Australian Government
Australian Signals Directorate

Information security manual

Guidelines for cryptography

Last updated: September 2026

Cryptographic fundamentals

Context

The purpose of cryptography is to provide confidentiality, integrity, authentication and non-repudiation of data. In doing so, confidentiality protects data by making it unreadable to all but authorised entities, integrity protects data from accidental or deliberate manipulation by entities, authentication ensures that an entity is who they claim to be, and non-repudiation provides proof that an entity performed a particular action.

In employing cryptography, data at rest can be encrypted to protect sensitive or classified data stored on information technology (IT) equipment and media. Similarly, data in transit can be encrypted to protect sensitive or classified data communicated over public network infrastructure. However, while cryptography can protect data at rest and in transit, it does not reduce the sensitivity or classification of the data; it only reduces the immediate consequences of the data being accessed by malicious actors.

Communications security doctrine

The Australian Signals Directorate (ASD) specifies additional communications security requirements in Australian Communications Security Instructions and ASD Broadcasts that must be complied with when operating High Assurance Cryptographic Equipment (HACE). Such requirements supplement these guidelines and, where conflicts occur, take precedence.

Control: ISM-0499; Revision: 12; Updated: Jun-25; Applicable: S, TS; Essential 8: N/A
Communications security doctrine and policy produced by ASD for the management and operation of HACE is complied with.

High Assurance Cryptographic Equipment

To ensure interoperability and maintain trust, all HACE must be issued an Approval for Use by ASD and be operated in accordance with the latest version of their associated Australian Communications Security Instructions.

Control: ISM-1802; Revision: 1; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A
HACE are issued an Approval for Use by ASD and operated in accordance with the latest version of their associated Australian Communications Security Instructions.

Cryptographic key management processes and procedures

Well-documented cryptographic key management processes and procedures can assist in the secure use and management of cryptographic keys and associated hardware and software. In doing so, cryptographic key management processes and procedures should cover cryptographic key generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.

Control: ISM-0507; Revision: 5; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Cryptographic key management processes, and supporting cryptographic key management procedures, are developed, implemented and maintained.

Cryptographic implementation assurance

Securely implementing cryptographic algorithms and protocols is a difficult task that requires expertise and diligence. In doing so, suppliers, and their cyber supply chains, need to carry out their duties competently and honestly as small flaws in cryptographic equipment, applications or libraries can be catastrophic and difficult to detect. Therefore, to provide a degree of cryptographic implementation assurance, cryptographic equipment, applications and libraries should be assessed by one of the following processes, listed in order of preference:

- a Common Criteria evaluation against an ASD-endorsed Protection Profile
- a Federal Information Processing Standard (FIPS) 140-3 cryptographic evaluation via the United States and Canada's Cryptographic Module Validation Program
- a cryptographic evaluation via the United States and Canada's Cryptographic Algorithm Validation Program
- a Common Criteria evaluation against an Evaluation Assurance Level
- an independent security review by a reputable process or body.

Where a suitable Common Criteria evaluated product does not exist, an alternate product capable of securely implementing ASD-Approved Cryptographic Algorithms (AACAs) and ASD-Approved Cryptographic Protocols (AACPs) may be used. However, cyber supply chain security risks still need to be considered to ensure the product does not present a high risk. For example, an organisation should still follow robust and secure procurement processes by selecting a product from a supplier with:

- a history of undertaking Common Criteria evaluations for their other products
- a demonstrated commitment to the security of their products and services, including by adopting Secure by Design principles and practices, responsively resolving known vulnerabilities, and providing clear end of life advice for consumers
- a demonstrated commitment to transparency for their products
- a strong track record of maintaining the security of their own systems
- sufficient information on how to securely configure their products.

Control: ISM-0457; Revision: 11; Updated: Sep-25; Applicable: OS, P; Essential 8: N/A
Cryptographic equipment, applications or libraries that have completed a Common Criteria evaluation against an ASD-endorsed Protection Profile are used when encrypting media that contains OFFICIAL: Sensitive or PROTECTED data.

Control: ISM-0460; Revision: 13; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A
HACE is used when encrypting media that contains SECRET or TOP SECRET data.

Control: ISM-0465; Revision: 11; Updated: Sep-25; Applicable: OS, P; Essential 8: N/A
Cryptographic equipment, applications or libraries that have completed a Common Criteria evaluation against an ASD-endorsed Protection Profile are used to protect OFFICIAL: Sensitive or PROTECTED data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.

