INTERNATIONAL STANDARD

ISO/IEC 15945

First edition
2002-02-01

Information technology — Security techniques — Specification of TTP services to support the application of digital signatures

Technologies de l'information — Techniques de sécurité — Spécifications des services TTP pour supporter l'application des signatures numériques

Reference number
ISO/IEC 15945:2002(E)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.ch
Web www.iso.ch

Printed in Switzerland

CONTENTS

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 3.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this International Standard may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 15945 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*, in collaboration with ITU-T. The identical text is published as ITU-T Rec. X.843.

Annexes A to C of this International Standard are for information only.

Introduction

Today the development of information technology, as well as that of the worldwide communication infrastructure, opens the possibility to implement electronic commerce in economically relevant dimensions. Digital signatures are an important technique to add security to these commercial applications and to other application fields with a need for legally effective electronic transactions.

Digital signatures are suitable to assure the integrity of data and the authentication of participants in transactions. They can supply an analogue of the handwritten signature for digital orders, offers and contracts. The most important property of digital signatures in this context is that a person who signed a document cannot successfully deny this fact. This property is called "non-repudiation of creation" of a document.

In several countries and in international contexts, legislation concerning digital signatures is being pushed forward with the aim to support the development of electronic commerce and other application fields with a need for legally effective electronic transactions.

A number of standards exist that specify digital signatures, as well as their use for different purposes, like non-repudiation or authentication. A number of commercial applications, as well as TTPs offering services in connection with digital signatures, are implemented or planned. Interoperability of these TTPs, among each other and with the commercial applications, is needed for an economically and legally effective worldwide use of digital signatures.

The goal of this Recommendation | International Standard is to define the services required to support the application of digital signatures for non-repudiation of creation. Since the use of digital signature mechanisms for non-repudiation of creation of a document implies integrity of the document and authenticity of the creator, the services described in this Recommendation | International Standard can also be combined to implement integrity and authenticity services. This is done in a way to promote interoperability among TTPs as well as between TTPs and commercial applications.

NOTE – There is no inherent reason why every TTP planning to support the application of digital signatures should be required to offer all of these services. It is possible that a number of TTPs offering different services cooperate in supporting the use of digital signatures. But, from the view of the potential commercial applications, the whole range of the services may be required and interoperability becomes even more important in this scenario. This is an additional justification to collect all these services together in one document.

INTERNATIONAL STANDARD
ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – SPECIFICATION OF TTP SERVICES TO SUPPORT THE APPLICATION OF DIGITAL SIGNATURES

1 Scope

This Recommendation | International Standard will define those TTP services needed to support the application of digital signatures for the purpose of non-repudiation of creation of documents.

This Recommendation | International Standard will also define interfaces and protocols to enable interoperability between entities associated with these TTP services.

Definitions of technical services and protocols are required to allow for the implementation of TTP services and related commercial applications.

This Recommendation | International Standard focuses on:

- implementation and interoperability;
- service specifications; and
- technical requirements.

This Recommendation | International Standard does not describe the management of TTPs or other organizational, operational or personal issues. Those topics are mainly covered in ITU-T Rec. X.842 | ISO/IEC TR 14516, *Information technology – Security techniques – Guidelines on the use and management of Trusted Third Party services*.

NOTE 1 – Because interoperability is the main issue of this Recommendation | International Standard, the following restrictions hold:

i) Only those services which may be offered by a TTP, either to end entities or to another TTP, are covered in this Recommendation | International Standard.

ii) Only those services which may be requested and/or delivered by means of standardizable digital messages are covered.

iii) Only those services for which widely acceptable standardized messages can be agreed upon at the time this Recommendation | International Standard is published are specified in detail.

Further services will be specified in separate documents when widely acceptable standardized messages are available for them. In particular, time stamping services will be defined in a separate document.

NOTE 2 – The data structures and messages in this Recommendation | International Standard will be specified in accordance to RFC documents, RFC 2510 and RFC 2511 (for certificate management services) and to RFC 2560 (for OCSP services). The certificate request format also allows interoperability with PKCS#10. See Annex C for references to the documents mentioned in this Note.

NOTE 3 – Other standardization efforts for TTP services in specific environments and applications, like SET or EDIFACT, exist. These are outside of the scope of this Recommendation | International Standard.

NOTE 4 – This Recommendation | International Standard defines technical specifications for services. These specifications are independent of policies, specific legal regulations, and organizational models (which, for example, might define how duties and responsibilities are shared between Certification Authorities and Registration Authorities). Of course, the policy of TTPs offering the services described in this Recommendation | International Standard will need to specify how legal regulations and the other aspects mentioned before will be fulfilled by the TTP. In particular, the policy has to specify how the validity of digital signatures and certificates is determined.

2 Normative references

The following normative documents contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. For dated references, subsequent amendments to, or revisions of, any of these publications do not apply. However, parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the normative documents indicated below. For undated references, the latest edition of the normative document referred to applies. Members of ISO and IEC maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.501 (1997) | ISO/IEC 9594-2:1998, *Information technology – Open Systems Interconnection – The Directory: Models*.
- ITU-T Recommendation X.509 (2000) | ISO/IEC 9594-8:2001, *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- ITU-T Recommendation X.520 (1997) | ISO/IEC 9594-6:1998, *Information technology – Open Systems Interconnection – The Directory: Selected attribute types*.
- ITU-T Recommendation X.680 (1997) | ISO/IEC 8824-1:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.681 (1997) | ISO/IEC 8824-2:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- ITU-T Recommendation X.682 (1997) | ISO/IEC 8824-3:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- ITU-T Recommendation X.683 (1997) | ISO/IEC 8824-4:1998, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- ITU-T Recommendation X.690 (1997) | ISO/IEC 8825-1:1998, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview*.
- ITU-T Recommendation X.813 (1996) | ISO/IEC 10181-4:1997, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Non-repudiation framework*.

2.2 Additional references

- ISO/IEC 9796-2:1997, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Mechanisms using a hash-function*.
- ISO/IEC 9796-3:2000, *Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms*.
- ISO/IEC 10118-1:1994, *Information technology – Security techniques – Hash-functions – Part 1: General*.
- ISO/IEC 10118-2:1994, *Information technology – Security techniques – Hash-functions – Part 2: Hash-functions using an n-bit block cipher algorithm*.
- ISO/IEC 10118-3:1998, *Information technology – Security techniques – Hash-functions – Part 3: Dedicated hash-functions*.
- ISO/IEC 11770-1:1996, *Information technology – Security techniques – Key management – Part 1: Framework*.
- ISO/IEC 11770-2:1996, *Information technology – Security techniques – Key management – Part 2: Mechanisms using symmetric techniques*.
- ISO/IEC 11770-3:1999, *Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques*.
- ISO/IEC 13888-1:1997, *Information technology – Security techniques – Non-repudiation – Part 1: General*.
- ISO/IEC 13888-2:1998, *Information technology – Security techniques – Non-repudiation – Part 2: Mechanisms using symmetric techniques*.
- ISO/IEC 13888-3:1997, *Information technology – Security techniques – Non-repudiation – Part 3: Mechanisms using asymmetric techniques*.
- ISO/IEC 14888-1:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 1: General*.

- ISO/IEC 14888-2:1999, *Information technology – Security techniques – Digital signatures with appendix – Part 2: Identity-based mechanisms*.

- ISO/IEC 14888-3:1998, *Information technology – Security techniques – Digital signatures with appendix – Part 3: Certificate-based mechanisms*.

- ISO/IEC 15946-2 (to be published), *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures*.

