INTERNATIONAL STANDARD

ISO 11568-4

First edition
1998-07-15

Banking — Key management (retail) —

Part 4:
Key management techniques using public key cryptography

Banque — Gestion de clés (services aux particuliers) —

Partie 4: Techniques de gestion de clés utilisant la cryptographie à clé publique

Reference number
ISO 11568-4:1998(E)

Contents

International Organization for Standardization
Case postale 56 • CH-1211 Genève 20 • Switzerland
Internet iso@iso.ch

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

International Standard ISO 11568-4 was prepared by Technical Committee ISO/TC 68, *Banking, securities and other financial services*, Subcommittee SC 6, *Retail financial services*.

ISO 11568 consists of the following parts, under the title *Banking — Key management (retail)*:

— *Part 1: Introduction to key management*

— *Part 2: Key management techniques for symmetric ciphers*

— *Part 3: Key life cycle for symmetric ciphers*

— *Part 4: Key management techniques using public key cryptography*

— *Part 5: Key life cycle for public key cryptosystems*

— *Part 6: Key management schemes*

Annexes A and B form an integral part of this part of ISO 11568. Annexes C, D and E are for information only.

Introduction

ISO 11568 describes procedures for the secure management of the cryptographic keys used to protect messages in a retail banking environment, for instance, messages between an acquirer and a card acceptor, or an acquirer and a card issuer. Management of keys used in an Integrated Circuit Card (ICC) environment is not covered by ISO 11568.

Whereas key management in a wholesale banking environment is characterized by the exchange of keys in a relatively high-security environment, this standard addresses the key management requirements that are applicable in the accessible domain of retail banking services. Typical of such services are point-of-sale/point-of-service (POS) debit and credit authorizations and automated teller machine (ATM) transactions.

ISO 11568 is a multi-part standard.

This part of ISO 11568 describes key management techniques which are appropriate for use with public key cryptosystems, and which, when used in combination, provide the key management services identified in ISO 11568-1. These services are:

— key separation

— key substitution prevention

— key identification

— key synchronisation

— key integrity

— key confidentiality

— key compromise detection

Banking — Key management (retail) —

Part 4:
Key management techniques using public key cryptography

1 Scope

This part of ISO 11568 specifies techniques for the use and protection of the cryptographic keys of public key cryptosystems, when used in a retail banking environment.

It is applicable to any organization which is responsible for implementing procedures for the protection of keys during the life cycle. The techniques described in this part of ISO 11568 enable compliance with the principles described in ISO 11568-1.

NOTE Details of the protection required during each step in the key life cycle for public key cryptosystems are specified in ISO 11568-5.

Public key cryptosystems embrace asymmetric ciphers, digital signature systems and public key distribution systems. Although this part of ISO 11568 describes techniques using these systems when specifically applied to key management, some of the techniques have equal applicability for the secure management of data.

The techniques are described for generic public key cryptosystems. Any required details which are specific to a particular system are described in an annex.

Algorithms approved for use with the techniques described in this part of ISO 11568 and the procedures for their approval are given in annex A.

Annex B provides a normative overview of public key certificate management.

Annex C provides a description of attribute certificates, a technique that enhances the functionality of public key certificates.

Annex D provides an introduction to the three types of public key cryptosystems indicated above.

2 Normative references

The following standards contain provisions which, through reference in this text, constitute provisions of this part of ISO 11568. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this part of ISO 11568 are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards.

ISO/IEC 8824:1990, *Information technology — Open Systems Interconnection — Specification of Abstract Syntax Notation One (ASN.1)*.

ISO/IEC 8825:1990, *Information technology — Open Systems Interconnection — Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.

ISO 8908:1993, *Banking and related services — Vocabulary and data elements*.

ISO/IEC 9594-8:1990, *Information technology — Open Systems Interconnection — The Directory — Part 8: Authentication framework*.

ISO/IEC 9796:1991, *Information technology — Security techniques — Digital signature scheme giving message recovery*.

ISO 9807:1991, *Banking and related financial services — Requirements for message authentication (retail)*.

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

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

ISO 11166 (all parts), *Banking — Key management by means of asymmetric algorithms*.

ISO/IEC 11770-3:—[1)], *Information technology — Security techniques — Key management — Part 3: Mechanisms using asymmetric techniques*.

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

ANSI X9.30.1-1995, *Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry — Part 1: The Digital Signature Algorithms (DSA)*.

ANSI X9.30.2-1993, *Public Key Cryptography — Part 2*.

AS2805-5.3 *Ciphers — DEA 2*.

3 Definitions

For the purposes of this part of ISO 11568, the definitions given in ISO 8908 and the following definitions apply.

3.1
asymmetric cipher
a cipher in which the encipherment key and the decipherment key are different, and it is computationally infeasible to deduce the decipherment key from the encipherment key

3.2
asymmetric key pair
a public key and related private key created by, and used with, a public key cryptosystem

3.3
certificate
the credentials of an entity, signed using the private key of the certification authority which issued it, and thereby rendered unforgeable

3.4
certification authority (CA)
a centre trusted to create and assign certificates

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

1) To be published.

3.5
computationally infeasible
the property that a computation is theoretically achievable but is not feasible in terms of the time or resources required to perform it with the current or predicted power of computers

3.6
credentials
key identification data for an entity, incorporating at a minimum the entity's distinguished name and public key

NOTE Additional data may be included.

3.7
digital signature
a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the origin and integrity of the data unit and protects the sender against forgery by third parties or the recipient

3.8
digital signature system
a public key cryptosystem which provides for the creation and subsequent verification of digital signatures

3.9
hash function
a one-way function which maps a set of arbitrary strings onto 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 which map to the same output.

3.10
key agreement
the establishment of a common secret key without reference to another common secret key

3.11
key pair owner
the party to which the key pair belongs

3.12
non-repudiation of origin
the property that the originator of a message and associated cryptographic check value (digital signature) is not able to subsequently deny, with an accepted level of credibility, having originated the message

3.13
public key cryptosystem
a 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

3.14
public key distribution system
a public key cryptosystem which allows a secret key to be jointly created by two communicating entities

3.15
public key user
the party which uses the public key of another party for a cryptographic service

NOTE The Certification Authority is not a public key user.

4 Uses of public key cryptosystems in retail banking systems

In retail banking systems, public key cryptosystems are used primarily for key management; firstly for the management of the keys of symmetric ciphers, and secondly for the management of the keys of the public key cryptosystems themselves. This clause describes these applications of public key cryptosystems; the techniques employed in support of these applications are described in clause 5.

4.1 Distribution of symmetric keys

Distribution of one or more keys of a symmetric cipher may be by key transport or by key agreement.

NOTE Mechanisms for the distribution of symmetric keys are described in ISO/IEC 11770-3, where key distribution is referred to as key establishment.

4.1.1 Key transport

When key transport is used, the symmetric keys shall be enciphered using an asymmetric cipher and the resulting enciphered key block shall be transmitted to the intended recipient. Key encipherment ensures the confidentiality of the symmetric keys during distribution; the authenticity and integrity of the key block or of the complete transmitted message may be ensured by signing the block or message using a digital signature system.

Key encipherment is described in clause 5.

NOTE ISO 11166-1 describes protocols for the transport of symmetric keys. The protocols use both key encipherment and digital signatures.

4.1.2 Key agreement

When key agreement is used, the keys for the symmetric cipher shall be established by the use of a public key distribution system (see annex D). The mechanism used shall ensure the authenticity of the communicating entities.

4.2 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.

NOTE Some applications are designed such that the required security is dependent on the non-disclosure of the public key.

One of the following methods may be used to ensure the authenticity and integrity of a public key during storage or distribution:

— sign the public key and associated data using a digital signature system, thereby creating a 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 the algorithm defined by ISO 9807 and a key used only for this purpose;

— encipher the public key and associated data, using a symmetric or asymmetric cipher.

Key encipherment is described in 5.2.

The following additional method may be used to ensure the authenticity and integrity of a public key during distribution only:

— distribute the public key over an unprotected channel, and distribute a key verification value of the public key and associated data using an authenticated channel with dual controls. Key verification is described in 5.5.

4.3 Storage and transfer of asymmetric private keys

Since the private key of an asymmetric key pair does not need to be provided to any site other than that of the user, in some cases it can be kept within the secure cryptographic device that generated it. If it must be output from the device that generated it (e.g. for transport to another secure cryptographic device where it is to be used, or for backup purposes) it shall be protected from compromise by at least one of the following three techniques:

— encipherment with another cryptographic key (see 5.2);

— dividing into two or more components, such that each bit in the protected key depends on all components;

— outputting into another secure cryptographic device, which is the secure cryptographic device where it is to be used, or a secure transport device intended for this use. (If the communications path is not fully secured, then the transfer shall only be permitted inside a secure environment.)