Control: ISM-0467; Revision: 12; Updated: Sep-23; Applicable: S, TS; Essential 8: N/A
HACE is used to protect SECRET and TOP SECRET data when communicated over insufficiently secure networks, outside of appropriately secure areas or via public network infrastructure.

Data recovery

To ensure that access to encrypted data is not lost due to the loss, damage or failure of an encryption key, it is important that where practical cryptographic equipment, applications and libraries provide a means of data recovery.

Control: ISM-0455; Revision: 5; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Where practical, cryptographic equipment, applications and libraries provide a means of data recovery to allow for circumstances where the encryption key is unavailable due to loss, damage or failure.

Handling encrypted IT equipment and media

When a user authenticates to the encryption functionality of IT equipment or media, encrypted data is made available. At such a time, the IT equipment or media should be handled according to its original sensitivity or classification. Once the user deauthenticates from the encryption functionality, such as by locking encrypted media, shutting down a device or activating a lock screen, the IT equipment or media can be considered protected by the encryption functionality again.

Control: ISM-0462; Revision: 8; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When a user authenticates to the encryption functionality of IT equipment or media, it is treated in accordance with its original sensitivity or classification until the user deauthenticates from the encryption functionality.

Transporting cryptographic equipment

Transporting cryptographic equipment in a keyed state may expose its keying material to potential compromise. Therefore, if cryptographic equipment is transported in a keyed state, it should be done based on the sensitivity or classification of its keying material.

Control: ISM-0501; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Keyed cryptographic equipment is transported based on the sensitivity or classification of its keying material.

Reporting cryptographic-related cyber security incidents

If cryptographic equipment or associated keying material is compromised, or suspected of being compromised, then the confidentiality and integrity of previous and future communications may also be compromised. In such cases, the cyber security incident should be reported to the chief information security officer, or one of their delegates, as soon as possible after it occurs, and all keying material should be changed.

Control: ISM-0142; Revision: 5; Updated: Jun-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The compromise or suspected compromise of cryptographic equipment or associated keying material is reported to the chief information security officer, or one of their delegates, as soon as possible after it occurs.

Control: ISM-1091; Revision: 6; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Keying material is changed when compromised or suspected of being compromised.

Further information

Further information on the design and validation of hardware and software cryptographic modules can be found in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 19790:2025, *Information security, cybersecurity and privacy protection – Security requirements for cryptographic modules* and ISO/IEC 24759:2025, *Information security, cybersecurity and privacy protection – Test requirements for cryptographic modules*.

Further information on United States standards based upon earlier versions of ISO/IEC 19790 and ISO/IEC 24759 can be found in FIPS 140-3, *Security Requirements for Cryptographic Modules* and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-140, *FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759*.

Further information on cryptographic key management practices can be found in ASD's *Managing cryptographic keys and secrets* publication.

Further information on cryptographic key management practices for HACE is available from ASD.

Further information on general cryptographic key management practices can be found in NIST SP 800-57 Part 1 Rev. 5, *Recommendation for Key Management: Part 1 – General*.

Further information on cyber supply chain risk management can be found in the 'Cyber supply chain risk management' section of the *Guidelines for procurement and outsourcing*.

Further information on evaluated products can be found in the 'Evaluated product procurement' section of the *Guidelines for evaluated products*.

Further information on the evaluation of cryptographic modules, including testing requirements, is available as part of the Cryptographic Module Validation Program which is jointly operated by NIST and the Canadian Centre for Cyber Security.

Further information on the evaluation of the implementation of cryptographic algorithms, including testing requirements, is available as part of the Cryptographic Algorithm Validation Program which is jointly operated by NIST and the Canadian Centre for Cyber Security.

Further information on the protection of IT equipment and media can be found in the Department of Home Affairs' *Protective Security Policy Framework*.

Cryptographic algorithms

Context

There is no guarantee of a cryptographic algorithm's resistance to currently unknown attacks. However, the cryptographic algorithms listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting. Approval for the use of the cryptographic algorithms listed in this section is limited to cases where they are implemented in accordance with these guidelines.

The approved asymmetric cryptographic algorithms are:

- Diffie-Hellman (DH) for agreeing on encryption session keys
- Elliptic Curve Diffie-Hellman (ECDH) for agreeing on encryption session keys
- Elliptic Curve Digital Signature Algorithm (ECDSA) for digital signatures
- Module-Lattice-Based Digital Signature Algorithm (ML-DSA) for digital signatures
- Module-Lattice-Based Key Encapsulation Mechanism (ML-KEM) for encapsulating encryption session keys (and similar keys)
- Rivest-Shamir-Adleman (RSA) for digital signatures and transporting encryption session keys (and similar keys).

