INTERNATIONAL STANDARD

ISO/IEC 27099

First edition
2022-07

# Information technology — Public key infrastructure — Practices and policy framework

Reference number
ISO/IEC 27099:2022(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

## Contents

Page

# 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection.*

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

# Introduction

The business objective of a public key infrastructure (PKI) is to establish and manage trust relationships. The services provided by the PKI should maintain that trust and organizational and technical security measures for an appropriate security level have to be defined and implemented for all entities participating in a PKI.

Institutions and intermediaries are building infrastructures to provide new electronic transaction capabilities for consumers, corporations, and government entities. As the volume of electronic transactions continues to grow, advanced security technology using digital signatures and trust services can become part of the transaction process. Transaction systems incorporating advanced security technology have requirements to ensure the confidentiality, integrity and availability of transactions conducted over communications networks.

Industry relies on several time-honoured methods of electronically identifying, authorizing, and authenticating entities and protecting transactions. These methods include, but are not limited to, personal identification numbers (PINs) and message authentication codes (MACs) for retail and wholesale transactions, user IDs and passwords for network and computer access, and key management for network connectivity. Over the past 30 years, industry has developed risk management processes and policies to support the use of these technologies.

The ubiquitous use of online services in public networks and the needs of the industry in general to provide safe, private, and reliable transaction and computing systems have given rise to advanced security technology incorporating public key cryptography. Public key cryptography requires a business-optimized infrastructure of technology, management, and policy (a public key infrastructure or PKI, as defined in this document) to satisfy requirements of electronic identification, authentication, message integrity protection and authorization in application systems. The use of standard practices for electronic identification, authentication and authorization in a PKI ensures more consistent and predictable security in these systems and confidence in electronic communications. Confidence (e.g. trust) can be achieved when adherence to standard practices can be ascertained.

Applications serving industry can be developed with digital signature and PKI capabilities. The safety and the soundness of these applications are based, in part, on implementations and practices designed to ensure the overall integrity of the infrastructure. Users of authority-based systems that electronically bind the identity of individuals and other entities to cryptographic materials (e.g. cryptographic keys) benefit from standard risk management systems and the base of auditable practices defined in this document.

This document provides a framework for managing a PKI through certificate policies, certification practice statements, control objectives and supporting procedures. The degree to which any entity in a transaction can rely on the implementation of public key infrastructure standards and the extent of interoperability between PKI-based systems will depend partly on factors relative to policy and practices defined in this document.

In some regions or countries there is a legislative framework which defines requirements for operation of PKI and other related trust services to achieve a recognized level of trust for a specific purpose commonly called “qualified”.

This document is derived from ISO 21188:2018, which content has been generalized in this document to be applicable to any application domain and to take into account general standards for information security. See Annex E for a description of major changes to ISO 21188:2018 clauses that have been made in order to produce this document.

# Information technology — Public key infrastructure — Practices and policy framework

## 1 Scope

This document sets out a framework of requirements to manage information security for Public key infrastructure (PKI) trust service providers through certificate policies, certificate practice statements, and, where applicable, their internal underpinning by an information security management system (ISMS). The framework of requirements includes the assessment and treatment of information security risks, tailored to meet the agreed service requirements of its users as specified through the certificate policy. This document is also intended to help trust service providers to support multiple certificate policies.

This document addresses the life cycle of public key certificates that are used for digital signatures, authentication, or key establishment for data encryption. It does not address authentication methods, non-repudiation requirements, or key management protocols based on the use of public key certificates. For the purposes of this document, the term “certificate” refers to public key certificates. This document is not applicable to attribute certificates.

This document uses concepts and requirements of an ISMS as defined in the ISO/IEC 27000 family of standards. It uses the code of practice for information security controls as defined in ISO/IEC 27002. Specific PKI requirements (e.g. certificate content, identity proofing, certificate revocation handling) are not addressed directly by an ISMS such as defined by ISO/IEC 27001 [26].

The use of an ISMS or equivalent is adapted to the application of PKI service requirements specified in the certificate policy as described in this document.

A PKI trust service provider is a special class of trust service for the use of public key certificates.

This document draws a distinction between PKI systems used in closed, open and contractual environments. This document is intended to facilitate the implementation of operational, baseline controls and practices in a contractual environment. While the focus of this document is on the contractual environment, application of this document to open or closed environments is not specifically precluded.

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements 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/IEC 9594-8, *Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks*

ISO/IEC 19790, *Information technology — Security techniques — Security requirements for cryptographic modules*

## 3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

**3.1**
**access point**
point at which the user may connect to the network or facility

**3.2**
**activation data**
data values, other than keys, which are required to operate cryptographic modules

Note 1 to entry: These data values should be protected.

EXAMPLE A PIN, a pass phrase, a biometric or a manually held key share.

**3.3**
**audit journal**
**audit log**
chronological record of system activities which is sufficient to enable the reconstruction, review, and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results

**3.4**
**authentication**
provision of assurance that a claimed identity of an entity is correct

Note 1 to entry: It applies a) at registration, the act of evaluating an end entity's (i.e. subscriber's) identity and verifying that it is correct for issuing of a *certificate* (3.7); b) during use, the act of comparing electronically submitted identity and credentials.

EXAMPLE User ID and password with stored values to prove identity.

**3.5**
**CA certificate**
public key certificate whose subject is a *CA* (3.17) and whose associated private key can be used to sign certificates or other CA related information

EXAMPLE CA related information includes revocation information, such as OCSP responses or CRLs.

**3.6**
**card bureau**
agent of the *CA* (3.17) or *RA* (3.44) that personalizes a *secure cryptographic device* (3.50) containing the subscriber's private key (as a minimum)

**3.7**
**certificate**
public key and identity of an entity, together with some other information, rendered unforgeable by signing the certificate information with the private key of the certification authority.

**3.8**
**certificate suspension**
**certificate hold**
suspension of the validity of a *certificate* (3.7)

**3.9**
**certificate issuer**
organization whose name appears in the issuer field of a *certificate* (3.7)

**3.10**
**certificate management**
process that covers the complete lifecycle from the initialization phase to the issuing phase to the cancellation phase

**3.11**
**certificate manufacturer**
**CM**
agent who performs the tasks of applying a digital signature to a certificate signing request on behalf of the *certificate issuer* (3.9)

**3.12**
**certificate policy**
**CP**
named set of rules that indicates the applicability of a certificate to a particular community or class of application with common security requirements

**3.13**
**certificate profile**
specification of the required format (including requirements for the usage of standard fields and extensions) for a particular type of *certificate* (3.7)

**3.14**
**certificate rekey**
process whereby an entity with an existing key pair and *certificate* (3.7) receives a new certificate for a new public key, following the generation of a new key pair

**3.15**
**certificate renewal**
**rollover**
process whereby an entity with an existing key pair and *certificate* (3.7) receives a new certificate for the same public key as the existing certificate, and with a new validity period

**3.16**
**certification**
creation of a public key certificate for a *subject* (3.53)

**3.17**
**certification authority**
**CA**
**issuing CA**
*entity* (3.28) that is identified as the issuer of a public key certificate

**3.18**
**certification path**
ordered list of one or more certificates, starting with a public-key certificate signed by the trust anchor, and ending with the public key certificate to be validated

EXAMPLE All intermediate public-key certificates, if any, are CA-certificates in which the subject of the preceding certificate is the issuer of the following certificate.

**3.19**
**certification practice statement**
**CPS**
statement of the practices employed by a *certification authority* (3.17) in issuing, managing, revoking, renewing, and rekeying certificates and which defines the equipment, policies, and procedures the CA uses to satisfy the requirements specified in the certificate policies that are supported by it

**3.20**
**certification request**
submission of a validated registration request by an *RA* (3.44), its agent or a subject to *a CA* (3.17) to register a subject's public key to be placed in a *certificate* (3.7)

**3.21**
**certificate revocation status**
status of a certificate, typically provided by a CA, that indicates whether a certificate within its validity period should be considered live, suspended, or revoked

**3.22**
**certificate validity**
determination at a particular time as to whether that time was within a certificate's validity period, was acceptable for the intended use, and possessed an acceptable *certificate revocation status* (3.21)

**3.23**
**certificate validity period**
bounded period of time that the *certificate* (3.7) is deemed fit for intended use

Note 1 to entry: Prior to this time, a certificate is pre-valid; following this time, a certificate is expired.

**3.24**
**compromise**
violation of the security of a system such that an unauthorized or unintended disclosure, modification, or falsification of sensitive information may have occurred

**3.25**
**cross certification**
certification of each other’s public keys by two *CAs* (3.17)

Note 1 to entry: This process may or may not be automated.

**3.26**
**digital signature**
cryptographic transformation that, when associated with a data unit, provides the services of origin authenticity, data integrity and signer non-repudiation

**3.27**
**end entity**
certificate subject that uses its private key for purposes other than signing certificates

**3.28**
**entity**
person, partnership, organization, or business that has a legal and separately identifiable existence

EXAMPLE A legal entity or an individual or *end entity* (3.27), or a *certification authority* (3.17), or *registration authority* (3.44).

**3.29**
**fingerprint**
sequence of bytes created by applying a cryptographic hash function over the encoding of a *certificate* (3.7) and may be used by the recipient to check the public key’s authenticity and integrity

**3.30**
**hardware token**
device which generates, uses, and stores cryptographic keys in a secure manner

**3.31**
**key escrow**
management function that allows access by an authorized party to a replicated private encipherment key

**3.32**
**key recovery**
ability to restore an entity’s private key or a symmetric encipherment key from secure storage in the event that such keys are lost, corrupted or otherwise become unavailable

**3.33**
**multiple control**
condition under which two (dual) or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key

**3.34**
**object identifier**
**OID**
unique series of integers that unambiguously identifies an information object

**3.35**
**online certificate status mechanism**
mechanism that allows *relying parties* (3.46) to request and obtain certificate status information without requiring the use of *CRLs*

**3.36**
**online certificate status protocol**
**OCSP**
protocol for determining the current status of a *certificate* (3.7) in lieu of or as a supplement to checking against a periodic *CRL* and which specifies the data that need to be exchanged between an application checking the status of a certificate and the server providing that status

**3.37**
**PKI disclosure statement**
document that supplements a *CP* (3.12) or *CPS* (3.19) by disclosing critical information about the policies and practices of a *CA* (3.17)/*PKI* (3.42)

Note 1 to entry: A PKI disclosure statement is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP or CPS documents. Consequently, it is not intended to replace a CP or CPS.

**3.38**
**PKI trust service provider**
one or more certification authorities providing a trust service with coherent policies and practices.

**3.39**
**policy authority**
**PA**
party or body with final authority and responsibility for specifying *certificate policies* (3.12)

Note 1 to entry: The policy authority may also ensure that *CA* (3.17) practices and controls as defined by the *CPS* (3.19) fully support the specified certificate policies

Note 2 to entry: A policy authority is often referred to as a policy management authority.

**3.40**
**policy mapping**
recognition that when a *CA* (3.17) in one domain certifies a *CA* in another domain, a particular *certificate policy* (3.12) in the second domain can be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain

Note 1 to entry: Policy mappings may be supported by information in cross-certificates.

**3.41**
**policy qualifier**
policy-dependent information that accompanies a *certificate policy* (3.12) identifier in an X,509 v3 certificate

**3.42**
**public key infrastructure**
**PKI**
structure of hardware, software, people, processes, and policies that employs digital signature technology to facilitate a verifiable association between the public component of an asymmetric public key pair with a specific subscriber that possesses the corresponding private key

Note 1 to entry: The public key may be provided for digital signature verification, authentication of the subject in communication dialogues, or for message encryption key exchange or negotiation

**3.43**
**PKI trust service provider**
**trust service provider**
trusted provider of services which support the use of public key certificates

**3.44**
**registration authority**
**RA**
entity whose primary functional role and responsibilities include identity validation of the subject for approving *certificate requests* (3.20) submitted to a *CA* (3.17)

Note 1 to entry: An RA can assist in the certificate application process, the revocation process or both. The RA does not need to be a separate body, but can be part of the CA.

**3.45**
**registration request**
submission by an entity to an *RA* (3.44) (or *CA* (3.17)) to register the entity's public key in a *certificate* (3.7)

**3.46**
**relying party**
**RP**
recipient of a *certificate* (3.7) who acts in reliance on that certificate, digital signatures verified using that certificate, or both

**3.47**
**relying party agreement**
**RPA**
statement provided by the *CA* (3.17) of the responsibilities between the relying party, the subject, and the CA

Note 1 to entry: The RPA may be included in the *CPS* (3.19) or provided as one or more external documents.

**3.48**
**repository**
system for storage and distribution of certificates and related information

EXAMPLE Certificate storage, certificate distribution, *certificate policy* (3.12) storage and retrieval, certificate status.

**3.49**
**root CA**
CA at the apex of a CA certificate hierarchy

Note 1 to entry: A root CA may be used as a *trust anchor* (3.58). Generally, the root CA certificate is self-signed, in which the identity and public key in the certificate are the same as the identity of the *certificate issuer* (3.9) and public key used to verify the certificate issuer's signature.

**3.50**
**secure cryptographic device**
device which holds the user's private key, protects this key against compromise and performs signing or decryption functions on behalf of the user

[SOURCE: ETSI TR 119 001]

EXAMPLE Key generation, cryptogram creation, PIN translation, certificate signing and secure storage of private keys.

**3.51**
**signature validation**
verification and confirmation that a digital signature is valid

Note 1 to entry: See also *certificate validity period* (3.23).

**3.52**
**signature verification**
check of the cryptographic value of a signature using data

**3.53**
**subject**
entity that controls the asymmetric key pair and may also be a *relying party* (3.46)

**3.54**
**subordinate CA**
**sub-CA**
**intermediate CA**
*CA* (3.17) that is lower relative to another CA in the CA hierarchy

**3.55**
**subscriber**
entity subscribing with a *certification authority* (3.17) on behalf of one or more subjects

Note 1 to entry: Where appropriate a subscriber may be represented by a natural person who is,

i) an employee of the subscriber, or

ii) an authorized agent of the subscriber

and who has express authority to represent the subscriber for specified purposes.

**3.56**
**tamper-evident**
evidence that an attack has been attempted

**3.57**
**terms and conditions**
collection of all documents issued by the CA which define the duties and rights of the PKI members

**3.58**
**trust anchor**
entity that is trusted by a relying party and used for validating certificates in certification paths

**3.59**
**trusted role**
job function that performs critical functions which, if performed unsatisfactorily, can have an adverse impact upon the degree of trust provided by the *CA* (3.17)

**3.60**
**trust service**
electronic service which enhances trust and confidence in electronic transactions

**3.61**
**validation service request**
enquiry by the *relying party* (3.46) to a validation service to check the validity of a *certificate* (3.7)

## 4 Abbreviated terms

| | |
|---|---|
| ASN.1 | Abstract Syntax Notation One |
| CRL | Certificate revocation list |
| CVSP | Certificate validation service provider |
| FIPS | Federal Information Processing Standard |
| FQDN | Fully qualified domain name |
| FTP | File transfer protocol |
| HSM | Hardware security module |
| HTTP | Hypertext transfer protocol |
| ID | Identifier |
| IETF | Internet Engineering Task Force |
| ISMS | Information security management system |
| MAC | Message authentication code |
| MITM | Man-in-the-middle attack |
| OID | Object identifier |
| PIN | Personal identification number |
| PKI | Public key infrastructure |
| RFC | Request for comment |
| RTO | Recovery time objective |
| SLA | Service level agreement |
| TLS | Transport layer security |
| TSA | Time-stamping authority |
| URL | Uniform resource locator |
| UTC | Coordinated universal time (Zulu or Greenwich Mean Time, Time GMT) |

## 5 Public key infrastructure (PKI) general concepts

### 5.1 General

This clause provides some background information in order to better understand the context in which these policies and practices are used within a PKI.

## 5.2 What is PKI?

### 5.2.1 General

This subclause describes the components of a PKI and illustrates the roles with responsibilities undertaken by the various entities within the PKI. The rapid growth of electronic commerce has brought with it the desire to conduct business-to-business, business-to-consumer, and government-to-consumer transactions across open networks such as the Internet. The design of the network transmission protocols creates problems for organisations and their customers conducting business transactions, who require the electronic identification and authentication of the transacting parties, proof of origin, message integrity protection and confidentiality services. Electronic authentication also raises significant issues with respect to evidence and contract, liability, privacy, consumer protection and trade.

Relying parties, as recipients of information, use TSPs to validate certificates used to authenticate online communications. A TSP can be an entity providing one or more trusted services, e.g. a certification authority, a registration service, or a revocation status service. A TSP is a recognized authority trusted by one or more relying parties to create and sign certificates. A TSP can also revoke certificates it has created and issued. A TSP operates one or more certification authorities (CAs) whose core functions are certificate issuing, certificate distribution and revocation status. Within an organization, a CA is not necessarily a business entity but can be a unit or a function providing CA functions that may be trusted by relying parties and subscribing parties.

Public key technology is used to support confidentiality, integrity, and authentication requirements. With public key cryptography, two keys are created (private and public). The private key is kept secret and the public key can be made publicly available in a certified form which guarantees its authenticity. The subject’s public key and identifying data are signed by the CA’s private key to create a certificate.

Certificates are created under certificate policies. Revealing the public key does not compromise the private key.

Organisations may use a PKI to service their business needs in the following example environments, depending upon their relationship with the relying party.

a) **Closed environment**: all entities (certificate subjects and relying parties) adhere to a single Organization’s trust service and share at least one certificate policy. An entity adhering to a trust service may act as a relying party or subscriber for certificates for itself or on behalf of other certificate subjects. In this case, subscribers and certificate subjects may be distinct entities bound by a business relationship which is outside the scope of this document.

b) **Contractual environment**: certificate subjects and relying parties can have separate TSPs. TSPs are bound by differing forms of contract covering certificate use. These forms comprise:

   1) multilateral, under agreed rules, with a single certificate policy;

   2) bilateral cross certification that can use different certificate policies;

   3) accreditation bridge that can recognize different certificate policies through a central organization or entity. This can be realized by the central organization publishing a trust list of certificate policies, or of certification authorities, which conform to common policy requirements.

See Figure 1 and Table 1.

c) **Open environment**: the organization can act as a TSP issuing certificates to the public and permits validation of certificates in an open network environment. TSPs can operate under voluntary TSP accreditation schemes or within an indigenous regulatory framework. Typically, there is no formal contract between the subscriber's TSP and the relying party.

NOTE An example of an open PKI is a trust service provider issuing certificates under REGULATION (EU) No 910/2014 (eIDAS).

A PKI comprises technical, process and people components that should harmonize into an effective infrastructure. As with any infrastructure, the business requirements should be initially determined. These requirements can be met by the deployment of a PKI.

See Annex D for a general description of the roles of certificates and PKI components.

### 5.2.2 Public key infrastructure process flow

The responsibilities, services and procedures required by a public key infrastructure are as follows:

- key generation;
- registration;
- certificate generation;
- distribution;
- usage;
- management of certificate expiry;
- renewal;
- rekey;
- revocation management;
- revocation status checking.

## 5.3 Use of PKI Service components within example business flows

### 5.3.1 General

The elements of the PKI process flow described in 5.2.2 may be provided by separate components of a PKI service, for example certificate generation and revocation status which are used to support separate parties as illustrated in Figure 1 below.

### 5.3.2 Illustration of certificate application in a contractual PKI environment

This subclause describes the organization using the PKI for support transactions to its customers within a scheme or where a contract with rules has been established between the parties. The corresponding PKI may be open or closed, and when closed the PKI is a third-party service provider. It will provide either certificate issuance or certificate validation services, or both services, to its customers, see Figure 1.

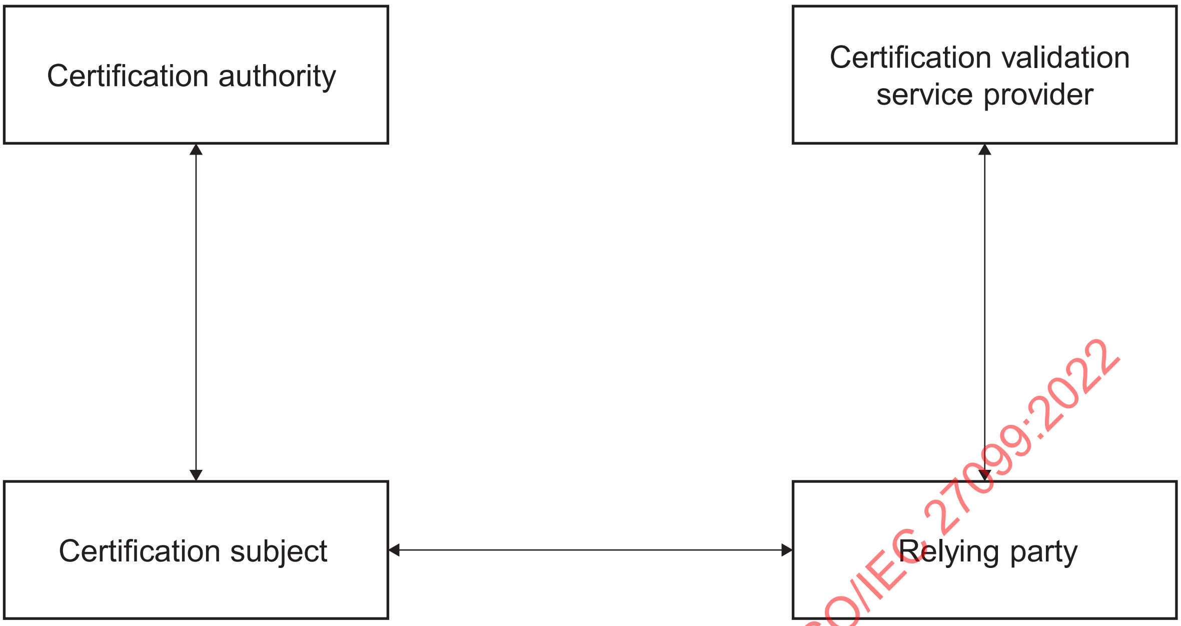

**Figure 1 — Four entities in a contractual environment**

Certificate validation service is for example, a service checking the validity of a certification path in accordance with RFC 5280:2008, section 6.

These service components can be used for example as in the illustrative business processes given in Table 1:

**Table 1 — Certificate application scenarios in a contractual environment**

| | Sample scenario | Sample requirements | PKI operations |
|---|---|---|---|
| 1 | Organization employee sends an email to a recipient. | — Authentication of sender for recipient. | — Organization requests certificate generation service component to provide new certificate for the employee prior to sending any messages<br>— Employee/sender digitally signs the email message<br>— Recipient checks the certificate validity including checking the certificate revocation status<br>— Recipient checks digital signature on email message using the public key from the employee certificate. |

**Table 1** *(continued)*

| | Sample scenario | Sample requirements | PKI operations |
|---|---|---|---|
| | | — Message integrity. | — Organization requests certificate generation service component to obtain new certificate for the employee prior to sending any messages<br>— Employee/sender digitally signs the email message<br>— Recipient checks digital signature. |
| | | — Confidentiality protection for message contents. | — Organization requests certificate generation service component to obtain new certificate for the employee prior to sending any messages<br>— Sender fetches the recipient's certificate from a shared directory<br>— Sender checks the certificate validity including its revocation status<br>— Sender encrypts message using recipient's public key<br>— Recipient decrypts message using recipient's private key. |
| 2 | Customer submits a purchase order to a merchant. | — Customer authorizes purchase order.<br>— Authentication of customer by merchant.<br>— Transaction message integrity. | — Customer requests certificate generation service component to provide new certificate for the employee prior to sending any messages<br>— Customer digitally signs purchase order with private key. |
| | | | — Recipient validates sender's certificate including status, certificate checking the revocation. |
| | | | — Merchant verifies digital signature. |
| 3 | Customer receives invoice from merchant. | — Message authentication. | — Check digital signature and validate certificate including checking the certificate revocation status. |
| 4 | An existing customer using an e-banking service to send high value payment instructions to bank. | — Strong mutual authentication.<br>— Message integrity.<br>— Confidentiality. | — Customer requests certificate generation service component to provide new certificate for the employee prior to sending any messages<br>— Customer validates bank's server certificate including checking the certificate revocation status<br>— Bank validates customer's certificate including checking the certificate revocation status. |
| | | | — Bank verifies digital signature. |

**Table 1** *(continued)*

| | Sample scenario | Sample requirements | PKI operations |
|---|---|---|---|
| | | | — Customer fetches Bank's certificate from repository<br>— Sender checks the certificate validity including its revocation status<br>— Customer encrypts message using Bank's public key<br>— Bank decrypts message using Bank's private key. |

## 5.4 Certification authority (CA)

A CA has a public/private key pair and uses a digital signature algorithm to produce certificates.

The CA's main purpose is to manage the certificate life cycle, see 7.15. The CA may delegate appropriate activities to a registration authority.

The binding of the entity's public key to its identity is accomplished by having the CA generate the certificate, thereby attesting to the relationship of the information therein and providing assurances of its integrity.

The binding of the entity's public key to its identity is validated using a CA trusted by the relying party, called the trust anchor. A chain of CA certificates is then validated up to the end entity's certificate. The trust anchor is commonly distributed as a CA Certificate, which may be self-signed if the trust anchor is a root CA. The trust anchor is distributed by secure means outside the PKI.

IETF RFC 5280 provides an example process for validation of a certificate chain (or path) from the trust anchor:

- Entities (including CAs) can use these certificates to authenticate themselves to relying parties. Hence, authentication can involve a chain of certificates. The verification of a chain of certificates begins with the trusted CA public key and ends with the certificate being validated. The trusted CA public key is to be obtained and authenticated by some means other than by the use of certificates. This is to ensure that the process begins securely. See ISO/IEC 9594-8.
- Once a certificate has been generated, the integrity of its contents is protected. This document does not require that certificates be given confidentiality protection. A valid copy of the CA's public key and the identity used as the certificate issuer is required by the relying party in order to validate a certificate.
- To communicate outside the root CA's domain, the root CA cross-certifies with the desired remote domain. Certification path validation then involves building a chain of certificates from the remote entity to the root CA by way of the cross-certified remote CA.
- In a non-hierarchical architecture, independent CAs can cross-certify each other by issuing certificates to each other. This results in a general network of trust relationships between CAs and allows each group (such as a retail credit authorization network, a clearing house, an organization, or a subgroup thereof) to have its own CA. An entity uses the public key of a selected CA for its trusted CA public key. The certification path consists of those certificates that chain back from the certificate being validated to the trusted CA of the relying party.
- In a bridge architecture, two or more independent hierarchical architectures are interconnected by a common bridge CA which cross certifies with each root CA. The separate root CAs are peers to each other and the bridge CA such that they do not need to cross certify with each other. The bridge CA allows a relying party in one hierarchical architecture to validate the certificate chain from another hierarchical architecture.

- A bridge can be realized by a common trusted authority issuing a list of trusted certification authorities.
- A compromise of the private key of a CA compromises all entities certified by that CA, because the holder of that private key can generate fraudulent certificates and then masquerade as one or more end entities or through cross-certification with one or more entities. Failure to provide compensating controls to deal with the possibility of compromise of transactions in a network can have catastrophic effects on organisations and their customers.
- Two or more CAs can join a common scheme for mutual recognition, e.g. implemented by a trust list. See also 5.10.1 for further discussion on trust models.

## 5.5 Business perspectives

### 5.5.1 General

In defining the business operations of the organization, many issues will be addressed.

### 5.5.2 Business risks

There is a business need to manage risks in conducting electronic commerce. PKI is one such control mechanism that can provide appropriate protection to manage those risks. PKI is a control mechanism that can be used for many different applications and can be seen as a common, reusable technology.

### 5.5.3 Applicability

The parties involved determine whether the certificate policy is appropriate to the business application and associated risks.

### 5.5.4 Legal issues

The legal perspective considers the certificate as an assertion, or a series of assertions made by the certification authority about the subject to the relying party. The CP (perhaps augmented by the CPS) establishes what assertions the certification authority is making. It can also specify what warranties the certification authority offers that these assertions are true, and what liabilities will be assumed or allocated by the certification authority in the event that an assertion is untrue. It can specify any limitations to these liabilities, such as specifying a group whose members are the only parties permitted to act as relying parties. It can specify the maximum liabilities per certificate or per transaction and specifies the types of transaction in which the warranties are in effect. It specifies procedures for submission of claims and for resolution of disputes. It specifies any conditions a relying party should fulfil or actions a relying party should perform before being authorized to rely on a certificate and its assertions.

The responsibilities and liabilities relating to a PKI, particularly where different businesses are involved, are commonly a major issue for a contractual PKI environment. The responsibility for and scale of commercial liability will be a significant factor in setting out the business requirements, especially for trust services.

For example, the European regulation (EU) No 910/2014 (the eIDAS regulation) defines requirements for qualified trust service provider for issuing qualified certificates supporting electronic signatures, electronic seals, and website authentication.

### 5.5.5 Regulatory issues

The regulatory perspective considers differences in the acceptability of PKI processes and services in the conduct of business related in alternative jurisdiction, industry standards or industry audit functions.

### 5.5.6 Business usage issues

Business usage, as described in 5.3, is between the entities defined in the environment (i.e. the certificate subject or, where applicable, the subscriber and the relying party). All parties should fulfil their obligations set forth in the CP or the agreement that defines these obligations. The certificate subject or, where applicable, the subscriber can then use the digital signature process to authorize a message or transaction and subsequently the relying party can then rely upon the authenticated signature.

Optionally, under a warranty scheme, a reliance limit can be established by the CP or by separate agreement. Where this is the case, the relying party can choose to seek a guarantee for that transaction, up to a specific limit.

### 5.5.7 Interoperability issues

The disparate business practices and related policies are often a further challenge in an open PKI environment from business and technological perspectives. However, in a contractual PKI environment, rules of operation are established specifically to overcome interoperability issues. In a closed environment, where the certificate issuer and the relying party are the same organization, it is up to that organization to resolve any interoperability issues. The disparate policies regarding use of the PKI need to be considered in setting out the business requirements for trust services.

The interoperability of trust services for organisations requires a governance framework that addresses the issues of:

- legal jurisdiction and responsibilities;
- commercial risk management considerations;
- technical recognition of the certificate and operational processing aspects;
- policy and trust scheme obligations.

Non-technical interoperability issues are resolved by adherence and by conformance to the contractual rules of the environment that describe the business contract responsibilities and liabilities according to the business application under the certificate policy interpretation.

The detailed CPS by itself does not form a suitable basis for interoperability between CAs operated by one or by different organizations. Rather, certificate policies best serve as the vehicle on which to base common interoperability standards, certificate requirements and common assurance criteria for an industry or global basis.

A CA with a single CPS can support multiple certificate policies (e.g. used for different application purposes or by different certificate user communities). In addition, different CAs, with nonidentical certification practice statements, can support the same CP.

a) A CP can apply more broadly than to just a single organizational unit or single organization. If a particular CP is widely recognized, it has great potential as the basis of automated certificate acceptance in many systems.

b) Organisations that operate public or inter-organizational certification authorities should document their own practices in CPSs. The CPS is one of the organization's means of protecting itself and positioning its relationships with subscribers and other entities.

c) Technical implementation can differ due to interpretation of standards and protocols by the PKI integrators. A technical comparison takes place within the PKI environment to ensure technical interoperability.

For interoperability of PKIs operated by different CAs, there is a need for a trusted path to enable a relying party to verify the certificates issued by another CA. This trusted path can be provided by one CA issuing a cross-certificate to another. This can even involve other third party CAs that assist in providing a trusted path through a chain of cross-certificates. Care needs to be taken in the policy implications of such cross-certificates and in particular that the implied trust relationship is matched by an appropriate business relationship.

CAs can be organized in a hierarchy with a “root” CA that is trusted by all relying parties to issue CA certificates for subordinate CAs. Special attention needs to be paid to the security controls applied to such root CAs since the impact of any successful attacks on such root CAs can be very significant. Furthermore, the needs for some areas of the policies and practices of such a root CA with regards to functions such as registration are likely to significantly differ.

## 5.6 Certificate policy (CP)

### 5.6.1 General

A CP is a common set of rules with regard to the level of trust that are met by associated certificates used for a particular purpose. The CP also specifies the criteria that are agreed upon and complied with by a certification authority before certificates issued by such a certification authority may be accepted by a relying party.

The entity that develops and maintains the CP can be known as the policy authority.

The CP focuses on what the certificate is to be used for and is defined independently of the details of the specific certificate operating environment policy usage of a CA.

The purpose of a CP includes:

- to define and limit the use of certificates;
- to specify requirements and obligations of certificate subject and, where applicable, subscriber, the certification authority and relying parties;
- to define liabilities for certificate subject and, where applicable, subscriber, the certification authority and relying parties;
- to specify policy administration process;
- to specify governing law.

It is recommended that the CP is based on IETF RFC 3647. Controls are defined in Clause 7.

In contractual environments, the CP may be subordinate to, or referenced from, contractual requirements established with a CA.

The PA that registers the object identifier also publishes a textual specification of the CP for examination by certificate users (See Annex A for additional information).

### 5.6.2 Policy Authority and certificate policy usage

A policy authority specifies the certificate policy that is adopted by the certification authorities that have their controls described in certification practice statements. A CP is created, maintained, distributed, and interpreted by the policy authority. The policy authority can either be represented by one organization or jointly by a number of major stakeholders.

Certificate policies are created for specific purposes within a PKI and business environment. There can be many certificate policies within one PKI, each defining the business/policy requirements for groups of certificates sharing common policy requirements. In each case the specific certificate policy can be developed by a policy authority. Alternatively, a PKI may adopt a standardised certificate policy (e.g. as defined in CA/Browser Forum Baseline Requirements or ETSI EN 319 411-1) directly or as the basis of its own policy.

As an example, a company wishing to transact with another company can require for business reasons the use of digitally signed messages. Each party would need to define their business requirements and adopt a certificate policy that meets those requirements. Both parties need to obtain a certificate from a certification authority that supports that certificate policy.

Examples of different certificate policy usage would include, but not be limited to:

a) subscription to the certificate policy for specific functional applications (e.g. server identification certificate for customer to authenticate their online service provider);

b) subscription to the certificate policy that matches the business application (e.g. customer signing a purchasing order from a merchant);

c) subscription to the certificate policy that matches a generic security application with a defined environment within prespecified restrictions (e.g. providing confidentiality protection on all message types to certificate subject across the Internet).

### 5.6.3 Certificate policies within a hierarchy of trust

PKIs can be structured into a hierarchy with the top or apex of the hierarchy being a root. The root delegates a portion of its trust to subordinate CAs based upon the organizational needs. The root and intermediate levels primarily authenticate and sign the digital certificates of subordinate levels and provide the structuring of business requirements by differentiating between organizational needs (e.g. between geopolitical or organizational regions, countries or states, organizational units). As illustrated in 5.12, the hierarchies permit the use of multiple certificate policies, each defining the different business requirements of facets of the business environment. With a hierarchy, each level is more granular or homogenous in its specificity of requirements to a “smaller” group of certificates issued to end-entities. Each group of certificate end-entities share a common set of certificate policies.

For example, the root level at the highest level of the hierarchy may be reflected as a self-signed certificate. It may be used as a trust anchor for the validation of certificates in the hierarchy.

The private key associated with this root certificate may have the complete capability and trust associated with the CA. This root can issue subordinate CAs, in order to compartmentalize risk and trust. The subordinate CAs may cascade into multiple levels, each trying to further reduce risk factors, such as separating out different certificate policies or limiting capabilities, or it may issue end-entities directly. In a hierarchy, the root is the most trusted point. Each subordinate level shares the trust between their peers, but each trusts the superior point from which they have been delegated responsibility.

Examples of different certificate policy usage include, but are not limited to:

a) certificate policy for identifying the root CA with its implied self-signed certificate (certificates issued under Policy A in Figure 2);

b) certificate policy for identifying a subordinate CA established under the root CA or another subordinate CA. To sign the public keys of the subordinate or intermediate CAs, the root CA acting as the ultimate parent in the CA hierarchy in the organization (certificates issued under Policy B in Figure 2).

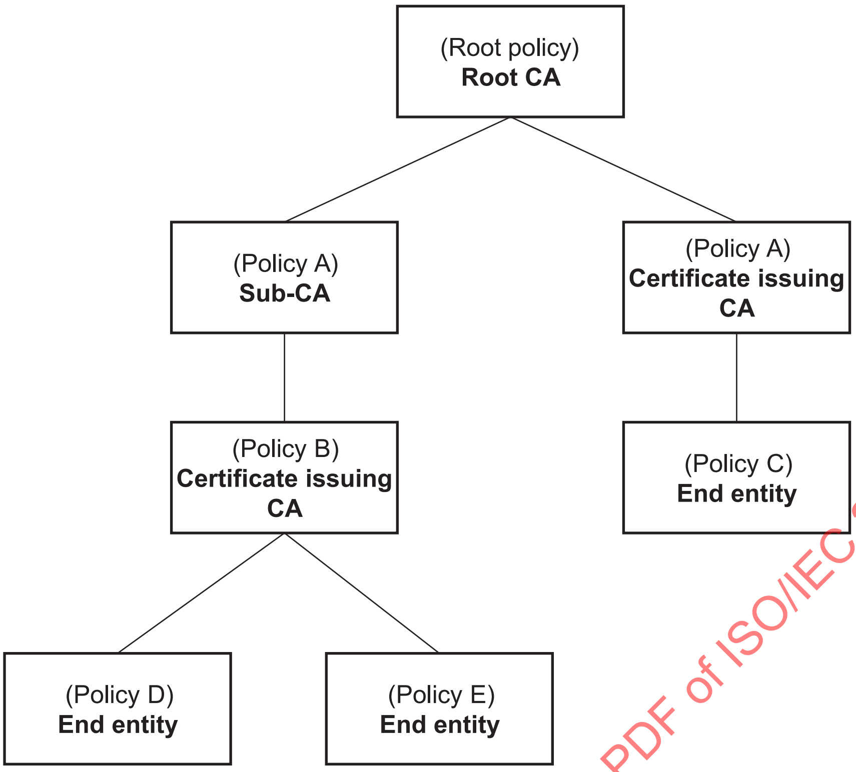

**Figure 2 — Root hierarchy creates a hierarchy of trust**

### 5.6.4 Certificate status

A policy authority specifies the conditions applicable to the states of a certificate issued under a specific CP.

A certificate may be in one of the following states at a given time. These states are not exclusive:

a) pre-valid - not yet operational; if the certificate expresses a validity period, the given time is prior to the commencement of the validity period;

b) live - operational; if the certificate expresses a validity period, the given time is during the validity period;

c) suspended - not operational; if the certificate expresses a validity period, the given time is during the validity period;

d) revoked - not operational; if the certificate expresses a validity period, the given time is during the validity period;

e) expired - not operational; if the certificate expresses a validity period, the given time is after the validity period.

Once a certificate is revoked or has expired it cannot return to an operational state.

The policy authority specifies the conditions applicable to the states of a certificate issued under a specific CP.

## 5.7 Certification practice statement (CPS)

### 5.7.1 General

The certification practice statement describes the necessary and sufficient procedures and controls employed by the CA in issuing, managing, revoking, and renewing or re-keying certificates.

The purpose of the certification practice statement is to clearly define the CA's procedures and practices to manage the risks associated with certificate policies. A useful approach in completing the certification practice statement is to follow IETF RFC 3647 and clearly define the step-by-step practices from certificate request/issuance, certificate verification and required supporting functions.

As indicated earlier, the CA is the entity responsible for performing the six service components (see 5.11) of a) registration, b) certificate manufacturer, c) dissemination, d) revocation management, e) revocation status service and f) subject device provision (optional). The CA is responsible for clearly defining the controls to accomplish these component services in meeting the requirements set forth in the CP. The controls are documented in the certification practice statement (CPS). The services and functions of a CA can be securely delegated in any manner it desires.

A CPS can take the form of a declaration by the CA of the details of its trustworthy system and the practices it employs in its operations to securely issue and manage its certificates. Portions of a certification practice statement can also be part of the contract between the CA and the subscriber.

The PKI disclosure statement may supplement a CP or CPS by disclosing critical information about the policies and practices of a CA. It does not substitute or replace the CP or CPS under which digital certificates are issued.

### 5.7.2 CPS creation

A certification authority in support of its operation prepares a CPS or an equivalent document as evidence of its ability to comply with one or many certificate policies. A formal CPS may not be compulsory in a contractual PKI environment and is often determined by either the rules of the community or the policy authority. While a simple conformance statement can suffice with a contractual PKI environment, a CPS, nevertheless, provides guidance for both internal processing and processing completed by delegated roles.

### 5.7.3 Purpose

The purpose of a certificate policy is to state "what is to be adhered to" by the CA, the subject and the relying parties, while a CPS states "how the certificate policy is adhered to" by the CA (i.e. the control processes the CA will use in creating and maintaining the digital certificate). The CP may be referenced in the digital certificate (in its "Certificate Policies" attribute). The relationship between the CP and CPS is similar in nature to the relationship of other business policies that state the requirements of the business, while operational units define the practices and procedures of how these policies are to be carried out.

### 5.7.4 Level of specificity

A certificate policy is prescriptive.

A certification practice statement is descriptive and detailed. Such documents are generally defined as internal operating procedure documents that can describe specific tasks and responsibilities within an organization. Such documentation can be used in the daily operation of the CA and reviewed by those performing a process review or audit.

### 5.7.5 Approach

The CP is based upon known business requirements.

A CPS is tailored to the organizational structure, operating procedures, facilities, and computing environment of a certification authority.

### 5.7.6 Audience and access

In general, the CP is managed as public information in the contractual environment, and therefore widely disseminated by the PA to all participants.

A CPS is a statement by a CA as to the control practices it will follow in issuing and maintaining certificates and clearly defines how its practices fully support the CP identified.

For example, the CP can state that all certificate registration transactions are considered sensitive and for reasons of individual privacy, all such transactions will be protected during transmission and storage. The CPS can then further identify that all certificate registration transactions will be encrypted during transmission and list the business divisions that are allowed access to the stored information. The CPS can also specify the algorithms and key lengths used for encryption during transmission and the access control mechanism used for storage. The CA's operating procedures, rather than the CP or CPS, would typically include more detailed information about the administration of the access control mechanisms.

## 5.8 Agreements

This subclause describes the relationships between the parties involved in the provision and use of PKI services and the associated agreements between these parties used to lay out their relative obligations.

The entity responsible for the provision of overall PKI service is the organization identified as the certificate issuer in the certificate, commonly referred to as the certification authority (CA).

The terms and conditions for the issuing of certificates by the CA to one or more subjects is laid out in a subscriber agreement between the CA and the entity subscribing to the CA. The subscriber agreement also binds the subscriber to its obligations.

The obligations between the CA and the entity relying on the certificate, for example to verify a signature received or encrypt data to be sent, are laid out in a relying party agreement.

A CA may sub-contract part of the obligations in a subscriber or relying party agreement to a separate service component provider. For example, all or part of the subscriber agreement may be taken on by the provider of registration services; or part of the relying party agreement relating to provision of revocation may be taken on by a provider of revocation management or revocation status services. However, ultimately it is the CA as identified as the certificate issuer who is responsible. Typically, there will be no requirement for a contract between the subscriber and the relying party.

## 5.9 Time-stamping

In some cases, a time-stamping service may be provided alongside a PKI service. Requirements for time-stamping services are outside the scope of this document.

The timing of events from a trusted time source (i.e. a time source known to be synchronized with coordinated universal time (UTC)) can be an important adjunct to the security services provided by a PKI. Not only is this necessary to place secured events within context (e.g. for dispute resolution) but also as a means of assurance of trust services.

There are two aspects of certificate usage where timing can be of particular importance. Firstly, trust services are based on certificates which have a validity period. If a signature is verified after the expiry of the signing key certificate, the validity of the signature cannot be ensured. Secondly, if a certificate is revoked then any use of the certificate after the time that it is revoked should be considered to be invalid. Thus, if there is significant time between the application of a certificate in securing data and the checking of the validity of the certificate, for example when applying a digital signature to stored data, it is important to be sure of the time at which the signature was applied. If it can be confirmed that a signature was created before the supporting certificate expired or was revoked, then the validity of the signature can be ensured long after either of those events. It is for the relying party to determine whether they accept the risk associated with a certificate that can have expired or been revoked in the interim period.

A method of providing assurance of the time that a signature was created is to employ a trusted third party, commonly called a time-stamping authority (TSA) to bind a time to the digital signature on or near the time that the signature was created. This technique is commonly called time-stamping. An example time-stamping protocol is defined in the ISO/IEC 18014 series. This time-stamping protocol uses a hash digest of the data to be time-stamped (e.g. signed data) along with a trusted source of time digitally signed by the trusted authority.

This time-stamping service may be used, for example, by the signatory immediately after signing or before being placed in long-term storage. Once time-stamped, the data can be assumed to be valid even if the supporting certificate subsequently expires or is revoked. Where data are to be archived over very long periods, for example beyond the validity period of TSA's own certificate, further time-stamps can be applied to ensure the ongoing protection of the signed data.

Such an application of time-stamping can also be used to protect a signatory "repudiating" a signature by subsequently claiming to have the signing key compromised and so causing the certificate to be revoked. If the signed data are time-stamped on or near the time that the signature was created, it can be shown to have been valid at that time even though the certificate can subsequently have been revoked.

A variation of the time-stamping mechanism is to link together a time-stamp token with others previously issued by a time-stamping authority to provide greater assurance in the security of a single time-stamp (see ISO/IEC 18014). Another variation is to employ several independent time-stamping authorities and so avoid dependence on a single trusted authority.

## 5.10 Trust models

### 5.10.1 Trust model considerations

CAs may be organized in a range of trust relationships. The conventional approach is to organize CAs into a hierarchical relationship as shown in the following Figure 3:

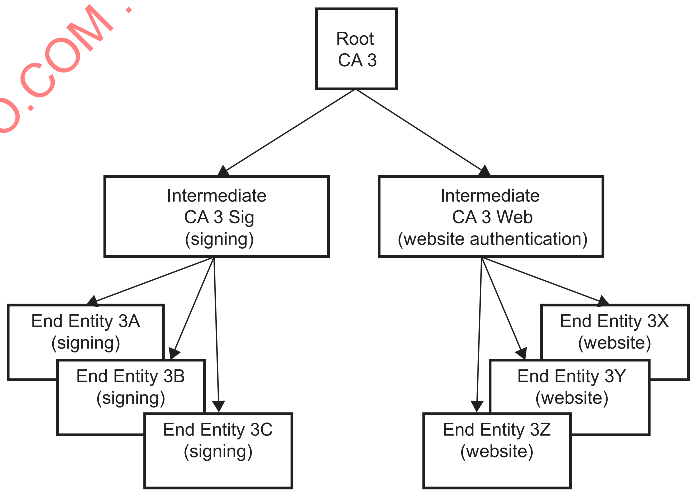

**Figure 3 — Hierarchical CA trust relationships**

At the top of the hierarchy is a root CA. If a relying party trusts the root CA, then it can establish a path of trust down to any end entity (EE) certified through the hierarchy.

The following three main approaches, see Figures 4, 5 and 6, have been adopted to enable relying parties to establish trust in a certificate where it does not have direct knowledge of the trustworthiness of the root CA. The following descriptions are a simplification of the actual trust management schemes, for example the trust link may occur not at the root CA but lower in a CA hierarchy.

### a) Bridge CA

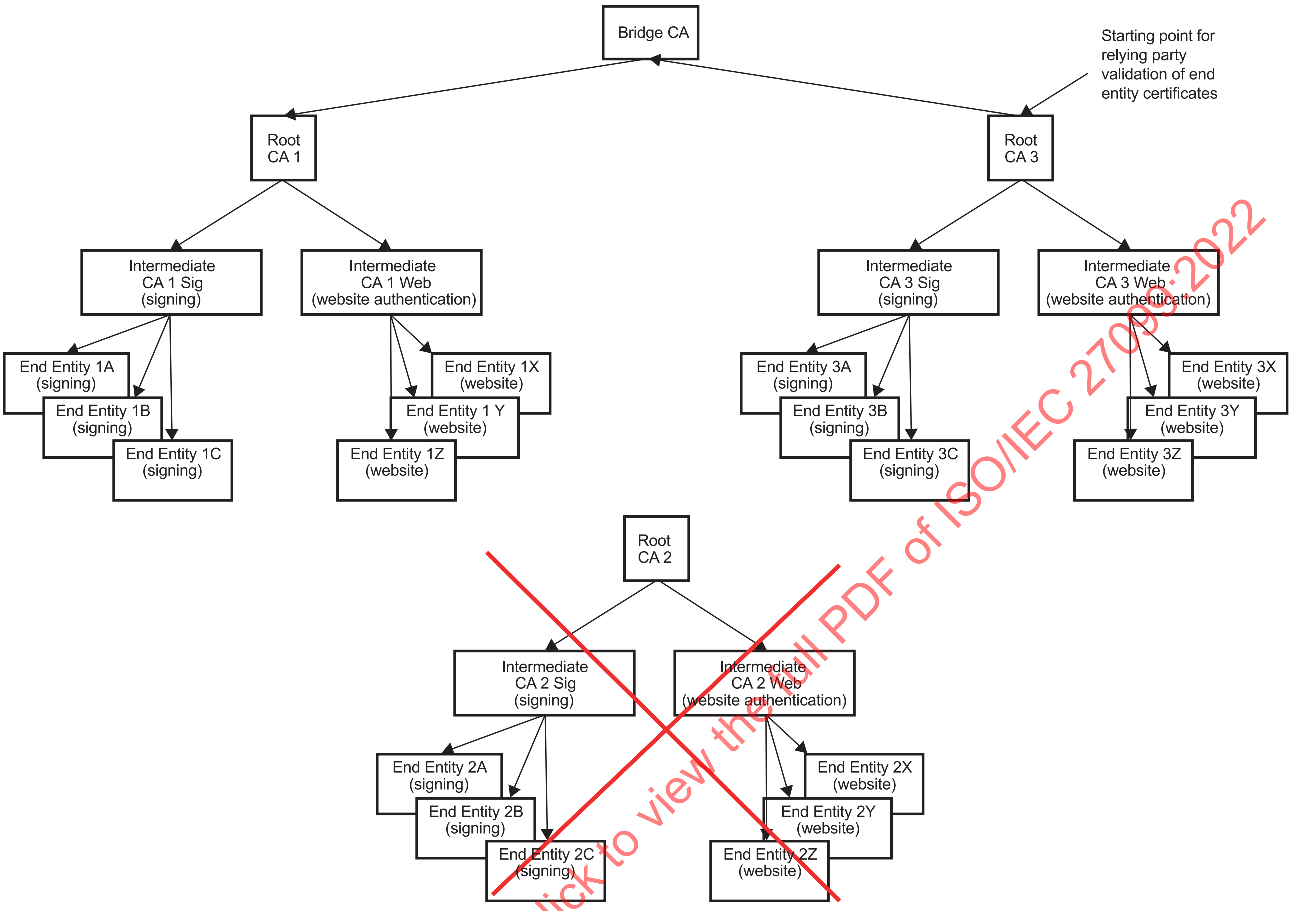

**Figure 4 — CA trust relationships with bridge CA**

In this case an authority is trusted by all CA hierarchies in a community (e.g. USA federal government) to only cross certify with CAs confirmed to be following agreed rules for example through audit. A CA hierarchy which meets the identified rules is then cross certified by the bridge CA operated by the trusted authority. A relying party which trusts a root CA in one hierarchy then can establish a trust path to end entities in another hierarchy.

### b) Application root CA Certificate Store

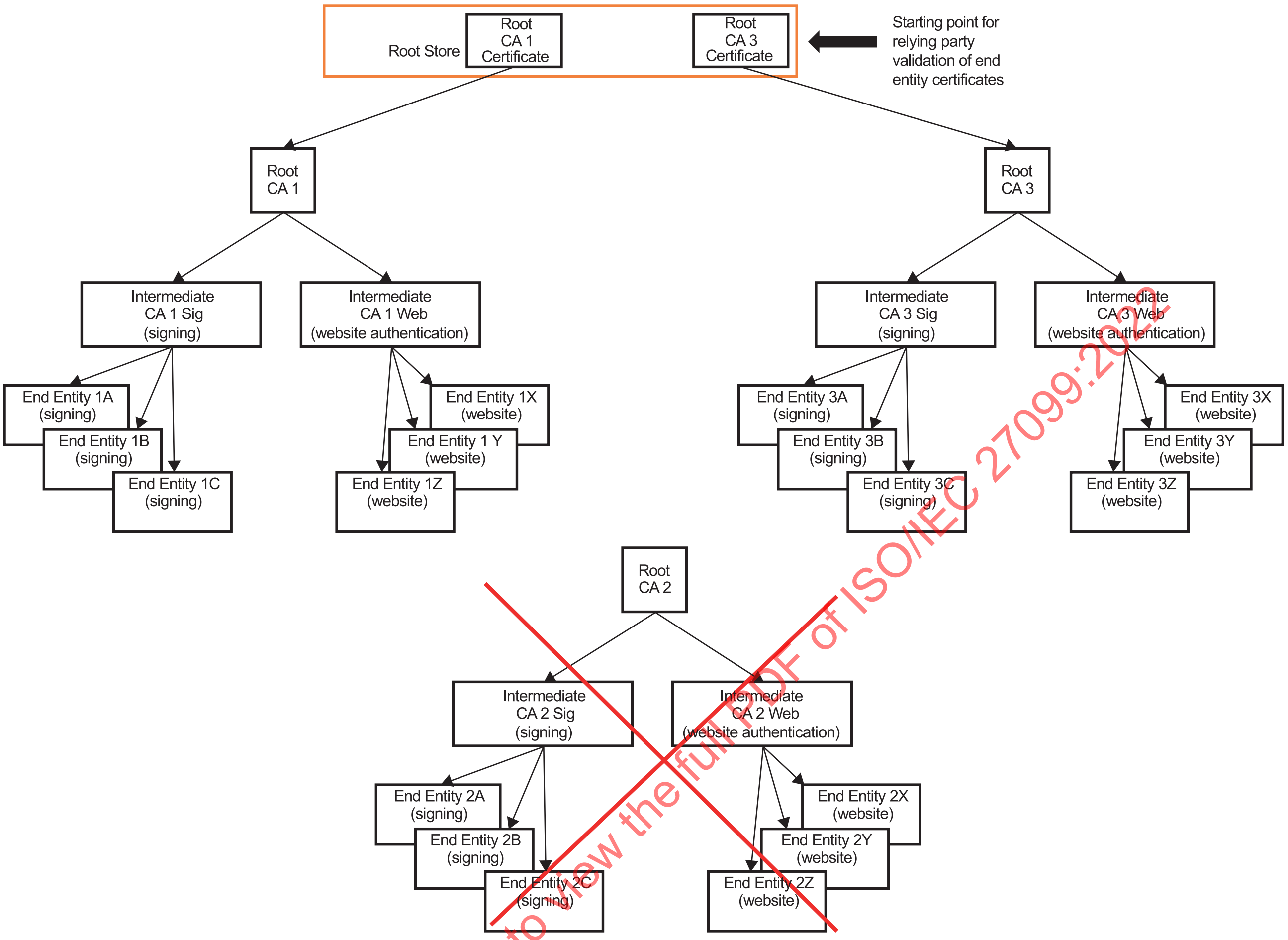

**Figure 5 — CA trust relationships with application root CA certificate store**

In this case an application provider is trusted to maintain a store of root certificates for CAs which are confirmed, for example by audit, to meet the policy defined by the application provider which may be based on common rules agreed by a community (e.g. CA/Browser Forum). The relying party applications only accept certificates in a path from a Root CA that are in the root store. The root store is implemented and managed on the application platform for the relying party.

c) Trusted List

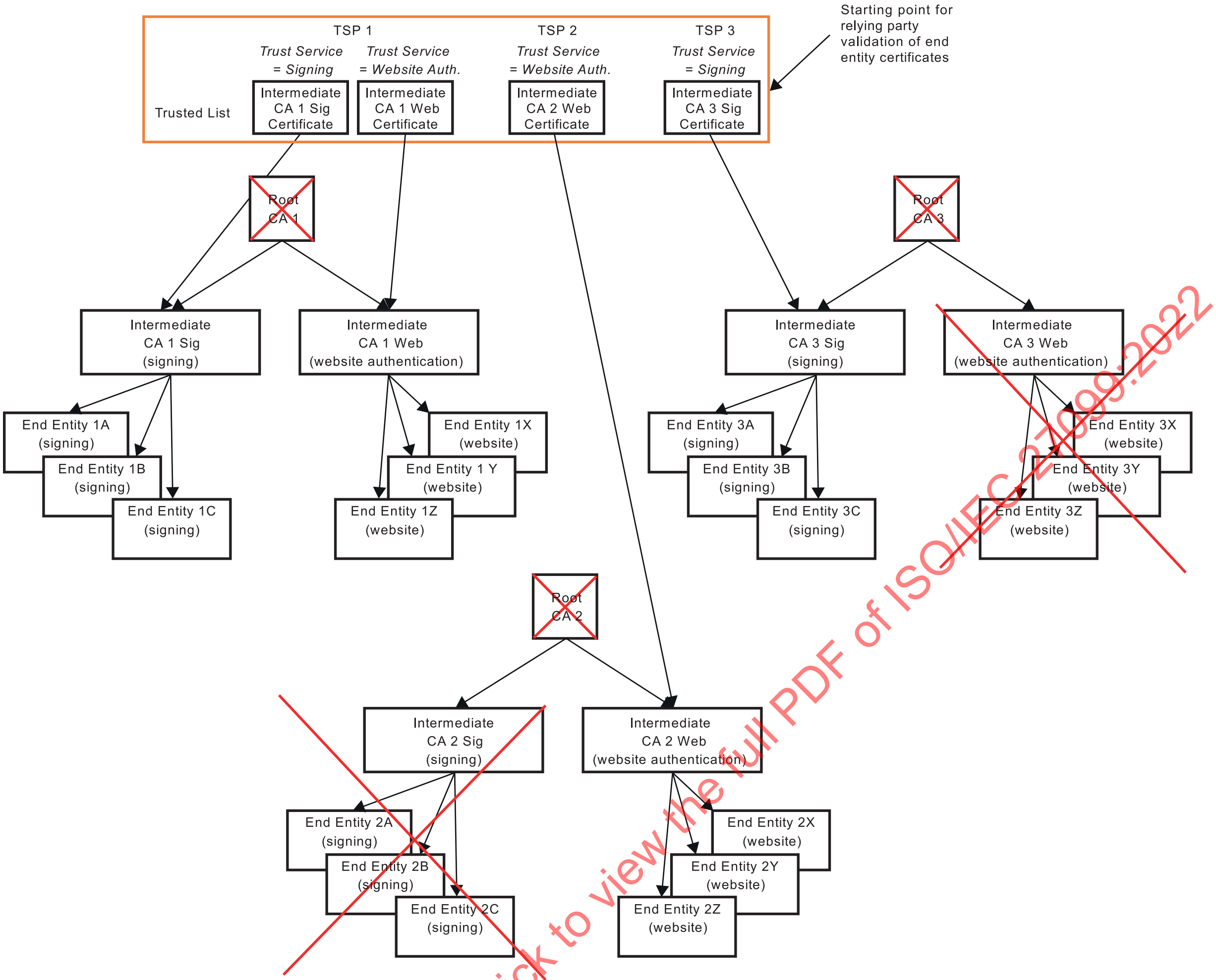

Figure 6 — CA trust relationships with Trusted List

In this case an authority maintains a list of trust anchors of trust service providers which are confirmed to meet given rules [e.g. as set by regulation (EU) No 910/2014] [25] for example through audit. This trust anchor may be an intermediate CA in the CA hierarchy giving greater control over the specific CA systems trusted for specific trust services. The relying party applications only accepts certificates in a path from a trust anchor that is in the trusted list and is used for the purpose identified in the trusted list.

### 5.10.2 Wildcard certificate considerations

Wildcard certificates allow the same certificate to be used for different systems. For example, the three domain names alice.example.com, bob.example.com and cortez.example.com can be served by the same certificate with the common name *.example.com. However, any illicit system inserted into the same domain such as rogue.example.com can reuse the same certificate and private key. Further, without using fully qualified domain names (FQDN) the certificate validation and system trust is weakened. An application only wanting to connect to alice.example.com would validate the server name against the wildcard "*" name such that any illicit connection to bob.example.com, cortez.example.com or any rogue name would appear valid. Wildcard certificates are not allowed by some organisations.

### 5.10.3 Relying party considerations

Relying parties are dependent on certificates but typically do not have a direct business relationship with the certification authority (CA). The relying party validates signatures and certificates according to a signature validation policy which can imply trust in the certification authority (CA) itself, or as a participant in a scheme of mutual recognition (i.e. a commonly accepted “qualified level” or being certified under a bridge-CA). Another possibility is that the relying party accepts the CA’s relying party agreement (RPA) explicitly or implicitly, regardless of whether the relying party has read or acknowledged the RPA.

The certificate validation is only successful if all the steps have been successfully completed. Otherwise, the certificate chain is invalid, and the relying party should reject the subject certificate. The first failure negates the need to continue processing all the steps. Most browsers allow users to accept invalid certificates and bypass certificate validation. For particular types of certificates, additional checks may need to be performed to validate a certificate. The relying party should perform certificate validation as recommended in RFC 5280.

Actions taken by relying parties should include the following.

- reject any signed message received after the revocation date requiring the use of the revoked certificate;
- reject any signed message received after the suspension date and prior to its release date requiring the use of the suspended certificate;
- immediately discontinue any keying material established or protected by revoked certificate and corresponding asymmetric private key;
- update an audit journal to reflect the actions taken and the reasons for the actions;
- provide notification to other entities (e.g. subject, relying parties);
- investigate the security incident and take appropriate supplementary actions to limit exposure.

## 5.11 Component services

A complete functional PKI is composed of multiple component services (e.g. those listed below) which may be provided by more than one PKI service provider. The requirements of a certificate policy need to clearly identify what are the requirements applicable to an individual component service or collection of services, with the entity identified as the issuer of a certificate having overall responsibility for ensuring the policy requirements are met. Contractual arrangement between the commissioning party (i.e. the issuer or its subcontractor) and its subcontractor need to ensure that the obligations and liabilities of each party are clearly established.

There needs to be consistency between the certification practice statements for the providers of the component services to ensure that all aspects of the certificate policy are covered. This needs to cover information or other assets transferred between separate service component providers.

The certification services are broken down in this document into the following component services for the purposes of classifying requirements:

a) Registration service:

This service verifies the identifier and any other applicable attributes of a subject. The results of this service are passed to the certificate manufacture service. The verification process may be an enduring process since the data collected during the initial registration need to be kept up-to-date. At any time, the data from the registration process maps unambiguously the subscriber to their provided data.

The registration service clearly defines the admissible identity proofing and verification processes. The CA or registration service clearly defines the set of information identifying an applicant’s information, both for natural and legal persons.

The registration service ensures integrity, authenticity, and confidentiality of subscriber registration data and status. The registration service should verify the applicants' information and the physical existence, directly or indirectly using appropriate measures.

b) Certificate manufacture service:

This service creates, and signs certificates based on the identity and other attributes verified by the registration service. This can include key generation. For further details see D.3.2.2.

This service signs with its private key the subject's public key and the subject's additional information for the creation of certificates. This service relies on the life cycle controls for maintenance, usage, archival, destruction, and key compromise (cf. 7.13.1, 7.13.2, 7.13.4, 7.13.5 and 7.13.6).

By signing the subject certificates with its private key, the CA provides trust in the certificates as it ensures that:

1) the subjects' identifiers and other attributes have been verified during the registration process;

2) only the subjects are in control (directly or indirectly through an agent) of their private keys corresponding to the public keys in the certificates;

3) the subjects have accepted the CA's disseminated terms and conditions.

Relying parties can use the CA's public key to verify the CA's signature in the generated certificates.

c) Dissemination service:

This service disseminates certificates to subjects, and if the subject consents, makes them available to relying parties. This service also makes available the TSP's terms and conditions, and any published policy and practice information, to subscribers and relying parties.

d) Revocation management service:

This service processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.

e) Revocation status service:

This service provides certificate revocation status information to relying parties.

This is usually carried out by online certificate status protocol (OCSP) or by certificate revocation list (CRL).

f) Subject device provision service (optional):

This service prepares, and provides or makes available secure cryptographic modules, or other secure devices, to subjects.

Examples of this service are:

1) a service which generates the subject's key pair and distributes the private key to the subject;

2) a service which prepares the subject's signature-creation module and enabling codes and distributes the module to the registered subject.

This subdivision of services is only for the purposes of clarification of policy requirements and places no restrictions on any subdivision of an implementation of the CA services.

See 7.14 for the applicable control objectives and procedures.

## 5.12 PKI hierarchies and independently managed CAs

PKI is defined with a hierarchy link between the different CAs (Root and Sub CA) and based on underlying technical components.

As described in 5.10.1, the basic structure of a PKI service is a hierarchy with a root CA at the top of the hierarchy. This may apply to separate CA components within the PKI hierarchy. This decision can be motivated by multiple factors like financial, technical expertise, or HR constraints. For example, a Registration service for a CA issuing Authentication and signature certificates in an open environment, will require helpdesk with adequate human resources that will be able to verify the identity of the end entity subscribing to such a certificate. It can also be the case where the revocation service has to be running 24×7, and thus the CA subcontracts this specific service to organisations having dedicated teams to support 24×7 operations.

In such use-cases, the CA should ensure that the subcontractors are legally liable covering all requirements and SLAs that the CA requests (and to which it is required to comply according to their own CP).

## 5.13 Root CA

### 5.13.1 General

A root CA is the top-level of a given PKI and at the highest level within a trust service provider's (TSP) domain. It represents the ‘trust anchor’ for the chain of trust. A root CA certificate is generally self-signed (i.e. the root CA signs a certificate that names itself as the certificate subject). When a CA is signed by a different CA certificate (i.e. a different named Subject), the certificate is considered cross-certified.

Major operating system and browser vendors embed and distribute the root CA certificates for many of their users.

As applications will trust any valid certificate that chains up to a root CA that is in its trust store, extra precautions to protect the integrity of the root CA and its private signing key need to be taken.

It is good practice for root CAs to be ‘offline’ or ‘air gapped’ from other networks, and only brought online in a controlled environment to issue certificates to other intermediate/issuing CAs, subordinate CAs, cross-certificates, and CRLs.

The requirements for the root CA should be consistent with the CP.

Root CA control objectives can be found in 7.16.

### 5.13.2 CA relationships and PKI hierarchies

In a hierarchical model, a root CA is deployed and various Intermediate CAs may be set up for various business units, domains, or communities of interest, in order to limit or mitigate risk. The root CA validates the intermediate CAs, which in turn issue certificates to lower tier CAs or directly to subscribers. A root CA has more stringent security requirements than an Intermediate CA. Although it is difficult for an attacker to access the root CA (which in some implementations is only online in the rare event that it issues, renews, rekeys, or revokes intermediate or subordinate CA certificates and publish revocation status information), one drawback to this model is that the root CA represents a single point of failure. In the hierarchical model, the root CA maintains the established “community of trust” by ensuring that each entity in the hierarchy conforms to a minimum set of practices. Adherence to the established policies may be tested through audits of the Intermediate and Subordinate CAs and, in several cases, the registration authorities.

In a cross-certified model, the root CAs from one or more PKI issue certificates naming each other as the subject. This allows for trust to be established across separate PKIs when relying parties may only have one of the root CAs in their trust store.

The bridge CA model is similar to the cross-certified model, with the main difference being that, rather than each root CA cross-certifying each other, an independent bridge CA issues one-way cross certificates to each root CA. Relying parties need only trust the bridge CA and will then automatically trust any certificate from any PKI that has a cross-certificate from the bridge CA. This allows for a more flexible hierarchy as the bridge CA can add new PKIs without requiring any actions from existing PKIs.

As the actions of the bridge CA impact all relying parties, bridge CAs often impose various conformance requirements (i.e. annual audits) as well as a common certificate policy.

## 6 Certificate policy (CP), certification practice statement (CPS) and their relationship to information security management system (ISMS)

### 6.1 General

The security policies for a particular environment should be based upon an agreed CP aimed at particular user communities and / or classes of application. In the case of closed environments, the CP can be established within its user communities for the required classes of application. In the case of contractual or open environments, the certificate policy is usually agreed between stakeholders involving the representation of interests of the PKI trust service provider and the user communities. In a contractual environment, the certificate policy is frequently established under the control of a policy authority. The policy authority is recommended practice but optional. This policy authority may operate under the contractual arrangements between the PKI service providers and the PKI user community (see 7.2). Regulations or procedures for the establishment of certificate policy requirements are outside the scope of this document

While a CP focuses on the PKI trust service provider's responsibilities as part of a wider PKI ecosystem, an ISMS has an internal focus. The scope of an ISMS is the security management within the organization of a PKI trust service provider. Both are linked through the CPS. The practices defined in the CPS should support the link between the wider PKI concerns in the CP and as a refinement of ISO/IEC 27001:2013, 5.2, the security policies for a particular environment based upon an agreed CP. Subscribers and relying parties within a PKI ecosystem need credible assurance that the practices defined in the CPS are adequate and properly managed and implemented. To have a common basis for providing such assurance, this document defines ISMS objectives, controls, and, where applicable, implementation guidance for PKI Trust Services.

An ISMS underpins some of the PKI requirements but not all requirements. An ISMS (e.g. based on ISO/IEC 27001 or equivalent) shall be in place to support the PKI requirements. An equivalent approach shall cover at least risk management and generally applicable security controls.

### 6.2 Certificate policy (CP) guidance

Certificates should be issued under at least one CP.

a) CP should describe the conditions for applicability of the certificates issued by the CA, including:

   1) specific permitted uses for the certificates if such use is limited to specific applications;

   2) limitations on the use of certificates if there are specified prohibited uses for such certificates.

b) CP should identify subscriber obligations and liabilities. Subscriber obligations and liabilities may be defined within or separate from the CP. The subscriber obligations and liabilities should include:

   1) providing information in certificate request that is accurate and that the act of accepting the certificate guarantees that information contained is accurate;

   2) guaranteeing that if the subscriber or the certificate subject generates the public key pairs, it will be done in a manner appropriate to the control objectives;

   3) protecting the access to the private key associated with certificate;

4) notifying the issuer of private key compromise or change of status within the time frame specified in the CP;

5) restricting the use of the certificate to the usage specified.

Subscriber obligations and liabilities may alternatively be defined in a document separate from the CP.

a) CP should identify issuer obligations and liabilities. Issuer obligations and liabilities may be defined within or separate from the CP. The issuer obligations and liabilities should include:

1) notifying the subject or, where applicable, the subscriber of the certificate that the certificate has been issued;

2) where possible notifying the subject or, where applicable, the subscriber whose certificate has been revoked, suspended, or unsuspended;

3) making available to relying parties the certificate status in accordance with the CP (e.g. by posting certificate status information in a repository available to participating subscribers and relying parties);

4) complying with the CP identified and its associated certification practice statement;

5) providing notification of any disclaimers of liability (e.g. for misuse of certificate for disallowed applications);

6) providing confidentiality protection to non-public subscriber and relying party information.

Issuer obligations and liabilities may alternatively be defined in a document separate from the CP.

d) CP should identify relying party obligations and liabilities. CP should include relying party obligations and liabilities in order to:

1) restrict usage to applications identified;

2) provide notification regarding any disallowance of claims of liability for misuse of the certificate on excluded applications;

3) check digital signature;

4) validate certificate content and status;

5) provide notification of applicable liability caps and warranties.

e) CP should identify any applicable reliance or financial limits for certificate usage

f) CP should state the minimum requirements for:

1) subscriber identification and authentication;

2) certificate status publication;

3) subject private key protection;

4) CA private key protection.

g) CP should state the minimum requirements for the mandatory X.509 v3 fields:

1) version number;

2) serial number;

3) signature algorithm;

4) issuer;

5) valid from and valid to dates;

6) subject;

7) public key algorithm and minimum key length;

8) required extensions.

h) In case of relevant changes of the CA structures, processes and assurances, the CP should be updated, and subscribers should be informed, and where possible relying parties should be informed, about the updates.

See Annex A for additional information on certificate policies.

### 6.3 Certification practice statement (CPS) guidance

a) A certification authority is required (see 7.2.2) to document its certification practices.

b) A CPS, or equivalent, is required (see 7.2.2) to support each CP under which the CA issues or manufactures certificates.

c) The TSP's CP is recommended to address the contents provided in IETF RFC 3647 that include the following high-level components to the level of detail required by the policy authority with reference to the relevant certificate policies:

1) introduction;

2) general provisions;

3) identification and authentication;

4) operational requirements;

5) physical, procedural and personnel security controls;

6) technical security controls;

7) certificate and CRL profiles;

8) practices administration.

d) A CA's certification practices are required to control procedures (see 7.1), which are appropriate, based on the CA's assessment of risks and meet the requirements of the supported certificate policies.

See IETF RFC 3647 for additional information on certification practice statements.

## 7 Certification authority objectives and controls

### 7.1 General

Control objectives in the areas of CA physical and environmental controls, CA key life cycle management, certificate life cycle management and root CA controls are presented in 7.2 to 7.17, representing baseline control criteria with which a CA shall comply and against which a CA can be evaluated or audited, unless the stated objectives are addressed by alternative requirements stated in the certificate policy. Such an evaluation can take the form of an internal audit or external audit using any appropriate audit methodology as can be defined by the rules of the contractual environment. In the case of the PKI subcontracting part, the CA remains ultimately responsible and should ensure that all necessary control objectives defined by the CA are applied across the different subcontractors that are part of this ecosystem.

A number of the control objectives are regarded as optional, that is they are only applicable if corresponding processes are supported by the CA. These include if the CA defines its own policy:

— Certificate Policy Management (7.2.1).

— CA-provided subject key generation services, if supported (7.14.1).

— CA-provided subject key storage and recovery services, if supported (7.14.2).

— Hardware token life cycle management, if supported (7.14.3).

— Subject key management, if supported (7.14.4).

— Certificate renewal, if supported (7.15.2).

— Certificate suspension, if supported (7.15.7).

— Subordinate CA certificate (7.17).

The control procedures described in 7.2 onwards represent recommended practices for business, operational and technical use by a certification authority unless the need for such controls are negated due to requirements stated in the certificate policy.

A CA's CPS shall contain only the control procedures that are appropriate based on the CA's assessment of risks in order to support the certificate policies under which certificates are issued.

In assessing the CA's conformance with the CA control objectives and procedures, the reviewer should review the CA's CPS, supported certificate policies, other CA business practices disclosures and other relevant CA documentation (e.g. CA operating procedures, security policies, network architecture diagrams and audit logs).

## 7.2 Certification practice statement and certificate policy management

### 7.2.1 Certificate policy management

| **Control objectives:** |
|---|
| If the CA defines its own policy: To ensure the business requirements and policies for using digital certificates are specified in a CP and supporting agreements. |

| **Control procedures: (only applicable if the CA manages its own CP)** | |
|---|---|
| | Policy authority (PA) management |
| 1 | There shall be a PA which has final authority and responsibility for specifying and approving certificate policies. |
| 2 | The PA shall have final authority and responsibility for approving the CA's certification practice statement (CPS). |
| 3 | The PA or delegated representative shall ensure the business application is using the appropriate certificate policy. |
| 4 | The PA shall maintain procedures for the changes to its certificate policies and should make this available to the affected parties. |
| 5 | The PA shall notify, in the first instance, those CAs that support its certificate policies in order that appropriate actions can be undertaken expeditiously. |
| | Certificate policies management |
| 6 | Certificate policies shall be approved by the policy authority in accordance with a defined review process, including responsibilities for maintaining the certificate policies. |

| | |
|---|---|
| 7 | The PA shall make available the certificate policies supported by the CA to all appropriate subscribers and relying parties. |
| | Multiple component services (If the PKI Service is provided by more than one component service provider) |
| 8 | The Certificate Policy shall identify the requirements which apply to each component service or collection of component services. |
| 9 | The logical entity identified as the issuer of the certificates (i.e. whose name is in the issuer field of an X509 certificate) shall ensure that the practices of all the component service providers meets the requirements of the Certificate Policy, including any liabilities and obligations regarding the issuance of certificates, in a manner that meets all the requirements of the Certificate Policy. |
| 10 | Information or other assets transferred between separate service component providers shall be protected in a way that ensures that all the requirements of the Certificate Policy are met. |

### 7.2.2 CPS and CA management

| **Control objectives:** |
|---|
| To provide management direction, support, and reasonable assurance that the CA's information security is in accordance with its CP and CPS |

| **Control procedures:** | |
|---|---|
| | Certification practice statement (CPS) management by CA |
| 1 | The CA shall ensure that its control processes, as stated in a certification practice statement (CPS) or equivalent, fully comply with the requirements of the CPs. This may be undertaken by a PA. |
| 2 | The CA shall ensure a certification practice statement (CPS), or other CA policy or practices documentation document is in place describing, at least, the following:<br>a) CA environmental controls;<br>b) key life cycle management controls;<br>c) certificate life cycle management controls.<br>This may be undertaken by a PA. |
| 3 | The CA shall have a review and approval process for its CPS, including any modifications. This may be undertaken by a PA. There shall be defined responsibilities for maintaining the CPS. |
| 4 | The CA shall make available its CPS to all appropriate parties. |
| 5 | In case of significant changes to a CA's structure, process and assurances, the CPS shall be revised. |
| 6 | Revisions to the CA's CPS shall be made available to appropriate parties. |

| | |
|---|---|
| 7 | The CPS should contain an explanation of the controls to ensure adherence to:<br>a) legislative requirements;<br>b) contractual requirements;<br>c) educational and notification requirements;<br>d) prevention and detection of virus and other malicious software;<br>e) business continuity requirements;<br>f) escalation requirements from the consequences of security policy violations or security incidents. |
| | CA management |
| 8 | The CA's controls shall be described in the CPS or equivalent documentation. |
| 9 | A CPS shall be defined by the CA or PA, approved by management of the PA, published, and communicated to employees and relevant external parties. |
| 10 | A CP and necessary supporting documents shall be defined by the PA. |
| 11 | If a PKI trust service provider delegates some of its services or functions to separate component service providers, the PKI trust service provider shall remain responsible for writing and maintaining the CPS. |

### 7.2.3 Subscriber and relying party agreements

| **Control objectives:** |
|---|
| To ensure that there are the appropriate agreements in place with subscribers and relying parties. |

| **Control procedures:** | |
|---|---|
| | Subscriber agreement |
| 1 | The certificate issuer, or service component provider(s) sub-contracted to the certificate issuer, shall have an agreement with its subscribers. |
| 2 | The subscriber agreement shall record the terms and conditions including the obligations of the parties of the agreement. |
| | Relying party agreement |
| 3 | The certificate issuer, or service component provider(s) sub-contracted to the certificate issuer, shall have a relying party agreement. |
| 4 | The relying party agreement shall record the terms and conditions for the use of the certificates by relying parties, including any obligations on the relying parties. |
| | Multiple component services<br>If the PKI Service is provided by more than one component service providers: |
| 5 | Agreements shall be in place between the commissioning party (i.e. the issuer or its subcontractor) and its subcontractor which ensure that the obligations and liabilities of each party are clearly established and are in line with the requirements of the Certificate Policy. |
| | Subject key compromise |
| 6 | The subscriber agreement shall specify the requirements for notification of the CA in the case of any event that affects the validity of the certificate. |

## 7.3 Information security

| Control objectives: |
|---|
| To ensure that:<br>— security is planned, managed, and supported within the organization;<br>— identified risks are managed effectively;<br>— the security of CA facilities, systems and information assets accessed by third parties is maintained;<br>— the security of information is maintained if the responsibility for CA sub-functions has been outsourced to another organization or entity. |

| Control procedures: | |
|---|---|
| | Information security policy |
| 1 | An information security policy document, that includes physical, personnel, procedural and technical controls, shall be approved by management, published, and communicated to all employees, and where relevant, third-party contractors. |
| 2 | Management of the CA should be able to demonstrate that the information security policy is implemented and adhered to. |
| 3 | The information security policy shall include the following:<br>a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing;<br>b) a statement of management intent, supporting the goals and principles of information security;<br>c) an explanation of the security policies, principles, standards, and conformance requirements of particular importance to the organization;<br>d) a definition of general and specific responsibilities for information security management, including reporting security incidents;<br>e) references to documentation that supports the policy;<br>f) optional controls specified in ISO/IEC 27002:2022. |
| 4 | There shall be a defined review process for maintaining the information security policy, including responsibilities and review dates. |
| | Information security infrastructure |
| 5 | Senior management or a high-level management information security committee shall have the responsibility of ensuring there is clear direction and management support to manage risks effectively. |
| 6 | There shall exist a risk management system, e.g. as defined in ISO/IEC 27005 to identify, analyse, evaluate, and treat trust service risks, taking into account business and technical issues. The results of the risk assessment shall be communicated to a management group or committee responsible to information security and risk management. |
| 7 | Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined. |
| 8 | A management authorization process for new information processing facilities shall exist and be followed. |
| | Security of third-party access |

| | |
|---|---|
| 9 | Procedures shall exist and be followed to control physical and logical access to CA facilities and systems by third parties (e.g. on-site contractors, trading partners and joint ventures). |
| 10 | If there is a business need for the CA to allow third party access to CA facilities and systems, a risk assessment shall be performed to determine security implications and specific control requirements. |
| 11 | Arrangements involving third party access to CA facilities and systems shall be based on a formal contract containing all necessary security requirements. |
| | Outsourcing |
| 12 | If the CA outsources the management and control of all or some of its information systems, networks, or desktop environments, the security requirements of the CA shall be addressed in a contract agreed between the parties. |
| 13 | If the CA chooses to delegate a portion of the CA roles and respective functions to another party, the CA shall be ultimately responsible for the completion of the outsourced functions and the definition and maintenance of a statement of its CPS. |
| 14 | Processes operated by subcontractors shall be subject to applicable requirements from this document. |
| 15 | The CA security operations relating to the process of certificate-management shall be separated from all other business-related activity of the CA. |

## 7.4 Asset classification and management

| **Control objective:** |
|---|
| To ensure that CA assets and information receive an appropriate level of protection in accordance with the requirements of all supported certificate policies and risk analysis.<br>To archive any information necessary for the renewal, re-keying, and update of certificates.<br>To ensure media are securely handled and protected from damage, theft, and unauthorized access. |

| **Control procedures:** | |
|---|---|
| 1 | Owners shall be identified for all CA assets and assigned responsibility for the maintenance of appropriate controls. |
| 2 | Inventories of CA assets shall be maintained. |
| 3 | The CA shall have implemented information classification and associated protective controls for information based on business needs and the business impacts associated with such needs. |
| 4 | Procedures shall be defined to ensure that information labelling and handling is performed in accordance with the CA’s information classification scheme. |
| 5 | Procedures for the management of removable computer media shall require the following:<br>a) if no longer required, the previous contents of any reusable media that are to be removed from the organization are erased or media is destroyed;<br>b) authorization is required for all media removed from the organization and a record of all such removals to maintain an audit trail is kept;<br>c) all media are stored in a safe, secure environment, in accordance with manufacturers' specifications. |

| | |
|---|---|
| 6 | Equipment containing storage media (e.g. fixed hard disks) shall be checked to determine whether they contain any sensitive data prior to disposal or reuse. Storage devices containing sensitive information shall be physically destroyed or securely overwritten prior to disposal or reuse. |
| 7 | If applicable, the CA shall implement procedures for the archiving of information on subscribers and their certificates sufficient for the certificate renewal, re-keying, and update processes. |
| 8 | Include optional controls specified in ISO/IEC 27002:2022, Clause 5. |

## 7.5 Human resources security

| **Control objective:** |
|---|
| To reasonably ensure that personnel and employment practices enhance and support the trustworthiness of the CA's operations. |

| **Control procedures:** | |
|---|---|
| 1 | The CA shall employ personnel who possess the relevant skills, knowledge, and experience appropriate for the job function. |
| 2 | Security roles and responsibilities, as specified in the organization's security policy, shall be documented. Trusted roles, on which the security of the CA's operation is dependent, shall be clearly identified. |
| 3 | Trusted roles shall at least include roles that involve the following responsibilities:<br>a) overall responsibility for administering the implementation of the CA's security practices;<br>b) approval of the generation, revocation, and suspension of certificates;<br>c) installation, configuration, and maintenance of the CA systems;<br>d) day-to-day operation of CA systems and system back-up and recovery;<br>e) viewing and maintenance of CA system archives and audit logs;<br>f) cryptographic key life cycle management functions (e.g. key component custodians);<br>g) CA systems development;<br>h) access and in charge of the regular analysis of the archives and the analysis of the event logs in order to detect any incident, anomaly, attempt of compromise, etc. |
| 4 | The CA's policies and procedures shall specify the background checks and clearance procedures required for trusted roles and non-trusted roles. As a minimum, verification checks on permanent staff should be performed at the time of job application and periodically for those individuals undertaking trusted roles as permitted under applicable requirements (these may include regulations). |
| 5 | An individual's trusted status shall be approved prior to gaining access to systems/facilities or performing actions requiring trusted status. |
| 6 | Contractors who perform trusted roles shall be subject to at least the same background check and personnel management procedures as employees. |
| 7 | Any contract arrangement between contractors and CAs shall allow for the provision of temporary contract personnel which explicitly allows the organization to take measures against contract staff who violate the organization's security policies. |

| | |
|---|---|
| 8 | A formal disciplinary process shall exist and be followed for employees who have violated organizational security policies and procedures. |
| 9 | Appropriate and timely actions shall be taken when employment is terminated so that controls (e.g. access controls) are not impaired. |
| 10 | Duress alarms should be provided for personnel who may be the target of coercion. |
| 11 | All employees of the organization and, where relevant, third-party contractors shall receive appropriate training in organizational policies and procedures. |
| 12 | Include optional controls specified in ISO/IEC 27002:2022, 5.3 regarding conflicts of interest. |
| 13 | Include optional controls specified in ISO/IEC 27002:2022, 6.4 regarding disciplinary procedures. |
| 14 | Include optional controls specified in ISO/IEC 27002:2022, 5.4 on management responsibilities in establishing roles and responsibilities. |
| 15 | Include optional controls specified in ISO/IEC 27002:2022, 5.2 and Clause 6. |

## 7.6 Physical and environmental security

| **Control objective:** |
|---|
| To provide reasonable assurance that:<br>— physical access to CA facilities is limited to authorized individuals;<br>— CA facilities are protected from environmental hazards;<br>— loss, damage or compromise of assets and interruption to business activities are prevented;<br>— compromise of information and information processing facilities is prevented. |

| **Control procedures:** | |
|---|---|
| | CA facility physical security |
| 1 | Physical access to CA facilities shall be limited to authorized individuals or, in the case of virtualised environment, CA software shall be isolated from other software and cannot be accessed by unauthorised individuals. |
| 2 | The perimeter of the building or site containing the CA's certificate manufacturing facility shall have a minimal number of controlled access points. |
| 3 | A manned reception area or other means of controlling physical access should be in place to restrict access to the building or site housing CA operations to authorized personnel only. |
| 4 | Physical barriers shall be in place (e.g. solid walls that extend from real floor to real ceiling) to prevent unauthorized entry and environmental contamination to the CA's certificate manufacturing facility. |
| 5 | Physical barriers and protection against radiant emission should be in place (e.g. Faraday cage) to prevent electromagnetic radiation emissions for any device containing a private key used for root CA operations (e.g. key generation and certification of CA certificates) and where CP or CPS dictate. |
| 6 | Fire doors on security perimeters around CA operational facilities shall be alarmed. |
| 7 | Intruder detection systems shall be installed and regularly tested to cover all external doors of the building housing the CA operational facilities. |
| 8 | Physical access to CA operational facilities shall be secured e.g. physically locked and alarmed when unoccupied. |

| | |
|---|---|
| 9 | All personnel should be required to wear visible identification. Employees should be encouraged to challenge anyone lacking recognizable identification. |
| 10 | All personnel entering and leaving CA operational facilities shall be logged (i.e. an audit trail of all access is securely maintained). |
| 11 | Visitors to CA facilities shall be supervised and their date and time of entry and departure recorded. |
| 12 | Third party support services personnel shall be granted restricted access to secure CA operational facilities only when required and such access is authorized and accompanied. |
| 13 | Access rights to CA facilities shall be regularly reviewed and updated. |
| 14 | Elements of CA's systems which are identified as critical to the security of its operations shall be within a physically secure boundary which physically restricts access to unauthorized personnel. |
| | Equipment security |
| 15 | The CA shall maintain an equipment inventory. |
| 16 | Equipment should be sited or protected in order to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |
| 17 | Equipment shall be protected from power failures and other electrical anomalies. |
| 18 | Power and telecommunications cabling carrying data or supporting CA services should be protected from interception or damage. |
| 19 | Equipment shall be maintained in accordance with the manufacturer's instructions or other documented procedures to ensure its continued availability and integrity. |
| 20 | All items of equipment containing storage media (fixed and removable disks) shall be checked to ensure that they do not contain sensitive data prior to their disposal. Storage media containing sensitive data shall be physically destroyed or securely overwritten prior to disposal or reuse. |
| 21 | Controls shall be implemented to protect against unintended removal of media containing sensitive data outside a physically secured environment. |
| | General controls |
| 22 | Sensitive or critical business information shall be locked away when not required and when the CA facility is vacated. |
| 23 | Procedures shall require that personal computers and workstations be logged off or protected by key locks, passwords, or other controls when not in use. |
| 24 | Procedures shall require that equipment, information, and software belonging to the organization cannot be taken off-site without authorization. |
| 25 | Physical access to the secure cryptographic device shall be limited to authorized entities under multiple control. |
| 26 | Include optional controls specified in ISO/IEC 27002:2022, Clause 7 for guidance. |

## 7.7 Operations security

**Control objective:**

**Control objectives:**

To provide reasonable assurance that:

a) correct and secure operation of CA information processing facilities is ensured;

b) the risk of CA systems failure is minimized;

c) the integrity of CA systems and information is protected against malware;

d) any damage from security incidents and malfunctions is minimized;

e) incident reporting and response procedures are established and maintained;

f) audit journals provide sufficient detail to reconstruct events and provide 'due care' requirements.

| **Control procedures:** | |
|---|---|
| | Operational procedures and responsibilities |
| 1 | CA operating procedures shall be documented and maintained for each functional area. |
| 2 | Formal management responsibilities and procedures shall exist to control all changes to CA equipment, software, and operating procedures. |
| 3 | Duties and areas of responsibility shall be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services. |
| 4 | Development and testing facilities shall have a physical or logical separation from operational facilities. |
| | System planning and acceptance |
| 5 | Capacity demands shall be monitored, and projections of future capacity requirements made to ensure that adequate processing power and storage are available. |
| 6 | Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance. |
| | Protection against viruses and malicious software |
| 7 | Detection and prevention controls to protect against viruses and malicious software shall be implemented. Appropriate employee awareness programmes should be in place. |
| | Incident reporting and response |
| 8 | A formal security incident reporting procedure shall exist setting out the actions to be taken on receipt of an incident report. This should include a definition and documentation of assigned responsibilities and escalation procedures. Any incidents shall be reported to responsible management as a matter of urgency. |
| 9 | The CA shall plan an appropriate reaction if security relevant algorithms or processes are broken/insecure. |
| 10 | The CA shall ensure timely, appropriate reaction to incidents. |
| 11 | Users of CA systems with trusted roles shall be required to note and report observed or suspected security weaknesses in, or threats to, systems or services to ensure an appropriate response to a security incident. |
| 12 | Procedures shall exist and be followed for reporting hardware and software malfunctions. |
| 13 | Procedures shall exist and be followed to ensure that faults are reported, and corrective action is taken. |

| | |
|---|---|
| 14 | A formal problem management process shall exist which allows the types, volumes and impacts of incidents and malfunctions to be documented, quantified, and monitored. |
| 15 | The CA needs to ensure that any security breach results in an appropriate countermeasure to limit the impact in a timely and coordinated manner |
| | Media handling and security |
| 16 | Procedures for the handling and storage of information shall exist and be followed in order to protect such information from unauthorized disclosure or misuse. |
| 17 | System documentation should be protected from unauthorized access. |
| 18 | Optional controls specified in ISO/IEC 27002:2022, Clause 8 should be considered. |

## 7.8 Access control

| **Control objectives:** |
|---|
| — To provide reasonable assurance that CA system access is limited to authorized individuals;<br>— To limit operating system access to authorized individuals with predetermined task privileges;<br>— To limit access to network segments housing CA systems to authorized individuals, applications, and services;<br>— To limit CA application use to authorized individuals. |

| **Control procedures:** | |
|---|---|
| | User access management |
| 1 | Business requirements for access control shall be defined and documented in an access control policy which includes at least the following:<br>a) roles and corresponding access permissions;<br>b) identification and authentication process for each user;<br>c) segregation of duties;<br>d) number of persons required to perform specific CA operations (i.e. *m* of *n* rule where *m* represents the number of key shareholders required to perform an operation and *n* represents the total number of key shares). |
| 2 | There shall be a formal trusted role user registration and deregistration procedure for granting access to CA information systems and services. |
| 3 | The allocation and use of privileges shall be restricted and done under multiple control. |
| 4 | The allocation of passwords shall be controlled through a formal management process. |
| 5 | Access rights for users with trusted roles shall be reviewed at regular intervals. |
| | Network access control |
| 6 | CA employed personnel shall be provided with access only to the services that they have been specifically authorized to use. The path from the user terminal to computer services shall be controlled. |
| 7 | Remote access to CA systems, made by CA employees or external systems, if permitted, shall require mutual authentication. |
| 8 | Connections made by CA employees to remote computer systems for CA activities shall be mutually authenticated. |

| | |
|---|---|
| 9 | Access to diagnostic ports shall be securely controlled. |
| 10 | Controls (e.g. firewalls) shall be in place to protect the CA's internal network domain from any unauthorized access from any other domain. |
| 11 | Controls shall be in place to limit the network services (e.g. HTTP, FTP) available to authorized users in accordance with the CA's access control policies. The security attributes of all network services used by the CA organization shall be documented by the CA. |
| 12 | Routing controls shall be in place to ensure that computer connections and information flows do not breach the CA's access control policy. |
| 13 | The CA shall ensure that local network components (e.g. firewalls and routers) are kept in a physically secure environment and their configurations periodically audited for conformance with the CA's configuration requirements. |
| 14 | Sensitive data shall be encrypted when exchanged over public or untrusted networks. |
| 15 | The CA shall monitor access to its systems to detect possible unauthorized access to sensitive resources and react in a timely manner. |
| 16 | The network relating to the process of certificate-management shall be separated from all other networks. The separation of the network should rely on an appropriate physical or logical separation from untrusted networks. For example, physical separation or appropriate firewall, switch and routing capability shall be utilized. |
| | Operating system access control |
| 17 | Operating systems shall be configured in accordance with the CA's operating system configuration standards and be periodically reviewed. |
| 18 | Operating system patches and updates shall be applied in a timely manner when deemed necessary based on a risk assessment. |
| 19 | Access to CA systems shall require a protected log-on process. |
| 20 | All CA personnel users shall have a unique identifier (user ID) for their personal and sole use so that activities can be traced to the responsible individual. Where shared or group accounts are required, other monitoring controls shall be implemented to maintain individual accountability. |
| 21 | Uses of system utility programmes shall be restricted to authorized personnel and be tightly controlled. |
| 22 | Inactive terminals serving CA systems shall require re-authentication prior to use. |
| 23 | The CA servers used for certificate manufacture shall be configured and tested to avoid known vulnerabilities. This covers configuration and setting of utilized hardware and software components (i.e. operating systems, CA server software or firewall components). |
| | Application access control |
| 24 | Access to information and application system functions shall be restricted in accordance with the CA's access control policy. |
| 25 | CA personnel shall be successfully identified and authenticated before using critical applications related to certificate management. |
| 26 | Sensitive systems (e.g. root CA) shall require a dedicated (isolated) computing environment. |
| 27 | Include optional controls specified in ISO/IEC 27002:2022, Clause 5 for guidance on object reuse. |

## 7.9 System acquisition development and maintenance

| **Control objective:** |
|---|
| To provide reasonable assurance that CA systems development and maintenance activities are authorized to maintain CA system integrity. |

| **Control procedures:** | |
|---|---|
| 1 | Business requirements for new systems, or enhancements to existing systems, shall specify the security requirements. |
| 2 | Software testing and change control procedures shall exist and be followed for the implementation of software on operational systems, including scheduled software releases, modifications, and emergency software fixes. |
| 3 | Change control procedures shall exist and be followed for the hardware, network component and system configuration changes. |
| 4 | Control shall be maintained over access to program source libraries. |
| 5 | Systems shall be reviewed and tested when operating system changes occur. |
| 6 | Modifications to software packages should be discouraged and all changes shall be strictly controlled. |
| 7 | The purchase, use, and modification of software shall be controlled and checked to protect against possible covert channels and Trojan code. This should include the authentication of the source of the software. These controls apply equally to outsourced software development. This should include accreditation to common criteria as defined by ISO/IEC 15408[17] or ISO/IEC 19790 (FIPS 140-2) or similar. |

## 7.10 Business continuity management

| **Control objectives:** | |
|---|---|
| — | To provide reasonable assurance of continuity of operations in the event of a disaster. |
| — | To provide reasonable assurance that potential disruptions to subscribers and relying parties are minimized as a result of the cessation or degradation of the CA's services. |

| **Control procedures:** | |
|---|---|
| 1 | The CA shall have a managed process for developing and maintaining its business continuity plans. The CA shall have a business continuity planning strategy based on an appropriate risk assessment. |

| | |
|---|---|
| 2 | The CA shall have a business continuity plan to maintain or restore the CA's operations in a timely manner following interruption to, or failure of, critical CA processes. Refer to ISO/IEC 27002:2022, Clause 5 for further guidance. The CA's business continuity plan should address the following:<br>a) the conditions for activating the plans;<br>b) emergency procedures;<br>c) fall-back procedures;<br>d) resumption procedures;<br>e) a maintenance schedule for the plan;<br>f) awareness and education requirements;<br>g) the responsibilities of the individuals;<br>h) recovery time objective (RTO);<br>i) regular testing of contingency plans;<br>j) compromise of the root keys. |
| 3 | The CA's business continuity plans shall include disaster recovery processes for all critical components of a CA system, for example, the hardware, software, and keys, in the event of a failure of one or more of these components. In particular, consideration should be given to recovery from compromise or loss of the CA private keys, for example the following controls may be applied:<br>a) cryptographic devices used for storage of back-up CA private keys shall be securely stored at an off-site location in order to be recovered by the CA in the event of a disaster at the primary CA facility;<br>b) the requisite secret key shares or key components needed to use and manage the disaster recovery cryptographic devices shall also be securely stored at an off-site location. |
| 4 | Back-up copies of essential business information shall be regularly taken. The security requirements of these copies shall be consistent with the controls for the information backed up. |
| 5 | Depending on availability requirements the CA should consider the preparation of an alternative site where core PKI operations can be restored in the event of a disaster at the CA's primary site. Relevant, fall-back equipment and back-up media shall be sited at a safe distance to avoid damage from disaster at the main site. |
| 6 | The CA's business continuity plans shall include procedures for securing its facility to the fullest extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original site or a remote site. |
| 7 | The CA's business continuity plans shall address the recovery procedures used if computing resources, software or data are compromised or suspected to be compromised. |
| 8 | Testing of business continuity management plans shall be carried out regularly to ensure that they are up to date and effective. |
| 9 | Business continuity plans shall be maintained by regular reviews and updates to ensure their continuing effectiveness. |
| 10 | Depending on the business continuity plan the storage of back-ups of systems, data and configuration information should be done at an alternative location. |
| 11 | The storage of required cryptographic materials (i.e. secure cryptographic devices and activation materials) should be done at an alternative location depending on the business continuity plan. |

| | |
|---|---|
| 12 | The availability of equipment and connectivity to enable recovery in line with the business continuity plan shall be ensured. |

## 7.11 Monitoring, conformance and compliance

| Control objectives: |
|---|
| To maintain controls to provide reasonable assurance that:<br>— controls conform with the relevant legal, regulatory, and contractual requirements;<br>— conformance to the CA's security policies and procedures is ensured;<br>— unauthorized CA system usage is detected. |

| Control procedures: | |
|---|---|
| | Compliance with legislation |
| 1 | The CA shall document procedures to ensure compliance with applicable legislation, e.g. restrictions on the use of material with respect to intellectual property rights, and on the use of proprietary software products. |
| 2 | Procedures shall exist to ensure that personal information is protected. |
| 3 | The information security policy shall assign a classification on information assets and require handling as appropriate. This should include the following:<br>a) the information that shall be kept confidential by CA or RA;<br>b) the information that is not considered confidential;<br>c) the policy on release of information to law enforcement officials;<br>d) information that can be revealed as part of civil discovery;<br>e) the conditions upon which information can be disclosed with the subject's consent;<br>f) any other circumstances under which confidential information can be disclosed. |
| 4 | Records relevant to monitoring and conformance (for audit logs, see 7.12) shall be protected from loss, destruction, and falsification. |
| | Review of security policy and technical conformance |
| 5 | Managers shall be responsible for ensuring that security procedures within their area of responsibility are carried out correctly. |
| 6 | The CA's operations shall be subject to regular review to ensure it is in accordance with its CPS. |
| 7 | The CA shall identify implementation best practice or standards that it applies and demonstrate that this has been complied with. |
| | Monitoring system access and use |
| 8 | Procedures for monitoring the use of CA systems shall be established and the results of the monitoring activities reviewed regularly. Alerting mechanisms shall be implemented to detect unauthorized access and unauthorized modification attempts. |

## 7.12 Audit journal security assurance

All entries in audit journals are required to be marked with a precise time. The time used to record events as required in the audit log is required to be synchronised with UTC at least once a day. While audit journals will normally be created and maintained by the CA management system, some audit journals can out of necessity be manual. The audit requirements are required to be specified in the CA's certification practice statement.

CA audit journal entries are required to include all certificate and key management operations, such as key generation, backup, recovery, and destruction, together with the identity of the person authorizing the operation and persons handling any key material (such as key fragments or keys stored in portable devices or media). Changes in the custody of private keys and associated parameters, and of devices or media holding keys, are required to be recorded in the audit journals. Audit journals should not record the plain text values of any private keys but can hold hash values as a means of identifying keys and validating their correctness as well as that of public keys derived from private keys by means of a one-way function.

A list of audit journal contents is provided in Annex C.

Audit journals are required to be maintained in a form that prevents unauthorized modification or destruction. Automated audit journals are required to be protected from modification or substitution. For example, by using a suitable hash or digital signature function. The private key pair used for signing the audit journal should not be used for any other purpose. In addition, the audit journal should only be retrieved by authorized individuals for valid business or security reasons.

Confidentiality and the need for access control to audit journal records are required to be noted at all times and restricted to authorized personnel only (this may include external auditors).

**Security quality assurance**

- Documented security quality assurance processes and procedures are required as part of the system of internal security control over certificate management. The audit journal is required to be reviewed regularly (e.g. daily) by a security quality assurance function. In some organizations, this function can be fulfilled by the audit department. The review is required to include the validation of the audit journal's integrity, and the identification and follow-up of exceptional, unauthorized, or suspicious activity (e.g. digital signature failures, access at unusual times or from unusual sources, unexpected increases in volume or saturation of system resources).
- The extent and frequency of review and management escalation requirements is required to be determined by a threat/risk evaluation. In high-risk applications and for legal purposes, CA systems can require end entities and relying parties to maintain an audit journal especially where subcontractors are managing certain part of the PKI on behalf of the TSP.

| **Control objectives:** |
|---|
| To ensure that:<br>— CA environmental, key management and certificate management events are accurately and appropriately logged;<br>— the confidentiality and integrity of current and archived audit logs are maintained;<br>— audit logs are completely and confidentially archived in accordance with disclosed business practices;<br>— audit logs are reviewed periodically by authorized personnel. |

| **Control procedures:** | |
|---|---|
| | Audit logs |
| 1 | The CA shall generate automatic (electronic) and manual audit logs as required by the certificate policy. |

| | |
|---|---|
| 2 | All journal entries shall include date and time of the entry. If relevant, also the following elements should be included:<br>a) serial or sequence number of entry (for automatic journal entries);<br>b) kind of entry;<br>c) source of entry (e.g. terminal, port, location, customer, etc.);<br>d) identity of the entity making the journal entry. |
| 3 | Current and archived audit logs shall be protected against unauthorised access, modification, or deletion. |
| 4 | The CA shall implement an audit trail with the purpose to identify evidence of any malicious activities. Roles and responsibilities for monitoring and reviewing these audit logs regularly shall be defined. |
| | Events logged |
| 5 | The CA shall log CA key life cycle management related events. This should include:<br>a) CA key generation;<br>b) installation of manual cryptographic keys and its outcome (with the identity of the operator);<br>c) CA key back-up;<br>d) CA key storage;<br>e) CA key recovery;<br>f) CA key escrow activities (if applicable);<br>g) CA key usage;<br>h) CA key archival;<br>i) withdrawal of keying material from service;<br>j) CA key destruction;<br>k) identity of the entity authorizing a key management operation;<br>l) identity of the entities handling any keying material (such as key components or keys stored in portable devices or media);<br>m) custody of keys and of devices or media holding keys;<br>n) compromise of a private key. |
| 6 | The CA shall log cryptographic device life cycle management related events. This should include where applicable:<br>a) device receipt and installation;<br>b) placing into or removing a device from storage;<br>c) device activation and usage;<br>d) device deinstallation ;<br>e) designation of a device for service and repair;<br>f) device retirement. |

| | |
|---|---|
| 7 | The CA shall log subject (if applicable) key life cycle management related events. This should include:<br>a) key generation;<br>b) key distribution (if applicable);<br>c) key back-up (if applicable);<br>d) key escrow (if applicable);<br>e) key storage;<br>f) key recovery (if applicable);<br>g) key archival (if applicable);<br>h) key destruction;<br>i) identity of the entity authorizing a key management operation;<br>j) key compromise. |
| 8 | The CA shall log (or require that the RA record) the certificate application information. This should include:<br>a) the method of identification applied, and information used to meet “know-your-customer” requirements;<br>b) record of unique identification data, numbers, or a combination thereof (e.g. applicant's driving license number) of identification documents;<br>c) storage location of copies of applications and identification documents;<br>d) identity of entity accepting the application;<br>e) method used to validate identification documents;<br>f) name of receiving CA or submitting RA;<br>g) the subject’s acceptance of the subscriber agreement;<br>h) the subscriber’s consent to allow the CA to keep records containing personal data and pass this information to specified third parties, and publication of certificates. |

| | |
|---|---|
| 9 | The CA shall log certificate life cycle management related events. This should include:<br>a) receipt of requests for certificate(s) – including initial certificate requests, renewal requests and rekey requests;<br>b) submissions of public keys for certification;<br>c) change of affiliation of an entity;<br>d) generation of certificates;<br>e) distribution of the CA's public key;<br>f) certificate revocation requests;<br>g) certificate revocation;<br>h) certificate suspension requests;<br>i) certificate suspension and reactivation;<br>j) generation and issuance of certificate revocation lists. |
| 10 | The CA shall log the security-sensitive events. This should include:<br>a) security sensitive files or records read or written, including the audit log itself;<br>b) actions taken against security sensitive data;<br>c) security profile changes;<br>d) use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication attempts);<br>e) security-sensitive transactions (e.g. account or name/address changes);<br>f) system crashes, hardware failures and other anomalies;<br>g) actions taken by individuals in trusted roles, computer operators, system administrators and system security officers;<br>h) change of affiliation of an entity;<br>i) decisions to bypass encryption/authentication processes or procedures;<br>j) access to the CA system or any component thereof. |
| 11 | Audit logs shall not record the private keys in any form (e.g. plaintext or enciphered). |
| 12 | CA computer system clocks shall be synchronized for accurate recording as defined in the CP or CPS that specifies the accepted time source. |
| | Audit log protection |
| 13 | Any private key used for signing audit logs shall not be used for any other purpose. This should apply equally to a symmetric secret key used with a symmetric MAC mechanism. |
| | Audit log retention |
| 14 | In addition to possible regulatory stipulation, an assessment of requirements shall be performed to determine the appropriate length of time for retention of audit logs. |
| 15 | The CA shall retain audit log data for the determined period (see control procedure 14 above). |
| 16 | The CA should maintain archived audit logs at a secure off-site location as determined by risk assessment. |
| | Review of audit logs |

| | |
|---|---|
| 17 | Current and archived audit logs shall only be retrieved by authorized individuals for valid business or security reasons. |
| 18 | Audit logs shall be reviewed according to the practices established in the CPS. |
| 19 | The review of current and archived audit logs should include a validation of the audit logs' integrity, and the identification and follow-up of exceptional, unauthorized, or suspicious activity.<br>Examples of conditions requiring analysis and possible action include unusual saturation of system resources, sudden and unexpected increases in volume and access at unusual times or from unusual places. |

## 7.13 CA key life cycle management controls

### 7.13.1 CA key generation

| **Control objective:** |
|---|
| — To provide reasonable assurance that CA key pairs are generated in accordance with defined key generation ceremony scripts and the requirements of the CPS.<br>— To provide reasonable assurance that:<br>a) Devices used for private key storage and recovery are tested for integrity before usage;<br>b) Access to CA cryptographic hardware is restricted to authorized personnel:<br>c) CA cryptographic hardware is functioning correctly. |

| **Control procedures:** | |
|---|---|
| | Generation of CA keys, including root CA keys |
| 1 | CA key generation shall be performed in accordance with a detailed CA key generation ceremony script that specifies the steps to be performed and participant responsibilities. The CA key generation script should include the following:<br>a) definition of roles and responsibilities;<br>b) approval for conduct of the key generation ceremony;<br>c) cryptographic hardware and activation materials required for the ceremony;<br>d) specific steps performed during the key generation ceremony;<br>e) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony;<br>f) sign-off from management and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script;<br>g) notation of any deviations from the key generation ceremony script.<br>Refer to Annex B for additional discussion of CA key generation ceremonies. |

| | |
|---|---|
| 2 | Generation of CA keys shall occur within a secure cryptographic device and shall be in accordance with the business requirements and in accordance with the CPS. The requirements of common criteria / ISO/IEC 15408 (suitable protection profile with EAL 4 AVA_VAN.5 or higher) or ISO/IEC 19790 should be taken into account. Such cryptographic devices shall perform key generation using a random number generator (RNG) or pseudo random number generator (PRNG). Prime number generation should take into account requirements of ISO/IEC 18032. |
| 3 | Generation of CA keys shall be undertaken in a physically secured environment (see 7.3) by personnel in trusted roles (see 7.3) under the principles of multiple control and split knowledge (See Annex B). |
| 4 | The CA shall either generate its own key pair in the same cryptographic device in which it will be used, or the private key shall be passed securely from the device where it was generated into the device where it will be used. |
| 5 | CA key generation shall generate keys with algorithm and key length which:<br>a) is suitable for the intended use;<br>b) is suitable for the validity period of the CA certificate;<br>c) takes into account requirements on parent and subordinate CA key sizes;<br>d) is in accordance with the CP. |
| 6 | The public key length to be certified by a CA shall be less than or equal to that of the CA's certifying public signing key. |
| 7 | Before going into production, the operation of the user software and cryptographic hardware shall be tested. |
| 8 | CA cryptographic hardware sent from the manufacturer should be sent in tamper evident packaging. The tamper evident seal should be checked to ensure it is intact. |
| 9 | CA cryptographic hardware sent from the manufacturer should be acceptance tested. |
| 10 | CA cryptographic hardware should be stored and used in a secure site, accessed only by authorized personnel. |
| 11 | CA cryptographic hardware when not attached to the CA system should be stored securely. |
| 12 | CA cryptographic hardware installation, removal, servicing, repair should be carried out by at least two authorized personnel. |
| 13 | CA cryptographic hardware should be verified on a regular basis. |

### 7.13.2 CA key storage, back-up, and recovery

| **Control objectives:** |
|---|
| To disseminate only correct certificates that can be validated by relying parties and to provide reasonable assurance that the integrity of the CA key and any associated parameters are maintained during initial and subsequent distribution. |

| **Control procedures:** | |
|---|---|
| 1 | The CA's private (signing and confidentiality) keys shall be stored and used within a secure cryptographic device meeting requirements based on a risk assessment and the business requirements of the CA and in accordance with the CA's CPS and applicable certificate policies. When defining the requirements, an appropriate ISO/IEC 15408 / common criteria protection profile EAL 4 AVA_VAN.5 (or higher), ISO/IEC 19790 / FIPS 140-2 level 3 (or higher), or equivalent standards should be considered and taken into account. |

| | |
|---|---|
| 2 | If the CA's private keys are exported from a secure cryptographic device to secure storage for purposes of offline processing or back-up and recovery, then they shall be exported within a secure key management scheme that may include any of the following:<br>a) cipher text using a key which is appropriately secured;<br>b) encrypted key fragments using multiple control and split knowledge/ownership;<br>c) another secure cryptographic module, such as a key transportation device using multiple control. |
| 3 | If the CA's private keys are backed up, they shall be backed up, stored, and recovered by authorized personnel in trusted roles, using multiple controls in a physically secured environment. The number of personnel authorized to carry out this function shall be kept to a minimum, while still ensuring the availability of sufficient staff for any controls requiring multiple personnel. |
| 4 | If the CA's private keys are backed up, back-up copies of the CA private keys shall be subject to the same or a greater level of security controls as keys currently in use. |
| 5 | The recovery of the CA's keys shall be carried out in as secure a manner as the back-up process. |
| | CA cryptographic device life cycle management |
| 6 | Upon the receipt of CA cryptographic hardware from the manufacturer, acceptance testing, and verification of firmware settings shall be performed. Upon the receipt of CA cryptographic hardware that has been serviced or repaired, acceptance testing, and verification of firmware settings shall be performed. |
| 7 | To prevent tampering, CA cryptographic hardware shall be stored and used in a secure site, with access limited to authorized personnel. This should include the following:<br>a) inventory control processes and procedures to manage the origination, arrival, condition, departure, and destination of each device;<br>b) access control processes and procedures to limit physical access to authorized personnel;<br>c) recording of all successful or failed access attempts to the CA facility and device storage mechanism (e.g. a safe) in audit logs;<br>d) incident handling processes and procedures to handle abnormal events, security breaches, and investigation and reports;<br>e) audit processes and procedures to verify the effectiveness of the controls. |
| 8 | The handling of CA cryptographic hardware, including the following tasks, should be performed in the presence of no less than two trusted employees:<br>a) installation of CA cryptographic hardware;<br>b) removal of CA cryptographic hardware from production;<br>c) servicing or repair of CA cryptographic hardware (including installation of new hardware, firmware, or software);<br>d) disassembly and permanent removal from use. |
| 9 | Devices used for private key storage and recovery and the interfaces to these devices shall be tested before usage for integrity (e.g. following manufacturer's instructions). |

### 7.13.3 CA public key distribution

| **Control objective:** |
|---|
| The CA shall maintain controls to provide reasonable assurance that the integrity and authenticity of the CA public key and any associated parameters are maintained during initial and subsequent distribution. |

| **Control procedures:** | |
|---|---|
| 1 | The CA shall provide a mechanism for validating the authenticity and integrity of the CA's public keys. Where a self-signed certificate is used for any CA, then the CA shall provide a mechanism to verify the authenticity of the self-signed certificate (e.g. publication of the certificate's fingerprint).<br>For subsequent and subordinate CA public keys, these shall be validated, by using a chaining method or similar process, to link back to the trusted root certificate. For a new root certificate, an out-of-band process can be required.<br>If applicable, the CA shall issue a link certificate for its new public key before the expiration of its current public key. |
| 2 | The initial distribution mechanism for the CA's public key shall be controlled as documented in the CA's CPS. This may include one of the following methods:<br>a) machine readable media (e.g. smart card, CD ROM) from an authenticated source;<br>b) embedding in an entity's cryptographic module;<br>c) other secure means that ensure authenticity and integrity. |
| 3 | The CA shall periodically generate new certificates that contain new public keys, according to the requirements of the CPS |
| 4 | The subsequent distribution mechanism for the CA's public key shall be controlled as documented in the CA's CPS. |
| 5 | Any new CA public key should be made available to relying parties. |

### 7.13.4 CA key usage

| **Control objective:** |
|---|
| The CA shall maintain controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations. |

| **Control procedures:** | |
|---|---|
| 1 | The activation of the CA private signing key shall be performed using at least dual control, by person(s) in a trusted role. It is recommended to use multi-party control (i.e. *m* of *n where n* > *m*). |
| 2 | Based on a risk assessment, the activation of the CA private key should be performed using multifactor authentication (e.g. smart card and password, biometric and password). |
| 3 | CA signing key(s) used for generating certificates or issuing revocation status information, shall not be used for any other purpose. |
| 4 | The CA's private keys shall only be used within physically secure premises (see 7.6). |
| 5 | The CA shall cease to use a key pair at the end of the key pair's defined operational lifetime or when the compromise of the private key is known or suspected. |

| | |
|---|---|
| 6 | Correct processing of CA cryptographic hardware should be verified on a periodic basis. |
| 7 | An annual review should be required by the PA on key lengths to determine the appropriate key usage period and the recommendations shall be acted upon. |

### 7.13.5 CA key archival and destruction

| **Control objectives:** |
|---|
| The CA shall maintain controls to provide reasonable assurance that:<br>— archived CA keys remain confidential and secured in the event that they are put back into production;<br>— CA keys are completely destroyed at the end of the key pair life cycle as determined by the CPS. |

| **Control procedures:** | |
|---|---|
| | CA key archival |
| 1 | Where CA private keys are archived, they shall be subject to the same or a greater level of security controls as keys currently in use. |
| 2 | Archived keys should only be put back into production when an incident results in a loss of production keys or where historical evidence requires validation. |
| | CA key destruction |
| 3 | Authorization to destroy a CA private key and how the CA's private key is destroyed (e.g. hardware token surrender, hardware token destruction or key overwrite) shall be limited in accordance with the CA's CPS. |
| 4 | All copies and fragments of the CA's private key shall be destroyed in a manner such that the private key cannot be retrieved. |
| 5 | If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose shall be erased from the device. |
| 6 | The CA shall destroy its corresponding private key and all the backups after revocation or regular end of validity of the CA certificate. |
| 7 | Destruction of CA keys shall be undertaken in a physically secured environment (see 7.6) by personnel in trusted roles (see 7.5) under the principles of multiple control. |
| 8 | Destruction of a key encrypting key used to protect the CA private key may be considered as destruction of the CA private key in a manner such that the private key cannot be retrieved. |
| 9 | Algorithms and key length for key encryption of keys held outside HSM shall be at least as strong as the keys being encrypted. |
| 10 | CA private key destruction shall be recorded and witnessed. |

### 7.13.6 CA key compromise

| **Control objective:** |
|---|
| The CA shall maintain controls to provide reasonable assurance that continuity of operations is maintained in the event of the compromise of the CA's private keys. |

| Control procedures: | |
|---|---|
| 1 | The CA’s business continuity plans shall address the compromise or suspected compromise of a CA's private keys as a disaster. |
| 2 | In the event of the compromise or suspected compromise of a CA's private signing key, disaster recovery procedures shall exist. Details of recovery of compromise such as whether to revoke and re-issue certificates shall be part of the CA’s disaster recovery plan. |
| 3 | The recovery procedures used if the CA's private key is compromised should include, where applicable, the following actions:<br>a) how to secure key usage in the re-established environment;<br>b) how the CA’s old public key is revoked or relying parties are otherwise made aware that the public key cannot be trusted;<br>c) the notification procedures for affected parties (e.g. impacted CAs, repositories, subscribers and CVSPs), including who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures, and encrypted data;<br>d) how the CA’s new public key is provided to the end entities and relying parties together with the mechanism for their authentication;<br>e) how the subject’s public keys are recertified. |
| 4 | In the event that the CA has to replace its root CA private key, procedures should be in place to ensure relying parties are aware that the public key cannot be trusted for the secure and authenticated revocation of the following:<br>a) the old CA root public key;<br>b) the set of all certificates (including any self-signed) issued by a root CA, or any CA based on the compromised private key;<br>c) any subordinate CA public keys and corresponding certificates that require recertification. |
| 5 | The CA business continuity plan should consider key replication techniques. |

## 7.14 Subject key life cycle management controls

### 7.14.1 CA-provided subject key generation services (if supported)

| Control objectives: |
|---|
| To ensure that the CA maintains controls to provide reasonable assurance that:<br>— subject keys generated by the CA (or RA or other authorized third party) are generated in accordance with the CP;<br>— subject keys generated by the CA (or RA or other authorized third party) are securely distributed to the subject by the CA (or RA or other authorized third party). |

| **Control procedures:** | |
|---|---|
| | CA (or RA or other authorized third party) provided subject key generation |
| 1 | Subject key generation performed by the CA (or other authorized third party) shall be protected from unauthorized disclosure and occur within a cryptographic device meeting requirements based on a risk assessment and the business requirements of the CA and in accordance with the applicable CP. The requirements in ISO/IEC 19790 (FIPS 140-2) or ISO/IEC 15408 (with an appropriate protection profile or security target) or common criteria or equivalent should be taken into account. |
| 2 | Subject key generation performed by the CA (or other authorized third party) shall use a key generation algorithm as specified in the CP. |
| 3 | Subject key generation performed by the CA (or other authorized third party) shall result in key sizes in accordance with the CP. |
| 4 | Cryptographic algorithms and key sizes stipulated by the CP shall be selected according to best practices. |
| 5 | Subject key generation performed by the CA shall be performed by a secure process in a process initiated by authorized personnel in accordance with the CA's CPS. |
| 6 | When subject key generation is performed by the CA (or other authorized third party), the CA (or other authorized third party) shall securely (confidentially) deliver the subject key pair(s) generated by the CA (or RA or other authorized third party) to the subject in accordance with the CP. The key pair shall be disseminated only to the subject. |
| 7 | Subject key generation shall only be carried out by a party authorized by the CA. |
| 8 | After the private key has been provided to the subscriber, it shall be destroyed without undue delay (including any copies) unless it is still needed for key storage, recovery, or back-up services. |

### 7.14.2 CA-provided subject key storage and recovery services (if supported)

**Control objectives:**

If the CA provides subject confidentiality key storage, recovery or escrow services, the CA shall maintain controls to provide reasonable assurance that:

— subject private keys stored by the CA remain confidential and maintain their integrity;

— subject private keys stored by the CA are completely destroyed at the end of the key pair life cycle;

— subject private keys archived and escrowed by the CA remain confidential.

| **Control procedures:** | |
|---|---|
| | CA-provided subject key storage, back-up, archival and recovery |
| 1 | Subject private keys stored by the CA (or trust service provider for key storage) shall be stored in accordance with the results of a risk assessment and the requirements of the CP, e.g. in encrypted form using an appropriate cryptographic algorithm and key length. |
| 2 | If the CA generates signing key pair(s) on behalf of a subscriber, the CA (or trust service provider for key storage) shall ensure that subject's private keys are not disclosed to any entity other than the owner (i.e. the subject) of the keys. |
| 3 | If the CA (or trust service provider for key storage) generates public/private signing key pair(s), it shall not maintain a copy of any subject's private signing key, once the subject confirms receipt of that key. |

| | |
|---|---|
| 4 | If the CA (or trust service provider for key storage) provides subject (confidentiality) key storage, back-up, and recovery, subject private (confidentiality) key back-up and recovery, then these services shall only be performed by authorized personnel. |
| 5 | If the CA (or trust service provider for key storage) provides subject key storage, back-up and recovery, controls shall exist to ensure that the integrity and confidentiality of the subject's private key is maintained throughout its life cycle, e.g. subject private (confidentiality) keys held by the CA shall be secured e.g. in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the requirements of the CP. |
| 6 | If the CA provides subject (confidentiality) key archival, all archived subscriber keys shall be destroyed at the end of the archive period. |
| 7 | In case the CA provides key recovery, the CA shall disseminate the subscriber or subject backup key following the same or equivalent requirements as for the original dissemination of the key. |
| 8 | In the case the CA provides key recovery, the CA should send notification to the subscriber of all attempts (successful or unsuccessful) to recover escrowed keys that are made by entities claiming to be the subscriber. |
| | CA-provided subject key destruction |
| 9 | If the CA provides subject (confidentiality) key storage, authorization to destroy a subject's private key and the means to destroy the subject's private (confidentiality) key (e.g. key overwrite) shall be limited in accordance with the CP. |
| 10 | If the CA provides subject (confidentiality) key storage, all copies and fragments of the subject's private key shall be destroyed at the end of the key pair life cycle. |
| | CA-provided subject key escrow |
| 11 | Subject private (confidentiality) keys escrowed by the CA for purposes of access by law enforcement shall be secured e.g. in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the requirements of the CP. |
| 12 | Subject private keys stored by the CA (or trust service provider for key storage) shall be protected from unauthorized access, exportation, and use based on a risk assessment and requirements of the CP. |
| | Subject key archival |
| 13 | The CP shall specify the private key protection requirements for archived subject private keys. |
| 14 | The CP shall specify the requirements for destruction of archived subject keys at the end of the archive period. |

### 7.14.3 Hardware token life cycle management if outsourced to an external service (if supported)

| **Control objectives:** |
|---|
| If the CA (or RA) distributes subject key pairs and certificates to minimize the risk of key compromise during hardware token preparation and dissemination that is, to provide reasonable assurance for:<br>a) securely controlling hardware token procurement, preparation, and personalization;<br>b) enabling hardware token usage by the CA (or RA or other authorized third party) prior to hardware token issuance;<br>c) securely storing and distribute hardware tokens;<br>d) securely replacing hardware tokens;<br>e) securely terminating hardware tokens returned to the CA (or RA or other authorized third party). |

| **Control procedures:** | |
|---|---|
| | Hardware token procurement |
| 1 | If the CA or RA engages a card bureau then a formal contract shall exist between the relevant parties. While card issuing functions may be delegated to third parties, the CA shall retain responsibility and liability for the hardware tokens. |
| 2 | Hardware tokens shall be logically protected during transport between the card manufacturer and the card issuer through the use of a secret transport key or pass phrase. |
| 3 | Hardware tokens issued to subject be demonstrated to meet the requirements of the CP. ISO/IEC 19790 (FIPS 140-2) or ISO/IEC 15408 with an appropriate protection profile or security target may be used to demonstrate that requirements are met. |
| 4 | The card bureau shall verify the physical integrity of hardware tokens upon receipt from the card manufacturer. |
| 5 | Hardware tokens shall be securely stored and under inventory control while under the control of the card issuer. |
| | Card preparation and personalization |
| 6 | Hardware token preparation processes and procedures, including the following, shall exist and be followed.<br>The hardware token shall be protected, in particular to prevent unauthorized modification of the software. |
| 7 | Hardware token personalization processes and procedures, including the following, shall exist and be followed:<br>a) the loading of identifying information on to the card;<br>b) generation of subject key pair(s) in accordance with 7.13 and the CP;<br>c) If the subject private key(s) are generated outside the hardware token, the key(s) shall be loaded in encrypted form. The CA shall ensure that access or manipulation of subscribers' private keys is not possible before, during and after the dissemination process;<br>d) loading subject certificate(s) on to the hardware token;<br>e) loading the CA's and other relevant certificates on to the hardware token;<br>f) logically protecting the hardware token from unauthorized access. |
| 8 | The card bureau or CA (or RA) shall log hardware token preparation and personalization in an audit log. |
| 9 | A hardware token shall not be issued unless it has been prepared and personalized by the card bureau, the CA, or the RA. |
| 10 | A hardware token shall be unusable unless in an activated state. |
| | Hardware token distribution |
| 11 | Processes and procedures shall exist and be followed for the distribution, tracking and accounting of the safe distribution of hardware tokens to subjects. All parties shall be aware of the procedures relevant to them. |
| 12 | Hardware token initial activation data (initializing PIN) shall be securely communicated to the subject or, where applicable, the subscriber using an out-of-band method. The subject shall be encouraged to change the initial activation data upon receipt to make the card active. |
| 13 | Distribution shall be logged by the card bureau or CA (or RA) in an audit log. |
| | Subject hardware token usage |

| | |
|---|---|
| 14 | The subject shall be provided with a mechanism that protects the access to the card data including the private keys stored on the hardware token during use by the subscriber (i.e. PIN access control mechanism – cardholder verification method). |
| 15 | The subject private keys on the hardware token shall not be exported to an application to undertake cryptographic (i.e. signing) functions. |
| 16 | The subject shall be required to use a mutual authentication mechanism for cryptographic application and card functions to ensure system integrity. |
| 17 | The subject shall be required to use an application that displays the message or the message's digest to the subject prior to signing message (or transaction) data. The subject hardware token application shall produce audit logs of all uses of the hardware token. This also includes all attempts in the private key owner verification process. This evidence can be presented by the subject or, where applicable, the subscriber, should relying parties dispute the authenticity or integrity of a transaction. |
| 18 | The hardware token shall be used by the subject or, where applicable, the subscriber in accordance with the terms of the CP. |
| | Hardware token replacement |
| 19 | Processes and procedures shall exist and be followed for replacement of a subject's lost or damaged hardware token. |
| 20 | In the event of card loss or damage, subject certificates shall be renewed with the same key or rekeyed with a new key in accordance with the CP (see 7.15). |
| 21 | Hardware token replacement shall be logged by the card bureau or CA (or RA) in an audit log. |
| | Hardware token termination |
| 22 | All HSMs returned to the CA (or RA) shall be deactivated or securely destroyed to prevent unauthorized use. |
| 23 | Hardware token termination shall be logged by the card bureau or CA (or RA) in an audit log. |

### 7.14.4 Subject key management, if supported

| **Control objective:** |
|---|
| To securely manage subject keys throughout the key life cycle. To ensure integrity of the private-public key pair and confidentiality of the private key. This only applies if the CA is managing keys on behalf of the subject. |

| **Control procedures:** | |
|---|---|
| | Subject key usage |
| 1 | Terms and conditions (or separate subscriber agreements) shall describe the required processes to be followed by the subscriber (and where applicable the subjects) of any use of the cryptographic mechanism (e.g. HSM or hardware token and software application). |
| 2 | The CP shall specify the acceptable uses for subject key pairs. |
| 3 | The CP shall specify the requirements for subject key usage. To securely manage subject keys throughout the key life cycle. To ensure integrity of the private-public key pair and confidentiality of the private key. |

| | |
|---|---|
| 4 | The CA or a component service shall reject a subscriber key if it evidently:<br>a) was generated with a vulnerable algorithm or an unsecure implementation of the chosen algorithm;<br>b) has an insufficient key length:<br>c) does not comply with other applicable cryptographic requirements. |
| 5 | The CA or a component service shall verify that a public key generated and provided by a registered subscriber belongs to the subscriber before it can be used within the PKI. |
| | Subject cryptographic hardware life cycle management |
| 6 | If required, the CP shall specify the requirements for use and handling of cryptographic hardware and subject authentication processes (and subsequent actions) where the cryptographic hardware is in other physical locations (i.e. an HSM attached to a mainframe or remote server). |
| | Subject key compromise |
| 7 | The CP shall specify the requirements for notification of the CA or RA in the event of subject key compromise. |

## 7.15 Certificate life cycle management controls

### 7.15.1 Subject registration

| **Control objectives:** |
|---|
| The CA shall maintain controls to provide reasonable assurance that:<br>— subjects (or where applicable the subscribers) are accurately identified in accordance with the applicable "know-your-customer" requirements;<br>— subjects' (or where applicable the subscribers') certificate requests are accurate, authorized, and complete. |

| **Control procedures:** | |
|---|---|
| | Identification and authentication |
| 1 | The CA shall verify or require that the RA verify the credentials presented by a subject as evidence of identity or authority to perform a specific role in accordance with the certificate policy. |
| 2 | The CA or RA shall verify the accuracy of the information included in the requesting entity's certificate request in accordance with the CP. |
| 3 | The CA or RA shall check the certificate request for errors or omissions in accordance with the CP. |
| 4 | For end entity certificates, the CA shall ensure that the signing request is securely submitted and is authenticated as coming from an authorized entity. |
| 5 | Encryption and access controls shall be used to protect the confidentiality and integrity of registration data in transit and in storage. |
| 6 | At the point of registration (before certificate issuance) the RA or CA shall inform the subject or, where applicable, the subscriber of the terms and conditions regarding use of the certificate. |
| 7 | Identification and authentication of a subject shall precede any other processes (e.g. certificate issuance) in connection with the subject in question as required by CP. |
| 8 | A record of registration and related administrative data presented by a subject as evidence of identity shall be kept by the RA or CA. |

| | Certificate request |
|---|---|
| 9 | The CA shall require that an entity requesting a certificate shall prepare and submit the appropriate certificate request data (registration request) to an RA (or the CA) as specified in the CP. |
| 10 | There shall be evidence of the subjects' agreement to the terms and conditions. |
| 11 | The CA (or RA) shall record the success or failure of the registration event in an audit log. |
| 12 | The CA shall store the certificate enrolment data in a database which is protected against unauthorized access, alteration, and deletion. |
| 13 | The CA or RA shall ensure that the 'Identification and registration' process is secure. In particular every transfer of registration and identification inside or outside the CA or RA shall be protected against eavesdropping and manipulation. |

### 7.15.2 Certificate renewal (if supported)

| **Control objective:** |
|---|
| If certificate renewal is supported under the CP, the CA shall maintain controls to provide reasonable assurance that corresponding requests are processed in a timely manner if and only if they are accurate, authorized, and complete. |

| **Control procedures:** | |
|---|---|
| | Certificate renewal request |
| 1 | The request shall identify the certificate to be renewed. |
| 2 | The CA shall ensure that the renewal request is securely submitted and is authenticated as coming from an authorized entity. |
| 3 | The CA shall issue a new certificate using the subject's previously certified public key only if its cryptographic security is still sufficient for the new certificate's intended lifetime and the requesting subscriber is authorized to request the certificate.<br>In particular, the CA shall not issue a new certificate if:<br>a) indications exist that the subject's private key has been compromised;<br>b) the previous certificate of the subscriber has been revoked;<br>c) the subscriber is still suspended. |
| 4 | The CA or the RA shall process the certificate renewal data to verify the identity of the requesting entity and identify the certificate to be renewed. |
| 5 | The CA shall verify the existence and validity of the certificate to be renewed. No renewal shall be permitted unless the existing certificate status is live (i.e. not revoked or suspended). |
| 6 | The CA or the RA shall verify that the request, including the extension of the validity period, meets the requirements defined in the CP. |
| 7 | The RA shall secure the part of the certificate renewal process, for which it (the RA) assumes responsibility, in accordance with the CP. |
| 8 | The CA shall ensure that renewal actions are recorded in an audit log. |
| 9 | The CA shall check the certificate renewal request for errors or omissions. This function can be delegated explicitly to the RA. |

| | |
|---|---|
| 10 | The CA or RA should notify subjects or, where applicable, subscribers prior to the expiration of their certificate of the need for renewal in accordance with the CP. The notifications from the CA or RA should inform that requests for renewal, rekeying or update of a certificate shall be submitted in due time by the subject. The CA should generate new certificates within the time frame communicated in the notifications to the subject. |
| 11 | The CA should issue a signed notification indicating the certificate renewal has been successful. |
| 12 | The CA shall make the new certificate available to the end entity in accordance with the CP. |
| 13 | The CA shall define Terms and Conditions in which cases renewal may be allowed |
| 14 | The CA shall check duly if the renewal of a certificate is appropriate. Requests to reuse an existing key shall take into account potential weaknesses in the key over the certificate lifetime. Also, it may be necessary to re-check claimed attributes. |

### 7.15.3 Certificate rekey

| **Control objective:** |
|---|
| To rekey only certificates containing correct subject information and provide reasonable assurance that certificate rekey requests are accurate, authorized, and complete. |

| **Control procedures:** | |
|---|---|
| 1 | The CA shall ensure that the rekey request is securely submitted and is authenticated as coming from an authorized entity. |
| 2 | The CA shall ensure rekey actions are recorded in an audit log. |
| 3 | The CA or the RA shall check the certificate rekey request for errors or omissions. |
| 4 | The CA or RA should notify subscribers prior to the expiration of their certificate of the need to rekey. |
| 5 | Prior to the rekeying of existing certificates, the CA or RA shall verify the following:<br>a) the signature on the certificate rekey data submission;<br>b) the existence and validity supporting the rekey request;<br>c) that the request meets the requirements defined in the CP.;<br>d) the certificate is not revoked, and its subject is not suspended;<br>e) the new certificate validity period is not extended beyond the expected end of life of the cryptographic algorithm or the key length of the associated key pair;<br>f) the relevant attributes of the certificate still match the current registration data of the certificate subject. |
| 6 | Where a new certificate is required by the subscriber, following revocation, the entity shall be required to apply for a new certificate in accordance with the CP. |
| 7 | Where a new certificate is required by the subscriber following expiration of the entity's certificate, the certificate can be automatically generated, or the entity shall be required to request a new certificate in accordance with the CP. |
| 8 | The CA shall define Terms and Conditions in which cases rekeying may be allowed. |

### 7.15.4 Certificate issuance

| Control objective: |
|---|
| To provide reasonable assurance that certificates are generated and issued (manufactured) in accordance with the CP. |

| Control procedures: | |
|---|---|
| 1 | The CA shall generate certificates using certificate request data and manufacture the certificate as defined by the appropriate certificate profile in accordance with ISO/IEC 9594-8 formatting rules. |
| 2 | Validity periods shall be set in the CP and shall be formatted in accordance with ISO/IEC 9594-8. |
| 3 | Extension fields shall be formatted in accordance with ISO/IEC 9594-8. |
| 4 | The CA shall log the event in an audit log including at least information identifying the<br>certificate issued. |
| 5 | Certificates shall be issued based on approved subject registration, certificate renewal or certificate rekey requests in accordance with 7.15.1, 7.15.2, and 7.15.3. |
| 6 | The CA should issue a notification to appropriate parties, e.g. the RA when a certificate is issued to a subject for whom the RA submitted a certificate request. |
| 7 | The CA shall issue an out-of-band notification to the subject or subscriber when a certificate is issued. When this notification includes initial activation data, then control processes shall ensure safe delivery to the subject. |
| 8 | Whether certificates expire, are revoked, or are suspended, copies of certificates shall be retained for the appropriate period of time specified in the CP. |
| 9 | Each certificate shall identify the applicable CP to which the CA conforms in each issued<br>Certificate. |

### 7.15.5 Certificate distribution

| Control objective: |
|---|
| To maintain controls to provide reasonable assurance that, upon issuance, complete and accurate certificates are available to any entity as defined in the CP. |

| Control procedures: | |
|---|---|
| 1 | The CA shall make the certificates issued by the CA available to relevant parties using an established mechanism (e.g. a repository such as a directory) in accordance with the CP. Possible mechanisms include:<br>a) collection – repository or online directory service;<br>b) delivery – distributed using protected media (e.g. CD-ROM or hardware token). |
| 2 | Only authorized CA personnel shall administer the CA's repository or alternative distribution mechanism. |
| 3 | The performance of the CA's repository or alternative distribution mechanism shall be monitored and managed. |

| | |
|---|---|
| 4 | Where required, certificates shall be made available for retrieval only in those cases for which the subject’s consent is obtained. If the CP requires that all certificates issued by the CA are made available, the CA shall not issue a certificate for a subject unless that subject's consent for such distribution is obtained. |

### 7.15.6 Certificate revocation

| **Control objective:** |
|---|
| To maintain controls to provide reasonable assurance that certificates are revoked in a timely manner and information about revoked certificates is published as dictated by risk, based on authorized and validated certificate revocation requests. |

| **Control procedures:** | |
|---|---|
| 1 | The CA shall provide a means to facilitate the secure and authenticated revocation of one or more certificates of one or more subjects without undue delay. |
| 2 | The CA shall ensure that the revocation request is securely submitted and is authenticated as coming from an authorized entity. |
| 3 | The CA shall update the certificate revocation list (CRL), online certificate status protocol (OCSP) responder, or other certificate status mechanisms in the time frames specified within the CP and in accordance with the format defined in ISO/IEC 9594-8. |
| 4 | The CA shall record all certificate revocation requests and their outcome in an audit log. See Annex C for further guidance. |
| 5 | The CA or RA can provide an authenticated acknowledgement (signature or similar) of the revocation to the entity who perpetrated the revocation request. |
| 6 | Even if certificate renewal is supported, a revoked certificate shall never be reinstated. |
| 7 | The CA should ensure that the subject or the subscriber are notified in the event of a certificate revocation. |
| 8 | The system hosting the revocation information shall be protected against system failure and attacks. The CA shall analyse the risk of a system failure and attacks against the system, taking the assumed traffic into account. |
| 9 | The CA shall ensure that the revocation information is secured against unauthorized modification. |
| 10 | The CA shall maintain controls to revoke certificates and publish appropriate information about the revoked certificates. |
| 11 | In case a legitimate revocation request is received, the CA or a corresponding component service shall update the revocation status information within the time frame specified in the CP or CPS. |

### 7.15.7 Certificate suspension (if supported)

| **Control objective:** |
|---|
| If supported, to suspend certificates or subscribers in a timely manner as dictated by risk, based on legitimate (i.e. authorized and validated) requests. |

| Control procedures: | |
|---|---|
| 1 | The CA shall define and implement a process for processing suspension requests in accordance with the CPS. Such a process shall be available to ensure the secure and authenticated suspension of the following:<br>a) one or more certificates of one or more subjects;<br>b) the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates;<br>c) all certificates issued by a CA, regardless of the public/private key pair used. |
| 2 | The CA shall ensure that the suspension request is securely submitted and is authenticated as coming from an authorized entity. |
| 3 | The CA or RA shall notify the subject and, where applicable, the subscriber in the event of a certificate suspension. |
| 4 | Certificate suspension requests shall be processed and validated in accordance with the requirements of the CP. |
| 5 | The CA shall update the certificate revocation list (CRL) and other certificate status mechanisms upon certificate suspension. Changes in certificate status shall be completed in a time frame determined by the CP. |
| 6 | Certificates shall be suspended only for the allowable length of time in accordance with the CP. |
| 7 | Once a certificate suspension (hold) has been issued, the suspension shall be handled in one of the following three ways:<br>a) an entry for the suspended certificate remains on the CRL with no further action;<br>b) the CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate;<br>c) the suspended certificate is unsuspended, and the entry removed from the CRL. |
| 8 | A certificate suspension (hold) entry shall remain on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first. The CP can specify the maximum number of occasions when the certificate status can be suspended and the maximum periodicity for this status. |
| 9 | The CA shall update the certificate revocation list (CRL) and other certificate status mechanisms upon the lifting of a certificate suspension in accordance with the CA's CP. |
| 10 | The CA shall verify or requires that the RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted. |
| 11 | Certificate suspensions and the lifting of certificate suspensions shall be recorded in an audit log. See Annex C for further guidance. |
| 12 | A certificate should be suspended only if it is likely that private key or other information in the certificate has not been compromised. |
| 13 | In case a legitimate suspension request is received, the CA or a corresponding component service shall update the suspension status information within the time frame specified in the CP or CPS. |
| 14 | The CA shall ensure that the suspension status information is secured against unauthorized modification. |
| 15 | The system hosting the suspension status information shall be protected against system failure and attacks. The CA shall analyse the risk of a system failure and attacks against the system, taking the assumed traffic into account. |

### 7.15.8 Revocation status information service

| **Control objective:** |
|---|
| To reliably provide up-to-date, complete, and accurate certificate status information to relevant entities (subscribers and relying parties or their agents, i.e. CVSPs) in accordance with the CP. |

| **Control procedures:** | |
|---|---|
| 1 | The CA shall make certificate status information available to relevant entities (relying parties or their agents) using an established mechanism in accordance with the CP. This can be achieved using:<br>a) request response method – a request from the relying party to the certificate status provider's responder; in turn, the certificate status provider's responder responds with the certificate status duly signed (OCSP is an example protocol using this method);<br>b) delivery method – a CRL signed by the CA and published within the policy's time frame. |
| | Applicable control procedures where CRLs are used |
| 2 | The CA shall digitally sign each CRL that it issues so that entities can validate the integrity of the CRL and the date and time of issuance. |
| 3 | The CA shall issue CRLs at regular intervals, as specified in the CP, even if no changes have occurred since the last issuance. |
| 4 | At a minimum, a CRL entry identifying a revoked certificate shall remain on the CRL until the end of the certificate's validity period. A retrospective view of a certificate status, at a given point in time, can be required. Therefore, CRL entries may need to be held beyond the life of a certificate validity period to prove its validity at the time of use. |
| 5 | If certificate suspension is supported, a certificate suspension (hold) entry, with its original action date and expiration date shall remain on the CRL until the normal expiration of the certificate or until the suspension is lifted. |
| 6 | CRLs shall be retained and archived for the appropriate period of time in accordance with the requirements of the CP, including the method of retrieval. |
| 7 | The CRL shall contain entries for all revoked unexpired certificates issued by the CA. A retrospective view of a certificate status, at a given point in time, can be required. Therefore, CRL entries may need to be held beyond the life of a certificate validity period to prove its validity at the time of use. |
| | Applicable control procedures where online certificate status mechanisms (e.g. OCSP) are used |

| | |
|---|---|
| 8 | Upon the receipt of a certificate status request (e.g. an OCSP request) from a relying party or its agent, the CA shall return a definitive response to the relying party or its agent if:<br>a) the request message is well formed;<br>b) the certificate status provider responder is configured to provide the requested service;<br>c) the request contains the information (certificate identity, e.g. serial number, OID) needed by the certificate status provider responder in accordance with the CP;<br>d) the certificate status provider's responder is able to locate the certificate and interpret its status.<br>Where these conditions are met, the CA or certificate status provider shall produce a signed response message indicating the certificate's status in accordance with the CP. If any of these conditions are not met, then a status may be returned in accordance with the CP such as “unknown”. |
| 9 | All response messages shall be digitally signed and include all required data in accordance with the CP. |
| 10 | The online certificate status mechanism shall make available information on revoked certificates and, where supported, suspended certificates. |

### 7.15.9 Controlled CA termination

| Control objective: |
|---|
| To maintain the CA’s responsibilities for an adequate transition period in accordance with the CP or terms and conditions in the event of the termination of the CA for whatever reason. In particular, to maintain the availability of timely, complete, and accurate information to relevant entities. |

| Control procedures: | |
|---|---|
| | Applicable control procedures where a CA is terminated |
| 1 | There shall be a termination plan established at the initiation of the CA which allocates responsibilities for overseeing the termination of the CA. The termination plan should include termination of any relationships with other CAs. The termination plan should be reviewed on a regular basis. |
| 2 | Address the termination of any back-up site used for business resumption. |
| 3 | The CA’s public key and certificate should be escrowed if appropriate. |
| 4 | The termination plan should include provisions for maintaining revocation status information |
| 5 | Develop a termination plan to minimize disruption, including notification to subscribers, preserving records, transferring business to a reliable successor. |
| 6 | The CA should retain the CA audit records for an appropriate time period, in line with contextual requirements. |
| 7 | The CA shall make certificate status information (including certificate revocation lists and other certificate status mechanisms) available to relevant entities (e.g. subscribers and relying parties or their agents, i.e. CVSPs) using mechanism in accordance with the CP. |

| | |
|---|---|
| 8 | The CA shall have a plan for the case of business termination, including at least:<br>a) the revocation service and further issuance of revocation information as appropriate;<br>b) the handling of the private keys of the CA;<br>c) if applicable, the handling of private keys of subscribers stored in the environment of the CA, if applicable;<br>d) if applicable, agreements with successor instances prior to the CA's termination;<br>e) financial arrangements (e.g. insurance) to pay for the costs to fulfil any remaining obligations in case of business termination. |
| 9 | The CA shall inform all stakeholders prior to its business termination. |
| 10 | Any restricted information that is no longer needed (e.g. for technical or regulatory reasons) shall be destroyed without undue delay after the CA business termination. |

## 7.16 Root CA controls

This subclause contains specific controls regarding root CAs. General controls concerning CAs, which also include root CAs, are shown in 7.6 to 7.13, and are not duplicated in this subclause.

### 7.16.1 Physical and environmental security

| **Control objective:** |
|---|
| To provide reasonable assurance depending on the complexity of the PKI environment that:<br>— Root CA private keys are held and used physically isolated from normal operations,<br>— Physical barriers are in place (e.g. Faraday cage) to prevent electromagnetic radiation emissions for all root CA operations as specified in the CP or CPS. |

| **Control procedures:** | |
|---|---|
| | Root CA physical security |
| 1 | See 7.6 for physical and environmental security controls. |
| 2 | If security cameras are used, then the security camera video retention policy should be set to an appropriate period. |
| 3 | A separation of duties policy shall be defined. |
| | Equipment |
| 4 | See 7.6 for equipment controls. |

### 7.16.2 Operations security

| **Control objective:** |
|---|
| To provide assurance that:<br>— correct and secure operation of root CA information processing facilities is ensured;<br>— the risk of root CA systems failure is minimized;<br>— the integrity of root CA systems and information is protected against malware;<br>— any damage from security incidents and malfunctions is minimized;<br>— incident reporting and response procedures are established and maintained. |

| Control procedures: | |
|---|---|
| 1 | See 7.7 Operations security. |
| 2 | Antivirus and Anti-malware software should be used for protecting against malware where appropriate. |
| 3 | Behavioural analytics tools shall be used in order to automatically determine activities that deviate from the normal. |
| 4 | Root CA systems shall require a dedicated (isolated) computing environment. |

### 7.16.3 Access control

| Control objective: | |
|---|---|
| — | To provide assurance that root CA system access is limited to authorized individuals; |
| — | To limit operating system access to authorized individuals with predetermined task privileges; |
| — | To limit access to network segments housing root CA systems to authorized individuals, applications, and services; |
| — | To limit root CA application use to authorized individuals. |

| Control procedures: | |
|---|---|
| 1 | See 7.8 Access control. |
| | Network access control |
| 2 | Root CA system shall reside in a high security zone and is isolated from other networks. |

### 7.16.4 Root CA key generation

| Control objective: |
|---|
| To provide assurance that root CA key pairs are generated in accordance with defined root CA key generation ceremony scripts and the requirements of the CP. |

| Control procedures: | |
|---|---|
| 1 | See 7.13.1 CA key generation. |
| 2 | Generation and use of root CA keys shall occur within a secure cryptographic device meeting the appropriate ISO/IEC 19790 (FIPS 140-2) or ISO/IEC 15408 (with an appropriate protection profile or security target) and the business requirements in accordance with the CPS. |
| 3 | There shall be a documented procedure for conducting root CA key pair generation. |
| 4 | The root CA shall test the procedure for conducting root CA key pair generation before live operation. |
| 5 | The root CA key shall have a key length that is appropriate for the algorithm and for the validity period of the CA certificate as disclosed in the CA's CP or CPS. |
| 6 | The root CA shall have a key size in accordance with the CA's CP or CPS. |
| 7 | Root CA key generation ceremonies shall be independently witnessed by internal and/or external auditors. |

### 7.16.5 Generation of root CA keys script requirements

| Control objective: |
|---|
| To ensure that a root CA key generation script is used to generate root CA keys |

| Control procedures: | |
|---|---|
| 1 | The root CA shall define and assign participant roles and responsibilities. |
| 2 | The root CA shall obtain management approval for conduct of the root key generation ceremony. |
| 3 | The root CA shall specific cryptographic hardware, software and other materials including identifying information. |
| 4 | The root CA shall perform specific steps during the key generation ceremony including;<br>a) hardware preparation;<br>b) verification of the integrity of the operating system and other software from its source (e.g. using hash totals). |
| 5 | The root CA shall specify physical security requirements for the ceremony location (e.g. barriers, access controls and logging controls). |
| 6 | The root CA shall produce procedures for secure storage of cryptographic hardware and activation materials following the key generation. |
| 7 | The root CA shall obtain sign-off on the script or in a log from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script. |
| 8 | The participants shall note any deviations from the key generation ceremony script (e.g. documentation of steps taken to address any technical issues) and provide this to CA management. |
| 9 | The root CA shall ensure that the integrity of the hardware/software used for key generation and the interfaces to the hardware/software is tested before production usage. |

### 7.16.6 Root CA public key distribution

| Control objective: |
|---|
| To ensure controls are maintained to provide reasonable assurance that the integrity and authenticity of the root CA public key and any associated parameters are maintained during initial and subsequent distribution. |

| Control procedures: | |
|---|---|
| 1 | See 7.13.3 CA Public key distribution. |
| 2 | Where a self-signed certificate is used for the root CA public key distribution process, the root CA shall provide a mechanism to verify the authenticity of the self-signed certificate (e.g. publication of the certificate's fingerprint). |

### 7.16.7 Root CA key compromise

| Control objective: |
|---|
| Controls shall be maintained to provide reasonable assurance that continuity of operations is maintained in the event of the compromise of the root CA's private keys. |

| Control procedures: | |
|---|---|
| 1 | See 7.13.6 CA Key compromise. |
| 2 | Compromise of the root CA key shall be addressed by the disaster recovery plan under 7.10. |
| 3 | A root CA key destruction script shall be produced to ensure the root CA is destroyed securely, see 7.13.5. |

## 7.17 CA certificate life cycle management controls – subordinate CA certificate

| Control objectives: - |
|---|
| To provide reasonable assurance that subordinate CAs operate securely and in line with applicable CPs and the CPS. |

| Control procedures: | |
|---|---|
| | Subordinate CA (sub-CA) registration |
| 1 | Subordinate CA certificate requests shall be accurate, authenticated and approved in accordance with the applicable CPs or CPS. |
| 2 | Subordinate CA certificate replacement (renewal and rekey) requests shall be accurate, authorized, and complete in accordance with the applicable CPs or CPS. |
| 3 | New, renewed, and rekeyed subordinate CA certificates shall be generated and issued in accordance with the applicable CPs or CPS. |
| 4 | Upon issuance, complete and accurate subordinate CA certificates shall be made available to relevant entities (subscribers and relying parties) in accordance with the applicable CP(s) or CPS. |
| 5 | Subordinate CA certificates shall be revoked based on authorized and validated certificate revocation requests. |
| 6 | Timely, complete, and accurate certificate status information (including CRLs and other certificate status mechanisms) shall be made available to any entity in accordance with the applicable CP(s) or CPS. |

# Annex A
(informative)

# Management by certificate policy

## A.1 Purpose of certificate policies

This annex describes certificate policies and identifies how they can be implemented to effectively manage the risks of parties in a PKI with its focus on a contractual environment. This annex draws on IETF RFC 3647[4] and provides further clarification on the use of certificate policies in an organisations' environment.

Certificate policies play a critical role in the administration of trusted transactions. The main purpose of a CP is to enable the relying party to determine whether the certificate and its underlying conditions are acceptable for a given transaction. Equally, the subscriber has clear guidance upon where they can use their private key to sign transactions and place reliance on the certification service to support it.

## A.2 Definition of a certificate policy

A CP is a unique named set of rules which describes the applicability of a certificate within a specified community or class of application. A CP acts as a record of permitted usage and associated provisions in terms of respective obligations, including liability and governance, between all involved parties. A certificate policy is published under the responsibility of a policy authority.

The CP should be used by various users of the certificate to decide whether or not to accept the binding between the subject (of the certificate) and the public key. The CP is represented by a registered object identifier (OID) in the X.509 v3 certificate.

The CP object identifier can be included in the following extensions in the X.509 v3 certificates: certificate policies, policy mappings and policy constraints. The object identifier(s) can appear in none, some, or all of these fields. The certificate policy can also be retrieved using a URL which can be identified in the certificate policies extension.

The policy authority or its agents can provide signed paper copies of the certificate policy to potential subscribers as a form of contractual binding or to relying parties. Relying parties on the other hand can use electronic links to locate the certificate policy. A CVSP can supply a service to relying parties to validate certificates as well as the applicability of the associated certificate policy.

## A.3 Establishing policies in certificates

OIDs are used to unambiguously identify certificate policies and policy qualifiers so that they can be processed by automated means in certificate-using applications and systems. These policies and policy qualifiers are listed in the certificate policies certificate extension by the issuing CA and are defined as:

```
certificatePolicies EXTENSION:: = {    SYNTAX
CertificatePoliciesSyntax
   IDENTIFIED BY  id-ce-certificatePolicies

}
In the certificatePolicies certificate extension, the object identifier
id-ce-certificatePolicies identifies a value of ASN.1 type
CertificatePoliciesSyntax, which is defined as:
CertificatePoliciesSyntax:: = SEQUENCE SIZE(1..MAX) OF PolicyInformation
PolicyInformation:: = SEQUENCE {    policyIdentifier  CertPolicyId,
policyQualifiers   OPTIONAL
}

CertPolicyId:: = OBJECT IDENTIFIER

PolicyQualifiers:: = SEQUENCE SIZE(1..MAX) OF PolicyQualifierInfo
```

When a **certificatePolicies** certificate extension is present in a certificate, it shall have at least one value of type **PolicyInformation**. Each instance of type **PolicyInformation** should contain a value of type **CertPolicyId**, an object identifier that identifies a CP. The **policyQualifiers** component of **PolicyInformation** lists the policy qualifiers associated with a given CP. This component is optional and need not be included.

The certificate policies listed in a **certificatePolicies** certificate extension are those that are recognized by the issuing CA as being applicable to that certificate. This policy information can be used by a relying party to determine the appropriate use of the key pair certified by the CA. A relying party can require a particular policy to be present in this extension before it accepts the certificate as valid for a particular use. Typically, a CP can be associated with a set of application programs which can be used by the owner of the certified key only when the CP is present.

A relying party or computer application can require that a specific policy be present in order to use the certificate. Policy qualifiers can, at the option of the relying party, be processed, or ignored.

When CP qualifiers are associated with a given CP, the optional **policyQualifiers** component of type **PolicyInformation** is present and contains at least one CP qualifier, a value of type **PolicyQualifierInfo** defined as:

```
PolicyQualifierInfo:: = SEQUENCE {    policyQualifierId  CERT-POLICY-
QUALIFIER.&id({SupportedPolicyQualifiers}),    qualifier          CERT-
POLICY-QUALIFIER.&Qualifier(
                          {SupportedPolicyQualifiers}
{@policyQualifierId})  OPTIONAL
}

SupportedPolicyQualifiers CERT-POLICY-QUALIFIER:: = { ... }
Type PolicyQualifierInfo is composed of two components, policyQualifierId and qualifier,
which are specified in terms of the &id and &Qualifier fields of the information object
class CERT-POLICY-QUALIFIER. This class is defined as:
CERT-POLICY-QUALIFIER:: = CLASS {
   &id          OBJECT IDENTIFIER UNIQUE,
   &Qualifier   OPTIONAL
}
  WITH SYNTAX { POLICY-QUALIFIER-ID &id [QUALIFIER-TYPE &Qualifier] }
```

The **policyQualifierId** component of **PolicyQualifierInfo** is defined in terms of the **&id** field and shall contain an object identifier value. The optional **qualifier** component is defined in terms of the **&Qualifier** field and can contain the value of any ASN.1 type.

A value of the **PolicyInformation** type identifies and conveys qualifier information for one CP. The component **policyIdentifier** contains an identifier of a CP and the component **policyQualifiers** contains policy qualifier values for that element.

## A.4 Certificate applicability under a named certificate policy

Once parties are able to identify and locate the CP relating to a certificate, the user should be able to determine what a certificate can be used for and any constraints. Policy authorities have the option of asking CAs to either:

a) issue one certificate with restricted association to one specific CP; or

b) allow one certificate to be associated with many CPs.

There are several issues here that require discussion. This is considered against the background of the following basic assumptions:

- Certificate policies are customer oriented in that certificates provide a control mechanism to help manage risks related to services provided to customers.
- Certificate policies and the applicability of a certificate need to be recognized by all parties including the issuer, the subscriber, the relying party and possibly the relying party's validation service provider.
- In the emerging trust services marketplace, it appears that there will be a proliferation of certificates by various trust service providers. The variety of naming conventions, in combination with the proliferation of certificates, can create confusion for an 'uneducated' consumer base as to which certificate to use for a particular application.

While customer knowledge on the management of certificates requires enhancing, and it can be argued that certificates should be transparent to some users, organisations can consider one-to-one as a prudent strategy initially. This will minimize confusion and facilitate learning on the part of the end user over a longer period to allow for familiarization and to allow time for software applications to handle multiple certificates more effectively.

One certificate with one CP will also minimize the level of consumer education for "how and why" a certificate can be used for particular applications. It is also essential that certificate policies are written in such a way that they are "customer friendly," unambiguous and clear in terms of responsibilities and liabilities. These are the terms and conditions for the subscriber's use of the certificate and should be clearly understood by them. Additionally, the relying party or their trust services provider will have definitive information as to which CP applies to the certificate presented. Unless this is stated explicitly in the transaction or predetermined, there should be a reliable mechanism to determine which is the applicable CP.

Additionally, for cross-certification it will be essential to have clarity regarding which CP applies to extend the use of a certificate. The one CP for one certificate strategy will minimize the technical, organizational, and operational requirements of cross-certification.

Some PKI domains restrict the use of the certificate policy extension. For example, the CA Browser Forum prohibits the use of the certificatePolicies extension in root CA certificates and provides explicit OIDs in its baseline requirements and for extended validation (EV) Certificates.

See https://cabforum.org for further information.

## A.5 Cross-certification, certificate chains, policy mapping and certificate policies

### A.5.1 Cross-certification

Cross-certification is the reciprocal certification process of certificate policies issued by two or more different policy authorities. Cross-certification enables the reciprocal use of the certificates owned by different policy authorities.

Cross-certification increases the usage and acceptability range of the subscriber's certificate under a given CP. Cross-certification requires a degree of conformity or equivalence in terms of interoperability of policy between the policy authorities and the controls implemented by the issuing CAs.

### A.5.2 Certificate chains

When validating the acceptability of a certificate it can be necessary to not only validate the entire sequence of certificates from the end entity using the certificate up to the root certificate, but also their respective certificates policies.

An acceptable policy identifier is the identifier of the CP required by the user of the certification path or the identifier of a policy that has been declared equivalent to it through policy mapping (see A.5.3).

It is recommended that the certificate policies extension be implemented as a critical extension. This field is processed in concert with the policyConstraints extension (see A.5.4) during the certification path validation, as described in ITU-T X.509 v3.

### A.5.3 Certificate policy mapping

This extension allows the policy authority, through its certificate issuers, to indicate that one or more of its certificate policies is considered equivalent to another CP used in that domain. The assignment of CP mappings is restricted to the policy authority and certification authority and can be further inhibited through the policyConstraints extension. This extension will support cross-certification by specifying the OIDs of equivalent certificate policies.

The syntax of this extension is:

```
policyMappings EXTENSION:: = {
   SYNTAX          PolicyMappingsSyntax
   IDENTIFIED BY   id-ce-policyMappings }
PolicyMappingsSyntax:: = SEQUENCE SIZE (1..MAX) OF SEQUENCE {
issuerDomainPolicy     CertPolicyId,
   subjectDomainPolicy    CertPolicyId }
```

This extension can, at the discretion of the certificate issuer and as stated in the CP, be either critical or non-critical.

CAs should generate this extension for CA digital signature certificates where policy mapping is applicable and include a combination of issuerDomainPolicy field(s) and subjectDomainPolicy field(s) with the applicable CertPolicyId field(s).

Relying parties should interpret the combination(s) of issuerDomainPolicy and subjectDomainPolicy CP object identifiers as equivalent.

### A.5.4 Policy constraints

The policy constraints extension supports two optional features. The first is the ability for a certification authority to require that explicit CP indications be present in all subsequent certificates in a certification path. Certificates at the start of a certification path can be considered by a certificate user to be part of a trusted domain (i.e. certification authorities are trusted for all purposes, so no particular CP is needed in the certificate policies extension). Such certificates need not contain explicit indications of CP. However, when a certification authority in the trusted domain certifies outside the domain, it can activate the requirement for explicit CP in subsequent certificates in the certification path. When used, the requireExplicitPolicy constraint requires that all certificates include an acceptable policy, not just those that follow the certificate that asserts the requirement.

The other optional feature in the policy constraints field is the ability for a certification authority to disable policy mapping by subsequent certification authorities in a certification path. It can be prudent to disable policy mapping when certifying outside the domain. This can assist in controlling risks due to transitive trust (e.g. a domain A trusts domain B, domain B trusts domain C, but domain A does not want to be forced to trust domain C).

The syntax of this extension is:

```
policyConstraints EXTENSION:: = {
   SYNTAX          PolicyConstraintsSyntax
   IDENTIFIED BY   id-ce-policyConstraints } PolicyConstraintsSyntax:: = SEQUENCE {
   requireExplicitPolicy     [0] SkipCerts OPTIONAL,
inhibitPolicyMapping       [1] SkipCerts OPTIONAL } SkipCerts:: = INTEGER (0..MAX)
```

This extension should be flagged critical.

## A.6 Certificate classes and naming

The use of certificate classes can be to distinguish between the different level of assurance and for describing specific third-party obligations for issuing, managing, suspending, and revoking certificates. Each level or class of certificate provides specific functionality and security features.

A critical issue for the relying party and to a degree the subscriber is ascertaining the level of assurance a particular certificate provides issued under a CP.

The identified options for policy authorities include the following.

- CP classifications based upon arbitrary values, such as bronze, silver, gold: it should be noted that this would make it difficult to provide any linear measure of the specific security service capability. Differences between classes can be multidimensional and can contain distinct attributes that are not precisely comparable to other classes. The use of certificate class names is perceived to have a "relative value" for their use and functionality.
- CP classifications based on recognized standards for contractual environment: for the end user the use of these certificate classes projects an "absolute value" on the type of security and liability issues associated with their usage.

The following assumptions also require consideration by policy authorities:

- Digital certificates can represent familiar brand names in the electronic marketplace.
- Consumer and business confidence are a measure of the recognition of brand(s) attached to security products and services, including the level of functionality and applicability of a certificate.
- Other naming conventions can be used which have no implicit value (e.g. 1, 2, 3) and concentrate on establishing usage differences rather than relative merit. However, it seems unlikely that these would be deemed appropriate to engender trust.
- The use of standards serves as a universally understood benchmark. However, care needs to be exercised on level of prescription to avoid placing any restriction on usage.

Certificate classifications based on absolute values such as low, medium, and high cannot project the type of image that organisations require for the development of electronically based trust services.

To promote wider acceptability and possibly reduce the level of end-user confusion for certificate usage, the recommendation is for certificate policies to conform with standards that are recognized, or specifications agreed upon by all the parties in the contractual environment.

## A.7 Certificate policy provisions

### A.7.1 General

This subclause briefly describes the terms of a CP.

### A.7.2 Interpretation

The CP should outline in its preamble what the CP is for in terms of service provision, the preconditions for the community and the relating legally binding contractual conditions. This can also include any regulatory requirements that are applicable to the community and use of the certificates under the CP.

This subclause should describe the intended community for the certificates and where appropriate their intended usage (e.g. whether the certificate can be used for remote authentication purposes, digital signing, or data confidentiality). It can also state any requirements for membership of the community (e.g. certificates may be issued to private account holders only, relying parties should have signed a relying party agreement with an approved or licensed entity as approved by the policy authority).