5 Techniques for the provision of key management services

This clause describes the techniques which 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.

It is often necessary (or desirable) to use a public key pair for multiple purposes, e.g. digital signatures and encipherment. In these cases, 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 a secure cryptographic device. 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 a secure cryptographic device are defined in ISO 13491-1.

5.1 Generation of an asymmetric key pair

The two keys of an asymmetric key pair are mathematically related as defined by the design of the particular public key cryptosystem. The relationship is such that it is computationally infeasible to determine the private key from the public key.

Most public key cryptosystems are based on modular arithmetic. The size of the modulus not only determines the sizes of the data and key blocks, but also the difficulty in breaking the system. Where the strength of the system is directly related to the size of the modulus, the modulus shall be chosen to be sufficiently large so as to render attacks computationally infeasible.

While ensuring that the required relationship between the two keys exists, key generation shall utilize a random or pseudo-random process such that it is not possible to predict any key or determine that certain keys within the key space are significantly more probable than others.

NOTE In some cryptosystems it is possible to use a known constant value for a part of the public key. This does not conflict with the requirement identified above.

5.2 Key encipherment

Key encipherment is a technique whereby one key is enciphered using another key. The resulting enciphered key may then be managed securely (with confidentiality and/or authenticity ensured) outside of a secure cryptographic device. A key used to perform such encipherment is called a key encipherment key (KEK).

Three differing cases of key encipherment involving asymmetric keys and ciphers are described here, namely:

a) Encipherment of a symmetric key using an asymmetric cipher.

b) Encipherment of an asymmetric key using an asymmetric cipher.

c) Encipherment of an asymmetric key using a symmetric cipher.

NOTE Key encipherment using a symmetric cipher to encipher a symmetric key is addressed in ISO 11568-2.

Although key encipherment ensures key confidentiality is maintained, other techniques may need to be employed in association with the key encipherment in order to ensure adequate key separation, e.g. key tagging (see 5.4).

5.2.1 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 may be created which incorporate the keys of both symmetric and asymmetric ciphers.

NOTE Key hierarchies are described in ISO 11568-2.

The symmetric key must be formatted into a data block appropriate to the encipherment operation. As the block size of asymmetric ciphers tend 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 may be incorporated in the data block.

5.2.2 Encipherment of an asymmetric key using an asymmetric cipher

Either the public key or the private key of an asymmetric cipher may itself be enciphered using an asymmetric cipher.

5.2.3 Encipherment of an asymmetric key using a symmetric cipher

Either the public key or the private key of an asymmetric cipher may be required to be enciphered using a symmetric cipher.

As the keys of asymmetric ciphers tend to be larger than the block size of symmetric ciphers, the asymmetric key must be formatted into multiple data blocks for encipherment. Therefore, the cipher block chaining mode of operation should be used for the encipherment operation.

NOTE 1 Modes of operation for an *n*-bit block cipher algorithm are standardized in ISO/IEC 10116.

Double-length keys shall be used in the encipherment of asymmetric private keys.

NOTE 2 Encipherment using a double-length key is described in ISO 11568-2.

5.3 Key certification

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

Key certification is a technique which 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 a user are together known as the user's credentials. The validity data typically incorporates user 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 user credentials using a private key owned by the Certification Authority and used only for this purpose.

The management of public key certificates is described in detail in annex B.

5.4 Key separation techniques

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 which prevents undetectable modifications to either.

5.4.1 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 which prevents undetectable modifications to either.

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 value 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 which allows the value of a key to be checked and verified, without exposing that value. The technique utilizes a Key Verification Code (KVC) which is cryptographically related to the key via a collision-resistant one-way function.

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.

For private keys, key verification may be used to ensure that an enciphered key has not been corrupted during transmission or transformation, or that the key has not been corrupted or overwritten in storage.

For public keys, key verification may additionally be used to facilitate key integrity checking. As long as the KVC is distributed via an integrity-assured channel, the public key can be distributed via a non-secure channel.

6 Public Key Certificate management

Public Key Certificates can be employed in order for one entity to use another entity's public key with an acceptable degree of confidence. The certificate provides a level of assurance for the integrity and authenticity of a public key. Certificates are generated by a Certification Authority (CA). The public key owner registers its identity and the corresponding public key with the CA. The CA provides the binding between the entity's identity and its public key. Subscribers can then obtain certificates directly from the CA or from the public key owner. For further information, see annex B.

