Guidelines for using cryptography

Cryptographic fundamentals

Purpose of cryptography

The purpose of cryptography is to provide confidentiality, integrity, authentication and non-repudiation of information. Confidentiality protects information by making it unreadable to all but authorised users, integrity protects information 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 information 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 information. However, as the information is encrypted, the consequences of the encrypted information being accessed by an adversary is considered to be less. Therefore, physical storage and handling requirements applied to the encrypted information can be reduced. As the sensitivity or classification of the unencrypted information does not change, additional layers of encryption cannot be used to further lower physical and handling requirements.

Additional cryptographic requirements

This document describes the general use of cryptography. Additional requirements can exist in consumer guides for cryptographic equipment or encryption software once they have completed an Australian Signals Directorate (ASD) Cryptographic Evaluation (ACE). Such requirements supplement this document and where conflicts occur take precedence.

Federal Information Processing Standard 140

The Federal Information Processing Standard (FIPS) 140 is a United States standard for the validation of both hardware and software cryptographic modules. FIPS 140 is in its second iteration and is formally referred to as FIPS 140-2. This document refers to the standard as FIPS 140, but it applies equally to FIPS 140-1, FIPS 140-2 and FIPS 140-3, which had been released in draft but has since been abandoned.
FIPS 140 is not a substitute for an ACE as it is concerned solely with the cryptographic functionality of a module and does not consider any other security functionality. Where a module’s cryptographic functionality has been validated under FIPS 140, ASD can at its discretion, and in consultation with the vendor, reduce the scope of an ACE.

**High assurance cryptographic equipment**

High assurance cryptographic equipment (HACE) is used by organisations to protect highly classified information. HACE is designed to lower the physical storage and handling requirements of highly classified information using cryptography. Due to the sensitive nature of HACE, and the limited information publicly available on it, organisations must contact the Australian Cyber Security Centre (ACSC) before using it.

**Reducing physical storage and handling requirements**

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

*Security Control: 1161; Revision: 4; Updated: Sep-18; Applicability: O; Priority: Must*

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 information.

*Security Control: 0457; Revision: 5; Updated: Sep-18; Applicability: P; Priority: Must*

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 information.

*Security Control: 0460; Revision: 8; Updated: Sep-18; Applicability: S, TS; Priority: Must*

HACE is used if an organisation wishes to reduce the physical storage or handling requirements for ICT equipment or media that contains highly classified information.

**Encrypting information 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; Priority: Should*

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; Priority: Must*

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 information at rest**

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

*Security Control: 1080; Revision: 2; Updated: Sep-18; Applicability: S, TS; Priority: Must*

In addition to any encryption already in place, an AACA is used to encrypt AUSTEO and AGAO information 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; Priority: Must
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 information, the encrypted information becomes accessible. At such a time, the ICT equipment or media should be handled according to its original sensitivity or classification. Once the user deauthenticate 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: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
When a user authenticates to encryption functionality for ICT equipment or media storing encrypted information, it is treated in accordance with its original sensitivity or classification until such a time that the user deauthenticate from the encryption functionality.

Reducing network infrastructure requirements

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

Security Control: 1162; Revision: 3; Updated: Sep-18; Applicability: O; Priority: Must
Cryptographic equipment or encryption software that implements an ASD Approved Cryptographic Protocol (AACP) is used to communicate sensitive information over public network infrastructure and through unsecured spaces.

Security Control: 0465; Revision: 6; Updated: Sep-18; Applicability: P; Priority: Must
Cryptographic equipment or encryption software that has completed an ACE is used to communicate classified information over official networks, public network infrastructure and through unsecured spaces.

Security Control: 0467; Revision: 8; Updated: Sep-18; Applicability: S, TS; Priority: Must
HACE is used to communicate highly classified information over networks of a lower classification, official networks, public network infrastructure and through unsecured spaces.

