at least 112 bits.

The key length should be increased to at least 128 bits by the end of 2030.

10 Key derivation functions

A KDF is a transformation of secret (as well as possibly non-secret) data into a cryptographically strong secret key. The following sections outline the KDFs that we recommend for the derivation of cryptographic keys from key establishment or pre-shared secrets, used for protecting UNCLASSIFIED, PROTECTED A and PROTECTED B information.

10.1 One-Step Key Derivation Function

We recommend the one-step KDF, as specified in NIST SP 800-56C Rev. 2: Recommendation for Key-Derivation Methods in Key Establishment Schemes.

10.2 Two-Step Key Derivation Function

We recommend the two-step, extraction-then-expansion, key derivation procedure, as specified in NIST SP 800-56C Rev. 2: Recommendation for Key-Derivation Methods in Key Establishment Schemes. Note that the HMAC-based extract-and-expand Key Derivation Function (HKDF) function used in the Transport Layer Security (TLS) version 1.3 protocol follows this specification.

10.3 Key derivation using pseudorandom functions

We recommend the KDFs using pseudorandom functions as specified in NIST SP 800-108 Rev. 1: Recommendation for Key Derivation Using Pseudorandom Functions.

10.4 Internet Key Exchange version 2 Key Derivation Function

When used in the context of the Internet Key Exchange version 2 (IKEv2) protocol, we recommend the IKEv2 KDF, as specified in NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions.

10.5 Transport Layer Security version 1.2 Key Derivation Function

When used in the context of the TLS version 1.2 protocol, we recommend the TLS 1.2 KDF, as specified in NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions.

10.6 Secure Shell Key Derivation Function

When used in the context of the Secure Shell (SSH) protocol, we recommend the SSH KDF, as specified in NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions.

10.7 Secure Real-time Transport Protocol Key Derivation Function

When used in the context of the Secure Real-time Transport Protocol (SRTP), we recommend the SRTP KDF, as specified in NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions.

10.8 Trusted Platform Module Key Derivation Function

When used in the context of a Trusted Platform Module (TPM) session, we recommend the TPM KDF, as specified in NIST SP 800-135 Rev. 1: Recommendation for Existing Application-Specific Key Derivation Functions.

10.9 Password-based Key Derivation Function

For protected data on storage devices, we recommend the Password-based KDF, as specified in NIST SP 800-132: Recommendation for Password-Based Key Derivation: Part 1: Storage Applications, using a password of at least 12 characters. For more information on passwords and passphrases, read the Cyber Centre's Best practices for passphrases and passwords (ITSAP.30.032).

11 Key wrap modes of operation

The following sections outline the key wrap modes of operation that we recommend for key wrapping to protect the confidentiality and integrity of cryptographic keys used for protecting UNCLASSIFIED, PROTECTED A and PROTECTED B information.

11.1 Advanced Encryption Standard Key Wrap

When input is known to always be a multiple of 64 bits, we recommend the AES Key Wrap mode, as specified in NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.

11.2 Advanced Encryption Standard Key Wrap with Padding

When input is not a multiple of 64-bits, we recommend the AES Key Wrap with Padding mode, as specified in NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping.

12 Random bit generators

An RBG produces a sequence of bits (0 or 1) which appear statistically independent and unbiased. We recommend RBGs as specified in NIST SP 800-90C: Recommendation for Random Bit Generator (RBG) Constructions. These constructions employ an entropy source and a Deterministic Random Bit Generator (DRBG).

A DRBG always produces the same output sequence when given the same initial seed. We recommend the following DRBGs, as specified in NIST SP 800-90A Rev. 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators, for producing random bits for cryptographic applications that protect UNCLASSIFIED, PROTECTED A and PROTECTED B information:

- Hash_DRBG
- HMAC_DRBG
- CTR_DRBG

The entropy source for RBG constructions and the initial seed for a DRBG should comply with NIST SP 800-90B Recommendations for Entropy Sources Used for Random Bit Generation and should be assessed to be at least 112 bits.

The assessed entropy of the initial seed for a DRBG should be increased to at least 128 bits by the end of 2030.

13 Commercial technologies assurance programs

In addition to using the cryptographic algorithms, parameters and key lengths recommended in this publication, we recommend the following to ensure a suitable level of cryptographic security:

- Cryptographic algorithm implementations should be tested and validated under the NIST Cryptographic Algorithm Validation Program (CAVP)
- Cryptographic modules should be tested and validated under the Cryptographic Module Validation Program (CMVP) for compliance with NIST FIPS 140-3: Security Requirements for Cryptographic Modules
- IT security products should be certified to the Common Criteria Standard by a Certificate Authorizing Member of the Common Criteria Recognition Arrangement

Products containing cryptographic modules validated under the CMVP are referenced on NIST CMVP-validated modules lists and are accompanied by a vendor-supplied, non-proprietary security policy document (read Selecting a CMVP validated product). The security policy document specifies the cryptographic security provided by a module and describes its capabilities, protection and access controls. We recommend using the security policy document to select suitable cryptographic security products and to configure those products in FIPS-approved modes of operation, as defined in Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, to ensure that only the algorithms recommended by the Cyber Centre are used.

14 Summary

Cryptography provides security mechanisms which can be used to protect the authenticity, confidentiality and integrity of sensitive information. Several algorithms may be required to satisfy security requirements, and each algorithm should be selected and implemented to ensure these requirements are met. This publication provides guidance on the use of the cryptographic algorithms recommended by the Cyber Centre to protect UNCLASSIFIED, PROTECTED A and PROTECTED B information.

A.1 Revisions

The original version of this document was published in August 2016. The summary below lists notable changes in the most recent revision (version 5), as well as in previous versions.

