Communications Security Establishment
Centre de la sécurité des télécommunications

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, email, or phone:

Contact Centre

contact@cyber.gc.ca

(613) 949-7048 or 1-833-CYBER-88

Effective date

This publication takes effect on March 18, 2024.

Revision history

Revision	Amendments	Date
1	First release	August 2, 2016
2	Updated version (version 2)	August 17, 2022
3	Updated version (version 3)	March 18, 2024

Overview

This document 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 document 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. Cryptography provides security mechanisms which can be used to protect the authenticity, confidentiality, and integrity of information.

Data authenticity, confidentiality, integrity, stakeholder authentication and accountability, and non-repudiation are all benefits of properly configured cryptography. Several algorithms may be required to satisfy these security requirements, and each algorithm should be selected and implemented to ensure these requirements are met.

D97-3/40-111-2024E-PDF
978-0-660-69874-8

Table of contents

List of figures

1 Introduction

Organizations rely on Information Technology (IT) systems to achieve business objectives. These interconnected systems can be the targets of serious threats and cyberattacks that jeopardize the availability, authenticity, confidentiality, and integrity of the information assets. Compromised networks, systems, or information can have adverse effects on business activities and may result in data breaches and financial loss.

This document aids technology practitioners in choosing and appropriately using cryptographic algorithms. When used with valid domain parameters and specific key lengths, the cryptographic algorithms listed in this document 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 IT Security Risk Management: A Lifecycle Approach (ITSG-33) [1][A]. For requirements on the use of Cyber Centre approved cryptography to protect PROTECTED C and Classified information, contact the Cyber Centre by email at contact@cyber.gc.ca.

This document complements the Treasury Board of Canada Secretariat (TBS) Guideline on Defining Authentication Requirements [2]. Organizations are responsible for determining their security objectives and requirements as part of their risk management framework.

1.1 Practitioner notes

In this document we make recommendations for cryptographic algorithms and parameters. We also list algorithms that should be "phased out" of use. New applications should not use these algorithms. Where these algorithms are used in existing applications, they should be replaced with algorithms that we recommend in this document. For certain algorithms we specify a date by which these algorithms should have been replaced. In other instances, these algorithms should be replaced as soon as possible.

Unless otherwise specified, when an algorithm requires a primitive, it should be chosen from those recommended in this document. For example, a hash function from Sections 6.2 or 6.3 should be used when using the Keyed-Hash Message Authentication Code (HMAC) from Section 8.1. Unless otherwise specified, when an algorithm requires a parameter, it should be chosen from those recommended in the given reference for the algorithm.

1.2 Policy drivers

The need to address and counter cyber threats and vulnerabilities currently threatening networks is a crucial step in securing networks, data, and assets. GC departments must ensure IT security policies and procedures are implemented in accordance with the TBS Policy on Government Security [3].

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

1.3 Relationship to the IT risk management process

The Cyber Centre's IT Security Risk Management: A Lifecycle Approach (ITSG-33) [1] guidelines suggest a set of activities at two levels within an organization: the departmental level and the information system level.