Encrypting particularly important information in transit

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

Security Control: 0469; Revision: 3; Updated: Sep-18; Applicability: S, TS; Priority: Must
In addition to any encryption already in place, an AACP is used to protect AUSTEO and AGAO information 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 use of HACE can be found in Australian Communications Security Instructions (ACSIs). ACSIs include requirements for the approved use of HACE and can be provided to organisations by the ACSC upon request.
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/](https://www.protectivesecurity.gov.au/physical/physical-security-entity-resources/).

Further information on the FIPS 140 standards is available at [https://csrc.nist.gov/publications/detail/fips/140/2/final](https://csrc.nist.gov/publications/detail/fips/140/2/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 information.

**High assurance cryptographic algorithms**

High assurance cryptographic algorithms, which are not covered in this section, can be used for the protection of highly classified information if they are suitably implemented in cryptographic equipment that has undergone a high assurance evaluation by ASD. Further information on high assurance cryptographic algorithms can be obtained by contacting 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 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 configured without a user’s knowledge. In combination with an assumed level of security confidence, this can represent a security risk.
When configuring cryptographic equipment or software that implement an AACA, 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: 5; Updated: Sep-18; Applicability: O, P; Priority: Must
If using cryptographic equipment or software that implements an AACA, only AACAs can be used.

Approved asymmetric/public key algorithms

Over the last decade, DSA and DH cryptosystems have been subject to increasingly successful sub-exponential index-calculus-based attacks. ECDH and ECDSA offer more security per bit increase in key size than DH or DSA and are considered more secure alternatives.

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

Using Diffie-Hellman

A modulus of at least 2048 bits for DH is considered best practice by the cryptographic community. A modulus smaller than 1024 bits for DH is considered cryptographically weak.

Security Control: 0472; Revision: 4; Updated: Sep-18; Applicability: O, P; Priority: Must
When using DH for agreeing on encryption session keys, a modulus of at least 1024 bits, preferably 2048 bits, is used.

Using the Digital Signature Algorithm

A modulus of at least 2048 bits for DSA is considered best practice by the cryptographic community. A modulus smaller than 1024 bits for DSA is considered cryptographically weak.

Security Control: 0473; Revision: 4; Updated: Sep-18; Applicability: O, P; Priority: Must
When using DSA for digital signatures, a modulus of at least 1024 bits, preferably 2048 bits, is used.

Using Elliptic Curve Cryptography

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

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

Using Elliptic Curve Diffie-Hellman

A field/key size of at least 256 bits for ECDH is considered best practice by the cryptographic community. A field/key size smaller than 160 bits for ECDH is considered cryptographically weak.

Security Control: 0474; Revision: 4; Updated: Sep-18; Applicability: O, P; Priority: Must
When using ECDH for agreeing on encryption session keys, a field/key size of at least 160 bits, preferably 256 bits, is used.

Using the Elliptic Curve Digital Signature Algorithm

A field/key size of at least 256 bits for ECDSA is considered best practice by the cryptographic community. A field/key size smaller than 160 bits for ECDSA is considered cryptographically weak.

Security Control: 0475; Revision: 4; Updated: Sep-18; Applicability: O, P; Priority: Must
When using ECDSA for digital signatures, a field/key size of at least 160 bits, preferably 256 bits, is used.
Using Rivest-Shamir-Adleman

A modulus of at least 2048 bits for RSA is considered best practice by the cryptographic community. A modulus smaller than 1024 bits for RSA is considered cryptographically weak.

**Security Control: 0476; Revision: 5; Updated: Sep-18; Applicability: O, P; Priority: Must**
When using RSA for digital signatures, and passing encryption session keys or similar keys, a modulus of at least 1024 bits, preferably 2048 bits, is used.

**Security Control: 0477; Revision: 6; Updated: Sep-18; Applicability: O, P; Priority: Must**
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 hashing algorithms

Research conducted by the cryptographic community has shown Secure Hashing Algorithm 1 (SHA-1) is susceptible to collision attacks. In 2017, researchers demonstrated a SHA-1 collision with Portable Document Format (PDF) files. A hashing algorithm from the SHA-2 family should be used instead of SHA-1.

