PRACTITIONER SERIES

INFORMATION TECHNOLOGY SECURITY GUIDANCE

CRYPTOGRAPHIC ALGORITHMS FOR UNCLASSIFIED, PROTECTED A, AND PROTECTED B INFORMATION

ITSP.40.111

August 2016

Canada

FOREWORD

The *Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental IT security coordinators to ITS Client Services at CSE.

For further information, please contact CSE's ITS Client Services area by e-mail at ITSclientservices@cse-cst.gc.ca or call (613) 991-7654.

EFFECTIVE DATE

This publication takes effect on (08/02/2016).

[Original signed by]
Scott Jones
Deputy Chief, IT Security

August 2, 2016
Date

OVERVIEW

The Government of Canada's (GC) 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 GC information.

Data authenticity, confidentiality and 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.

The information in this publication identifies and describes approved cryptographic algorithms and appropriate methods of use to protect the confidentiality of PROTECTED A and PROTECTED B information and the integrity of information to the medium injury level as defined in CSE's *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [6].

TABLE OF CONTENTS

1 INTRODUCTION

Government of Canada (GC) departments rely on Information Technology (IT) systems to achieve business objectives. These interconnected systems are often subject to serious threats that can have adverse effects on departmental business activities. Compromises to GC networks can be expensive and threaten the availability, authenticity, confidentiality, and integrity of the GC information assets.

The GC uses cryptography to protect the authenticity, confidentiality, and integrity of its information. When used with valid domain parameters and specific key lengths, the cryptographic algorithms listed in Information Technology Security Guidance for Practitioners (ITSP).40.111 are approved cryptographic mechanisms for protecting UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

For requirements on the use of CSE-approved cryptography to protect PROTECTED C and Classified information, refer to CSE's *ITSD-01A: IT Security Directive for the Application of Communications Security using CSE-Approved Solutions* [1] [1].

ITSP.40.111 has been created to aid the technology practitioner in choosing and appropriately using cryptographic algorithms to protect UNCLASSIFIED, PROTECTED A, and PROTECTED B information. ITSP.40.111 complements the Treasury Board of Canada Secretariat (TBS) *Guideline on Defining Authentication Requirements* [2] and supersedes ITSB-111.

1.1 POLICY DRIVERS

The need to address and counter cyber threats and vulnerabilities currently threatening GC networks is a crucial step in securing GC networks, data and assets. As such, GC departments must ensure IT security policies and procedures are implemented in accordance with the following TBS policies:

- *Policy on Management of Information Technology* [3];
- *Policy on Government Security* [4]; and
- Operational Security Standard: Management of Information Technology Security [5].

1.2 APPLICABLE ENVIRONMENTS

The information in ITSP.40.111 provides cryptographic guidance for IT solutions at the UNCLASSIFIED, PROTECTED A, and PROTECTED B levels. Systems operating in the PROTECTED C or Classified domains may require additional design considerations that are not within the scope of this document[2]. It is the department's responsibility as part of a risk management framework to determine the security objectives required to protect departmental information and services.

[1] Numbers in square brackets indicate reference material. A list of references is located in the Supporting Content section.
[2] Contact CSE COMSEC client services for guidance regarding cryptographic solutions in the PROTECTED C or Classified domains.

1.3 RELATIONSHIP TO THE IT RISK MANAGEMENT PROCESS

CSE's *ITSG-33 IT Security Risk Management: A Lifecycle Approach* [6] guidelines suggest a set of activities at two levels within an organization; the departmental level and the information system level.

