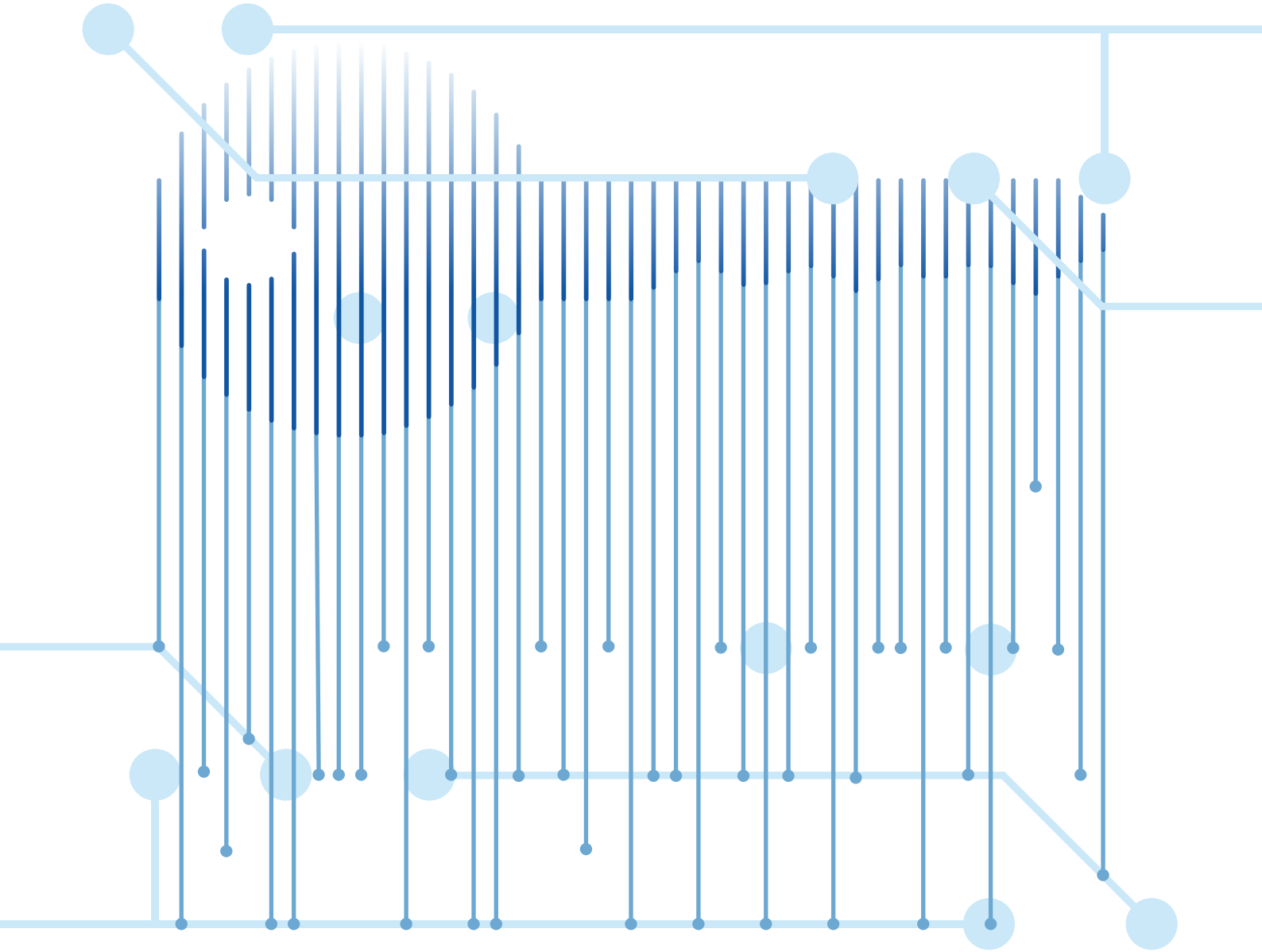
Managing cryptographic keys and secrets



Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

Australian Government

Department of Industry, Science and Resources

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

National Cyber Security Centre

a part of GCHQ

National Cyber Security Centre

NEW ZEALAND

JPCERT CC®

国家サイバー統括室

National Cybersecurity Office

Table of contents

Introduction

The world is increasingly relying on online services, digitalisation of data and interconnected systems, cyber security is a vital way in which we protect critical sectors. Good security hygiene keeps participants from making mistakes and makes it harder for malicious cyber actors to cause damage. One important aspect of cyber security is cryptographic keys and secrets management systems. Cryptographic keys and secrets are required for services that secure data, provide integrity, confidentiality, non-repudiation and access control. Cryptographic keys and secrets are a critical asset of many organisations and a core component of cyber security, which must be carefully managed and protected throughout their life cycle.

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) and the Department of Industry Science and Resources (DISR) have developed this guide to help organisational personnel in understanding the **threat environment and the value of implementing secure keys and secrets management** to make better informed decisions.

The compromise of any private key or secret can have significant, or even severe, negative operational, financial and reputational impacts on an organisation. Organisations must seek to implement mitigations to ensure their organisational keys and secrets are protected and so they are positioned to respond quickly and effectively in the case of a security incident.

Organisations should have a comprehensive understanding of the threat environment which will enable them to build a strong Key Management Plan (KMP) to address their own unique environment and all cryptographic material management, enabling positive security outcomes. A KMP should be prepared in the context of both internal and external threats, how compromise can occur, and what can be done to mitigate and respond to any potential threats.