Figure 1 IT security risk management process

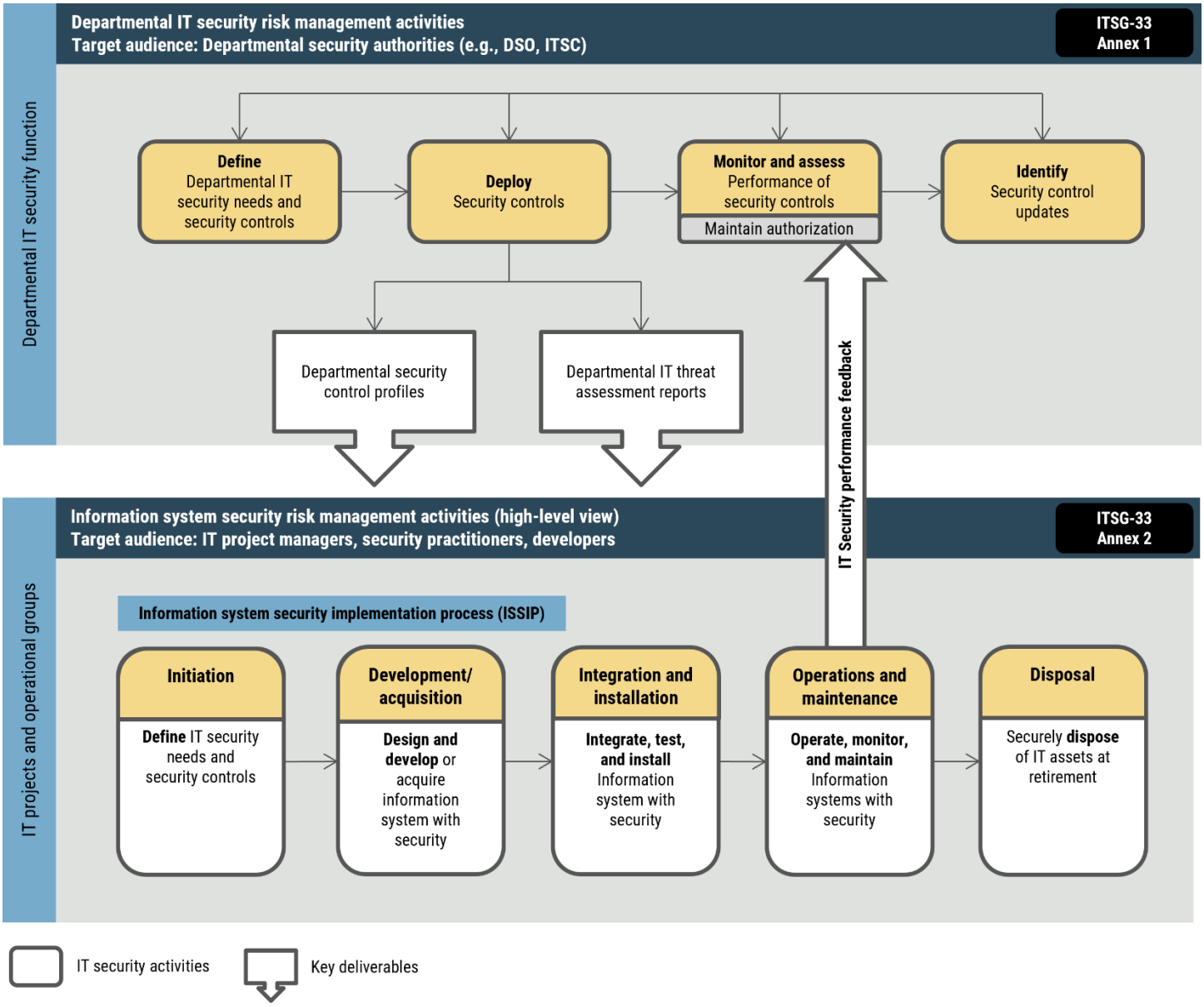

Figure Caption: This figure describes the high-level departmental IT security risk management process and associated activities, as well as the information system security risk management activities. It also highlights how the IT security risk management activities at both levels act together in a continuous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

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 activities. These activities are described in detail in Annex 1 - Departmental IT security risk management activities (ITSG-33) [1].

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) [1].

2 Encryption algorithms

The following section outlines the encryption algorithms that we recommend for protecting the confidentiality of UNCLASSIFIED, PROTECTED A, and PROTECTED B information. We also specify encryption algorithms that were recommended in a previous version of this document but should have been phased out by the end of 2023.

2.1 Advanced Encryption Standard algorithm

We recommend the Advanced Encryption Standard (AES) algorithm as specified in National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Information Processing Standards Publication 197: Advanced Encryption Standard [4] with key lengths of 128, 192, and 256 bits.

2.2 Triple Data Encryption Algorithm

The use of 3-key Triple Data Encryption Algorithm (TDEA) should have been phased out by the end of 2023.

