INTERNATIONAL STANDARD

ISO/IEC 27099

First edition
2022-07

Information technology — Public key infrastructure — Practices and policy framework



Reference number
ISO/IEC 27099:2022(E)

© ISO/IEC 2022



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2022

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

© ISO/IEC 2022 – All rights reserved

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 14
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 16
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 19
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 **30**

© ISO/IEC 2022 – All rights reserved

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 ... 39
7.8 Access control ... 40
7.9 System acquisition development and maintenance ... 42
7.10 Business continuity management ... 42
7.11 Monitoring, conformance and compliance ... 44
7.12 Audit journal security assurance ... 44
7.13 CA key life cycle management controls ... 49
7.13.1 CA key generation ... 49
7.13.2 CA key storage, back-up, and recovery ... 50
7.13.3 CA public key distribution ... 52
7.13.4 CA key usage ... 52
7.13.5 CA key archival and destruction ... 53
7.13.6 CA key compromise ... 53
7.14 Subject key life cycle management controls ... 54
7.14.1 CA-provided subject key generation services (if supported) ... 54
7.14.2 CA-provided subject key storage and recovery services (if supported) ... 55
7.14.3 Hardware token life cycle management if outsourced to an external service (if supported) ... 56
7.14.4 Subject key management, if supported ... 58
7.15 Certificate life cycle management controls ... 59
7.15.1 Subject registration ... 59
7.15.2 Certificate renewal (if supported) ... 60
7.15.3 Certificate rekey ... 61
7.15.4 Certificate issuance ... 62
7.15.5 Certificate distribution ... 62
7.15.6 Certificate revocation ... 63
7.15.7 Certificate suspension (if supported) ... 63
7.15.8 Revocation status information service ... 65
7.15.9 Controlled CA termination ... 66
7.16 Root CA controls ... 67
7.16.1 Physical and environmental security ... 67
7.16.2 Operations security ... 67
7.16.3 Access control ... 68
7.16.4 Root CA key generation ... 68
7.16.5 Generation of root CA keys script requirements ... 69
7.16.6 Root CA public key distribution ... 69
7.16.7 Root CA key compromise ... 69
7.17 CA certificate life cycle management controls – subordinate CA certificate ... 70

Annex A (informative) **Management by certificate policy** ... **71**

Annex B (informative) **CA key generation ceremony** ... **78**

Annex C (informative) **Certification authority audit journal contents and use** ... **82**

Annex D (informative) **Certificate and PKI roles** ... **85**

Annex E (informative) **Changes to ISO 21188:2018 to produce ISO/IEC 27099** ... **91**

Bibliography ... **93**

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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

© ISO/IEC 2022 – All rights reserved

— 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

© ISO/IEC 2022 – All rights reserved

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)

© ISO/IEC 2022 – All rights reserved

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

© ISO/IEC 2022 – All rights reserved

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

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved

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

© ISO/IEC 2022 – All rights reserved

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.

© ISO/IEC 2022 – All rights reserved