Annex A
(normative)

Approved algorithms and algorithm approval procedure

This annex identifies the algorithms which are approved for use in key management using public key cryptography, and details the procedure that allows additional algorithms to be approved.

A.1 Approved algorithms

A.1.1 Algorithms approved for encipherment

RSA Ref: AS2805, Part 5.3.

A.1.2 Algorithms approved for digital signatures

RSA Ref: ISO/IEC 9796.

DSA Ref: ANSI X9.30, Part 1.

A.1.3 Approved hash functions

ISO/IEC 10118 (all parts), *Hash functions*.

MD5

SHA Ref: ANSI X9.30, Part 2.

A.1.4 Approved algorithms for public key distribution systems

X9.42 *Diffie-Hellman*.

A.2 Procedure for approval of an algorithm

The following procedure for approval of an algorithm for use with this part of ISO 11568 shall be used by ISO/TC 68.

A.2.1 Justification of proposal

ISO/TC 68 shall require the originator to justify a proposal by describing:

a) the purpose the proposal is to serve;

b) how this purpose is better achieved by the proposal than algorithms already in the standard;

c) additional merits not described elsewhere;

d) experience in use with the new algorithm.

A.2.2 Documentation

The proposed algorithm shall be completely documented when submitted for consideration. The documentation shall include:

a) a full description of the algorithm proposed;

b) a clear acknowledgement that the algorithm satisfies, or is compatible with, all the requirements of this part of ISO 11568;

c) a definition and explanation of any new terms, factors, or variables introduced;

d) a step-by-step example illustrating the operation of the algorithm;

e) detailed information on any prior testing to which the proposed algorithm has been subjected, particularly concerning its security, reliability and stability. Such information should include an outline of the testing procedures used, the results of the tests, and the identity of the agency or group performing the tests and certifying the results (that is, sufficient information should be provided to enable an independent agency to conduct the same tests and to compare the results achieved).

A.2.3 Public disclosure

Any algorithm submitted for consideration shall be free of security classification. If copyright or patent application has been made on the algorithm, the originator shall submit the appropriate letter stating that the originator is willing to grant a license under these copyrights and patents on reasonable and non-discriminatory terms and conditions to anyone wishing to obtain such a license to allow free and unconditional use by testers, users and suppliers of supporting equipment or material. All documentation and information submitted with the request for consideration of the algorithm shall be considered public information available to any individual, organization or agency for review, testing and usage.

A.2.4 Examination of proposals

ISO/TC 68 shall examine and prepare a report on each new proposal submitted. The report shall normally be sent to the ISO/TC 68 Secretariat within 180 days of receipt of the proposal (see A.2.5). The report shall state if the proposal is adequately documented, if it has been properly tested and certified already, and if the proposed algorithm satisfies the conditions and requirements of this part of ISO 11568. The examination may also include submission of the proposal for public review (see A.2.5).

The ISO/TC 68 Secretariat shall determine in each case whether such report and recommendations are best prepared by correspondence between the members or by a meeting. If a meeting is to be held, at least 60 days notice of the date shall be given and of the papers to be dealt with at the meeting.

Where a majority of members of ISO/TC 68 recommends the rejection of the proposal, the Secretariat shall notify the originator, in writing, advising of the rejection and the reasons for it.

A.2.5 Public review

ISO/TC 68 shall forward proposals which it considers should be accepted (and which have not already been subjected to extensive testing or experience) to selected agencies or institutions with an international reputation in this field. These agencies and institutions will be requested to examine and report on the proposals within 90 days of receipt.

NOTE This period of public review may extend the 180 days allowed for ISO/TC 68 to prepare its overall report on the proposal (see A.2.4).

A.2.6 Appeal procedure

Originators whose proposals are rejected by ISO/TC 68 (see A.2.4) may ask the Secretariat of ISO/TC 68 to have the proposals subjected to public review (see A.2.5) if this has not already been done. If, following submission of the public review reports, ISO/TC 68 still recommends rejection, the originator may request the ISO/TC 68 Secretariat to circulate

the proposal, together with copies of all relevant reports on it, for ballot by P-members of the subcommittee whose ruling in the matter shall be final.

A.2.7 Incorporation of new algorithms

New algorithms recommended for acceptance by ISO/TC 68, together with relevant reports on them, shall be circulated for letter ballot by the Secretariat of ISO/TC 68 to all P-members of the subcommittee. Proposals approved as a result of this process shall be forwarded to the secretariat of ISO/TC 68 for action under the abbreviated procedure to amend an existing standard (see 5.10.11 of Part 1 of the Directives for Technical Work of ISO). Once approval is given, the new encipherment algorithm shall be added to this standard.

A.2.8 Maintenance

An algorithm approved by the method described in this part of ISO 11568 shall be reviewed at intervals of not more than five years.

Annex B
(normative)

Public Key Certificate management

B.1 Introduction

Public Key Certificates should be employed in order to establish and maintain the association between the Key Pair Owner and the public key. The certificate provides a high level of assurance for the integrity, authenticity, and ownership of a public key.

This normative annex presents the following information, divided into three clauses:

Clause B.2 describes who the entities are, identifies documents, and explains these relationships for certificate management.

Clause B.3 describes what the processes are and defines the responsibilities for each of the entities for certificate management.

Clause B.4 defines the mandatory, recommended and optional data elements contained within a Public Key Certificate.

Additional information for certificate management and certificate data elements can be found in the ANSI standard X9.57 which specifies Public Key Certificates. Both standards use ASN.1 as described in ISO/IEC 8824, ISO/IEC 8825 and ISO/IEC 9594-8.

B.2 Entities and documents

B.2.1 Identification documents

Identification documents are the physical or electronic documents submitted to the Certification Authority for establishing the identity of the Key Pair Owner.

B.2.2 Credentials

Credentials are the physical or electronic documents submitted to the Certification Authority for establishing the identity of the public key. Refer to B.4.2.

B.2.3 Public Key Certificates

Public Key Certificates are the physical or electronic documents ensuring the binding between the identity of the Key Pair Owner and the corresponding public key by means of a digital signature, generated by a Certification Authority and its private key. Refer to B.4.1.

B.2.4 Certification Authority

The Certification Authority (CA) is an authorized agent who provides the following services:

a) confirms the identity of the Key Pair Owner;

b) verifies the correctness of the public key[2)];

c) generates a Public Key Certificate;

d) issues the Public Key Certificate to the Key Pair Owner (who in turn may distribute the certificate to Public Key Users); and

e) possibly distributes or makes available the Public Key Certificate to Public Key Users.

B.2.5 Key Pair Owner

A Key Pair Owner is the owner of the private and public key pair and the user of the private key, who either generated the asymmetric keys or securely obtained the asymmetric keys from a trusted third party.

B.2.6 Public Key User

A Public Key User is the user of the public key, which was extracted from a Public Key Certificate originally obtained from a Certification Authority. The Public Key User authenticates the certificate by verifying the CA's signature using the CA's public key. A Public Key Certificate implies authentication of the Key Pair Owner's identity and provides integrity of the owner's identity and his public key.

The Public Key User shall initially obtain the CA's public key in such a manner that its authenticity and integrity is established and maintained. This may be accomplished using Public Key Certificates from another CA whose public key is already established, manual exchange of the CA's public key since the data is not secret, or other cryptographic techniques including symmetric and asymmetric key management schemes.

B.2.7 Entities and documents relationships

Figure B.1 is a visual representation depicting the relationships between the entities and the documents described above.

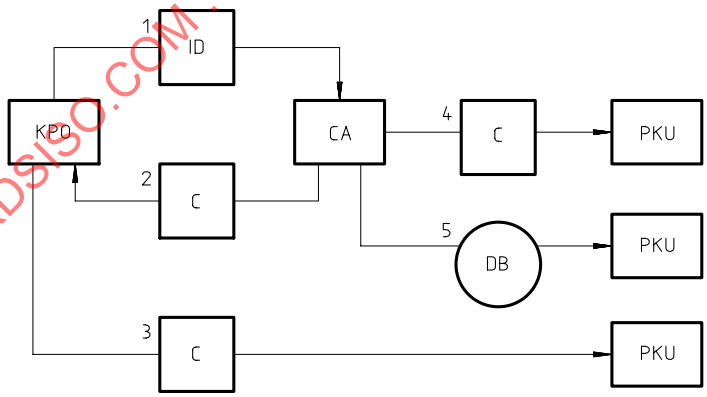

Figure B.1

2) For example, the Key Pair Owner can generate a digital signature using the private key and the CA can verify the signature using the public key. As another example, the CA can encrypt a message using the public key which the Key Pair Owner can decrypt using the private key. In both examples, the CA is assured that the Key Pair Owner actually retains the corresponding private key.

a) The Key Pair Owner (KPO) registers the proper Identification Documentation (ID) and credentials with the Certification Authority (CA)[3].

b) The CA generates the Public Key Certificate (C) and transfers a copy to the owner (KPO).

c) The owner may distribute certificate (C) copies to one or more Public Key User (PKU).

d) The CA may also distribute certificate copies to one or more users (PKU).

e) The CA may alternatively make certificates available to users by placing them on a database (DB) or a public directory.

B.3 Processes and responsibilities

This subclause describes the responsibilities of each entity for the following certificate management processes:

— Registration of a Key Pair Owner.

— Generation and transfer of a certificate.

— Distribution of a certificate.

— Revocation of a certificate.

— Usage of a certificate by a Public Key User.

Note that all actions taken by a Certification Authority shall be logged in an audit journal which is reviewed periodically.

B.3.1 Registration of a Key Pair Owner

Registration is the process whereby the public key's identity and the owner's identity are established by means of validating the owner’s credentials and identification documents.

The appropriate identification documents and credentials shall be submitted either directly to the CA or to a Local Registration Authority (LRA) who is recognized by the CA to validate identification documents. The LRA is a function performed either by the CA or a third party.

The LRA shall validate the identification documents and either creates or verifies a unique name for the Key Pair Owner. If the LRA is not part of the CA, then secure means shall be used to ensure the authenticity and integrity of the owner’s identity and credentials during transfer from the LRA to the CA.

An independent notification shall be used to verify that the submitted identification documents and credentials were correct and authorized This requires a written or verbal confirmation obtained via a different channel other than the original one whereby the documents were obtained.

This registration process shall be performed for each Public Key Certificate issued by a CA.

B.3.2 Generation and transfer of a certificate

Generation is the process whereby a Public Key Certificate is created by the CA.

3) Note that if the CA generates the KPO's asymmetric key pair, the KPO does not necessarily register its credentials with the CA as the credentials do not contain the public key.

Upon successful completion of the registration process, the CA shall create the certificate by signing the appropriate information, as defined in clause B.4, and concatenating the digital signature to the above signed data. The issuance of a certificate ensures that the owner's identity and public key are authentic and the digital signature provides integrity of the information.

Transfer is the process whereby the Public Key Certificate is returned to the Key Pair Owner.

The CA may issue the Public Key Certificate to the Key Pair Owner at the time of generation or at a later time via the distribution mechanism.

In addition, the CA may send an independent notification to the Key Pair Owner that a certificate has in fact been issued.

B.3.3 Distribution of a certificate

Distribution is the process whereby Public Key Users may obtain the Public Key Certificates for usage. Optionally, the certificate may contain an expiry date which indicates the end of its operational use.

Certificates may be obtained from either the Key Pair Owner or the CA. The actual distribution method may vary, including mailed documents, electronic media and on-line data bases. In any case, the CA's public key needs to be known to the Public Key User for validating the certificate.

B.3.4 Revocation of a certificate

Revocation is the process whereby a certificate is brought to the end of its operational use prior to the expiry date. The certificate may be revoked for security reasons due to a possible or suspected compromise of either the entity's or the CA's private key or for other business reasons. At a minimum, a Certificate Revocation List (CRL) shall be maintained by the CA. All revoked certificates are added to the list regardless of the termination reason.

The CRL shall be available for all Public Key Users. For example, the CA may distribute revocation notices directly to the Public Key Users or maintain the CRL as an on-line database.

The CA shall maintain the integrity of the CRL and ensure the authenticity of the entries. The integrity and authenticity of the CRL shall be maintained by signing the entire CRL or applying message authentication as defined in ISO 9807, to ensure its integrity and provide independent verification. If revocations are individually distributed, they shall also be signed by the CA.

In addition, the CA shall send an independent signed revocation notice to the Key Pair Owner that a certificate has been revoked.

B.3.5 Usage of a certificate by a Public Key User

Usage is the process whereby a Public Key User employs the Public Key Certificate. Before the Public Key User may make use of the certificate, the certificate shall be validated. This is accomplished in the following manner:

— Ensure that the correct Public Key Certificate is selected.

— Ensure that the certificate has not been revoked by checking that the certificate does not appear in the CRL.

— If start or expiry dates are contained in the certificate, ensure that the certificate is active.

— Verify the integrity of the certificate information (i.e. verify the digital signature using the CA's public key).

B.4 Certificate data elements

This clause defines the data elements within a certificate. Options for data elements are defined as:

M: Mandatory data elements shall be present.

R: Recommended data elements should be present.

O: Optional data elements may be present.

Information is presented by a hierarchy of tables, the high level being the certificate itself, as described in B.4.1 with further details described in B.4.2 and B.4.3.

B.4.1 Public Key Certificate data elements

Table B.1

Public Key Certificate data elements	
op	**data element(s):**
M	1. Key Pair Owner Credentials[4)]
O	2. Certificate Serial Number
O	3. Certificate Start Date
R	4. Certificate Expiry date
R	5. CA Information[4)]
O	6. Attribute Certificate Indicator
M	7. Digital Signature

Note that the data elements presented in B.4.1 are listed in recommended order. The following are descriptions for each data element.

B.4.1.1 Key Pair Owner Credentials

See B.4.2 for descriptions.

B.4.1.2 Certificate Serial Number

This is a number assigned by the CA to uniquely identify each certificate issued by the CA. This may be used in conjunction with certificate storage or in association with attribute certificates.

B.4.1.3 Certificate Start Date

This is the beginning date from which the certificate is usable, typically the issuance date assigned by the CA. Refer to B.3.2.

B.4.1.4 Certificate Expiry Date

This is the end date after which the certificate is no longer usable, assigned by the CA. Refer to B.3.4.

4) These data elements are further defined in B.4.2 and B.4.3, respectively.

B.4.1.5 CA Information

See B.4.3 for descriptions.

B.4.1.6 Attribute Certificate Indicator

This is a value indicating that one or more corresponding attribute certificates exists which further define the usage of a KPO's asymmetric key pair. Refer to annex C.

B.4.1.7 Digital Signature

This is the value generated from the public key cryptographic algorithm. Typically, the signature length is reduced by first applying a hash function to the data. However, in some cases the signature may be generated without the benefit of a hash.

B.4.2 Key Pair Owner Credentials

Table B.2

Key Pair Owner Credentials	
op	**data element(s):**
M	1. Relative Distinguished Name
M	2. Public Key Value
R	3. Public Key Length
R	4. Public Key Name
R	5. Public Key Parameter: Modulus
R	6. Public Key Parameter: Algorithm Identifier
R	7. Public Key Parameter: Hash Identifier
O	8. Time and Date of Submission

Note that the data elements presented in B.4.2 are listed in optional (op) order. The following are descriptions for each data element.

B.4.2.1 Relative Distinguished Name

This is the Key Pair Owner's name, unique relative to all Key Pair Owners registered with the same Certification Authority.

B.4.2.2 Public Key Value

This is the value of the Key Pair Owner's public key, typically expressed in binary or hexadecimal digits.

B.4.2.3 Public Key Length

This is the length of the public key, typically expressed as the number of bits.

B.4.2.4 Public Key Name

This is the public key's name, unique relative to all public keys for each Key Pair Owner.

The following data elements are recommended parameters which are specific to a given public key algorithm. Additional parameters may be necessary to completely define the algorithm.

B.4.2.5 Public Key Parameter: Modulus

This is the modulus value used with the public key algorithm, which is typically non-secret data.

B.4.2.6 Public Key Parameter: Algorithm Identifier

This is a value which identifies the specific public key algorithm intended for use with the Key Pair Owner's public key.

B.4.2.7 Public Key Parameter: Hash Identifier

This is a value which identifies the specific hash function used in conjunction with the Key Pair Owner's public key for digital signatures.

B.4.2.8 Time and Date of Submission

This is the time and date of the Key Pair Owner's registration with the LRA or CA, which may not necessarily coincide with the start date.

B.4.3 CA Information

Table B.3

CA Information	
op	**data element(s):**
R	1. CA Distinguished Name
O	2. CA Public Key Parameter: Modulus
O	3. CA Public Key Parameter: Algorithm Identifier
O	4. CA Public Key Parameter: Hash Identifier

Note that the data elements presented in B.4.3 are listed in optional (op) order. The following are descriptions for each data element.

B.4.3.1 CA Distinguished Name

This is the CA's name, unique relative to all other Certification Authorities.

B.4.3.2 CA Public Key Parameter: Modulus

This is the modulus value used with the CA's public key algorithm.

B.4.3.3 CA Public Key Parameter: Algorithm Identifier

This is a value which identifies the specific public key algorithm intended for use with the CA's public key.

B.4.3.4 CA Public Key Parameter: Hash Identifier

This is a value which identifies the specific hash function used in conjunction with the CA's public key for signing certificates.

Annex C
(informative)

Attribute Certificate

C.1 Attribute Certificate

Attribute Certificates are a technique to enhance the functionality of Public Key Certificates while still maintaining interoperability with existing certificates, such as those defined in the ITU standard X.509.

The existence of one or more Attribute Certificates is denoted in the Public Key Certificate by the Attribute Certificate Indicator. Conversely, the Certificate Serial Number from the Public Key Certificate is contained in each Attribute Certificate.

The Public Key Certificate provides the Public Key User with a valid public key which is used to either encrypt information or to verify the signature on information. The purpose for which that information can be used is specified in an Attribute Certificate.

C.2 Examples of Attribute Certificates

For example, a Public Key Certificate would allow a merchant or an acquirer to verify the signature on a retail transaction which provides authenticity of the Key Pair Owner. However, the Public Key Certificate by itself may not authorize the Key Pair Owner to execute such a transaction.

In this example, another entity known as the Attribute Authority may issue one or more Attribute Certificates for the Key Pair Owner. Note that the Attribute Authority (AA) is not necessarily the same entity as the Certification Authority (CA).

The AA may issue an Attribute Certificate which contains the Public Key Certificate Serial Number and provides authorization to the Key Pair Owner for retail purchases up to a certain monetary limit. Thus, the merchant or acquirer, after verifying the signature and examining the Attribute Certificate, could approve the signed retail transaction.

In addition, the same Attribute Certificate could contain multiple monetary limits for different types of retail transactions, such as cash advances, hotels, restaurants, etc.

The same AA may issue another Attribute Certificate which might contain similar monetary information for different countries.

A different AA may issue another Attribute Certificate which might contain similar monetary information but for a different financial institution.

C.3 Roles and responsibilities

The roles and responsibilities are similar for Attribute Certificates as those for Public Key Certificates.

C.3.1 Certificatation Authority

The responsibility of the CA is the same as described for Public Key Certificate management (refer to B.2.4).

C.3.2 Key Pair Owner

The responsibility of the Key Pair Owner is to ensure that the AA has the Public Key Certificate and any other appropriate information that the AA requires.

C.3.3 Attribute Authority

The responsibilities of the AA are as follows:

— obtain the CA's public key, either using initial key procedures or certificates;

— obtain the Public Key Certificate either from the Key Pair Owner or the original CA;

— verify the CA's signature on the Public Key Certificate of the Key Pair Owner;

— specify the appropriate information to the Key Pair Owner necessary for issuing a certificate;

— obtain the appropriate information from the Key Pair Owner, preferably signed by the Key Pair Owner;

— verify the Key Pair Owner's signature, if the information is signed;

— generate and issue the Attribute Certificate, as described in clause C.4.

The format and data content is described in clause C.4.

C.3.4 Public Key User

The responsibilities of the Public Key User are as follows:

— obtain the CA's and AA's public keys, either using initial key procedures or certificates;

— obtain the Public Key Certificate and the Attribute Certificate, either from the Key Pair Owner or the original CA and AA, respectively;

— verify the CA's signature on the Public Key Certificate of the Key Pair Owner;

— verify the AA's signature on the Attribute Certificate of the Key Pair Owner;

— verify the Key Pair Owner's signature on the transaction;

— approve the transaction or execute the requested function, if appropriate.

C.4 Attribute Certificate data elements

Table C.1

Attribute Certificate data elements	
op	**data element(s):**
O	1. Key Pair Owner Credentials[5)]
R	2. Certificate Serial Number[5)]
O	3. Certificate Start Date
R	4. Certificate Expiry date
R	5. AA Information
M	6. Attribute Information
M	7. Digital Signature

C.4.1 Key Pair Owner Credentials

This is the same information as discussed in annex B. If the original Public Key Certificate does not contain a Certificate Serial Number, then these data elements shall be present to ensure uniqueness.

C.4.2 Certificate Serial Number

This is the same information as discussed in annex B and is recommended as the pointer back to the original Public Key Certificate.

C.4.3 Certificate Start Date

This is the same information as discussed in annex B, except that the AA specifies this data.

C.4.4 Certificate Expiry Date

This is the same information as discussed in annex B except that the AA specifies this data.

C.4.5 AA Information

This is similar to the information as discussed in annex B for Certification Authorities.

C.4.6 Attribute Information

This is the information which specifies the actual use of the Key Pair Owner's private key.

C.4.7 Digital Signature

This is the same information as discussed in annex B except that the AA generates the digital signature using its private key.

5) Note that one of these data elements shall be present in order to provide the link to the corresponding Public Key Certificate.