CRYPTOGRAPHIC STANDARDS FOR INFORMATION PROTECTION

Architecture, Standards and Planning Branch
Office of the CIO ● Province of BC
People ● *Collaboration* ● *Innovation*

Document Version 1.7

Replaces: Version 1.6

Cryptographic Standards for Information Protection

Table of Contents

DOCUMENT CONTROL

Date	Author	Version	Change Reference
Oct 9, 2008	Lee & Walker	DRAFT	Initial draft presented to ASRB
Dec 11, 2008	Lee & Walker	DRAFT	Final DRAFT endorsed by ASRB
Dec 23 2008	Lee & Walker	1.0	Approved by CIO
June 9, 2009	Lee & Walker	1.1	Update
July 8, 2010	Lee & Walker	1.2	Update
Aug 12, 2011	Lee & Walker	1.3	Update
Aug 19, 2012	Lee & Walker	1.4	Update
Jan 02, 2015	R. Walker	1.5	Additions, Updates & Maintenance
Dec 19, 2016	R. Walker	1.6	Multi-Use Digital Certificates & Maintenance
Feb 28, 2017	R. Walker	1.7	Issuing Authority for User Certificates

Version 1.7 (Feb 2017) highlights:

- REVISED: Section 2.2 Issuance of User Certificates

Version 1.6 (Nov 2016) highlights:

- NEW: Section 2.5 Multi-Use Digital Certificates
- VALIDATED: URL's

Version 1.5 (Mar 2015) highlights:

- REVISED: Section 3.1 Web Protocol
- UPDATES: All Sections, verified URL's.
- NEW: Section 4.8 Whole disk encryption for Macs
- REVISED: Front Cover Refreshed

Version 1.4 (Aug 2012) highlights:

- NEW: Chapter 1: Algorithms and Key Sizes
- REMOVED: (Old) Section 1.4 Length of Public Keys.
- REVISED: Section 3.3 File Transfer Protocol with Security.
- REVISED: Section 4.3 USB Flash Drives.

Version 1.3 (Aug 2011) highlights:

- NEW: Section 3.7 Portable External Hard Drives.
- REVISED: Section 1.5 Certificate Status Checking (removed some guidance).
- REVISED: Some wording changes for improved clarity.
- Some formatting improvements.

Version 1.2 (July 2010) highlights: (Cont'd)

- NEW: Section 1.5 Certificate Status Checking.
- REVISED: Section 1.3 Issuance of Server Certificates.
    - The standard has been reworded for improved clarity – the scope & intent are unchanged
    - The context has been reworded for improved clarity around applicability.
- All references to WTS have been changes to Shared Services BC.

The "**Changed:**" date reflects only changes thought to be of possible material impact.

Version 1.1 (June 2009) highlights:

- New: Appendix A: Compliance Schedule for Web Service SOAP Security.
- Moved to: Appendix B: Compliance Schedule for Cryptographic Standards.
- Minor changes to parameters prescribed in SOAP security specification.

Version 1.0 (Jan. 2009) highlights:

- Approved and Published

INTRODUCTION

This document contains a family of standards for the cryptographic protection of information. These are standards of the Government of British Columbia, approved by the Chief Information Officer (CIO).

APPLICABILITY

For many of standards in this document the question of applicability rests with the information owner. In these cases, applicability may be determined by the following steps:

Step 1: A set of business requirements is gathered and documented.

Step 2: A Privacy Impact Assessment is performed and documented.

Step 3: A Security and Threat Risk Assessment is performed and documented.

Step 4: Based on a review of 1-3 above, determine if cryptographic controls are required.

Step 5: If controls are required use this family of standards for further planning.

Each standard in this family provides further information on applicability.

COMPLIANCE SCHEDULE

The compliance schedule for these standards is located in the Appendix.

NOTES TO USERS

Terminology

The term "MUST" is defined as an absolute requirement of the specification.

"SHOULD" (when in upper case) means that there may be valid reasons in particular circumstances to use alternate methods, but the full implications must be understood and carefully weighed before choosing a different course. The use of an alternate method requires the approval of the ADM of the information owner. For the purposes of these standards "information owner" is defined in the Province's Information Security Policy.

Shared Services BC (SSBC) Support for Cryptographic Standards

This document assumes the availability of certain products and services from Shared Services BC (SSBC). SSBC will be providing support for the January 2009 Cryptographic Standards as the infrastructure evolves and will be balancing service enhancements with the need to carefully manage rates. Full compliance (as per Compliance Timelines section) across SSBC services will be a multi-year undertaking.

Topics Not Included

There are some subject areas which, for various reasons, could not be accommodated in the time available to develop these standards. At some future point, more topics will be addressed.

Some topics NOT currently covered:

- Cryptographic controls applied by database management systems for the purposes of protecting back-up data
- Virtual private network systems
- Server side disk encryption: Windows, Linux, MVS, UNIX.
- Cryptographic controls for Directory Access Protocol
- Protection of activation data for digital certificate request fulfilment

1. ALGORITHMS AND KEY SIZES	**Effective: 2012-08-19** **Reviewed: 2014-08-19**
1.1 Public Key Algorithm	**Changed: 2012-08-19**

Purpose

This standard provides guidance on controls used for the protection of information and systems.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Algorithms and key size are critical aspects of cryptographic information protection. This section is intended to help implementers make informed decisions in the absence of specific directives elsewhere in this family of standards.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where public key cryptography is being applied in circumstances not covered by any other standard in this family, implementers MUST use one of the following choices:

1. RSA based cryptography
   - 1.1 The RSA key size MUST be no less than 1024 bits.
   - 1.2 The RSA key size SHOULD be 2048 bits.

2. Elliptic curve cryptography (ECC).
   - 2.1 ECC curve and key parameters MUST be selected from among those recommended in FIPS 186-3, APPENDIX D.
   - 2.2 The bit length of '*n*' specified in Table D-1 MUST be no less than 224.

