17.9. Key Management

Objective

17.9.1. Cryptographic keying material is protected by key management procedures.

Context

Scope

17.9.2. This section covers information relating to the general management of cryptographic system material. Detailed key management guidance is not provided in this manual as there is a wide variety of cryptographic systems and technologies available, and there are varied security risks for each.

17.9.3. If High Assurance Cryptographic Equipment is being used agencies are required to comply with the NZCSI standards. This is outside of the scope of this section.

17.9.4. In a cloud environment, options for the management of cryptographic keys include on premises key generation and outsourcing the control of cryptographic keys to a cloud service provider.

17.9.5. A number of key management offerings, such as Hold Your Own Keys (HYOK), Bring Your Own Keys (BYOK), and Control Your Own Keys (CYOK), are available. However, the implementation and role designations often vary widely. As such, a single agreed definition of each may not always be practical or helpful when considering which key management option is most suited to an agency's requirements.

17.9.6. When considering key management options agencies need to consider the ownership, control, and possession aspects relating to cryptographic keys, and how these may impact security and business outcomes.

Applicability for cryptographic systems

17.9.7. In general, the requirements specified in the NZISM apply equally to cryptographic systems. Where the requirements for cryptographic systems are different, the variations are contained in this section, and take precedence over requirements specified elsewhere in the NZISM.

Background

17.9.8. Encryption is an unparalleled technology for the protection of information, but it relies on the strength of the algorithm, the strength of the key and, most importantly, strong key management.

17.9.9. All encryption has four important characteristics:

- the value of the data to be protected and the level of protection required to protect it,
- the algorithm used to encrypt the data,
- the protocol used to apply the algorithm, and
- the encryption key.

17.9.10. In almost all cases the algorithm is in the public domain and is not a secret. When an encryption algorithm is publicly available, security rests entirely on the secrecy of the encryption key. It is also true that the effectiveness of most encryption systems depends on the secrecy of the encryption key. Approved Cryptographic Algorithms are described in Section 17.2. and Approved Cryptographic Protocols (applying the algorithms) are described in Section 17.3. These sections also specify key strengths to resist attempts to compromise the key through cryptanalysis.

17.9.11. While any algorithm can, theoretically, be broken through cryptanalysis, this may require the use of vast computing power and other resources, making this approach infeasible. If, however, the encryption key is compromised, there is no need to attack the algorithm itself. Attacks on encryption systems will likely target the weakest point, most frequently these are the safeguards that are used to protection the key. Attempts to compromise keys and key management are more likely and more efficient than attacks on the algorithm itself. This is why strong key management is vital in order to protect the encryption key and keep the key secure and secret. When key management fails, cryptographic security is compromised.

17.9.12. Almost all internet security protocols use cryptography for authentication, integrity, confidentiality, and non-repudiation. It is vital that good key management is implemented if these security protocols are to be protected, considered reliable, and provide required levels of assurance to

organisations and users.

17.9.13. In some cases, trusted third-party key management service providers furnish assistance to agencies in the generation, storage, operation, management, and retirement of keys associated with the agency.

Key management

17.9.14. For encryption to be used effectively, the encryption keys must be managed and protected with the same care and security as the data originally encrypted, as long as the same key is being used to decrypt or recover data.

17.9.15. Key management encompasses the operations and tasks necessary to create, protect, and control the use of cryptographic keys. The process from creation to destruction of the encryption key is described as the key management life cycle.

Key management life cycle

17.9.16. The key management lifecycle covers:

- key generation,
- key registration,
- secure key storage,
- key distribution and installation,
- key use,
- key rotation,
- key backup (operational, backup and archive),
- key replacement and reissue,
- key recovery,
- key revocation,
- key suspension,
- key retirement, and
- key destruction.

Open networks

17.9.17. Open networks, by definition, seek to establish arbitrary connections without there necessarily being a pre-existing relationship. Protocols have been developed to manage this requirement through key exchange protocols and through trusted agents, most often a National Authority or Certificate Authority. Again it is important that approved protocols and algorithms, as specified in this document, are used. Refer to sections 17.2 Approved Cryptographic Algorithms and 17.3 Approved Cryptographic Protocols.