We no longer recommend the use of the TDEA specified in NIST SP 800-67 Revision 2: Recommendation for the Triple Data Encryption Algorithm Block Cipher [5]. Legacy applications still using the 3-key option of TDEA should note the important restriction that one key bundle should not be used to encrypt more than 2^{20} 64-bit data blocks [5].

2.3 CAST5

The use of CAST5 should have been phased out by the end of 2023.

We no longer recommend the CAST5 algorithm specified in Request for Comments (RFC) 2144: The CAST-128 Encryption Algorithm [6].

3 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 2.1.

3.1 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 SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques [7]:

- Electronic Codebook (ECB) – ECB mode is only suitable for situations where a single block of data is being encrypted or as specified in derived algorithms such as key wrapping (see Section 10). 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 SP800-38A [7]. Protocols typically specify particular padding methods that may be used. If no padding method is specified, we recommend the following modes from NIST Addendum to SP 800-38A: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode [8]:
    - CBC-CS1
    - CBC-CS2
    - CBC-CS3

Note several important requirements from SP800-38A [7]:

- the 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.
- the 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 [9].

3.2 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 [10]
- Galois/Counter Mode (GCM) as specified in NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode [11]

4 Key establishment schemes

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.

4.1 Rivest-Shamir-Adleman

We recommend the Rivest-Shamir-Adleman (RSA)-based key-transport and key-agreement schemes as specified in NIST SP 800-56B Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography [12] 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.

4.2 Finite Field Cryptography Diffie-Hellman and Menezes-Qu-Vanstone (MQV)

We recommend the Finite Field Cryptography (FFC) Diffie-Hellman (DH) and FFC Menezes-Qu-Vanstone (MQV)-based key-agreement schemes with valid domain parameters for the FB or FC FFC parameter-size sets as specified in NIST SP 800-56A Revision 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography [13]. 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.

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

We recommend the Elliptic Curve Cryptography (ECC) Cofactor Diffie-Hellman (ECC CDH) and ECC Menezes-Qu-Vanstone (ECC MQV)-based key-agreement schemes as specified in the NIST SP 800-56A Revision 3: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography [13]. We recommend the following elliptic curves specified in the NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14]:

- 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 [15].

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 the NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14].

5 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 document but should be phased out by the end of 2030.

5.1 Rivest-Shamir-Adleman

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 [16] 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.

5.2 Digital Signature Algorithm

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

We no longer recommend the Digital Signature Algorithm (DSA) as specified in NIST FIPS 186-4: Digital Signature Standard [15] with valid domain parameters for a field size of at least 2048 bits.

5.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

We recommend the Elliptic Curve Digital Signature Algorithm (ECDSA) and deterministic ECDSA[B] as specified in NIST FIPS 186-5: Digital Signature Standard [16]. We recommend the following elliptic curves specified in NIST SP 800-186: Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14]:

- 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 [15].

[B] From [16], 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.

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 [14]**.**

5.4 Edwards-Curve Digital Signature Algorithm (EdDSA)

We recommend the Edwards-Curve Digital Signature Algorithm (EdDSA) as specified in NIST FIPS 186-5: Digital Signature Standard [16] with the following elliptic curves specified in NIST SP 800-186 Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters [14]:

- Edwards25519
- Edwards448

We do not recommend the prehash version HashEdDSA.

5.5 Stateful hash-based signature schemes

We recommend stateful hash-based signatures be used only in situations where all of the following apply:

1. when a post quantum signature scheme must be implemented in the near future, before other general-purpose post quantum signature schemes are standardized (see Section 13);
2. when the implementation will have a long lifetime and it will not be practical to transition to a new digital signature scheme once the implementation has been deployed;
3. when the slow key generation and signing computations are operationally acceptable; and,
4. when state management can be implemented.

In these situations, we recommend the following hash-based signature schemes as specified in NIST SP 800-208: Recommendation for Stateful Hash-based Signatures Scheme [17], using one of the hash functions SHA-256, SHA-256/192, SHAKE256/256, SHAKE256/192 specified in Section 2.3 of [17]:

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

6 Hash functions

The following section outlines the hash functions that we recommend for use with the cryptographic algorithms specified in this publication for protecting UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

6.1 SHA-1

We no longer recommend the use of SHA-1 as specified in NIST FIPS 180-4: Secure Hash Standard [18], which was previously approved for use with keyed-hash message authentication codes, key derivation functions, and random bit generators.