Additional Guidance

SHOULD and MUST are defined in the section **NOTES TO USERS**.

References

NIST - FIPS 186-4 Digital Signature Standard (DSS) (APPENDIX D)
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

1. ALGORITHMS AND KEY SIZES	**Effective: 2012-08-19** **Reviewed: 2014-08-19**
1.2 Block Cipher Algorithm	**Changed: 2012-08-19**

Purpose

This standard provides guidance on controls used for the protection of information and systems.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Algorithms and key size are critical aspects of cryptographic information protection. This section is intended to help implementers make informed decisions in the absence of specific directives elsewhere in this family of standards.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where a block cypher is being applied in circumstances not covered by any other standard in this family, implementers MUST use the following:

1. Advanced Encryption Standard (AES), NIST - FIPS 197
    1.1 The AES key size MUST be no less than 256 bits.

Additional Guidance

None.

References

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

1. ALGORITHMS AND KEY SIZES	**Effective: 2012-08-19** **Reviewed: 2014-08-19**
1.3 Hashing Algorithms	**Changed: 2012-08-19**

Purpose

This standard provides guidance on controls used for the protection of information and systems.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Hash functions, also known as message digest functions, can play a critical role in protection of information. This section is intended to help implementers make informed decisions in the absence of specific directives elsewhere in this family of standards.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where a hash function is being applied in circumstances not covered by any other standard in this family, implementers SHOULD use the following:

1. Secure Hash Algorithm as specified in NIST - FIPS PUB 180-3

   1.2 The block size MUST be no less than 256 bits (i.e. SHA-256).

Additional Guidance

SHOULD and MUST are defined in the section **NOTES TO USERS**.
Where the technology is available legacy systems should migrate to SHA-256.

References

NIST - FIPS PUB 180-3 Secure Hash Standard (SHS)
http://csrc.nist.gov/publications/PubsFIPS.html#fips180-4

2. DIGITAL CERTIFICATES	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
2.1 Multi-factor Authentication	**Changed: 2012-08-19**

Purpose

This section specifies the government's standard for user multi-factor authentication. Multi-factor authentication lowers the risk of unauthorized access to protected government information assets.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

One aspect of protecting information is ensuring that only authorized persons can access it. User ID and password are commonly used for this purpose. The effectiveness of user authentication depends on the confidence in the identity of the person requesting access. Confidence can be improved by using multi-factor authentication (MFA). MFA is an effective means to ensure the authenticity of the person making such a request.

By specifying an X.509 digital certificate protected on a tamper-resistant device this standard mandates a uniform, standardized approach for two-factor authentication. Solutions requiring more than two factors may be granted as an exception by the OCIO. The main target of this standard is government information systems. However, the approach taken will enable benefits in other areas. Digital certificates can be used for controlling building access, performing digital signatures and supporting non-repudiation.

This standard applies where there is a need for multi-factor authentication for system users.

The need for multi-factor authentication is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where multi-factor authentication is required it MUST be implemented as follows:

One authentication factor MUST be based on a X.509 certificate stored on a tamper-resistant device that meets FIPS 140-2 Level 2 and is issued under a government approved registration process. The tamper-proof device MUST also meet the requirements of ISO 7816-1 *Identification Cards – Integrated Circuit Cards Part 2: Cards with Contacts – Dimensions and Locations of Contacts*.

The X.509 certificate attributes MUST conform to the Identity Information Management Standards for the province.

Additional Guidance

- The issuance of user certificates is covered in Section 2.2.
- The above authentication standard should be integrated with WEB single sign-on, VPN, email, and other standard government services.

References

OCIO – Information Security Policy 6.6.1 Network security configuration control
OCIO – Information Security Policy 6.9.1 Electronic commerce
OCIO – Information Security Policy 6.10.3 Protection of information system logging facilities
OCIO – Information Security Policy 7.1.1 Access control policy management
OCIO – Information Security Policy 7.2.2 Allocation and use of system privileges
OCIO – Information Security Policy 7.5.4 Control of system utility programs
OCIO – Information Security Policy 8.3 Cryptographic controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Liberty Alliance – Strong Authentication

http://www.projectliberty.org/liberty/strategic_initiatives/strong_authentication

Multi-factor authentication methods will be compatible with the province's recommendations for a building access solution. The following identification card (i.e. smartcard) standards have been included for reference:

- ISO 7810
- ISO 7811
- ISO 7812
- ISO 7813
- ISO 7816
- ISO 4909
- NIST - FIPS 201-1

NIST - FIPS 140-2 Security Requirements for Cryptographic Modules
http://www.csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

2. DIGITAL CERTIFICATES	**Effective: 2009-01-14** **Reviewed: 2017-02-29**
2.2 Issuance of User Certificates	**Changed: 2017-02-29**

Purpose

This standard specifies how digital certificates (for end-users) will be issued by Province of British Columbia to employees, business partners and optionally to the broader public sector.

This standard helps protect the Province's information and technology assets. The desired outcome is to preserve the privacy of sensitive information and to position the Province's IM/IT infrastructure to meet evolving business needs.

This standard provides specific guidance for the application of security policy.

Context

In early 2016 a Digital Certificate Service (DCS) was launched by the Office of the Government Chief Information Officer (OCIO). This new service contains all the public key infrastructure, policies and procedures needed for issuing and managing digital certificates for end-users. It provides foundational infrastructure to further secure the Province's information assets and communications.

A Digital certificate is a credential that is issued by an authority in accordance with a strictly defined process, much like a driver's license. The issuing authority is responsible for the policies and procedures required to ensure the integrity of the system. The type of certificates issued by the DCS are for end-users, such as employees or partners of the Province.

The requirement to apply cryptographic controls (e.g. user certificate) is determined by a Privacy Impact Assessment, a Security Threat and Risk Assessment, or the business requirements.