The advice in this publication has considered threats to the following types of cryptographic keys and secrets:

- **Asymmetric keys** - Two mathematically related keys – a public and a private key – that are used to perform complementary operations, such as encryption, decryption, signature generation and signature verification.
- **Digital certificate** - An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.
- **Symmetric key** - A cryptographic key that is used to perform both the cryptographic operations and its inverse: that is, encryption and decryption, or to create a message authentication code or verify a message authentication code.
- **Secret** - A confidential and controlled piece of data shared between multiple entities to gain or grant access to a resource, typically used for machine-to-machine access or authorisation, such as an Application Programming Interface (API) key.

The ASD's ACSC, the Department of Industry Science and Resources (DISR) and the following international partners provide the recommendations in this guide:

- Canadian Centre for Cyber Security (Cyber Centre)
- United Kingdom's National Cyber Security Centre (NCSC-UK)
- New Zealand's National Cyber Security Centre (NCSC-NZ)
- Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
- Japan National Cybersecurity Office (NCO)

Audience

This paper is written for **organisational security personnel** – including architects, IT security, crypto custodians and managers – whose organisations rely on, use or manage cryptographic keys and secrets. This advice applies to Cloud Service Providers and enterprise organisations with on-premises or hybrid environments.

This document assumes a moderate level of computing and cyber security knowledge on the part of the reader.

Secure by Design

This guidance is part of the broader Secure by Design initiative by the authoring agencies.

- ASD - https://www.cyber.gov.au/resources-business-and-government/governance-and-user-education/secure-by-design

A KMP sets out organisational practices and procedures that aim to ensure secure life cycle management for keys and secrets. Secure key and secret management is a key pillar of ASD's ACSC Secure by Design Foundation 2 - Early and Sustained Security – 'Following an early and sustained security-first approach when developing and procuring products is an investment that facilitates both technology manufacturers and technology consumers to be resilient to cyber risks'.

In their most fundamental form, keys and secrets support the following functions:

- **Confidentiality:** they allow data to be transmitted or stored securely allowing only authorised entities access.
- **Integrity:** they ensure that data is authentic and has not been changed.
- **Authentication and non-repudiation:** they allow the key holder to provide an identity for authentication.

Understanding the threat environment

When organisations use keys and secrets within their information environment, a comprehensive understanding of the current and emerging threat environment can assist them in making informed decisions to appropriately manage organisational risks. Understanding the ways in which malicious cyber actors can compromise keys and secrets, empowers organisations to implement security mitigations to prevent, minimise and detect compromise, reducing the overall organisational impact from a security incident.

Organisations can stay informed by following advisories and alert services:

- ASD - https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories
- NCSC UK - https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories

The compromise of secrets or cryptographic material at any point in the life cycle can have a severe impact on the security posture of an organisation. It is critical that organisations can trust the keys and secrets used within their information environment.

> The worst form of key or secret compromise is one that is not detected

Common compromises

Key or secret compromise can occur when a protective mechanism fails, at which point the key or secret can no longer be considered trusted. The unauthorised disclosure of a key or secret means that information secured by that key or secret could be exposed to unauthorised entities, be altered without detection, allow unauthorised access, or prevent authorised access.

Common types of compromise include:

- **Brute force:** the key or secret can by guessed, because the key space not large enough, insufficient entropy is used, or a weak algorithm is selected.
- **Unauthorised access:** a key or secret is accessed, used or destroyed by an unauthorised user.
- **Key integrity:** the key or secret is modified or substituted.
- **Malicious trust:** a malicious key or secret is placed in a position of trust.
- **Human error:** improper generation, handling or usage of keys or secrets.

By understanding the types of compromises that can occur and how these may occur within or to an organisation, organisations can build out their KMP to ensure that the right mitigations and response plans are in place.

The following are examples of the impact of a compromised key:

- https://www.cisa.gov/sites/default/files/2025-03/CSRBReviewOfTheSummer2023MEOIntrusion508.pdf
- https://www.ccn.com/education/crypto/14-billion-bitcoin-heist-lubian-wallet-flaw-arkham/
- https://www.bleepingcomputer.com/news/security/new-shrinklocker-ransomware-uses-bitlocker-to-encrypt-your-files/
- https://www.bleepingcomputer.com/news/security/hackers-steal-162-million-from-wintermute-crypto-market-maker/
- https://arstechnica.com/information-technology/2015/03/in-major-goof-uber-stored-sensitive-database-key-on-public-github-page/

Threat model

The diagram below details possible points at which a malicious cyber actor may attempt to compromise keys and secrets. The diagram is an example only and each organisation will need to consider its own environment and use cases. The following potential attack surfaces are identified:

1. compromise of an external service
2. external attack against a user environment
3. malicious cyber actor in the user environment
4. external attack against the organisation's environment
5. malicious cyber actor in the organisation's environment.

