INTERNATIONAL STANDARD

ISO 21188

Second edition
2018-04

Public key infrastructure for financial services — Practices and policy framework

Infrastructure de clé publique pour services financiers — Pratique et cadre politique

Reference number
ISO 21188:2018(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

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

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO 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).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security*.

This second edition cancels and replaces the first edition, ISO 21188:2006, which has been technically revised, and incorporates ISO 15782-1:2009 and ISO 15782-2:2001.

The main changes to the previous edition are:

— Clause 2, ISO/IEC 7811 removed as it is a standard for magnetic stripes;

— 3.21, 'hold' removed from definition of 'certification authority';

— 7.3.6 and D.4, references to ISO 15782-1, Annex J removed;

— 7.4.1, "be performed by authorized personnel" changed to "be performed in a process initiated by authorized personnel";

— all instances of 'shall', 'should' and 'may' checked and updated if necessary;

— paragraph added to 5.4:

'Two or more CAs can join a common scheme for mutual recognition, e.g. implemented by a trust list. Certificates issued by one CA can then be validated by relying parties who are customers of another CA belonging to the scheme.';

— control added to 7.2.2:

'Responsible management of the CA should be able to demonstrate that the information security policy is implemented and adhered to.';

— proposal added to 7.2.2:

'Procedures should exist to carry out a risk assessment to identify, analyse and evaluate 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.';

— general editorial changes.

Introduction

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

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

The ubiquitous use of online services in public networks by the financial industry and the needs of the industry in general to provide safe, private and reliable financial 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 financial 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 compliance to standard practices can be ascertained.

Applications serving the financial services 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.

Members of ISO/TC 68 have made a commitment to public key technology by developing technical standards and guidelines for digital signatures, key management, certificate management and data encryption. This document provides a framework for managing a PKI through certificate policies, certification practice statements, control objectives and supporting procedures. For implementers of this document, the degree to which any entity in a financial transaction can rely on the implementation of public key infrastructure standards and the extent of interoperability between PKI-based systems using this document will depend partly on factors relative to policy and practices defined in this document.

Public key infrastructure for financial services — Practices and policy framework

1 Scope

This document sets out a framework of requirements to manage a PKI through certificate policies and certification practice statements and to enable the use of public key certificates in the financial services industry. It also defines control objectives and supporting procedures to manage risks. While this document addresses the generation of public key certificates that might be used for digital signatures or key establishment, it does not address authentication methods, non-repudiation requirements or key management protocols.

This document draws a distinction between PKI systems used in closed, open and contractual environments. It further defines the operational practices relative to financial-services-industry-accepted information systems control objectives. This document is intended to help implementers to define PKI practices that can support multiple certificate policies that include the use of digital signature, remote authentication, key exchange and data encryption.

This document facilitates the implementation of operational, baseline PKI control practices that satisfy the requirements for the financial services industry in a contractual environment. While the focus of this document is on the contractual environment, application of this document to other environments is not specifically precluded. For the purposes of this document, the term "certificate" refers to public key certificates. Attribute certificates are outside the scope of this document

This document is targeted for several audiences with different needs and therefore the use of this document will have a different focus for each.

Business managers and analysts are those who require information regarding using PKI technology in their evolving businesses (e.g. electronic commerce); see Clauses 1 to 6.

Technical designers and implementers are those who are writing their certificate policies and certification practice statement(s); see Clauses 6 to 7 and Annexes A to G.

Operational management and auditors are those who are responsible for day-to-day operations of the PKI and validating compliance to this document; see Clauses 6 to 7.

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 — The Directory — Part 8: Public-key and attribute certificate frameworks*

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

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

ISO/IEC 18032, *Information technology — Security techniques — Prime number generation*

ISO/IEC 18033-1, *Information technology — Security techniques — Encryption algorithms — Part 1: General*

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

ISO/IEC 18033-3, *Information technology — Security techniques — Encryption algorithms — Part 3: Block ciphers*

ISO/IEC 18033-4, *Information technology — Security techniques — Encryption algorithms — Part 4: Stream ciphers*

3 Terms and definitions

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

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

— ISO Online browsing platform: available at https://www.iso.org/obp/3.1

— IEC Electropedia: available at http://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
authentication
provision of assurance that a claimed identity of an entity is correct

Note 1 to entry: 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; b) during use, the act of comparing electronically submitted identity and credentials (i.e. user ID and password) with stored values to prove identity.

3.4
authentication data
information used to verify the claimed identity of an entity, such as an individual, defined role, corporation or institution

3.5
CA certificate
public key certificate whose subject is a CA (3.21) and whose associated private key is used to sign certificates and other CA related information (e.g. CRL, OCSP responses)

3.6
card bureau
agent of the *CA* (3.21) or *RA* (3.49) that personalizes an *ICC* (3.35) containing the subscriber's private key (as a minimum)

3.7
cardholder
subject to whom the integrated circuit card containing private and public key pair and *certificates* (3.8) has been issued

3.8
certificate
public key and identity of an entity (*authentication data* (3.4)), together with some other information, rendered unforgeable by signing the certificate information with the private key of the certifying authority that issued that public key certificate

3.9
certificate suspension
certificate hold
suspension of the validity of a *certificate* (3.8)

3.10
certificate issuer
organization whose name appears in the issuer field of a *certificate* (3.8)

3.11
certificate management
management of public key certificates covering the complete life cycle from the initialization phase to the issuing phase to the cancellation phase

3.12
certificate manufacturer
agent who performs the tasks of applying a digital signature to a certificate signing request on behalf of the *certificate issuer* (3.10)

3.13
certificate policy
CP
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

3.14
certificate profile
specification of the required format (including requirements for the usage of standard fields and extensions) for a particular type of *certificate* (3.8)

3.15
certificate rekey
process whereby an entity with an existing key pair and *certificate* (3.8) receives a new certificate for a new public key, following the generation of a new key pair

3.16
certificate renewal
rollover
issuing an entity with a new version of an existing certificate with a new validity period

3.17
certificate revocation list
CRL
list of revoked *certificates* (3.8)

3.18
certificate validation service
service provided by the *CA* (3.21) or its agent which performs the task of confirming the validity of a *certificate* (3.8) to a *relying party* (3.52)

3.19
certificate validation service provider
CVSP
entity (3.32) that provides certificate validation services to its relying party customers

3.20
certification
creation of a public key certificate for a *subject* (3.58)

3.21
certification authority
CA
entity (3.32) trusted by one or more entities to create, assign and revoke public key certificates

3.22
certification path
ordered sequence of certificates of entities which, together with the public key of the initial entity in the path, can be processed to obtain the public key of the final entity in the path

3.23
certification practice statement
CPS
statement of the practices which a *certification authority* (3.21) employs in issuing, managing, revoking and renewing 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

3.24
certification request
submission of a validated registration request by an *RA* (3.49), its agent or a subject to a *CA* (3.21) to register a subject's public key to be placed in a *certificate* (3.8)

3.25
certification response
message sent, following certification, from a *CA* (3.21) in response to a certificate request

3.26
certificate validity
validity
applicability (fitness for intended use) and status (valid, unknown, revoked or expired) of a *certificate* (3.8)

3.27
compromise
violation of the security of a system such that an unauthorized disclosure modification or falsification of sensitive information can have occurred

3.28
cross certification
mutual certification of each other's public keys by two *CAs* (3.21)

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

3.29
cryptographic hardware
cryptographic device
hardware security module
hardware cryptographic module
hardware which provides a set of secure cryptographic services, e.g. key generation, cryptogram creation, PIN translation and certificate signing

3.30
digital signature
cryptographic transformation that, when associated with a data unit, provides the services of origin authenticity data integrity and signer non-repudiation

3.31
end entity
certificate subject that uses its private key for purposes other than signing certificates

3.32
entity
person, partnership, organization or business that has a legal and separately identifiable existence

EXAMPLE A legal entity or an individual or *end entity* (3.31), such as *certification authority* (3.21), *registration authority* (3.49) or *end entity* (3.31).

3.33
audit journal
audit log
event journal
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

3.34
functional testing
portion of security testing in which the advertised features of a system are tested for correct operation

3.35
integrated circuit card
ICC
card into which has been inserted one or more electronic components in the form of microcircuits to perform processing and memory functions

3.36
issuing CA
CA (3.21) that issued the certificate in the context of a particular *certificate* (3.8)

3.37
key escrow
management function that allows access by an authorized party to a replicated private encipherment key

3.38
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

3.39
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

3.40
object identifier
OID
unique series of integers that unambiguously identifies an information object

3.41
online certificate status mechanism
mechanism that allows *relying parties* (3.52) to request and obtain certificate status information without requiring the use of *CRLs* (3.17)

3.42
online certificate status protocol
OCSP
protocol for determining the current status of a certificate in lieu of or as a supplement to checking against a periodic *CRL* (3.17) 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

3.43
operating period
period of a certificate beginning on the date and time it is issued by a *CA* (3.21) (or on a later date and time, if stated in the certificate), and ending on the date and time it expires or is revoked

3.44
PKI disclosure statement
document that supplements a *CP* (3.13) or *CPS* (3.23) by disclosing critical information about the policies and practices of a *CA* (3.21)/*PKI* (3.48)

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

3.45
policy authority
PA
party or body with final authority and responsibility for specifying *certificate policies* (3.13) and ensuring *CA* (3.21) practices and controls as defined by the *CPS* (3.23) fully support the specified certificate policies

3.46
policy mapping
recognition that when a *CA* (3.21) in one domain certifies a *CA* in another domain, a particular *certificate policy* (3.13) 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: See *cross certification* (3.28).

3.47
policy qualifier
policy-dependent information that accompanies a *certificate policy* (3.13) identifier in an X.509 certificate

3.48
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, and/or for message encryption key exchange or negotiation

3.49
registration authority
RA
entity whose primary functional role and responsibilities include identity validation of the subject for approving *certificate requests* (3.24) submitted to a *CA* (3.21)

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.

3.50
registration request
submission by an entity to an *RA* (3.49) (or *CA* (3.21)) to register the entity's public key in a certificate

3.51
registration response
message sent by an *RA* (3.49) (or *CA* (3.21)) to an entity in response to a registration request

3.52
relying party
RP
recipient of a certificate who acts in reliance on that certificate, digital signatures verified using that certificate, or both

3.53
relying party agreement
RPA
legally binding statement provided by the *CA* (3.21) of the expected responsibilities between the relying party, the subject and the CA

Note 1 to entry: The RPA might be included in the *CPS* (3.23) or provided as one or more external documents.

3.54
repository
system for storage and distribution of certificates and related information

EXAMPLE Certificate storage, certificate distribution, *certificate policy* (3.13) storage and retrieval, certificate status.

3.55
root CA
trust anchor
CA (3.21) at the apex of the *CA* hierarchy

3.56
signature validation
verification and confirmation that a digital signature is valid

Note 1 to entry: See also *certificate validity* (3.26).

3.57
signature verification
check of the cryptographic value of a signature using data

3.58
subject
entity that owns the asymmetric key pair and may also be a *relying party* (3.52)

3.59
subject CA
CA (3.21) that is certified by the *issuing CA* (3.36) and hence complies with the *certificate policy* (3.13) of the issuing CA

3.60
subordinate CA
sub-CA
intermediate CA
CA (3.21) that is lower relative to another CA in the CA hierarchy

3.61
subscriber
entity subscribing with a *certification authority* (3.21) on behalf of one or more subjects

3.62
superior CA
CA (3.21) that is higher relative to another *subordinate CA* (3.60) in the CA hierarchy, but is not a *root CA* (3.55)

3.63
tamper-evident
provides evidence that an attack has been attempted

3.64
tamper-resistant
provides passive physical protection against an attack

3.65
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* (3.21)

3.66
trust services provider
TSP
approved organization (as determined by the contractual participants) providing trust services, through a number of *certification authorities* (3.21), to their customers who may act as subscribers or *relying parties* (3.52)

Note 1 to entry: A trust services provider can also provide certificate validation services.

3.67
validation service request
enquiry by the *relying party* (3.52) to a validation service to check the validity of a *certificate* (3.8)

4 Abbreviated terms

ASN.1	Abstract Syntax Notation One
CA	certification authority
CM	certificate manufacturer
CP	certificate policy
CPS	certification practice statement
CRL	certificate revocation list
CVSP	certificate validation service provider
EMV	Eurocard MasterCard Visa
CPS	certification practice statement
FI	financial institution
FIPS	Federal Information Processing Standard
FQDN	fully qualified domain name
FTP	file transfer protocol
HSM	hardware security module

HTTP	hypertext transfer protocol
ICC	integrated circuit card
ID	identifier
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
MAC	message authentication code
MITM	man-in-the-middle attack
OCSP	online certificate status protocol
OID	object identifier
PA	policy authority
PIN	personal identification number
PKI	public key infrastructure
PKIX	Public Key Infrastructure (X.509) (IETF Working Group)
RA	registration authority
RFC	request for comment
RP	relying party
SAN	storage area network
TLS	transport layer security
TSA	time stamping authority
TSP	trust services provider
URL	uniform resource locator
UTC	universal time coordinated (zulu or Greenwich Mean Time, Time GMT)

5 Public key infrastructure (PKI)

5.1 General

Before addressing the details of PKI policy and practices requirements, this document provides some background information in order for the reader 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 financial institutions 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.

PKIs are a practical technical solution to the problems posed by open networks. Financial institutions are becoming trust services providers (TSPs), to take advantage of the growing market for security and authentication in online communications. 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 or a validation 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 certificate validation. Within a financial institution, 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 protects 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.

Financial institutions may use a PKI to service their business needs in the following environments, depending upon their relationship with the relying party. Examples of each are provided in Tables 1 to 3.

a) **Closed environment**: all entities (certificate subjects and relying parties) adhere to a single financial institution's trust service, and shall share at least one certificate policy. See Figure 1 and Table 1. 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 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 2 and Table 2.

c) **Open environment**: the financial institution 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. See Figures 3 and 4 and Table 3.

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

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;

— certification;

— distribution;

— usage;

— expiry;

— renewal;

— rekey;

— revocation management;

— revocation status checking.

5.3 Business requirement impact on PKI environment

5.3.1 General

This clause uses business scenarios to illustrate the key differences between the closed, open and contractual environments. Tables 1 to 3 describe typical business scenarios, sample (security) requirements, and the associated PKI operations that would be performed if PKI was utilized to address the requirements.

5.3.2 Illustration of certificate application in a closed environment

This subclause describes several scenarios where the financial institution can use PKI for internal purposes and to support its services and communications internally or to its customers.

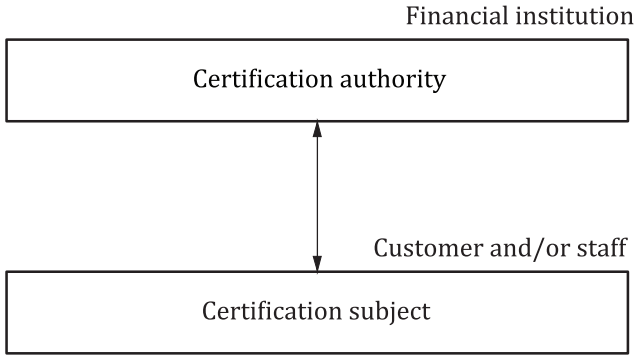

Figure 1 — Two entities in a closed environment

Table 1 — Certificate application scenarios in a closed environment

	Typical scenarios	Sample requirements	PKI operations
1	The financial institution (FI) sends an email to a customer (e.g. notification of deposit rate change).	— Authentication of sender for recipient. — Message integrity for sender and recipient.	— Sender creates digital signature. — Recipient validates sender's certificate. — Recipient verifies digital signature.
2	Exchange of sensitive emails between employees contained within the FI's network boundaries.	— Authentication of sender for recipient.	— Recipient validates sender's certificate.
		— Message integrity for sender and recipient.	— Sender creates digital signature. — Recipient verifies digital signature.
		— Confidentiality protection for message contents.	— Sender fetches recipient's certificate from directory. — Sender encrypts message with recipient's public key. — Recipient decrypts message with recipient's private key.
3	The internal network distribution of the FI's software to customer facing devices (e.g. ATM software).	— Proof that the software that is being loaded into the device comes from an authentic source.	— FI digitally signs software applications. — Recipient verifies digital signature — Recipient validates FI's certificate.

5.3.3 Illustration of certificate application in a contractual PKI environment

This subclause describes the financial institution 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 might 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.

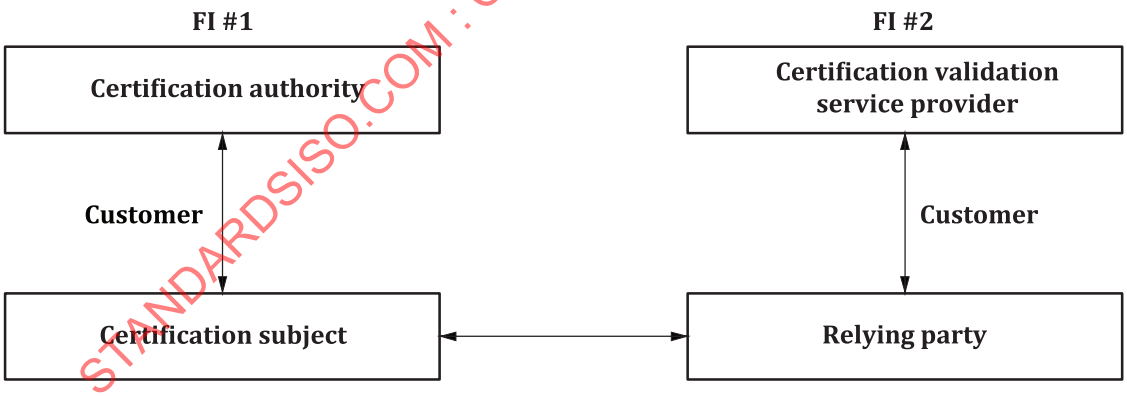

Figure 2 — Four entities in a contractual environment

Table 2 — Certificate application scenarios in a contractual environment

	Typical scenario	Sample requirements	PKI operations
1	FI employee sends an email via the Internet to a customer that uses another TSP.	— Authentication of sender for recipient.	— Recipient validates sender's certificate.
		— Message integrity.	— Customer checks digital signature.
		— Confidentiality protection for message contents.	— Sender fetches recipient's certificate from directory. — Sender encrypts message using recipient's public key. — Recipient decrypts message using recipient's private key.
2	Customer submits a purchase order to a merchant.	— Customer authorizes purchase order. — Authentication of customer by merchant. — Transaction message integrity.	— Customer digitally signs purchase order with private key.
			— Recipient validates sender's certificate.
			— Merchant verifies digital signature.
3	Customer receives invoice from merchant.	— Message authentication.	— Check digital signature and validate certificate.
4	An existing customer using an e-banking service to send high value payment instructions to FI.	— Strong mutual authentication. — Message integrity. — Confidentiality.	— Customer validates FI's server certificate. — FI validates customer's certificate.
			— FI verifies digital signature.
			— Customer fetches FI's certificate from directory. — Customer encrypts message using FI's public key. — FI decrypts message using FI's private key.
5	EMV purchase by a cardholder at point of sale.	— Authentication of ICC by terminal off-line.	— ICC creates digital signature. — Terminal checks ICC authenticity using ICC issuer public key certified by scheme CA.

5.3.4 Illustration of certificate application in an open environment

This subclause describes the financial institution's possible use of PKI to enable open external communication for itself, its own customers and external trading partners. The financial institution can offer trust services to its customers, such as "certificate validation service provider" or "certificate issuer.

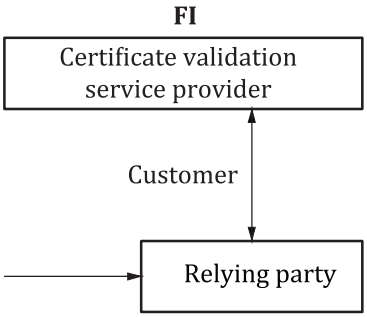

Figure 3 — FI acting as certificate validation service provider in an open environment

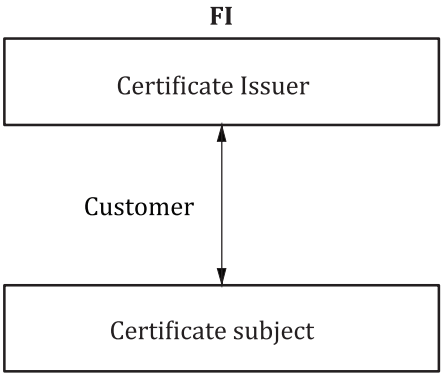

Figure 4 — FI acting as certificate issuer in an open environment

Table 3 — Certificate application scenarios in an open environment

	Scenario	Sample requirements	PKI operations
1	Website visitor downloads executable code while browsing a financial institution's website.	— Authentication of FI.	— User validates FI's certificate.
		— Integrity of FI executable code.	— User verifies FI's digital signature.
2	A customer visits an FI website.	— Authentication of an official FI website (i.e. not spoofed).	— User validates FI's server certificate.
3	Exchange of emails between two employees from different FIs via the Internet where there is no formal agreement in place.	— Authentication of sender for recipient.	— Each FI employee validates the sender's certificate.
		— Message integrity and non-repudiation proof.	— Each FI employee verifies digital signature.
		— Confidentiality protection for message contents.	— Each FI employee fetches recipient's certificate from directory.
4	An important electronic document (e.g. financial results) is published.	— Authentication of source and integrity of content.	— The user validates the FI's certificate. — The user verifies the digital signature.
5	Exchange of sensitive emails between two customers using different TSPs.	— Authentication of sender for recipient.	— Each customer validates the sender's certificate.
		— Message integrity.	— Each customer verifies the digital signature on the message received.
		— Confidentiality protection for message contents.	— Each customer fetches the recipient's certificate from the directory.

In these scenarios the users, FI employees or customers' certificates can be provided by the FI acting as certificate issuer, and whenever a user, FI employee or customer needs to validate a certificate, he or she can use a certificate validation service provided by the FI acting as CVSP.

5.4 Certification authority (CA)

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

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 an entity's public key and identity is validated by using the public key of one or more CAs. A CA can issue certificates to any entities, including CAs.

— 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 shall 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 is required by the relying party in order to validate a certificate. Given that the CA is a trusted entity, this permits the validation of the binding between an entity's public key, its identity and other needed information.

— In general, there are several PKI architectures that are available, including hierarchical, non-hierarchical and bridge. In a hierarchical architecture, authorities are arranged under a "root" CA that issues certificates to subordinate CAs. These subordinate CAs can issue certificates to CAs subordinate to them or to end entities. In a hierarchical architecture, the public key of the root CA functions as the trusted CA public key and is known to every entity. Any entity's certificate can be validated by validating the certification path of signature certificates that leads from the certificate being validated back to the trusted CA public key of the root CA. In this architecture, the root CA is a mutual point of trust for all entities.

— To communicate outside the root CA's domain, the root CA shall cross-certify 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 public key 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, a financial institution 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. Failure to provide compensating controls to deal with the possibility of compromise of transactions in a financial network can have catastrophic effects on financial institutions and their customers.

— Two or more CAs can join a common scheme for mutual recognition, e.g. implemented by a trust list. Certificates issued by one CA can then be validated by relying parties who are customers of another CA belonging to the scheme.

5.5 Business perspectives

5.5.1 General

A financial institution's future ability to participate in an online global economy depends on the existence of a trusted and secure environment in which to conduct business in the electronic medium.

The ideal goal of any financial institution is to establish a security infrastructure for an online marketplace that will allow it an opportunity to support internal security needs, to enhance and service its customer base as well as to enter new markets for the provision of trust services. In defining the business operations of the financial institution, 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 infrastructure.

5.5.3 Applicability

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

5.5.4 Legal issues

The legal perspective considers the public key 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.

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 and/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). Both parties shall 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 financial institution, 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 financial institutions 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 and/or by different certificate user communities). In addition, different CAs, with non-identical 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) Financial institutions that operate public or inter-organizational certification authorities shall 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 shall take 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.

Where interoperability is required or anticipated between PKIs operated by different CAs under different certificate policies, either:

— relying parties operating under one PKI shall accept policies used by its own CA and that of another CA;

or

— there shall be a recognized equivalence mapping from the policy used by the external CA to that used by the relying party's own CA; this equivalence mapping needs to be established by the relying party's CA to provide a one-way mapping to the external policy. However, in practice, mutual equivalence is established between CAs by bilateral agreement.

5.5.8 Audit journal requirements

5.5.8.1 General

CA systems shall keep audit journals that provide sufficient detail to reconstruct events and provide "due care" requirements. All entries in audit journals shall be marked with a precise time. The time used to record events as required in the audit log shall 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 shall be specified in the CA's certification practice statement.

CA audit journal entries shall 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, shall be recorded in the audit journals. Audit journals shall 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 F.

Audit journals shall be maintained in a form that prevents unauthorized modification or destruction. Automated audit journals shall be protected from modification or substitution. The use of a hash and a digital signature can be used. The private key pair used for signing the audit journal shall not be used for any other purpose. In addition, the audit journal shall only be retrieved by authorized individuals for valid business or security reasons.

Confidentiality and the need for access control to audit journal records shall be noted at all times.

5.5.8.2 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 shall 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 shall 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 shall 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.

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 shall be met by associated certificates used for a particular purpose. The CP also specifies the criteria that shall be agreed upon and complied with by a certification authority before certificates issued by such a certification authority may be accepted by a relying party. It is developed by a policy authority. The policy authority writing the CP can

range from a single business entity to a collection of entities such as a payment association established to interchange transactions between the member entities.

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.

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.

A CP shall be represented by a unique registered object identifier which needs to be recognized by members of the contractual environment. The PA that registers the object identifier also publishes a textual specification of the CP for examination by certificate users. (See Annex C for additional information.)

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

5.6.2 Certificate policy usage

Certificate policies are created for specific purposes within a PKI and business environment. There can be many certificate policies within one root hierarchy, each defining the business/policy requirements for groups of certificates sharing common policy requirements. In each case, the policy authority shall develop the specific certificate policy and ensure that the certificate practices statement of the certification authority creating the certificates adequately address the requirements of each certificate policy.

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

a) certificate policy for specific functional applications (e.g. server identification certificate for customer to authenticate their online banking 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 are commonly 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 Clause 6, 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 by definition shall use a self-signed certificate and can only be used to sign subordinate certificates. A subordinate CA shall be defined based upon geopolitical, organizational or other requirements. The subordinate CAs may cascade into multiple levels based upon multiple structural needs or it may issue certificates to end-entities.

In a hierarchy, the root shall be the most trusted point. Each subordinate level shares the trust between their peers, but each shall trust 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 5);

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 FI (certificates issued under Policy B in Figure 5).

In Figure 6, the policy authority issues the root policy and all subordinate policies within the hierarchy of trust.

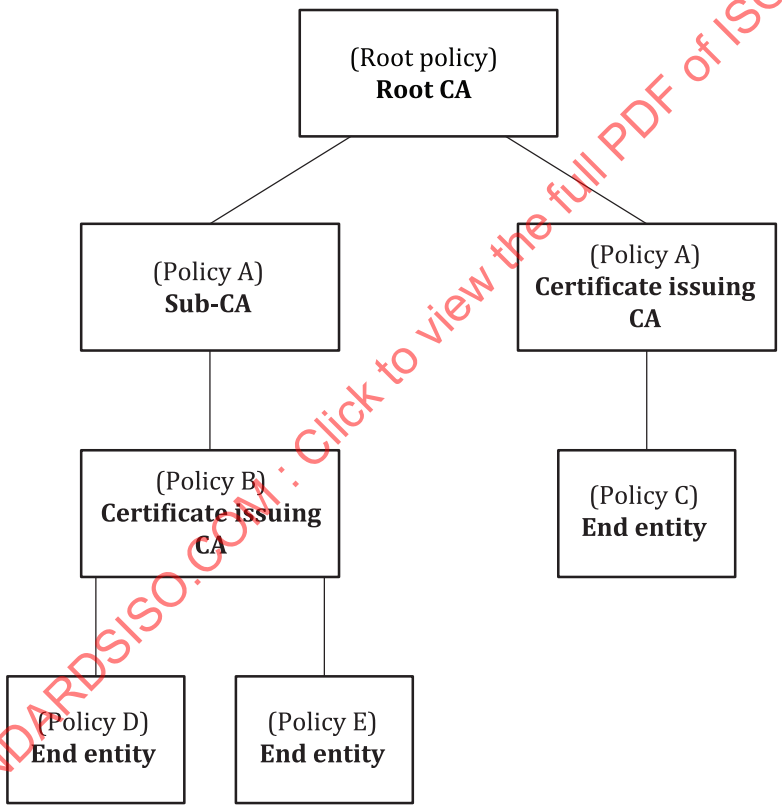

Figure 5 — Root hierarchy creates a hierarchy of trust

5.6.4 Certificate status

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

A certificate may be in one of the following states:

a) pre-valid – not operational;

b) live – operational;

c) suspended – not operational;

d) revoked – not operational;

e) expired – not operational.

Once a certificate is revoked or has expired it cannot return to an operational state. Once a revoked certificate has expired, it no longer needs to be on a CRL.

The policy authority shall specify 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 to meet the requirements of the certificate policies.

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 the outline provided in Annex B 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 five roles of 1) registration, 2) certificate manufacturer, 3) certificate issuer, 4) repository and 5) validation services. The CA is responsible for clearly defining the controls to accomplish these roles in meeting the requirements set forth in the CP. The controls are documented in the certification practice statement (CPS). The roles and functions of a CA can be securely delegated in any manner it desires, but all the roles and functions shall be completed and the CPS shall be written and maintained by the CA.

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 roles of the certificate policy and certification practice statement are illustrated in 5.7.3 and 5.7.6.

5.7.2 Authority

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 represent one financial institution or be shared by a number of major stakeholders. 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 is not compulsory in a contractual PKI environment and is often determined by either the rules of the community or the policy authority. In any event, the CA shall have documented its practices. While a simple compliance 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 is included by reference in the digital certificate. 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. In an open environment, the trusted service provider shall publicly disclose its certification practice statement through an online means that is available on a 24/7 basis.

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. The CP shall clearly identify the distribution policy of public, sensitive and confidential information both within the contractual environment and to appropriate external parties.

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. It is therefore by its nature a sensitive document which can be considered confidential. If the circulation of the CPS is restricted, financial institutions can use a PKI disclosure statement, indicating the type and nature of the controls without disclosing specific control details to support the CP. In an open environment, the trusted service provider shall publicly disclose its certification practice statement through an online means that is available on a 24/7 basis.

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 confidential 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

In order to formalize the relationships, there shall be a subscriber agreement between the certificate issuer and the subscriber. The subscriber agreement describes the terms and conditions of service provision and also binds the subscriber to its obligations specified in the certificate policy. The policy authority shall make the certificate policy available to the subscriber.

There shall be a relying party agreement between the certificate validation service provider and the relying party. The policy authority shall make the certificate policy available to the relying party and the CVSP.

Typically, there will be no contract between the subscriber and the relying party.

The CPS shall be made available by the certificate manufacturer to the certificate issuer and to the policy authority. Typically, the CPS will not be made available to subscribers and relying parties or the CVSP. Typically, a PKI disclosure statement can be used for this purpose or, alternatively, an independent assessment can be used to determine the suitability of the controls described in the CPS. However, at its discretion, the certification authority can provide copies of its CPS to the CVSP. The contents of the PKI disclosure statement are determined at the discretion of the CA.

When a PKI operates within a scheme, the scheme will typically specify requirements that should be met by entities within the PKI. The policy authority is responsible for ensuring that the CP complies with the scheme rules. For purposes of interoperability each respective CA's CPS or PKI disclosure statement can be made available to the respective CAs prior to cross-certification.

Figure 6 provides an overview of the typical control documents within the standard financial PKI model.

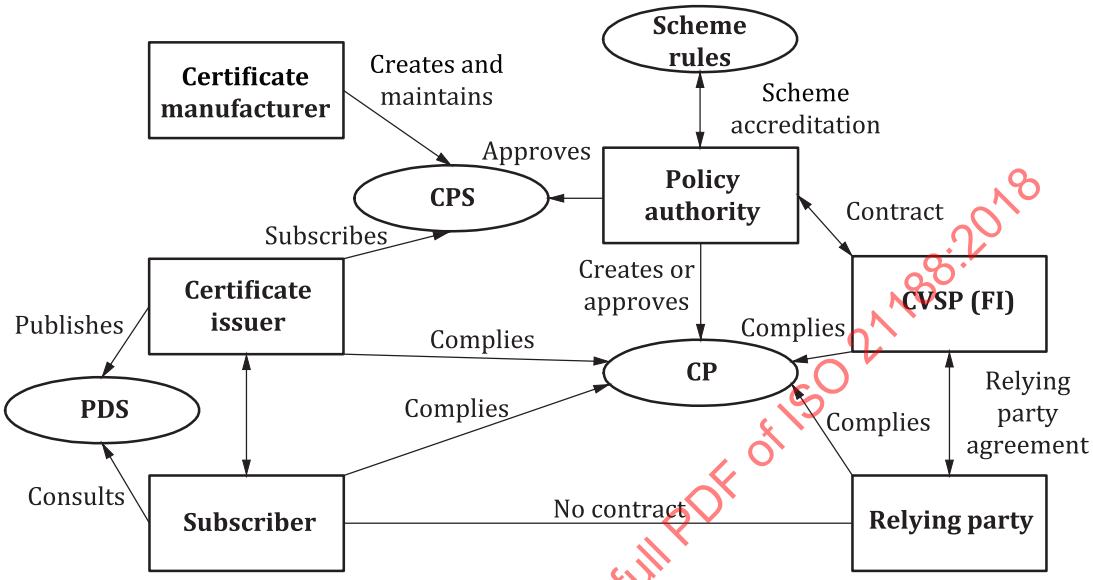

Figure 6 — Control documents within standard financial PKI model

5.9 Time-stamping

The timing of events from a trusted time source (i.e. a time source known to be synchronized with universal coordinated 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 is 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 certificate cannot be ensured. Secondly, if a certificate is revoked then any use of the certificate after the time that it is revoked could 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 protection, 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 could 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 ISO 18014. 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 could 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 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

The trustworthiness of CA by a relying party can be achieved by various trust models; for more information, see Annex G.

— first party trust model

— second party trust model

— third party trust model

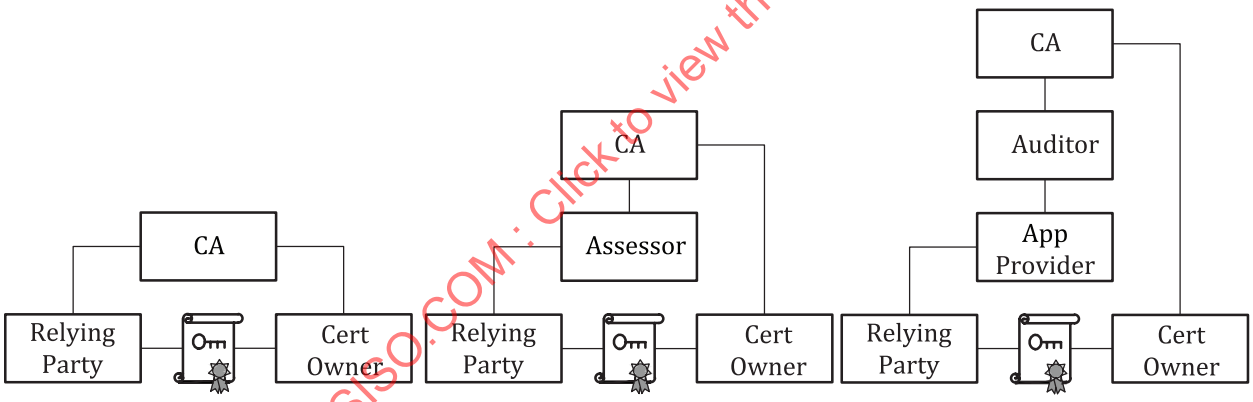

Figure 7 — CA trust models

Figure 7 shows several alternative trust models. The first party trust model is where the relying party validates its trustworthiness of the CA, so the CA is a first party to the relying party. The second party trust model is where the relying party's confidence of the CA is based on an evaluation provided by an assessor. The third party trust model is where the relying party actually puts its trustworthiness on the application developer, whose acceptance of the CA is based on the findings of the auditor, so the CA is a third party to the relying party.

The WebTrust for CA and EV audits are examples of a third party trust model. The second party assessor can be a licensed WebTrust auditor or equivalent assessor. Applications shall recognize the policy qualifier type **id-qt-ev**:: = iso (1) identified-organization (3) dod (6) internet (1) security (5) mechanisms (5) pkix (7) kp (3) qt (2) qt-ev (3) as follows:

a) Each EV certificate in the validation certificate chain shall contain the policy qualifier type **id-qt-ev** including the root CA certificate.

b) Any EV certificate without the policy qualifier type **id-qt-ev** shall be invalid.

c) An application certificate practices shall include error handling of invalid certificates.

5.10.2 Wildcard considerations

Wildcard certificates allow the same certificate to be used for difference systems. For example, the three domain names alice.example.com, bob.example.com and cortez.example.com can be services by the same certificate with the common name *.example.com. However, any illicit system inserted into the same domain such as rogue.example.com could 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 financial institutions.

a) Certificates shall only use fully qualified domain names (FQDN).

b) The subject alternate name (SAN) certificate extension shall be used for multiple domain names.

5.10.3 Relying party considerations

5.10.3.1 General

Relying parties are dependent on certificates but typically do not have a direct business relationship with the certificate authority (CA). The relying party validates signatures and certificates according to a signature validation policy which can imply trust in the certificate authority 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. Consequently, actions taken by the relying party shall include the following.

5.10.3.2 Certificate validation

The relying party shall perform certificate validation consisting of the following steps:

1) determine the complete certificate chain, consisting of the subject certificate, typically one or more intermediary (subordinate) CA certificates, and the trust anchor (the root CA certificate);

2) authorize the subject certificate;

3) authorize the trust anchor and intermediary CA certificates;

4) verify the validity dates and operation period;

5) verify the key usage and extended key usage for each certificate;

6) verify the CA signature for each certificate;

7) verify the status (e.g. revoked or suspended) for each certificate.

The certificate validation is only successful if all of the steps have been successfully completed. Otherwise, the certificate chain is invalid and the relying party shall reject the subject certificate. The first failure negates the need to continue processing all of the steps. Most browsers allow users to accept invalid certificates and bypass certificate validation.

5.10.3.3 Certificate revocation or suspension

Actions taken by relying parties shall 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.

Actions taken by relying parties shall include the following.

— provide notification to other entities (e.g. subject, relying parties);

— investigate the security incident and take appropriate supplementary actions to limit exposure.

6 Certificate policy and certification practice statement requirements

6.1 Certificate policy (CP)

Certificates shall be issued under at least one CP. A certificate issued in the X509 v3 format shall be explicitly associated with one certificate policy.

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

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

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

b) CP shall in accordance:

   — be uniquely identified;

   — contain its name;

   — identify where the document can be acquired (e.g. URL, email address, OID).

c) CP shall provide a definition of terms used within the policy (where such definitions differ from those defined in Clause 3).

d) CP shall provide procedures for administration. CP shall include administrative procedures in order to:

   — identify policy authority;

   — identify procedures for publication, change and subsequent notification;

   — identify the version number and effective date;

   — include an expiry date if applicable.

e) CP shall identify subscriber obligations and liabilities. CP shall include subscriber obligations and liabilities in order to:

   — provide information in certificate request that is accurate and that the act of accepting the certificate guarantees that information contained is accurate;

   — guarantee 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;

   — protect the access to the private key associated with certificate;

   — notify the issuer of private key compromise or change of status within the timeframe specified in the CP;

— restrict the use of the certificate to the usage specified.

f) CP shall identify issuer obligations and liabilities. CP shall include issuer obligations and liabilities in order to:

— notify the subject and, where applicable, the subscriber of the certificate that the certificate has been issued;

— notify the subject and, where applicable, the subscriber whose certificate has been revoked, suspended or unsuspended;

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

— comply with the CP identified and its associated certification practice statement;

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

— provide confidentiality protection to non-public subscriber and relying party information.

g) CP shall identify relying party obligations and liabilities. CP shall include relying party obligations and liabilities in order to:

— restrict usage to applications identified;

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

— check digital signature;

— validate certificate content and status;

— provide notification of applicable liability caps and warranties.

h) CP shall identify any applicable reliance or financial limits for certificate usage.

i) CP shall state the minimum requirements for:

— subscriber identification and authentication;

— certificate status publication;

— subscriber private key protection;

— CA private key protection.

j) CP shall state the minimum requirements for the mandatory X.509 v3 fields:

— version number;

— serial number;

— signature algorithm;

— issuer;

— valid from and valid to dates;

— subject;

— public key algorithm and minimum key length;

— required extensions.

See Annex A for additional information on certificate policies.

6.2 Certification practice statement (CPS)

a) A certification authority shall document its certification practices.

b) A CPS or equivalent shall support each CP under which the CA issues or manufactures certificates.

c) The CA's certification practices shall address the contents provided in Annex B 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 shall comply with the control objectives in 7.2.

e) A CA's certification practices shall include those control procedures specified in Clause 7, which are appropriate based on the CA's assessment of risks and meet the requirements of the supported certificate policies.

See Annex B for additional information on certification practice statements.

7 Certification authority control procedures

7.1 General

Control objectives in the areas of CA environmental controls, CA key life cycle management controls and certificate life cycle management controls are presented in 7.2 to 7.6, representing baseline control criteria with which a CA shall comply and against which a CA can be evaluated or audited. 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.

A number of the control objectives are regarded as optional and would only be applicable if supported by the CA. These include:

— CA-provided subject key generation services;

— CA-provided subject key storage, recovery and escrow services;

— integrated circuit card (ICC) life cycle management;

— certificate renewal;

— certificate suspension.

The control procedures described in this clause represent recommended practices for business, operational and technical use by a certification authority. Certain control procedures (i.e. control procedures using the word "shall") are required for compliance with this document.

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 compliance 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 CA environmental controls

7.2.1 Certification practice statement and certificate policy management

Control objectives:
The CA shall maintain controls to provide reasonable assurance that its certification practice statement (CPS) and certificate policy (CP) management processes are effective. The policy authority (PA) shall have the responsibility of defining the business requirements and policies for using digital certificates and is specified in a certificate policy (CP) and supporting agreements.

Control procedures:	
	Policy authority (PA) management
1	The PA should be responsible for ensuring that the CA's control processes, as stated in a certification practice statement (CPS) or equivalent, fully comply with the requirements of the CP.
2	The PA shall have final authority and responsibility for specifying and approving certificate policies.
3	The PA shall have final authority and responsibility for approving the CA's certification practice statement (CPS).
4	The PA shall ensure a certification practice statement (CPS) or equivalent document is in place at least describing the following: a) CA environmental controls; b) key life cycle management controls; c) certificate life cycle management controls.
5	The PA or delegated representative shall ensure the business service application is using the appropriate certificate policy.
6	The PA shall maintain procedures for the termination of certificate policies, notifying the affected parties. The PA shall notify, in the first instance, those CAs that support its certificate policies in order that appropriate actions can be undertaken expeditiously.
7	The PA shall maintain procedures in the event of its termination. In this event, affected parties shall be notified and the transference of relevant archived records to a custodian shall take place.
	Certificate policies management
8	Certificate policies shall be approved by the policy authority in accordance with a defined review process, including responsibilities for maintaining the certificate policies.
9	A defined review process shall exist to ensure that certificate policies are capable of support by the controls specified in the CPS.
10	The PA shall make available the certificate policies supported by the CA to all appropriate subscribers and relying parties.
11	The PA shall periodically conduct assessments to determine the adequacy of the CP to address business risks.
	Certification practice statement (CPS) management by CA

12	The CA's CPS shall be approved by the PA and modified in accordance with a defined review process, including responsibilities for maintaining the CPS.
13	The CA shall make available its certification practice statement (CPS) to all appropriate parties.
14	Revisions to the CA's CPS shall be made available to appropriate parties.
15	The CPS shall contain an explanation of the controls to ensure compliance with: a) legislative requirements; a) contractual requirements; b) educational and notification requirements; c) prevention and detection of virus and other malicious software; d) business continuity requirements; e) escalation requirements from the consequences of security policy violations or security incidents.
	CA management
16	The CA's controls shall be described in the CPS or equivalent documentation.

7.2.2 Security management

Control objectives:
The CA shall maintain controls to provide reasonable assurance that: — security is planned, managed and supported within the organization; — identified risks are managed effectively; — the security of CA facilities, systems and information assets accessed by third parties is maintained; — the security of information is maintained when 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.
2	Responsible 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: a) a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; b) a statement of management intent, supporting the goals and principles of information security; c) an explanation of the security policies, principles, standards and compliance requirements of particular importance to the organization; d) a definition of general and specific responsibilities for information security management, including reporting security incidents; e) references to documentation that supports the policy.
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 and/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	Procedures should exist to carry out a risk assessment to identify, analyse and evaluate 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, and/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.

7.2.3 Asset classification and management

Control objective:
The CA shall maintain controls to provide reasonable assurance that CA assets and information receive an appropriate level of protection based upon the requirements of all supported certificate policies and risk analysis.

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.

7.2.4 Personnel security

Control objective:
The CA shall maintain controls to provide reasonable assurance 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 in job descriptions. 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: a) overall responsibility for administering the implementation of the CA's security practices; b) approval of the generation, revocation and suspension of certificates; c) installation, configuration and maintenance of the CA systems; d) day-to-day operation of CA systems and system back-up and recovery; e) viewing and maintenance of CA system archives and audit logs; f) cryptographic key life cycle management functions (e.g. key component custodians); g) CA systems development.
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 shall be performed at the time of job application and periodically for those individuals undertaking trusted roles.
5	An individual's trusted status shall be approved prior to gaining access to systems/facilities or performing actions requiring trusted status.
6	CA employees and trusted roles shall sign a confidentiality (non-disclosure) agreement as a condition of employment.
7	Contractors who perform trusted roles shall be subject to at least the same background check and personnel management procedures as employees.
8	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. Protective measures may include: a) bonding requirements on contract personnel; b) indemnification for damages due to contract personnel wilful harmful actions; c) financial penalties.
9	A formal disciplinary process shall exist and be followed for employees who have violated organizational security policies and procedures.
10	Appropriate and timely actions shall be taken when employment is terminated so that controls (e.g. access controls) are not impaired.
11	Duress alarms shall be provided for personnel who might be the target of coercion.
12	All employees of the organization and, where relevant, third party contractors shall receive appropriate training in organizational policies and procedures.

7.2.5 Physical and environmental security

Control objectives:
The CA shall maintain controls to provide reasonable assurance that: — physical access to CA facilities is limited to authorized individuals; — CA facilities are protected from environmental hazards; — loss, damage or compromise of assets and interruption to business activities are prevented; — compromise of information and information processing facilities is prevented.

Control procedures:	
	CA facility physical security
1	Physical protection should be achieved through the creation of restricted security perimeters (e.g. physical and logical barriers). The CA's certificate manufacturing facility shall be protected with its own unique physical perimeter.
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 should be in place (e.g. Faraday cage) to prevent electromagnetic radiation emissions for all root CA operations (e.g. key generation and certification of CA certificates) and where certificate policies 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	CA operational facilities shall be physically locked and alarmed when unoccupied.
9	All personnel shall be required to wear visible identification. Employees should be encouraged to challenge anyone not wearing visible identification.
10	Access to CA operational facilities shall be controlled and restricted to authorized persons through the use of authentication controls.
11	All personnel entering and leaving CA operational facilities shall be logged (i.e. an audit trail of all access is securely maintained).
12	Visitors to CA facilities shall be supervised and their date and time of entry and departure recorded.
13	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.
14	Access rights to CA facilities shall be regularly reviewed and updated.
	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 shall be protected from interception or damage.

19	Equipment shall be maintained in accordance with the manufacturer's instructions and/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.
	General controls
21	Sensitive or critical business information shall be locked away when not required and when the CA facility is vacated.
22	Procedures shall require that personal computers and workstations be logged off or protected by key locks, passwords or other controls when not in use.
23	Procedures shall require that equipment, information and software belonging to the organization cannot be taken off-site without authorization.
24	Physical access to the cryptographic module shall be limited to authorized entities under dual control.

7.2.6 Operations management

Control objectives:
The CA shall maintain controls to provide reasonable assurance that: — the correct and secure operation of CA information processing facilities is ensured; — the risk of CA systems failure is minimized; — the integrity of CA systems and information is protected against viruses and malicious software; — damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures; — media are securely handled to protect them from damage, theft and unauthorized access.

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 be separated 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	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.
10	Procedures shall exist and be followed for reporting hardware and software malfunctions.
11	Procedures shall exist and be followed to ensure that faults are reported and corrective action is taken.
12	A formal problem management process shall exist which allows the types, volumes and impacts of incidents and malfunctions to be documented, quantified and monitored.
	Media handling and security
13	Procedures for the management of removable computer media shall require the following: 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; 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; c) all media are stored in a safe, secure environment, in accordance with manufacturers' specifications.
14	Equipment containing storage media (i.e. 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.
15	Procedures for the handling and storage of information shall exist and be followed in order to protect such information from unauthorized disclosure or misuse.
16	System documentation should be protected from unauthorized access.

7.2.7 System access management

Control objectives:
The CA shall maintain controls to provide reasonable assurance that CA system access is limited to authorized individuals. Such controls shall provide reasonable assurance that: — operating system access is limited to authorized individuals with predetermined task privileges; — access to network segments housing CA systems is limited to authorized individuals, applications and services; — CA application use is limited 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: a) roles and corresponding access permissions; b) identification and authentication process for each user; c) segregation of duties; 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 dual controlled.

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 direct access only to the services that they have been specifically authorized to use. The path from the user terminal to computer services is 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 or CA systems to remote computer systems 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 compliance with the CA's configuration requirements.
14	Sensitive data shall be encrypted when exchanged over public or untrusted networks.
	Operating system access control
15	Operating systems shall be configured in accordance with the CA's operating system configuration standards and be periodically reviewed.
16	Operating system patches and updates shall be applied in a timely manner when deemed necessary based on a risk assessment.
17	Automatic terminal identification shall be used to authenticate connections to specific locations and to portable equipment.
18	Access to CA systems shall require a protected log-on process.
19	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.
20	Uses of system utility programmes shall be restricted to authorized personnel and be tightly controlled.
21	Inactive terminals serving CA systems shall require re-authentication prior to use.
22	Restrictions on connection times should be used to provide additional security for high-risk applications.
23	Sensitive operating system data shall be protected against disclosure to unauthorized users.
	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.

7.2.8 Systems development and maintenance

Control objective:
The CA shall maintain controls 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 control 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 15408 or similar.

7.2.9 Business continuity management

Control objectives:
The CA shall maintain controls to provide reasonable assurance of continuity of operations in the event of a disaster. Such controls shall include at a minimum: — the development and testing of a CA disaster recovery plan; — the storage of required cryptographic materials (i.e. secure cryptographic device and activation materials) at an alternative location; — the storage of back-ups of systems, data and configuration information at an alternative location; — the availability of an alternative site, equipment and connectivity to enable recovery. The CA shall maintain controls 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. The CA's business continuity plan shall address the following: a) the conditions for activating the plans; b) emergency procedures; c) fallback procedures; d) resumption procedures; e) a maintenance schedule for the plan; f) awareness and education requirements; g) the responsibilities of the individuals; h) recovery time objective (RTO); i) regular testing of contingency plans.
3	The CA's business continuity plans shall include disaster recovery processes for all critical components of a CA system, including the hardware, software and keys, in the event of a failure of one or more of these components. Specifically: 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; 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	The CA shall identify and arrange for an alternative site where core PKI operations can be restored in the event of a disaster at the CA's primary site. Fallback 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 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 and/or data are corrupted or suspected to be corrupted.
8	Business continuity plans shall be tested 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.

7.2.10 Monitoring and compliance

Control objectives:
The CA shall maintain controls to provide reasonable assurance that: — it conforms with the relevant legal, regulatory and contractual requirements; — compliance with the CA's security policies and procedures is ensured; — unauthorized CA system usage is detected.

Control procedures:	
	Compliance with requirements
1	The CA shall have implemented procedures to ensure compliance with restrictions on the use of material with respect to intellectual property rights, and on the use of proprietary software products.
2	Controls shall be in place to ensure access to or use of cryptographic hardware and software.
3	Procedures shall exist to ensure that personal information is protected.
4	The information security policy shall address the following: a) the information that shall be kept confidential by CA or RA; b) the information that is not considered confidential; c) the policy on release of information to law enforcement officials; d) information that can be revealed as part of civil discovery; e) the conditions upon which information can be disclosed with the subject's consent; f) any other circumstances under which confidential information can be disclosed.
5	Important records of the CA shall be protected from loss, destruction and falsification.
	Review of security policy and technical compliance
6	Managers should be responsible for ensuring that security procedures within their area of responsibility are carried out correctly.
7	The CA's operations shall be subject to regular review to ensure compliance with its CPS.
8	CA systems shall be periodically checked for compliance with security implementation standards.
	Monitoring system access and use
9	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.

7.2.11 Audit logging

Control objectives:
The CA shall maintain controls to provide reasonable assurance that: — CA environmental, key management and certificate management events are accurately and appropriately logged; — the confidentiality and integrity of current and archived audit logs are maintained; — audit logs are completely and confidentially archived in accordance with disclosed business practices; — 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 the following elements: a) date and time of the entry; b) serial or sequence number of entry (for automatic journal entries); c) kind of entry; d) source of entry (e.g. terminal, port, location, customer, etc.); e) identity of the entity making the journal entry.
	Events logged
3	The CA shall log the following CA and subject (if applicable) key life cycle management related events: a) CA key generation; b) installation of manual cryptographic keys and its outcome (with the identity of the operator); c) CA key back-up; d) CA key storage; e) CA key recovery; f) CA key escrow activities (if applicable); g) CA key usage; h) CA key archival; i) withdrawal of keying material from service; j) CA key destruction; k) identity of the entity authorizing a key management operation; l) identity of the entities handling any keying material (such as key components or keys stored in portable devices or media); m) custody of keys and of devices or media holding keys; n) compromise of a private key.
4	The CA shall log the following cryptographic device life cycle management related events: a) device receipt and installation; b) placing into or removing a device from storage; c) device activation and usage; d) device deinstallation; e) designation of a device for service and repair; f) device retirement.

5	If the CA provides subject key management services, the CA shall log the following subject key life cycle management related events: a) key generation; b) key distribution (if applicable); c) key back-up (if applicable); d) key escrow (if applicable); e) key storage; f) key recovery (if applicable); g) key archival (if applicable); h) key destruction; i) identity of the entity authorizing a key management operation; j) key compromise.
6	The CA shall record (or require that the RA record) the following certificate application information: a) the method of identification applied and information used to meet "know-your-customer" requirements; b) record of unique identification data, numbers or a combination thereof (e.g. applicant's driving license number) of identification documents, if applicable; c) storage location of copies of applications and identification documents; d) identity of entity accepting the application; e) method used to validate identification documents, if any; f) name of receiving CA or submitting RA, if applicable; g) the subject's acceptance of the subscriber agreement; 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.
7	The CA shall log the following certificate life cycle management related events: a) receipt of requests for certificate(s) – including initial certificate requests, renewal requests and rekey requests; b) submissions of public keys for certification; c) change of affiliation of an entity; d) generation of certificates; e) distribution of the CA's public key; f) certificate revocation requests; g) certificate revocation; h) certificate suspension requests (if applicable); i) certificate suspension and reactivation; j) generation and issuance of certificate revocation lists.

8	The CA shall log the following security-sensitive events: a) security sensitive files or records read or written, including the audit log itself; b) actions taken against security sensitive data; c) security profile changes; d) use of identification and authentication mechanisms, both successful and unsuccessful (including multiple failed authentication attempts); e) security-sensitive non-financial transactions (e.g. account or name/address changes); f) system crashes, hardware failures and other anomalies; g) actions taken by individuals in trusted roles, computer operators, system administrators and system security officers; h) change of affiliation of an entity; i) decisions to bypass encryption/authentication processes or procedures; j) access to the CA system or any component thereof.
9	Audit logs shall not record the private keys in any form (e.g. plaintext or enciphered).
10	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
11	Current and archived audit logs shall be maintained in a form that prevents their modification or unauthorized destruction.
12	Digital signatures shall be used to protect the integrity of audit logs where applicable or required.
13	The 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 archival
14	The CA shall archive audit log data on a periodic basis.
15	In addition to possible regulatory stipulation, a risk assessment shall be performed to determine the appropriate length of time for retention of archived audit logs.
16	The CA should maintain archived audit logs at a secure off-site location for a predetermined period 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. 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.

7.3 CA key life cycle management controls

7.3.1 CA key generation

Control objective:
The CA shall maintain controls to provide reasonable assurance that CA key pairs are generated in accordance with defined key generation ceremony scripts and the requirements of the CPS.

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 shall include the following: a) definition of roles and responsibilities; b) approval for conduct of the key generation ceremony; c) cryptographic hardware and activation materials required for the ceremony; d) specific steps performed during the key generation ceremony; e) procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony; f) sign-off from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; g) notation of any deviations from the key generation ceremony script. Refer to Annex D for additional discussion of CA key generation ceremonies.
2	Generation of CA keys shall occur within a cryptographic module meeting the requirements of ISO 19790 and ISO 13491-1 and the business requirements in accordance with the CPS. Such cryptographic devices shall perform key generation using a random number generator (RNG) or pseudo random number generator (PRNG) as specified in ISO/IEC 18032.
3	Generation of CA keys shall be undertaken in a physically secured environment (see 7.2.5) by personnel in trusted roles (see 7.2.4) under the principles of multiple control and split knowledge. (See Annex D)
4	The CA shall generate its own key pair in the same cryptographic device in which it will be used or the key pair is injected directly from the device where it was generated into the device where it will be used.
5	CA key generation shall generate keys which: a) are appropriate for the intended application or purpose and commensurate with the identified risks; b) use an approved algorithm as specified in ISO/IEC 18033, parts 1 to 4; c) have a key length that is appropriate for the algorithm and for the validity period of the CA certificate; d) take into account requirements on parent and subordinate CA key sizes; e) are in accordance with the CP.
6	Generation of CA keys shall result in key size in accordance with the CP. The public key length to be certified by a CA shall be less than or equal to that of the CA's private signing key.
7	The integrity of the hardware/software used for key generation and the interfaces to the hardware/software shall be tested before production usage.

7.3.2 CA key storage, back-up and recovery

Control objectives:
The CA shall maintain controls to provide reasonable assurance that: — CA private keys remain confidential and maintain their integrity; — access to CA cryptographic hardware is limited to authorized individuals.

Control procedures:	
1	The CA's private (signing and confidentiality) keys shall be stored and used within a secure cryptographic device meeting the appropriate ISO 15408 protection profile, ISO 19790 or FIPS 140-2 level requirement based on a risk assessment and the business requirements of the CA and in accordance with the CA's CPS and applicable certificate policies.
2	If the CA's private keys are not exported from a secure cryptographic module, then the CA private key shall be generated, stored and used within the same cryptographic module.
3	If the CA's private keys are exported from a secure cryptographic module 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 can include any of the following: a) cipher text using a key which is appropriately secured; b) encrypted key fragments using multiple control and split knowledge/ownership; c) another secure cryptographic module, such as a key transportation device using multiple control.
4	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.
5	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. 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 with the following characteristics: a) inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device; b) access control processes and procedures to limit physical access to authorized personnel; c) recording of all successful or failed access attempts to the CA facility and device storage mechanism (e.g. a safe) in audit logs; d) incident handling processes and procedures to handle abnormal events, security breaches, and investigation and reports; e) audit processes and procedures to verify the effectiveness of the controls.
8	When not attached to the CA system, the CA cryptographic hardware shall be stored in a tamper-resistant container that is stored securely under multiple controls (i.e. a safe).
9	The handling of CA cryptographic hardware, including the following tasks, shall be performed in the presence of no less than two trusted employees: a) installation of CA cryptographic hardware; b) removal of CA cryptographic hardware from production; c) servicing or repair of CA cryptographic hardware (including installation of new hardware, firmware or software); d) disassembly and permanent removal from use.
10	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).

7.3.3 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). For subsequent and/or subordinate CA public keys, these shall be validated, by using a chaining method or similar process, to link back to trusted root certificate. For a new root certificate, an out-of-band process can be required.
2	The initial distribution mechanism for the CA's public key shall be controlled as documented in the CA's CPS. CA public keys shall be initially distributed within a certificate using one of the following methods in accordance with the CA's CPS: a) machine readable media (e.g. smart card, CD ROM) from an authenticated source; b) embedding in an entity's cryptographic module; c) other secure means that ensure authenticity and integrity.
3	The CA's public key shall be changed (rekeyed) periodically according to the requirements of the CPS. Sufficient advance notice shall be provided to avoid disruption of the CA services.
4	The subsequent distribution mechanism for the CA's public key shall be controlled as documented in the CA's CPS.
5	If an entity already has an authenticated copy of the CA's public key, a new CA public key shall be distributed using one of the following methods in accordance with the CA's CPS: a) direct electronic transmission from the CA; b) placing in a remote cache or directory; c) loading into a cryptographic module; d) any of the methods used for initial distribution.

7.3.4 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 multi-party control (i.e. *m* of *n*) with a minimum value of three recommended for *m*.
2	If necessary, 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 and/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 7.2.5).

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.

7.3.5 CA key archival and destruction

Control objectives:
The CA shall maintain controls to provide reasonable assurance that: — archived CA keys remain confidential and secured in the event that they are put back into production; — 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	Archived CA keys shall be subject to the same or a greater level of security controls as keys currently in use.
2	The CA's private keys shall not be destroyed until the business purpose or application has ceased to have value or legal obligations have expired.
3	Archived keys shall only be put back into production when a security incident results in a loss of production keys or where historical evidence requires validation. Control process shall be required to ensure the integrity of the CA systems and the key sets.
4	Archived keys shall be recovered for the shortest possible time period to meet business requirements.
	CA key destruction
5	Authorization to destroy a CA private key and how the CA's private key is destroyed (e.g. token surrender, token destruction or key overwrite) shall be limited in accordance with the CA's CPS.
6	All copies and fragments of the CA's private key shall be destroyed in a manner such that the private key cannot be retrieved.
7	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.

7.3.6 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 including the revocation and reissue of all certificates that were signed with that CA's private key shall exist.

3	The recovery procedures used if the CA's private key is compromised shall include the following actions: a) how to secure key usage in the environment is re-established; b) how the CA's old public key is revoked; c) the notification procedures for affected parties (e.g. impacted CAs, repositories, subscribers and CVSPs); d) how the CA's new public key is provided to the end entities and relying parties together with the mechanism for their authentication; 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 shall be in place for the secure and authenticated revocation of the following: a) the old CA root public key; b) the set of all certificates (including any self-signed) issued by a root CA or any CA based on the compromised private key; c) any subordinate CA public keys and corresponding certificates that require recertification.
5	The CA's business continuity plan for key compromise shall address who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures and encrypted data.
6	The CA business continuity plan should consider key replication techniques.

7.4 Subject key life cycle management controls

7.4.1 CA-provided subject key generation services (if supported)

Control objectives:
If the CA provides subscriber key management services, the CA shall maintain controls to provide reasonable assurance that: — subject keys generated by the CA (or RA or other authorized third party) are generated in accordance with the CP; — 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 occur within a secure cryptographic device, meeting the appropriate ISO 19790 security level 1 requirements based on a risk assessment and the business requirements of the CA and in accordance with the applicable CP. Such cryptographic devices shall perform subject key generation using a random number generator (RNG) or pseudo random number generator (PRNG) as specified in ISO/IEC 18032.
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	Subject key generation performed by the CA shall be performed in a process initiated by authorized personnel in accordance with the CA's CPS.
5	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.
6	Subject key generation shall not be performed by the RA.

7.4.2 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 archived by the CA remain confidential; — subject private keys stored by the CA are completely destroyed at the end of the key pair life cycle; — subject private keys escrowed by the CA remain confidential.

Control procedures:	
	CA-provided subject key storage, back-up and recovery
1	Subject private keys stored by the CA (or trust service provider for key storage) shall be stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and requirements of the CP.
2	If the CA generates 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 of the subject's private (confidentiality) key is maintained throughout its life cycle.
	CA-provided subject key archival
6	Subject private (confidentiality) keys archived by the CA shall be stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the requirements of the CP.
7	If the CA provides subject (confidentiality) key archival, all archived subscriber keys shall be destroyed at the end of the archive period.
	CA-provided subject key destruction
8	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.

9	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
10	Subject private (confidentiality) keys escrowed by the CA for purposes of access by law enforcement shall be stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and the requirements of the CP.

7.4.3 Integrated circuit card (ICC) life cycle management (if supported)

Control objectives:
If the CA (or RA) distributes subject key pairs and certificates using integrated circuit cards (ICCs), the CA (or RA) shall maintain controls to provide reasonable assurance that: — ICC procurement, preparation and personalization are securely controlled by the CA (or RA or other authorized third party); — ICC usage is enabled by the CA (or RA or other authorized third party) prior to ICC issuance; — ICCs are securely stored and distributed by the CA (or RA or other authorized third party); — ICCs are securely replaced by the CA (or RA or other authorized third party); — ICCs returned to the CA (or RA or other authorized third party) are securely terminated.

Control procedures:	
	ICC 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 ICCs.
2	ICCs 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	ICCs issued to subject shall meet the appropriate ISO/IEC 15408 protection profile, ISO card standard [e.g. ISO/IEC 7810, ISO/IEC 7813, ISO/IEC 7816 (parts 1–12 and 15), ISO 10202] or FIPS 140-2[12] level requirement based on a risk assessment and the requirements of the CP.
4	The card bureau shall verify the physical integrity of ICCs upon receipt from the card manufacturer.
5	ICCs shall be securely stored and under inventory control while under the control of the card issuer.
	Card preparation and personalization
6	ICC preparation processes and procedures, including the following, shall exist and be followed: a) loading of the card operating system; b) creation of logical data structures (card file system and card security domains); c) loading of applications; d) logically protecting the ICC to prevent unauthorized modification of the card operating system, card file system, card security domains and applications.

7	ICC personalization processes and procedures, including the following, shall exist and be followed: a) the loading of identifying information on to the card; b) generation of subject key pair(s) in accordance with 7.4.1 and the CP; c) loading subject private key(s) on to the ICC (if generated outside the card) in encrypted form; d) loading subject certificate(s) on to the ICC; e) loading the CA and other certificates for the contractual environment on to the ICC; f) logically protecting the ICC from unauthorized access.
8	The card bureau or CA (or RA) shall log ICC preparation and personalization in an audit log.
9	An ICC shall not be issued unless the card has been prepared and personalized by the card bureau, the CA or the RA.
10	An ICC shall be unusable unless in an activated state.
	ICC distribution
11	Processes and procedures shall exist and be followed for the distribution, tracking and accounting for the safe receipt subscriber ICCs to subjects.
12	ICC 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	ICC distribution shall be logged by the card bureau CA (or RA) in an audit log.
	Subject ICC 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 ICC during use by the subscriber (i.e. PIN access control mechanism – cardholder verification method).
15	The subject private keys on the ICC 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 ICC application shall produce audit logs of all uses of the ICC. 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 and/or integrity of a transaction.
18	The ICC shall be used by the subject or, where applicable, the subscriber in accordance within the terms of the CP.
	ICC replacement
19	Processes and procedures shall exist and be followed for replacement of a subject's lost or damaged ICC.
20	In the event of card loss or damage, subject certificates shall be renewed or rekeyed in accordance with the CP (see 7.5.2 and 7.5.3).
21	ICC replacement shall be logged by the card bureau or CA (or RA) in an audit log.
	ICC termination
22	All ICCs returned to the ICC or CA (or RA) shall be deactivated or securely destroyed to prevent unauthorized use.
23	ICC termination shall be logged by the card bureau or CA (or RA) in an audit log.

7.4.4 Requirements for subject key management

Control objective:
The CA shall prescribe the means to securely manage subject keys throughout the key life cycle.

Control procedures:	
	Subject key generation
1	The CP shall specify the appropriate ISO 19790 (FIPS 140-2) security level requirements for cryptographic modules used for subject key generation.
2	The CP shall specify the key generation algorithm(s) that can be used for subject key generation.
3	The CP shall specify the acceptable key sizes for subject key generation.
	Subject key storage, back-up and recovery
4	The CA or RA shall provide or make available the mechanisms to allow the subscriber to access (i.e. private key owner verification method), manage and control the usage of their private keys.
5	The CP shall specify the private key protection requirements for stored subject private keys.
6	The CP shall state the circumstances and authority of when the subject's private key will be restored and the control processes.
7	The CP shall specify the private key protection requirements for back-up copies of subject private keys stored by the subject.
	Subject key usage
8	Banking 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 ICC and software application).
9	The CP shall specify the acceptable uses for subject key pairs.
10	The CP shall specify the requirements for subject key usage.
	Subject key archival
11	The CP shall specify the private key protection requirements for archived subject private keys.
12	The CP shall specify the requirements for destruction of archived subject keys at the end of the archive period.
	Subject key destruction
13	The CP shall specify the means through which subject key destruction can be performed.
14	The CP or CPS shall specify the requirements for destruction of all copies and fragments of the subject's private key at the end of the key pair life cycle.
	Subject cryptographic hardware life cycle management
15	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
16	The CP shall specify the requirements for notification of the CA or RA in the event of subject key compromise.

7.5 Certificate life cycle management controls

7.5.1 Subject registration

Control objectives:
The CA shall maintain controls to provide reasonable assurance that: — subjects (or where applicable the subscribers) are accurately identified in accordance with the applicable “know-your-customer” requirements; — subjects' (or where applicable the subscriber's) 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: a) For individual end entity certificates, the CA or RA shall verify (as determined by the CP) the identity of the person whose name is to be included in the subject distinguished name field of the certificate. An individual name which cannot be verified shall not be included in the subject distinguished name. b) For organizational certificates (including role based, server, network resource or code signing), the CA or RA shall verify (as determined by the CP) the legal existence of the organization's name to be included in the organization attribute in the subject distinguished name field of the certificate and the authority of the requesting party. An unauthenticated organization name shall not be included in a certificate. c) For organizational certificates containing a domain name of an organization, the CA or RA shall verify (as determined by the CP) the organization's ownership, control or right to use the domain name included in the common name attribute of the subject distinguished name field of the certificate and the authority of the requesting party. An unauthenticated domain name shall not be included in a certificate.
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 use the RA's public key contained in the requesting entity's certificate request to verify signature on the certificate request submission.
5	The CA shall verify the uniqueness of the subject's fully qualified distinguished name (FQDN) and public key within the boundaries or community defined by the CP.
6	Encryption and access controls shall be used to protect the confidentiality and integrity of registration data in transit and in storage.
7	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.
	Certificate request
8	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.
9	The CA shall require that the requesting entity submit its public key in a self-signed message to the CA for certification. The CA shall require that the requesting entity digitally sign the registration request using the private key that relates to the public key contained in the registration request in order to: a) allow the detection of errors in the certificate application process; b) prove possession of the companion private key for the public key being registered; c) verify the integrity of the entity's distinguished name, public key and other information in the certificate signature request (CSR).
10	The certificate request shall be treated as acceptance of the terms of conditions by the requesting entity to use that certificate as described in the subscriber agreement.
11	The CA shall validate the identity of the RA authorized to issue registration requests under a specific CP.
12	The CA shall require that RAs submit the requesting entity's certificate request data to the CA in a message (certificate request) signed by the RA. The CA shall verify the RA's signature on the certificate request and submit a certification response.

13	The CA shall require that the RA secure that part of the certificate application process for which it (the RA) assumes responsibility in accordance with the CA's CPS.
14	The CA (or RA) shall record the success or failure of the registration even in an audit log.
15	The CA shall verify the authenticity of the submission by the RA in accordance with the CA's CPS.

7.5.2 Certificate renewal (if supported)

Control objective:
If certificate renewal is supported under the CP, the CA shall maintain controls to provide reasonable assurance that certificate renewal requests are accurate, authorized and complete.

Control procedures:	
	Certificate renewal request
1	The certificate renewal request shall include at least the subject's distinguished name and the serial number of the certificate (or other information that identifies the certificate). (The CA will only renew certificates that were issued by itself.)
2	The CA shall require that the requesting entity digitally sign the certificate renewal request using the private key that relates to the public key contained in the requesting entity's existing public key certificate.
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 no indications exist that the subject's private key has been compromised.
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 or the RA shall validate the signature on the certificate renewal request.
6	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).
7	The CA or the RA shall verify that the request, including the extension of the validity period, meets the requirements defined in the CP. The start date in the renewed certificate should be the same as in the original certificate.
8	If an RA is used, the CA shall require that the RAs submit the certificate renewal data to the CA in a message (certificate renewal request) signed by the RA.
9	The RA shall secure that part of the certificate renewal process for which it (the RA) assumes responsibility in accordance with the CP.
10	The CA shall require that external RAs record their actions in an audit log.
11	The CA shall verify the authenticity of the submission by the RA.
12	The CA shall verify the RA's signature on the certificate renewal request.
13	The CA shall check the certificate renewal request for errors or omissions. This function can be delegated explicitly to the RA.
14	The CA or RA shall notify subjects or, where applicable, subscribers prior to the expiration of their certificate of the need for renewal in accordance with the CP.
15	The CA shall issue a signed notification indicating the certificate renewal has been successful.
16	The CA shall make the new certificate available to the end entity in accordance with the CP.

7.5.3 Certificate rekey

Control objective:
The CA shall maintain controls to provide reasonable assurance that certificate rekey requests are accurate, authorized and complete.

Control procedures:	
1	The CA shall require that the requesting entity digitally sign using the existing private key the certificate rekey request containing the new public key.
2	The CA or the RA shall verify that the certificate rekey request meets the requirements defined in the relevant CP.
3	If an RA is used, the CA shall require that RAs submit the entity‘s certificate rekey request to the CA in a message signed by the RA.
4	If an RA is used, the CA shall require that the RA secure that part of the certificate rekey process for which it (the RA) assumes responsibility.
5	If an RA is used, the CA shall require that external RAs record their actions in an audit log.
6	If an RA is used, the CA shall verify the RA's signature on the certificate rekey request.
7	The CA or the RA shall check the certificate rekey request for errors or omissions.
8	The CA or RA shall notify subscribers prior to the expiration of their certificate of the need to rekey.
9	Prior to the generation and issuance of new certificates, the CA or RA shall verify the following: a) the signature on the certificate rekey data submission; b) the existence and validity supporting the rekey request; c) that the request meets the requirements defined in the CP.
10	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.
11	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.

7.5.4 Certificate issuance

Control objective:
The CA shall maintain controls 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 9594-8 formatting rules.
2	Validity periods shall be set in the CP and are formatted in accordance with ISO 9594-8.
3	Extension fields shall be formatted in accordance with ISO 9594-8.

4	The CA shall sign the end entity's certificate public key and other relevant information with the CA's private signing key: a) The CA shall verify its own digital signature b) The CA shall not issue a failed signature c) The CA shall record the event in an audit log Delivery of the private key material shall be authenticated: a) The recipient shall authenticate the electronic delivery. b) The recipient shall authenticate the physical delivery.
5	Certificates shall be issued based on approved subject registration, certificate renewal or certificate rekey requests in accordance with 7.5.1 to 7.5.3.
6	The CA shall issue a signed notification to 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 when a certificate is issued. Where 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.

7.5.5 Certificate distribution

Control objective:
The CA shall 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. Trusted mechanisms include: a) collection – repository or online directory service; b) delivery – distributed using protected media (e.g. CD-ROM or ICC).
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	The integrity of the repository or alternative distribution mechanism shall be maintained and administered.
5	Where required, certificates shall be made available for retrieval only in those cases for which the subject's consent is obtained.
6	When cryptography is used to protect the CA public key, the private key used to generate the digital signature or the secret key used to compute the MAC or HMAC shall not be used for any other purpose.

7.5.6 Certificate revocation

Control objective:
The CA shall maintain controls to provide reasonable assurance that certificates are revoked in a timely manner as dictated by risk, based on authorized and validated certificate revocation requests.

Control procedures:	
1	The CA shall provide a means of rapid communication to facilitate the secure and authenticated revocation of the following: a) one or more certificates of one or more subjects; 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; c) all certificates issued by a CA, regardless of the public/private key pair used.
2	The CA shall verify or require that the RA verify the identity and authority of the entity requesting revocation of a certificate in accordance with the CP.
3	If an RA accepts revocation requests, the CA shall require that the RA submit signed certificate revocation requests to the CA in an authenticated manner in accordance with the CP.
4	If an RA accepts and forwards revocation requests to the CA, the CA shall provide a signed acknowledgement of the revocation request and confirmation of actions to the requesting RA.
5	The CA shall update the certificate revocation list (CRL) online certificate status protocol (OCSP) responder or other certificate status mechanisms in the timeframes specified within the CP and in accordance with the format defined in ISO 9594-8.
6	The CA shall record all certificate revocation requests and their outcome in an audit log, as specified in Annex F.
7	The CA or RA can provide an authenticated acknowledgement (signature or similar) of the revocation to the entity who perpetrated the revocation request.
8	Where certificate renewal is supported, when a certificate is revoked, all valid instances of the certificate shall also be revoked and shall never be reinstated.
9	The subject (and where applicable, the subscriber) of a revoked or suspended certificate shall be informed of the change of status of its certificate.
10	The subject (or RA) shall perform the following actions: — provide notification to other entities (e.g. relying parties, regulatory agencies); — investigate the security incident and take appropriate supplementary actions to limit exposure

7.5.7 Certificate suspension (if supported)

Control objective:
If certificate suspension is supported, the CA shall maintain controls to provide reasonable assurance that certificates are suspended in a timely manner as dictated by risk, based on authorized and validated certificate suspension requests.

Control procedures:	
1	In accordance with the CA's CPS, the CA provides a means of rapid communication, in place to facilitate the secure and authenticated suspension of the following: a) one or more certificates of one or more subjects; 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; c) all certificates issued by a CA, regardless of the public/private key pair used.
2	The CA shall verify or require that the RA verify the identity and authority of the entity requesting suspension and reactivation of a certificate in accordance with the CP.

3	If an RA accepts suspension requests, the RA shall submit signed certificate suspension requests to the CA in an authenticated manner in accordance with the CP.
4	The CA or RA shall notify the subject and, where applicable, the subscriber in the event of a certificate suspension.
5	Certificate suspension requests shall be processed and validated in accordance with the requirements of the CP.
6	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 timeframe determined by the CP.
7	Certificates shall be suspended only for the allowable length of time in accordance with the CP.
8	Once a certificate suspension (hold) has been issued, the suspension shall be handled in one of the following three ways: a) an entry for the suspended certificate remains on the CRL with no further action; b) the CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate; c) the suspended certificate is unsuspended and the entry removed from the CRL.
9	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. If the limit is reached the PA can be notified for further investigation.
10	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.
11	The CA shall verify or require that the RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted.
12	Certificate suspensions and the lifting of certificate suspensions shall be recorded in an audit log, as specified in Annex F.

7.5.8 Certificate validation services

Control objective:
The CA shall maintain controls to provide reasonable assurance that timely, complete and accurate certificate status information (including certificate revocation lists and other certificate status mechanisms) is made available 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: a) request response method – a request signed by 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); b) delivery method – a CRL signed by the CA and published within the policy's timeframe.
	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 archived 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, could 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.
8	Old CRLs shall be retained for the appropriate period of time specified in the CA's CP.
	Applicable control procedures where online certificate status mechanisms (e.g. OCSP) are used
9	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: a) the request message is well formed; b) the certificate status provider responder is configured to provide the requested service; 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; d) the certificate status provider's responder is able to locate the certificate and interpret its status. 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 of "unknown" can be returned.
10	All response messages shall be digitally signed and include all required data in accordance with the CP.

7.6 Controlled CA termination

Control objective:
The CA shall maintain controls to provide reasonable assurance that timely, complete and accurate information (including certificate revocation lists and other certificate status mechanisms) is made available to relevant entities (subscribers and relying parties or their agents, i.e. CVSPs) in accordance with the CP in the event of the termination of the CA for whatever reason

Control procedures:	
	Applicable control procedures where a CA is terminated
1	Establish an advisory board at the initiation of the Certification Authority with the responsibility of overseeing the termination of the CA or the termination of relationships with any other CA.
2	Address the termination of any back-up site used for business resumption
3	Ensure that the CA's public key and certificate are escrowed
4	Provide a capability to re-validate any subscriber's digital signature after the CA is terminated
5	Develop a termination plan to minimize disruption, including notification to subscribers, preserving records, transferring business to a reliable successor
6	Retention of the root CA database for a year

7.7 CA certificate life cycle management controls – subordinate CA certificate

Control objectives:-
The parent CA shall maintain controls to provide reasonable assurance that: — subordinate CA certificate requests are accurate, authenticated and approved; — subordinate CA certificate replacement (renewal and rekey) requests are accurate, authorized and complete; — new, renewed and rekeyed subordinate CA certificates are generated and issued in accordance with the CP; — upon issuance, complete and accurate subordinate CA certificates are available to relevant entities (subscribers and relying parties) in accordance with the CP; — subordinate CA certificates are revoked based on authorized and validated certificate revocation requests; — timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the CP.

Control procedures:	
	Subordinate CA (sub-CA) registration
1	The parent CP shall specify the requirements for submission of sub-CA certification requests.
2	The parent CA shall authenticate the sub-CA certificate request in accordance with the parent's CP.
3	The parent CA shall audit the sub-CA certificate applicant's compliance with the requirements of the parent CA's CP before approving a sub-CA certificate request, or alternatively the sub-CA shall present its CPS for audit.
	Sub-CA renewal
4	Where sub-CA certificate renewal is permitted, the parent CA's CP shall specify the requirements for submission of sub-CA renewal requests.
5	Where sub-CA certificate renewal is permitted, the parent CA shall authenticate the sub-CA certificate renewal request in accordance with the CA's CP.
	Sub-CA rekey
6	The parent CA's CP shall specify the requirements for submission of sub-CA rekey requests.
7	The parent CA shall authenticate the sub-CA certificate rekey request in accordance with the CP.
	Sub-CA certificate issuance
8	The parent CA shall generate certificates: a) using the appropriate certificate profile in accordance with the CP and ISO 9594-8 formatting rules; b) with the validity periods formatted in accordance with ISO 9594-8 and the CP; c) where extensions are used, with extension fields formatted in accordance with ISO 9594-8 and the CP.
9	The parent CA shall sign the sub-CA certificate with the parent CA's private signing key.
	Sub-CA certificate distribution
10	The parent CA shall make sub-CA certificates available to relevant entities (e.g. relying parties) using an established mechanism (e.g. a repository such as a directory) in accordance with the parent CA's CP.
	Sub-CA certificate revocation
11	The parent CA shall verify the identity and authority of the entity requesting revocation of a sub-CA certificate in accordance with the parent CA's CP.

12	The parent CA shall update the certificate revocation list (CRL) and other sub-CA certificate status mechanisms upon certificate revocation in accordance with the parent CA's CP.
	Sub-CA certificate status information processing
13	The parent CA shall make sub-CA certificate status information available to relying parties using an established mechanism (e.g. CRL, OCSP) in accordance with the parent CA's CP.

Annex A
(informative)

Management by certificate policy

A.1 Introduction and 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 RFC 3647[11], its predecessor RFC 2527[9], and provides further clarification on the use of certificate policies in a financial services 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 and/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, version 3 certificate.

The CP object identifier can be included in the following extensions in the X.509, version 3 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  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** shall 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 criticality indicator in each **certificatePolicies** certificate extension can be set to either critical or non-critical by the certificate issuer. If this extension is set to critical, the extension indicates that the certificate should only be used by a relying party for the purposes implied by its certificate policies. A particular CP can require the certificate-using system to process any qualifier values in a particular way, to further restrict or to expand the valid uses of a certificate.

If the certificate policies extension is set to non-critical, use of this extension does not necessarily constrain certificate-using systems to use the certificate in accordance with the policies listed in the certificate. But 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.

Policy qualifier types can be registered by any organization. The following policy qualifier types are defined in IETF RFC 2459[8], certificate and CRL profile:

a) The certification practice statement pointer qualifier contains a pointer to a certification practice statement (CPS) published by the CA. The pointer is in the form of a uniform resource locator (URL).

b) The user notice qualifier contains a text string that is to be displayed to a certificate user (including subscribers and relying parties) prior to the use of the certificate. The text string can be an IA5 string or a BMP string – a subset of the ISO/IEC 10646-1 multiple octet coded character set. A CA can invoke a procedure that requires that the certificate user acknowledges that the applicable terms and conditions have been disclosed or accepted.

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 shall 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, financial institutions 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 shall 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 shall 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).

Setting the certificate policies extension field as critical forces the application to check that acceptable certificate policies in the chain are present. It is therefore recommended that the certificate policies extension be implemented as a critical extension. This field is processed in concert with the policyConstraints extension (A.5.4) during the certification path validation, as described in ITU-T Recommendation X.509.

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 Types of certificate

The type of certificate that can be required is complex, with a wide variety of user needs requiring a range of different solutions. The policy authority can adopt a general-purpose strategy for a CP without usage restriction. Alternatively, a policy authority can construct certificate policies for specific purposes to restrict inappropriate usage or to limit liability.

Consequently, the main types of end-entity certificate are:

— application-specific (attribute-based) certificates: these certificates are issued to support specific applications, products and/or services where the requirements for authorization are explicit;

— generic certificates: a single certificate based on the authenticity of specific information proves the identity of the holder of a public key, which constitutes the basis for authorization.

A single certificate can be used to support multiple applications. The use of a single certificate will need to meet the requirements of the most highly classified application.

It is assumed that general-purpose certificates will predominate for subscribers because:

— ID-only based certificates are likely to become a commodity in the medium-to-long term;

— in the medium-to-long term, attribute-based or customized certificates can be a source of added value;

— the uses for digital signatures and certificates both internally and externally have yet to be fully exploited or developed.

The amount of assurance required directly correlates to the business risks for each entity in a transaction. The degree of assurance will more often than not vary according to the party's role and the appetite for risk. A “fit-for-purpose” approach is discussed in A.7. The early state of a market for trust services in general, combined with the technological immaturity of the marketplace, suggest that initial

efforts to define an all-encompassing system allowing for policy granularity is not a feasible option for the initial deployment.

It is recommended that generic certificates be issued to subscribers utilized to establish a system of minimum requirements for all categories of services for the initial stages for a PKI deployment. This approach takes into consideration the subsequent supplemental requirements that can be drawn up by the market for further categories of certificate policies and related trust services.

There are other types of certificate policies designated for specific purposes, such as server certificates and using certificates to create a PKI hierarchy.

A.7 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 project 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 is 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 could 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 in the context of financial services 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 financial institutions 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.8 Certificate policy provisions

A.8.1 General

This clause briefly describes the terms of a CP.

A.8.2 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 section 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 might be issued to private account holders only, relying parties shall have signed a relying party agreement with an approved or licensed entity as approved by the policy authority).

A.8.3 Obligations

The main responsibilities for each entity are stated in terms of their respective roles – policy authority, CA, subscriber, relying party and certificate validation service provider.

The policy authority is responsible for ensuring it conducts an efficient and trustworthy service in line with terms agreed with contracting parties or schemes. The CA is responsible for ensuring that certificates are issued in accordance with the CP. The CA is also responsible for ensuring that changes in certificate status are reflected in its own repositories and those of authorized certificate validation authorities within the specified time as stated in the CP.

The subscribing customer is responsible for protecting the access to the private keys in accordance with the terms of the subscriber agreement. This means that any access to the use of the private key is never revealed (e.g. PIN to unauthorized users). The subscriber is also required to inform the registration authority or agent if they believe that their key has been compromised.

A relying party should exercise reasonable judgement when deciding whether to rely upon a certificate, but shall only rely on a certificate that has not been revoked, suspended or expired, notwithstanding when the private key was used for the transaction.

A.8.4 Enforcement

The CP shall state the governing law, applicable contracts or schemes and methods for establishing definitive ruling where there are conflicting clauses or there are no documented provisions or set precedents.

A.8.5 Liability

This subclause concentrates on the liabilities of businesses to both the subscriber and the relying party.

The liabilities to the subscriber will always be covered by a contractual relationship. The terms and conditions of issue and use of a certificate are covered by the appropriate CP. These will be established before the subscriber obtains the certificate and can be designed to ensure that all anticipated liabilities are addressed and, if possible, limited.

The liabilities to the relying party are potentially more complicated. As stated previously, the relying party can have no contractual relationship with any of the CA/RA/repository, but can use the services of a known and trusted certificate validation service provider. The following three simple examples serve to illustrate the various ways in which liability could be controlled or limited.

— The CP can identify the circumstances in which the relying party needs to do no more than check the validity of the certificate's signature and that it is within its validity period. In such a case, analogous to a cheque guarantee card, the authenticity of the certificate is itself sufficient to rely on, although the policy can limit the liability on any particular "transaction." The value of the certificate, therefore, is seen by the relying party to be in that "guaranteed," yet limited, liability.

— In other circumstances the CP can require (but cannot force) the relying party to obtain an online validation of the certificate from the CA/RA (via a repository) before acceptance. In this way the

certificate acts purely as a means of identification with no inherent value. Each transaction is effectively authorized online, and there is no liability for unauthorized transactions.

— Where the relying party has control over the software/environment in which the relying party will use the certificate, a relying party agreement can be presented, which shall be actively accepted before the certificate can be used. Until this becomes a standard means of using certificates and is widely implemented in the commercial and freeware products such as browsers and email packages, this will not be a reliable way to limit liability.

A.8.6 Operational requirements

The following processes with specified timings should be stated:

— initial registration application including the type of identity credentials;

— certificate request, issuance and acceptance;

— certificate validation methods;

— certificate suspension and revocation together with reasons for certificate revocation and suspension (including who authorized, procedures described and notification).

A statement should be made on how certificate rollover will be managed (e.g. automatic or reverification of identity) or whether new key pairs shall be generated. A statement should also be made on how certificate modification, if supported, will be managed (e.g. what authentication procedures are required in order to modify the information in an existing certificate).

The technical security controls can be stated here that detail how the private/public key pair is generated and installed and the standards relevant to denote compliance. Controls to manage access to the private key are also given, together with notification on private key escrow, back-up and archiving.

The certificate profile should be appended to demonstrate what values should be placed in the respective fields and provide guidance on how to determine those values.

A.9 Certificate policy management

The CP shall show its unique name, its policy qualifier, the policy version, its status, the policy reference OID and its date of issue and, where appropriate, its date of expiry.

The CP should contain contact details of the policy authority, which include postal address, telephone numbers, business operating hours and possibly an email address for customer support.

Publication and repository contact details should be clearly shown together with methods for clarifying issues on:

— CP administration;

— confidentiality of policy information;

— change control process;

— notification of changes;

— identification credentials and registration process.

A CP should have a start date and, where possible, an expiry date. It can be difficult to manage issued certificates with various expiry dates without a policy expiry date.

It should also state where paper and electronic copies of the CP might be obtained.

The CP should describe the processes the policy authority invokes to check that a CA's CPS is capable of supporting the requirements of the CP.

The policy authority shall ensure that the controls specified in the CA's CPS are appropriate to support the CP.

A formal method of auditing the CA against its CPS within specified time periods (e.g. two years) should be agreed upon between the policy authority and the CA. If the CA wishes to vary the clauses in its CPS then this and an agreed method of dispute resolution is advised in order to resolve issues promptly.

Annex B
(informative)

Elements of a certification practice statement

B.1 General

A certification practice statement (CPS) should contain a reference to all components and subcomponents contained in this annex.

It is not necessary for a CPS to include a definitive statement for every such topic. A particular CPS can state "not in practice" for a component, subcomponent or element on which the particular CPS imposes no requirements. This will indicate to the reader that a conscious decision was made to include or exclude that topic. This facilitates comparison of certification practice statements when making decisions on the suitability of the practices to business applications. This annex follows the structure of RFC 2527[9], which has been superseded by RFC 3647[11]. A table cross-referencing the changes from RFC 2527 to RFC 3647 can be found in Annex E.

B.2 Introduction

B.2.1 General

The introduction component of a CPS has the following subcomponents:

— overview;

— identification;

— community and applicability;

— contact details.

B.2.2 Overview

This subcomponent provides a general introduction (e.g. general purpose of the practice statement).

B.2.3 Identification

This subcomponent provides any applicable names or other identifiers, including ASN.1 object identifiers.

B.2.4 Community and applicability

This subcomponent describes the types of entities that issue certificates or that are certified as subject CAs, the types of entities that perform RA functions and the types of entities that are certified as subject end entities or subscribers.

NOTE Examples of entities for subject CAs include subordinate organizations such as banks, bank branches or divisions, government agencies or departments. For example, suppose a bank claims that it issues CA certificates to its branches only. Then the user of a CA certificate issued by the bank can assume that the subject CA in the certificate is a branch of the bank. Examples of subject RA entities are customer service or data security departments. Examples of subject end entities include retail or wholesale bank customers, cardholders, individual investors, policyholders and employees.

This subcomponent also contains:

— a list of applications for which the issued certificates are suitable;

— a list of applications for which use of the issued certificates is limited, or a list of applications for which use of the issued certificates is prohibited.

B.2.5 Contact details

This subcomponent includes the name and mailing address of the authority that is responsible for the registration, maintenance and interpretation of this CPS. It also includes the name, electronic mail address, telephone number and fax number for all appropriate contact persons.

B.3 General provisions

B.3.1 General

This component specifies any applicable presumptions on a range of legal and general practice topics, including:

— obligations;

— liability;

— interpretation and enforcement;

— publication and repositories;

— compliance audit;

— confidentiality.

Each subcomponent may need to separately state provisions applying to the entity types: CA, repository, RA, subscriber and relying party.

B.3.2 Obligations

This subcomponent contains, for each entity type, any applicable provisions regarding the entity's obligations to other entities. Such provisions can include:

— CA and/or RA or certificate status provider obligations:

— notification of issuance of a certificate to the subscriber who is the subject of the certificate being issued;

— notification of issuance of a certificate to parties other than the subject of the certificate;

— notification of revocation or suspension of a certificate to the subscriber whose certificate is being revoked or suspended;

— notification of revocation or suspension of a certificate to parties other than the subject whose certificate is being revoked or suspended;

— subscriber obligations;

— accuracy of representations in certificate application;

— protection of the entity's private key;

— protection of the mechanism to enable the use of the private key (i.e. cardholder verification method);

— restrictions on private key and certificate use;

— notification upon private key compromise;

— relying party obligations:

— purposes for which certificate is used;

— digital signature verification responsibilities;

— revocation and suspension-checking responsibilities;

— acknowledgement of applicable liability caps and warranties;

— repository obligations;

— timely publication of certificates and revocation information;

— certificate status provider:

— to make validation service available and responsive within service level agreement levels;

— to validate certificate accurately.

B.3.3 Liability

This subcomponent contains, for each entity type, any applicable provisions regarding apportionment of liability, such as:

— warranties and limitations on warranties;

— kinds of damage covered (e.g. indirect, special, consequential, incidental, punitive, liquidated damage, negligence and fraud) and disclaimer;

— loss limitations (caps) per certificate or per transaction;

— other exclusions (e.g. acts of God, other party responsibilities).

B.3.4 Interpretation and enforcement

This subcomponent contains any applicable provisions regarding interpretation and enforcement of the CP or CPS, addressing such topics as:

— corporate security policy and procedures;

— governing law;

— severance of provisions, survival, merger and notice;

— dispute resolution procedures.

B.3.5 Publication and repositories

This subcomponent contains any applicable provisions regarding:

— CA obligations to make available information regarding its practices, its certificates and the current status of such certificates;

— frequency of publication;

— classification of published information including CP definitions, CPS, certificates, certificate status and CRLs;

— requirements pertaining to the use of repositories including online certificate status verification (if supported).

B.3.6 Compliance audit

This subcomponent addresses the following:

— frequency of compliance audit for each entity;

— auditor's relationship to the entity being audited (i.e. a statement that the auditor shall be independent);

— general list of topics covered under the compliance audit including CA environmental controls, key management controls and certificate life cycle management controls.

B.3.7 Confidentiality

This subcomponent addresses the following:

— types of information that should be kept confidential by CA or RA;

— types of information that are not considered confidential;

— who is entitled to be informed of reasons for revocation and suspension of certificates;

— policy on release of information to law enforcement officials;

— information that can be revealed as part of civil discovery to conform with regulatory requirements;

— conditions upon which CA or RA can disclose and to whom upon owner's request;

— any other circumstances under which confidential information can be disclosed.

B.4 Identification and authentication

B.4.1 General

This component describes the procedures used to authenticate a certificate applicant to a CA or RA prior to certificate issuance. It also describes how parties requesting rekey or revocation are authenticated. This component also addresses naming practices, including name ownership recognition and name dispute resolution.

This component has the following subcomponents:

— initial registration;

— routine rekey;

— rekey after revocation;

— revocation request;

— suspension request.

B.4.2 Initial registration

This subcomponent includes the following elements regarding identification and authentication procedures during entity registration or certificate issuance:

— types of names assigned to the subject;

NOTE 1 Examples include X.500 distinguished name, Internet email address and URL.

— whether names shall be meaningful or not;

NOTE 2 The term "meaningful" means that the name form has commonly understood semantics to determine identity of the person and/or organization. Directory names and RFC 822[7] names can be more or less meaningful.

— rules for interpreting various name forms;

— whether names shall be unique;

— how name claim disputes are resolved;

— recognition, authentication and role of trademarks;

— if and how the subject should prove possession of the companion private key for the public key being registered;

NOTE 3 Examples of proof include the issuing CA generating the key, or requiring the subject to send an electronically signed request or to sign a challenge.

— authentication requirements for organizational identity of subject (CA, RA or end entity);

NOTE 4 Types of organization identity authentication include articles of incorporation, duly signed corporate resolutions, a company seal and notarized documents.

— authentication requirements for a person acting on behalf of a subject (CA, RA or end entity);

NOTE 5 Types of individual identity authentication include physical recognition, knowledge of an individual, identification card biometrics (thumb print, 10 fingerprints, face, palm and retina scans), a driving license, a passport, voice recognition or an established employee authentication method.

— number of pieces of identification evidence required;

— how a CA or RA validates the pieces of identification evidence provided as genuine or the procedures for achieving this remotely;

— if the individual shall present personally to the authenticating CA or RA;

— how an individual as an organizational representative is authenticated and whether they are authorized (mandated) by the company to act on its behalf.

NOTE 6 Examples include duly signed authorization papers or corporate ID badge.

B.4.3 Routine rekey

This subcomponent describes the identification and authentication procedures for routine rekeying for each subject type (CA, RA and end entity).

The identification practice for routine rekey should be the same as the one for initial registration unless the expiring certificate is used for authentication prior to its expiration date. The rekey authentication may be accomplished using the techniques for initial identification and authorization or using digitally signed requests.

B.4.4 Rekey after revocation — no key compromise

This subcomponent describes the identification and authentication procedures for rekey for each subject type (CA, RA, CVSP and end entity) after the subject certificate has been revoked. If a certificate has been revoked then its status shall not be changed.

This identification and authentication practice should be the same as that for initial registration.

B.4.5 Revocation request

This subcomponent describes the identification and authentication procedures for a revocation request by each subject type (CA, RA and end entity) or other authorized party (as stated in the CP) or by a regulatory authority.

NOTE The identification practices for revocation request could be the same as that for initial registration since the same subject certificate needs to be revoked. The authentication practices could accept a revocation request digitally signed by subject. The authentication information used during initial registration could be acceptable for revocation request. Other less stringent authentication practices could be defined.

B.4.6 Suspension request

This subcomponent describes the identification and authentication procedures for a suspension request by each subject type (CA, RA and end entity) or other authorized party (as stated in the CP) or by a regulatory authority.

NOTE The identification practices for suspension request could be the same as that for initial registration since the same subject certificate needs to be suspended. The authentication practices could accept a suspension request digitally signed by subject. The authentication information used during initial registration could be acceptable for suspension request. Other less stringent authentication practices could be defined.

B.5 Operational requirements

B.5.1 General

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, CVSP or end entities with respect to various operational activities.

This component consists of the following subcomponents:

— certificate application;

— certificate issuance;

— certificate acceptance;

— certificate validation;

— certificate suspension and revocation;

— security audit procedures;

— records archival;

— key changeover;

— compromise and disaster recovery;

— CA termination.

Within each subcomponent, separate consideration may need to be given to issuing CA, repository, subject CAs, RAs and end entities.

B.5.2 Certificate application

This subcomponent is used to state requirements regarding subject enrolment and request for certificate issuance.

B.5.3 Certificate issuance

This subcomponent is used to state requirements regarding issuance of a certificate and notification to the applicant of such issuance.

B.5.4 Certificate acceptance

This subcomponent is used to state requirements regarding acceptance of an issued certificate and for consequent publication of certificates.

B.5.5 Certificate suspension, revocation and status management

This subcomponent addresses the following:

— conditions to be fulfilled under which a certificate may be revoked;

— who can request the revocation of the entity certificate;

— procedures used for certificate revocation request;

— revocation request grace period, if any, available to the subject;

— conditions to be fulfilled under which a certificate may be suspended;

— who can request the suspension of a certificate;

— procedures to request certificate suspension;

— how long the suspension may last;

— conditions to be fulfilled under which a suspended certificate may be returned to a live status;

— if a CRL mechanism is used, the issuance availability and frequency of updates;

— requirements on relying parties to check CRLs;

— online status checking availability and guaranteed response times;

— requirements on relying parties to perform online status checks;

— requirements on the certificate status provider to enable the authentication of a status response to a relying party;

— other forms of official suspension, revocation or certificate status notices available;

— a requirement on validation authorities and relying parties to check other forms of official suspension, revocation or certificate status notices;

— any variations on these stipulations when the suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation).

B.5.6 Security audit procedures

This subcomponent is used to describe event logging and audit systems. Elements include the following:

— types of event recorded;

NOTE Examples of audit events include requests to create a certificate, requests to suspend or revoke a certificate, key compromise notification, creation of a certificate, revocation of a certificate, issuance of a certificate, issuance of a CRL, issuance of key compromise CRL, establishment of trusted roles on the CA, actions of trusted personnel and changes to CA keys.

— frequency with which audit logs are processed or audited;

— period for which audit logs are kept;

— protection of audit logs;

— who can view audit logs and under what authority;

— protection against modification of audit log;

— protection against deletion of audit log;

— audit log back-up procedures;

— whether the audit log accumulation system is internal or external to the entity;

— whether the subject who caused an audit event to occur is notified of the audit action;

— vulnerability assessments.

B.5.7 Records archival

This subcomponent is used to describe general records archival (or records retention) policies, including the following:

— types of event recorded;

NOTE Examples of archive events include requests to create a certificate, requests to revoke a certificate, key compromise notification, creation of a certificate, revocation of a certificate, issuance of a certificate, issuance of a CRL, issuance of key compromise CRL and changes to CA keys.

— retention period for archive;

— protection of archive;

— who can view the archive;

— protection against modification of archive;

— protection against deletion of archive;

— archive back-up procedures;

— requirements for time-stamping of records;

— whether the archive collection system is internal or external;

— procedures to obtain and verify archive information.

B.5.8 Key changeover

This subcomponent describes the procedures to provide a new public key to a CA user.

B.5.9 Compromise and disaster recovery

This subcomponent describes requirements relating to notification and recovery procedures in the event of compromise of a CA's private key or disaster. Disaster recovery includes the revocation and reissue of all certificates that were signed with the CA's private key. Each of the following circumstances may need to be addressed separately.

— The recovery procedures used if computing resources, software and/or data are corrupted or suspected of being corrupted: these procedures describe how a secure environment is re-established, which certificates are revoked, whether the entity key is revoked, how the new entity public key is provided to the users and how the subjects are recertified.

— The recovery procedures used if the entity public key is revoked: these procedures describe how a secure environment is re-established, how the new entity public key is provided to the users and how the subjects are recertified.

— The recovery procedures used if the entity key is compromised: these procedures describe how a secure environment is re-established, how the new entity's public key is obtained and how the entity is recertified.

B.5.10 CA termination

This subcomponent describes requirements relating to procedures for termination and for notification of termination of a CA or RA, including the identity of the custodian of CA and RA archival records. Consideration should be given to what information should be retained from a regulatory and risk perspective.

B.6 Physical, procedural and personnel security controls

B.6.1 General

This component describes physical, procedural and personnel controls used by the issuing CA to perform securely the functions of key generation, subject authentication, certificate issuance, certificate revocation, audit and archival.

This component can also be used to define controls on repository, subject CAs, RAs and end entities. The controls for the subject CAs, RAs, and end entities can vary by entity.

These controls are crucial to trusting the certificates since lack of physical, procedural and personnel security may compromise CA operations resulting, for example, in the creation of certificates or CRLs with erroneous information or the compromise of the CA private key.

This component consists of three subcomponents:

— physical security controls;

— procedural controls;

— personnel security controls.

Within each subcomponent, separate consideration will, in general, need to be given to each entity type, i.e. issuing CA, repository, subject CAs, RAs and end entities.

B.6.2 Physical security controls

In this subcomponent, the physical controls on the facility housing the entity systems are described.

NOTE Examples of physical access controls include monitored facility, guarded facility, locked facility, access controlled using tokens, access controlled using biometrics and access controlled through an access list.

Topics addressed can include:

— site location and construction;

— physical access;

— cryptographic hardware;

— power and air conditioning;

— water exposures;

— fire prevention and protection;

— electromagnetic protection;

— media storage;

— waste disposal;

— off-site back-up.

B.6.3 Procedural controls

In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role.

NOTE Examples of the roles include system administrator, system security officer and system auditor. The duties of the system administrator are to configure, generate, boot and operate the system. The duties of the system security officer are to assign accounts and privileges. The duties of the system auditor are to set up system audit profile, perform audit file management and conduct audit review.

For each task identified for each role, it should also be stated how many individuals are required to perform the task (*n* out of *m* rule). Identification and authentication requirements for each role can also be defined.

B.6.4 Personnel security controls

This subcomponent addresses the following:

— background checks and clearance procedures required for the personnel filling the trusted roles;

The background checks can include clearance level (e.g. none, sensitive, confidential, secret, top secret) and the clearance granting authority name. In lieu of or in addition to a defined clearance, the background checks can include types of background information (e.g. name, place of birth, date of birth, home address, previous residences, previous employment and any other information that can help determine trustworthiness). The description should also include which information was verified and how.

— background checks and clearance procedures requirements for other personnel, including janitorial staff;

NOTE For example, the CP can impose personnel security requirements on the network system administrator responsible for a CA network access.

— training requirements and training procedures for each role;

— disciplinary procedures to be followed as a result of unauthorized actions, unauthorized use of authority and unauthorized use of entity systems by personnel;

Each authorized person should be accountable for his/her actions.

— controls on contracting personnel;

— documentation (e.g. operations or training manual) to be supplied to personnel.

B.7 Technical security controls

B.7.1 General

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g. PINs, passwords or manually held key shares). This component can also be used to impose constraints on registration authorities, repositories, subject CAs and end entities to protect their cryptographic keys and crucial security parameters. Secure key management is crucial to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, audit and archival. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on repositories, subject CAs, RAs and end entities.

This component has the following subcomponents:

— key pair generation and installation;

— private key protection in its storage and use;

— distribution of the private key where created by the CA or card bureau;

— other aspects of key pair management;

— activation data;

— computer security controls;

— life cycle security controls;

— network security controls;

— cryptographic module engineering controls.

B.7.2 Key pair generation and installation

Key pair generation and installation need to be considered for the issuing CA, repositories, subject CAs, RAs and subject end entities. For each of these types of entity, the following questions potentially need to be answered.

— Who generates the end entity's public, private key pair?

— How is the private key stored and provided securely to the end entity?

— How is the entity's public key provided securely to the certificate manufacturer?

— If the entity is a CA or certificate status provider (issuing or subject) how is the entity's public key certificate securely provided to the end entities?

— What are the algorithms used and what are key sizes?

— Who generates the public key parameters?

— Is the quality of the parameters checked during key generation?

— Is the key generation performed in hardware or software?

— For what purposes may the key be used, or for what purposes should usage of the key be restricted? (For X.509 certificates, these purposes should map to the key usage flags in the Version 3, X.509 certificates.)

B.7.3 Private key protection

Requirements for private key protection need to be considered for the issuing CA, repositories, subject CAs, RAs and subject end entities. For each of these types of entity, the control requirements can be different and to enable this to be determined the following questions potentially need to be answered.

— What standards, if any, are required for the module used to generate the keys? For example, are the keys certified by the infrastructure required to be generated using a module compliant with the FIPS 140-2? If so, what is the required FIPS 140-2 level of the module?

— Is the private key under *n* out of *m* multi-person control? If yes, provide *n* and *m* (two-person control is a special case of *n* out of *m*, where $n = m = 2$).

The *n* out of *m* rule allows a key or key activation data to be split in *m* parts. The *m* parts may be given to *m* different individuals. Any *n* parts out of the *m* parts may be used to fully reconstitute the key, but having any $n-1$ parts provides one with no information about the key.

— Is the private key escrowed? If so, who is the escrow agent, what form is the key escrowed in (examples include plaintext, encrypted, split key) and what are the security controls on the escrow system?

A key can be escrowed, backed up or archived. Each of these functions has a different purpose. Thus, a key may go through any subset of these functions depending on the requirements. The purpose of escrow is to allow a third party (such as an organization or government) to legally obtain the key without the cooperation of the subject. The purpose of back-up is to allow the subject to reconstitute the key in case of the destruction of the key. The purpose of archive is to provide for reuse of the key in future (e.g. use the private key to decrypt a document).

— Is the private key backed up? If so, who is the back-up agent, what form is the key backed up in (examples include plaintext, encrypted, split key) and what are the security controls on the back-up system?

— Is the private key archived? If so, who is the archival agent, what form is the key archived in (examples include plaintext, encrypted, split key) and what are the security controls on the archival system?

— Who enters the private key in the cryptographic module? In what form (i.e. plaintext, encrypted or split key)? How is the private key stored in the module (i.e. plaintext, encrypted or split key)?

— Who can activate (use) the private key? What actions shall be performed to activate the private key (e.g. login, power on, supply PIN, insert token/key, automatic)? Once the key is activated, is the key active for an indefinite period, active for one time or active for a defined time period?

— Who can deactivate the private key and how? Examples of how might include logout, power off, remove token/key, automatic or time expiration.

— Who can destroy the private key and how? Examples of how might include token surrender, token destruction or key overwrite.

B.7.4 Other aspects of key pair management

Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs and subject end entities. For each of these types of entity, the following questions potentially need to be answered.

— Is the public-key archived? If so, who is the archival agent and what are the security controls on the archival system? The archival system should provide integrity controls other than digital signatures since the archival period may be greater than the cryptanalysis period for the key and the archive requires tamper protection, which is not provided by digital signatures.

— What are the usage periods, or active lifetimes, for the public and the private key respectively?

B.7.5 Activation data

Access to the private key needs to be protected initially and throughout its continued use while it is still valid. Activation data are used in the authentication mechanism to validate the private key owner. Activation data refer to data values other than keys that are required to operate cryptographic modules and that need to be protected. Protection of activation data potentially needs to be considered for the issuing CA, subject CAs, RAs and end entities. Such consideration potentially needs to address the entire life cycle of the activation data from generation through archival and destruction. For each of the entity types (issuing CA, repository, subject CA, RA and end entity) all of the questions listed in B.7.2 to B.7.4 potentially need to be answered with respect to activation data rather than with respect to keys.

NOTE Examples of activation data are a PIN, pass phrase or biometric.

B.7.6 Computer security controls

This subcomponent is used to describe computer security controls such as use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object reuse, audit, identification and authentication, trusted path, functional testing, security testing and penetration testing. Product assurance may also be addressed.

B.7.7 Life cycle security controls

This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security and configuration management security during product maintenance, software engineering practices, software development methodology, modularity and layering, use of failsafe design and implementation techniques (e.g. defensive programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware and hardware to ensure their correct operation.

B.7.8 Network security controls

This subcomponent addresses network security related controls, including firewalls.

B.7.9 Cryptographic mechanism engineering controls

This subcomponent addresses the following aspects of a cryptographic module: identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility and self tests. Requirements can be expressed through reference to a standard such as FIPS 140-2.

A cryptographic mechanism is a combination of hardware and software and, where specific devices are used, associated firmware. The compliance description should be specific and detailed. For example, for each FIPS 140-2 requirement, describe the level and state whether an accredited laboratory has certified the level.

B.8 Certificate and CRL profiles

B.8.1 General

This component is used to specify the certificate format and, if CRLs are used, the CRL format. Assuming use of the X.509 certificate and CRL formats, this includes information on profiles, versions and extensions used and whether they need to be digitally signed.

This component has three subcomponents:

— certificate profile;

— CRL profile;

— OCSP profile.

B.8.2 Certificate profile

This subcomponent addresses such topics as:

— version number(s) supported;

— certificate extensions populated and their criticality;

— cryptographic algorithm object identifiers;

— name forms used for the CA, RA and end entity names;

— name constraints used and the name forms used in the name constraints;

— applicable certificate policy object identifier(s);

— usage of the policy constraints extension;

— policy qualifiers syntax and semantics;

— processing semantics for the critical certificate policy extension;

— contents and usage of non-standard extensions.

B.8.3 CRL profile

This subcomponent addresses such topics as:

— version numbers supported for CRLs;

— the availability and frequency of CRL updates;

— whether the CRLs require to be digitally signed;

— CRL and CRL entry extensions populated and their criticality.

B.8.4 OCSP profile

If applicable, this subcomponent addresses such topics as:

— OCSP request requirements;

— definitive response message requirements;

— the availability and guaranteed response times;

— whether the status responses require to be digitally signed;

— error message requirements.

B.9 Practices administration

B.9.1 General

This component is used to specify how practices will be maintained.

It contains the following subcomponents:

— change procedures;

— publication and notification procedures;

— CP compliance.

B.9.2 Change procedures

It will occasionally be necessary to change certificate policies and certification practice statements. Some of these changes will not materially reduce the assurance that a CP or its implementation provides, and will be judged by the policy administrator as not changing the acceptability of certificates asserting the policy for the purposes for which they have been used. Such changes to certificate policies and certification practice statements need not require a change in the CP object identifier or the CPS pointer (URL). Other changes to a CP and CPS will change the acceptability of certificates for specific purposes, and these changes will require changes to the CP object identifier or CPS pointer (URL).

This subcomponent contains the following information.

— A list of components, subcomponents and/or elements thereof that can be changed without notification and without changes to the CP object identifier or CPS pointer (URL).

— A list of components, subcomponents and/or elements thereof that can change following a notification period without changing the CP object identifier or CPS pointer (URL). The procedures to be used to notify interested parties (e.g. relying parties, certification authorities) of the CP or certification practice statement changes are described. The description of notification procedures includes the notification mechanism, notification period for comments, mechanism to receive, review and incorporate the comments, mechanism for final changes to the policy and the period before final changes become effective.

— A list of components, subcomponents and/or elements, changes to which require a change in CP object identifier or CPS pointer (URL).

B.9.3 Publication and notification procedures

This subcomponent contains the following elements:

— a list of components, subcomponents and elements thereof that exist but that are not made publicly available;

An organization may choose not to make public some of its security controls, clearance procedures or some others elements, due to their sensitivity.

— descriptions of mechanisms used to distribute the CP or make it available, including access controls.

B.9.4 CP compliance

This subcomponent describes the processes to check that a CPS complies with the requirements of the CP.

Annex C
(informative)

Object identifiers (OID)

C.1 Why have an OID?

An OID is required so that relying party software can mechanically identify a CP (e.g. the CP document applicable to the root CA, which establishes one or more of the policy domains). Each subordinate CA would need an OID to identify their CPS.

C.2 What is an OID?

An object identifier (OID) is a unique series of integers that unambiguously identifies an information object. The ASN.1 standards define an information object as a "well-defined piece of information, definition or specification which requires a name in order to identify its use in an instance of communication." Object identifiers can be used to provide a name for anything, including a CP, CPS, cryptographic algorithm, business, organization, file format, role, product, device, document version or standard.

The ISO/TC 68 organization is identified by the object identifier value 1.3.133. This value is the TC 68 "arc", the OID value which TC 68 controls as registrar and under which TC 68 is authorized by ISO to assign object identifiers. TC 68 member countries are identified under the OID 1.3.133.16, and each TC 68 member country has been assigned their own OID, for which they are the solely responsible registrar. OIDs can be obtained from the TC 68 Secretariat or from member countries that elect to assign values.

The set of all ISO/TC 68 standards is identified by the OID 1.3.133.17. This document is identified by the OID value 1.3.133.17.21188. OIDs can be communicated in any number of ways, by voice, by handwriting on paper or by a computer program, so the form of representation of these values can vary widely. The OID for this document can be represented in a binary format convenient for use by an application program, or represented using the ASN.1 basic value notation as "iso(1) identified-organization(3) tc68(133) standard(17) pki-cp-cps(21188)", or represented using the ASN.1 XML value notation as the XML markup value "<pki-cp-cps> 1.3.133.17.21188 </pki-cp-cps>".

It is envisaged that policy OIDs will be embedded in digital certificates so that PKI service providers, end entities and others can determine the set of rules under which an issuer/certificate manufacturer has generated a certificate. A standard set of CP OIDs could enable the automated processing of policy and practice information by digital certificate application programs. An object identifier should be obtained and registered for each certificate policy to uniquely identify that certificate policy. The typical way to obtain an OID is to go to the appropriate national registration authority for OIDs.

C.3 Registration of OIDs

Recommendation X.660 of ISO/IEC 9834-1:1993 defines the general procedures for the operation of registration authorities. The current International Standard was approved jointly by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU).

These international standards organizations control all of the top level OID arcs, the values that can appear in the first position of any OID integer series. These values are represented as the OID values itu-t(0), "iso(1)" and "joint-iso-itu-t(2)" and form the root of a registration-hierarchical-name-tree (RH-name-tree) of all possible OID values. The leaf and non-leaf nodes of this tree correspond to objects that

are registered. Non-leaf nodes correspond to registration authorities whose registration responsibility has been delegated to them by their superior node.

The international standards organizations delegate the management of assigned arcs to other responsible bodies who serve as registrars. ISO has done so by assigning an arc to TC 68. To guarantee that no OID was assigned more than once, TC 68 then designed a schema for managing the OIDs that it would assign under its arc. TC 68 then formed an object identifier tree by assigning OID values under its arc. It chose to delegate management of registration responsibility to nodes under its arc by assigning an arc to each of its member countries. This ensures that OID assignments by member countries are unique and never collide with assignments made by other registration authorities, and that each member country can assign OIDs independent of TC 68 and of all other member countries.

C.4 Why do you need an OID and how should they be managed?

An OID plus other components are used to manage access to directory resources. The OID is also embedded in a certificate extension. However, a challenging issue is how to manage change to the CP document. As a hash is involved, each time the CP document is changed then the OID that names the CP document could be changed. This is not very satisfactory. Alternatively, as the hash identifies the version of the CP document, then the same OID could be kept and the hash changed.