Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Cryptography

Cryptographic fundamentals

Purpose of cryptography

The purpose of cryptography is to provide confidentiality, integrity, authentication and non-repudiation of data. Confidentiality protects data by making it unreadable to all but authorised users, integrity protects data from accidental or deliberate manipulation, authentication ensures that a person or entity is who they claim to be, and non-repudiation provides proof that a user performed an action and prevents them from denying that they did so.

Using encryption

Encryption of data at rest can be used to reduce the physical storage and handling requirements for ICT equipment and media while encryption of data in transit can be used to provide protection for sensitive or classified data communicated over public network infrastructure.

When organisations use encryption for data at rest, or data in transit, they are not reducing the sensitivity or classification of data. However, as the data is encrypted, the consequences of the encrypted data being accessed by an adversary is considered to be less. Therefore, physical storage and handling requirements applied to the encrypted data can be reduced. As the sensitivity or classification of the unencrypted data does not change, additional layers of encryption cannot be used to further lower physical and handling requirements.

Additional cryptographic requirements

These guidelines describe the general use of cryptography. The Australian Signals Directorate (ASD) may specify additional requirements in consumer guides for cryptographic equipment or encryption software once they have completed an ASD Cryptographic Evaluation (ACE). Such requirements supplement these guidelines and where conflicts occur take precedence.

International standards for cryptographic modules

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19790:2012, ***Information technology – Security techniques – Security requirements for cryptographic modules***, and ISO/IEC 24759:2017, ***Information technology – Security techniques – Test requirements for cryptographic modules***, are international standards for the design and validation of hardware and software cryptographic modules.

Federal Information Processing Standard (FIPS) 140-3, ***Security Requirements for Cryptographic Modules***, is a United States standard based upon ISO/IEC 19790:2012, ISO/IEC 24759:2017 and the National Institute of Standards and Technology (NIST) Special Publication (SP) 180-140 series.

Where a cryptographic module's functionality has been validated under FIPS 140-2, FIPS 140-3 or ISO/IEC 19790:2012, ASD can at its discretion reduce the scope of an ACE.

High Assurance Cryptographic Equipment

High Assurance Cryptographic Equipment (HACE) is used by organisations to protect highly classified data. HACE is designed to lower the physical storage and handling requirements of highly classified data using cryptography. Due to the sensitive nature of HACE, organisations must comply with all communications security and equipment-specific doctrine produced by the Australian Cyber Security Centre (ACSC).

Reducing physical storage and handling requirements

When encryption is applied to data it provides an additional layer of defence. Encryption does not change the sensitivity or classification of the data, but when encryption is used, the physical storage and handling requirements of ICT equipment and media may be reduced.

Security Control: 1161; Revision: 5; Updated: Jun-21; Applicability: O
Encryption software that implements an ASD Approved Cryptographic Algorithm (AACA) is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains sensitive data.

Security Control: 0457; Revision: 6; Updated: Jun-21; Applicability: P
Encryption software that has completed an ACE is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains classified data.

Security Control: 0460; Revision: 9; Updated: Jun-21; Applicability: S, TS
HACE is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains highly classified data.

Encrypting data at rest

Full disk encryption provides a greater level of protection than file-based encryption. While file-based encryption may encrypt individual files, there is the possibility that unencrypted copies of files may be left in temporary locations used by an operating system.

Security Control: 0459; Revision: 3; Updated: Sep-18; Applicability: O, P
Encryption software used for data at rest implements full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition.

Security Control: 0461; Revision: 5; Updated: Sep-18; Applicability: S, TS
HACE used for data at rest implements full disk encryption, or partial encryption where access controls will only allow writing to the encrypted partition.

Encrypting particularly important data at rest

Due to the sensitivities associated with Australian Eyes Only (AUSTEO) and Australian Government Access Only (AGAO) data, it needs to be encrypted when at rest.

Security Control: 1080; Revision: 3; Updated: Jun-21; Applicability: S, TS
In addition to any encryption already in place, an AACA is used to encrypt AUSTEO and AGAO data when at rest on a system.

Data recovery

The requirement for cryptographic equipment and encryption software to provide a key escrow function, where practical, was issued under a cabinet directive in July 1998.

Security Control: 0455; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Where practical, cryptographic equipment and encryption software provides a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.

Handling encrypted ICT equipment and media

When a user authenticates to encryption functionality for ICT equipment or media storing encrypted data, the encrypted data becomes accessible. At such a time, the ICT equipment or media should be handled according to its original sensitivity or classification. Once the user deauthenticates from encryption functionality (e.g. shuts down a device, activates a lock screen) the ICT equipment or media can return to potentially being handled at a lower level.

Security Control: 0462; Revision: 6; Updated: Jun-21; Applicability: O, P, S, TS
When a user authenticates to encryption functionality for ICT equipment or media storing encrypted data, it is treated in accordance with its original sensitivity or classification until such a time that the user deauthenticates from the encryption functionality.

Encrypting data in transit

Where insufficient physical security is provided for the protection of data communicated over network infrastructure or via wireless networks, encryption can be used to assist in protecting such data from compromise.

Security Control: 1162; Revision: 4; Updated: Jun-21; Applicability: O
Cryptographic equipment or encryption software that implements an ASD Approved Cryptographic Protocol (AACP) is used to communicate sensitive data over public network infrastructure and through unsecured spaces.

Security Control: 0465; Revision: 7; Updated: Jun-21; Applicability: P
Cryptographic equipment or encryption software that has completed an ACE is used to communicate classified data over official networks, public network infrastructure and through unsecured spaces.

Security Control: 0467; Revision: 9; Updated: Jun-21; Applicability: S, TS
HACE is used to communicate highly classified data over networks of a lower classification, official networks, public network infrastructure and through unsecured spaces.

Encrypting particularly important data in transit

Due to the sensitivities associated with AUSTEO and AGAO data, it needs to be encrypted when being communicated across network infrastructure.

Security Control: 0469; Revision: 4; Updated: Jun-21; Applicability: S, TS
In addition to any encryption already in place, an AACP is used to protect AUSTEO and AGAO data when communicated across network infrastructure.

Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the ***Guidelines for Evaluated Products***.

Further information on the storage and transfer of ICT equipment and media can be found in the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF), ***Physical security for entity resources*** policy, at https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/Pages/default.aspx.

Further information on the ACE program is available at https://www.cyber.gov.au/acsc/view-all-content/programs/asd-cryptographic-evaluation-program.

Further information on international standards for cryptographic modules and their evaluation can be found in:

- ISO/IEC 19790:2012, ***Information technology – Security techniques – Security requirements for cryptographic modules***, at https://www.iso.org/standard/52906.html
- ISO/IEC 24759:2017, ***Information technology – Security techniques – Test requirements for cryptographic modules***, at https://www.iso.org/standard/72515.html
- FIPS 140-3, ***Security Requirements for Cryptographic Modules***, at https://csrc.nist.gov/publications/detail/fips/140/3/final
- NIST SP 800-140, ***FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759***, at https://csrc.nist.gov/publications/detail/sp/800-140/final.

ASD Approved Cryptographic Algorithms

Evaluated cryptographic implementations

Implementations of the algorithms in this section need to undergo an ACE before they can be approved to protect classified data.

High assurance cryptographic algorithms

High assurance cryptographic algorithms, which are not covered in this section, can be used for the protection of highly classified data if they are suitably implemented in HACE. Further information on high assurance cryptographic algorithms can be obtained from the ACSC.

ASD Approved Cryptographic Algorithms

There is no guarantee of an algorithm's resistance against currently unknown attacks. However, the algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting and have not been found to be susceptible to any feasible attacks. There have been some cases where theoretically impressive security vulnerabilities have been found; however, these results are not of practical application.

AACAs fall into three categories: asymmetric/public key algorithms, hashing algorithms and symmetric encryption algorithms.

The approved asymmetric/public key algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys
- Digital Signature Algorithm (DSA) for digital signatures
- Elliptic Curve Diffie-Hellman (ECDH) for key exchange
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures
- Rivest-Shamir-Adleman (RSA) for digital signatures and passing encryption session keys or similar keys.

The approved hashing algorithm is Secure Hashing Algorithm 2 (SHA-2) (i.e. SHA-224, SHA-256, SHA-384 and SHA-512).

The approved symmetric encryption algorithms are Advanced Encryption Standard (AES) using key lengths of 128, 192 and 256 bits, and Triple Data Encryption Standard (3DES) using three distinct keys.

Where there is a range of key sizes for an algorithm, some of the smaller key sizes are not approved as they do not provide an adequate safety margin against possible future attacks. For example, advances in integer factorisation methods could render smaller RSA moduli vulnerable.

Using ASD Approved Cryptographic Algorithms

If cryptographic equipment or software implements unapproved algorithms, as well as AACAs, it is possible that these unapproved algorithms could be used without a user's knowledge. In combination with an assumed level of security confidence, this can represent a security risk. As such, organisations can ensure that only the AACA can be used by disabling the unapproved algorithms (which is preferred) or advising users not to use the unapproved algorithms via usage policies.

Security Control: 0471; Revision: 6; Updated: Jun-20; Applicability: O, P
Only AACAs are used by cryptographic equipment and software.

Approved asymmetric/public key algorithms

DH and DSA are vulnerable to different attacks than ECDH and ECDSA. As a result, ECDH and ECDSA offer more effective security per bit increase. This leads to smaller data requirements which in turn means that elliptic curve variants have become de facto global standards. For reduced data cost, and to promote interoperability, ECDH and ECDSA should be used when possible.

Security Control: 0994; Revision: 5; Updated: Sep-18; Applicability: O, P
ECDH and ECDSA are used in preference to DH and DSA.

Using Diffie-Hellman

A modulus of 2048 bits for correctly implemented DH provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

When DH in a prime field is used, the prime modulus impacts the security of the algorithm. The security considerations when creating such a prime modulus can be found in NIST SP 800-56A Rev. 3, along with a collection of commonly used secure moduli.

Security Control: 0472; Revision: 5; Updated: Dec-20; Applicability: O, P
When using DH for agreeing on encryption session keys, a modulus of at least 2048 bits is used.

Security Control: 1629; Revision: 0; Updated: Dec-20; Applicability: O, P
When using DH for agreeing on encryption session keys, a modulus and associated parameters are selected according to NIST SP 800-56A Rev. 3.

Using the Digital Signature Algorithm

A modulus of 2048 bits for correctly implemented DSA provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

Security Control: 0473; Revision: 5; Updated: Dec-20; Applicability: O, P
When using DSA for digital signatures, a modulus of at least 2048 bits is used.

Security Control: 1630; Revision: 0; Updated: Dec-20; Applicability: O, P
When using DSA for digital signatures, a modulus and associated parameters are generated according to FIPS 186-4.

Using Elliptic Curve Cryptography

The curve used within an elliptic curve algorithm impacts the security of the algorithm. Only approved curves should be used.

Security Control: 1446; Revision: 1; Updated: Sep-18; Applicability: O, P
When using elliptic curve cryptography, a curve from FIPS 186-4 is used.

Using Elliptic Curve Diffie-Hellman

When using a curve from FIPS 186-4, a base point order and key size of at least 224 bits for correctly implemented ECDH provides 112 bits of effective security strength. Security of a curve selected from another source cannot be assumed to have the same security using base point order and key size alone.

Security Control: 0474; Revision: 5; Updated: Dec-20; Applicability: O, P
When using ECDH for agreeing on encryption session keys, a base point order and key size of at least 224 bits is used.

Using the Elliptic Curve Digital Signature Algorithm

When using a curve from FIPS 186-4, a base point order and key size of 224 bits for correctly implemented ECDSA provides 112 bits of effective security strength. Security of a curve selected from another source cannot be assumed to have the same security using base point order and key size alone.

Security Control: 0475; Revision: 5; Updated: Dec-20; Applicability: O, P
When using ECDSA for digital signatures, a base point order and key size of at least 224 bits is used.

Using Rivest-Shamir-Adleman

A modulus of 2048 bits for correctly implemented RSA provides 112 bits of effective security strength. Taking into account projected technological advances, it is assessed that 112 bits of effective security strength will remain secure until 2030.

Security Control: 0476; Revision: 6; Updated: Dec-20; Applicability: O, P
When using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 2048 bits is used.

Security Control: 0477; Revision: 6; Updated: Sep-18; Applicability: O, P
When using RSA for digital signatures, and for passing encryption session keys or similar keys, a key pair for passing encrypted session keys that is different from the key pair used for digital signatures is used.

Approved symmetric encryption algorithms

The use of Electronic Codebook Mode with block ciphers allows repeated patterns in plaintext to appear as repeated patterns in ciphertext. Most plaintext, including written language and formatted files, contains significant repeated patterns. As such, an adversary can use this to deduce possible meanings of ciphertext. The use of other modes such as Galois/Counter Mode, Cipher Block Chaining, Cipher Feedback or Output Feedback can prevent such attacks, although each has different properties which can make them inappropriate for certain use cases.

Security Control: 0479; Revision: 4; Updated: Sep-18; Applicability: O, P
Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.

Using the Triple Data Encryption Standard

Using three distinct keys for 3DES is deemed the only secure option for practical purposes. All other keying options are susceptible to attacks that reduce the security of 3DES and are therefore not deemed secure. Where practical, organisations should use an approved implementation of AES, instead of 3DES.

Security Control: 0480; Revision: 6; Updated: Sep-18; Applicability: O, P
3DES is used with three distinct keys.

Protecting highly classified data

ASD has approved the following cryptographic algorithms for the protection of highly classified data when used in an evaluated implementation.

Recommended algorithms and key sizes should be given preference in order to ensure interoperability with the Commercial National Security Algorithm (CNSA) Suite.

Purpose	Algorithm	Approved for SECRET	Approved for TOP SECRET	Recommended
Encryption	AES	AES-128 AES-192 AES-256	AES-256	AES-256
Hashing	SHA-2	SHA-256 SHA-384 SHA-512	SHA-384 SHA-512	SHA-384
Digital signatures	ECDSA	NIST P-256 NIST P-384 NIST P-521	NIST P-384 NIST P-521	NIST P-384
	RSA	3072 bit key or larger	3072 bit key or larger	3072 bit key
Key exchange	DH	3072 bit key or larger	3072 bit key or larger	3072 bit key
	ECDH	NIST P-256 NIST P-384 NIST P-521	NIST P-384 NIST P-521	NIST P-384
	RSA	3072 bit key or larger	3072 bit key or larger	3072 bit key

Security Control: 1232; Revision: 5; Updated: May-19; Applicability: S, TS
AACAs are used in an evaluated implementation.

Security Control: 1468; Revision: 5; Updated: Oct-19; Applicability: S, TS
Preference is given to using the CNSA Suite algorithms and key sizes.

Further information

Further information on selecting evaluated products can be found in the evaluated product acquisition section of the ***Guidelines for Evaluated Products***.

Further information on DH can be found in Diffie, W and Hellman, ME, ***New Directions in Cryptography***, IEEE Transactions on Information Theory, vol. 22, is. 6, pp. 644-654, November 1976.

Further information on DSA can be found in FIPS 186-4, ***Digital Signature Standard (DSS)***, at https://csrc.nist.gov/publications/detail/fips/186/4/final.

Further information on ECDH can be found in:

- American National Standards Institute (ANSI) X9.63-2011 (R2017), ***Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography***, at https://infostore.saiglobal.com/en-au/Standards/ANSI-X9-63-2011-R2017--2086_SAIG_ABA_ABA_5343/
- ANSI X9.42-2003 (R2013), ***Public Key Cryptography for the Financial Services Industry, Agreement of Symmetric Keys Using Discrete Logarithm Cryptography***, at https://infostore.saiglobal.com/en-au/Standards/ANSI-X9-42-2003-R2013--2071_SAIG_ABA_ABA_5311/
- NIST SP 800-56A Rev. 3, ***Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography***, at https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final.

Further information on ECDSA can be found in:

- ANSI X9.63-2011 (R2017), ***Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography***, at https://infostore.saiglobal.com/en-au/Standards/ANSI-X9-63-2011-R2017--2086_SAIG_ABA_ABA_5343/
- ANSI X9.62-2005, ***Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)***, at https://infostore.saiglobal.com/en-au/Standards/ANSI-X9-62-2005-2085_SAIG_ABA_ABA_5340/
- FIPS 186-4, ***Digital Signature Standard (DSS)***, at https://csrc.nist.gov/publications/detail/fips/186/4/final.

Further information on the CNSA Suite can be found in the ***CNSA Suite and Quantum Computing FAQ*** at https://apps.nsa.gov/iaarchive/library/ia-guidance/ia-solutions-for-classified/algorithm-guidance/cnsa-suite-and-quantum-computing-faq.cfm.

Further information on RSA can be found in Internet Engineering Task Force (IETF) Request for Comments (RFC) 8017, ***PKCS #1: RSA Cryptography Specifications Version 2.2***, at https://tools.ietf.org/html/rfc8017.

Further information on SHA can be found in FIPS 180-4, ***Secure Hash Standard (SHS)***, at https://csrc.nist.gov/publications/detail/fips/180/4/final.

Further information on AES can be found in FIPS 197, ***Advanced Encryption Standard (AES)***, at https://csrc.nist.gov/publications/detail/fips/197/final.

ASD Approved Cryptographic Protocols

Evaluated cryptographic implementations

Implementations of the protocols in this section need to undergo an ACE before they can be approved to protect classified data.

High assurance cryptographic protocols

High assurance cryptographic protocols, which are not covered in this section, can be used for the protection of highly classified data if they are suitably implemented in HACE. Further information on high assurance cryptographic protocols can be obtained from the ACSC.

ASD Approved Cryptographic Protocols

In general, ASD only approves the use of cryptographic equipment and software that has passed a formal evaluation. However, ASD approves the use of some cryptographic protocols even though their implementations in specific

cryptographic equipment or software has not been formally evaluated by ASD. This approval is limited to cases where they are used in accordance with these guidelines.

The AACPs are:

- Transport Layer Security (TLS)
- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extension (S/MIME)
- OpenPGP Message Format
- Internet Protocol Security (IPsec)
- Wi-Fi Protected Access 2 (WPA2).

Using ASD Approved Cryptographic Protocols

If cryptographic equipment or software implements unapproved protocols, as well as AACPs, it is possible that these unapproved protocols could be used without a user's knowledge. In combination with an assumed level of security confidence, this can represent a security risk. As such, organisations can ensure that only AACPs can be used by disabling unapproved protocols (which is preferred) or advising users not to use unapproved protocols via usage policies.

Security Control: 0481; Revision: 5; Updated: Jun-20; Applicability: O, P
Only AACPs are used by cryptographic equipment and software.

Further information

Further information on AACPs can be found in the found in the following sections of these guidelines.

Further information on the use of WPA2 in wireless networks can be found in the wireless networks section of the ***Guidelines for Networking***.

Further information on the OpenPGP Message Format can be found in IETF RFC 3156, ***MIME Security with OpenPGP***, at https://tools.ietf.org/html/rfc3156.

Transport Layer Security

Definitions

The terms Secure Sockets Layer (SSL) and TLS have traditionally been used interchangeably. However, as SSL 3.0 is no longer an AACP, instances of 'SSL' refer to SSL version 3.0 and below while 'TLS' refers to TLS 1.0 and beyond.

Using Transport Layer Security

The latest version of TLS is version 1.3, which was released in August 2018.

When using ICT equipment or software that implements TLS, security controls for using AACPs also need to be consulted in the ASD Approved Cryptographic Protocols section of these guidelines.

Security Control: 1139; Revision: 5; Updated: Oct-19; Applicability: O, P, S, TS
Only the latest version of TLS is used.

Security Control: 1369; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
AES in Galois Counter Mode is used for symmetric encryption.

Security Control: 1370; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS

Only server-initiated secure renegotiation is used.

Security Control: 1372; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
DH or ECDH is used for key establishment.

Security Control: 1448; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
When using DH or ECDH for key establishment, the ephemeral variant is used.

Security Control: 1373; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Anonymous DH is not used.

Security Control: 1374; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
SHA-2-based certificates are used.

Security Control: 1375; Revision: 3; Updated: Oct-19; Applicability: O, P, S, TS
Cipher suites are configured to use SHA-2 as part of the Message Authentication Code and Pseudo-Random Function.

Security Control: 1553; Revision: 0; Updated: Oct-19; Applicability: O, P, S, TS
TLS compression is disabled.

Perfect Forward Secrecy

Using Perfect Forward Secrecy (PFS) reduces the impact of the compromise of a TLS session.

Security Control: 1453; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
PFS is used for TLS connections.

Further information

Further information on handling TLS traffic through gateways can be found in the web content filters section of the ***Guidelines for Gateways***.

Further information on the implementation of TLS for websites can be found in in the ACSC's ***Implementing Certificates, TLS and HTTPS*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-certificates-tls-and-https.

Further information on TLS can be found in IETF RFC 8446 and its related updates:

- IETF RFC 8446, ***The Transport Layer Security (TLS) Protocol Version 1.3***, at https://tools.ietf.org/html/rfc8446
- IETF RFC 5705, ***Keying Material Exporters for Transport Layer Security (TLS)***, at https://tools.ietf.org/html/rfc5705
- IETF RFC 6066, ***Transport Layer Security (TLS) Extensions: Extension Definitions***, at https://tools.ietf.org/html/rfc6066.

Secure Shell

Using Secure Shell

When using ICT equipment or software that implements SSH, security controls for using AACPs also need to be consulted in the ASD Approved Cryptographic Protocols section of these guidelines.

Configuring Secure Shell

SSH version 1 was found to have a number of security vulnerabilities. As such, it was replaced by SSH version 2. A number of security risks also exist when SSH is configured in an insecure manner. For example, forwarding connections and access privileges, using host-based authentication, and permitting system administrator logins. The configuration

settings below are based on OpenSSH. Organisations using other implementations of SSH should adapt these settings to suit their SSH implementation.

Security Control: 1506; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The use of SSH version 1 is disabled.

Security Control: 0484; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The configuration settings in the following table are implemented for the SSH daemon.

Configuration	*Description*
ListenAddress xxx.xxx.xxx.xxx	*On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces*
AllowTCPForwarding no	*Disable connection forwarding*
GatewayPorts no	*Disable gateway ports*
PermitRootLogin no	*Disable the ability to login directly as root*
HostbasedAuthentication no	*Disable host-based authentication*
IgnoreRhosts yes	*Disable rhosts-based authentication*
PermitEmptyPasswords no	*Do not allow empty passphrases*
Banner x	*Configure a suitable login banner*
LoginGraceTime xx	*Configure a login authentication timeout of no more than 60 seconds*
X11Forwarding no	*Disable X11 forwarding*

Authentication mechanisms

Public key-based authentication schemes offer stronger authentication than passphrase-based authentication schemes due to passphrases being more susceptible to guessing attacks. Therefore, if passphrases are used, counter-measures should be put in place to reduce the chance of a successful brute force attack.

Security Control: 0485; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Public key-based authentication is used for SSH connections.

Security Control: 1449; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
SSH private keys are protected with a passphrase or a key encryption key.

Automated remote access

If using logins without a passphrase for automated purposes, a number of security risks may arise, specifically:

- if access from unknown Internet Protocol (IP) addresses is not restricted, an adversary could automatically authenticate to systems without needing to know any passphrases

- if port forwarding is not disabled, or it is not configured securely, access may be gained to forwarded ports thereby creating a communication channel between an adversary and a host
- if agent credential forwarding is enabled, an adversary could connect to the stored authentication credentials and use them to connect to other trusted hosts, or even intranet hosts if port forwarding has been allowed as well
- if X11 display remoting is not disabled, an adversary could gain control of displays as well as keyboard and mouse control functions
- if console access is allowed, every user who logs into the console could run programs that are normally restricted to authenticated users.

To assist in mitigating these security risks, it is essential that the 'forced command' option is used to specify what command is executed and parameter checked is enabled.

Security Control: 0487; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When using logins without a passphrase for automated purposes, the following are disabled:

- *access from IP addresses that do not require access*
- *port forwarding*
- *agent credential forwarding*
- *X11 display remoting*
- *console access.*

Security Control: 0488; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
If using remote access without the use of a passphrase, the 'forced command' option is used to specify what command is executed and parameter checked is enabled.

SSH-agent

SSH-agent or other similar key caching programs hold and manage private keys stored on workstations and respond to requests from remote systems to verify these keys. When an SSH-agent launches, it requests the user's passphrase to unlock the user's private key. Subsequent access to remote systems is performed by the agent and does not require the user to re-enter their passphrase. Screen locks and expiring key caches ensure that the user's private key is not left unlocked for a long period of time. Furthermore, to limit the exposure of credentials, agent credential forwarding should only be enabled when SSH traversal is required.

Security Control: 0489; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
When SSH-agent or other similar key caching programs are used, it is only on workstations and servers with screen locks, key caches are set to expire within four hours of inactivity, and agent credential forwarding is enabled only when SSH traversal is required.

Further information

Further information on SSH can be found in IETF RFC 4252 and its updates:

- IETF RFC 4252, ***The Secure Shell (SSH) Authentication Protocol***, at https://tools.ietf.org/html/rfc4252
- IETF RFC 8308, ***Extension Negotiation in the Secure Shell (SSH) Protocol***, at https://tools.ietf.org/html/rfc8308
- IETF RFC 8332, ***Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol***, at https://tools.ietf.org/html/rfc8332.

Further information on configuring OpenSSH can be found at https://www.openssh.com/manual.html and https://man.openbsd.org/sshd_config.

Secure/Multipurpose Internet Mail Extension

Using Secure/Multipurpose Internet Mail Extension

S/MIME 2.0 required the use of weaker cryptography (40-bit keys) than is approved for use in these guidelines. Version 3.0 was the first version to become an IETF standard.

Organisations choosing to implement S/MIME should be aware of the inability of many content filters to inspect encrypted messages and attachments for inappropriate content, and for server-based antivirus software to scan for viruses and other malicious code.

When using ICT equipment or software that implements S/MIME, security controls for using AACPs also need to be consulted in the ASD Approved Cryptographic Protocols section of these guidelines.

Security Control: 0490; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Versions of S/MIME earlier than 3.0 are not used.

Further information

Further information on S/MIME can be found in IETF RFC 8551, ***Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification***, at https://tools.ietf.org/html/rfc8551.

Internet Protocol Security

Using Internet Protocol Security

When using ICT equipment or software that implements IPsec, security controls for using AACPs also need to be consulted in the ASD Approved Cryptographic Protocols section of these guidelines.

Internet Security Association Key Management Protocol authentication

Most IPsec implementations handle a number of methods for authentication as part of Internet Security Association Key Management Protocol (ISAKMP). These can include digital certificates, encrypted nonces or pre-shared keys. These methods are all considered suitable for use.

Mode of operation

IPsec can be operated in transport mode or tunnel mode. The tunnel mode of operation provides full encapsulation of IP packets while the transport mode of operation only encapsulates the payload of the IP packet.

Security Control: 0494; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Tunnel mode is used for IPsec connections; however, if using transport mode, an IP tunnel is used.

Protocol selection

IPsec contains two major protocols, Authentication Header (AH) and Encapsulating Security Payload (ESP). In order to provide a secure Virtual Private Network style connection, both authentication and encryption are needed. AH and ESP can provide authentication for the entire IP packet and the payload respectively. However, ESP is generally preferred for authentication since AH by its nature has network address translation limitations. However, if maximum security is desired at the expense of network address translation functionality, then ESP can be wrapped inside of AH, which will then authenticate the entire IP packet and not just the encrypted payload.

Security Control: 0496; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The ESP protocol is used for IPsec connections.

Key exchange

There are several methods for establishing shared keying material for an IPsec connection, including manual keying and Internet Key Exchange (IKE) version 1 and 2. IKE addresses a number of security risks associated with manual keying, and for this reason is the preferred method for key establishment.

Security Control: 1233; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
IKE is used for key exchange when establishing an IPsec connection.

Internet Security Association Key Management Protocol modes

ISAKMP main mode provides greater security than aggressive mode since all exchanges are protected.

Security Control: 0497; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
If using ISAKMP in IKE version 1, aggressive mode is disabled.

Security association lifetimes

Using a secure association lifetime of four hours, or 14400 seconds, provides a balance between security and usability.

Security Control: 0498; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
A security association lifetime of less than four hours, or 14400 seconds, is used.

Hashed Message Authentication Code algorithms

The approved Hashed Message Authentication Code (HMAC) algorithms are HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512.

Security Control: 0998; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
HMAC-SHA256, HMAC-SHA384 or HMAC-SHA512 is used as a HMAC algorithm.

Diffie-Hellman groups

Using a larger DH group provides more security for the key exchange. The minimum modulus size needed is specified in the ASD Approved Cryptographic Algorithms section of these guidelines.

Security Control: 0999; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
The largest modulus size possible for all relevant components in the network is used when conducting a key exchange.

Perfect Forward Secrecy

Using PFS reduces the impact of the compromise of a security association.

Security Control: 1000; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
PFS is used for IPsec connections.

Internet Key Exchange Extended Authentication

XAuth using IKE version 1 has documented security vulnerabilities associated with its use.

Security Control: 1001; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
The use of XAuth is disabled for IPsec connections using IKE version 1.

Further information

Further information on IPsec can be found in IETF RFC 4301 and its updates:

- IETF RFC 4301, ***Security Architecture for the Internet Protocol***, at https://tools.ietf.org/html/rfc4301
- IETF RFC 6040, ***Tunnelling of Explicit Congestion Notification***, at https://tools.ietf.org/html/rfc6040
- IETF RFC 7619, ***The NULL Authentication Method in the Internet Key Exchange Protocol Version 2 (IKEv2)***, at https://tools.ietf.org/html/rfc7619.

Cryptographic system management

Cryptographic systems

Cryptographic systems are comprised of cryptographic equipment and keying material. Where security controls for cryptographic systems are different to other systems, the variations are contained in this section.

Commercial grade cryptographic equipment

Transporting Commercial Grade Cryptographic Equipment (CGCE) in a keyed state may expose the keying material in it to potential compromise. Therefore, if CGCE is transported in a keyed state it should be done based on the sensitivity or classification of the keying material in it.

If CGCE or associated keying material is compromised or suspected of being compromised (e.g. stolen, lost, copied or communicated over the internet) then the confidentiality and integrity of previous and future communications may also be compromised.

Security Control: 0501; Revision: 4; Updated: Sep-18; Applicability: O, P
Keyed CGCE is transported based on the sensitivity or classification of the keying material in it.

Security Control: 0142; Revision: 3; Updated: Jun-19; Applicability: O, P
The compromise or suspected compromise of CGCE or associated keying material is reported to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after it occurs.

Security Control: 1091; Revision: 5; Updated: Jun-19; Applicability: O, P
Keying material is changed when compromised or suspected of being compromised.

High Assurance Cryptographic Equipment

HACE can be used by organisations to protect highly classified data. Organisations using HACE must comply with all communications security and equipment-specific doctrine produced by the ACSC for the management and use of HACE.

Security Control: 0499; Revision: 9; Updated: Jun-21; Applicability: S, TS
All communications security and equipment-specific doctrine produced by the ACSC for the management and use of HACE is complied with.

Storing cryptographic equipment

As cryptographic equipment can protect sensitive or classified data, additional physical security controls should be applied to its storage.

Security Control: 0505; Revision: 6; Updated: Jun-21; Applicability: O, P, S, TS
Cryptographic equipment is stored in a room that meets the requirements for a server room based on the sensitivity or classification of the data the cryptographic equipment processes.

Security Control: 0506; Revision: 3; Updated: Sep-18; Applicability: S, TS
Areas in which HACE is used are separated from other areas and designated as a cryptographic controlled area.

Further information

Further information on Security Zones and secure rooms can be found in AGD's PSPF, ***Entity facilities*** policy, at https://www.protectivesecurity.gov.au/physical/entity-facilities/Pages/default.aspx.