Communications Security Establishment | Centre de la sécurité des télécommunications

PRACTITIONER SERIES

INFORMATION TECHNOLOGY SECURITY GUIDANCE

GUIDANCE ON SECURELY CONFIGURING NETWORK PROTOCOLS

ITSP.40.062

August 2016

Canada

FOREWORD

The *Guidance on Securely Configuring Network Protocols* 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 securely transmit sensitive data and information is fundamental to the delivery of programs and services. Cryptographic security protocols provide security mechanisms which can be used to ensure the confidentiality, integrity, and authenticity of sensitive GC information.

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

The information in this publication identifies and describes acceptable security protocols and their appropriate methods of use to ensure continued protection of UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

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, confidentiality, and integrity of the GC information assets.

The Information Technology Security Guidance for the Practitioner (ITSP).40.062 provides GC departments guidance on:

- Securely configuring network protocols to protect UNCLASSIFIED, PROTECTED A, and PROTECTED B information;
- Approved algorithms that the Communications Security Establishment (CSE) recommends for use with these network protocols; and
- Standards and National Institute of Standards and Technology (NIST) special publications that provide additional information on these network protocols.

ITSP.40.062 has been created to aid the technology practitioner in choosing and using appropriate security protocols for protecting UNCLASSIFIED, PROTECTED A, and PROTECTED B information and complements the Treasury Board of Canada Secretariat (TBS) *Guideline on Defining Authentication Requirements* [1][1].

ITSP.40.062 supersedes *ITSB-60 - Guidance on the Use of the Transport Layer Security Protocol within the Government of Canada* and *ITSB-61 - Guidance on the Use of the IP Security Protocol within the Government of Canada* and should be used in conjunction with *ITSP.40.111 - Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* [2].

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.40.062 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.