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

6.2 SHA-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 [18] for use with digital signature schemes, keyed-hash message authentication codes, key derivation functions, and random bit generators. The truncated hash function SHA-256/192 specified in [17] is only recommended for use with the stateful hash-based signature schemes listed in Section 5.5.

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

6.3 SHA-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 [19] for use with digital signature schemes, keyed-hash message authentication codes, key derivation functions, and random bit generators.

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

7 Extendable-Output Functions (XOF)

The following section outlines the Extendable-Output Functions (XOFs) that we recommend for use with select cryptographic algorithms specified in this publication for protecting UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

7.1 SHAKE

We recommend SHAKE128 and SHAKE256 as specified in NIST FIPS 202: SHA-3 Standard: Permutation Based Hash and Extendable-Output Functions [19] for use in the following:

- The digital signature schemes RSA (Section 5.1), ECDSA (Section 5.3) and EdDSA (Section 5.4)
- Stateful hash-based digital signature schemes in Section 5.5
- KMAC in Section 8.4

8 Message Authentication Codes (MAC)

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.

8.1 Keyed-Hash Message Authentication Code (HMAC)

We recommend Keyed-Hash Message Authentication Code (HMAC) as specified in NIST FIPS 198-1: The Keyed-Hash Message Authentication Code [20] 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.

8.2 Cipher-based Message Authentication Code (CMAC)

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 [21] with a key length of at least 112 bits.

The key length should have been increased to at least 128 bits by the end of 2023.

8.3 Galois/Counter Mode Message Authentication Code (GMAC)

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 [11]. GMAC is only recommended for use with the AES algorithm as specified in Section 2.1.

8.4 KECCAK Message Authentication Code (KMAC)

We recommend KMAC128 and KMAC256 as specified in NIST SP 800-185: SHA3-Derived Functions: cSHAKE, KMAC, TupleHash and ParallelHash [22] 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 Key Derivation Functions (KDF)

The following sections outline the KDF 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.

9.1 One-Step KDF

We recommend the One-Step Key Derivation Function (KDF) as specified in NIST SP 800-56C Revision 2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes [23].

9.2 Two-Step KDF

We recommend the Two-Step Extraction-then-Expansion Key Derivation procedure as specified in NIST SP 800-56C Revision 2: Recommendation for Key-Derivation Methods in Key-Establishment Schemes [23]. Note that the HKDF function used in the Transport Layer Security version 1.3 (TLS 1.3) protocol follows this specification.

9.3 Key derivation using pseudorandom functions

We recommend the KDFs using Pseudorandom Functions (PRFs) as specified in NIST SP 800-108 Revision 1: Recommendation for Key Derivation Using Pseudorandom Functions [24].

9.4 Internet Key Exchange version 2 (IKEv2) KDF

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 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.5 Transport Layer Security version 1.2 (TLS 1.2) KDF

When used in the context of the Transport Layer Security version 1.2 (TLS 1.2) protocol, we recommend the TLS 1.2 KDF as specified in NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.6 Secure Shell (SSH) KDF

When used in the context of the Secure Shell (SSH) protocol, we recommend the SSH KDF as specified in NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.7 Secure Real-time Transport Protocol (SRTP) KDF

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 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.8 Trusted Platform Module (TPM) KDF

When used in the context of a Trusted Platform Module (TPM) session, we recommend the TPM KDF as specified in NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions [25].

9.9 Password-Based Key Derivation Function (PBKDF)

For protected data on storage devices, we recommend the Password-Based Key Derivation Function (PBKDF) as specified in NIST SP 800-132 Recommendation for Password-Based Key Derivation: Part 1: Storage Applications [26] using a password of at least 12 characters. For more information on passwords and passphrases, see Best Practices for Passphrases and Passwords (ITSAP.30.032) [27].