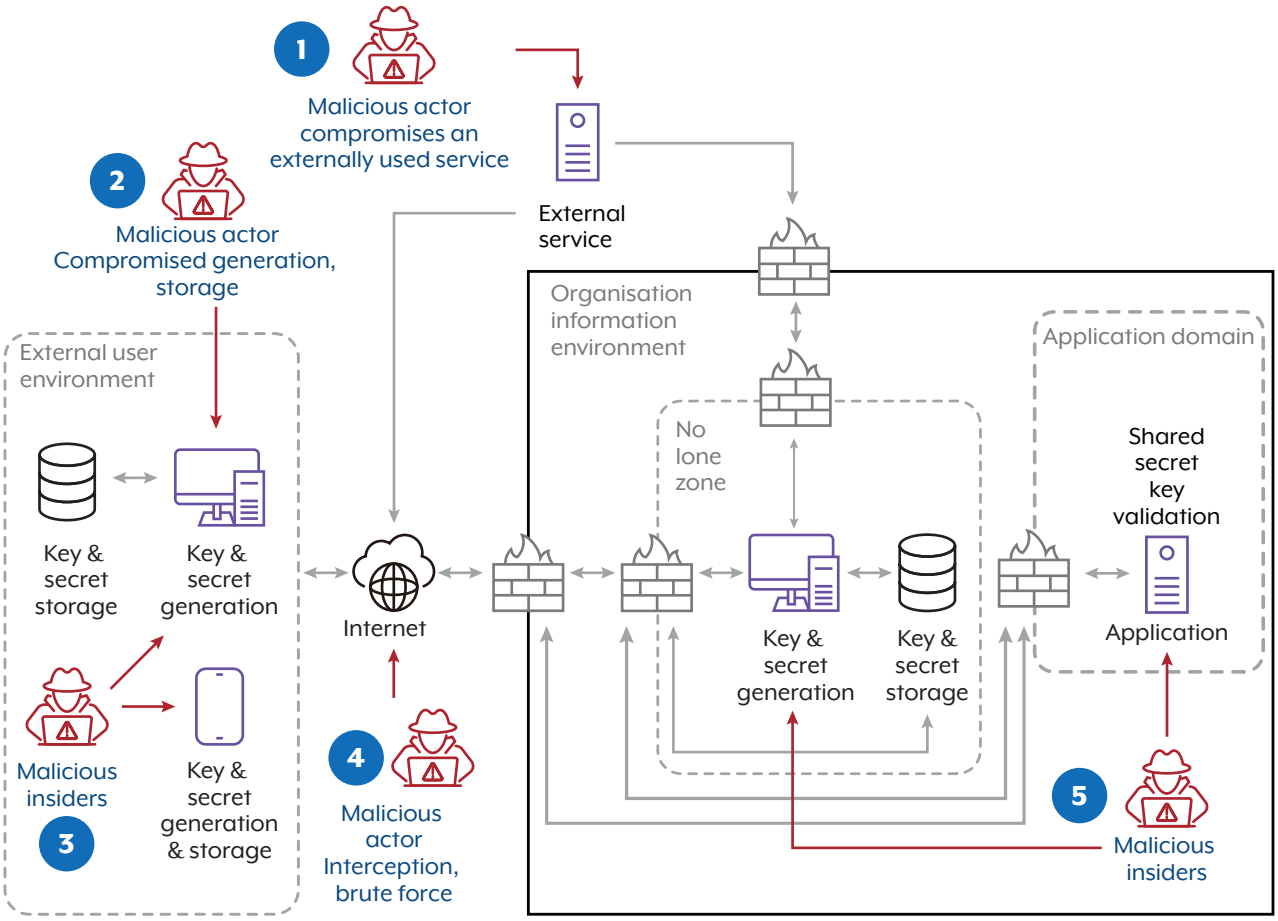


Figure 1. Threat environment

The following table describes some common malicious actions or attacks, the details of each, the vector from which the attack or action may occur and suggestion on possible mitigation strategies.

Table 1: Opportunity for malicious actions or attacks

Opportunity for malicious actions or attacks	Description	Attack vectors: Figure 1	Possible mitigation strategies
Predictable keys and secrets	Keys and secrets are generated from a predictable source of randomness that could be determined and used to predict key or secret generation.	2, 3, 4, 5	Ensure that a cryptographically supported or true random number generator with sufficient entropy is used when generating keys or secrets.
Insufficient length	A key or secret length is used that can be brute forced with existing or near future computing or technological advances.	2, 3, 4, 5	Ensure that a key or secret of sufficient length is used – one that will cover current brute force attacks and possible future brute force attacks throughout the lifetime of the data or resource being protected.
Weak algorithm	An algorithm with known weaknesses is used to protect a resource.	2, 3, 4, 5	Ensure that all algorithms used are free from known weakness and are deemed to be of sufficient strength at the time of selection to protect resources for their known lifetime and the ability to promptly address any newly discovered weaknesses.
Insecure storage or backup	The storage, including in configuration files or backup technology, used for key and secret management has vulnerabilities or weaknesses that could be exploited to compromise the confidentiality or integrity of a key or secret.	2, 3, 4, 5	Hardware Security Modules (HSM) provide enhanced storage and usage security controls for keys and secrets. Where a HSM is not available organisations can consider Software Security Modules (SSM). All other types of storage, including backups, need to have sufficient controls to the level of protection required by the key or secret. Note, backups and recovery mechanisms are an additional attack surface that need to be analysed and secured.
Overprivileged users	An overprivileged user exploits their access to perform unauthorised actions with accessible keys or secrets.	3, 5	Principle of least privilege must be followed, and logging and monitoring must be used to identify any unauthorised actions.