The only approved hashing algorithm for general-purpose use is Secure Hashing Algorithm 2 (SHA-2). However, Secure Hashing Algorithm 3 (SHA-3), including its extendable-output functions, is approved exclusively for use within ML-DSA and ML-KEM.

The only approved symmetric cryptographic algorithm is Advanced Encryption Standard (AES).

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

The minimum targets used for the effective security strength of cryptographic algorithms listed within this section are:

- 112 bits for non-classified data
- 112 bits for OFFICIAL: Sensitive data
- 112 bits for PROTECTED data
- 128 bits for SECRET data
- 192 bits for TOP SECRET data.

Certain key sizes and parameters, such as specific elliptic curves, are preferred to promote interoperability with the United States' National Security Agency's *Commercial National Security Algorithm Suite 2.0*.

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

Using cryptographic algorithms

When encryption is applied to data at rest, it provides an additional layer of defence against unauthorised access by malicious actors. In doing so, it is critical that an AACA or high assurance cryptographic algorithm is used. Furthermore, if cryptographic equipment, applications or libraries implement unapproved cryptographic algorithms, it is possible that these cryptographic algorithms could be used without a human user's knowledge. In combination with an assumed level of security confidence, this can represent a security risk. As such, an organisation should ensure that only AACAs or high assurance cryptographic algorithms can be used by disabling all unapproved cryptographic algorithms (preferred) or by advising human users not to use the unapproved cryptographic algorithms via usage policies.

Control: ISM-1080; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An AACA or high assurance cryptographic algorithm is used when encrypting data at rest.

Control: ISM-0471; Revision: 9; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only AACAs or high assurance cryptographic algorithms are used by cryptographic equipment, applications and libraries.

Asymmetric cryptographic algorithms

ECDH is vulnerable to different types of attacks than DH. Consequently, ECDH offers more effective security per bit increase in key size than DH. This leads to smaller data requirements, which in turn means that the elliptic curve variants have become de facto global standards. For reduced data cost, and to promote interoperability, ECDH should be used in preference to DH where possible.

Control: ISM-0994; Revision: 7; Updated: Mar-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
ECDH is used in preference to DH.

Using Diffie-Hellman

A modulus of 2048 bits for correctly implemented DH provides 112 bits of effective security strength, with larger modulus sizes providing more bits of effective security strength.

When DH in a prime field is used, the prime modulus impacts the security of the cryptographic 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.

Taking into account projected technological advances in quantum computing, DH will not be approved beyond 2030.

Control: ISM-0472; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
When using DH for agreeing on encryption session keys, a modulus of at least 2048 bits is used, preferably 3072 bits.

Control: ISM-1759; Revision: 0; Updated: Mar-22; Applicable: S, TS; Essential 8: N/A
When using DH for agreeing on encryption session keys, a modulus of at least 3072 bits is used, preferably 3072 bits.

Control: ISM-1629; Revision: 1; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
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 Elliptic Curve Cryptography

The curve used within an elliptic curve cryptographic algorithm impacts the security of the cryptographic algorithm. As such, only suitable curves from NIST SP 800-186 should be used.

Control: ISM-1446; Revision: 3; Updated: Mar-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using elliptic curve cryptography, a suitable curve from NIST SP 800-186 is used.

Using Elliptic Curve Diffie-Hellman

When identifying a suitable curve from NIST SP 800-186, a base point order and key size of at least 224 bits for correctly implemented ECDH provides 112 bits of effective security strength, with larger key sizes providing more 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.

Taking into account projected technological advances in quantum computing, ECDH will not be approved beyond 2030.

Control: ISM-0474; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
When using ECDH for agreeing on encryption session keys, a base point order and key size of at least 224 bits is used, preferably the NIST P-384 curve.

Control: ISM-1761; Revision: 0; Updated: Mar-22; Applicable: S; Essential 8: N/A
When using ECDH for agreeing on encryption session keys, NIST P-256, P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Control: ISM-1762; Revision: 0; Updated: Mar-22; Applicable: TS; Essential 8: N/A
When using ECDH for agreeing on encryption session keys, NIST P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Using the Elliptic Curve Digital Signature Algorithm

When identifying a suitable curve from NIST SP 800-186, a base point order and key size of 224 bits for correctly implemented ECDSA provides 112 bits of effective security strength, with larger key sizes providing more 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.

Taking into account projected technological advances in quantum computing, ECDSA will not be approved beyond 2030.

Control: ISM-0475; Revision: 7; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
When using ECDSA for digital signatures, a base point order and key size of at least 224 bits is used, preferably the P-384 curve.

Control: ISM-1763; Revision: 0; Updated: Mar-22; Applicable: S; Essential 8: N/A
When using ECDSA for digital signatures, NIST P-256, P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Control: ISM-1764; Revision: 0; Updated: Mar-22; Applicable: TS; Essential 8: N/A
When using ECDSA for digital signatures, NIST P-384 or P-521 curves are used, preferably the NIST P-384 curve.

Using post-quantum cryptographic algorithms

Post-quantum cryptographic algorithms are more complex than their traditional counterparts. To reduce the risk that vulnerabilities are introduced via implementation errors, approval is given to specific post-quantum cryptographic standards. In doing so, FIPS 204 and FIPS 203 state that other foundational standards must also be adhered to, including the required use of FIPS 140-3 validated cryptographic modules. However, while the use of FIPS 140-3 validated modules is preferred, it is not required.

Control: ISM-1990; Revision: 1; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using ML-DSA and ML-KEM, as per FIPS 204 and FIPS 203 respectively, adherence to pre-requisite FIPS 140-3 validation is preferred.

Using the Module-Lattice-Based Digital Signature Algorithm

The effective security strength of ML-DSA has a complex dependency on numerous parameters with different effective security strengths targeted by different standardised parameter sets. The ML-DSA standard contains three different parameter sets: ML-DSA-44, ML-DSA-65 and ML-DSA-87. The use of ML-DSA-65 and ML-DSA-87 are approved.

When using ML-DSA for digital signing, it may be either hedged or deterministic, with the hedged variant providing effective protection from certain side-channel attacks that apply to the deterministic variant. For this reason, the hedged variant should be used whenever possible. The deterministic variant should not be used unless the nature of the digital signing platform renders the creation of random data infeasible, which is a mandatory step for the hedged variant.

When using ML-DSA for digital signing, signing a message first involves hashing the message using SHAKE128 or SHAKE256. In environments where the message being hashed is large, and the digital signing platform lacks hardware support for SHAKE128 and SHAKE256, pre-hashed variants of ML-DSA might be used to reduce computational overheads. In such cases, pre-hashed variants of ML-DSA take as their input a hash of the message as computed by an alternative, and less computationally expensive, hashing algorithm. In such cases, care should be taken to ensure that an appropriate alternative hashing algorithm is being used, such as a SHA-2 hashing algorithm. In such cases, the hash used should be twice as long as the desired effective security strength. In practice, this requires the use of at least SHA-384 for the pre-hashed variant of ML-DSA-65 and at the use of at least SHA-512 for the pre-hashed variant of ML-DSA-87.

For interoperability and maintainability reasons, ML-DSA-65 will not be approved beyond 2030.

Control: ISM-1991; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using ML-DSA for digital signatures, ML-DSA-65 or ML-DSA-87 is used, preferably ML-DSA-87.

Control: ISM-1992; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using ML-DSA for digital signatures, the hedged variant is used whenever possible.

Control: ISM-1993; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Pre-hashed variants of ML-DSA-65 and ML-DSA-87 are only used when the performance of default variants is unacceptable.

Control: ISM-1994; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When the pre-hashed variants of ML-DSA-65 and ML-DSA-87 are used, at least SHA-384 and SHA-512 respectively are used for pre-hashing.

Using the Module-Lattice-Based Key Encapsulation Mechanism

The effective security strength of ML-KEM has a complex dependency on numerous parameters with different effective security strengths targeted by different standardised parameter sets. The ML-KEM standard contains three different parameter sets: ML-KEM-512, ML-KEM-768 and ML-KEM-1024. The use of ML-KEM-768 and ML-KEM-1024 are approved.

For interoperability and maintainability reasons, ML-KEM-768 will not be approved beyond 2030.

Control: ISM-1995; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using ML-KEM for encapsulating encryption session keys (and similar keys), ML-KEM-768 or ML-KEM-1024 is used, preferably ML-KEM-1024.

Using Rivest-Shamir-Adleman

A modulus of 2048 bits for correctly implemented RSA provides 112 bits of effective security strength, with larger modulus sizes providing more bits of effective security strength.

Taking into account projected technological advances in quantum computing, RSA will not be approved beyond 2030.

Control: ISM-0476; Revision: 8; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
When using RSA for digital signatures, and transporting encryption session keys (and similar keys), a modulus of at least 2048 bits is used, preferably 3072 bits.

Control: ISM-1765; Revision: 1; Updated: Dec-24; Applicable: S, TS; Essential 8: N/A
When using RSA for digital signatures, and transporting encryption session keys (and similar keys), a modulus of at least 3072 bits is used, preferably 3072 bits.

Control: ISM-0477; Revision: 9; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using RSA for digital signatures, and for transporting encryption session keys (and similar keys), a different key pair is used for digital signatures and transporting encryption session keys.

Using Secure Hashing Algorithms

For most purposes, a hashing algorithm with an output size of 224 bits provides 112 bits of effective security strength, with larger output sizes providing more bits of effective security strength.

Only SHA-2 hashing algorithms are approved for general-purpose use. Approval of SHA-3 and extendable-output functions (i.e. SHA3-256, SHA3-512, SHAKE128 and SHAKE256) is restricted to use within internal steps of ML-DSA and ML-KEM.

For interoperability and maintainability reasons, SHA-224 and SHA-256 will not be approved beyond 2030.

Control: ISM-1766; Revision: 1; Updated: Dec-24; Applicable: NC, OS, P; Essential 8: N/A
When using SHA-2 for hashing, an output size of at least 224 bits is used, preferably SHA-384 or SHA-512.

Control: ISM-1767; Revision: 1; Updated: Dec-24; Applicable: S; Essential 8: N/A
When using SHA-2 for hashing, an output size of at least 256 bits is used, preferably SHA-384 or SHA-512.

Control: ISM-1768; Revision: 1; Updated: Dec-24; Applicable: TS; Essential 8: N/A
When using SHA-2 for hashing, an output size of at least 384 bits is used, preferably SHA-384 or SHA-512.

Using symmetric cryptographic algorithms

When using AES, a key size of 128 bits provides 128 bits of effective security strength, with larger key sizes providing more bits of effective security strength.

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, malicious actors can use this to deduce possible meanings of ciphertext. The use of other modes, such as Cipher Block Chaining, Cipher Feedback, Galois/Counter Mode or Output Feedback, can prevent such attacks, although each has different properties that can make them inappropriate for certain use cases. AES is the only approved symmetric cryptographic algorithm.

For interoperability and maintainability reasons, AES-128 and AES-192 will not be approved beyond 2030.

Control: ISM-1769; Revision: 1; Updated: Dec-24; Applicable: NC, OS, P, S; Essential 8: N/A
When using AES for encryption, AES-128, AES-192 or AES-256 is used, preferably AES-256.

Control: ISM-1770; Revision: 0; Updated: Mar-22; Applicable: TS; Essential 8: N/A
When using AES for encryption, AES-192 or AES-256 is used, preferably AES-256.

Control: ISM-0479; Revision: 5; Updated: Dec-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Symmetric cryptographic algorithms are not used in Electronic Codebook Mode.

Transitioning to post-quantum cryptography

The consensus model for quantum computing allows for different types of quantum attacks against traditional cryptography. While the direct impact of these quantum attacks varies across different cryptographic algorithms, there is a stark difference in impact between asymmetric cryptographic algorithms and symmetric cryptographic algorithms.

One known quantum attack (using Shor's algorithm) effectively defeats all traditional cryptography that relies upon asymmetric cryptographic algorithms such as DH, ECDH, ECDSA or RSA. The efficiency of this is such that it is infeasible to securely use these AACAs in the presence of a cryptographically relevant quantum computer (CRQC). While a CRQC does not currently exist, the trajectory of technological advances in quantum computing means that these AACAs will need to be phased out in favour of alternative AACAs that offer greater protection. As such, the development or procurement of new cryptographic equipment, applications and libraries, which are intended to be used beyond 2030, should be undertaken with the goal of supporting ASD-approved post-quantum cryptographic algorithms by 2030.

The impact of quantum attacks on hashing algorithms and symmetric cryptographic algorithms, such as SHA-2 and AES, is unlikely to be felt for some time. However, for interoperability reasons, the design and provision of new cryptographic equipment, applications and libraries, which are intended to be used beyond 2030, should support SHA-384, SHA-512 and AES-256.

Control: ISM-2073; Revision: 0; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A post-quantum cryptography transition plan is developed, implemented and maintained.

Control: ISM-1917; Revision: 3; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The development and procurement of new cryptographic equipment, applications and libraries ensures support for the use of ML-DSA-87, ML-KEM-1024, SHA-384, SHA-512 and AES-256 by no later than 2030.

Post-quantum traditional hybrid schemes

A post-quantum traditional hybrid scheme is a multi-algorithm scheme where at least one cryptographic algorithm is a post-quantum cryptographic algorithm (e.g. ML-KEM) and at least one cryptographic algorithm is a traditional cryptographic algorithm (e.g. RSA). Generally, such schemes have the advantage of the security offered by the traditional cryptographic algorithm if the post-quantum cryptographic algorithm is vulnerable to an implementation flaw or new attack. This advantage comes at the cost of increased complexity, making maintenance, analysis and secure implementation more difficult, as well as having greater computational and bandwidth overheads.

The use of post-quantum traditional hybrid schemes is not recommended; however, it is not prohibited. If such schemes are to be used, at least one of the post-quantum or traditional cryptographic algorithms, or both, should be an AACA. It is important to note though, that in the presence of a CRQC, the security of such schemes is reduced to that provided by the post-quantum cryptographic algorithm. As such, there is no practical value in the use of such schemes in the presence of a CRQC. An organisation choosing to implement a post-quantum traditional hybrid scheme should also keep in mind the eventual additional cost of transitioning to a pure post-quantum scheme in the future.

Control: ISM-1996; Revision: 0; Updated: Dec-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When a post-quantum traditional hybrid scheme is used, either the post-quantum cryptographic algorithm, the traditional cryptographic algorithm or both are AACAs.

Further information

Further information on planning for the transition to post-quantum cryptography can be found in ASD's *Planning for post-quantum cryptography* and *Post-quantum questions to ask your vendors* publications.

Further information on post-quantum traditional hybrid schemes can be found in the United Kingdom's National Cyber Security Centre's *Next steps in preparing for post-quantum cryptography* guidance.

Further information on how to combine the different components of a post-quantum traditional hybrid scheme used for key encapsulation can be found in NIST SP 800-56C Rev. 2, *Recommendation for Key-Derivation Methods in Key-Establishment Schemes*. This publication does not pertain to post-quantum traditional hybrid schemes used for digital signatures.

Cryptographic protocols

Context

There is no guarantee of a cryptographic protocol's resistance to currently unknown attacks. However, the cryptographic protocols listed in this section have been extensively scrutinised by industry and academic communities in a practical and theoretical setting. Approval for the use of the cryptographic protocols listed in this section is limited to cases where they are implemented in accordance with these guidelines.

The AACPs are:

- Internet Protocol Security (IPsec)
- Media Access Control Security
- OpenPGP Message Format

- Secure Shell (SSH)
- Secure/Multipurpose Internet Mail Extensions (S/MIME)
- Transport Layer Security (TLS)
- Wi-Fi Protected Access 2
- Wi-Fi Protected Access 3.

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

Using cryptographic protocols

When encryption is applied to data in transit, it provides an additional layer of defence against unauthorised access or manipulation by malicious actors. In doing so, it is critical that an AACP or high assurance cryptographic protocol is used. Furthermore, if cryptographic equipment, applications or libraries implement unapproved cryptographic protocols, it is possible that these cryptographic protocols could be used without a human user's knowledge. In combination with an assumed level of security confidence, this can represent a security risk. As such, an organisation should ensure that only AACPs or high assurance cryptographic protocols can be used by disabling all unapproved cryptographic protocols (preferred) or by advising human users not to use the unapproved cryptographic protocols via usage policies.

Control: ISM-0469; Revision: 7; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
An AACP or high assurance cryptographic protocol is used when encrypting data in transit.

Control: ISM-0481; Revision: 8; Updated: Sep-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only AACPs or high assurance cryptographic protocols are used by cryptographic equipment, applications and libraries.

Further information

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

Further information on the use of Media Access Control Security can be found in the 'Wired networks' section of the *Guidelines for networking*.

Further information on the use of Wi-Fi Protected Access 2 and Wi-Fi Protected Access 3 can be found in the 'Wireless networks' section of the *Guidelines for networking*.

Internet Protocol Security

Context

When using IT equipment or applications that implement IPsec, security controls for using AACAs and AACPs in the 'Cryptographic algorithms' and 'Cryptographic protocols' sections of these guidelines will also need to be consulted.

Mode of operation

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

Control: ISM-0494; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Tunnel mode is used for IPsec connections; however, if using transport mode, an IP tunnel is used.

Protocol selection

IPsec contains two major protocols, the Authentication Header (AH) protocol and the Encapsulating Security Payload (ESP) protocol. To provide a secure virtual private network style connection, authentication and encryption are needed. While the AH and ESP protocols can provide authentication, for the IP packet and the payload respectively, only the ESP protocol can provide encryption.