10 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. We also specify a key wrap mode of operation that was recommended in a previous version of this document but should have been phased out by the end of 2023.

10.1 AES Key Wrap (KW)

When input is known to always be a multiple of 64-bits, we recommend the AES Key Wrap (KW) mode as specified in NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping [28].

10.2 AES Key Wrap with Padding (KWP)

When input is not a multiple of 64-bits, we recommend the AES Key Wrap with Padding (KWP) mode as specified in NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping [28].

10.3 Triple Data Encryption Algorithm Key Wrap (TKW)

The use of TKW should have been phased out by the end of 2023.

We no longer recommend the Triple Data Encryption Algorithm Key Wrap (TKW) mode as specified in NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping [28], which was previously approved with a key length of 168 bits.

11 Deterministic Random Bit Generators (DRBGs)

We recommend the following Deterministic Random Bit Generators (DRBGs) as specified in NIST SP 800-90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators [29] for producing random bits for cryptographic applications that protect UNCLASSIFIED, PROTECTED A, and PROTECTED B information:

- Hash_DRBG
- HMAC_DRBG
- CTR_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.

12 Commercial technologies assurance programs

In addition to using the cryptographic algorithms, parameters, and key lengths recommended in this document to ensure a suitable level of cryptographic security, we recommend the following with respect to implementation assurance programs:

1. Cryptographic algorithm implementations should be tested and validated under the Cryptographic Algorithm Validation Program (CAVP) [30].
2. Cryptographic modules should be tested and validated under the Cryptographic Module Validation Program (CMVP) [31] for compliance to FIPS 140-3: Security Requirements for Cryptographic Modules [32].
3. Information technology security products should be evaluated and certified to meet the Common Criteria standard [33] by a Certificate Authorizing Scheme that is a member of the international Common Criteria Recognition Arrangement.

Products containing cryptographic modules validated under the CMVP are referenced on CMVP module validation lists and are accompanied by a vendor-supplied, non-proprietary security policy document (see 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 Mode of Operation as defined in Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program [34] to ensure that only the Cyber Centre recommended algorithms are used.

13 Preparing for post quantum cryptography

Quantum computers threaten to break the public key cryptosystems and weaken the symmetric cryptosystems that we currently use. Although quantum technologies are not yet powerful enough to break the cryptography recommended in this publication, there is significant research in the area. In 2016, NIST initiated a process to solicit, evaluate, and standardize post quantum public-key cryptographic algorithms. In July 2022, NIST announced the initial selections for standardization [35], and we expect to include these in an update to this document once the standards are published.

NIST is expecting to finalize the first set of standards in 2024. In the meantime, we recommend the following high-level steps:

- Evaluate the sensitivity of your organization's information and determine its lifespan to identify information that may be at risk (e.g., as part of on-going risk assessment processes)
- Review your IT lifecycle management plan and budget for potentially significant software and hardware updates
- Educate your workforce on the quantum threat
- Consider using Stateful Hash-based Signature schemes if you meet the criteria in Section 5.5

For more detailed information on how to prepare, see Preparing Your Organization for The Quantum Threat to Cryptography (ITSAP.00.017) [36].

Organizations should wait until standards for post-quantum public-key encryption and signature schemes are finalized before using any candidate algorithm to protect information or systems.

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 Cyber Centre recommended cryptographic algorithms to protect UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

15 Supporting content

15.1 List of abbreviations

Term	Definition
AES	Advanced Encryption Standard
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CDH	Cofactor Diffie-Hellman
CCM	Cipher Block Chaining Message Authentication Code
CFB	Cipher Feedback
CMAC	Cipher-based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CS	Ciphertext Stealing
CSE	Communications Security Establishment
CTR	Counter
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FFC	Finite Field Cryptography
FIPS	Federal Information Processing Standards
GC	Government of Canada
GCM	Galois/Counter Mode
GMAC	Galois/Counter Mode Message Authentication Code
HMAC	Keyed-Hash Message Authentication Code
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IT	Information Technology
ITS	Information Technology Security
ITSG	Information Technology Security Guidance
ITSP	Information Technology Security Guidance for Practitioners

Term	Definition
KDF	Key Derivation Function
KMAC	KECCAK Message Authentication Code
KW	Key Wrap
KWP	Key Wrap with Padding
MAC	Message Authentication Code
MQV	Menezes-Qu-Vanstone
NIST	National Institute of Standards and Technology
OFB	Output Feedback
PRF	Pseudorandom Function
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SP	Special Publication
SRTP	Secure Real-time Transport Protocol
SSH	Secure Shell
TBS	Treasury Board of Canada Secretariat
TDEA	Triple Data Encryption Algorithm
TKW	Triple Data Encryption Algorithm Key Wrap
TLS	Transport Layer Security
TPM	Trusted Platform Module
TRA	Threat and Risk Assessment
XOF	eXtendable Output Function

15.2 Glossary

Term	Definition
Authentication	A measure designed to provide protection against fraudulent transmissions or imitations by establishing the validity of a transmission, message, or originator.
Authenticity	The state of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator.
Availability	The state of being accessible and usable in a timely and reliable manner.
Classified Information	Information related to the national interest that may qualify for an exception or exclusion under the Access to Information Act or Privacy Act and the compromise of which could reasonably be expected to cause injury to the national interest.
Confidentiality	The state of being disclosed only to authorized principals.

Term	Definition
Cryptographic Algorithm Validation Program (CAVP)	A program that is used to validate the functional correctness of the cryptographic algorithms implemented in the cryptographic module.
Cryptographic Module	The set of hardware, software, and/or firmware that implements cryptographic security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.
Cryptographic Module Validation Program (CMVP)	A joint NIST and Cyber Centre program that is used to validate cryptographic modules to FIPS 140-3 Security Requirements for Cryptographic Modules, and other NIST cryptographic standards and recommendations. The CMVP has transitioned from FIPS 140-2.
Cryptography	The discipline that treats the principles, means, and methods for making plain information unintelligible. It also means reconverting the unintelligible information into intelligible form.
Decryption	A process that converts encrypted data into plain form by reversing the encryption process.
Deterministic Random Bit Generator (DRBG)	A Random Bit Generator (RBG) produces a sequence of bits (0 or 1) which appear statistically independent and unbiased. Given the same input “seed”, a Deterministic RBG always produces the same output sequence
Digital Signature	A cryptographic transformation of data which provides data integrity and data origin authentication.
Encryption	The transformation of readable data into an unreadable stream of characters using a reversible coding process.
Federal Information Processing Standards (FIPS) Publication 140-3	A publication which specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting Protected information. The requirement covers eleven functionality areas related to the design and implementation of a cryptographic module.
Hash function	A procedure to transform a message of arbitrary length into 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.
Integrity	The accuracy and completeness of information and assets and the authenticity of transactions.
Key Derivation Function	A transformation of secret (as well as possibly non-secret) data into cryptographically strong secret keys.
Key Establishment	A procedure by which multiple participants create or obtain shared secrets, such as cryptographic keys.
Key Management	Procedures and mechanisms for generating, disseminating, replacing, storing, archiving, and destroying keys which control encryption or authentication processes.
Key Wrap	A mode of operation used to encrypt cryptographic keys, as well as provide for their authenticity and integrity.
Message Authentication Code	A fixed-length tag used to verify the authenticity and integrity of a message.
Mode of Operation	A procedure for using an encryption algorithm, sometimes for a specific purpose (such as Key Wrap).
Non-repudiation	A measure designed to provide protection against an individual falsely denying having performed an action.
eXtendable Output Function (XOF)	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.

15.3 References

1. Canadian Centre for Cyber Security. IT Security Risk Management: A Lifecycle Approach (ITSG-33). November 2012.
2. Treasury Board of Canada Secretariat. Guideline on Defining Authentication Requirements. November 2012.
3. Treasury Board of Canada Secretariat. Policy on Government Security. July 2019.
4. National Institute of Standards and Technology. Advanced Encryption Standard. Federal Information Processing Standards (FIPS) Publication 197. November 2001. Updated May 2023.
5. National Institute of Standards and Technology. Recommendation for the Triple Data Encryption Algorithm Block Cipher. Special Publication 800-67 Revision 2. November 2017.
6. Adams, C. The CAST-128 Encryption Algorithm. Request for Comments (RFC) 2144. Internet Engineering Task Force (IETF), May 1997.
7. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation - Methods and Techniques. Special Publication 800-38A. December 2001.
8. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode. Addendum to NIST Special Publication 800-38A. October 2010.
9. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices. Special Publication 800-38E. January 2010.
10. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality. Special Publication 800-38C. May 2004. Updated July 2007.
11. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode. Special Publication 800-38D. November 2017.
12. National Institute of Standards and Technology. Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography. Special Publication 800-56B Revision 2. March 2019.
13. National Institute of Standards and Technology. Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography. Special Publication 800-56A Revision 3. April 2018.
14. National Institute of Standards and Technology. Recommendations for Discrete Logarithm-based Cryptography: Elliptic Curve Domain Parameters. Special Publication 800-186. February 2023.
15. National Institute of Standards and Technology. Digital Signature Standard. Federal Information Processing Standards (FIPS) Publication 186-4. July 2013.
16. National Institute of Standards and Technology. Digital Signature Standard. Federal Information Processing Standards (FIPS) Publication 186-5. February 2023.
17. National Institute of Standards and Technology. Recommendation for Stateful Hash-based Signatures Scheme. Special Publication 800-208. October 2020.

18. National Institute of Standards and Technology. Secure Hash Standard. Federal Information Processing Standards (FIPS) Publication 180-4. August 2015.
19. National Institute of Standards and Technology. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. Federal Information Processing Standards (FIPS) Publication 202. August 2015.
20. National Institute of Standards and Technology. The Keyed-Hash Message Authentication Code. Federal Information Processing Standards (FIPS) Publication 198-1. July 2008.
21. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. Special Publication 800-38B. May 2005. Updated June 2016.
22. National Institute of Standards and Technology. SHA-3 Derived Functions: cSHAKE, KMAC, TupleHash, and ParallelHash. Special Publication 800-185. December 2016.
23. National Institute of Standards and Technology. Recommendation for Key Derivation Methods in Key-Establishment Schemes. Special Publication 800-56C Revision 2. August 2020.
24. National Institute of Standards and Technology. Recommendation for Key Derivation Using Pseudorandom Functions. Special Publication 800-108 Revision 1. August 2022.
25. National Institute of Standards and Technology. Recommendation for Existing Application-Specific Key Derivation Functions. Special Publication 800-135 Revision 1. December 2011.
26. National Institute of Standards and Technology. Recommendation for Password Based Key Derivation: Part 1: Storage Applications. Special Publication 800-132. December 2010.
27. Canadian Centre for Cyber Security. Best Practices for Passphrases and Passwords (ITSAP.30.032). September 2019.
28. National Institute of Standards and Technology. Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping. Special Publication 800-38F. December 2012.
29. National Institute of Standards and Technology. Recommendation for Random Number Generation Using Deterministic Random Bit Generators. Special Publication 800-90A Revision 1. June 2015.
30. National Institute of Standards and Technology. Cryptographic Algorithm Validation Program CAVP. October 2016.
31. National Institute of Standards and Technology. Cryptographic Module Validation Program CMVP. October 2016.
32. National Institute of Standards and Technology. Security Requirements for Cryptographic Modules. Federal Information Processing Standards (FIPS) Publication 140-3. March 2019.
33. Canadian Centre for Cyber Security. Common Criteria. September 2018.
34. National Institute of Standards and Technology. Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program. March 2023.
35. Canadian Centre for Cyber Security. *NIST Announces Post-Quantum Cryptography Selections*. July 2022.
36. Canadian Centre for Cyber Security. Preparing Your Organization for The Quantum Threat to Cryptography. ITSAP.00.017. February 2021.