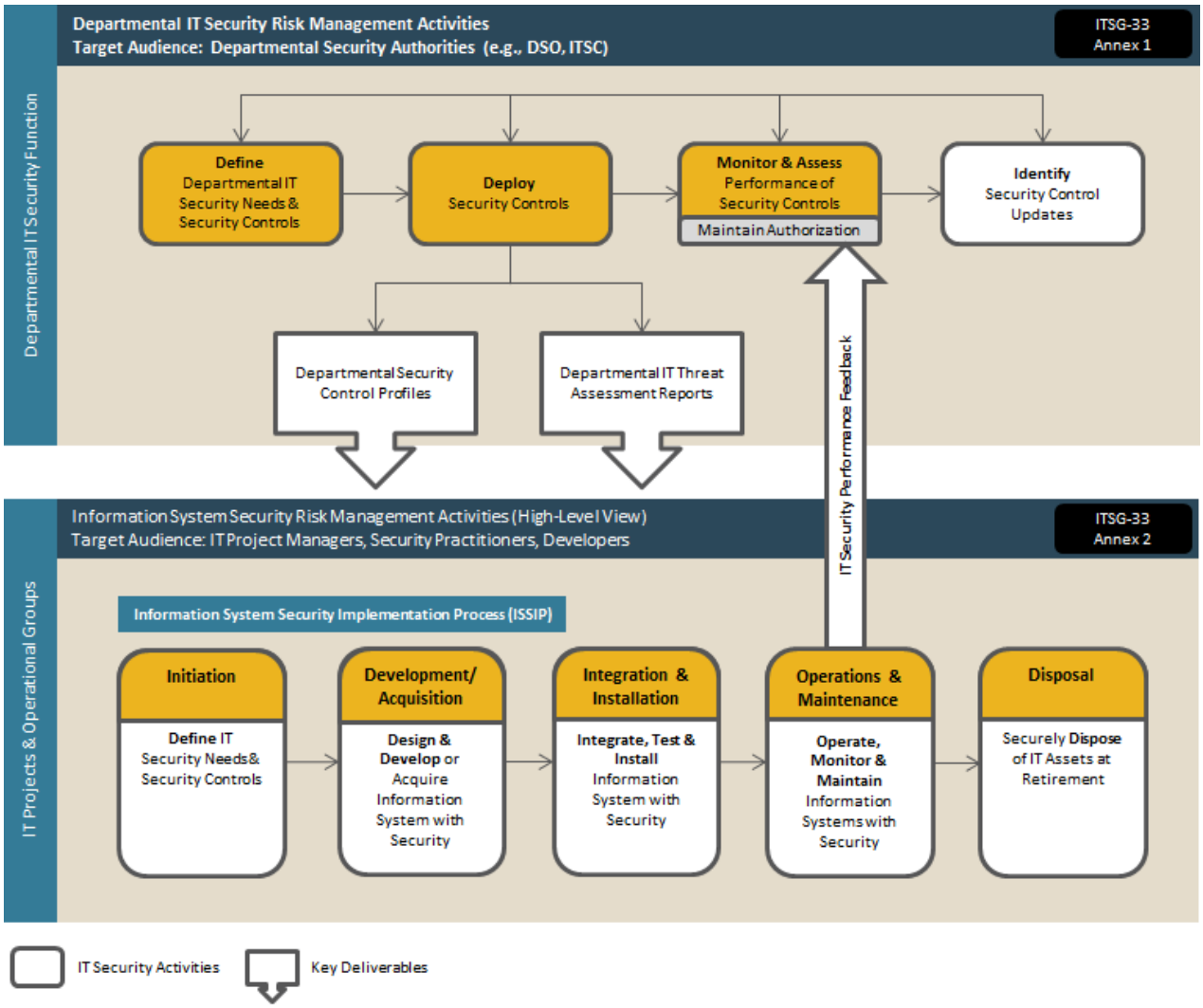

Figure 1 IT Security Risk Management Process

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.40.062 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.40.062 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 PUBLIC KEY INFRASTRUCTURE

Public Key Infrastructures (PKIs) support the management of public keys for security services in PKI-enabled protocols, including Transport Layer Security (TLS), Internet Protocol Security (IPsec), and Secure/Multipurpose Internet Mail Extensions (S/MIME).

PKI key management guidance is provided in *NIST Special Publication (SP) 800-57 Part 3 Rev 1 Recommendation for Key Management Part 3: Application-Specific Key Management Guidance* [7]. CSE recommends following the guidance on the installation and administration of PKI in NIST SP 800-57 Part 3 Rev 1 section 2 [7].

Public key certificates should be formatted in the X.509 version 3 certificate format as specified in *Request for Comments (RFC) 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [8].

Protocol implementations should support multiple certificates with their associated private keys to support algorithm and key size agility. Public key certificates used for signing, key agreement, or key encipherment should be distinguished by the key usage extension asserting one of the following values:

- digitalSignature;
- keyEncipherment; or
- keyAgreement.

To satisfy the cryptographic guidance provided in ITSP.40.111 [2], SHA-1 should not be used for public key certificate digital signature generation or verification.

3 TRANSPORT LAYER SECURITY

Transport Layer Security (TLS) is a protocol developed to protect the authenticity, confidentiality, and integrity of Internet communications between server and client applications.

TLS servers and clients should be configured to use TLS 1.2 as specified in *RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2* [9]. **Older versions of TLS and all versions of Secure Sockets Layer (SSL) should not be used since vulnerabilities exist.**

Detailed TLS configuration guidance for both servers and clients is provided in *NIST Special Publication (SP) 800-52 Rev 1 Guidelines on the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations* [10]. CSE recommends following the guidance on the selection, configuration, and administration of TLS server and client found in NIST SP 800-52 Rev 1 sections 3.9 and 4.9 [10] respectively. In addition to supporting the TLS extensions listed in NIST SP 800-52 Rev 1 section 3.4 [10], CSE recommends that TLS servers support the Encrypt-then-MAC extension as specified in *RFC 7366 Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)* [11].

Servers using TLS to protect HTTP traffic (i.e. HTTPS) should support HTTP Strict Transport Security (HSTS) as specified in *RFC 6797 HTTP Strict Transport Security (HSTS)* [12].

An email server acting as a Message Transfer Agent (MTA) for Simple Mail Transfer Protocol (SMTP) should support the negotiation of TLS with other MTAs. SMTP traffic can be upgraded to TLS using STARTTLS as specified in *RFC 3207 SMTP Service Extension for Secure SMTP over Transport Layer Security* [41] or, preferably, DNS-Based Authentication of Named Entities (DANE) TLS as specified in *RFC 7672 SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)* [42]. Note, however, that these opportunistic encryption techniques are only supported on a hop-by-hop basis; end-to-end message protection is provided by S/MIME (see Section 6).

