INTERNATIONAL STANDARD

**ISO 21188**

First edition
2006-05-01

# Public key infrastructure for financial services — Practices and policy framework

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

Reference number
ISO 21188:2006(E)

© ISO 2006

**PDF disclaimer**

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

© ISO 2006

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

 © ISO 2006 – All rights reserved

# Contents

Page



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-8f76ce8da001/iso-21188-2006

© ISO 2006 – All rights reserved

## 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.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

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.

ISO 21188 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006


© ISO 2006 – All rights reserved

# 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 authority systems 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 last twenty years the financial services industry has developed risk management processes and policies to support the use of these technologies in financial applications.

The expanded use of Internet technologies by the financial services 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f5ace81ad01/iso-21188-2006

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 International Standard.

Members of the International Organization of Standardization Technical Committee 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. ISO 15782 parts 1 and 2 define a certificate management system for financial industry use, but does not include certificate policy and certification practices requirements. This International Standard complements ISO 15782 parts 1 and 2 by providing a framework for managing a PKI through certificate policies, certification practice statements, control objectives and supporting procedures. For implementers of these International Standards, 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 these International Standards will depend partly on factors relative to policy and practices defined in this document.

© ISO 2006 – All rights reserved

iTeh STANDARD PREVIEW
(standards.iteh.ai)

ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

# Public key infrastructure for financial services — Practices and policy framework

## 1 Scope

This International Standard 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.

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

This International Standard 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 International Standard 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 International Standard.

iTeh STANDARD Preview
(standards.iteh.ai)

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

ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

**Business Managers and Analysts** are those who require information regarding using PKI technology in their evolving businesses (e.g., electronic commerce) and should focus on Clauses 1 to 6.

**Technical Designers and Implementers** are those who are writing their certificate policy(ies) and certification practice statement(s) and should focus on Clauses 6 to 8 and Annexes A to F.

**Operational Management and Auditors** are those who are responsible for day-to-day operations of the PKI and validating compliance to this document and should focus on Clauses 6 to 8.

## 2 Normative references

The following referenced documents are indispensable for the application 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 7810, *Identification cards — Physical characteristics*

ISO/IEC 7811, *Identification cards — Recording technique* (parts 1 to 5)

ISO/IEC 7813, *Identification cards — Financial transaction cards*

ISO/IEC 7816, *Identification cards — Integrated circuit cards* (parts 1 to 12 and 15)

ISO/IEC 9594-8:1995, *Information Technology — Open Systems Interconnection — The Directory: Authentication Framework*

© ISO 2006 – All rights reserved

ISO/IEC 9834-1:1993, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: General procedures — Part 1*

ISO 10202, *Financial transaction cards — Security architecture of financial transaction systems using integrated circuit cards* (eight parts)

ISO/IEC 10646-1, *Information technology — Universal Multiple-Octet Coded Character Set (UCS) — Part 1: Architecture and Basic Multilingual Plane*

ISO/IEC 15408, *Information technology — Security techniques — Evaluation criteria for IT security (three parts)*

ISO 15782-1:2003, *Certificate management for financial services — Part 1: Public key certificates*

ISO 15782-2, *Banking — Certificate Management — Part 2: Certificate Extensions*

ISO/IEC 17799, *Information technology — Security techniques — Code of practice for information security management*

ISO 18014-2, *Information technology — Security techniques — Time-stamping services — Part 2: Mechanisms producing independent tokens*

ISO 18014-3, *Information technology — Security techniques — Time-stamping services — Part 3: Mechanisms producing linked tokens*

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

ISO 18033, *Information technology — Security techniques — Encryption algorithms* (parts 1 to 4)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

## 3 Terms and definitions

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

**3.1**
**activation data**
data values, other than keys, which are required to operate cryptographic modules and which need to be protected (e.g. a PIN, a pass phrase, a biometric, or a manually held key share)

**3.2**
**authentication**
verification of an individual's claimed identity:

a) at registration, the act of evaluating end entities' (i.e., subscribers') credentials as evidence for their claimed identity;

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

**3.3**
**authentication data**
information used to verify the claimed identity of an entity, such as an individual, defined role, corporation or institution

**3.4**
**card bureau**
agent of the **CA** (3.18) or **RA** (3.46) that personalizes an **ICC** (3.32) containing the subscriber's private key (as a minimum)


© ISO 2006 – All rights reserved

**3.5**
**cardholder**
subject to whom the integrated circuit card containing private and public key pairs and **certificates** (3.6) has been issued

**3.6**
**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 certifying authority that issued that public key certificate

**3.7**
**certificate hold**
**certificate suspension**
suspension of the validity of a **certificate** (3.6)

**3.8**
**certificate issuer**
organization whose name appears in the issuer field of a **certificate** (3.6)

**3.9**
**certificate manufacturer**
agent who performs the tasks of applying a digital signature to a certificate signing request on behalf of the **certificate** (3.6) issuer

**3.10**
**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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

**3.11**
**certificate profile**
specification of the required format (including requirements for the usage of standard fields and extensions) for a particular type of **certificate** (3.6)

**3.12**
**certificate re-key**
process whereby an entity with an existing key pair and **certificate** (3.6) receives a new **certificate** for a new public key, following the generation of a new key pair

**3.13**
**certificate renewal**
**rollover**
process whereby an entity is issued a new instance of an existing certificate with a new validity period

**3.14**
**certificate revocation list**
**CRL**
list of revoked **certificates** (3.6)

**3.15**
**certificate validation service**
service provided by the **CA** (3.18) or its agent which performs the task of confirming the validity of a **certificate** (3.6) to a **relying party** (3.49)

**3.16**
**certificate validation service provider**
**CVSP**
**entity** (3.29) that provides certificate validation services to its relying party customers

© ISO 2006 – All rights reserved

**3.17**
**certification**
process of creating a public key certificate for an **entity** (3.29)

**3.18**
**certification authority**
**CA**
entity trusted by one or more entities to create, assign and revoke or hold public key certificates

**3.19**
**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

**3.20**
**certification practice statement**
**CPS**
statement of the practices which a **certification authority** (3.18) employs in issuing 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

**3.21**
**certification request**
submission of a validated registration request by an **RA** (3.46), its agent or a subject to a **CA** (3.18) to register a subject's public key to be placed in a **certificate** (3.6)

iTeh STANDARD PREVIEW
(standards.iteh.ai)

**3.22**
**certification response**
message sent, following certification, from a **CA** (3.18) in response to a certificate request

ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

**3.23**
**certificate validity**
**validity**
applicability (fitness for intended use) and status (live, suspended, revoked or expired) of a **certificate** (3.6)

**3.24**
**compromise**
violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred

**3.25**
**cross certification**
process by which two **CAs** (3.18) mutually certify each other's public keys

NOTE This process may or may not be automated.

**3.26**
**cryptographic hardware**
**cryptographic device**
**hardware security module**
hardware cryptographic module

**3.27**
**digital signature**
cryptographic transformation that, when associated with a data unit, provides the services of origin authentication, data integrity and signer non-repudiation

**3.28**
**end entity**
certificate subject that uses its private key for purposes other than signing certificates


© ISO 2006 – All rights reserved

**3.29**
**entity**
**CA** (3.18), **RA** (3.46) or **end entity** (3.28)

**3.30**
**event journal**
**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

**3.31**
**functional testing**
portion of security testing in which the advertised features of a system are tested for correct operation

**3.32**
**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

**3.33**
**issuing certification authority**
**issuing CA**
in the context of a particular certificate, the issuing **CA** (3.18) is the **CA** that issued the certificate

iTeh STANDARD PREVIEW
(standards.iteh.ai)

**3.34**
**key escrow**
management function that allows access by an authorized party to a replicated private encipherment key

ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

NOTE This may be a legal requirement to allow law enforcement officials to gain access to an entity and/or CA's private confidentiality key.

**3.35**
**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

**3.36**
**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

**3.37**
**object identifier**
**OID**
unique series of integers that unambiguously identifies an information object

**3.38**
**online certificate status mechanism**
mechanism that allows **relying parties** (3.49) to request and obtain certificate status information without requiring the use of **CRLs** (3.14)

**3.39**
**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** (3.14) 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

© ISO 2006 – All rights reserved

**3.40**
**operating period**
period of a certificate beginning on the date and time it is issued by a **CA** (3.18) (or on a later date and time, if stated in the certificate), and ending on the date and time it expires or is revoked

**3.41**
**PKI disclosure statement**
document that supplements a **CP** (3.10) or **CPS** (3.20) by disclosing critical information about the policies and practices of a **CA** (3.18)/**PKI** (3.45)

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

**3.42**
**policy authority**
**PA**
party or body with final authority and responsibility for specifying **certificate policie**s (3.10) and ensuring **CA** (3.18) practices and controls as defined by the **CPS** (3.20) fully support the specified **certificate policies**

**3.43**
**policy mapping**
recognition that, when a **CA** (3.18) in one domain certifies a **CA** in another domain, a particular **certificate policy** (3.10) in the second domain may 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 See 3.25, cross certification.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

**3.44**
**policy qualifier**
policy-dependent information that accompanies a **certificate policy** (3.10) identifier in an X.509 certificate

ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

**3.45**
**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 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.

**3.46**
**registration authority**
**RA**
entity that is responsible for identification and authentication of subjects of certificates, but is not a **CA** (3.18), and hence does not sign or issue certificates

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

**3.47**
**registration request**
submission by an entity to an **RA** (3.46) [or **CA** (3.18)] to register the entity's public key in a certificate

**3.48**
**registration response**
message sent by an **RA** (3.46) [or **CA** (3.18)] to an entity in response to a registration request


© ISO 2006 – All rights reserved

**3.49**
**relying party**
**RP**
recipient of a certificate who acts in reliance on that certificate, digital signatures verified using that certificate, or both

**3.50**
**repository**
system for storage and distribution of certificates and related information (i.e., certificate storage, certificate distribution, **certificate policy** (3.10) storage and retrieval, certificate status, etc.)

**3.51**
**root CA**
**CA** (3.18) at the apex of the **CA** hierarchy

**3.52**
**signature verification**
⟨in relation to a digital signature⟩ accurate determination:

a) that the digital signature was created during the operational period of a valid certificate by the private key corresponding to the public key listed in the **certificate** (3.6);

b) that the message has not been altered since its digital signature was created.

**3.53**
**subject**
entity whose public key is certified in a public key certificate

iTeh STANDARD PREVIEW
(standards.iteh.ai)

**3.54**
**subject CA**
**CA** (3.18) that is certified by the issuing **CA** and hence complies with the **certificate policy** (3.10) of the issuing **CA**

ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006

**3.55**
**subject end entity**
end entity that is the subject of a **certificate** (3.6)

**3.56**
**subordinate CA**
**sub-CA**
**CA** (3.18) that is lower relative to another **CA** in the **CA** hierarchy

**3.57**
**subscriber**
entity subscribing with a **certification authority** (3.18) on behalf of one or more subjects

**3.58**
**superior CA**
**CA** (3.18) that is higher relative to another [**subordinate CA** (3.56)] in the **CA** hierarchy, but is not a root **CA**

**3.59**
**tamper evident**
possessing a characteristic that provides evidence that an attack has been attempted

**3.60**
**tamper resistant**
possessing a characteristic that provides passive physical protection against an attack

© ISO 2006 – All rights reserved

**3.61**
**trusted role**
job function that performs critical functions which, if performed unsatisfactorily, may have an adverse impact upon the degree of trust provided by the **CA** (3.18)

**3.62**
**trust services provider**
**TSP**
approved organization (as determined by the contractual participants) providing trust services, through a number of **certification authorities** (3.18), to their customers who may act as subscribers or **relying parties** (3.49)

NOTE A trust services provider may also provide certificate validation services.

**3.63**
**validation service request**
enquiry by the **relying party** (3.49) to a validation service to check the validity of a **certificate** (3.6)

## 4 Abbreviated terms

| Abbreviation | Meaning |
|---|---|
| ASN.1 | Abstract Syntax Notation One |
| CA | Certification Authority |
| CM | Certificate Manufacturer |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CVSP | Certificate Validation Service Provider |
| EMV | Eurocard MasterCard Visa |
| FI | Financial Institution |
| FIPS | Federal Information Processing Standard |
| FTP | File Transfer Protocol |
| HSM | Hardware Security Module |
| HTTP | Hypertext Transfer Protocol |
| ICC | Integrated Circuit Card |
| ID | Identifier |
| IEC | International Electrotechnical Commission |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization |

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ee8da001/iso-21188-2006


© ISO 2006 – All rights reserved

| Abbreviation | Meaning |
|---|---|
| ITU | International Telecommunications Union |
| LDAP | Lightweight Directory Access Protocol |
| MAC | Message Authentication Code |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PA | Policy Authority |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure (X.509) (IETF Working Group) |
| POS | Point Of Sale |
| RA | Registration Authority |
| RFC | Request For Comment |
| RP | Relying Party |
| SSL | Secure Sockets Layer |
| TLS | Transport Layer Security |
| TSA | Time stamping Authority |
| TSP | Trust Services Provider |
| TTP | Trusted Third Party |
| URL | Uniform Resource Locator |

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO 21188:2006
https://standards.iteh.ai/catalog/standards/sist/8d1e7475-f065-4cdc-935e-6f76ce8da001/iso-21188-2006

## 5 Public key infrastructure (PKI)

### 5.1 General

Before addressing the details of PKI policy and practices requirements, this International Standard provides some background information in order for the reader to better understand the context in which these policies and practices are used within a PKI.

### 5.2 What is PKI?

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

© ISO 2006 – All rights reserved