Public key infrastructure

17.9.18. Public key infrastructure (PKI) is the system used to create, issue, manage, and revoke digital certificates and their associated cryptographic keys. PKI has many different applications, and typically is used for encrypting and digitally signing data in order to authenticate and protect data in transmission, and supporting confidentiality and privacy. It is used extensively in ecommerce, internet banking, and secure email as well as being a key element in protecting website traffic.

Outsourcing key management

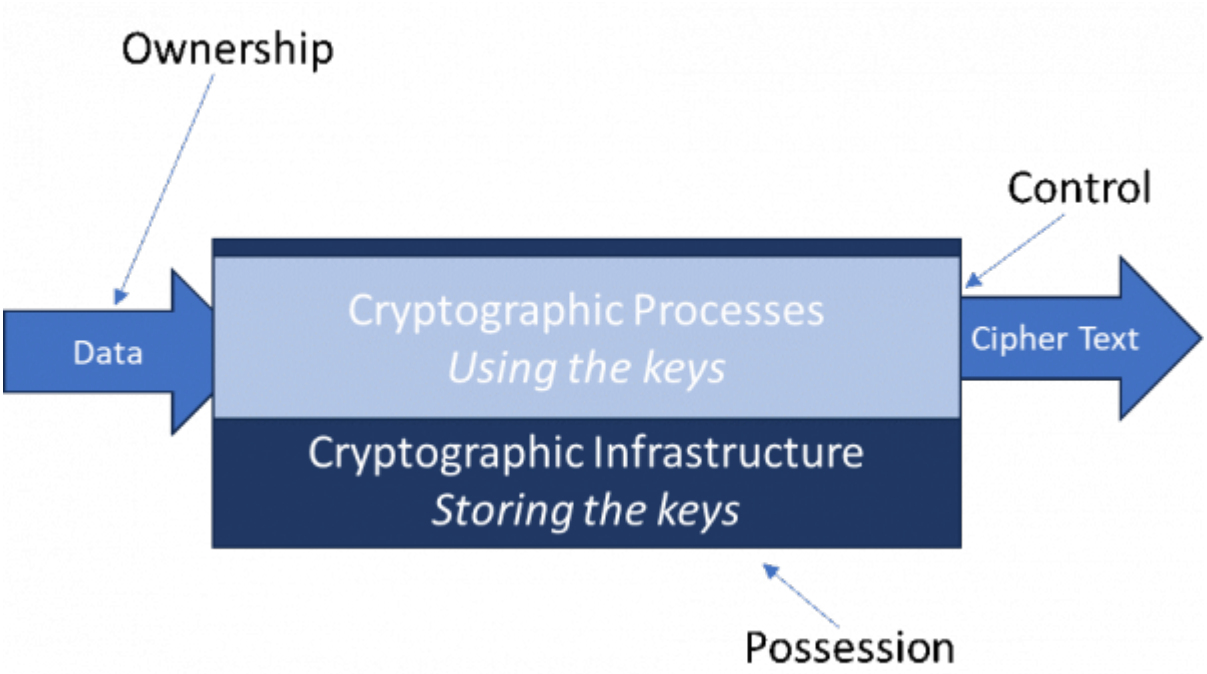
17.9.19. The goal of key management, both for use within an organisation or in the cloud, is to enable data encryption by securing access to cryptographic keys. This includes using a combination of cryptography and secure hardware to generate keys securely, to manage access and destruction of keys.

17.9.20. As stated previously, the ownership, control, and possession are three key aspects relevant to key management. Understanding the differences between them will assist evaluating different key managements that meet an agency's requirements.

17.9.21. For the purpose of this section these are defined as follows:

Owner ship	Specifies to whom the cryptographic keys belong. This is usually the custodian. Ownership of the key applies to the owner of the encrypted data, the owner of the encryption and/or decryption process, and the owner of the key infrastructure.
Control	Specifies who carries out key management lifecycle tasks, including having the option of precluding others from doing these tasks.
Possess ion	Specifies ownership of the infrastructure or location where the keys and encrypted data physically reside.