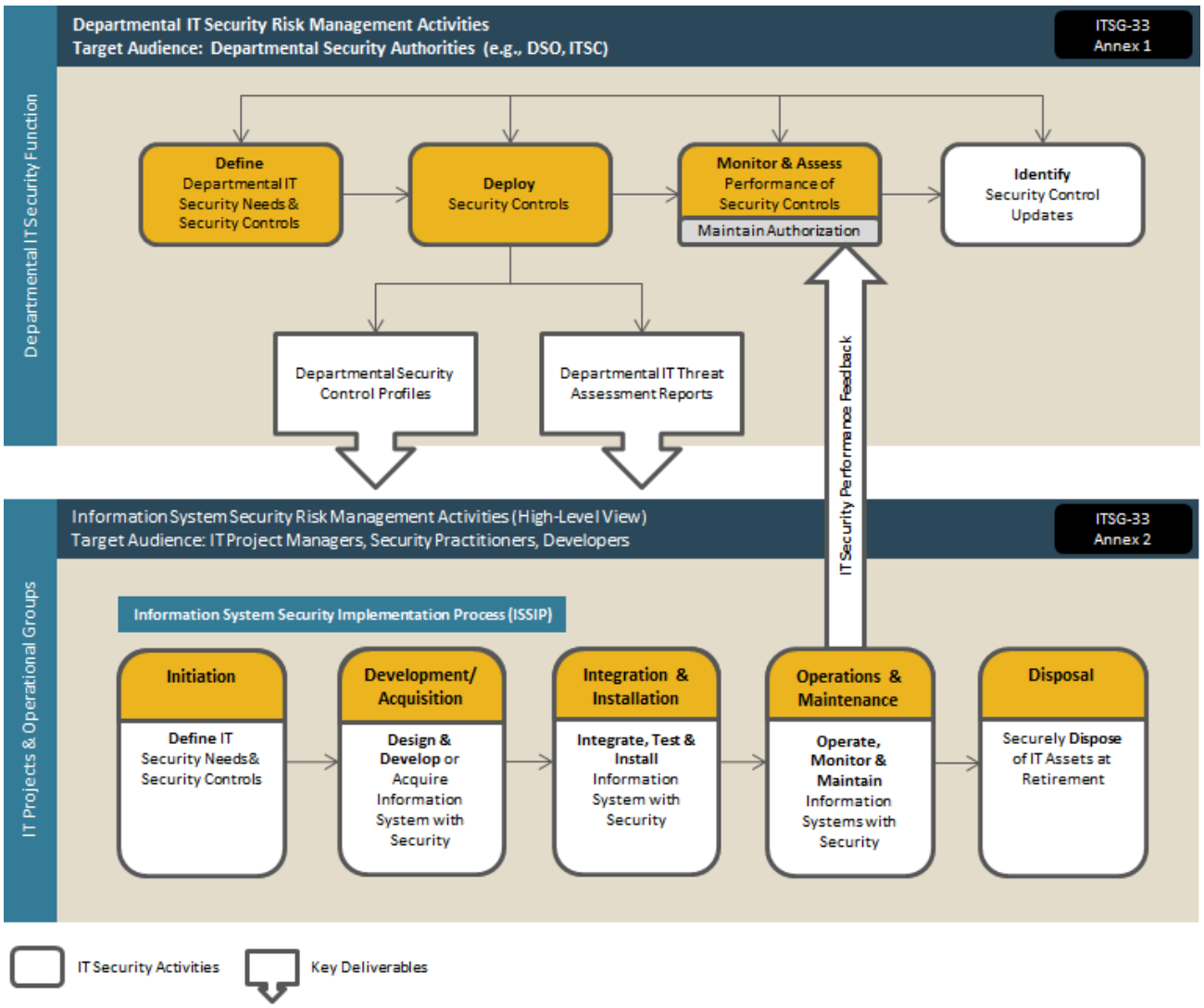

Figure 1 IT Security Risk Management Process

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. ITSP.40.111 will need to be considered during the Define, Deploy, and Monitor and Assess activities. These activities are described in detail in Annex 1 of ITSG-33 [6].

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, and continued performance of the implemented security controls is assessed, reported back and acted upon to address any issues. ITSP.40.111 will need to be considered during all Information System level activities. These activities are described in detail in Annex 2 of ITSG-33 [6].

2 ENCRYPTION ALGORITHMS

The following sections outline the cryptographic algorithms that are approved by CSE for encrypting data to protect the confidentiality of information.