**Security Control: 1054; Revision: 4; Updated: Sep-18; Applicability: O, P; Priority: Must**
A hashing algorithm from the SHA-2 family is used instead of SHA-1.

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; Priority: Should**
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; Priority: Must**
3DES is used with three distinct keys.

Protecting highly classified information

ASD has approved the following cryptographic algorithms for the protection of highly classified information when used in an evaluated implementation. Recommended algorithms and key sizes should be given preference where possible for interoperability with the Commercial National Security Algorithm (CNSA) Suite.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Algorithm</th>
<th>Approved for SECRET</th>
<th>Approved for TOP SECRET</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>AES</td>
<td>AES-128</td>
<td>AES-256</td>
<td>AES-256</td>
</tr>
<tr>
<td>Hashing</td>
<td>SHA-2</td>
<td>SHA-256</td>
<td>SHA-384</td>
<td>SHA-384</td>
</tr>
<tr>
<td>----------</td>
<td>------------</td>
<td>--------------</td>
<td>--------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SHA-384</td>
<td>SHA-512</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Digital signatures</td>
<td>ECDSA</td>
<td>NIST P-256</td>
<td>NIST P-384</td>
<td>NIST P-384</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIST P-384</td>
<td>NIST P-521</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td>3072 bit key</td>
<td>3072 bit key</td>
<td>3072 bit key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or larger</td>
<td>or larger</td>
<td>or larger</td>
</tr>
<tr>
<td>Key exchange</td>
<td>DH</td>
<td>3072 bit key</td>
<td>3072 bit key</td>
<td>3072 bit key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or larger</td>
<td>or larger</td>
<td>or larger</td>
</tr>
<tr>
<td>ECDH</td>
<td></td>
<td>NIST P-256</td>
<td>NIST P-384</td>
<td>NIST P-384</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NIST P-384</td>
<td>NIST P-521</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RSA</td>
<td></td>
<td>3072 bit key</td>
<td>3072 bit key</td>
<td>3072 bit key</td>
</tr>
<tr>
<td></td>
<td></td>
<td>or larger</td>
<td>or larger</td>
<td>or larger</td>
</tr>
</tbody>
</table>

Further information on selecting evaluated products can be found in the [Evaluated product acquisition](#) section of the [Guidelines for evaluated products](#).


Further information on ECDH can be found in:


Further information on ECDSA can be found in:


**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 information.

**High assurance cryptographic protocols**

Protocols for HACE, which are not covered in this section, can be used for the protection of highly classified information if they are suitably implemented in cryptographic equipment that has undergone a high assurance evaluation by ASD. Further information on high assurance cryptographic protocols can be obtained by contacting 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 this document.

The AACP's 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 relatively weak protocols could be configured without a user’s knowledge. In combination with an assumed level of security confidence, this represents a security risk.

When configuring cryptographic equipment or software that implements an AACP, 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.

While many AACPs support authentication, organisations should be aware that these authentication mechanisms are not foolproof. To be effective, these mechanisms should also be securely implemented and protected. This can be achieved by providing appropriate private key protection, ensuring the correct management of certificate authentication processes, including certificate revocation checking, and using a legitimate identity registration scheme.

Security Control: 0481; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
If using cryptographic equipment or software that implements an AACP, only AACAs can be used.

Further information

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

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: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
The latest version of TLS is used.

Security Control: 1369; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
AES in Galois Counter Mode is used for symmetric encryption when available.

Security Control: 1370; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
A TLS implementation that supports secure renegotiation is used.

Security Control: 1371; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
If secure renegotiation is not available, renegotiation is disabled.

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

Security Control: 1448; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
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; Priority: Must
Anonymous DH is not used.

Security Control: 1374; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
SHA-2-based certificates are used where possible.

Security Control: 1375; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Cipher suites are configured to use SHA-2 as part of the Message Authentication Code and Pseudo-Random Function
where possible.

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; Priority: Should
PFS is used for TLS connections.

Further information

Further information on handling TLS traffic through gateways can be found in the Web content and connections
section of the Guidelines for gateway management.

Further information on TLS can be found in IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3,

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; Priority: Should
The use of SSH version 1 is disabled.

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

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ListenAddress xxx.xxx.xxx.xxx</td>
<td>On machines with multiple interfaces, configure the SSH daemon to listen only on the required interfaces</td>
</tr>
<tr>
<td>AllowTCPForwarding no</td>
<td>Disable connection forwarding</td>
</tr>
<tr>
<td>GatewayPorts no</td>
<td>Disable gateway ports</td>
</tr>
</tbody>
</table>

Further information on handling TLS traffic through gateways can be found in the Web content and connections
section of the Guidelines for gateway management.

Further information on TLS can be found in IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3,
<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PermitRootLogin no</td>
<td>Disable the ability to login directly as root</td>
</tr>
<tr>
<td>HostbasedAuthentication no</td>
<td>Disable host-based authentication</td>
</tr>
<tr>
<td>IgnoreRhosts yes</td>
<td>Disable rhosts-based authentication</td>
</tr>
<tr>
<td>PermitEmptyPasswords no</td>
<td>Do not allow empty passphrases</td>
</tr>
<tr>
<td>Banner x</td>
<td>Configure a suitable login banner</td>
</tr>
<tr>
<td>LoginGraceTime xx</td>
<td>Configure a login authentication timeout of no more than 60 seconds</td>
</tr>
<tr>
<td>X11Forwarding no</td>
<td>Disable X11 forwarding</td>
</tr>
</tbody>
</table>

### 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; Priority: Should**

Public key-based authentication is used for SSH connections.

**Security Control: 1449; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should**

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; Priority: Should**

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; Priority: Should

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; Priority: Should

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


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 this document. 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; Priority: Should

Versions of S/MIME earlier than 3.0 are not used.

Further information

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; Priority: Should
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 (VPN) 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; Priority: Must
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; Priority: Must
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; Priority: Should
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; Priority: Should
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; Priority: Must
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; Priority: Should
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; Priority: Should
PFS is used for IPsec connections.

Internet Key Exchange Extended Authentication

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

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

Further information


Cryptographic system management

Cryptographic systems

Cryptographic systems are comprised of cryptographic equipment and keying material. In general, security controls specified for systems in this document apply equally to cryptographic systems. However, where security controls for cryptographic systems are different, the variations are contained in this section and overrule security controls specified elsewhere in this document.

Compromise of keying material

If keying material is suspected at any time of being compromised (e.g. stolen, lost, copied or communicated over the Internet) then the confidentiality and integrity of previous and future communications encrypted with that keying material may also be compromised.

ACSI 107 B applies to all organisations including contractors. Its requirements cover HACE used to protect highly classified information. For cyber security incidents involving the suspected compromise of keying material used for HACE, the ACSC will investigate the possibility of compromise and, where possible, initiate action to reduce the impact of the compromise.
Security Control: 0142; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Communications security custodians are notified of any suspected compromise of keying material.

Security Control: 0143; Revision: 7; Updated: Sep-18; Applicability: S, TS; Priority: Must
The ACSC is notified of any suspected compromise of HACE or associated keying material.

Security Control: 1091; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must
Keying material is revoked when suspected of being compromised.

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.

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

High assurance cryptographic equipment

HACE can be used by organisations to protect highly classified information. ACSI 53 E, ACSI 103 A, ACSI 105 B, ACSI 107 B, ACSI 173 A and equipment-specific doctrine outline the requirements that need to be complied with for the use of HACE.

Security Control: 0499; Revision: 8; Updated: Apr-19; Applicability: S, TS; Priority: Must
ACSI 53 E, ACSI 103 A, ACSI 105 B, ACSI 107 B, ACSI 173 A and the latest equipment-specific doctrine is complied with when using HACE.

Storing cryptographic equipment

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

Security Control: 0505; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should
Cryptographic equipment is stored in a room that meets the requirements for a server room based on the sensitivity or classification of the information the cryptographic equipment processes.

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

Further information

Further information on the use of HACE can be found in associated ACSIs. ACSIs can be provided to organisations by the ACSC upon request.