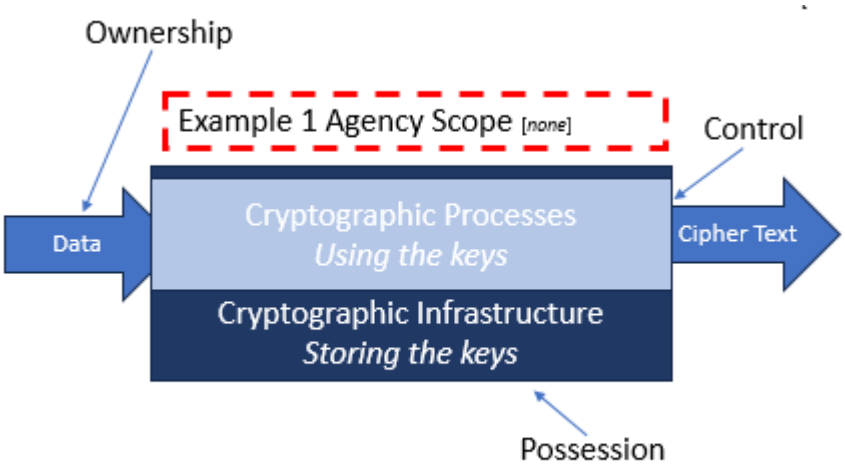
17.9.22. The following diagram depicts the relationship between ownership, possession, and control aspects within the key management process, including the likely points within it, where the aspects would be positioned. Subsequent paragraphs expand on these concepts by applying them to specific scenarios.



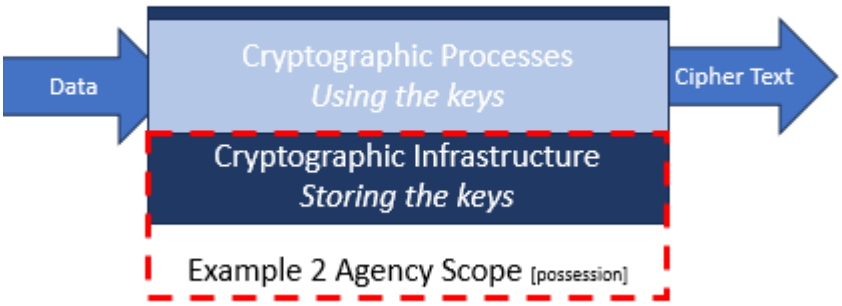
Commonly used key management scenarios

17.9.23. Within industry a number of approaches are available to manage end users' cryptographic keys. There are variations in how these may be defined, therefore an awareness around how role attribution is allocated within a provider's own key management offering is an important consideration when deciding on a solution.

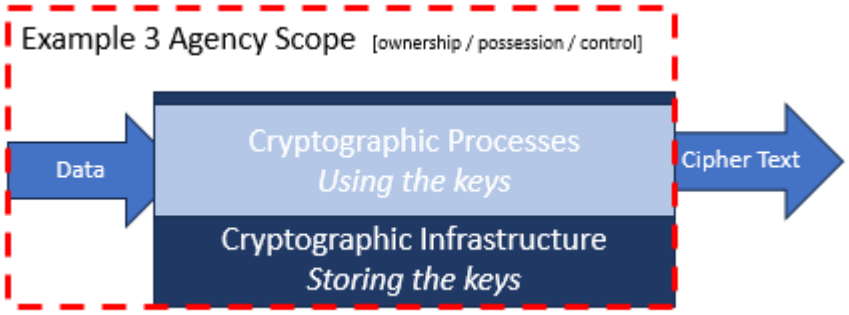
Example 1: The provider generates, manages, and stores the encryption and decryption keys. This option may reduce the amount of overhead an agency outlays compared to if they maintain their own key infrastructure. However, if an agency changes providers this may present challenges around compatibility, as well as financial implications.



Example 2: The customer generates and manages encryption keys, and the cloud provider can access the keys to encrypt and decrypt the customer's data. This option may reduce the level of control an agency has over the confidentiality of their data. A key consideration for choosing this option is likely to be the sensitivity of the data to be stored.



Example 3: An Agency generates and manages encryption keys including its storage. Data encryption occurs prior to movement into a cloud environment. The provider does not have access to file content. This option may be more suitable for agencies that require greater security around sensitive data. The cloud environment is used for storing the customer's encrypted data.



17.9.24. The following includes considerations that should form part of a technical evaluation when deciding on a key management solution.

- The value of data to be stored including protection requirements for that data.
- Whether the key management solution can be integrated with other data storage services.
- The number and types of keys required to secure data and whether a provider can meet these expectations.
- Whether an externally generated key provides sufficient assurance than if the key was generated using on premises infrastructure.
- Whether keys can be automatically rotated.
- The level of investment, resourcing, and technology required to support and maintain a key management infrastructure.
- Whether a provider's key revocation process adequately meets agencies' expectations around the removal of access to data.

Risks

17.9.25. There are a number of specific risks related to the management of cryptographic keys. These include:

- Keys exposed to unauthorised persons or applications, potentially compromising the keys or data the encryption is protecting.
- Lost or unrecoverable cryptographic keys.
- Software based key management, which provides only limited protection.
- Fragmented key management as new systems are introduced such as when changes occur to the physical custody of hardware outside of a trusted environment.
- Poorly documented and understood key management processes and activities increasing the possibility of compromise and potentially increasing compliance costs.
- Inadequate separation of duties within the ownership, control, and possession of keys, resulting in non-compatible duties being allocated to the same party, potentially resulting in unauthorised access of tenancy data.
- Lack of interoperability if an agency's key management infrastructure is not compatible with that offered by a cloud service provider.

17.9.26. Several factors should be understood and assessed conjointly to enable decisions on which key management option is most suitable for security and business requirements. These factors include:

- scenario,
- consideration,
- risk,
- business and/or security priority, and
- outsource aspect.

17.9.27. The following table provides an example of how the factors listed above can be considered collectively when undertaking a technical evaluation. It may also be useful when developing key or risk management plans. It is not intended to be definitive, but rather to assist agencies evaluate different key management options.

Scenario	Consideration	Risk	Security and/or business priority	Outsource aspect
Agency generated and management of encryption keys including its storage.	Inadequate separation of duties within the ownership, control, and possession of keys, resulting in non-compatible duties being allocated to the same party, potentially resulting in unauthorised access of tenancy data.	Keys exposed to unauthorised persons or applications, potentially compromising the keys or data the encryption is protecting.	Sensitivity and value of the data. This is summarised by the classification of the data but may not always reflect the values of aggregation, cost of compliance breaches, or reputation damage from a breach.	Control
Agency generates the key, and it is migrated to a cloud where the provider can use the keys to perform encryption and decryption operations.	Whether the key management solution can be integrated with other data storage services.	Lack of interoperability if an agency's key management infrastructure is not compatible with that offered by a cloud service provider.	The variety of key types, data formats, algorithms, protocols, and sources.	Possession
Cloud provider generates, manages, and stores keys used to encrypt and decrypt data.	Whether an externally generated key provides sufficient assurance than if the key was generated using on premises infrastructure.	Poorly documented and understood key management processes and activities increasing the possibility of compromise and potentially increasing compliance costs.	Sensitivity and value of the data. This is summarised by the classification of the data but may not always reflect the value of aggregation, cost of compliance, breaches, or reputation damage from a breach.	Ownership

Prioritisation

17.9.28. Prioritisation helps identify and manage requirements for the use and management of cryptography and key management systems. This will determine the extent and complexity of the key management programme. Important aspects to consider are:

- Sensitivity and value of the data. This is summarised by the classification of the data but may not always reflect the values of aggregation, cost of compliance breaches or reputation damage from a breach.
- The volume of data and keys.
- The variety of key types, data formats, algorithms, protocols and sources.
- The speed and frequency of transactions, requirements for data access and availability.

References

17.9.29. Further information on key management can be found in the following references:

Title	Publisher	Description and source
Common key management system models for the cloud	CRYPTOMATHIC	Explains the four primary cloud KMS pattern combinations, and their suitability depending on an organisation's requirements. Common Key Management System Models for the Cloud (cryptomathic.com)
Options for key management in the cloud	CSA	Provides guidance and description around different key management patterns. https://cloudsecurityalliance.org/blog/2022/03/24/ownership-control-and-possession-options-for-key-management-in-the-cloud/
Choosing and configuring a KMS for secure key management in the cloud	NCSC/UK	How to choose, use, and configure cloud services safely and what security risks need to be considered. Choosing and configuring a KMS for secure key management... - NCSC.GOV.UK
ISO/IEC 11770 Information Technology – Security Techniques – Key Management	ISO / IEC	ISO/IEC 11770-1:2010 - Information technology — Security techniques — Key management — Part 1: Framework
Guidelines for Cryptographic Key Management	IETF	RFC 4107 - Guidelines for Cryptographic Key Management (ietf.org)
Key management and key establishment	NIST	Key Management | CSRC (nist.gov)
Key management interoperability specification and profile	OASIS	Key Management Interoperability Protocol Specification and Key Management Interoperability Protocol Profiles OASIS Standards published - OASIS Open (oasis-open.org)

Rationale & Controls

Developing key management plans

17.9.30.R.01. **Rationale**

Most modern cryptographic systems are designed to be highly resistant to cryptographic analysis, and it should be assumed that a determined attacker could obtain details of the cryptographic logic. Cryptographic system material is safeguarded by implementing a key management plan (KMP) encompassing personnel, physical, and information security.

17.9.30.R.02. **Rationale**

Depending on the security requirements of an agency, different key management models or combination of models may be adopted to allocate the ownership, control, and possession for keys. It should be noted that the greater the sharing model adopted the less control of keys an agency may have.

17.9.30.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3016]

Agencies SHOULD assess the risks associated around key ownership, possession, and control against their own security and business requirements.

17.9.30.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3018]

Agencies SHOULD develop a KMP when they have implemented a cryptographic system using commercial grade cryptographic equipment.

17.9.30.C.03. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3017]

The level of detail included in a KMP MUST be consistent with the criticality and classification of the information to be protected.

Contents of key management plans

17.9.31.R.01. **Rationale**

When agencies implement the recommended contents for KMPs they will have a good starting point for the protection of cryptographic systems and their material within their agencies.

17.9.31.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3021]

The table below describes the minimum contents which SHOULD be documented in the KMP.

Topic	Content
Objectives	• Objectives of the cryptographic system and KMP, including organisational aims. • Refer to relevant NZCSIs.
System description	• The environment. • Maximum classification of information protected. • Topology diagram(s) and description of the cryptographic system topology including data flows. • The use of keys. • Key algorithm. • Key length. • Key lifetime.
Roles and administrative responsibilities	• Documents roles and responsibilities, including, if relevant, the COMSEC custodian, cryptographic systems administrator, record keeper, cloud service provider, and auditor.
Accounting	• How accounting will be undertaken for the cryptographic system. • What records will be maintained. • How records will be audited.
Classification	• Classification of the cryptographic system hardware. • Classification of cryptographic system software. • Classification of the cryptographic system documentation.
Information security incidents	• A description of the conditions under which compromise of key material should be declared. • References to procedures to be followed when reporting and dealing with information security incidents.
Key management	• Who generates keys. • How keys are delivered. • How keys are received. • Key distribution, including local, remote and central. • How keys are installed. • How keys are transferred. • How keys are stored. • How keys are recovered. • How keys are revoked. • How keys are destroyed. • Each time key information or material is accessed, details are captured in logs. • Approved access lists to cryptographic keys.
Maintenance	• Maintaining the cryptographic system software and hardware. • Destroying equipment and media.
References	• Vendor documentation. • Related policies.