As the combined use of the AH protocol and the ESP protocol is not supported by Internet Key Exchange (IKE) version 2, the ESP protocol should be used for authentication and encryption of IPsec connections.

Control: ISM-0496; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The ESP protocol is used for authentication and encryption of IPsec connections.

Key exchange

There are several methods for establishing shared keying material for IPsec connections, including manual keying and the IKE protocol. As the IKE protocol addresses several security risks associated with manual keying, it is the preferred method for key establishment. As IKE version 1 has been deprecated, IKE version 2 should be used.

Control: ISM-1233; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
IKE version 2 is used for key exchange when establishing IPsec connections.

Encryption algorithms

The only approved encryption algorithm for IPsec connections is AES. IKE version 2 supports the use of AES with Cipher Block Chaining, Counter Mode, Counter with Cipher Block Chaining Message Authentication Code, and Galois/Counter Mode. However, supported modes may vary between different cryptographic equipment, applications and libraries.

Control: ISM-1771; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
AES is used for encrypting IPsec connections, preferably ENCR_AES_GCM_16.

Pseudorandom function

IKE version 2 requires the use of a PRF to generate random data for cryptographic operations. The approved hashing algorithms that can be used for the PRF are HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512.

For interoperability and maintainability reasons, HMAC-SHA256 will not be approved beyond 2030.

Control: ISM-1772; Revision: 0; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
PRF_HMAC_SHA2_256, PRF_HMAC_SHA2_384 or PRF_HMAC_SHA2_512 is used for IPsec connections, preferably PRF_HMAC_SHA2_512.

Integrity algorithms

The approved integrity algorithms for IPsec connections are HMAC-SHA256, HMAC-SHA384 and HMAC-SHA512. However, if using AES with Galois/Counter Mode as the encryption algorithm, it can also be used for authentication purposes. In such cases, the integrity algorithm should be configured as NONE.

For interoperability and maintainability reasons, HMAC-SHA256 will not be approved beyond 2030.

Control: ISM-0998; Revision: 5; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
AUTH_HMAC_SHA2_256_128, AUTH_HMAC_SHA2_384_192, AUTH_HMAC_SHA2_512_256 or NONE (only with AES-GCM) is used for authenticating IPsec connections, preferably NONE.

Diffie-Hellman groups

A sufficiently large DH modulus provides greater security for key exchanges when establishing IPsec connections.

Taking into account projected technological advances in quantum computing, DH and ECDH will not be approved beyond 2030.

Control: ISM-0999; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
DH or ECDH is used for key establishment of IPsec connections, preferably 384-bit random ECP group, 3072-bit MODP Group or 4096-bit MODP Group.

Security association lifetimes

Using a security association lifetime of less than four hours (14400 seconds) for IKE version 2 can provide a balance between security and usability.

Control: ISM-0498; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A security association lifetime of less than four hours (14400 seconds) is used for IPsec connections.

Perfect Forward Secrecy

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

Control: ISM-1000; Revision: 4; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
PFS is used for IPsec connections.

Secure Shell

Context

When using IT equipment or applications that implement SSH, security controls for using AACAs and AACPs in the ‘Cryptographic algorithms’ and ‘Cryptographic protocols’ sections of these guidelines will also need to be consulted.

Configuring Secure Shell

SSH version 1 was found to have multiple vulnerabilities and was subsequently replaced by SSH version 2. As such, an organisation implementing SSH should disable the use of SSH version 1. In addition, several security risks exist when SSH is configured in an insecure manner. To mitigate these security risks, SSH should be configured as per the settings below.

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

Control: ISM-1506; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The use of SSH version 1 is disabled for SSH connections.

Control: ISM-0484; Revision: 7; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The SSH daemon is configured to:

- *only listen on the required interfaces (ListenAddress xxx.xxx.xxx.xxx)*
- *have a suitable login banner (Banner x)*
- *have a login authentication timeout of no more than 60 seconds (LoginGraceTime 60)*
- *disable host-based authentication (HostbasedAuthentication no)*
- *disable rhosts-based authentication (IgnoreRhosts yes)*
- *disable the ability to log in directly as root (PermitRootLogin no)*
- *disable empty passwords (PermitEmptyPasswords no)*
- *disable connection forwarding (AllowTCPForwarding no)*
- *disable gateway ports (GatewayPorts no)*
- *disable X11 forwarding (X11Forwarding no).*

Authentication mechanisms

As public key-based authentication schemes offer stronger authentication than password-based authentication schemes, due to being much less susceptible to brute-force attacks, they should be used for SSH connections. Furthermore, to protect SSH private keys, access to such keys should be protected via the use of passwords or key encryption keys.

