

Australian Standard[®]

**Electronic funds transfer—
Requirements for interfaces**

**Part 6.1.4: Key management—
Asymmetric cryptosystems—Key
management and life cycle**



This Australian Standard® was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 13 January 2009. This Standard was published on 11 February 2009.

The following are represented on Committee IT-005:

- Australian Association of Permanent Building Societies
 - Australian Bankers Association
 - Australian Electrical and Electronic Manufacturers Association
 - Australian Information Industry Association
 - Australian Payments Clearing Association
 - Australian Retailers Association
 - Reserve Bank of Australia
-

This Standard was issued in draft form for comment as DR 08013.

Standards Australia wishes to acknowledge the participation of the expert individuals that contributed to the development of this Standard through their representation on the Committee and through the public comment period.

Keeping Standards up-to-date

Australian Standards® are living documents that reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued.

Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments that may have been published since the Standard was published.

Detailed information about Australian Standards, drafts, amendments and new projects can be found by visiting www.standards.org.au

Standards Australia welcomes suggestions for improvements, and encourages readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.org.au, or write to Standards Australia, GPO Box 476, Sydney, NSW 2001.

Australian Standard[®]

**Electronic funds transfer—
Requirements for interfaces**

**Part 6.1.4: Key management—
Asymmetric cryptosystems—Key
management and life cycle**

First published as AS 2805.6.1.4—2009.

COPYRIGHT

© Standards Australia

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia GPO Box 476, Sydney, NSW 2001, Australia

ISBN 0 7337 9013 5

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems.

The objective of this Standard is to align Australian usage with world best practice and facilitate financial services interoperability.

This Standard is identical with, and has been reproduced from ISO 11568-4:2007, *Banking—Key management (retail)—Part 4: Asymmetric cryptosystems—Key management and life cycle*.

As this Standard is reproduced from an international standard, the following applies:

- (a) Its number appears on the cover and title page while the international standard number appears only on the cover.
- (b) In the source text ‘this part of ISO 11568’ should read ‘this Australian Standard’.
- (c) A full point substitutes for a comma when referring to a decimal marker.

References to International Standards should be replaced by references to Australian or Australian/New Zealand Standards, as follows:

<i>Reference to International Standard</i>		<i>Australian or Australian/New Zealand Standard</i>	
ISO		AS ISO/IEC	
10118	Information technology—Security techniques—Hash functions	10118	Information technology—Security techniques—Hash functions
		AS	
11568	Banking—Key management (retail)	2805	Electronic funds transfer—Requirements for interfaces
11568-1	Part 1: Principles	2805.6.1.1	Part 6.1.1: Key management—Principles
11568.2	Part 2: Symmetric ciphers, their key management and life cycle	2805.6.1.2	Part 6.1.2: Key management—Symmetric ciphers, their key management and life cycle
13491	Banking—Secure cryptographic devices (retail)	2805	Electronic funds transfer—Requirements for interfaces
13491-1	Part 1: Concepts, requirements and evaluation methods	2805.14.1	Part 14.1: Secure cryptographic devices (retail)— Concepts, requirements and evaluation methods
13491-2	Part 2: Security compliance checklists for devices used in magnetic stripe card systems	2805.14.2	Part 14.2: Secure cryptographic devices (retail)—Security compliance checklists for devices used in magnetic stripe card systems
ISO/IEC		AS/NZS ISO/IEC	
18033	Information technology—Security techniques—Encryption algorithms	18033	Information technology—Security techniques
18033-2	Part 2: Asymmetric ciphers	18033.2	Part 2: Asymmetric cryptosystems

Only international references or Australia/New Zealand Standards have been listed.

The term 'normative' is used to define the application of the annex to which it applies. A normative annex is an integral part of a standard.

CONTENTS

	<i>Page</i>	
1	Scope	1
2	Normative references	1
3	Terms and definitions.....	2
4	Uses of asymmetric cryptosystems in retail financial services systems.....	3
4.1	General.....	3
4.2	Establishment and storage of symmetric keys	4
4.3	Storage and distribution of asymmetric public keys	4
4.4	Storage and transfer of asymmetric private keys	4
5	Techniques for the provision of key management services	4
5.1	Introduction	4
5.2	Key encipherment.....	4
5.3	Public key certification.....	5
5.4	Key separation techniques	6
5.5	Key verification	6
5.6	Key integrity techniques	7
6	Asymmetric key life cycle	8
6.1	Key life cycle phases	8
6.2	Key life cycle stages — Generation	9
6.3	Key storage	12
6.4	Public key distribution	14
6.5	Asymmetric key pair transfer	14
6.6	Authenticity prior to use	16
6.7	Use.....	17
6.8	Public key revocation	17
6.9	Replacement.....	18
6.10	Public key expiration	18
6.11	Private key destruction	18
6.12	Private key deletion	19
6.13	Public key archive.....	19
6.14	Private key termination	19
6.15	Erasure summary.....	20
6.16	Optional life cycle processes	20
Annex A	(normative) Approved algorithms.....	21
Bibliography	22

INTRODUCTION

ISO 11568 is one of a series of International Standards describing procedures for the secure management of cryptographic keys used to protect messages in a retail financial services environment; e.g. messages between an acquirer and a card acceptor, or an acquirer and a card issuer.

This part of ISO 11568 addresses the key management requirements that are applicable in the domain of retail financial services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machines (ATM) transactions.

ISO 11568-2 and ISO 11568-4 describe key management techniques which, when used in combination, provide the key management services identified in ISO 11568-1. These services are:

- a) key separation;
- b) key substitution prevention;
- c) key identification;
- d) key synchronization;
- e) key integrity;
- f) key confidentiality;
- g) key compromise detection.

This part of ISO 11568 also describes the key life cycle in the context of secure management of cryptographic keys for asymmetric cryptosystems. It states both requirements and implementation methods for each step in the life of such a key, utilizing the key management principles, services and techniques described herein and in ISO 11568-1. This part of ISO 11568 does not cover the management or key life cycle for keys used in symmetric ciphers, which are covered in ISO 11568-2.

This part of ISO 11568 is one of a series that describes requirements for security in the financial services environment, as follows:

ISO 9564-1; ISO 9564-2; ISO 9564-3; ISO/TR 9564-4; ISO 11568; ISO 13491; ISO/TR 19038.

AUSTRALIAN STANDARD

Electronic funds transfer—Requirements for interfaces

Part 6.1.4:

Key management—Asymmetric cryptosystems—Key management and life cycle

1 Scope

This part of ISO 11568 specifies techniques for the protection of symmetric and asymmetric cryptographic keys in a retail financial services environment using asymmetric cryptosystems and the life cycle management of the associated asymmetric keys. The techniques described in this part of ISO 11568 enable compliance with the principles described in ISO 11568-1. For the purposes of this document, the retail financial services environment is restricted to the interface between:

- a card-accepting device and an acquirer;
- an acquirer and a card issuer;
- an ICC and a card-accepting device.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 9564-1, *Banking — Personal Identification Number (PIN) management and security — Part 1: Basic principles and requirements for online PIN handling in ATM and POS systems*

ISO/IEC 9796-2:2002, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*

ISO/IEC 10116:1997, *Information technology — Security techniques — Modes of operation for an n-bit block cipher*

ISO/IEC 10118 (all parts), *Information technology — Security techniques — Hash functions*

ISO 11568-1, *Banking — Key management (retail) — Part 1: Principles*

ISO 11568-2, *Banking — Key management (retail) — Part 2: Symmetric ciphers, their key management and life cycle*

ISO/IEC 11770-3, *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*

ISO 13491-1, *Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*

ISO 13491-2, *Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in financial transactions*

ISO/IEC 14888-3, *Information technology — Security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*

ISO 15782-1:2003, *Certificate management for financial services — Part 1: Public key certificates*

ISO/IEC 15946-3:2002, *Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment*

ISO 16609:2004, *Banking — Requirements for message authentication using symmetric techniques*

ISO/IEC 18033-2, *Information technology — Security techniques — Encryption algorithms — Part 2: Asymmetric ciphers*

ANSI X9.42-2003, *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*

3 Terms and definitions

For the purposes of this document, the definitions in ISO 11568-1, ISO 11568-2 and the following apply.

3.1

asymmetric cipher

cipher in which the encipherment key and the decipherment key are different, and in which it is computationally infeasible to deduce the (private) decipherment key from the (public) encipherment key

3.2

asymmetric cryptosystem

cryptosystem consisting of two complementary operations each utilizing one of two distinct but related keys, the public key and the private key, having the property that it is computationally infeasible to determine the private key from the public key

3.3

asymmetric key pair generator

secure cryptographic device used for the generation of asymmetric cryptographic keys

3.4

certificate

credentials of an entity, signed using the private key of the certification authority which issued it, and thereby rendered unforgeable

3.5

certification authority

CA

entity trusted by one or more entities to create, assign and revoke or hold public key certificates

NOTE Optionally the certification authority can create and assign keys to the entities.

3.6

communicating party

party that sends or receives the public key for the communication with the party that owns the public key

3.7

computationally infeasible

property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it

3.8**credentials**

identification data for an entity, incorporating at a minimum the entity's distinguished name and public key

NOTE Additional data can be included.

3.9**cryptoperiod**

time span during which a specific key is authorized for use or in which the keys for a given system may remain in effect

3.10**digital signature system**

asymmetric cryptosystem that provides for the creation and subsequent verification of digital signatures

3.11**hash function**

one-way function that maps a set of strings of arbitrary length on to a set of fixed-length strings of bits

NOTE A collision-resistant hash function is one with the property that it is computationally infeasible to construct distinct inputs that map to the same output.

3.12**independent communication**

process that allows an entity to counter-verify the correctness of a credential and identification documents prior to producing a certificate (e.g., call-back, visual identification, etc.)

3.13**key agreement**

process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key

3.14**key share**

one of at least two parameters related to a cryptographic key generated in such a way that a quorum of such parameters can be combined to form the cryptographic key but such that fewer than a quorum provide no information about the key

3.15**non-repudiation of origin**

property that the originator of a message and associated cryptographic check value (i.e., digital signature) is not able to subsequently deny, with an accepted level of credibility, having originated the message

4 Uses of asymmetric cryptosystems in retail financial services systems**4.1 General**

Asymmetric cryptosystems include asymmetric ciphers, digital signature systems and key agreement systems.

In financial services systems, asymmetric cryptosystems are used predominantly for key management; firstly for the management of the keys of symmetric ciphers, and secondly for the management of the keys of the asymmetric cryptosystems themselves. This clause describes these applications of asymmetric cryptosystems. Clause 5 describes the techniques employed in support of these applications relating to key management services and certificate management. Clause 6 describes how these techniques and methods are used in relation to the security and implementation requirements for the key pair life cycle.

4.2 Establishment and storage of symmetric keys

Keys of a symmetric cipher may be established by key transport or by key agreement. Mechanisms for key transport and key agreement are described in ISO/IEC 11770-3. The mechanisms used shall ensure the authenticity of the communicating parties.

Symmetric keys shall be stored as described in ISO 11568-2.

4.3 Storage and distribution of asymmetric public keys

The public key of an asymmetric key pair needs to be distributed to, and stored by, one or more users for subsequent use as an encipherment key and/or signature verification key, or for use in a key agreement mechanism. Although this key need not be protected from disclosure, the distribution and storage procedures shall ensure that key authenticity and integrity is maintained as defined in 5.6.1.

Mechanisms for the distribution of asymmetric public keys are described in ISO/IEC 11770-3.

4.4 Storage and transfer of asymmetric private keys

The private key of an asymmetric key pair does not necessarily need to be distributed to any entity. In some cases it can be maintained only within the secure cryptographic device (SCD) that generated it.

If it must be output from the SCD that generated it (e.g., for transfer to another SCD where it is to be used, or for backup purposes) it shall be protected from compromise by at least one of the following techniques:

- encipherment with another cryptographic key as defined in 5.2;
- if non-encrypted and outside an SCD, as key shares using an acceptable key segmentation algorithm (see clause 6.3.2.3 and Bibliography [8]);
- outputting into another SCD, which either is the SCD where it is to be used, or is a secure key transfer device intended for this use; if the communications path is not fully secured, then the transfer shall only be permitted inside a secure environment.

The integrity of the private key shall be ensured using one of the techniques defined in 5.6.2.

5 Techniques for the provision of key management services

5.1 Introduction

This clause describes the techniques that may be used, individually or in combination, to provide the key management services introduced in ISO 11568-1. Some techniques provide multiple key management services.

Asymmetric key pairs should not be used for multiple purposes. However, if a key pair is used for multiple purposes, e.g. digital signatures and encipherment, then special key separation techniques shall be employed which ensure that the system is not open to attack by transformations using the key pair. The selected techniques shall be implemented in an SCD. The functionality of the cryptographic device shall ensure that the implementation of a technique is such that the intended purpose of the technique is achieved.

The characteristics and management requirements for an SCD are defined in ISO 13491-1.

5.2 Key encipherment

5.2.1 General

Key encipherment is a technique whereby one key is enciphered using another key. The resulting enciphered key may then exist securely outside of an SCD. A key used to perform such encipherment is called a key encipherment key (KEK).

Two differing cases of key encipherment involving asymmetric keys and ciphers are described here:

- a) encipherment of a symmetric key using an asymmetric cipher;
- b) encipherment of an asymmetric key using a symmetric cipher.

5.2.2 Encipherment of a symmetric key using an asymmetric cipher

Encipherment of a symmetric key using the public key of an asymmetric cipher is typically used for the distribution of that key using a non-secure channel. The enciphered key may be a working key, or may itself be a KEK. Thus, mixed key hierarchies, as described in ISO 11568-2, may be created which incorporate the keys of both symmetric and asymmetric ciphers.

The symmetric key shall be formatted into a data block appropriate to the encipherment operation. As the block size of asymmetric ciphers tends to be larger than the key size of symmetric ciphers, it is usually possible to include more than one key in the data block for encipherment. Additionally, formatting information, random padding and redundancy characters shall be incorporated in the data block (see ISO/IEC 18033-2).

5.2.3 Encipherment of an asymmetric key using a symmetric cipher

Asymmetric keys may be enciphered using a symmetric cipher.

As the keys of asymmetric cryptosystems tend to be larger than the block size of symmetric ciphers, the asymmetric key may be formatted into multiple data blocks for encipherment. Therefore, the cipher block chaining mode of operation (see ISO/IEC 10116) or an equivalent operation shall be used for encipherment.

Due consideration shall be paid to known attacks when assessing the equivalent strength of various cryptographic algorithms. Generally an algorithm can be said to provide s bits of strength where the best-known attack would take, on average, $2^{s-1}T$ to attack, where T is the amount of time that is required to perform one encryption of a plaintext value and comparison of the result against the corresponding ciphertext value.

For example in ISO/IEC 10116, an attack against 112-bit TDEA is presented that requires $O(k)$ space and $2^{120-\log k}$ operations, where k is the number of known plaintext-ciphertext pairs. As discussed in reference [11], given 2^{40} known plaintext-ciphertext pairs, this reduces the strength of two-key (112-bit) TDEA to 80 bits. Recommended equivalent key sizes at the time of publication are given in Table 1. In assessing these numbers, consideration must be paid to any further developments in cryptanalysis, factoring and computing generally.

NOTE Currently, in the retail banking environment, where TDEA keys are used for protecting other keys, and are changed such that the collection of quantities of plaintext/ciphertext pairs sufficient to significantly weaken the underlying cipher is improbable, 112-bit TDEA can be considered to offer sufficient security for the protection of 168-bit TDEA and 2 048-bit RSA keys.

Table 1 — Encryption algorithms — Equivalent strengths

Effective strength	Symmetric	RSA	Elliptic curve
80	112-bit TDEA (with 2^{40} known pairs)	1 024	160
112	112-bit TDEA (with no known pairs)	2 048	224
	168-bit TDEA		

5.3 Public key certification

Key certification is a technique that, when used in accordance with ISO 15782-1, ensures the authenticity of a public key by creating a digital signature for the key and associated validation data. Prior to using the public key, a recipient checks its authenticity by verifying the digital signature.

The public key and associated validity data for the owner are together known as the owner's credentials. The validity data typically incorporates owner and key identification data, and key validity data (e.g., expiry date). A key certificate is issued by a trusted third party referred to as the Certification Authority. A key certificate is created by signing the owner's credentials using a private key owned by the Certification Authority and used only for this purpose.

An independent communication shall be used to verify that the identification of the key and its owner are correct and authorized. This may require confirmation obtained via a different channel from the one whereby the information was originally obtained.

During distribution to authorized recipients, or during storage in a key database, the authenticity of the public key shall be ensured.

5.4 Key separation techniques

5.4.1 General

In order to ensure that a stored key is useable only for its intended purpose, key separation for stored keys shall be provided by one or more of the following:

- a) physically segregating stored keys as a function of their intended purpose;
- b) storing a key enciphered under a key encipherment key dedicated to encipherment of a specific type of key;
- c) modifying or appending information to a key as a function of its intended purpose, prior to encipherment of the key for storage i.e., key tagging.

5.4.2 Key tagging

5.4.2.1 General

Key tagging is a technique for identifying the type of a key existing outside a secure cryptographic facility and the uses to which that key can be put. The key value and its privileges are bound together in a manner that prevents undetectable modifications to either.

5.4.2.2 Explicit key tagging

Explicit key tagging involves the use of a field containing information defining the limits of privilege for the associated key and key type. This field is bound together with the key value in a manner that prevents undetectable modifications to either.

5.4.2.3 Implicit key tagging

Implicit key tagging does not rely on the use of an explicit field containing information defining the limits of privilege for the associated key and key type, but rather relies on other characteristics of the system such as the position of the key in the record, or the associated functions to determine and limit the rights and privileges of the key.

5.5 Key verification

Key verification is a technique that allows the value of a key to be checked and verified, without exposing any secret values and without using public key certificates. The technique utilizes a key verification code (KVC) that is cryptographically related to the key via a collision-resistant one-way function. For example, the reference KVC may be computed as the hash of the public or private key and associated data using an algorithm defined in ISO/IEC 10118.

At any time following initial generation of the KVC, the key can again be input to the one-way function. If the resulting KVC is identical to the initial KVC, it is assumed that the value of the key is unchanged.

Key verification can be used to establish that one or more of the following conditions have been met:

- a) a key has been correctly entered into a cryptographic device;
- b) a key has been correctly received over a communications channel;
- c) a key has not been altered or substituted.

For public keys, as long as the KVC is distributed via an integrity-assured channel, the public key can be distributed via a non-secure channel. Prior to installing the public key for use, the user shall validate it by re-computing the KVC and comparing it with the reference KVC.

It shall be infeasible to modify or substitute the reference KVC and public key (and associated data) in such a way that the recomputed KVC of the modified/substituted public key (and associated data) equals the modified/substituted reference KVC. This can be achieved by either of the following:

— by ensuring the integrity of the KVC (see ISO 16609);

or

— by separately storing/distributing the reference KVC in such a way that modification/substitution of the reference KVC cannot be coordinated with modification/substitution of the public key (and associated data) (e.g., dual controls).

5.6 Key integrity techniques

5.6.1 Public key

One or more of the following techniques shall be used to ensure public key integrity:

- sign the public key and associated data using a digital signature system, thereby creating a public key certificate; key certificates, and the management of the keys used to create and verify the certificates, are described in 5.3 and Clause 6;
- create a MAC for the public key and associated data, using an algorithm defined by ISO 16609 and a key used only for this purpose;
- store the public key in an SCD (see ISO 13491-1 and ISO 13491-2);
- distribute the public key over an unprotected channel, and distribute a key verification code of the public key and associated data over an integrity assured channel such as an authenticated channel with dual controls. Key verification is described in 5.5;
- use authenticated encryption.

5.6.2 Private key

One or more of the following techniques shall be used to ensure private key integrity:

- create a MAC for the private key and associated data, using an algorithm defined by ISO 16609 and a key used only for this purpose;
- store the private key in an SCD (see ISO 13491-1 and ISO 13491-2);

- use authenticated encryption;
- store as integrity protected key shares;
- verify that the private key and the authenticated public key form a valid key pair, by firstly applying a transformation on arbitrary data using one of the keys and then applying the complementary transformation using the other key and then confirming the result against the expected result. This operation shall be wholly conducted within an SCD and all intermediate and final results of the transformation destroyed.

6 Asymmetric key life cycle

6.1 Key life cycle phases

The key life cycle consists of three phases:

- a) pre-use: during which the key pair is generated and may be transferred;
- b) use: during which the public key is distributed to one or more parties for operational use and the private key is retained in an SCD;
- c) post-use: during which the public key of a key pair is archived and the private key of a key pair is terminated.

A schematic overview of the private key (S) life cycle and the public key (P) life cycle are given respectively in Figures 1 and 2. The figures show how a given operation on a key changes its state. The life cycle of public key certificates can be found in ISO 15782-1.

A cryptographic key is considered to be a single object of which multiple instances may exist at different locations and in different forms. A clear distinction is made between the following operations:

- distribution of the public key to a communicating party (see 6.4);
- transfer of a key pair to its owner in an implementation where the party does not have the capacity to generate key pairs (see 6.5).

And also a clear distinction is made between:

- destruction of a single private key instance (see 6.11);
- deletion of a private key from a given location which implies destruction of all instances of this key at that location (see 6.12);
- termination of a private key, which implies deletion of the key from all locations (see 6.14).

Every operation performed on a key changes its state. This clause specifies the requirements for obtaining a given state or performing a given operation.

Requirements applying to specific life cycle stages are specified in 6.2.

NOTE 1 Requirements for archiving private keys for the purpose of subsequent decipherment of data that may have been encrypted under the corresponding public key are considered to be outside of the likely usage of this part of ISO 11568.

NOTE 2 The requirements hereafter could depend upon implementation of key pair generation. In particular, the requirements are different if the key pair is generated by a third party asymmetric key pair generator or if the owner generates and stores its key pair.

6.2 Key life cycle stages — Generation

6.2.1 General

The asymmetric key pair generation is the process by which a new pair of keys composed of a private key and the related public key is generated for use in a specific asymmetric cryptosystem. The two keys of an asymmetric key pair are mathematically related as defined by the design of the particular asymmetric cryptosystem. The relationship is such that it is computationally infeasible to determine the private key from the public key.

The key pair generation process is achieved by or on behalf of a single party. This party becomes the owner of the key pair.

Each private key and each private key component shall be generated in such a way that it is not feasible to predict any private key nor to determine that certain private keys are significantly more probable than others from the set of possible private keys. See Bibliography [4]. The process shall incorporate random or pseudo-random values.

An asymmetric key pair shall be generated in such a way that the secrecy of the private key and the integrity of the public key is assured. For the generation of an asymmetric key pair for non-repudiation service, the integrity of the public key and the secrecy of the private key shall be provable to a third party.

The private key shall not be available in human-comprehensible form.

If the key pair is generated by a system that will not use it:

- the private key and all related secret seed elements shall be deleted immediately after the transfer has been ensured;
- the integrity of the private key shall be ensured.

Asymmetric key pairs, when generated, should have a replacement date to establish their life cycle.

The size of the asymmetric key pair shall be chosen to be sufficiently large to render attacks computationally infeasible.

Generation of an asymmetric key pair shall be performed by a certification authority (CA), the key pair owner or an authorized third party. The roles and responsibilities of the entity performing the key pair generation are described in 6.2.2 to 6.2.4.

6.2.2 Certification authority

The CA shall generate the asymmetric key pair in an SCD and shall transfer the private key to the key pair owner in accordance with the requirements in 6.5. The CA shall transfer the public key to the key pair owner in a certificate.

The CA shall neither record nor retain the private key or any other information that could possibly compromise the private key or allow it to be recreated.

6.2.3 Key pair owner

The key pair owner shall generate the asymmetric key pair in an SCD and shall either:

- generate the key pair in the same cryptographic device in which it will be used;
- or
- securely transfer the private key from the device where it was generated into the device(s) in which it will be used.

The key pair owner shall retain as few copies of the private key as is operationally feasible.

NOTE The fewer the instances of the private key, the stronger the claim of non-repudiation, as there is a lower probability of compromise.

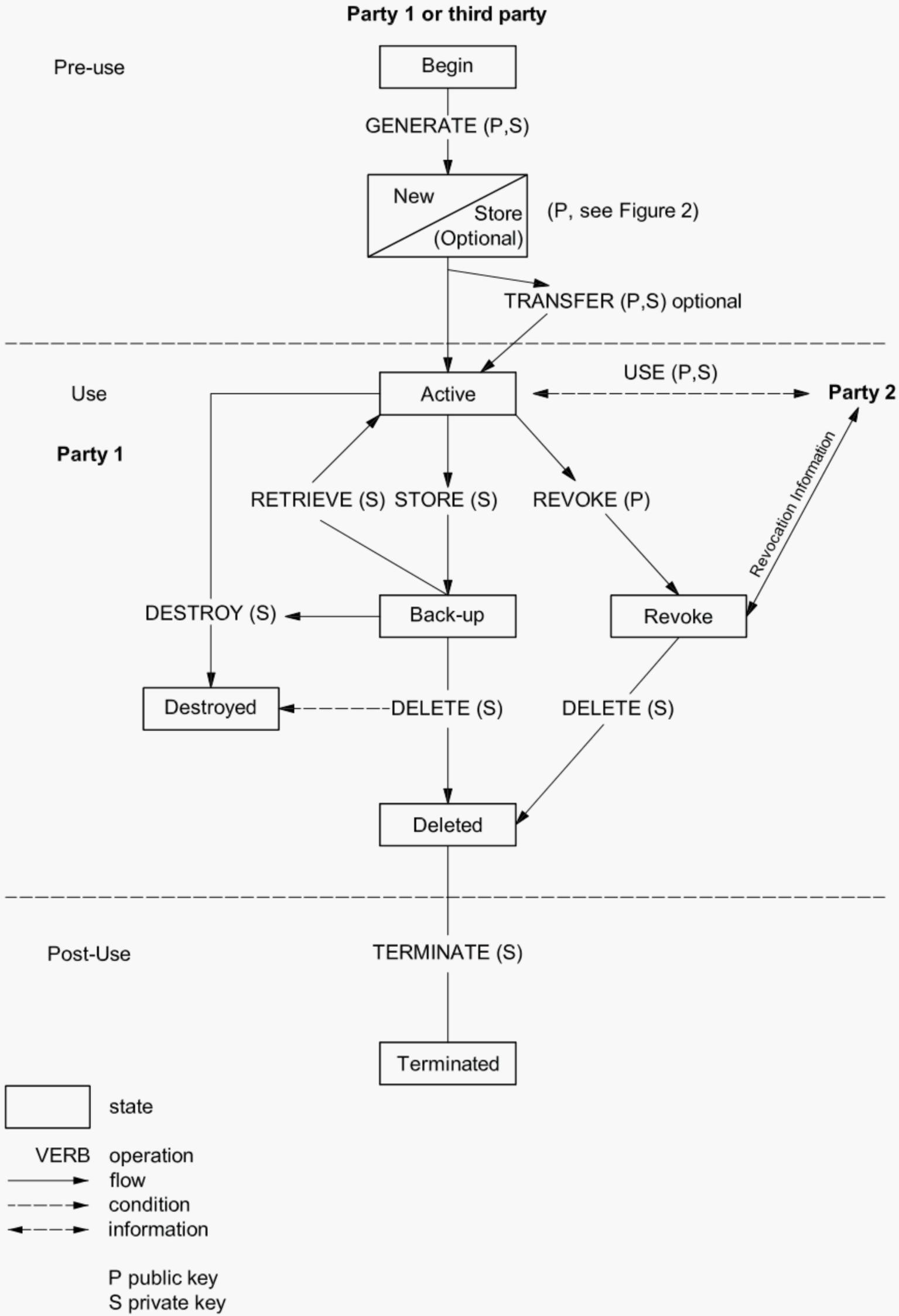


Figure 1 — Private key life cycle

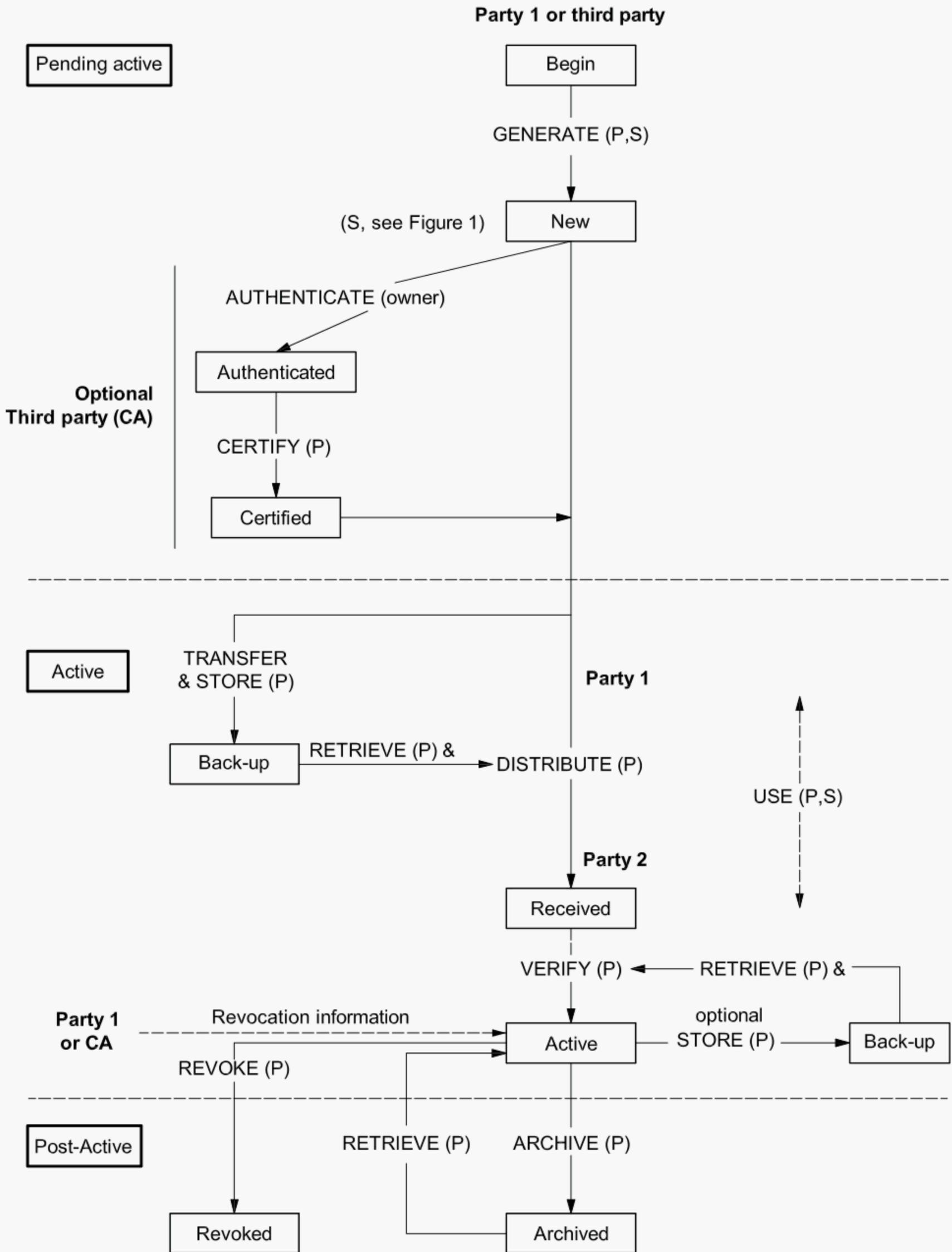


Figure 2 — Public key life cycle

6.2.4 Third party

The third party shall generate the asymmetric key pair in an SCD and shall transfer the private key to the key pair owner in accordance with the requirements in 6.5.

The third party shall transfer the public key to the key pair owner in accordance with the requirements in 6.5.2.

The third party shall neither record nor retain the private key or any other information that could possibly compromise the private key or allow it to be recreated.

6.3 Key storage

6.3.1 Introduction

During storage, keys shall be protected against unauthorized disclosure and substitution, and key separation shall be provided.

Storage of the private key requires that secrecy and integrity are ensured. Storage of the public key requires that authenticity and integrity are ensured.

6.3.2 Permissible forms for private keys

6.3.2.1 General

One of the following techniques shall be used to store private keys:

- a) plaintext key: in an SCD;
- b) key shares: in at least two shares, designed and managed so that no one individual can gain access to a quorum (the number of tokens required to reconstruct the key);
- c) enciphered keys: enciphered under a key encipherment key.

6.3.2.2 Plaintext private key

A plaintext private key shall exist only within an SCD. An SCD shall comply with the requirements as stated in ISO 13491-1.

6.3.2.3 Key shares

A private key existing in the form of at least two separate key shares shall be protected by the principles of split knowledge and dual control.

Access to fewer than the number of shares required to reconstruct the plain text private key shall give no information about the key. A key share shall be accessible only to that person or group of persons to whom it has been entrusted and only for the minimum duration required. A person with access to one share of the key shall not have access to any other share of that key.

Key shares shall be stored in such a way that unauthorized access has a high probability of being detected. If key shares are stored in enciphered form, all requirements for enciphered keys shall apply. Key shares may be stored in a key transfer device (see ISO 13491-2).

A key share shall be conveyed to authorized persons by means of a key mailer or key transfer device. If a key mailer is used, it shall be printed in such a way that the key share cannot be observed until the serialized envelope is opened. The envelope shall display the minimum data necessary to deliver the key mailer to the authorized person. A key mailer shall be constructed such that it is highly likely that accidental or fraudulent opening will be obvious to a recipient, in which case the key share shall not be used.

If a key share is in an insecure token (e.g., printed in plaintext inside a mailer), it shall be accessible to only one authorized person at only one point in time, and only for as long as required for the share to be entered into an SCD.

6.3.2.4 Enciphered private key

Encipherment of a key using a key encipherment key shall take place within an SCD.

The encipherment of a private key shall be implemented as specified in 5.2.3.

6.3.3 Permissible forms for public keys

6.3.3.1 General

In an asymmetric cryptosystem there is no secrecy requirement for the storage of the public key, but authenticity and integrity of this key shall be ensured.

It shall not be possible to substitute or alter any public key or associated information without detection.

A public key shall be stored either in plaintext or enciphered forms as detailed in 6.3.3.2 and 6.3.3.3 respectively.

6.3.3.2 Plaintext public key

When the public key is stored in plaintext as a certificate, the techniques described in Clause 5 shall apply for the production of this certificate.

When the public key does not appear as a certificate, it shall be stored with sufficient protection to ensure that the value of the key and its identity cannot be modified without detection as follows:

a) in plain text in an SCD designed to detect unauthorized key replacement;

or

b) in plain text using key verification techniques as defined in 5.5.

6.3.3.3 Enciphered public key

In some instances, the authenticity and integrity of a public key can be achieved by encipherment e.g., by inclusion of check values in the enciphered data. Such encipherment shall be as defined in 5.2.

6.3.4 Protection against substitution during storage

When plaintext public keys are stored and are not in the form of a certificate or when their certificate has been checked and they will be used without re-checking the certificate, integrity and authenticity shall be ensured by means described in 6.3.3 and by techniques described in Clause 5.

Protection against substitution of the public key during storage is essential. For example, the substitution of a public key used for encipherment may result in a threat to data secrecy.

One means of protecting a public key against substitution is to implement the same techniques as for a private key. Another means is to store the public key in a certificate, allowing verification of the key's integrity and authenticity before use.

The unauthorized substitution of stored public keys shall be prevented by one or more of the following means.

- a) Physically and procedurally preventing unauthorized access to the key storage area.
- b) Storing a key enciphered as a function of its intended use and ensuring that it is not possible to know both a plaintext value and its corresponding ciphertext enciphered under the key encipherment key.
- c) Storing a certificate containing a public key and verifying the certificate prior to its use. The authenticity and integrity of the public key used to verify the certificate shall be ensured.

If unauthorized key substitution is known or suspected, the public key shall be updated with the correct public key.

6.3.5 Provisions for key separation

In order to ensure that each key of an asymmetric key pair is only usable for its intended purpose, key separation for stored keys shall be provided by one or more of the following means.

- a) Physically segregating stored keys as a function of their intended purpose.
- b) Storing a key enciphered under a key encipherment key dedicated to encipherment of a specific type of key.
- c) Modifying or appending information to a key as a function of its intended purpose, prior to encipherment of the key for storage.
- d) For public keys, providing a certificate including the usage of the key.

6.3.6 Key back-up

Key back-up is the storage of a copy for the purpose of reinstating a key that is accidentally destroyed but the compromise of which is not suspected.

Back-up copies shall be held in one of the permissible forms of the key. All back-up copies of keys shall be subject to the same or greater level of security control as keys in current use.

Key back-up is ensured using the same principles and techniques as for key storage.

6.4 Public key distribution

Key distribution is the process by which a public key is conveyed to the party intended to use it.

Any distribution method (manual or automated) shall ensure the integrity and authenticity of the public key. The substitution of a public key during distribution shall be prevented. This can be achieved by maintaining the public key in the forms described in 6.3.3.

6.5 Asymmetric key pair transfer

6.5.1 Process

6.5.1.1 General

The asymmetric key pair transfer is the process by which the key pair and the certificate of the public key are conveyed to the owner of the key pair. This process occurs when the owner does not have the capacity to generate their key pair.

The owner shall be authenticated prior to being given their key pair.

The techniques used for public key distribution are described in 4.3.

The techniques used for protection against substitution during distribution are described in Clause 5.

The transfer of the public and private keys of an asymmetric key pair shall use one of the techniques described in this clause and summarized in Table 2.

Suitable techniques for transferring private and public keys are provided in ISO/IEC 11770-3.

Table 2 — Permissible asymmetric key pair transfer techniques

Key forms	Techniques		
	Manual	Electronic	
		Direct	Network
Plaintext key	P	P,S	P
Key shares	P,S	P,S	P
Enciphered keys	P,S	P,S	P,S
Certificate	P	P	P
P: Public key, S: Private key			

6.5.1.2 Plaintext private key

The general requirements for the transfer and loading of plaintext private keys are as follows.

- a) The key transfer process shall ensure the confidentiality and integrity of the plaintext key.
- b) The key transfer and loading processes shall be performed according to the principles of dual control and split knowledge.
- c) An SCD shall transfer a plaintext private key only when at least two authorized persons are authenticated by the device, e.g., by means of passwords.
- d) A plaintext private key shall be loaded into an SCD only when it can be assured that the device has not been subject to prior tampering which might lead to the disclosure of keys or sensitive data.
- e) A plaintext private key shall be transferred between SCDs only when it can be ensured that there is no tap at the interface that might disclose any element of the transferred key.
- f) When a device is used to transfer private keys between the cryptographic device that generates the key and the cryptographic device that will use the key, this device shall be an SCD. After loading of the key into the target device, the key transfer device shall not retain any information that might disclose that key.
- g) When a key transfer device is used, the key (and its identifier, if explicit key identification is used) shall be transferred from the cryptographic device that generated the key into the key transfer device. This portable device shall be physically transported to the cryptographic device that will actually use the key.

Appropriate custody shall be maintained over the key transfer device to ensure that the private key can only be transferred to the intended key-using device. The key (and its identifier) shall then be transferred from the key transfer device into the key-using device.

6.5.1.3 Private key shares

The key shares that will form the key shall be entered into the device manually or using a key transfer device.

The general requirements of the transfer and loading of private key shares are as follows.

- a) The key share transfer process shall not disclose any portion of a key share to an unauthorized person.
- b) Key shares shall be loaded into an SCD only when it can be assured that the device has not been subject to prior tampering which might lead to the disclosure of keys or sensitive data.
- c) Key shares shall be transferred into an SCD only when it can be ensured that there is no active or passive tapping mechanism at the interface that might disclose the transferred shares.
- d) The key transfer and loading process shall be performed according to the principles of dual control and split knowledge.
- e) The required quorum of key shares shall be entered individually by the holders of those key shares.

The key verification methods described in 5.5 may be used to verify correct key share entry. When the last share has been entered, the cryptographic device shall perform the action required to construct the key.

6.5.1.4 Enciphered private key

Enciphered keys may be transferred and loaded electronically via a communication channel. Encipherment of a key using a key encipherment key shall take place within an SCD. In this case, the requirements described in 5.2.3 shall apply.

The process of transferring enciphered private keys shall protect against key substitution and modification.

Key identifier and related data shall be transferred together with the private key.

6.5.2 Public key transfer

Public key transfer techniques shall ensure the authenticity of the key.

When the key pair is not generated by the key owner then, prior to the distribution of the public key, the correct transfer of the key pair should be verified. If performed, the verification shall occur by applying a transformation on arbitrary data using one of the keys and then applying the complementary transformation using the other key. The result shall then be confirmed against the expected result. This operation shall be wholly conducted within the SCD and all intermediate and final results of the transformation destroyed.

6.6 Authenticity prior to use

The authenticity and integrity of the public key shall be verified prior to each use or the public key shall be maintained in such a manner that the authenticity and integrity are ensured during operational use.

Certification may be used to provide this assurance (see 5.3). Alternatively, the methods described in 5.5 may be used.

6.7 Use

The use of asymmetric private and public keys is described in Clause 4.

In an asymmetric cryptosystem, each key of a key pair is used for separate functions. The following requirements address both keys of a key pair except where otherwise mentioned.

- a) Unauthorized use of a private key shall be prevented.
- b) A key shall be used for only one purpose, e.g., only authenticity or only confidentiality, except when used as described in 5.1.
- c) A key shall be used only for its intended purpose in its intended locations.
- d) Any private key shall exist in the minimum number of locations consistent with effective system operations.
- e) A key pair shall no longer be used at the end of the cryptoperiod or when the compromise of the private key is known or suspected.
- f) A public key should be used only when its authenticity and integrity have been verified and are correct.
- g) The secrecy and integrity of a private key shall be protected. Therefore, it shall not be used outside an SCD.
- h) Physical and logical controls shall be implemented to prevent unauthorized key use.
- i) The recipient of a public key shall verify its integrity and authenticity before use.

Clause 5 contains a list of techniques that should be used to obtain proper key separation and to verify integrity and authenticity of a public key.

Subsequent use of a key suspected of compromise shall be prevented by either:

- a) deleting the key from all operational locations;
- b) blocking the means used to obtain the key.

6.8 Public key revocation

Public key revocation is the process whereby the use of a public key is terminated for one of the following reasons:

- private key compromise;
- business reasons.

When a private key compromise is known or suspected, the corresponding public key shall be revoked as soon as practical. If the key pair under suspicion is used as a key encipherment key, then all keys which are hierarchically under it shall be terminated.

For business reasons, authorized entities may rescind the use of an asymmetric key pair. In this case, the public key shall be revoked.

Public key users shall be notified that a public key has been revoked and upon receipt of such notification shall cease using that public key. Such notification can be active, such as broadcasting to all public key users that a public key has been revoked, or passive, such as posting the revocation on a broadly accessible data base.

A public key that has been revoked may need to be used to verify information that has been previously signed, or may be needed for legal purposes and will be recovered from the archive.

6.9 Replacement

Key pair replacement is the process whereby a new key pair replaces a revoked or expired key pair.

Key replacement shall be implemented by repeating the appropriate key generation, transfer, distribution and loading procedures.

If the key pair has expired or is revoked due to business reasons, e.g., change of SCD ownership, replacement of the key pair may not be necessary or appropriate.

During key pair replacement, the key pair owner shall adhere to all of the requirements for key pair generation.

During key pair replacement, the key pair owner shall adhere to all of the requirements for public key registration.

Key replacement shall occur:

a) at the end of the cryptoperiod;

or

b) when compromise of the private key is known or suspected;

or

c) as required to address business needs.

In the case of key replacement, both the public and the private key of a key pair shall be replaced.

A key shall be replaced within the time deemed feasible to perform any known attack upon the data enciphered under this key, or within the time deemed feasible to determine the private key by cryptanalytic attack (for guidance see Bibliography [11]) This will depend upon the specific implementation and the technology available at the time of the attack.

Replacement of a key pair shall take place in all operational locations where the keys exist.

Keys that have been replaced shall not be returned to active use.

Key replacement requires that the old private key shall be destroyed.

6.10 Public key expiration

Public keys, when generated and issued for use, typically have an expiry date that determines the key pair life cycle. Public keys shall not be used beyond their expiry date.

6.11 Private key destruction

An instance of a private key shall be destroyed when it is no longer required for active use. Electronic instances of a private key may be destroyed by erasure. However, information may still reside at the operational location so that the key may subsequently be restored for active use.

The associated public key shall not be distributed again to communicating parties. If public keys are stored at communicating parties' locations, they shall be informed of the destruction of the associated private key.

When an SCD is permanently removed from service, all private keys stored within the device shall be destroyed.

Private key destruction shall be implemented either by completely overwriting the key with a new key value or a value that may be non-secret such that no information about the erased key is retained, or by destroying the key storage media following the procedures outlined in ISO 9564-1.

6.12 Private key deletion

Key deletion occurs when all instances of the private key have been destroyed at a given location.

Private key deletion shall be implemented by completely erasing all forms of the key at an operational location whether the key is physically secured, enciphered or in the form of components.

When a key component available in human-comprehensible form is to be deleted, the media on which the key component is recorded shall be destroyed by burning or an equivalently effective process.

6.13 Public key archive

Public key archive is the process by which a public key is stored for the purpose of verifying signatures that occurred prior to revocation. After such verification, the instance of the key necessary to perform the verification should be destroyed.

An archived public key shall be securely stored in order to ensure its integrity as long as data verifiable by this key still exists.

Public key archive shall be protected with the same level of security as for public key storage (see 6.3).

The separation of archived keys from active keys and protection against substitution of active keys by archived keys shall be achieved by using one of the appropriate techniques as described in ISO 11568-2 and in 5.4.

The key encipherment key used for the archival process shall not intentionally be the same as any of the key encipherment keys used to encipher active keys.

6.14 Private key termination

Private key termination occurs when the private key has been deleted from all locations where it has ever occurred. Subsequent to private key termination, no information shall exist from which the private key can feasibly be reconstructed.

NOTE Archiving of private keys is unnecessary.

Private key termination shall be effected by destroying all instances of the key at all locations according to the requirements and methods described in 6.12.

6.15 Erasure summary

Table 3 — Effects of erasure

Action	Location	Information affected	
		Instance of a key	Information for reconstruction
Destruction	Single	Single instance erased	—
Deletion	Single	All instances erased	erased
Termination	All	All instances erased	erased

6.16 Optional life cycle processes

6.16.1 Public key certification

Public key certification is the process by which a trusted third party, referred to as the certification authority, establishes a proof that links a public key and other relevant information to its owner.

Key certification and the certification authority are described in 5.3.

The public key of the certification authority that is used to verify the public key in a certificate should be transferred to the user in an authenticated way.

6.16.2 Key retrieval

Retrieval of a public key from back-up shall be implemented by one of the methods described for public key distribution and loading in 6.4.

Retrieval of a private key from back-up shall be implemented by one of the methods described for private key storage in 6.3.

Annex A (normative)

Approved algorithms

A.1 General

This annex identifies the algorithms that are approved for use in key management using public key cryptography. The procedure that allows additional algorithms to be approved is described in ISO 11568-1. Symmetric key algorithms that are approved for use with this part of ISO 11568 are listed in ISO 11568-2.

A.2 Approved algorithms

A.2.1 Algorithms approved for public key transport systems

RSA Ref: ISO/IEC 18033-2.

ECIES-KEM (Key Encapsulation Method) Ref: ISO/IEC 18033-2.

A.2.2 Algorithms approved for public key agreement systems

Diffie-Hellman Ref: ANSI X9.42.

EC-DH Ref: ISO/IEC 15946-3.

EC-MQV Ref: ISO/IEC 15946-3.

A.2.3 Algorithms approved for digital signatures

RSA Ref: ISO/IEC 9796-2.

DSA Ref: ISO/IEC 14888-3.

ECDSA Ref: ISO/IEC 14888-3.

A.2.4 Approved hash functions

ISO/IEC 10118 (all parts).

Bibliography

- [1] ISO/IEC 9797-1, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*
- [2] ISO/IEC 9797-2, *Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a dedicated hash-function*
- [3] ISO/IEC 11770-1:1996, *Information technology — Security techniques — Key management — Part 1: Framework*
- [4] ISO/IEC 11770-2:1996, *Information technology — Security techniques — Key management — Part 2: Mechanisms using symmetric techniques*
- [5] ISO/IEC 18032, *Information technology — Security techniques — Prime number generation*
- [6] ISO 21188, *Public key infrastructure for financial services — Practices and policy framework*
- [7] ANSI X9.57, *Public Key Cryptography for the Financial Services Industry: Certificate Management*
- [8] SHAMIR, A. *How to share a secret*, Communications of the ACM, November 1979
- [9] ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*
- [10] MENEZES, A., VAN OORSCHOT, P. and VANSTONE, S. *Handbook of Applied Cryptography*, CRC Press, 1996
- [11] Special Publication 800-57 *Recommendation for Key Management — Part 1: General (Revised)*, National Institute of Standards and Technology
- [12] ISO/IEC 9796-3, *Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*
- [13] ISO 9807, *Banking and related financial services — Requirements for message authentication (retail)*
- [14] ANSI X9.30-1, *Public Key Cryptography for the Financial Services Industry — Part 1: The Digital Signature Algorithm (DSA)*
- [15] BSR X9.102-200x¹⁾, *Symmetric Key Cryptography for the Financial Services Industry: Wrapping of Keys and Associated Data*
- [16] AS 2805.5.3, *Electronic funds transfer — Requirements for interfaces — Ciphers — Data encipherment algorithm 2 (DEA 2)*

1) Draft

Standards Australia

Standards Australia develops Australian Standards® and other documents of public benefit and national interest. These Standards are developed through an open process of consultation and consensus, in which all interested parties are invited to participate. Through a Memorandum of Understanding with the Commonwealth Government, Standards Australia is recognized as Australia's peak non-government national standards body. Standards Australia also supports excellence in design and innovation through the Australian Design Awards.

For further information visit www.standards.org.au

Australian Standards®

Committees of experts from industry, governments, consumers and other relevant sectors prepare Australian Standards. The requirements or recommendations contained in published Standards are a consensus of the views of representative interests and also take account of comments received from other sources. They reflect the latest scientific and industry experience. Australian Standards are kept under continuous review after publication and are updated regularly to take account of changing technology.

International Involvement

Standards Australia is responsible for ensuring the Australian viewpoint is considered in the formulation of International Standards and that the latest international experience is incorporated in national Standards. This role is vital in assisting local industry to compete in international markets. Standards Australia represents Australia at both the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Sales and Distribution

Australian Standards®, Handbooks and other documents developed by Standards Australia are printed and distributed under license by SAI Global Limited.

For information regarding the development of Standards contact:

Standards Australia Limited
GPO Box 476
Sydney NSW 2001
Phone: 02 9237 6000
Fax: 02 9237 6010
Email: mail@standards.org.au
Internet: www.standards.org.au

For information regarding the sale and distribution of Standards contact:

SAI Global Limited
Phone: 13 12 42
Fax: 1300 65 49 49
Email: sales@sai-global.com



ISBN 0 7337 9013 5

This page has been left intentionally blank.