Accounting

17.9.32.R.01. **Rationale**

As cryptographic equipment, and the keys they store, provide a significant security function for systems it is important that agencies are able to account for all cryptographic equipment.

17.9.32.C.01. **Control System Classifications(s): Secret, Confidential, Top Secret; Compliance: Must** [CID:3024]

Agencies MUST be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue.

17.9.32.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3025]

Agencies SHOULD be able to readily account for all transactions relating to cryptographic system material including identifying hardware and all software versions issued with the equipment and materials, including date and place of issue.

Audits, compliance and inventory checks

17.9.33.R.01. **Rationale**

Cryptographic system audits are used as a process to account for cryptographic equipment.

17.9.33.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3028]

Agencies MUST conduct audits using two personnel with cryptographic system administrator access.

17.9.33.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3029]

Agencies SHOULD conduct audits of cryptographic system material:

- on handover/takeover of administrative responsibility for the cryptographic system;
- on change of personnel with access to the cryptographic system; and
- at least annually.

17.9.33.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3030]

Agencies SHOULD perform audits to:

- account for all cryptographic system material; and
- confirm that agreed security measures documented in the KMP are being followed.

Access register

17.9.34.R.01. **Rationale**

Access registers can assist in documenting personnel that have privileged access to cryptographic systems along with previous accounting and audit activities for the system.

17.9.34.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3033]

Agencies MUST hold and maintain an access register that records cryptographic system information such as:

- details of personnel with system administrator access;
- details of those whose system administrator access was withdrawn;
- details of system documents;
- accounting activities; and
- audit activities.

Cryptographic system administrator access

17.9.35.R.01. **Rationale**

The cryptographic system administrator is a highly privileged position which involves granting privileged access to a cryptographic system. Therefore extra precautions need to be put in place surrounding the security and vetting of the personnel as well as the access control procedures for individuals designated as cryptographic system administrators.

17.9.35.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3036]

Before personnel are granted cryptographic system administrator access, agencies MUST ensure that they have:

- a demonstrated need for access;
- read and agreed to comply with the relevant Key Management Policy and Plan (KMP) for the cryptographic system they are using;
- a security clearance at least equal to the highest classification of information processed by the cryptographic system;
- agreed to protect the authentication information for the cryptographic system at the highest classification of information it secures;
- agreed not to share authentication information for the cryptographic system without approval;
- agreed to be responsible for all actions under their accounts;
- agreed to report all potentially security related problems to the GCSB; and
- ensure relevant staff have received appropriate training.

Area security and access control

17.9.36.R.01. **Rationale**

As cryptographic equipment contains particularly sensitive information additional physical security measures need to be applied to the equipment.

17.9.36.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3039]

Cryptographic system equipment SHOULD be stored in a room that meets the requirements for a server room of an appropriate level based on the classification of information the cryptographic system processes.

17.9.36.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3040]

Areas in which cryptographic system material is used SHOULD be separated from other areas and designated as a controlled cryptography area.

High assurance cryptographic equipment

17.9.37.R.01. **Rationale**

The NZCSI series of documents provide product specific policy for HACE.

17.9.37.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3043]

Agencies MUST comply with NZCSI when using HACE.

Transporting commercial grade cryptographic equipment & products

17.9.38.R.01. **Rationale**

Transporting commercial grade cryptographic equipment in a keyed state exposes the equipment to the potential for interception and compromise of the key stored within the equipment. When commercial grade cryptographic equipment is transported in a keyed state it needs to be done so according to the requirements for the classification of the key stored in the equipment.

17.9.38.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3048]

Unkeyed commercial grade cryptographic equipment MUST be distributed and managed by a means approved for the transportation and management of government property.

17.9.38.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3050]

Keyed commercial grade cryptographic equipment MUST be distributed, managed and stored by a means approved for the transportation and management of government property based on the classification of the key within the equipment.

17.9.38.C.03. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:3053]

Agencies SHOULD NOT transport commercial grade cryptographic equipment or products in a keyed state.