INTERNATIONAL STANDARD

ISO 21188

Second edition
2018-04

Public key infrastructure for financial services — Practices and policy framework

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

Reference number
ISO 21188:2018(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

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

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

The main changes to the previous edition are:

- Clause 2, ISO/IEC 7811 removed as it is a standard for magnetic stripes;
- 3.21, ‘hold’ removed from definition of ‘certification authority’;
- 7.3.6 and D.4, references to ISO 15782-1, Annex J removed;
- 7.4.1, “be performed by authorized personnel” changed to “be performed in a process initiated by authorized personnel”;
- all instances of ‘shall’, ‘should’ and ‘may’ checked and updated if necessary;
- paragraph added to 5.4:

  ‘Two or more CAs can join a common scheme for mutual recognition, e.g. implemented by a trust list. Certificates issued by one CA can then be validated by relying parties who are customers of another CA belonging to the scheme.’;
- control added to 7.2.2:

  ‘Responsible management of the CA should be able to demonstrate that the information security policy is implemented and adhered to.’;
- proposal added to 7.2.2:

  ‘Procedures should exist to carry out a risk assessment to identify, analyse and evaluate trust service risks, taking into account business and technical issues. The results of the risk assessment shall be communicated to a management group or committee responsible to information security and risk management.';

- general editorial changes.

Introduction

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

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

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

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

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

INTERNATIONAL STANDARD ISO 21188:2018(E)

Public key infrastructure for financial services — Practices and policy framework

1 Scope

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

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

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

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

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

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

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

2 Normative references

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

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

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

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

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

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

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

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

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

3 Terms and definitions

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

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

- ISO Online browsing platform: available at https://www.iso.org/obp/3.1
- IEC Electropedia: available at http://www.electropedia.org/

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

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

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

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

3.3
authentication
provision of assurance that a claimed identity of an entity is correct

Note 1 to entry: a) at registration, the act of evaluating an end entity's (i.e. subscriber's) identity and verifying that it is correct for issuing of a certificate; b) during use, the act of comparing electronically submitted identity and credentials (i.e. user ID and password) with stored values to prove identity.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

3.23
certification practice statement
CPS
statement of the practices which a *certification authority* (3.21) employs in issuing, managing, revoking and renewing certificates and which defines the equipment, policies and procedures the *CA* uses to satisfy the requirements specified in the certificate policies that are supported by it

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

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

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

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

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

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

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

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

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

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

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

3.33
audit journal
audit log
event journal
chronological record of system activities which is sufficient to enable the reconstruction, review and examination of the sequence of environments and activities surrounding or leading to each event in the path of a transaction from its inception to the output of the final results

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

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

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

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

3.38
key recovery
ability to restore an entity's private key or a symmetric encipherment key from secure storage in the event that such keys are lost, corrupted or otherwise become unavailable

3.39
multiple control
condition under which two (dual) or more parties separately and confidentially have custody of components of a single key that, individually, convey no knowledge of the resultant cryptographic key

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

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

3.42
online certificate status protocol
OCSP
protocol for determining the current status of a certificate in lieu of or as a supplement to checking against a periodic *CRL* (3.17) and which specifies the data that need to be exchanged between an application checking the status of a certificate and the server providing that status

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

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

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

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

3.46
policy mapping
recognition that when a *CA* (3.21) in one domain certifies a *CA* in another domain, a particular *certificate policy* (3.13) in the second domain can be considered by the authority of the first domain to be equivalent (but not necessarily identical in all respects) to a particular certificate policy in the first domain

Note 1 to entry: See *cross certification* (3.28).

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

3.48
public key infrastructure
PKI
structure of hardware, software, people, processes and policies that employs digital signature technology to facilitate a verifiable association between the public component of an asymmetric public key pair with a specific subscriber that possesses the corresponding private key

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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