Opportunity for malicious actions or attacks	Description	Attack vectors: Figure 1	Possible mitigation strategies
Lack of rotation	The longer a key or secret is in use, the greater the likelihood of hitting safety limits of high throughout applications or of an undetected compromise.	2, 4	A KMP containing lifetimes, the cryptoperiod, and rollover plans for all organisational keys and secrets, should be calculated using the following factors: • The originator usage period (OUP): the time during which cryptographic protection is applied to data. • The recipient usage period (RUP): The period during which protected data may be processed.
Ineffective revocation	A malicious cyber actor could use an old key or secret that should have been revoked to perform unauthorised actions.	2, 4	Ensure the key management plan contains revocation policies and processes for all organisational keys and secrets.
Key exposure – interception	A key or secret that has been exposed through interception or handling error is used by a malicious cyber actor to perform unauthorised actions.	2, 4	Keys should only be shared or distributed to those who require access, limiting the distribution will reduce exposure. Additionally, effective logging and monitoring are used to detect and respond to unauthorised use of keys and secrets.
Ineffective logging and monitoring	Without sufficient logging and visibility, security incidents may go undetected. The lack of actionable log data hinders an incident response teams' ability to promptly investigate and mitigate incidents.	1, 2, 3, 4, 5	Effective logging and monitoring are used to detect and respond to unauthorised use of keys and secrets.
Malicious insiders	A trusted insider performs an unauthorised action which compromises a key or secret.	3, 5	Implement no lone zones and secondary verification of changes or actions. Reduce access to critical functions through the separation of tasks, using the recommended positions of trust in this guide. Additionally, keys and secrets are not stored in clear text and effective logging and monitoring are used to detect and respond to unauthorised use of keys and secrets.

Opportunity for malicious actions or attacks	Description	Attack vectors: Figure 1	Possible mitigation strategies
Non-malicious insider	A trusted insider makes an error that exposes or compromises a key or secret	3, 5	Implement no lone zones and secondary verification of changes or actions. Reduce access to critical functions through the separation of tasks, using the recommended positions of trust in this guide. Additionally, keys and secrets are not stored in clear text and effective logging and monitoring are used to detect and respond to unauthorised use of keys and secrets.
Insecure transmission or exchange	The transmission or exchange of a key or secret is intercepted by a malicious cyber actor and used for unauthorised actions.	1, 2, 3, 4, 5	Ensure the transmission or exchange mechanism is secure. Additionally use alternative channels to verify the integrity of exchange as required.
External service compromise	Any external services that an organisation integrates with is compromised which could then exploit organisational keys or secrets, these could include time source service, trust broker, cloud service provider or partner organisations.	1, 4	Verified and secure external services are used or moved internally where possible. Effective logging and monitoring are used to detect and respond to unauthorised use of keys and secrets. Specific agreements with the external service provider for handling keys and secrets that adhere to their security policies.

Key and secret management

Effective management of keys and secrets is paramount to ensuring their integrity and secrecy. The following are significant areas of key and secret management organisations need to cover in their key management plans:

- Governance - security policies and procedures
- Generation - the creation of keys and secrets
- Registration, storage and access - the registration secure storage and access of keys and secrets
- Distribution - the secure exchange of keys and secrets between multiple parties
- Rollover and destruction - the changing and destruction
- Chains of trust - the process of trusting keys issued by a certificate authority
- Positions of trust - trusted roles in keys and secret management
- Oversight - auditing and monitoring

Failure in any of these areas can lead to the compromise of the key or secret and to the compromise of the organisation.

Governance

Cryptographic material management policies are established to describe the goals, responsibilities, and overall requirements for the management of keys and secrets used to protect data, provide integrity and confidentiality and non-repudiation and for granting access to resources. Management procedures are implemented through a combination of security mechanisms and actions. An organisation can use security mechanisms (e.g., safes, alarms, random number generators, encryption algorithms, signature, and authentication algorithms) as tools to implement key and secret policies. Organisations should establish their security policies and procedures that govern their KMP's activities and ensure compliance with relevant standards and regulations.

Generation

A key or secret can be generated through a management system or by a trusted third party. Organisations should preference generation in hardware security modules (HSM), where a HSM is not available a software security module (SSM) can be substituted. Generation should use a cryptographically secure pseudo random, or true random if available, number generator with sufficient entropy. Organisations need to ensure that the location at which the key or secret is generated has the highest levels of trust, as the point of generation has a high risk of compromise. Organisations should preference modules that are compliant with the NIST FIPS 140-3 security requirements for cryptographic modules.

Keys need to have a key space that can provide adequate protection for the entire lifetime of the protected data. Where there is a range of key sizes for a cryptographic algorithm, a size must be selected that provides the level of protection required in relation to the level of efficiency required. Some key sizes in certain algorithms are known either to be insecure against current attacks or not to provide an adequate safety margin against possible future attacks. Secrets should be generated with sufficient entropy that they cannot be brute forced within the lifetime of the resource they provide access to.

Further information on suggested key sizes and generation can be found at:

- ASD, Information Security Manual - https://www.cyber.gov.au/resources-business-and-government/essential-cybersecurity/ism/cybersecurity-guidelines/guidelines-cryptography
- UK-based systems owners should consult the NCSC UK - https://www.ncsc.gov.uk/contact
- NIST, Transitioning the Use of Cryptographic Algorithms and Key Lengths - https://csrc.nist.gov/pubs/sp/800/131/a/r2/final
- NIST, Recommendation for Cryptographic Key Generation - https://csrc.nist.gov/pubs/sp/800/133/r2/final

The increasing capabilities of quantum computing are making current cryptographic algorithms and key agreement protocols insecure and obsolete. Organisations need to be aware of which algorithms and protocols they are using, and which are more susceptible to being broken by quantum computing. Organisations should make moving to quantum resistant algorithms and protocols part of their KMP.