2.1 ADVANCED ENCRYPTION STANDARD ALGORITHM

The Advanced Encryption Standard (AES) algorithm as specified in *National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Publication 197: Advanced Encryption Standard* [7] with key lengths of 128, 192 and 256 bits is approved for encrypting PROTECTED A and PROTECTED B information.

2.2 TRIPLE DATA ENCRYPTION ALGORITHM

The 3-key option of the Triple Data Encryption Algorithm (TDEA) as specified in *NIST Special Publication (SP) 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm Block Cipher* [8] with a key length of 168 bits is approved for encrypting PROTECTED A and PROTECTED B information.

The use of 3-key TDEA should be discontinued by the end of 2030.

2.3 CAST5

The CAST5 algorithm as specified in *Request for Comments (RFC) 2144 The CAST-128 Encryption Algorithm [9]* with a key length of 128 bits is approved for encrypting PROTECTED A and PROTECTED B information.

3 ENCRYPTION ALGORITHM MODES OF OPERATION

The following sections outline the encryption algorithm modes of operation that are approved by CSE.

3.1 PROTECTING THE CONFIDENTIALITY OF INFORMATION

When used with an approved encryption algorithm the following modes of operation as specified in *NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation – Methods and Techniques* [10] are approved to protect the confidentiality of PROTECTED A and PROTECTED B information:

- Electronic Codebook (ECB);
- Cipher Block Chaining (CBC);
- Cipher Feedback (CFB);
- Output Feedback (OFB); and
- Counter (CTR).

When used with an approved encryption algorithm the following Cipher Block Chaining with Ciphertext Stealing (CBC-CS) modes of operation as specified in the *Addendum to NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for CBC Mode* [28] are approved to protect the confidentiality of PROTECTED A and PROTECTED B information:

- CBC-CS1;
- CBC-CS2; and
- CBC-CS3.

When used with the AES encryption algorithm the 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* [11] is approved to protect the confidentiality of PROTECTED A and PROTECTED B information on storage devices.

3.2 PROTECTING THE CONFIDENTIALITY AND AUTHENTICITY OF INFORMATION

When used with an approved encryption algorithm, the following modes of operation are approved by CSE to protect the confidentiality and authenticity of PROTECTED A and PROTECTED B information and the 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* [12]; and
- Galois/Counter Mode (GCM): As specified in *NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode* [13].

4 KEY ESTABLISHMENT SCHEMES

The following sections outline the key establishment schemes that are approved by CSE for use with approved cryptographic algorithms.

4.1 RIVEST, SHAMIR, ADLEMAN

The Rivest, Shamir, Adleman (RSA)-based key-transport and key-agreement schemes as specified in *NIST SP 800-56B Revision 1: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography* [14] with an RSA modulus length of at least 2048 bits are approved for key establishment for protecting PROTECTED A and PROTECTED B information.

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

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 with a field size of at least 2048 bits as specified in *NIST SP 800-56A Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* [15] are approved for key establishment for protecting PROTECTED A and PROTECTED B information.

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

The Elliptic Curve Cryptography (ECC) Cofactor Diffie-Hellman (CDH) and ECC MQV-based key-agreement schemes with valid domain parameters for the EB, EC, ED or EE parameter-size sets with a subgroup order size of at least 224 bits as specified in *NIST SP 800-56A Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography [15]* are approved for key establishment for protecting PROTECTED A and PROTECTED B information. CSE strongly recommends using the elliptic curve domain parameters in Appendix D of *NIST FIPS 186-4: Digital Signature Standard* [16] for ECC CDH and ECC MQV.

The EC, ED, or EE parameter-size sets with a subgroup order size of at least 256 bits should be used by the end of 2030.

5 DIGITAL SIGNATURE ALGORITHMS

The following sections outline the digital signature algorithms that are approved by CSE for digital signature applications.

5.1 RSA

The RSA digital signature algorithm as specified in *NIST FIPS 186-4: Digital Signature Standard* [16] and *RSA PKCS #1 v2.2: RSA Cryptography Standard* [17] with an RSA modulus length of at least 2048 bits is approved for data integrity and data origin authentication of UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

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

5.2 DIGITAL SIGNATURE ALGORITHM

The Digital Signature Algorithm (DSA) as specified in *NIST FIPS 186-4: Digital Signature Standard* [16] with valid domain parameters and a prime modulus length of at least 2048 bits is approved for data integrity and data origin authentication of UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

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

5.3 ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM

The Elliptic Curve Digital Signature Algorithm (ECDSA) as specified in *NIST FIPS 186-4: Digital Signature Standard* [16] with valid domain parameters for a field size of at least 224 bits is approved for data integrity and data origin authentication of UNCLASSIFIED, PROTECTED A, and PROTECTED B information. CSE strongly recommends using the elliptic curve domain parameters in Appendix D of *FIPS 186-4: Digital Signature Standard* [16] for ECDSA.

The field size should be increased to at least 256 bits by the end of 2030.

6 SECURE HASH ALGORITHMS

The following sections outline the secure hash algorithms (SHA) that are approved by CSE for use with the specified, approved cryptographic algorithms.

6.1 SHA-1

SHA-1 as specified in *NIST FIPS 180-4: Secure Hash Standard* [18] is approved for use with keyed-hash message authentication codes, key derivation functions and random bit generators for protecting UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

SHA-1 is not approved for use with digital signature algorithms.

6.2 SHA-2

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] are approved for use with digital signature algorithms, keyed-hash message authentication codes, key derivation functions and random bit generators for protecting UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

6.3 SHA-3

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* [29] are approved for use with digital signature algorithms, keyed-hash message authentication codes, key derivation functions and random bit generators for protecting UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

7 MESSAGE AUTHENTICATION CODES

The following sections outline the message authentication code algorithms that are approved by CSE for data integrity and data origin authentication.

7.1 KEYED-HASH MESSAGE AUTHENTICATION CODE

Keyed-Hash Message Authentication Code (HMAC) as specified in *NIST FIPS 198-1: The Keyed-Hash Message Authentication Code* [19] with a key length of at least 112 bits is approved for data integrity and data origin authentication of UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

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

7.2 CIPHER-BASED MESSAGE AUTHENTICATION CODE

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* [20] with a key length of at least 112 bits is approved for data integrity and data origin authentication of UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

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

7.3 GALOIS/COUNTER MODE MESSAGE AUTHENTICATION CODE

Galois/Counter Mode Message Authentication Code (GMAC) as specified in *NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode* [13] is approved for data integrity and data origin authentication of UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

8 KEY DERIVATION FUNCTIONS

The following sections outline the key derivation functions that are approved by CSE for the derivation of cryptographic keys from key-establishment or pre-shared secrets.

8.1 SINGLE-STEP KEY DERIVATION FUNCTION

The Single-Step Key Derivation Function (KDF) as specified in *NIST SP 800-56A Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography* [15] is approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

8.2 KEY DERIVATION USING PSEUDORANDOM FUNCTIONS

The KDFs using Pseudorandom Functions (PRFs) as specified in *NIST SP 800-108: Recommendation for Key Derivation Using Pseudorandom Functions* [21] are approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

8.3 EXTRACTION-THEN-EXPANSION KEY DERIVATION FUNCTION

The Extraction-then-Expansion KDFs as specified in *NIST SP 800-56C: Recommendation for Key Derivation through Extraction then Expansion* [22] are approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

8.4 INTERNET KEY EXCHANGE VERSION 1 KEY DERIVATION FUNCTION

When used in the context of the Internet Key Exchange version 1 (IKEv1) protocol with an approved Keyed-Hash Message Authentication Code and an approved Secure Hash Algorithm the IKEv1 KDF as specified in *NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] is approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

8.5 INTERNET KEY EXCHANGE VERSION 2 KEY DERIVATION FUNCTION

When used in the context of the Internet Key Exchange version 2 (IKEv2) protocol with an approved Keyed-Hash Message Authentication Code and an approved Secure Hash Algorithm the IKEv2 KDF as specified in *NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] is approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

8.6 TRANSPORT LAYER SECURITY VERSION 1.2 KEY DERIVATION FUNCTION

When used in the context of the Transport Layer Security version 1.2 (TLS 1.2) protocol with an approved Keyed-Hash Message Authentication Code and an approved Secure Hash Algorithm the TLS 1.2 KDF as specified in *NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] is approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

8.7 SECURE SHELL KEY DERIVATION FUNCTION

When used in the context of the Secure Shell (SSH) protocol with an approved Secure Hash Algorithm the SSH KDF as specified in *NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] is approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

8.8 SECURE REAL-TIME TRANSPORT PROTOCOL KEY DERIVATION FUNCTION

When used in the context of the Secure Real-time Transport Protocol (SRTP) with an approved encryption algorithm the SRTP KDF as specified in *NIST SP 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions* [27] is approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

8.9 TRUSTED PLATFORM MODULE KEY DERIVATION FUNCTION

When used in the context of a Trusted Platform Module (TPM) session with an approved Keyed-Hash Message Authentication Code and an approved Secure Hash Algorithm the TPM KDF as specified in *NIST SP 800-135: Recommendation for Existing Application-Specific Key Derivation Functions* [27] is approved for the derivation of keys for protecting PROTECTED A and PROTECTED B information.

9 KEY WRAP MODES OF OPERATION

The following sections outline the Key Wrap (KW) modes of operation that are approved by CSE for key wrapping to protect the confidentiality and integrity of cryptographic keys.

9.1 AES KEY WRAP

The KW mode as specified in *NIST SP 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping* [23] is approved to protect the confidentiality and integrity of cryptographic keys for protecting PROTECTED A and PROTECTED B information.

9.2 AES KEY WRAP WITH PADDING

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* [23] is approved to protect the confidentiality and integrity of cryptographic keys for protecting PROTECTED A and PROTECTED B information.

9.3 TRIPLE DATA ENCRYPTION ALGORITHM KEY WRAP

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* [23] and with a key length of 168 bits is approved to protect the confidentiality and integrity of cryptographic keys for protecting PROTECTED A and PROTECTED B information.

The use of 3-key TDEA in TKW should be discontinued by the end of 2030.

10 DETERMINISTIC RANDOM BIT GENERATORS

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* [24] are approved by CSE for the production of random bits for cryptographic applications for protecting UNCLASSIFIED, PROTECTED A, and PROTECTED B information:

- Hash_DRBG;
- HMAC_DRBG; and
- CTR_DRBG.

The use of Dual_EC_DRBG is no longer approved.

11 COMMERCIAL TECHNOLOGIES ASSURANCE PROGRAMS

In addition to using CSE-approved cryptographic algorithms, parameters and key lengths to ensure a suitable level of cryptographic security, the following guidance on implementation assurance requirements should also be considered:

- Cryptographic algorithm implementations should be tested and validated under the Cryptographic Algorithm Validation Program (CAVP);
- Cryptographic modules should be tested and validated under the Cryptographic Module Validation Program (CMVP) for compliance to *FIPS 140-2* [25];
- 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. The security policy document specifies the cryptographic security provided by a module and describes its capabilities, protection, and access controls. The security policy document should be used 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 140-2 and the Cryptographic Module Validation Program* [26] to ensure that only CSE-approved algorithms are used; and
- Information technology security products should be evaluated and certified to meet the Common Criteria standard by a Certificate Authorizing Scheme that is a member of the international Common Criteria Recognition Arrangement.

12 SUMMARY

Cryptography provides security mechanisms which can be used to protect the authenticity, confidentiality, and integrity of GC 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 CSE-approved cryptographic algorithms to protect UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

12.1 CONTACTS AND ASSISTANCE

If your department would like more detailed information on Cryptographic Algorithms for Protected Information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

13 SUPPORTING CONTENT

13.1 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
CSE	Communications Security Establishment
CTR	Counter
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code
ECC	Elliptic Curve Digital Signature Algorithm
ECDSA	Elliptic Curve Cryptography
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
KDF	Key Derivation Function
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	Tripe Data Encryption Key Wrap
TLS	Transport Layer Security
TPM	Trusted Platform Module
TRA	Threat and Risk Assessment

13.2 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.
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 CSE program that is used to validate cryptographic modules to FIPS 140-2 Security Requirements for Cryptographic Modules, and other NIST cryptographic standards and recommendations.
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 voice or data information into plain form by reversing the encryption process.
Digital Signature	A cryptographic transformation of data which provides the service of authentication, data integrity, and signer non-repudiation.
Encryption	The transformation of readable data into an unreadable stream of characters using a reversible coding process.
Federal Information Processing Standards (FIPS) Publication 140-2	Specify 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.
Integrity	The accuracy and completeness of information and assets and the authenticity of transactions.
Key Management	Procedures and mechanisms for generating, disseminating, replacing, storing, archiving, and destroying keys which control encryption or authentication processes.

13.3 REFERENCES

Number	Reference
1	Communications Security Establishment. *ITSD-01A: IT Security Directive for the Application of Communications Security using CSE-Approved Solutions*, January, 2014
2	Treasury Board of Canada Secretariat. *Guideline on Defining Authentication Requirements,* November 2008.
3	Treasury Board of Canada Secretariat. *Policy on the Management of Information Technology,* 1 July 2007.
4	Treasury Board of Canada Secretariat. *Policy on Government Security,* 1 July 2009.
5	Treasury Board of Canada Secretariat. *Operational Security Standard: Management of Information Technology,* n.d.
6	Communications Security Establishment. *ITSG-33 IT Security Risk Management: A Lifecycle Approach,* December 2014.
7	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 197 Advanced Encryption Standard,* 26 November 2001.
8	National Institute of Standards and Technology. *Special Publication 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm Block Cipher,* January 2012.
9	Adams, C. *The CAST-128 Encryption Algorithm* Internet RFCs, ISSN 2070-1721, RFC 2144, May 1997.

10	National Institute of Standards and Technology. *Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation – Methods and Techniques,* December 2001.
11	National Institute of Standards and Technology. *Special Publication 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices,* January 2010.
12	National Institute of Standards and Technology. *Special Publication 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality* May 2004.
13	National Institute of Standards and Technology. *Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode,* November 2007.
14	National Institute of Standards and Technology. *Special Publication 800-56B Revision 1: Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography,* August 2009.
15	National Institute of Standards and Technology. *Special Publication 800-56A Revision 2: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography,* May 2013.
16	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 186-4: Digital Signature Standard,* July 2013.
17	RSA Laboratories. *RSA PKCS #1 v2.2: RSA Cryptography Standard,* October 2012.
18	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 180-4: Secure Hash Standard,* August 2015.
19	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 198-1: The Keyed-Hash Message Authentication Code,* July 2008.
20	National Institute of Standards and Technology. *Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication,* May 2005.
21	National Institute of Standards and Technology. *Special Publication 800-108: Recommendation for Key Derivation Using Pseudorandom Functions,* October 2009.
22	National Institute of Standards and Technology. *Special Publication SP 800-56C: Recommendation for Key Derivation through Extraction then Expansion,* November 2011.
23	National Institute of Standards and Technology. *Special Publication 800-38F: Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping,* December 2012.
24	National Institute of Standards and Technology. *Special Publication 800-90A Revision 1: Recommendation for Random Number Generation Using Deterministic Random Bit Generators,* June 2015.
25	National Institute of Standards and Technology. *Federal Information Processing Standards 140-2,* November 2001.
26	National Institute of Standards and Technology. *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program,* May 2016.
27	National Institute of Standards and Technology. *Special Publication 800-135 Revision 1: Recommendation for Existing Application-Specific Key Derivation Functions*, December 2011.
28	National Institute of Standards and Technology. *Addendum to NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation: Three Variants of Ciphertext Stealing for*

	CBC Mode, October 2010.
29	National Institute of Standards and Technology. *Federal Information Processing Standards Publication 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions,* August 2015.