A.1.1 Version 5

- We updated section 2 to say that this document now includes phase-out dates for quantum-vulnerable key establishment schemes and digital signature schemes
- We added phase-out dates for the use of all quantum-vulnerable key establishment schemes and digital signature schemes. The phase-out dates can be found in each affected subsection:
  - For key establishment schemes:
    - Section 5.1 Rivest-Shamir-Adelman
    - Section 5.2 Finite Field Cryptography Diffie-Hellman and Menezes-Qu-Vanstone
    - Section 5.3 Elliptic curve cryptography Cofactor Diffie-Hellman and Menezes-Qu-Vanstone
  - For digital signature schemes:
    - Section 6.1 Rivest-Shamir-Adelman
    - Section 6.3 Elliptic Curve Digital Signature Algorithm (ECDSA)
    - Section 6.4 Edwards Curve Digital Signature Algorithm (EdDSA)
- In section 5.2, we removed the specific parameter-size set recommendations to align with field size phase-out requirements
- We renamed section 12 from “Deterministic Random Bit Generators” to “Random Bit Generators” and added new guidance on the use of RBGs and entropy sources for RBGs
- We modified the third bullet point in section 13 for clarity

A.1.2 Version 4 (March 2025)

- We included the new NIST post-quantum standards:
  - NIST FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism (Section 5.4)
  - NIST FIPS 204 Module-Lattice-Based Digital Signature Standard (Section 6.5)
  - NIST FIPS 205 Stateless Hash-Based Digital Signature Standard (Section 6.6)
- We updated the section on post-quantum cryptography and moved it to Section 2
- In Section 3: Encryption algorithms, we removed the subsections on TDEA and CAST5, as all use of TDEA and CAST5 should have been phased out by the end of 2023
- In Section 6.7: Stateful Hash-Based Signature Schemes, we clarified guidance for use of stateful hash-based signatures with respect to other post-quantum signature schemes

- In Section 8.7: Hash functions, extendable output functions, we added ML-KEM, ML-DSA, and SLH-DSA to the list of algorithms that can use SHAKE. We also added the distinction that SLH-DSA and EdDSA only allow for SHAKE256, (and for EdDSA it is only with curve Ed448)
- In Section 9.2: Cipher-based message authentication code, we removed the statement requiring a key length increase to at least 128 bits by 2023. Instead, we recommended that CMAC only be used with AES, as TDEA and CAST5 have been removed
- In Section 11: Key wrap modes of operation, we removed the subsection on TDEA Key Wrap, as all use of TDEA should have been phased out by the end of 2023
- We removed the supporting content section. References are linked throughout the document, glossary items are either defined in the text or in the Cyber Centre glossary, and abbreviations are spelled out when they first appear in the document

A.1.3 Version 3 (March 2024)

- We made various changes to align with FIPS 186-5:
  - In Section 4.3: ECC DH and MQV and Section 5.3: ECDSA, we only recommend the use of 4 elliptic curves (Curve P-224, Curve P-256, Curve P-384 and Curve P-521). We added a note that Curve P-224 and all binary curves should be phased out by the end of 2030. In Section 5.3, we explicitly recommend deterministic ECDSA
  - In Section 5: Digital signature schemes, we recommend phasing out DSA by the end of 2030, and added the new subsection 5.4 Edwards-Curve Digital Signature Algorithm
- We added a new section on XOFs (Section 7)
- In Section 8: Message authentication codes, we added the new subsection on KMAC (Section 8.4)
- In Section 11: Deterministic random bit generators, we added the following requirements on the assessed entropy of the initial seed for a DRBG
  - The initial seed for a DRBG should contain entropy assessed to be at least 112 bits. We recommend that additional entropy be periodically added to the DRBG via the reseed function
  - The assessed entropy of the initial seed for a DRBG should be increased to at least 128 bits by the end of 2030

A.1.4 Version 2 (August 2022)

- We updated language from “approved/discontinued” to “recommend/phase out”
- We replaced references to CSE with the Cyber Centre
- In Section 2: Encryption algorithms, we recommend phasing out CAST5 and TDEA by 2023. The 2016 version did not have a discontinuation date for CAST5, and version 2 recommended discontinuing TDEA by 2030. We also added a restriction that 1 key bundle should not be used to encrypt more than 2^{20} 64-bit data blocks in TDEA
- In Section 3: Encryption algorithm modes of operation, we provided some additional guidance on the use of ECB mode, as well as recommendations for IV generation
- In Section 5: Digital signature schemes, we added a new subsection on Stateful Hash-based signature schemes

- In Section 6: Secure hash algorithms, we no longer recommend the use of SHA-1, which was previously approved for use with HMACs, KDFs and RBGs. We added stronger wording (in bold) warning against its use for any application that requires collision resistance. We also added phase-out dates for SHA-224 and SHA3-224
- In Section 7: Message authentication codes, we updated the recommendation for the CMAC key length to be increased to at least 128 bits by the end of 2023 (we previously recommended 2030). We also added the statement “GMAC is only recommended for use with the Advanced Encryption Standard (AES) algorithm as specified in Section 2.1”, which was not explicitly stated in the previous version
- In Section 8: Key derivation functions, we updated some of the wording. For example, Single-Step KDFs and Extraction-Then-Expansion KDFs are now referred to as One-Step and Two-Step KDFs respectively (this is consistent with the referenced NIST standards). We removed the IKEv1 KDF and added a section for password-based KDFs
- In Section 9: Key wrap modes of operation, we no longer recommend the Triple Data Encryption Algorithm Key Wrap (TKW). We also recommend a phase-out date of 2023 (previously 2030)
- In Section 11: Commercial technologies assurance programs, we added a reference to the CAVP and to the common criteria program. We also added the Cyber Centre website as a reference
- We added a new section entitled “Preparing for post-quantum cryptography” (Section 12)