Further information on quantum resistant algorithms can be found at:

- NSA - https://media.defense.gov/2025/May/30/2003728741/-1/-1/0/CSA_CNSA_2.0_ALGORITHMS.PDF

Registration, storage and access

Keys and secrets, need to be registered and stored in a secure manner with only authorised users or systems granted access. At rest, access and integrity should be protected with an algorithm of sufficient strength that provides encryption and data integrity for the lifetime of the data. Utilising a HSM or SSM for storage, access and cryptographic operations will mitigate significant exposure and compromise risks. Recovery and escrow are additional functions that organisations may need to support. These functions add risks to usage and management that need to be considered within the context of the organisation and the systems in which keys and secrets are used.

Owners or accountable authorities of keys and secrets within the organisation need to regularly audit and verify access to ensure that only authorised entities have access. Keys and secrets must be protected through an effective access control solution. Unauthorised access to private keys or secrets, especially undetected unauthorised access, can lead to significant compromise of an organisation. Improper trust of a public key can compromise an organisation by allowing unauthorised access through malicious private keys.

Certain storage or usage locations, such as volatile and non-volatile memory, will at some point have access to the clear text private key or secret. This makes them vulnerable to memory dumps or unintended logging, which can cause exposure. Data stored in memory for a long time can become “burned in”. This can be mitigated by splitting the key or secret into components that are frequently updated. Additionally, the loss or corruption of the memory media on which keys or secrets are stored can lead to compromise. If an organisation suspects that a private key or secret has been compromised through exploited storage, memory corruption or memory leak, they need to follow

their KPM rollover procedures. If a malicious public key has been trusted, organisations should follow their incident response procedures for unauthorised access.

Storage should be physically constrained to be in the control of only trustworthy people, see Positions of Trust. When keys are managed externally, they should be physically constrained by trustworthy partners to ensure that no copy of the key or information that could help recover the key be located physically where it may be susceptible to disclosure. Agreements with external partners need to ensure that protection of keys and secrets provides sufficient protection in all cases. To counter other threats, cryptographic protections should be used.

Distribution

Public keys and secrets can be exchanged between parties to facilitate or grant access to systems, applications or data. This can occur between the organisation generating keys and secrets and its customers or from a third party to the organisation itself. Each scenario has unique risk factors that both the sender and the receiver need to consider. Ensuring that the chosen exchange method is verifiable and secure is important in reducing the risk of compromise.

Establishing a shared secret to be used for communication, access or to exchange other keys or secrets is a fundamental aspect of many cryptographic protocols. Organisations should ensure they are using industry standardised cryptographic protocols that have been verified, such as TLS or IPSec. For example, one party encrypts an ephemeral key using a shared secret or a public key and sends it to a second party who decrypts it. Public keys or shared secrets are necessary to support many technologies and transactions. Organisations need to ensure that all parties with access to shared secrets have protections in place that meet organisational risk tolerances and that only trusted public keys are used before an exchange occurs.

Interception during an exchange can allow a malicious cyber actor to use a legitimate key or secret to impersonate a user or gain access to a resource without detection. Organisations need to ensure the exchange mechanism used provides confidentiality and integrity, as well as ensuring that any indication of compromise results in the organisation implementing their rollover procedures.

Rollover and destruction

Rollover is the process of generating and using a new key or secret to replace one already in use. Destruction is the process of permanently removing all traces of key and secret material when they are no longer needed. Before destruction, organisations need to consider the need to still validate, decrypt or access data protected by end-of-life keys and secrets. These may need to be stored and protected beyond the intended use life cycle. Rollover can be executed due to several different triggers including key or secret compromise, certificate expiration, vulnerability as a result of use or age, insufficient key length, or other identified vulnerabilities in the generation or use of a key or secret. The process normally includes adding a new key or secret to a service while continuing to use the earlier one. This allows services and users a chance to rollover, beginning the use of the new key while both keys are present, and then at a future advised time the initial key or secret is removed.

Key rollover can be scheduled (routine) or unscheduled, due to any of the triggers listed in the organisations KMP. Frequency of rollover needs to manage the risks of lifetime vs those that arise during rollover; more frequent rollovers does not translate to increased security, however rollover procedures should be practiced and tested so operational issues are unlikely to arise during necessary rollovers. Unplanned events such as compromise or missed expiry dates will mean immediate rollover is required, which may cause disruption as end users or services migrate to the new key or secret.

From the moment key or secret material is generated it is vulnerable to compromise, until the point at which it is no longer used and destroyed. The rate at which a key or a secret age depends on several factors, according to its intended purpose; thus, any decisions on the longevity of a generated key or secret will be unique to each organisation and should be included in their KMP. Rollovers need to be planned and managed to avoid synchronisation and other risks.

Chains of trust

Chains of trust are important for establishing and maintaining security and integrity. A chain of trust establishes trust between entities by verifying digital certificate validity. The hierarchical structure of a chain of trust enables it to verify the authenticity and integrity of digital certificates, assure that the identity of entities involved in the communication can be trusted and that the transmitted data is secure.

A chain of trust can be described as a hierarchical trust model in that it is composed of one root Certificate Authority (CA) and one or more intermediate CAs. Intermediate CAs provide redundancy, while the root CA is usually offline. This means that even if the intermediate CA is compromised, the root CA can revoke the intermediate CA.

The following diagram shows the standard chain of trust. By trusting a certificate above a dashed line, inherent trust is given to all certificates below that dashed line.

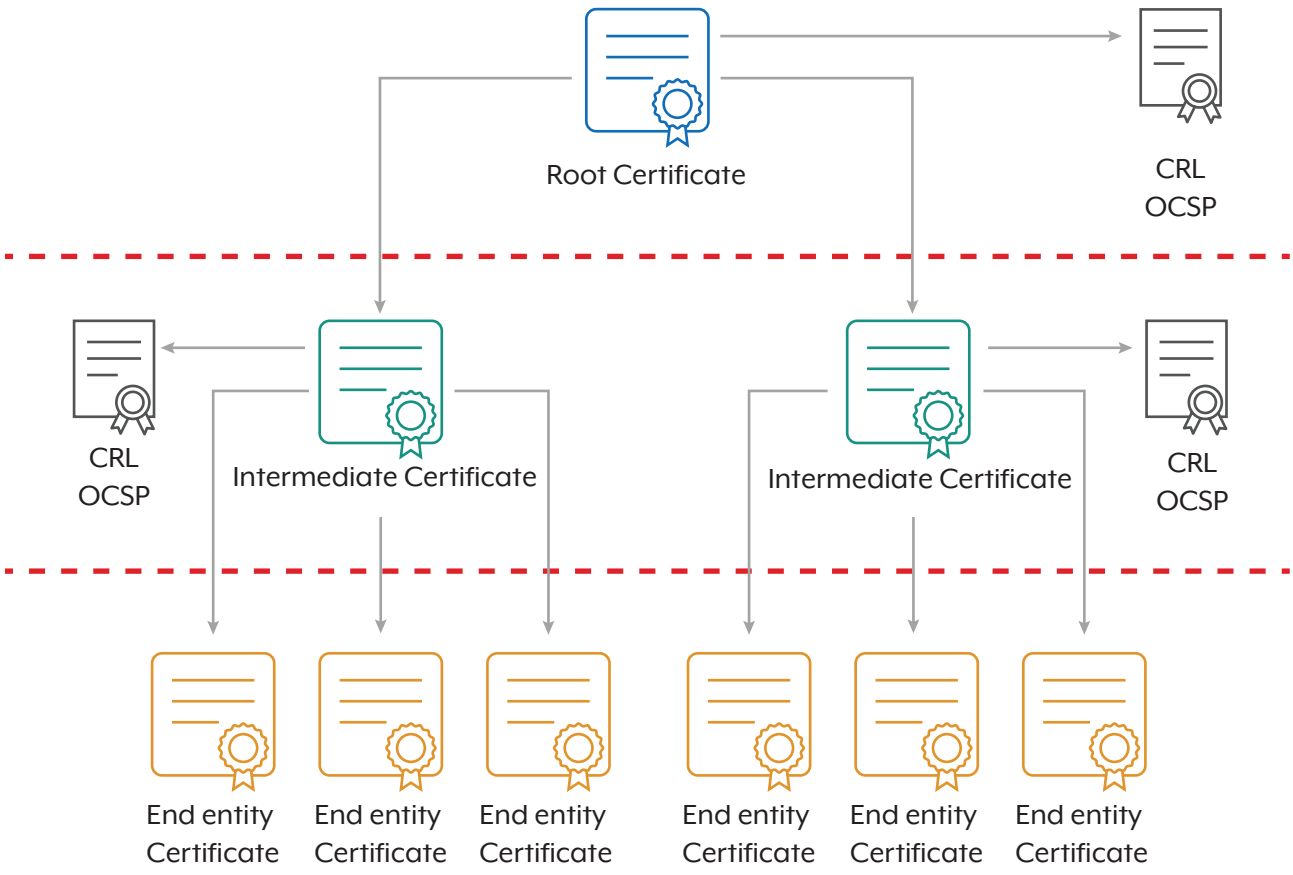


Figure 2. PKI Chain of trust

The following outlines an established best-practice approach in creating a chain of trust:

- **Certificate validation:** The first step is to validate the certificates in the chain. This involves verifying the digital signatures on each certificate using the public key of the issuing CA. The certificates are checked for tampering, ensuring that the information has been kept the same since the certificate was issued. If any certificate fails the validation process, the chain of trust is broken.
- **Chain of trust verification:** The chain of trust is verified by ensuring that the sequence of issuing CAs in the chain eventually leads to a trusted CA, an entry in the entity's list of trusted CAs. This ensures that the intermediate CAs in the chain are trusted, and that the certificate being validated can be trusted.
- **Certificate expiration check**: Each certificate in the chain has an expiration date. The client software checks that the certificates are valid within their specified time frame. An expired certificate is considered invalid and cannot be trusted. If any certificate in the chain has expired, the chain of trust is broken.
- **Revocation checking:** Revocation checks ensure that the issuing CA has not revoked a certificate before its expiration date. Certificates can be revoked for various reasons (that is compromise or suspicion of fraudulent activity). The most common methods for revocation checks are:
  - C**ertificate revocation lists (CRLs)** - contains a list of identifiers of certificates signed by the CA's private key, that have been revoked. If the CA's certificate is renewed with a new key pair, the CA maintain two separate CRLs - one for each key pair maintained by the CA.
  - **Online certificate status protocol (OCSP)** - provides a responder service that can either connect directly to a CA database or inspect the CRLs published by the CA to provide a signed statement attesting to the revocation status of a specific certificate.
- **Root certificates:** Are a self-signed digital Root Certificate Authorities (Root CAs).and are required to establish trust in certificate chains. These Root CAs are normally pre-installed in operating systems or hardware and are inherently trusted. The certificates in the chain are validated by the chain of trust.

By trusting an intermediate or root certificate, a chain of trust is established that allows systems and users to establish trust by presenting a digital signature connected to their public certificate signed by a certificate in the chain. This can provide access and authorisation to resources. All trusted certificates need to be monitored for misuse. Certificate expiry dates need to be set to an appropriate timeframe, checked on each used and renewed in a timely manner or revoked if compromise is detected. This includes revoking the trust of any certificate signed by a compromised certificate. Establishing trust with a malicious intermediate certificate can allow malicious cyber actors to create new end entity certificates and gain unauthorised access to systems and resources. Organisations must validate that only verified public certificates are trusted.

Positions of trust

A position of trust (Position of trust | Cyber.gov.au) is one that involves duties that require a higher level of assurance. Positions of trust can include, system administrators, privileged users or those with access to high-value keys and secrets. Positions within an organisation that have access to keys and secrets have a significant number of additional responsibilities that they are required to perform to keep the keys and secrets they control secure. Some of these responsibilities are outline in Appendix: Positions of Trust.

The people in these positions often also have access to critical systems, data and infrastructure. This makes them more of a target for cyber-attacks and increases the risk of potential insider threats. If a person in a position of trust is compromised or acts maliciously, there can be severe operational, financial and reputational consequences for an organisation.

Cyber security relies on the trust and integrity of those who have access to sensitive data, therefore individuals in positions of trust need to be reliable and responsible enough to have such access. Due to the heightened risk, these positions require additional screening measures beyond a standard background check in order to ensure that a minimum level of trust and integrity is upheld by all staff who have access to organisational keys and secrets.

Individuals in these positions must remain vigilant and engaged in cyber security efforts, by proactively identifying and mitigating potential risks as they arise. Overprivileged users can use their access to undertake malicious acts. These users can change, damage or expose data using the keys and secrets they have access to. Similarly, applications or systems can be abused to exploit the keys, secrets and access they have.

While some positions of trust are necessary, they should be limited by following the principle of least privilege and with separation of duties, along with regular revalidation that the privileged access is necessary. When privileged access goes unchecked for long periods of time, it can lead to significant organisational data compromise.

Oversight

Organisations should prescribe the audit and monitoring reporting requirements, circumstances, roles, responsibilities, facilities, and methods for auditing key and secret material. The audit requirements will depend on the sensitivity of the resources being protected or accessed. Audits should include the facilities that distribute or receive keys and secrets and the devices that are used for generation, storage and execution. Monitoring activities of keys and secrets needs to include certificate statuses, expiration dates and any indicators of compromise. However, care should be taken not to log sensitive key or secret information that could be abused if the monitoring system were to become compromised. Alerts raised from monitoring need to trigger appropriate remedial actions when required, such as rollover or revocation. The auditing and monitoring elements should be used to detect and prevent unauthorised access or misuse of keys and secrets.

Appendix

Glossary

Term	Definition
Asymmetric key	Two related keys – a public and private key, which are used to perform complementary operations, such as encryption, decryption, signature generation, or signature verification.
Ciphertext	Encrypted, non-human readable information.
Cryptographic material	All material, including documents, devices, or equipment that contains cryptographic information and is essential to the encryption, decryption, or authentication of telecommunications.
Data integrity	The assurance that data has been created, amended or deleted only by authorised individuals.
Decryption	The process of converting ciphertext back into plaintext.
Digital certificate	An electronic document used to identify an individual, a system, a server, a company, or some other entity, and to associate a public key with the entity. A digital certificate is issued by a certification authority and is digitally signed by that authority.
Digital signature	A cryptographic process that allows the proof of the source (with non-repudiation) and the verification of the integrity of data.
Secure Enclave/Vault	A dedicated piece of hardware or software specifically designed and built to provide high levels of protection to the data stored within.
Encryption	The conversion of plaintext into unreadable ciphertext (typically using cryptographic algorithms and keys) to protect the confidentiality of data at rest or in transit. Ciphertext is returned to plaintext by performing decryption.
Entropy	A measure of the amount of randomness or uncertainty.
Ephemeral key	A temporary cryptographic key used for a single session or transaction and then discarded.
Hardware Security Module (HSM)	A physical computing device that safeguards cryptographic keys and provides cryptographic processing. A HSM is or contains a cryptographic module. HSMs are commonly deployed in Public Key Infrastructure, digital identity solutions and payment systems.
Hash function	A function that converts data to a fixed length output whose properties include: • one-way - it is computationally infeasible to find any input that maps to any new pre-specified output • collision-resistant - it is computationally infeasible to find any distinct inputs that map to the same output