Control: ISM-0485; Revision: 3; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Public key-based authentication is used for SSH connections.

Control: ISM-1449; Revision: 2; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SSH private keys are protected with a password or a key encryption key.

Automated remote access

If using logins without a password for automated purposes, several security risks may arise, specifically:

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

- if port forwarding is not disabled, or it is not configured securely, access may be gained to forwarded ports, creating a communication channel between malicious actors and a host
- if agent credential forwarding is enabled, malicious actors 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 forwarding is not disabled, malicious actors could gain control of displays as well as keyboard and mouse control functions
- if console access is allowed, every user who logs in to the console could run applications 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 checking is enabled.

Control: ISM-0487; Revision: 6; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When using logins without a password for SSH connections, the following are disabled:

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

Control: ISM-0488; Revision: 5; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
If using remote access without the use of a password for SSH connections, the 'forced command' option is used to specify what command is executed and parameter checking is enabled.

SSH-agent

SSH-agent and similar key caching applications manage private keys stored on workstations and servers. Once a private key has been unlocked and loaded into a key cache, subsequent access to remote systems can occur without the private key being unlocked again. When such functionality is used, screen locks, where applicable, and expiring cached private keys can be used to ensure that private keys are not available for use for extended periods.

Control: ISM-0489; Revision: 7; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
When SSH-agent or similar key caching applications are used, cached private keys have a maximum lifetime of four hours and, where applicable, screen locks are used on workstations and servers.

Further information

Further information on configuring OpenSSH is available from the OpenSSH project.

Secure/Multipurpose Internet Mail Extensions

Context

When using IT equipment or applications that implement S/MIME, security controls for using AACAs and AACPs in the ‘Cryptographic algorithms’ and ‘Cryptographic protocols’ sections of these guidelines will also need to be consulted.

Configuring Secure/Multipurpose Internet Mail Extensions

S/MIME version 2.0 required the use of weaker cryptography than approved for use in these guidelines. As such, S/MIME version 3.0 was the first version to be approved for use as an AACP.

Control: ISM-0490; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Versions of S/MIME earlier than S/MIME version 3.0 are not used for S/MIME connections.

Transport Layer Security

Context

When using IT equipment or applications that implement TLS, security controls for using AACAs and AACPs in the ‘Cryptographic algorithms’ and ‘Cryptographic protocols’ sections of these guidelines will also need to be consulted.

Configuring Transport Layer Security

The terms Secure Sockets Layer and TLS have traditionally been used interchangeably. However, Secure Sockets Layer and TLS version 1.2 and earlier are no longer considered suitable for use as an AACP. As such, an organisation implementing TLS should use only the latest version of TLS (i.e. TLS version 1.3). In addition, several security risks exist when TLS is configured in an insecure manner. To mitigate these security risks, TLS clients and servers should be configured to enforce secure settings at the time of the TLS handshake. In situations where this is not possible, such as for some multi-tenancy environments (e.g. content delivery networks), additional security controls will need to be implemented. For example, by further restricting the permitted TLS configuration within Layer 7 authorisation logic.

Control: ISM-1139; Revision: 6; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only the latest version of TLS is used for TLS connections.

Control: ISM-1369; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
AES-GCM is used for encryption of TLS connections.

Control: ISM-1370; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Only server-initiated secure renegotiation is used for TLS connections.

Control: ISM-1372; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The ephemeral variant of DH or ECDH is used for key establishment of TLS connections.

Control: ISM-1373; Revision: 2; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Anonymous DH is not used for TLS connections.

Control: ISM-1374; Revision: 3; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SHA-2-based certificates are used for TLS connections.

Control: ISM-1375; Revision: 4; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
SHA-2 is used for the Hash-based Message Authentication Code (HMAC) and pseudorandom function (PRF) for TLS connections.

Control: ISM-1553; Revision: 1; Updated: Mar-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
TLS compression is disabled for TLS connections.

Control: ISM-1453; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Perfect Forward Secrecy (PFS) is used for TLS connections.

Further information

Further information on implementing TLS can be found in ASD's *Implementing certificates, TLS, HTTPS and opportunistic TLS* publication.

Further information on TLS filtering in gateways can be found in the 'Web content filters' section of the *Guidelines for gateways*.

Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre