

Information technology — Public key infrastructure — Practices and policy framework

National foreword

This British Standard is the UK implementation of ISO/IEC 27099:2022.

The UK participation in its preparation was entrusted to Technical Committee IST/33/4, Security Controls and Services.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2022
Published by BSI Standards Limited 2022

ISBN 978 0 539 03435 6

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 September 2022.

Amendments/corrigenda issued since publication

Date	Text affected
------	---------------

INTERNATIONAL STANDARD

ISO
27099

First edition
2022-07-08

Information technology — Public key infrastructure — Practices and policy framework



Reference number
ISO 27099:2022(E)
Documents
Document Sharing Hub
© ISO 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO 2022, Published in Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

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

Contents

Page

Foreword	v
Introduction	vi
1 Scope	1
2 Normative references	1
3 Terms and definitions	1
4 Abbreviated terms	8
5 Public key infrastructure (PKI) general concepts	8
5.1 General	8
5.2 What is PKI?	9
5.2.1 General	9
5.2.2 Public key infrastructure process flow	10
5.3 Use of PKI Service components within example business flows	10
5.3.1 General	10
5.3.2 Illustration of certificate application in a contractual PKI environment	10
5.4 Certification authority (CA)	13
5.5 Business perspectives	14
5.5.1 General	14
5.5.2 Business risks	14
5.5.3 Applicability	14
5.5.4 Legal issues	14
5.5.5 Regulatory issues	15
5.5.6 Business usage issues	15
5.5.7 Interoperability issues	15
5.6 Certificate policy (CP)	16
5.6.1 General	16
5.6.2 Policy Authority and certificate policy usage	17
5.6.3 Certificate policies within a hierarchy of trust	17
5.6.4 Certificate status	18
5.7 Certification practice statement (CPS)	19
5.7.1 General	19
5.7.2 CPS creation	19
5.7.3 Purpose	19
5.7.4 Level of specificity	19
5.7.5 Approach	20
5.7.6 Audience and access	20
5.8 Agreements	20
5.9 Time-stamping	20
5.10 Trust models	21
5.10.1 Trust model considerations	21
5.10.2 Wildcard certificate considerations	24
5.10.3 Relying party considerations	24
5.11 Component services	25
5.12 PKI hierarchies and independently managed CAs	27
5.13 Root CA	27
5.13.1 General	27
5.13.2 CA relationships and PKI hierarchies	27
6 Certificate policy (CP), certification practice statement (CPS) and their relationship to information security management system (ISMS)	28
6.1 General	28
6.2 Certificate policy (CP) guidance	28
6.3 Certification practice statement (CPS) guidance	30
7 Certification authority objectives and controls	31

7.1	General.....	30
7.2	Certification practice statement and certificate policy management.....	31
7.2.1	Certificate policy management.....	31
7.2.2	CPS and CA management.....	32
7.2.3	Subscriber and relying party agreements.....	33
7.3	Information security.....	34
7.4	Asset classification and management.....	35
7.5	Human resources security.....	36
7.6	Physical and environmental security.....	37
7.7	Operations security.....	40
7.8	Access control.....	41
7.9	System acquisition development and maintenance.....	44
7.10	Business continuity management.....	44
7.11	Monitoring, conformance and compliance.....	46
7.12	Audit journal security assurance.....	47
7.13	CA key life cycle management controls.....	51
7.13.1	CA key generation.....	51
7.13.2	CA key storage, back-up, and recovery.....	53
7.13.3	CA public key distribution.....	55
7.13.4	CA key usage.....	55
7.13.5	CA key archival and destruction.....	56
7.13.6	CA key compromise.....	56
7.14	Subject key life cycle management controls.....	58
7.14.1	CA-provided subject key generation services (if supported).....	58
7.14.2	CA-provided subject key storage and recovery services (if supported).....	59
7.14.3	Hardware token life cycle management if outsourced to an external service (if supported).....	60
7.14.4	Subject key management, if supported.....	62
7.15	Certificate life cycle management controls.....	63
7.15.1	Subject registration.....	63
7.15.2	Certificate renewal (if supported).....	64
7.15.3	Certificate rekey.....	65
7.15.4	Certificate issuance.....	67
7.15.5	Certificate distribution.....	67
7.15.6	Certificate revocation.....	68
7.15.7	Certificate suspension (if supported).....	68
7.15.8	Revocation status information service.....	71
7.15.9	Controlled CA termination.....	72
7.16	Root CA controls.....	73
7.16.1	Physical and environmental security.....	73
7.16.2	Operations security.....	73
7.16.3	Access control.....	74
7.16.4	Root CA key generation.....	74
7.16.5	Generation of root CA keys script requirements.....	75
7.16.6	Root CA public key distribution.....	75
7.16.7	Root CA key compromise.....	76
7.17	CA certificate life cycle management controls – subordinate CA certificate.....	76
Annex A (informative) Management by certificate policy.....		77
Annex B (informative) CA key generation ceremony.....		84
Annex C (informative) Certification authority audit journal contents and use.....		88
Annex D (informative) Certificate and PKI roles.....		91
Annex E (informative) Changes to ISO 21188:2018 to produce ISO/IEC 27099.....		97
Bibliography.....		99

Foreword

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

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

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

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

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

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

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

Introduction

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

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

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

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

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

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

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

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

Information technology — Public key infrastructure — Practices and policy framework

1 Scope

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

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

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

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

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

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

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 9594-8, *Information technology — Open systems interconnection — Part 8: The Directory: Public-key and attribute certificate frameworks*

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

3 Terms and definitions

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

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

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

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

3.1 access point

point at which the user may connect to the network or facility

3.2 activation data

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

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

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

3.3 audit journal audit log

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

3.4 authentication

provision of assurance that a claimed identity of an entity is correct

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

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

3.5 CA certificate

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

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

3.6 card bureau

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

3.7 certificate

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

3.8 certificate suspension certificate hold

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

3.9 certificate issuer

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

3.10 certificate management

process that covers the complete lifecycle from the initialization phase to the issuing phase to the cancellation phase

3.11

certificate manufacturer

CM

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

3.12

certificate policy

CP

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

3.13

certificate profile

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

3.14

certificate rekey

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

3.15

certificate renewal

rollover

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

3.16

certification

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

3.17

certification authority

CA

issuing CA

entity (3.28) that is identified as the issuer of a public key certificate

3.18

certification path

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

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

3.19

certification practice statement

CPS

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

3.20

certification request

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

3.21

certificate revocation status

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

3.22

certificate validity

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

3.23

certificate validity period

bounded period of time that the *certificate* ([3.7](#)) is deemed fit for intended use

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

3.24

compromise

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

3.25

cross certification

certification of each other's public keys by two CAs ([3.17](#))

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

3.26

digital signature

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

3.27

end entity

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

3.28

entity

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

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

3.29

fingerprint

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

3.30

hardware token

device which generates, uses, and stores cryptographic keys in a secure manner

3.31

key escrow

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

3.32

key recovery

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

3.33

multiple control

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

3.34

object identifier

OID

unique series of integers that unambiguously identifies an information object

3.35

online certificate status mechanism

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

3.36

online certificate status protocol

OCSP

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

3.37

PKI disclosure statement

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

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

3.38

PKI trust service provider

one or more certification authorities providing a trust service with coherent policies and practices.

3.39

policy authority

PA

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

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

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

3.40

policy mapping

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

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

3.41

policy qualifier

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

3.42
public key infrastructure
PKI

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

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

3.43
PKI trust service provider
trust service provider

trusted provider of services which support the use of public key certificates

3.44
registration authority
RA

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

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

3.45
registration request

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

3.46
relying party
RP

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

3.47
relying party agreement
RPA

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

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

3.48
repository

system for storage and distribution of certificates and related information

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

3.49
root CA

CA at the apex of a CA certificate hierarchy

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

3.50

secure cryptographic device

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

[SOURCE: ETSI TR 119 001]

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

3.51

signature validation

verification and confirmation that a digital signature is valid

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

3.52

signature verification

check of the cryptographic value of a signature using data

3.53

subject

entity that controls the asymmetric key pair and may also be a *relying party* ([3.46](#))

3.54

subordinate CA

sub-CA

intermediate CA

CA ([3.17](#)) that is lower relative to another CA in the CA hierarchy

3.55

subscriber

entity subscribing with a *certification authority* ([3.17](#)) on behalf of one or more subjects

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

- i) an employee of the subscriber, or
- ii) an authorized agent of the subscriber

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

3.56

tamper-evident

evidence that an attack has been attempted

3.57

terms and conditions

collection of all documents issued by the CA which define the duties and rights of the PKI members

3.58

trust anchor

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

3.59

trusted role

job function that performs critical functions which, if performed unsatisfactorily, can have an adverse impact upon the degree of trust provided by the CA ([3.17](#))

3.60

trust service

electronic service which enhances trust and confidence in electronic transactions

3.61

validation service request

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

4 Abbreviated terms

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

5 Public key infrastructure (PKI) general concepts

5.1 General

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

5.2 What is PKI?

5.2.1 General

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

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

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

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

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

- a) **Closed environment:** all entities (certificate subjects and relying parties) adhere to a single Organization's trust service and share at least one certificate policy. An entity adhering to a trust service may act as a relying party or subscriber for certificates for itself or on behalf of other certificate subjects. In this case, subscribers and certificate subjects may be distinct entities bound by a business relationship which is outside the scope of this document.
- b) **Contractual environment:** certificate subjects and relying parties can have separate TSPs. TSPs are bound by differing forms of contract covering certificate use. These forms comprise:
 - 1) multilateral, under agreed rules, with a single certificate policy;
 - 2) bilateral cross certification that can use different certificate policies;
 - 3) accreditation bridge that can recognize different certificate policies through a central organization or entity. This can be realized by the central organization publishing a trust list of certificate policies, or of certification authorities, which conform to common policy requirements.

See [Figure 1](#) and [Table 1](#).

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

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

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

See [Annex D](#) for a general description of the roles of certificates and PKI components.

5.2.2 Public key infrastructure process flow

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

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

5.3 Use of PKI Service components within example business flows

5.3.1 General

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

5.3.2 Illustration of certificate application in a contractual PKI environment

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

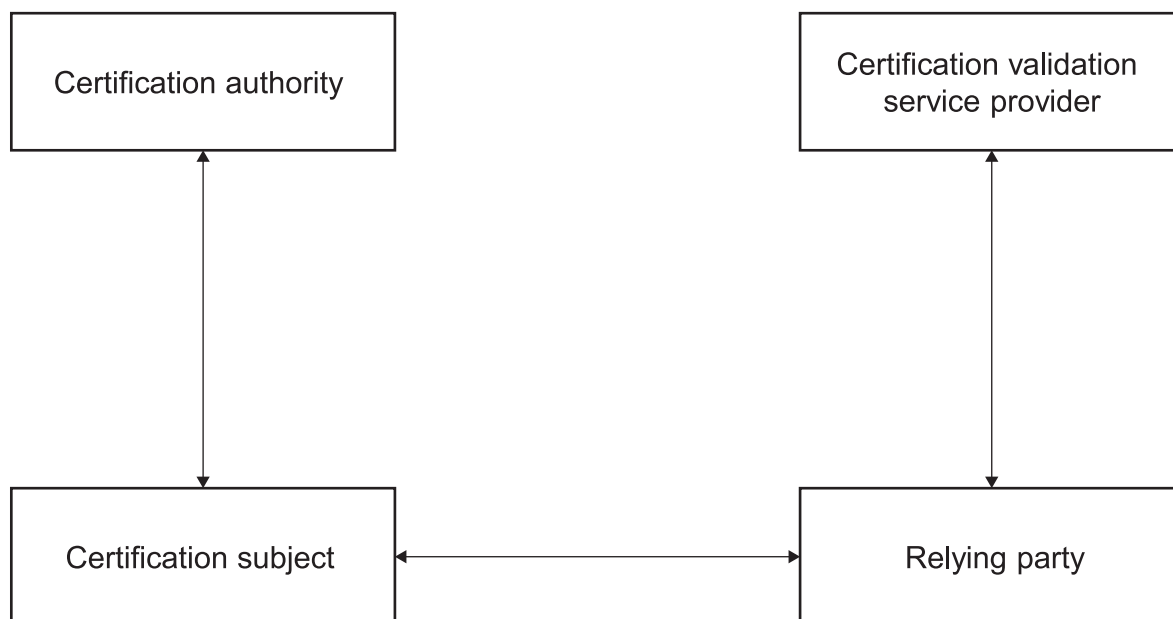


Figure 1 — Four entities in a contractual environment

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

These service components can be used for example as in the illustrative business processes given in [Table 1](#):

Table 1 — Certificate application scenarios in a contractual environment

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

	Sample scenario	Sample requirements	PKI operations
		— Message integrity.	— Organization requests certificate generation service component to obtain new certificate for the employee prior to sending any messages — Employee/sender digitally signs the email message — Recipient checks digital signature.
		— Confidentiality protection for message contents.	— Organization requests certificate generation service component to obtain new certificate for the employee prior to sending any messages — Sender fetches the recipient's certificate from a shared directory — Sender checks the certificate validity including its revocation status — 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 requests certificate generation service component to provide new certificate for the employee prior to sending any messages — Customer digitally signs purchase order with private key.
			— Recipient validates sender's certificate including status, certificate checking the revocation.
			— Merchant verifies digital signature.
3	Customer receives invoice from merchant.	— Message authentication.	— Check digital signature and validate certificate including checking the certificate revocation status.

	Sample scenario	Sample requirements	PKI operations
4	An existing customer using an e-banking service to send high value payment instructions to bank.	— Strong mutual authentication. — Message integrity. — Confidentiality.	— Customer requests certificate generation service component to provide new certificate for the employee prior to sending any messages — Customer validates bank's server certificate including checking the certificate revocation status — Bank validates customer's certificate including checking the certificate revocation status.
			— Bank verifies digital signature.
			— Customer fetches Bank's certificate from repository — Sender checks the certificate validity including its revocation status — Customer encrypts message using Bank's public key — Bank decrypts message using Bank's private key.

5.4 Certification authority (CA)

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

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

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

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

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

- Entities (including CAs) can use these certificates to authenticate themselves to relying parties. Hence, authentication can involve a chain of certificates. The verification of a chain of certificates begins with the trusted CA public key and ends with the certificate being validated. The trusted CA public key is to be obtained and authenticated by some means other than by the use of certificates. This is to ensure that the process begins securely. See ISO/IEC 9594-8.
- Once a certificate has been generated, the integrity of its contents is protected. This document does not require that certificates be given confidentiality protection. A valid copy of the CA's public key

and the identity used as the certificate issuer is required by the relying party in order to validate a certificate.

- To communicate outside the root CA's domain, the root CA cross-certifies with the desired remote domain. Certification path validation then involves building a chain of certificates from the remote entity to the root CA by way of the cross-certified remote CA.
- In a non-hierarchical architecture, independent CAs can cross-certify each other by issuing certificates to each other. This results in a general network of trust relationships between CAs and allows each group (such as a retail credit authorization network, a clearing house, an organization, or a subgroup thereof) to have its own CA. An entity uses the public key of a selected CA for its trusted CA public key. The certification path consists of those certificates that chain back from the certificate being validated to the trusted CA of the relying party.
- In a bridge architecture, two or more independent hierarchical architectures are interconnected by a common bridge CA which cross certifies with each root CA. The separate root CAs are peers to each other and the bridge CA such that they do not need to cross certify with each other. The bridge CA allows a relying party in one hierarchical architecture to validate the certificate chain from another hierarchical architecture.
- A bridge can be realized by a common trusted authority issuing a list of trusted certification authorities.
- A compromise of the private key of a CA compromises all entities certified by that CA, because the holder of that private key can generate fraudulent certificates and then masquerade as one or more end entities or through cross-certification with one or more entities. Failure to provide compensating controls to deal with the possibility of compromise of transactions in a network can have catastrophic effects on organisations and their customers.
- Two or more CAs can join a common scheme for mutual recognition, e.g. implemented by a trust list. See also [5.10.1](#) for further discussion on trust models.

5.5 Business perspectives

5.5.1 General

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

5.5.2 Business risks

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

5.5.3 Applicability

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

5.5.4 Legal issues

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

submission of claims and for resolution of disputes. It specifies any conditions a relying party should fulfil or actions a relying party should perform before being authorized to rely on a certificate and its assertions.

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

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

5.5.5 Regulatory issues

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

5.5.6 Business usage issues

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

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

5.5.7 Interoperability issues

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

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

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

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

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

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

- a) A CP can apply more broadly than to just a single organizational unit or single organization. If a particular CP is widely recognized, it has great potential as the basis of automated certificate acceptance in many systems.
- b) Organisations that operate public or inter-organizational certification authorities should document their own practices in CPSs. The CPS is one of the organization's means of protecting itself and positioning its relationships with subscribers and other entities.
- c) Technical implementation can differ due to interpretation of standards and protocols by the PKI integrators. A technical comparison takes place within the PKI environment to ensure technical interoperability.

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

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

5.6 Certificate policy (CP)

5.6.1 General

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

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

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

The purpose of a CP includes:

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

It is recommended that the CP is based on IETF RFC 3647. Controls are defined in [Clause 7](#).

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

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

5.6.2 Policy Authority and certificate policy usage

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

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

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

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

- a) subscription to the certificate policy for specific functional applications (e.g. server identification certificate for customer to authenticate their online service provider);
- b) subscription to the certificate policy that matches the business application (e.g. customer signing a purchasing order from a merchant);
- c) subscription to the certificate policy that matches a generic security application with a defined environment within prespecified restrictions (e.g. providing confidentiality protection on all message types to certificate subject across the Internet).

5.6.3 Certificate policies within a hierarchy of trust

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

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

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

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

- a) certificate policy for identifying the root CA with its implied self-signed certificate (certificates issued under Policy A in [Figure 2](#));
- b) certificate policy for identifying a subordinate CA established under the root CA or another subordinate CA. To sign the public keys of the subordinate or intermediate CAs, the root CA acting as the ultimate parent in the CA hierarchy in the organization (certificates issued under Policy B in [Figure 2](#)).

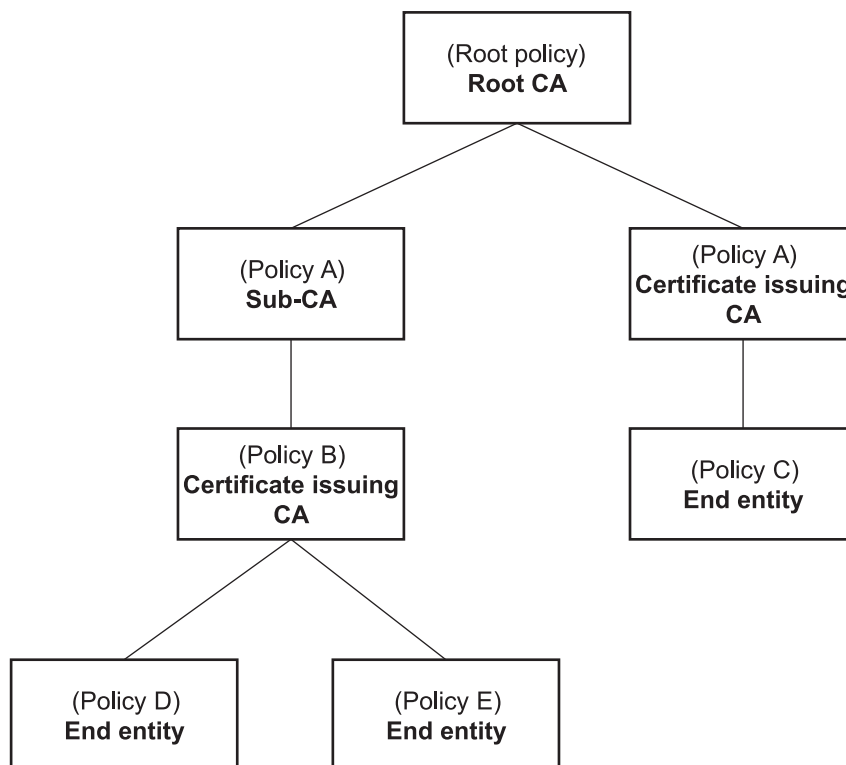


Figure 2 — Root hierarchy creates a hierarchy of trust

5.6.4 Certificate status

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

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

- a) pre-valid - not yet operational; if the certificate expresses a validity period, the given time is prior to the commencement of the validity period;
- b) live - operational; if the certificate expresses a validity period, the given time is during the validity period;
- c) suspended - not operational; if the certificate expresses a validity period, the given time is during the validity period;
- d) revoked - not operational; if the certificate expresses a validity period, the given time is during the validity period;
- e) expired - not operational; if the certificate expresses a validity period, the given time is after the validity period.

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

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

5.7 Certification practice statement (CPS)

5.7.1 General

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

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

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

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

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

5.7.2 CPS creation

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

5.7.3 Purpose

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

5.7.4 Level of specificity

A certificate policy is prescriptive.

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

5.7.5 Approach

The CP is based upon known business requirements.

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

5.7.6 Audience and access

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

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

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

5.8 Agreements

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

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

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

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

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

5.9 Time-stamping

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

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

There are two aspects of certificate usage where timing can be of particular importance. Firstly, trust services are based on certificates which have a validity period. If a signature is verified after the expiry of the signing key certificate, the validity of the signature cannot be ensured. Secondly, if a certificate is revoked then any use of the certificate after the time that it is revoked should be considered to be

invalid. Thus, if there is significant time between the application of a certificate in securing data and the checking of the validity of the certificate, for example when applying a digital signature to stored data, it is important to be sure of the time at which the signature was applied. If it can be confirmed that a signature was created before the supporting certificate expired or was revoked, then the validity of the signature can be ensured long after either of those events. It is for the relying party to determine whether they accept the risk associated with a certificate that can have expired or been revoked in the interim period.

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

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

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

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

5.10 Trust models

5.10.1 Trust model considerations

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

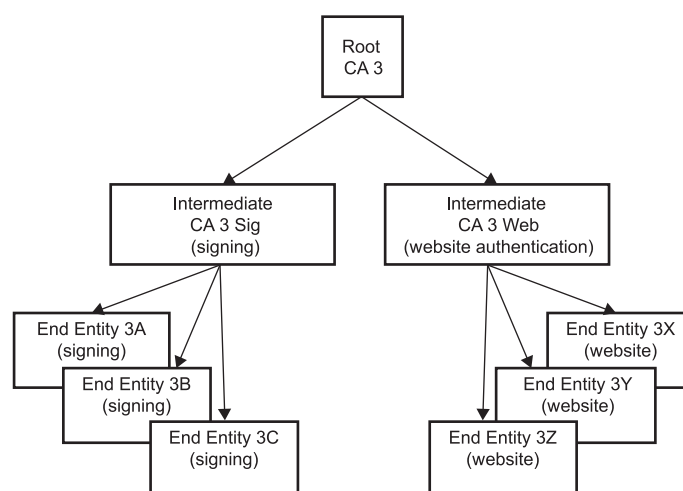


Figure 3 — Hierarchical CA trust relationships

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

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

a) Bridge CA

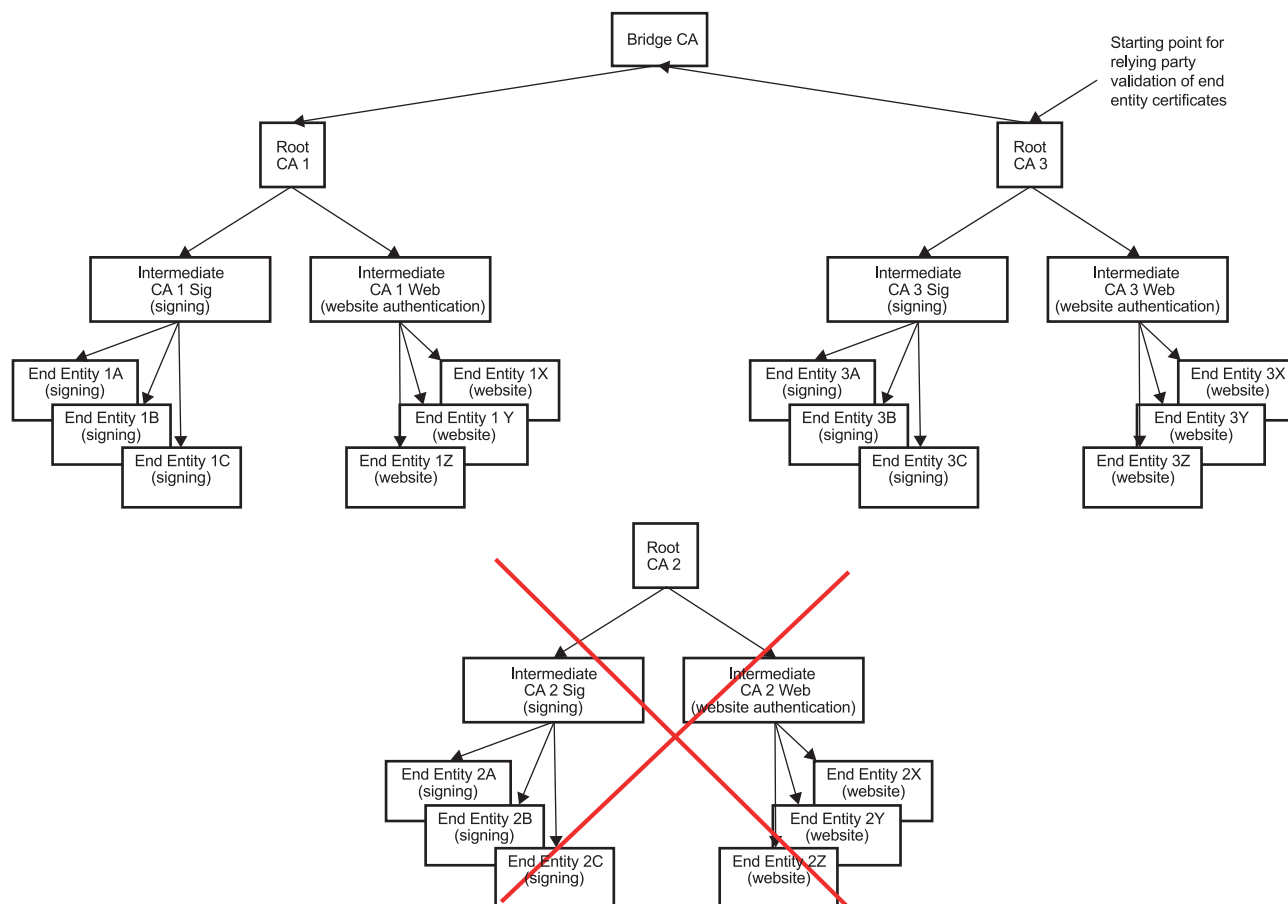
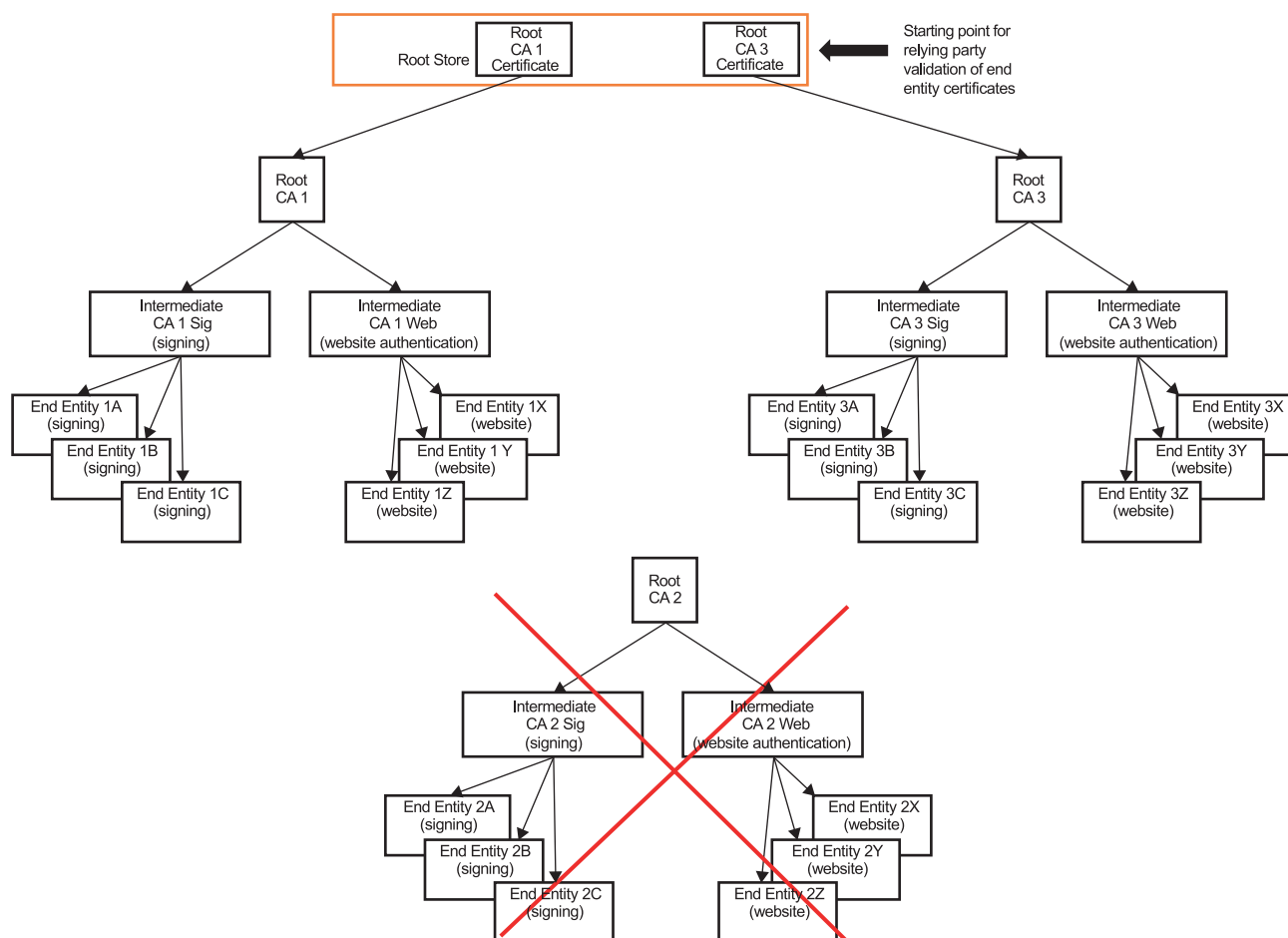


Figure 4 — CA trust relationships with bridge CA

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

b) Application root CA Certificate Store**Figure 5 — CA trust relationships with application root CA certificate store**

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

c) Trusted List

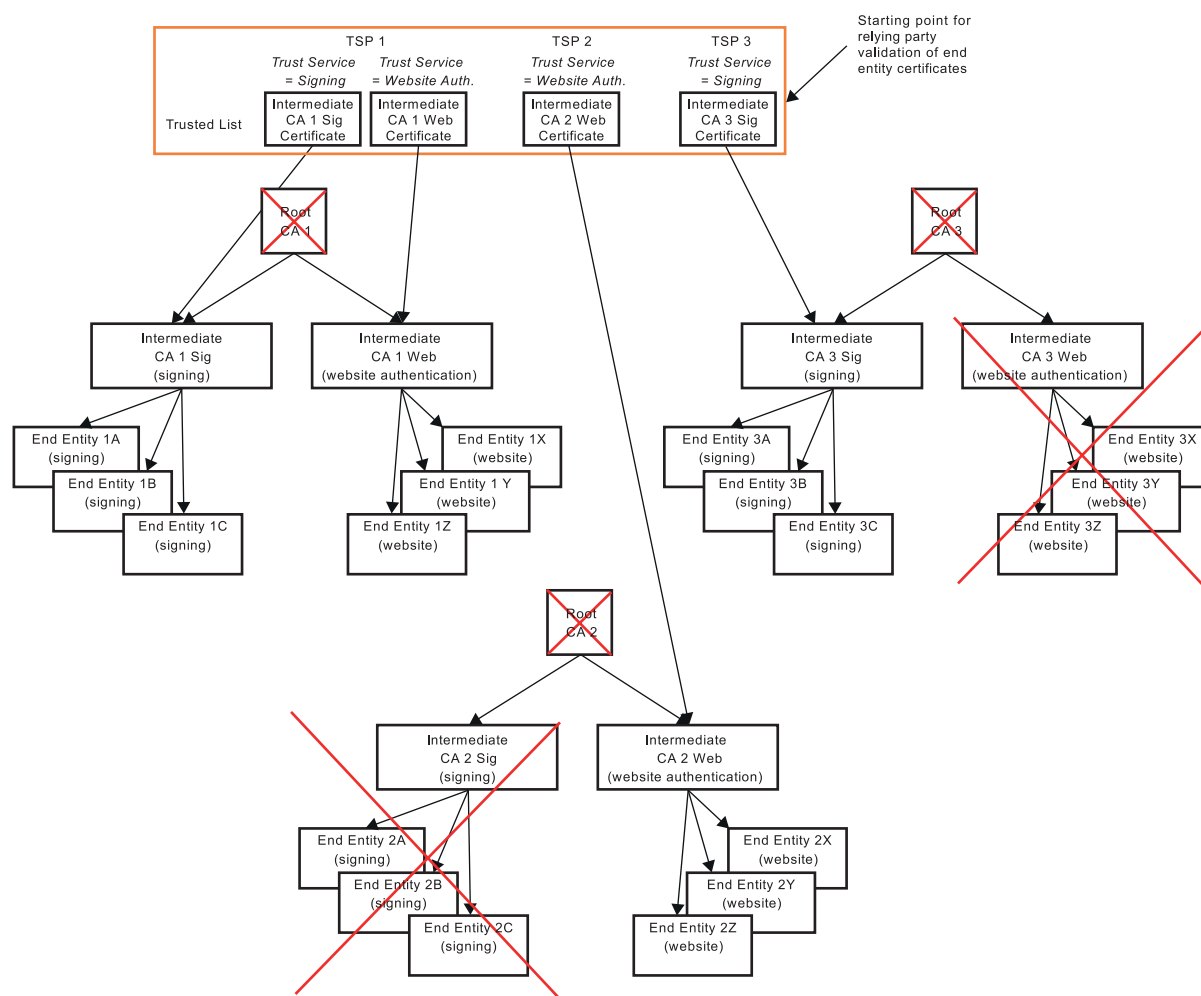


Figure 6 — CA trust relationships with Trusted List

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

5.10.2 Wildcard certificate considerations

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

5.10.3 Relying party considerations

Relying parties are dependent on certificates but typically do not have a direct business relationship with the certification authority (CA). The relying party validates signatures and certificates according

to a signature validation policy which can imply trust in the certification authority (CA) itself, or as a participant in a scheme of mutual recognition (i.e. a commonly accepted “qualified level” or being certified under a bridge-CA). Another possibility is that the relying party accepts the CA’s relying party agreement (RPA) explicitly or implicitly, regardless of whether the relying party has read or acknowledged the RPA.

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

Actions taken by relying parties should include the following.

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

5.11 Component services

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

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

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

a) Registration service:

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

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