3 Definitions

The following term is defined in ISO/IEC 11770-1:

key management

The following term is defined in ISO/IEC 10181-1:

Trusted Third Party (TTP)

The following terms are defined in ITU-T Rec. X.509 | ISO/IEC 9594-8:

CA-certificate
Certification Authority (CA)
public key certificate

NOTE – The shorter term "certificate" will also be used in this Recommendation | International Standard to denote "public key certificate".

certificate policy
certificate revocation list (CRL)
certification path

The following terms are defined in ISO/IEC 10118-1:

hash function
hash-code (hash-value)

The following term is defined in ISO/IEC 14888-1:

domain parameter

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.1 certificate management services: All services needed for the maintenance of the lifecycle of certificates, including registration, certification, distribution, and revocation of certificates.

3.2 certification service: The service of creating and assigning certificates performed by a CA and described in ISO/IEC 9594-8:1995.

3.3 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 protect the sender and the recipient of the data unit against forgery by third parties, and the sender against forgery by the recipient.

NOTE – Digital signatures may be used by end entities (see below) for the purposes of authentication, of data integrity, and of non-repudiation of creation of data. The usage for non-repudiation of creation of data is the most important one for legally binding digital signatures. The definition above is taken from ISO/IEC 9798-1.

3.4 directly trusted CA: A directly trusted CA is a CA whose public key has been obtained and is being stored by an end entity in a secure, trusted manner, and whose public key is accepted by that end entity in the context of one or more applications.

3.5 directly trusted CA key: A directly trusted CA key is a public key of a directly trusted CA. It has been obtained and is being stored by an end entity in a secure, trusted manner. It is used to verify certificates without being itself verified by means of a certificate created by another CA.

NOTE – If, for example, the CAs of several organizations cross-certify each other (see Annex A), the directly trusted CA for an entity may be the CA of the entity's organization. Directly trusted CAs and directly trusted CA keys may vary from entity to entity. An entity may regard several CAs as directly trusted CAs.

3.6 directory service: A service to search and retrieve information from a catalogue of well defined objects, which may contain information about certificates, telephone numbers, access conditions, addresses, etc. An example is provided by a directory service conforming to the ITU-T Rec. X.500 | ISO/IEC 9594-1.

3.7 key distribution service: The service of distributing keys securely to authorized entities performed by a Key Distribution Center and described in ISO/IEC 11770-1.

3.8 non-repudiation of creation: Protection against an entity's false denial of having created the content of a message (i.e. being responsible for the content of a message).

3.9 personal security environment (PSE): Secure local storage for an entity's private key, the directly trusted CA key and possibly other data. Depending on the security policy of the entity or the system requirements, this may be, for example, a cryptographically protected file or a tamper resistant hardware token.

3.10 personalization service: The service of storing cryptographic information (especially private keys) to a PSE.

NOTE – The organizational and physical security measures for a service like this are not in the scope of this Recommendation | International Standard. For organizational measures, refer to ITU-T Rec. X.842 | ISO/IEC TR 14516 Guidelines on the use and management of Trusted Third Party services.

3.11 public key directory (PKD): A directory containing a well defined (sub)set of public key certificates. This directory can contain certificates from different Certification Authorities.

3.12 public key infrastructure (PKI): The system consisting of TTPs, together with the services they make available to support the application (including generation and validation) of digital signatures, and of the persons or technical components, who use these services.

NOTE – Sometimes the persons and the technical components participating in a PKI, by using the services of TTPs, but not being TTPs themselves, are referred to as end entities. An example of a technical equipment used by an end entity is a smartcard which may be used as a storage and/or processing device.

3.13 registration authority (RA): Authority entitled and trusted to perform the registration service as described below.

3.14 registration service: The service of identifying entities and registering them in a way that allows the secure assignment of certificates to these entities.

3.15 time stamping service: A service which attests the existence of electronic data at a precise instant of time.

NOTE – Time stamping services are useful and probably indispensable to support long-term validation of signatures. They will be defined in a separate document.

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

CA	Certification Authority
CRL	Certificate Revocation List
EE	End Entity
OCSP	On-line Certificate Status Protocol
PKD	Public Key Directory
PKI	Public Key Infrastructure
PSE	Personal Security Environment
RA	Registration Authority
TTP	Trusted Third Party

5 Descriptive classification of services

This clause describes services that may be used within the context of TTP services for digital signatures. Here a high-level description for those services is given, this description is independent of data formats, algorithms, description languages, etc.

A detailed specification of some of these services is given in the following clauses.

It is not required that every TTP planning to support the application of digital signatures offers all of these services. It is possible that a number of TTPs, offering different services, cooperate in supporting the use of digital signatures.

NOTE 1 – Because interoperability is the main issue of this Recommendation | International Standard, only those services which are offered by a TTP, either to end entities or to another TTP, are described here. Furthermore, only those services are covered which may be requested and/or delivered by means of standardizable digital messages. (However, this does not imply that standardized messages are in fact defined for all services mentioned in this Recommendation | International Standard.)

The following examples show services that are **not** covered:

1) Logging of security relevant events. With respect to a digital signature PKI this is an internal service of TTPs but not offered to entities.
2) General cryptographic services (e.g. encryption service). Processes like encryption are part of some services but not relevant as stand-alone service in the context of digital signatures.
3) Key archiving or recovery. This may be an internal service for directly trusted CA keys. This will usually not be done for digital signature keys of end entities.

NOTE 2 – Time stamping services will be defined in a separate document.

5.1 Certificate management services

This subclause contains a description of the following services that are part of the certificate lifecycle:

- Registration;
- Public Key Certification;
- Revocation of Certificates;
- Certificate Update; and
- Key Update.

A detailed specification for the online message flow of these services (except certificate status determination) is given in clause 7, and the ASN.1 specification of the data structures needed for these messages is given in clause 8. The analogue specifications for online certificate status determination (see 5.1.3.3, second method) are given in clause 9.

The directory access protocols used to make certificates and CRLs publicly available are not specified here since specifications for these protocols already exist in ITU-T Rec. X.511 | ISO/IEC 9594-3 and ITU-T Rec. X.519 | ISO/IEC 9594-5.

NOTE – Other protocols for directory access are LDAP (RFCs 1777, 2555 and 2587-LDAPv2) or WEB-access (RFC 2585).

Figure 1 gives an overview over the architecture of a PKI with some example services.

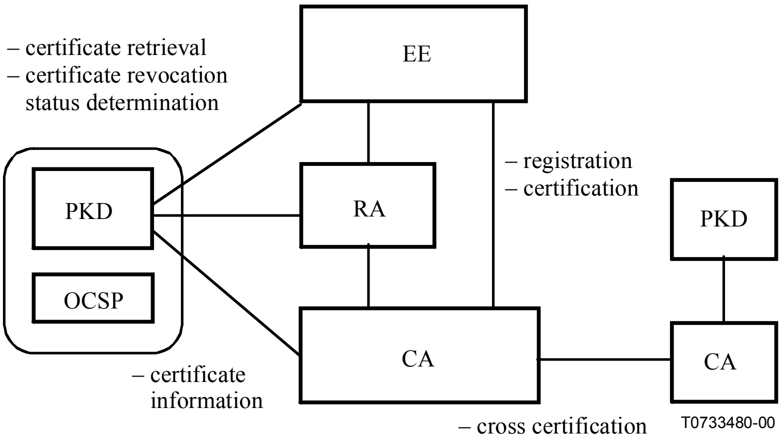

Figure 1 – Overview of Certificate Management Services

5.1.1 Registration

The trustworthiness of any Public Key infrastructure relies on the proper identification and registration of entities.

For all end entities, an RA (which may also be the CA) has to verify the end entity's identity by suitable means, and has to assign an unambiguous and unique name to each end entity within its own domain. The certificate policy determines the kind of means to be used for identification (e.g. ID documents) and whether the end entity has to be present in person. Aliasing of end entity's names may also be required. Those end entities which are technical components are registered according to the security policy for the application, e.g. network management. Applications, for which the distinction between human and non-human end entities is important, should make this distinction clear within the certificate. For example, a "name" could be "device type X", number "Y" located in "Z", the distinction could be made according to policy, or an extension may indicate the difference.

A registration form may be used to collect the relevant data, e.g. name, business unit, business address, and delivery address for the keying material.

EXAMPLE: A scenario within a company may be that each employee has to be present in person at the relevant personnel office, showing his valid identity card. The personnel officer in charge attests the identity and sends a signed registration form to the CA.

5.1.2 Public Key certification

The CA is responsible for the certification process, the binding of an entity's name or a pseudonym with public keys. A certificate format is described in ITU-T Rec. X.509 | ISO/IEC 9594-8.

This Recommendation | International Standard requires that proof of possession of the private key corresponding to the public key included in the certificate is carried out in the course of the certification service. Depending on policy, a CA may guarantee further properties of the public key of the end entity, e.g. by including one or both of the services described in 5.3.2 and 5.3.3.

5.1.3 Revocation of certificates

5.1.3.1 General considerations

A major concern with public key certificates is that they may have to be *revoked* prior to their scheduled expiration time due to different circumstances. Revoking may be done by the issuing CA or by another authority, depending on the policy.

The revocation is mandatory, if a private key is compromised. Other reasons may be change of name, termination of employment, etc.

The certificate policy should state all revocation reasons. Some of these reasons can be found in ITU-T Rec. X.509 | ISO/IEC 9594-8. The policy should include who can request revocations, and also if a specific token can be used to identify entities who are authorized to revoke certificates such as one-time revocation passwords.

5.1.3.2 Revocation methods

Two different methods can be used to revoke certificates:

1) Issuing of a Certificate revocation list (CRL).

   A CRL is a periodically issued list which is signed by the CA and identifies all certificates that are revoked.

   Revocation leads to an immediate entry in the CRL which also includes the time of revocation of the concerned certificate. Additionally, the policy of the CA may require that the certificate is removed from the PKD.

   NOTE – Depending on the policy, it may be suitable to keep the certificate in order to check the validity of signatures made before the revocation date (e.g. if the revocation reason is not key compromise).

   In addition to the periodic publishing, the updated CRL may be published immediately.

   ISO/IEC 11770-1 identifies two different revocation time stamps:

   – The time of known or suspected compromise; and

   – the time at which the CA was notified of the compromise by the entity.

   Depending on the policy, the entry of the certificate in the CRL may be deleted when the certificate expires (compare 5.1.3.3 Certificate revocation status determination).

2) Storing the status of the certificate in an internal trusted database of the CA and offering online certificate status information to entities (compare 5.1.3.3 Certificate revocation status determination).

Both methods may be combined.

If a key is compromised, the standard procedure is to revoke the corresponding certificate, re-initialize the end entity, generate a new public/private key pair, and certify the new public key with the previous attributes.

Depending on the policy, a certificate may:

- be revoked permanently;
- be suspended. The CRL entry includes a flag indicating the status "on hold".

The policy of the CA shall specify what the status "on hold" means with regard to the level of trust it represents to an entity, and how an entity should treat this situation. For example, a certificate might be suspended as a result of an unauthorized revocation request. Some policies do not allow the status "on hold" at all.

EXAMPLE: A policy may state the following: Whenever a verification is performed, it shall be rejected as long as the certificate is suspended. When an evidence is verifiable using a suspended certificate, the result of the verification shall be negative if a result is immediately needed, but can also be interpreted as a conditional validity. When the suspension is followed by a revocation, then the evidence becomes invalid and the revocation date shall be the date of the start of the suspension (i.e. not the date of the end of the suspension).

5.1.3.3 Certificate revocation status determination

This service allows an entity to determine if a certificate is revoked. This can be done by different methods corresponding to the methods of revocation as described in 5.1.3.2:

1) Method 1: Checking the PKD and CRL.
2) Method 2: To request on-line the status from a TTP that is trusted for that purpose. The TTP's answer has to be conveyed in an authentic manner to the entity.

5.1.3.4 Revocation of a CA certificate

A special scenario is encountered if a CA's private key is compromised. If that occurs:

- the certificate of the public key corresponding to the CA's compromised key has to be revoked.

  Trust in the certificates, calculated with the compromised key of the CA, is not provided any more by the CA's signature contained in these certificates. However, it is possible to guarantee the validity of such certificates with other means (e.g. if the certificates are stored in a trustworthy way by a TTP which provides an OCSP service). In any case, the entities should obtain a new certificate and a new directly trusted CA key for future signatures.

  Depending on the policy, the certificates calculated with the compromised key are revoked as a means of informing the end entities about the necessity of getting new certificates.

  In some situations, depending on the certificate policy and the system architecture, new key pairs should be generated for the entities.

  It is important to note that under this scenario, any signatures that were issued before the compromise occurred, and are made secure by additional means (e.g. that are time-stamped by a time stamping authority whose certificate is still valid), may still be considered valid, depending on policy, while any signatures issued after the time of determined compromise, or not made secure by additional means, will be considered invalid.

- if the public key corresponding to the CA's compromised private key is cross-certified with other CAs, an alert message has to be sent to the other CAs. This alert message will notify them to revoke the cross-certified CAs certificate.

5.1.4 Certificate update

In case of expiration of a certificate, it may be updated by issuing a new certificate for the public key of the entity that was already contained in the old certificate.

This method shall not be used if:

- the key pair of the entity is compromised; or
- the state of cryptography indicates that the public key algorithm in connection with the parameters of the key pair may not guarantee security of signatures generated with this key pair for the validity period of the new certificate; or
- the new certificate will have substantial differences in terms of policy, extensions or attributes from the old certificate.

The certificate policy of the CA may specify that a simplified registration procedure is acceptable to issue a new certificate.

EXAMPLE: If the old certificate is not revoked, this may be accepted as sufficient to issue a new certificate.

The change of non-critical attributes in a certificate during its period of validity, such as name or affiliation (e.g. by a change to another department), may also lead to the requirement for a recertification of the amended attributes with the same keys as before. Nevertheless, in this case the previous certificate has to be revoked.

5.1.5 Key update

A new key pair is generated, either by the entity itself or by the TTP, and a certificate is issued for the public key of this new pair.

This method shall be chosen in case of expiration of a certificate if certificate update is not acceptable for one of the reasons given in 5.1.4. Depending on the policy of the CA, it may also be used in other situations.

The certificate policy of the CA may specify that a simplified registration procedure is acceptable to issue a certificate for an updated key.

5.2 Key management services

General descriptions for key management services are given in ISO/IEC 11770 (all parts).

This subclause contains a description only of those key management services that may be offered as a part of services related to the certificate lifecycle (compare 5.1). The detailed specification for the on-line message flow of those services in clause 7, and the ASN.1 specification of the data structures in clause 8, cover the key management services as far as they result in on-line messages between CA, RA and/or EE.

5.2.1 Key generation

In the context of digital signatures, TTPs may generate private/public key pairs for end entities if this is not done by the entities themselves. Though the service might be offered by independent TTPs, it is assumed further on that it is done either by a CA or a RA in response to a certification request or by the end entity prior to a certification request.

5.2.2 Key distribution

5.2.2.1 Distribution of private keys

For the description of the service, "key distribution", different modes of key transmission (on-line or off-line) and the key generating component (TTP or entity) can be distinguished. In the case of a centralized key generation, the TTP is responsible for a secure transmission of the entity's private key and public key certificate. Moreover, it must be ensured that an entity's private key will be sent in a confidential manner. This can be achieved by encrypting this key with a special (symmetric) transportation key known only to the TTP and the corresponding entity. Alternatively, the private key may be transmitted using appropriate secure hardware facilities as for example, smartcards. The transmission of the private key is not necessary if the entity is able to generate its own asymmetric key pair. In this case, the TTP merely has to perform some plausibility checks (e.g. if the entity is able to sign a message with a private key corresponding to the public key), to certify the entity's public key, and to make this certificate available.

5.2.2.2 Distribution of public keys

Public keys must be made available to entities in a way that guarantees their authenticity. In the case of certified public keys, the key distribution is done by distribution of the certificate and authenticity is guaranteed by the signature of the CA which has created the certificate.

In the case of a directly trusted CA key, other means of secure distribution have to be used. If private keys of an entity are distributed to an entity using a secure hardware token, this token can also be used for delivery of the CA key. In other cases an additional process is required. See ISO/IEC 11770-3, subclause 8.1 "Public key distribution without a trusted third party" for methods to do this.

5.2.3 Personalization

The storage of private keys and additional data may be provided by using a physical token. In this situation the personalization of a token has to be supported by the CA, RA or end entities. For example, the personalization of smartcards may include set-up procedures (e.g. creation of the file system), the selection of a random PIN (Personal Identification Number) or password and the shipment and storage of all relevant data within a smartcard.

5.3 Other services

5.3.1 Cross certification

Cross certification is a service offered to allow verification of signatures from end entities with certificates from one CA by end entities with certificates from another CA. For example, a CA1 issues a certificate for a CA2 in another PKI with the effect that entities trusting CA1 can verify certificates of entities in the other PKI via a certification path including this new certificate.

A detailed specification for the on-line message flow of this service is given in clause 7 and the ASN.1 specification of the data structures needed for these messages is given in clause 8.

5.3.2 Domain parameter validation

Domain Parameter Validation is the validation of a proposed set of domain parameters to ensure that each parameter in the set meets all the attributes that are claimed for it.

EXAMPLES:

a) a valid parameter may be required to be a prime: to validate this, a primality test (perhaps probabilistic) is run to make sure that the claimed prime is actually a prime;

b) a valid parameter may be required to be in some arithmetic relationship with some other parameter(s): to validate this, the arithmetic relationship is tested to ensure it holds;

c) a specific weak case (for example, on an exclude list) may be checked to ensure it does not apply to the set in question; or

d) a parameter may be required to be generated by use of a seed in a canonical seeded hash function: to validate this, the seed is input to the canonical seeded hash function to ensure that it actually does generate the parameter.

The generator of a set of domain parameters should ensure that they pass domain parameter validation. Whether anyone else needs to do domain parameter validation depends on the trust relationship between the generator and the entity. If a set of invalid domain parameters is used, unpredictable results may occur, including loss of any intended security. As domain parameters are typically public, it is best if the validation can be done in an off-line manner (that is, not needing the generator of the domain parameters to answer queries) and this is typically the case.

Usually a CA will generate and validate a set of domain parameters which can then be implicitly trusted by all members of the PKI.

5.3.3 Public key validation

Public Key Validation is the validation of a claimed public key to ensure it conforms to the arithmetic requirements for such a key, that is, that the claimed public key is plausible. Public Key Validation assumes that any domain parameters have previously been validated.

EXAMPLES:

a) a valid parameter may be required to be in a specific range of values: to validate this, the claimed parameter is tested to ensure it is in the correct range;

b) a valid parameter may be required to have a specific order (typically a large prime order): to validate this, the claimed parameter is tested to ensure it has the correct order; or

c) a valid parameter may be required to be in a specific arithmetic relationship with some other parameter(s), to validate this, the arithmetic relationship is tested.

If an invalid public key is used, unpredictable results may occur, including loss of any intended security of the owner of the associated private key, recipients of documents signed with that key, or both. A trusted third party, such as a CA, can do Public Key Validation to assure all entities in its domain.

5.3.4 Certificate validation

If an end entity that wants to rely on a digital signature of another end entity is not able to verify the corresponding certificate, it may ask a TTP to do this.

Certificate validation concerns the validity of a single certificate. A single certificate may be supplied in the request, or that single certificate may be supplied and followed by a sequence of certificates (not necessarily forming a certification path).