Scope

This standard applies to end-user certificates issued in the name of (i.e. representing) the Province of British Columbia. This standard does not apply to, or restrict, user certificates issued by partners (e.g. other governments, external agencies) to the Province for accessing external services.

Standard

1.1 The Digital Certificate Service of the OCIO is the exclusive issuing authority for end-user certificates bearing the name "Province of British Columbia".

1.2 User certificates bearing the name "Province of British Columbia" issued by or on behalf of the Province MUST be obtained through the Digital Certificate Service.

1.3 Subscribers MUST follow the certificate management policies and procedures set forth by the OCIO DCS.

Additional Guidance

- A subscriber is a program area, ministry or agency that adopts the use of user certificates.
- This standard will be updated as new or additional certificate authorities are authorized.

References

OCIO – Information Security Policy 8.3 Cryptographic controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols

http://tools.ietf.org/html/rfc4210

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509-201210-I/en

2. DIGITAL CERTIFICATES	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
2.3 Issuance of Server Certificates	**Changed: 2011-08-11**

Purpose

This section specifies the government's standard for the issuance of digital certificates for server systems. This standard provides a unifying direction for all ministries and agencies that require digital certificates.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Digital certificates play an important role in the protection of information. This standard specifies the way X.509 certificates for servers will be issued.

A server is a system or device connected to a network that offers services to clients. While providing a service, a server may itself request a service from another system, thus acting in the role of client. If a certificate is being used to identify a system (in either roles of server or client) then this standard applies.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

The following requirement governs all parties whose internet domain name is managed by Shared Services BC:

Where an X.509 certificate is required for system authentication it MUST be obtained through Shared Services BC.

Additional Guidance

- None.

References

OCIO – Information Security Policy 8.3 Cryptographic controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509-201210-I/en

2. DIGITAL CERTIFICATES	**Effective: 2010-01-26** **Reviewed: 2014-08-19**
2.4 Certificate Status Checking	**Changed: 2010-04-30**

Purpose

This section specifies government requirements for checking the status of X.509 digital certificates.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

X.509 certificates play a role in providing assurance for the authenticity of an assertion. Assertions are such things as: a digital signature on a contract or the user-ID used for a logon request. Every certificate has an associated status. A certificate's status is important. For example if a certificate's status is "REVOKED" that certificate is no longer valid as a proof of identity for signing a document or logging on to a system.

This standard specifies the steps that should be taken to check the status of a X.509 certificate. It is intended to cover all uses of X.509 certificates, e.g. signing and authentication.

Standard

When an X.509 certificate is used to make an assertion the status of the certificate SHOULD be checked, subject to availability, by one of the following methods:

1. Online Certificate Status Protocol (OCSP) as defined in RFC 2560.
2. Certificate Revocation List (CRL) as defined in RFC 5280.

Additional Guidance

- Shared Services BC will provide certificate status information, via OCSP for certificates issued by the Public Works and Government Services Canada (PWGSC) Certificate Authority of the Government of Canada.

- Government systems validating PWGSC certificates should obtain certificate status information from Shared Services BC.

References

OCIO – Information Security Policy 8.3 Cryptographic controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP
http://tools.ietf.org/html/rfc6277

IETF - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
http://tools.ietf.org/html/rfc6818

2. DIGITAL CERTIFICATES	**Effective: 2016-11-17** **Reviewed: TBD**
2.5 Multi-use SSL Certificates	**Changed: 2016-11-17**

Purpose

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure and better positioned to support future business needs.

Context

SSL Certificates are important because they underpin citizen trust in government's online services. Certificates are also important because they help ensure the trustworthy administration of the Province's data centers.

The Province employs many SSL certificates, some of which are of a type known as "multi-use".

Multi-use certificates involve wider, more serious security considerations than regular SSL certificates. For example, multi-use certificates can be used to establish trust outside of the original context. Consequently, they can inconspicuously introduce risks to other provincial services and users (i.e. beyond the original business area). Because this risk is inconspicuous, it undermines risk management and good security practice.

Therefore, multi-use certificates should only be used after a careful security analysis.
The term "multi-use" encompasses 2 kinds of SSL certificates: wildcard and multi-domain. (Multi-domain certificates are also known as SAN or UC certificates.)

This standard sets conditions on multi-use SSL certificates for domains owned or operated on behalf of the Province of BC.

Standard

Part 1 of 2: **Multi-domain certificates**

Part 1 applies to Multi-domain X.509 certificates that DO NOT contain a hostname with an embedded '' character.*

1.1 New deployments of multi-domain certificates MUST be appraised in a Security Threat and Risk Assessment (STRA).

Part 2 of 2: **Wildcard certificates**

A wildcard certificate is any kind of X.509 certificate containing a hostname (for server identity) that has an embedded wildcard character '' in it.*

2.1 The use of *.gov.bc.ca is prohibited. *(cont'd)*

2.2 Existing certificates using "*.gov.bc.ca" MUST be removed from service upon reaching their expiry date.

a. In special circumstances an OCIO exemption may be applied for.

2.1 New deployments of wildcard certificates MUST be appraised in a Security Threat and Risk Assessment (STRA).

a. The STRA MUST address risks related to using a wildcard certificate.

b. Common risks, as well as business risks, must be considered.

2.3 A wildcard application form must be submitted for review.
Note: this form is available from the OCIO's Information Security Branch.

a. The STRA must accompany the application form.

b. The requesting Ministry must agree to implement the STRA's recommendations for mitigating common risks. (i.e. risks impacting other parties)

c. The business owner must acknowledge the business risks identified in the STRA.

Additional Guidance

1. A certificate that has been appraised under an existing, valid STRA (as per 1.1 or 2.3) does not require a new STRA for the routine renewal of that certificate.
2. This standard does not prohibit wildcard certificates for sub-domains.
3. The term "**business owner**" refers to the Assistant Deputy Minister of the business line.
4. The term "**risk**" means the potential for loss.
5. A **business risk** is a potential for loss that is limited to the line of business.
6. A **common risk** is a potential for loss that extends beyond the line of business.
7. For this standard, the definition of a **Wildcard** certificate is any type of certificate (i.e. including multi-domain certificates) that contains one or more hostnames (for server identity) that contain a wildcard character '*'.
8. **Multi-domain** certificates are also known as: Unified Communications Certificates (UC) and Subject Alternate Name Certificates (SAN).

References

OCIO – Information Security Policy 8.3 Cryptographic controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Understanding Multi-Use Certificates
http://wiki.apache.org/httpd/UnderstandingMultiUseSSLCertificates

RFC 2818 HTTP Over TLS
https://tools.ietf.org/html/rfc2818

3. INFORMATION IN TRANSIT	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
3.1 Web Protocol	**Changed: 2015-05-28**

Purpose

This standard provides direction for all ministries and agencies having requirements for secure web communications based on hypertext transfer protocol (HTTP). It specifies the standard for protecting personal and sensitive information communicated over the HTTP protocol.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens and will make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Over the past decade various industry standards have been proposed to help secure web (i.e. HTTP) communications. As time passed and shortcomings emerged these standards have been improved. This government-wide standard is meant to ensure that the most current, reliable protocols are being used to protect information.

This standard applies where there is a need to apply cryptographic controls to secure HTTP.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required for HTTP, they MUST be implemented as follows:

PART 1 of 3: CERTIFICATES

1.1 An X.509 certificate MUST be used for performing server authentication.

1.2 Public facing sites using HTTPS SHOULD use an Extended Validation (EV) Certificate.

PART 2 of 3: TRANSPORT LAYER

2.1. HTTPS MUST be used with TLS 1.1 or above - subject to availability.

2.2. Web servers supporting TLS 1.1 or above MUST disable ALL versions of SSL.

2.3. Sites not supporting TLS 1.1 or above MUST decommission SSL by Jan. 1, 2016.

PART 3 of 3: ENCRYPTION

3.1. HTTPS MUST be used with AES.

3.2. The AES key length MUST not be less than 128 bits.

3.3. Web servers supporting HTTPS MUST disable RC4.

3.4. Perfect forward secrecy SHOULD be used where available.

Additional Guidance

- Regular scans for HTTPS vulnerabilities are recommended.
- Support for forward secrecy is recommended where higher security is required and performance requirements allow.
- The software implementing HTTPS should be patched on a timely basis.
- Server certificates must conform to sections 2.3 and 1.1 of this standard.
- All reasonable measures should be taken to protect the server's private key.
- For applications requiring high assurance, client side certificates for mutual authentication should be used.
- Client certificates must conform to section 2.1 of this standard: Multi-factor Authentication and to section 2.2: Issuance of User Certificates.

References

OCIO – Information Security Policy 6.6.1 Secured path
OCIO – Information Security Policy 7.4.2 Remote access to government networks or services
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls
OCIO – Information Security Policy 7.7.2 Teleworking security

Wikipedia – Forward Secrecy
http://en.wikipedia.org/wiki/Forward_secrecy

IETF – The Transport Layer Security (TLS) Protocol Version 1.2
http://tools.ietf.org/html/rfc5246

Industry forum for EV certificates
http://www.cabforum.org/

Guidelines for the Issuance and Management of Extended Validation Certificates
https://cabforum.org/documents/

IETF – Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T – Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509-201210-I/en

NIST – FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

3. INFORMATION IN TRANSIT	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
3.2 SSH (for Administration Purposes)	**Changed: 2009-01-14**

Purpose

This standard provides direction for all ministries and agencies responsible for the administration of remote systems and network attached devices. It specifies the standard for protecting sensitive telecommunications by providing confidentiality and authentication.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

All devices and systems attached to a network must be administered. Because of the distributed nature of networks the administration function is usually performed remotely. This raises a need for authentication and information protection.

This standard applies in situations where a command line is used for performing remote administration of a system or device.

Standard

Command line administration of remote systems and devices MUST be done by employing SSH Version 2 or higher. The encryption algorithm used MUST be AES with a minimum key length of 256 bits. Mutual authentication MUST be used between user and server.

Additional Guidance

- Server certificates must conform to sections 2.3 and 1.1 of this standard.
- All reasonable measures should be taken to protect the server's private key.
- Client certificates must conform to section 2.1 of this standard: Multi-factor Authentication and to section 2.2: Issuance of User Certificates.

References

OCIO – Information Security Policy 6.6.1 Secured path
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls

IETF – The Secure Shell (SSH) Authentication Protocol
http://tools.ietf.org/html/rfc4252

IETF – Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T – Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509-201210-I/en

NIST – FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

3. INFORMATION IN TRANSIT	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
3.3 File Transfer Protocol with Security	**Changed: 2012-08-19**

Purpose

This standard provides direction for all ministries and agencies having requirements for secure file transfer based on File Transfer Protocol (FTP). It specifies the standard for protecting personal and sensitive information communicated via FTP by providing confidentiality and authentication.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

File Transfer Protocol (FTP) is a commonly used utility for transferring files between computers. The FTP protocol is insecure. Over the past decade various standards have been proposed to improve the security of FTP. This standard is meant to help ensure that FTP is deployed securely.

This standard applies where there is a need to apply cryptographic controls to secure FTP.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

FTP-based file transfers that require cryptographic controls MUST employ one of the following two choices:

1. SSH File Transfer Protocol Version 2 (commonly referred to as SFTP)
   1.1. The encryption algorithm used MUST be AES with a minimum key length of 256 bits.
   1.2. If server certificates are used, they SHOULD conform to section 2.3 of this standard.
   1.3. If client certificates are used, they SHOULD conform to sections 2.1 and 2.2 of this standard.
   1.4. If data with an information security classification MEDIUM or above will be handled, both client and server authentication based on public key cryptography MUST be used.

2 FTP over TLS/SSL (commonly referred to as FTPS)

2.1 The encryption algorithm used MUST be AES with a minimum key length of 256 bits.

2.2 Both control and data channels MUST be encrypted.

2.3 Server certificates MUST conform to section 2.3 of this standard.

2.4 Where client certificates are used, they MUST conform to section 2.1 and 2.2 of this standard.

2.5 If data with an information security classification MEDIUM or above will be handled, both client and server authentication based on public key cryptography MUST be used.

Additional Guidance

- Anonymous login should be disabled on the server side.
- All reasonable measures should be taken to protect the server's private key.

References

OCIO – Information Security Policy 6.5.1 Safeguarding backup facilities and media
OCIO – Information Security Policy 6.6.1 Secured path
OCIO – Information Security Policy 6.8.1 Electronic information exchange
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls

IETF - File Transfer Protocol
http://tools.ietf.org/html/rfc959

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

IETF - SSH File Transfer Protocol
http://tools.ietf.org/html/draft-ietf-secsh-filexfer-13

IETF - The Secure Shell (SSH) Protocol Architecture
http://tools.ietf.org/html/rfc4251

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509-201210-I/en

3. INFORMATION IN TRANSIT	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
3.4 Web Service SOAP Security	**Changed: 2009-06-09**

Purpose

This standard provides direction for all ministries and agencies using or planning to use secure SOAP Web Service interactions. It specifies the standard for protecting personal and sensitive information communicated via SOAP messages by providing confidentiality and authentication.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

SOAP, formerly known as the Simple Object Access Protocol, is a protocol for exchanging structured information between computer systems. The main purpose of the SOAP specification is to define structured message exchange. The specification does not attempt to define a security model. Instead SOAP foresees “security” as being defined elsewhere. This approach, while justifiable, has resulted in a host of deployments using incompatible security solutions. This hampers interoperability.

By specifying a single security model this specification aims to:

- Better position us to support business objectives
- Increase security robustness
- Reduce non-essential complexity
- Improve interoperability

This standard applies where there is a need to apply cryptographic controls to secure SOAP with Web Services.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they MUST be implemented as follows:

SOAP Web services that require cryptographic controls MUST be compliant with WS-I Basic Security Profile 1.0 with the following provisions:

Transport layer implementations must comply with one of the following two choices:

- TLS implementations SHOULD implement TLS_RSA_WITH_AES_128_CBC_SHA
- SSL implementations SHOULD implement SSL_RSA_WITH_AES_128_CBC_SHA

Cryptographic modules implementing the above SHOULD be validated to FIPS 140-2.

Additional Guidance

- A SOAP message supporting the authentication of a user would be an example use case for this standard.

References

OCIO – Information Security Policy 6.6.1 Secured path
OCIO – Information Security Policy 6.8.1 Electronic information exchange
OCIO – Information Security Policy 6.9.2 On-line transaction security
OCIO – Information Security Policy 6.9.3 Internet site security
OCIO – Information Security Policy 7.2.3 Authentication credential management
OCIO – Information Security Policy 8.1.1 Security requirements of information systems

WS-I - Security Challenges, Threats and Countermeasures
http://www.ws-i.org/Profiles/BasicSecurity/SecurityChallenges-1.0.pdf

WS-I - Basic Security Profile
http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html

Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

4. INFORMATION AT REST	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
4.1 Windows Full Disk Encryption	**Changed: 2009-01-14**

Purpose

This standard provides direction for all ministries and agencies responsible for information stored in hard drives on computer systems. It specifies the standard for protecting information on hard drives.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Access to information stored on computers is largely dependent on controls provided by the operating system. This information is stored on a hard disk. In some circumstances, operating systems protections can be bypassed leaving the hard disk vulnerable. This raises a need for another level of protection for the drive itself. This protection can be achieved by using hard drive encryption. Even if a computer is lost or stolen encryption provides protection against unauthorized disclosure of information.

The integrity of cryptographic systems depends on preserving secrecy. Thus, it follows that cryptographic keys must be managed securely throughout their lifetime. The typical events in the lifecycle of a cryptographic key include (but are not limited to): generation, distribution, storage, access (e.g. backup, archive, recovery) and destruction.

This standard pertains to the encryption of logical disk volumes under the control of Microsoft Windows Vista or above running on non-server systems.

Standard

Hard disks under the control of Windows Vista or its successors MUST be encrypted. Cryptographic operations MUST be performed with Trusted Platform Module (TPM) 1.2 or higher compliant hardware. The encryption algorithm used MUST be AES with a minimum key length of 256 bits.

Key management MUST be documented and performed in accordance with the following requirements:

- Key Storage
    - The master encryption key shall reside within the TPM hardware and MUST not leave the TPM for the master key’s service life.
- Key Recovery

    - The key recovery password MUST be protected by at least two levels of independent access controls and limited to an audience of personnel authorized for the task of information recovery.
- Logging Transactions
    - All access to the key recovery passwords MUST be recorded in an audit trail.

Information owners MUST ensure that information custodians produce documentation for the above.

Additional Guidance

- Strong protection measures should be taken to protect the key recovery password.
- The master encryption key should reside in the TPM at all times.
- Shared Services BC has chosen to meet the above requirements with a service offering based on BitLocker.
- BitLocker should be deployed in advanced mode with hibernation.
- The BIOS boot order should not be changeable by the user.

References

OCIO – Information Security Policy 5.2.5 Equipment security controls
OCIO – Information Security Policy 6.7.1 Portable storage devices – mandatory controls
OCIO – Information Security Policy 6.7.3 Media handling procedures
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Microsoft - BitLocker Drive Encryption
http://social.TechNet.microsoft.com/Search/en-US?query=bitlocker&ac=3

Trusted Platform Module (TPM) Specifications
https://www.trustedcomputinggroup.org/specs/TPM/

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

4. INFORMATION AT REST	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
4.2 Windows File Encryption	**Changed: 2009-01-14**

Purpose

This section specifies the standard for protecting information stored in individual files.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Within a program area business circumstances will arise under which it is necessary to take additional steps to protect individual files. This protection can be achieved through the use of file encryption.

This standard applies where there is a need to apply cryptographic controls to secure files under the control of a Windows operating system. These controls supplement the basic operating system controls and are intended for end users to apply on a discretionary basis.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they MUST be implemented as follows:

Discretionary file encryption controls MUST be provided by Shared Services BC as a single government-wide solution meeting the following requirements:

- The solution MUST integrate seamlessly with existing government PKI and infrastructure.
- The solution MUST provide individual user and group permission-based access controls.
- The solution MUST be capable of remote administration.
- Files MUST be encrypted with AES 256.
- The file encryption process MUST be automated and transparent to the end-user.
- The solution MUST integrate seamlessly and securely with all currently supported Windows files system types.

Key management MUST be documented and performed in accordance with the following requirements:

- Key Recovery

    - File encryption keys MUST be recoverable.
- Key Backup
    - The file encryption key MUST be backed up on a central server.
    - When a file encryption key is backed up the key MUST be encrypted.
    - A documented process MUST be established to access the backed up keys.
- Logging Transactions
    - All access to the backed-up key MUST be recorded in an audit trail.

Information owners MUST ensure that information custodians produce documentation for the above.

Additional Guidance

- Client certificates must conform to section 1.1 of this standard: Multi-factor Authentication and to section 1.2: Issuance of User Certificates.
- All reasonable measures should be taken to protect PKI private keys.
- Extra care should be taken to protect recovery keys.

References

OCIO – Information Security Policy 6.7.4 Protection of systems documentation
OCIO – Information Security Policy 8.3.1 Acceptable use of cryptography
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Microsoft – Using Encrypted File System (EFS)
http://technet.microsoft.com/en-us/library/bb457116.aspx

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

4. INFORMATION AT REST	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
4.3 USB Flash Drives	**Changed: 2012-08-19**

Purpose

This section specifies the standard for protecting information stored on USB flash drives.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Business circumstances arise under which it is necessary to store files on a USB flash drive (i.e., a form of portable storage device). Steps must be taken to protect files stored on this device. This protection can be achieved by using file encryption.

This standard applies to all USB flash drives used to store government information.

Standard

Only USB flash drives obtained through Shared Services BC may be used for storing government information.

Part 1 of 2: MANDATORY REQUIREMENTS, for all flash drives:

1.1 USB flash drives MUST be certified by NIST to FIPS 140-2 Level 2 or above.

1.2 All user writeable partitions on the drive MUST be fully encrypted.

1.3 The encryption algorithm MUST be AES, i.e. FIPS 192.

1.4 The AES encryption key MUST be a MINIMUM of 256 bits long.

1.5 The device MUST lockdown after consecutive failed login attempts.

1.6 The number of failed login attempts MUST not exceed 12.

1.7 The USB flash drive MUST enforce the use of a complex password.

Part 2 of 2: CONDITIONAL REQUIREMENTS, applicable when handling information with a security classification of “HIGH”.

2.1 USB flash drives MUST be certified by NIST to FIPS 140-2 Level 3.

Additional Guidance

- None

References

OCIO – Information Security Policy 6.7.1 Portable storage devices – mandatory controls
OCIO – Information Security Policy 6.7.3 Media handling procedures
OCIO – Information Security Policy 7.3.1 Selection of Passwords
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

Microsoft – Using Encrypted File System (EFS)
http://technet.microsoft.com/en-us/library/bb457116.aspx

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

NIST - FIPS 140-2 Security Requirements for Cryptographic Modules
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

4. INFORMATION AT REST	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
4.4 Backup Data	**Changed: 2009-01-14**

Purpose

This standard provides direction for ministries and agencies responsible for performing the systematic backup of data. It specifies the standard for the protection of information stored on external backup media.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

The term "backup" refers to the process of making copies of data to protect against data loss.

Backup systems vary widely across different hardware platforms, operating environments and vendor solutions. This specification provides a system-independent set of requirements.

This standard applies where there is a need to apply cryptographic controls to secure information that is systematically being backed up to external media.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they MUST be implemented as follows:

Backup data that requires encryption MUST be encrypted with AES.

A minimum key length of 256 bits MUST be used.

Key management MUST be documented and performed in accordance with the following requirements:

- Key Recovery
  - Encryption keys MUST be recoverable.
- Logging Transactions
  - All access to the backed up data MUST be recorded in an audit trail.

Information owners MUST ensure that information custodians produce documentation for the above.

Additional Guidance

- Periodic verification of backed up data should be performed.
- External media may be interpreted to mean a sibling disk system.

References

OCIO – Information Security Policy 6.5.1 Safeguarding backup facilities and media
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - The Secure Shell (SSH) Authentication Protocol
http://tools.ietf.org/html/rfc4252

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

4. INFORMATION AT REST	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
4.5 Extracted Data on Portable Media	**Changed: 2009-01-14**

Purpose

This standard provides direction for ministries and agencies performing the extraction of data onto portable media.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

The term “extracted data” normally refers to a data set comprised of selected records extracted from a source data set. Extracted data is used for decision support, research, agency reporting or other business related purpose. For this specification “extracted data” is meant to include any computer file being transferred from a source system onto portable media. A common scenario is where extracted data is stored on portable media for transfer between parties, a provider and consumers.

There are foreseeable risks associated with handling and transporting extracted data on portable media. These risks require that measures be taken to protect confidentiality.

Section 7.7.1 of the B.C. Government’s Information Security Policy (ISP) requires the “encryption of stored data” when placed on a portable storage device.

This standard specifies how the ISP Section 7.7.1 encryption requirement is to be implemented.

Standard

Extracted data placed on portable media MUST be encrypted with AES.

A minimum key length of 256 bits MUST be used.

Key management MUST be documented and performed in accordance with the following requirements:

- Key Exchange
  - Encryption keys MUST be handled in a manner that does not put extracted data at risk of disclosure when the media is lost or misplaced.
  - Encryption keys MUST never be transported together with the media.

Additional Guidance

- Key exchange using public key infrastructure is recommended.

- Information temporarily stored on a portable storage device should be transferred to the government network as soon as practicable and then deleted from the portable storage device.

References

OCIO – Information Security Policy 6.5.1 Safeguarding backup facilities and media
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - The Secure Shell (SSH) Authentication Protocol
http://tools.ietf.org/html/rfc4252

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

4. INFORMATION AT REST	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
4.6 Document Signing	**Changed: 2009-01-14**

Purpose

This standard provides direction for ministries and agencies with requirements for the digital signing of documents.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Digital signatures ensure the authenticity of the author and the integrity of the content of a document.

This standard applies where there is a need to apply cryptographic controls to ensure the authenticity and integrity of a document.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they MUST be implemented as follows:

The signing of digital documents MUST be based on X.509 certificates. The signing key pair MUST be distinct from the encryption key pair. The signing key MUST not be recoverable.

When the signing key is lost, stolen or compromised, the user MUST report the incident so that the key can be revoked.

When a user's signing key is revoked and the user is eligible to possess a key, a new key MUST be generated for the user.

When a user is no longer eligible to possess a signing key due to the employment status change, the manager MUST report the change so that the key can be revoked.

Additional Guidance

- Client certificates must conform to section 2.1 of this standard: Multi-factor Authentication and to section 2.2: Issuance of User Certificates.

References

OCIO – Information Security Policy 6.5.1 Safeguarding backup facilities and media
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
https://www.itu.int/rec/T-REC-X.509

NIST - FIPS 186 DSS Digital Signature Standard
http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf

4. INFORMATION AT REST	**Effective: 2011-04-25** **Reviewed: 2014-08-19**
4.7 Portable External Hard Drives	**Changed: 2011-04-25**

Purpose

This section specifies the encryption standard for protecting information stored on portable external hard disk drives and portable external solid state drives (SSD).

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Business circumstances arise under which it is necessary to store files on a portable, external hard disk drive. The Information Security Policy requires that steps be taken to protect files stored on portable storage devices regardless of the security classification of the stored information. The use of encryption is a requirement under this policy.

This standard applies to portable, external hard disk drives and solid state drives used to store information for or on behalf of the Province of British Columbia.

Standard

Part 1 of 2: MINIMUM REQUIREMENTS:

1.1 All information stored on a drive MUST be encrypted using AES encryption.

1.2 The AES encryption key MUST be a MINIMUM of 256 bits long.

1.3 All user writeable partitions on the drive MUST be fully encrypted.

Part 2 of 2: CONDITIONAL REQUIREMENTS, when handling information with a security classification of "HIGH":

2.1 All information stored on a drive MUST be encrypted using an AES hardware encryption module that conforms to **FIPS 140-2 Level 3**. (This clause overrides clause 1.1.)

2.2 The cryptographic modules implementing FIPS 140-2 Level 3 MUST have a FIPS 140-2 Validation Certificate.

Additional Guidance

- Part 1 permits software based encryption, part 2 allows only hardware based encryption.
- See references for a list of validated FIPS 140-2 cryptographic modules.

- A drive or drive array that is stationary by design (i.e. designed to be used at a single, fixed, secure location) and is thus not at risk of being lost, misplaced or stolen is not considered portable.
- Where an STRA is deemed necessary for the safe use of a portable storage device, the STRA should assess the need for a credential recovery process to ensure ongoing user/owner access to the information stored on the device.
- A credential can be in a form of a key or a password with or without a username.
- Where a credential recovery process is required it should incorporate the following:
  1. The credential should be handled and protected like a secret.
  2. Access to and distribution of the credential should be limited to authorized persons based on a need-to-know principle.
  3. The information owner (e.g. ministry) should not need to depend on the device user for the recovery of the credential, unless the risk is deemed acceptable by the owner.

References

1. Information Security Classification Framework
http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-security-classification-framework

2. NIST Cryptographic Module Validation Program
http://csrc.nist.gov/groups/STM/cmvp/index.html

3. Validated FIPS 140-1 and FIPS 140-2 Cryptographic Modules
http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

4. NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

5. NIST - FIPS 140-2 Security Requirements for Cryptographic Modules
http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

6. OCIO - Information Security Policy Home Page
http://www.cio.gov.bc.ca/information-security-policy/

7. OCIO – Information Security Policy 6.7.1 Portable storage devices – Mandatory Controls

8. OCIO – Information Security Policy 6.7.3 Media Handling Procedures

9. OCIO – Information Security Policy 7.7.1 Mobile Computing & Teleworking – Controls

10. OCIO – Information Security Policy 11.1.6 Regulation of Cryptographic Controls

4. INFORMATION AT REST	**Effective: 2015-05-28** **Reviewed: 2015-05-28**
4.8 OS X Full Disk Encryption	**Changed: 2015-05-28**

Purpose

This standard specifies the configuration to be used for protect information residing on Apple Mac computers.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure and better positioned to meet future business needs.

Context

The ability to protect information stored on computer hard drives depends on controls provided by the operating system. In some circumstances, operating systems controls can be bypassed leaving the information on the hard disk vulnerable to disclosure. This raises the need for an additional means of information protection. Whole disk encryption provides this protection. It is the best defense against unauthorized disclosure in the event a computer is lost or stolen.

Whole disk encryption depends on a password and secret key. If the user-password is forgotten or the secret key becomes corrupted the information on the disk may be unrecoverable. Thus, it is necessary to ensure the information on an encrypted disk is recoverable, independent of the end user.

To protect information, cryptographic keys must be managed securely throughout their lifetime. The typical events in the lifecycle of a cryptographic key include (but are not limited to): generation, distribution, storage, access (e.g. backup, archive, recovery) and destruction.

This standard is not mandatory for stationary OS X computers located in secure facilities.

Standard

Part 1 of 2: Encryption

Objective: To protect the information on a lost or stolen device from unauthorized exposure.

1. OSX versions below release 10.7 SHOULD be upgraded to 10.7 or above.
2. Hard disks under the control of OSX 10.7 or above MUST be encrypted.
3. The disk encryption algorithm used MUST be XTS-AES-128 (per: NIST 800-38E).

(Continued…)

Part 2 of 2: Institutional recovery

Objective: To provide the Province with the ability to recover encrypted information.

1. Encrypted drive contents MUST be recoverable independently of the end-user.
2. A recovery key (or master password or equivalent) MUST be kept in escrow.
3. Escrowed keys MUST reside on infrastructure controlled by the Province of BC.
4. Access to escrowed keys MUST be recorded in an audit trail.

Additional Guidance

- Apple's FileVault 2 meets the requirements of this standard.

References

OCIO – Information Security Policy 5.2.5 Equipment security controls
OCIO – Information Security Policy 6.7.1 Portable storage devices – mandatory controls
OCIO – Information Security Policy 6.7.3 Media handling procedures
OCIO – Information Security Policy 11.1.6 Regulation of cryptographic controls

NIST 800-38E: Recommendation for Block Cipher Modes of Operation:
The XTS-AES Mode for Confidentiality on Storage Devices
http://csrc.nist.gov/publications/nistpubs/800-38E/nist-sp-800-38E.pdf

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

5. MESSAGING	**Effective: 2009-01-14** **Reviewed: 2014-08-19**
5.1 Email	**Changed: 2009-01-14**

Purpose

This standard specifies the security controls for the protection and authenticity of email messages.

The strategic aim of this standard is to support the Government's goals through improvements to our IM/IT security infrastructure. These improvements will help protect the privacy of citizens, make the infrastructure more secure, sustainable and better positioned to support the business needs of the future.

Context

Many routine government business matters are conducted through email messaging. These messages may contain sensitive information. It is important to know, with confidence, that the sender identity is authentic. Furthermore, it is important to protect these messages while in transit. Industry standards have been developed for the authenticity and protection of email messages.

This standard applies where there is a need to apply cryptographic controls to secure email messages.

The need for cryptographic controls is determined by a Security Threat and Risk Assessment or the business requirements or a Privacy Impact Assessment.

Standard

Where cryptographic controls are required they MUST be implemented as follows:

The authentication, integrity, non-repudiation of origin and confidentiality of email messages MUST be protected by an S/MIME version 3.1 or above based solution.

Secure email solution for government MUST be provided by Shared Services BC as a centrally managed government-wide solution.

The solution MUST seamlessly integrate with the government’s email messaging system, operating systems, and the government’s public key infrastructure.

Certificates for digital signature and encryption MUST be distinct.

Additional Guidance

- Client certificates must conform to section 2.1 of this standard: Multi-factor Authentication and to section 2.2: Issuance of User Certificates.

- SHOULD and MUST are defined in the section **NOTES TO USERS**.

References

OCIO – Information Security Policy 6.8.1 Electronic information exchange
OCIO – Information Security Policy 6.8.4 Exchanges of information – general requirements
OCIO – Information Security Policy 7.7.1 Mobile computing and teleworking – controls

IETF - S/MIME Version 3.1 Message Specification (RFC 3851)
http://www.ietf.org/rfc/rfc3851.txt

IETF - S/MIME Version 3.1 Certificate Handling (RFC 3850)
http://www.ietf.org/rfc/rfc3850.txt

IETF - X.509 Certificate Extension for Secure/Multipurpose Internet Mail Extensions (S/MIME) Capabilities (RFC 4262)
http://www.ietf.org/rfc/rfc4262.txt

IETF - Internet X.509 Public Key Infrastructure Certificate Management Protocols
http://tools.ietf.org/html/rfc4210

ITU-T - Recommendation X.509 The Directory: Public-key and Attribute Certificate Frameworks
http://www.itu.int/rec/T-REC-X.509

NIST - FIPS 197 Advanced Encryption Standard (AES)
http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf

APPENDICES

APPENDIX A: Compliance Schedule for Web Service SOAP Security

The following schedule has been developed in cooperation with the ministries, endorsed by the Architecture and Standards Review Board and approved by the government Chief Information Officer.

1) Shared service and inter-organizational[1] SOAP provider interfaces must be upgraded to comply with the standard and be released into production by December 10, 2010.

2) Shared service and inter-organizational SOAP consumer interfaces must be upgraded to comply with the standard no later than 12 months after the publication of the corresponding provider interface.

3) All new SOAP interfaces (provider and consumer[2]) to be released into production must comply with the standard starting from December 10, 2009.

4) Legacy SOAP interfaces (provider and consumer) not covered above should be brought into compliance on a best effort basis, unless they pose a security risk[3] or collide with an OCIO objective.

[1] The term "inter-organizational" includes ministry-to-ministry, ministry-to-agency, ministry-to-service provider, etc.

[2] This is Subject to the availability of provider interfaces.

[3] Interfaces that pose a security risk should be dealt with on a priority basis.

APPENDIX B: Compliance Schedule for Cryptographic Standards

The following schedule has been developed in cooperation with the ministries, endorsed by the Architecture and Standards Review Board and approved by the government Chief Information Officer.

Appendix B applies for all standards except Web Service SOAP Security. The compliance schedule for Web Service SOAP Security is covered in Appendix A.

For existing systems:
An existing system should be brought into compliance only if it poses an unacceptable security risk or if for some other reason non-compliance raises a tangible issue. Bringing existing systems into compliance simply for the sake of compliance is not advocated.

For new systems:
The standard should be factored in as a requirement for the procurement of new systems. Where a new system cannot reasonably be made compliant and if that does not pose an unacceptable security risk and does not collide with OCIO strategic objectives then an exception may be obtained through the Office of the Government Chief Information Officer.