When TLS is used to protect the confidentiality of PROTECTED A and PROTECTED B information or the integrity of UNCLASSIFIED, PROTECTED A, and PROTECTED B information, implementations should mutually authenticate between the server and client using X.509 version 3 certificates.

3.1 TLS CIPHER SUITES

The following TLS cipher suites satisfy the cryptographic guidance provided in ITSP.40.111 [2]:

- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256;
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384;
- TLS_ECDHE_ECDSA_WITH_AES_128_CCM;
- TLS_ECDHE_ECDSA_WITH_AES_256_CCM;
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256;
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384;
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA;
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA;
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256;
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384;

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256;
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384;
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA;
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA;
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256;
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256;
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384;
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384;
- TLS_DHE_RSA_WITH_AES_128_CCM;
- TLS_DHE_RSA_WITH_AES_256_CCM;
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256;
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256;
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256;
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256;
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA;
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA;
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA;
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA;
- TLS_RSA_WITH_AES_128_GCM_SHA256;
- TLS_RSA_WITH_AES_256_GCM_SHA384;
- TLS_RSA_WITH_AES_128_CCM;
- TLS_RSA_WITH_AES_256_CCM;
- TLS_RSA_WITH_AES_128_CBC_SHA256;
- TLS_RSA_WITH_AES_256_CBC_SHA256;
- TLS_RSA_WITH_AES_128_CBC_SHA;
- TLS_RSA_WITH_AES_256_CBC_SHA;
- TLS_RSA_WITH_3DES_EDE_CBC_SHA;
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA;
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA;
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA; and
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA.

CSE strongly recommends selecting TLS cipher suites using ephemeral Diffie-Hellman **(DH) and ephemeral** Elliptic Curve Diffie-Hellman **(ECDH) (those with DHE or ECDHE specified in the cipher suite name) since they**

provide perfect forward secrecy. When using a cipher suite that provides perfect forward secrecy, the compromise of a long-term private key used in deriving a subsequent session key does not cause the compromise of prior session keys.

The TLS cipher suites listed above are listed in CSE-recommended order of preference; however, TLS servers and clients may use any or all of the listed cipher suites in any order.

TLS_RSA_WITH_AES_128_CBC_SHA is a mandatory cipher suite for TLS 1.2 as specified in RFC 5246 [9]. Therefore, TLS servers and clients should support TLS_RSA_WITH_AES_128_CBC_SHA to ensure interoperability, but the other listed suites should be preferred.

Cipher suites do not specify a key size for the public key algorithm. TLS servers and clients should ensure that the server and client ephemeral key-pairs used to establish the master secret satisfy the key length requirements specified in ITSP.40.111 [2].

The secure hash algorithm specified in the cipher suite name is used for Keyed-Hash Message Authentication Code (HMAC) and/or Pseudo-Random Function (PRF) computation, not for digital signature generation or verification; SHA-1 is approved for keyed-hash message authentication codes and may be specified in TLS cipher suites that satisfy the cryptographic guidance provided in ITSP.40.111 [2].

To satisfy the cryptographic guidance provided in ITSP.40.111 [2], SHA-1 should not be used for digital signature generation or verification.

4 INTERNET PROTOCOL SECURITY

Internet Protocol Security (IPsec) is a suite of network protocols developed to protect the authenticity, confidentiality, and integrity of Internet communications between network hosts, gateways, and devices. IPsec also provides access control, replay protection and traffic analysis protection.

IPsec hosts, gateways and devices should be configured to use IPsec as specified in *RFC 4301 Security Architecture for the Internet Protocol* [13], *RFC 4302 IP Authentication Header* [14], RFC 4303 *IP Encapsulating Security Payload (ESP)* [15] and *RFC 7321 Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)* [16].

IPsec key management guidance is provided in *NIST SP 800-57 Part 3 Rev 1* [7]. CSE recommends following the guidance on the installation and administration of IPsec found in NIST SP 800-57 Part 3 Rev 1 section 3 [7].

When IPsec is used to protect the confidentiality of PROTECTED A and PROTECTED B information or the integrity of UNCLASSIFIED, PROTECTED A, and PROTECTED B information, digital signatures should be used for authentication. Pre-shared keys should not be used for authentication without careful consideration.

IPsec should use Encapsulated Security Payload (ESP) in tunnel mode to protect authenticity, integrity, and confidentiality of the packets and packet headers. Authentication Header (AH) should not be used, as it does not protect confidentiality.

IKEv2 as specified in *RFC 7296 Internet Key Exchange Protocol Version 2 (IKEv2)* [17] is recommended over IKEv1 as specified in *RFC 2409 The Internet Key Exchange (IKE)* [18]. If IKEv1 is required, main mode should be used for IKE phase 1 and quick mode for IKE phase 2. Aggressive mode should not be used for IKE phase 1 and informational and group modes should not be used for IKE phase 2.

When using RSA digital signature authentication in IKEv2, the RSA Probabilistic Signature Scheme (RSASSA-PSS) as specified in *RFC 7427 Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)* [19], is recommended over PKCS#1 v1.5.

4.1 IPSEC CIPHER SUITES

IPsec cryptographic algorithm guidance is provided in *NIST SP 800-57 Part 3 Rev 1 Section 3.2.1* [7]. CSE recommends following the cryptographic guidance found in NIST SP 800-57 Part 3 Rev 1 section 3.2.1 [7]. In addition to the algorithms listed in NIST 800-57 Part 3 Rev 1 section 3.2.1 [7], the CAST5 encryption algorithm may be used to satisfy the cryptographic guidance provided in ITSP.40.111 [2].

The cryptographic user interface suites ("UI suites") for IPsec as specified in *RFC 6379 Suite B Cryptographic Suites for IPsec* [20] specify values for cryptographic options used in IPsec. Suite-B-GCM-128 and Suite-B-GCM-256 as specified in *RFC 6379 Suite B Cryptographic Suites for IPsec* [20], satisfy the cryptographic guidance provided in ITSP.40.111 [2] and are recommended for use. Table 1 outlines the IPsec cipher suite.

Table 1 IPsec Cipher Suite

	SUITE-B-GCM-128	SUITE-B-GCM-256
Encapsulating Security Payload (ESP) Encryption	Advanced Encryption Standard (AES) with 128-bit keys and 16-octet Integrity Check Value in GCM mode	AES with 256-bit keys and 16-octet Integrity Check Value in GCM mode
IKEv2 Encryption	AES with 128-bit keys in Cipher Block Chaining (CBC) mode	AES with 256-bit keys in CBC mode
IKEv2 PRF	Keyed-Hash Message Authentication Code (HMAC)-SHA-256	HMAC-SHA-384
IKEv2 Integrity	HMAC-SHA-256-128	HMAC-SHA-384-192
IKEv2 Diffie-Hellman (DH) group	256-bit random ECP group	384-bit random ECP group

5 SECURE SHELL

Secure Shell (SSH) is a protocol developed to protect the authenticity, confidentiality, and integrity of remote access, file transfer and point-to-point tunnelling over the Internet.

SSH servers and clients should be configured to use SSH protocol version 2.0 as specified in *RFC 4251 The Secure Shell (SSH) Protocol Architecture* [21], *RFC 4252 The Secure Shell (SSH) Authentication Protocol* [22], *RFC 4253 The Secure Shell (SSH) Transport Layer Protocol* [23] and *RFC 4254 The Secure Shell (SSH) Connection Protocol* [24].

SSH key management guidance is provided in *NIST SP 800-57 Part 3 Rev 1* [7]. CSE recommends following the guidance on the installation and administration of SSH found in NIST SP 800-57 Part 3 Rev 1 section 10 [7].

SSH public key authentication or Kerberos authentication are recommended over password authentication. SSH host-based authentication should not be used as it is vulnerable to IP address spoofing.

5.1 SSH PARAMETER SELECTION

SSH cryptographic algorithm guidance is provided in *NIST SP 800-57 Part 3 Rev 1* [7]. CSE recommends following the SSH Transport Layer Protocol cryptographic guidance found in NIST SP 800-57 Part 3 Rev 1 section 10.2.1 [7]. In addition to the algorithms listed in NIST SP 800-57 Part 3 Rev 1 section 10.2.1 [7] the CAST5 encryption algorithm may be used to satisfy the cryptographic guidance provided in ITSP.40.111 [2].

5.1.1 ENCRYPTION ALGORITHM SELECTION

CBC mode should not be used in SSH as its use in SSH is vulnerable to a plaintext recovery attack.

The following SSH encryption algorithms satisfy the cryptographic guidance provided in ITSP.40.111 [2]:

- aes128-ctr (RFC 4344 [34]);
- aes192-ctr (RFC 4344 [34]);
- aes256-ctr (RFC 4344 [34]);
- 3des-ctr (RFC 4344 [34]);
- cast128-ctr (RFC 4344 [34]);
- AEAD_AES_128_GCM (RFC 5647 [35]); and
- AEAD_AES_256_GCM (RFC 5647 [35]).

The AEAD algorithms protect both authenticity and confidentiality. Therefore, when AEAD algorithms are used a separate HMAC is not required.

5.1.2 MAC ALGORITHM SELECTION

In addition to the AEAD authenticated encryption algorithms specified above, the following SSH HMAC algorithms satisfy the cryptographic guidance provided in ITSP.40.111 [2]:

- hmac-sha1 (RFC 4253);
- hmac-sha2-256 (RFC 6668 [36]); and

- hmac-sha2-512 (RFC 6668 [36]).

5.1.3 KEY EXCHANGE ALGORITHM

The following SSH key exchange algorithms satisfy the cryptographic guidance provided in ITSP.40.111 [2] when used with parameter sets of the appropriate size:

- diffie-hellman-group-exchange-sha256 (RFC 4419 [37]);
- ecdh-sha2 (RFC 5656 [38]);
- ecmqv-sha2 (RFC 5656 [38]); and
- rsa2048-sha256 (RFC 4432 [39]).

5.1.4 PUBLIC KEY ALGORITHM

SSH optionally allows for authentication using public keys. The following SSH public key algorithms satisfy the cryptographic guidance provided in ITSP.40.111 [2]:

- ecdsa-sha2-nistp224(RFC 5656 [38]);
- ecdsa-sha2-nistp256(RFC 5656 [38]);
- ecdsa-sha2-nistp384(RFC 5656 [38]);
- ecdsa-sha2-nistp521 (RFC 5656 [38]);
- x509v3-rsa2048-sha256 (RFC 6187 [40])
- x509v3-ecdsa-sha2-nistp224 (RFC 6187 [40]);
- x509v3-ecdsa-sha2-nistp256 (RFC 6187 [40]);
- x509v3-ecdsa-sha2-nistp384 (RFC 6187 [40]); and
- x509v3-ecdsa-sha2-nistp521 (RFC 6187 [40]).

The raw RSA key format “ssh-rsa” uses SHA-1 for digital signing. To satisfy the cryptographic guidance provided in ITSP.40.111 [2], “ssh-rsa” should not be used.

6 SECURE/MULTIPURPOSE INTERNET MAIL EXTENSIONS

Secure/Multipurpose Internet Mail Extensions (S/MIME) is a standard developed to protect the authenticity, confidentiality, and integrity of electronic messages over the Internet.

S/MIME applications should be configured as specified in *RFC 5751 Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification* [25] and *RFC 5652 Cryptographic Message Syntax (CMS)* [26].

Guidance on the use of Elliptic Curve Cryptography (ECC) in CMS for digital signature generation and the exchange of keys to encrypt or authenticate messages is provided in in *RFC 5753 Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)* [27].

The use of SHA-1 for digital signature generation does not satisfy the cryptographic guidance provided in ITSP.40.111 [2] and should not be used as a digestAlgorithm to sign messages.

The use of the RSASSA-PSS is recommended over PKCS #1 v1.5 as the encoding mechanism for RSA digital signatures. This applies to both X.509 Certificates as specified in *RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters* [28] and to Signed-data content types as specified in *RFC 4056 Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)* [29]

CSE recommends using RSA-KEM for RSA encryption within the EnvelopedData content type as specified in *Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS) RFC 5990* [30]. RSAES-OAEP as specified in *Use of the RFC 3560 RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)* [31] and *RFC 5756 Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters* [28] may also be used. S/MIME implementations using PKCS #1 v1.5 encoding could be vulnerable to the Million Message Attack described in *RFC 3218 Preventing the Million Message Attack on Cryptographic Message Syntax,* [32]; software vendors allowing this encoding for RSA decryption within S/MIME should indicate mitigations to avoid the attack.

If signing with multiple signature algorithms, the multipleSignatures CMS attribute should be used as specified in *RFC 5752 Multiple Signatures in Cryptographic Message Syntax (CMS)* [33].

7 COMMERCIAL TECHNOLOGIES ASSURANCE PROGRAMS

Implementations of PKI, TLS, IPsec, SSH and S/MIME should follow the implementation assurance guidance in section 11 of ITSP.40.111 *Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information* [2].

8 SUMMARY

Cryptographic security protocols provide security mechanisms which can be used to protect the authenticity, confidentiality, and integrity of GC information. Various protocols may be required to satisfy these security requirements, and each protocol should be selected and implemented to ensure these requirements are met. This publication provides guidance on the use of security protocols to protect UNCLASSIFIED, PROTECTED A, and PROTECTED B information.

8.1 CONTACTS AND ASSISTANCE

If your department would like more detailed information on Securely Configuring Network Protocols, please contact:

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

9 SUPPORTING CONTENT

9.1 LIST OF ABBREVIATIONS

Term	Definition
AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AH	Authentication Header
CA	Certification Authority
CBC	Cipher Block Chaining
CAVP	Cryptographic Algorithm Validation Program
CMS	Cryptographic Message Syntax
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
CSE	Communications Security Establishment
DANE	DNS-Based Authentication of Named Entities
DH	Diffie-Hellman
DTLS	Datagram Transport Layer Security
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Ephemeral Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECP	Elliptic Curve Groups modulo a Prime
ESP	Encapsulating Security Payload
FIPS	Federal Information Processing Standard
GC	Government of Canada
GCM	Galois/Counter Mode
HMAC	Keyed-Hash Message Authentication Code
HSTS	HTTP Strict Transport Security
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
IT	Information Technology
ITS	Information Technology Security
ITSG	Information Technology Security Guidance
ITSP	Information Technology Security Guidance for the Practitioner

MAC	Message Authentication Code
MTA	Message Transfer Agent
PFS	Perfect Forward Secrecy
PKI	Public Key Infrastructure
PRF	Pseudo-Random Function
NIST	National Institute of Standards and Technology
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SA	Security Association
SHA	Secure Hash Algorithm
SSH	Secure Shell
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SP	Special Publication
SSL	Secure Socket Layer
TBS	Treasury Board of Canada Secretariat
TLS	Transport Layer Security

9.2 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.
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 Standard (FIPS) 140-1, 140-2, and 140-3	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.
Forward Secrecy	A property of key establishment protocols where the compromise of the long-term private key will not allow an adversary to re-compute previously derived keys or sessions.
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.

9.3 REFERENCES

Number	Reference
1	Treasury Board of Canada Secretariat. *Guideline on Defining Authentication Requirements,* November 2008.
2	Communications Security Establishment. *ITSP.40.111 Cryptographic Algorithms for UNCLASSIFIED, PROTECTED A, and PROTECTED B Information, August* 2016.
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. *Special Publication 800-57 Part 3 Rev 1 Recommendation for Key Management Part 3: Application-Specific Key Management Guidance*,
8	Cooper, D., et al. *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* Internet RFCs, ISSN 2070-1721, RFC 5280*,* May 2008.
9	Dierks, T., and E. Rescorla. *The Transport Layer Security (TLS) Protocol Version 1.2,* Internet RFCs, ISSN 2070-1721, RFC 5246, August 2008.
10	National Institute of Standards and Technology. *Special Publication (SP) 800-52 Rev 1 Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations.* April 2014.
11	Gutman, P. *Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)*. Internet RFCs, ISSN 2070-1721, RFC 7366, September 2014.
12	Hodges, J., C. Jackson, and A. Barth. *HTTP Strict Transport Security (HSTS)*. Internet RFCs, ISSN 2070-1721, RFC 6797, November 2012.
13	Kent, S., and K. Seo. *Security Architecture for the Internet Protocol.* Internet RFCs, ISSN 2070-1721, RFC 4301, December 2005.
14	Kent, S. *IP Authentication Header*. Internet RFCs, ISSN 2070-1721, RFC 4302, December 2005.
15	Kent, S. *IP Encapsulating Security Payload (ESP)*. Internet RFCs, ISSN 2070-1721, RFC 4303, December 2005.

16	McGrew, D., and P. Hoffman. *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*. Internet RFCs, ISSN 2070-1721, RFC 7321, August 2014.
17	Kaufman, C., et al. *Internet Key Exchange Protocol Version 2 (IKEv2)*. Internet RFCs, ISSN 2070-1721, RFC 7296, October 2014.
18	Harkins, D., and D. Carrel. *The Internet Key Exchange (IKE)*. Internet RFCs, ISSN 2070-1721, RFC 2409, November 2009.
19	Kivinen, T., and J. Snyder. *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*. Internet RFCs, ISSN 2070-1721, RFC 7427, January 2015.
20	Law, L., and J. Solinas. *Suite B Cryptographic Suites for IPsec*. Internet RFCs, ISSN 2070-1721, RFC 6379, October 2011.
21	Ylonen, T., and C. Lonvick, Ed. *The Secure Shell (SSH) Protocol Architecture*. Internet RFCs, ISSN 2070-1721, RFC 4251, January 2006.
22	Ylonen, T., and C. Lonvick, Ed. *The Secure Shell (SSH) Authentication Protocol*. Internet RFCs, ISSN 2070-1721, RFC 4252, January 2006.
23	Ylonen, T., and C. Lonvick, Ed. *The Secure Shell (SSH) Transport Layer Protocol*. Internet RFCs, ISSN 2070-1721, RFC 4253, January 2006.
24	Ylonen, T., and C. Lonvick, Ed. *The Secure Shell (SSH) Connection Protocol*. Internet RFCs, ISSN 2070-1721, RFC 4254, January 2006.
25	Ramsdell, B., and S. Turner. *Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification*. Internet RFCs, ISSN 2070-1721, RFC 5751, January 2010.
26	Housley, R. *Cryptographic Message Syntax (CMS)*. Internet RFCs, ISSN 2070-1721, RFC 5652, September 2009.
27	Turner, S., and D. Brown. *Use of Elliptic Curve Cryptography (ECC) Algorithms in Cryptographic Message Syntax (CMS)*. Internet RFCs, ISSN 2070-1721, RFC 5753, January 2010.
28	Turner, S., et al. *Updates for RSAES-OAEP and RSASSA-PSS Algorithm Parameters*. Internet RFCs, ISSN 2070-1721, RFC 5756, January 2010.
29	Schaad, J. *Use of the RSASSA-PSS Signature Algorithm in Cryptographic Message Syntax (CMS)*. Internet RFCs, ISSN 2070-1721, RFC 4056, June 2005.
30	Randall, J., et al. *Use of the RSA-KEM Key Transport Algorithm in the Cryptographic Message Syntax (CMS)*. Internet RFCs, ISSN 2070-1721, RFC 5990, September 2010.
31	Housley, R. *Use of the RSAES-OAEP Key Transport Algorithm in Cryptographic Message Syntax (CMS)*. Internet RFCs, ISSN 2070-1721, RFC 3560, July 2003.
32	Rescorla, R. *Preventing the Million Message Attack on Cryptographic Message Syntax*. Internet RFCs, ISSN 2070-1721, RFC 3218, January 2002.
33	Turner, S., and J. Schaad. *Multiple Signatures in Cryptographic Message Syntax (CMS)*. Internet RFCs, ISSN 2070-1721, RFC 5752, January 2010.
34	Bellare, M., T. Kohno, and C. Namprempre. *The Secure Shell (SSH) Transport Layer Encryption Modes.* Internet RFCs, ISSN 2072-1721, RFC 4344, January 2006.
35	Igoe, K., and J. Solinas. *AES Galois Counter Mode for the Secure Shell Transport Layer Protocol*. Internet RFCs, ISSN 2070-1721, RFC 5647, August 2009.
36	Bider, D., and M. Baushke. *SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol*. Internet RFCs, ISSN 2070-1721, RFC 6668, July 2012.

37	Friedl, M., N. Provos, and W. Simpson. *Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol*. Internet RFCs, ISSN 2070-1721, RFC 4419, March 2006.
38	Stebila, D., and J. Green. *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer.* Internet RFCs, ISSN 2070-1721, RFC 5656, December 2009.
39	Harris, B. *RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol.* Internet RFCs, ISSN 2070-1721, RFC 4432, March 2006.
40	Igoe, K., and D. Stebila. *X.509v3 Certificates for Secure Shell Authentication*. Internet RFCs, ISSN 2070-1721, RFC 6187, March 2011.
41	Hoffman, P., *SMTP Service Extension for Secure SMTP over Transport Layer Security*, Internet RFCs, ISSN 2070-1721, RFC 3207, February 2002.
42	Dukhovni, V., et al.SMTP *Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)*, Internet RFCs, ISSN 2070-1721, RFC 7672, October 2015.