Term	Definition
Key management	The use and management of cryptographic keys, secrets and associated hardware and software. It includes their generation, registration, distribution, installation, usage, protection, storage, access, recovery and destruction.
Key rollover	The process of generating and using a new key (symmetric key or asymmetric key pair) to replace one already in use.
Key space	The total number of possible keys that can be generated for a given cryptographic algorithm. A larger key space provides greater security.
Malicious cyber actor	Refers to individuals, groups, or entities who intentionally cause harm or disruption to digital systems, networks, data, or other valuable assets.
No lone zone	A designated controlled area that can only be occupied by 2 or more people.
Non-repudiation	Providing proof that a user performed an action and in doing so, prevents the user from denying that they did so.
Plaintext	Unencrypted, human readable information.
Public Key Infrastructure (PKI)	A set of roles, policies, hardware, software and procedures needed to create, manage, distribute, use, store and revoke digital certificates and manage public-key encryption.
Secret	A confidential and controlled piece of data typically used for machine-to-machine access or authorisation, such as an API key.
Security domain	A system or collection of systems operating under a consistent security policy that defines the classification, releasability and special handling caveats for data processed within the domain.
Software Security Module (SSM)	A dedicated piece of software that provides greater security measures for storing and processing keys and secrets.
Symmetric key	A cryptographic key that is used to perform both a cryptographic operation and its inverse: that is. encryption and decryption or creating a message authentication code or verifying a message authentication code.

Positions of trust

A position of trust is one that involves duties that require a higher level of assurance when working with keys and secrets. Organisations may need to consider these and other positions and activities unique to their context when creating their KMPs.

Table 2: Positions of trust activities

Position	Activities
Crypto custodian	• Access the safes containing cryptographic material • Conduct safe audit as required • Manage HSM function and keys • Store backup private key passwords • Safe-hand all cryptographic material • Escort staff requiring access to a physical security domain for support and networking purposes, and during the key signing ceremonies • Witness all security domain activities • Conduct the crypto custodian steps in the key signing ceremonies • Have good technical understanding of crypto and security processes • Access security domain physical keys • Veto activities that are not documented and/or are contrary to established knowledge and procedures • Witness the key signing ceremonies in a security domain
Developer	• View production data and configuration, with the exception of secrets and key data, with a witness present • Develop code that interacts with keys and secrets
IT Security	• Manage cyber incident for the organisation • Holds backup material
Manager	• Authorise access and delegate responsibilities to any of the material or system as required either under normal conditions (written) or in emergencies (verbal). • Manage investigations of security activities with the security team
Physical security	• Hold universal access to building and break glass access to safes • Is the contact for safe passphrase change • Add/remove staff access • Manage organisational risk and assets • Field compliance framework enquiries

Position	Activities
PKI Manager	• Administer the PKI CA systems • Process requests for issuing, renewing, and revoking organisational certificates • Hand out the public key material for organisations to access the system • Register certificates • Manage certificates in the shared drive • Access the safes for media containing the private key material • Conduct safe audit as required • Sign receipt of crypto materials • Witness the generation of new key material • Safeguard material until relocated in the safes • Act as custodian of the private key materials during the key signing ceremonies
Security	• Conduct compliance and accreditation activities • Conduct other security activities as required • Investigate security incidents as directed by the security manager • Conduct audits of the PKI and HSMs as required
System administrator	• Access the IT equipment rooms • Access, monitor and make changes to the system • Access to administration keys and secrets • Hold key to secure server rooms
Technical specialist	• Provide HSM solutions and advice • Provide server advice • Manage server configurations • Prepare scripts for rebuilding servers • Provide technical support

References

NIST, SP 800-130: A Framework for Designing Cryptographic Key Management Systems

NIST, Personal Identity Verification (PIV) of Federal Employees and Contractors

NIST, Digital Signature Standard (DSS)

NIST, Security and Privacy Controls for Information Systems and Organizations

NIST, SP 800-57 Part 1 Rev. 5: Recommendation for Key Management: Part 1 – General

NIST, SP 800-57 Part 2 Rev. 1: Recommendation for Key Management: General Best Practices for Key Management

NIST, SP 800-57 Part 3 Rev. 1: Recommendation for Key Management, Part 3: Application-Specific Key Management Guidance

IETF, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

NIST, FIPS 140-3 Security Requirements for Cryptographic Modules

NIST, Transitioning the Use of Cryptographic Algorithms and Key Lengths

Supporting resources

Choosing Secure and Verifiable Technologies

Choosing Secure and Verifiable Technologies is a co-sealed publication led by ASD's ACSC. It provides organisations with advice and guidance on procuring digital products and services following secure by design practices and principles. For more information, please visit Choosing Secure and Verifiable Technologies | Cyber.gov.au.

Secure by Design Foundations

ASD's ACSC Secure by Design Foundations (the Foundations) have been designed for both technology manufacturers and consumers, to assist in the adoption of secure by design. Each Foundation identifies key areas of focus and associated mitigated risks. For more information, please visit Secure by Design Foundations | Cyber.gov.au.

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default

The Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and Default whitepaper is a co-sealed publication led by the Cybersecurity and Infrastructure Security Agency (CISA). It provides technology manufacturers with advice on developing products with secure by design and secure by default strategies. It is underpinned by three founding principles for technology manufacturing leaders: take ownership of customer security outcomes; embrace radical transparency and accountability; and lead from the top. For more information, please visit Shifting the Balance of Cybersecurity Risk | Cyber.gov.au.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website Commonwealth Coat of Arms Information and Guidelines | pmc.gov.au.

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre