BS ISO 21188:2018

BSI Standards Publication

Public key infrastructure for financial services — Practices and policy framework

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2018

National foreword

This British Standard is the UK implementation of ISO 21188:2018. It supersedes BS ISO 21188:2006, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Financial services.

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

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

© The British Standards Institution 2018
Published by BSI Standards Limited 2018

ISBN 978 0 580 82629 0

ICS 35.240.40

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 April 2018.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2018

INTERNATIONAL STANDARD

ISO 21188

Second edition
2018-04-03

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)

Documents
Document Sharing Hub

© ISO 2018

Full document details: BS ISO 21188:2018

COPYRIGHT PROTECTED DOCUMENT

© ISO 2018, 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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2018

Contents

Page

Foreword ... **v**
Introduction ... **vii**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **2**
4 Abbreviated terms ... **8**
5 Public key infrastructure (PKI) ... **9**
5.1 General ... 9
5.2 What is PKI? ... 10
5.2.1 General ... 10
5.2.2 Public key infrastructure process flow ... 11
5.3 Business requirement impact on PKI environment ... 11
5.3.1 General ... 11
5.3.2 Illustration of certificate application in a closed environment ... 11
5.3.3 Illustration of certificate application in a contractual PKI environment ... 12
5.3.4 Illustration of certificate application in an open environment ... 13
5.4 Certification authority (CA) ... 15
5.5 Business perspectives ... 16
5.5.1 General ... 16
5.5.2 Business risks ... 16
5.5.3 Applicability ... 16
5.5.4 Legal issues ... 16
5.5.5 Regulatory issues ... 16
5.5.6 Business usage issues ... 16
5.5.7 Interoperability issues ... 17
5.5.8 Audit journal requirements ... 18
5.6 Certificate policy (CP) ... 19
5.6.1 General ... 19
5.6.2 Certificate policy usage ... 19
5.6.3 Certificate policies within a hierarchy of trust ... 20
5.6.4 Certificate status ... 21
5.7 Certification practice statement (CPS) ... 21
5.7.1 General ... 21
5.7.2 Authority ... 21
5.7.3 Purpose ... 22
5.7.4 Level of specificity ... 22
5.7.5 Approach ... 22
5.7.6 Audience and access ... 22
5.8 Agreements ... 22
5.9 Time-stamping ... 23
5.10 Trust models ... 24
5.10.1 Trust model considerations ... 24
5.10.2 Wildcard considerations ... 25
5.10.3 Relying party considerations ... 25
6 Certificate policy and certification practice statement requirements ... **26**
6.1 Certificate policy (CP) ... 26
6.2 Certification practice statement (CPS) ... 28
7 Certification authority control procedures ... **28**
7.1 General ... 28
7.2 CA environmental controls ... 29
7.2.1 Certification practice statement and certificate policy management ... 29
7.2.2 Security management ... 30

© ISO 2018 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

7.2.3 Asset classification and management ... 31
7.2.4 Personnel security ... 32
7.2.5 Physical and environmental security ... 33
7.2.6 Operations management ... 34
7.2.7 System access management ... 35
7.2.8 Systems development and maintenance ... 37
7.2.9 Business continuity management ... 37
7.2.10 Monitoring and compliance ... 39
7.2.11 Audit logging ... 39
7.3 CA key life cycle management controls ... 43
7.3.1 CA key generation ... 43
7.3.2 CA key storage, back-up and recovery ... 44
7.3.3 CA public key distribution ... 45
7.3.4 CA key usage ... 46
7.3.5 CA key archival and destruction ... 46
7.3.6 CA key compromise ... 47
7.4 Subject key life cycle management controls ... 48
7.4.1 CA-provided subject key generation services (if supported) ... 48
7.4.2 CA-provided subject key storage and recovery services (if supported) ... 48
7.4.3 Integrated circuit card (ICC) life cycle management (if supported) ... 49
7.4.4 Requirements for subject key management ... 51
7.5 Certificate life cycle management controls ... 52
7.5.1 Subject registration ... 52
7.5.2 Certificate renewal (if supported) ... 53
7.5.3 Certificate rekey ... 54
7.5.4 Certificate issuance ... 54
7.5.5 Certificate distribution ... 55
7.5.6 Certificate revocation ... 56
7.5.7 Certificate suspension (if supported) ... 56
7.5.8 Certificate validation services ... 57
7.6 Controlled CA termination ... 58
7.7 CA certificate life cycle management controls — subordinate CA certificate ... 59

Annex A (informative) **Management by certificate policy** ... **61**

Annex B (informative) **Elements of a certification practice statement** ... **70**

Annex C (informative) **Object identifiers (OID)** ... **85**

Annex D (informative) **CA key generation ceremony** ... **87**

Annex E (informative) **Mapping of RFC 2527 to RFC 3647** ... **91**

Annex F (normative) **Certification authority audit journal contents and use** ... **92**

Annex G (informative) **Alternative trust models** ... **95**

Bibliography ... **107**

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

© ISO 2018 – All rights reserved

AVA Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

shall be communicated to a management group or committee responsible to information security and risk management.';

— general editorial changes.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

This page deliberately left blank

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2018

INTERNATIONAL STANDARD **ISO 21188:2018**

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 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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)

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

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

3.64
tamper-resistant
provides passive physical protection against an attack

3.65
trusted role
job function that performs critical functions which, if performed unsatisfactorily, can have an adverse impact upon the degree of trust provided by the *CA* (3.21)

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

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

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

4 Abbreviated terms

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

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

5 Public key infrastructure (PKI)

5.1 General

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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

5.2 What is PKI?

5.2.1 General

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

PKIs are a practical technical solution to the problems posed by open networks. Financial institutions are becoming trust services providers (TSPs), to take advantage of the growing market for security and authentication in online communications. Relying parties, as recipients of information, use TSPs to validate certificates used to authenticate online communications. A TSP can be an entity providing one or more trusted services, e.g. a certification authority or a validation service. A TSP is a recognized authority trusted by one or more relying parties to create and sign certificates. A TSP can also revoke certificates it has created and issued. A TSP operates one or more certification authorities (CAs) whose core functions are certificate issuing, certificate distribution and certificate validation. Within a financial institution, a CA is not necessarily a business entity but can be a unit or a function providing CA functions that may be trusted by relying parties and subscribing parties.

Public key technology is used to support confidentiality, integrity and authentication requirements. With public key cryptography, two keys are created (private and public). The private key is kept secret and the public key can be made publicly available in a certified form which protects its authenticity. The subject's public key and identifying data are signed by the CA's private key to create a certificate. Certificates are created under certificate policies. Revealing the public key does not compromise the private key.

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

a) **Closed environment**: all entities (certificate subjects and relying parties) adhere to a single financial institution's trust service, and shall share at least one certificate policy. See Figure 1 and Table 1. An entity adhering to a trust service may act as a relying party or subscriber for certificates for itself or on behalf of other certificate subjects. In this case, subscribers and certificate subjects may be distinct entities bound by a business relationship which is outside the scope of this document.

b) **Contractual environment**: certificate subjects and relying parties can have separate TSPs. TSPs are bound by differing forms of contract covering certificate use. These forms comprise:

   1) multilateral, under agreed rules, with a single certificate policy;

   2) bilateral cross certification that can use different certificate policies;

   3) accreditation bridge that can recognize different certificate policies through central organization or entity. This can be realized by the central organization publishing a trust list of certificate policies, or of certification authorities, which conform to common policy requirements.

   See Figure 2 and Table 2.

c) **Open environment**: the financial institution can act as a TSP issuing certificates to the public and permits validation of certificates in an open network environment. TSPs can operate under voluntary TSP accreditation schemes or within an indigenous regulatory framework. Typically,

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

there is no formal contract between the subscriber's TSP and the relying party. See Figures 3 and 4 and Table 3.

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

5.2.2 Public key infrastructure process flow

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

— key generation;

— registration;

— certification;

— distribution;

— usage;

— expiry;

— renewal;

— rekey;

— revocation management;

— revocation status checking.

5.3 Business requirement impact on PKI environment

5.3.1 General

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

5.3.2 Illustration of certificate application in a closed environment

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

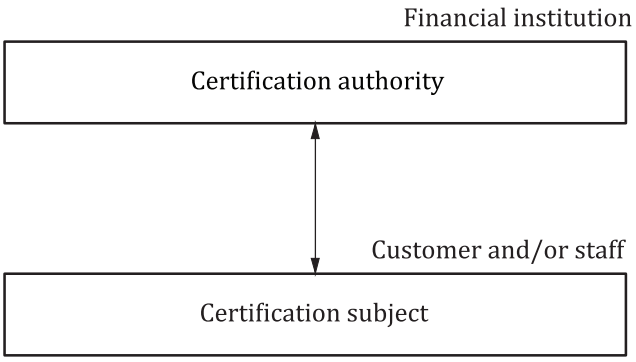

Figure 1 — Two entities in a closed environment

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

Table 1 — Certificate application scenarios in a closed environment

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

5.3.3 Illustration of certificate application in a contractual PKI environment

This subclause describes the financial institution using the PKI for support transactions to its customers within a scheme or where a contract with rules has been established between the parties. The corresponding PKI might be open or closed, and when closed the PKI is a third party service provider. It will provide either certificate issuance or certificate validation services, or both services, to its customers.

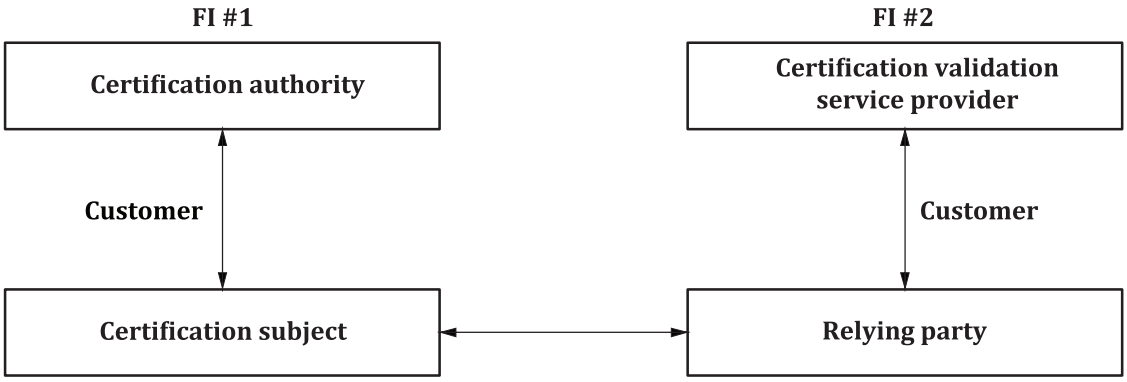

Figure 2 — Four entities in a contractual environment

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

Table 2 — Certificate application scenarios in a contractual environment

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

5.3.4 Illustration of certificate application in an open environment

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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

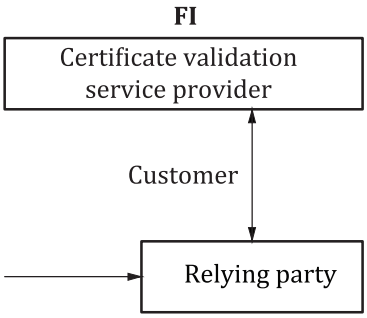

Figure 3 — FI acting as certificate validation service provider in an open environment

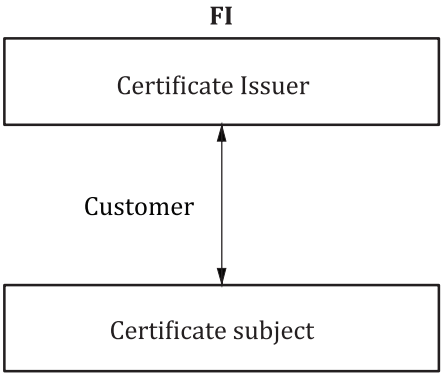

Figure 4 — FI acting as certificate issuer in an open environment

Table 3 — Certificate application scenarios in an open environment

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

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

5.4 Certification authority (CA)

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

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

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

— Entities (including CAs) can use these certificates to authenticate themselves to relying parties. Hence, authentication can involve a chain of certificates. The verification of a chain of certificates begins with the trusted CA public key and ends with the certificate being validated. The trusted CA public key shall be obtained and authenticated by some means other than by the use of certificates. This is to ensure that the process begins securely. See ISO/IEC 9594-8.

— Once a certificate has been generated, the integrity of its contents is protected. This document does not require that certificates be given confidentiality protection. A valid copy of the CA's public key is required by the relying party in order to validate a certificate. Given that the CA is a trusted entity, this permits the validation of the binding between an entity's public key, its identity and other needed information.

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

— To communicate outside the root CA's domain, the root CA shall cross-certify with the desired remote domain. Certification path validation then involves building a chain of certificates from the remote entity to the root CA by way of the cross-certified remote CA.

— In a non-hierarchical architecture, independent CAs can cross-certify each other by issuing public key certificates to each other. This results in a general network of trust relationships between CAs and allows each group (such as a retail credit authorization network, a clearing house, a financial institution or a subgroup thereof) to have its own CA. An entity uses the public key of a selected CA for its trusted CA public key. The certification path consists of those certificates that chain back from the certificate being validated to the trusted CA of the relying party.

— In a bridge architecture, two or more independent hierarchical architectures are interconnected by a common bridge CA which cross certifies with each root CA. The separate root CAs are peers to each other and the bridge CA such that they do not need to cross certify with each other. The bridge CA allows a relying party in one hierarchical architecture to validate the certificate chain from another hierarchical architecture.

— A bridge can be realized by a common trusted authority issuing a list of trusted certification authorities.

— A compromise of the private key of a CA compromises all entities certified by that CA, because the holder of that private key can generate fraudulent certificates and then masquerade as one or more end entities. Failure to provide compensating controls to deal with the possibility of compromise

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

of transactions in a financial network can have catastrophic effects on financial institutions and their customers.

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

5.5 Business perspectives

5.5.1 General

A financial institution's future ability to participate in an online global economy depends on the existence of a trusted and secure environment in which to conduct business in the electronic medium. The ideal goal of any financial institution is to establish a security infrastructure for an online marketplace that will allow it an opportunity to support internal security needs, to enhance and service its customer base as well as to enter new markets for the provision of trust services. In defining the business operations of the financial institution, many issues will be addressed.

5.5.2 Business risks

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

5.5.3 Applicability

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

5.5.4 Legal issues

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

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

5.5.5 Regulatory issues

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

5.5.6 Business usage issues

Business usage, as described in 5.3, is between the entities defined in the environment (i.e. the certificate subject or, where applicable, the subscriber and the relying party). Both parties shall fulfil their

© ISO 2018 – All rights reserved
AVA Documents Document Sharing Hub
Full document details: BS ISO 21188:2018

obligations set forth in the CP or the agreement that defines these obligations. The certificate subject or, where applicable, the subscriber can then use the digital signature process to authorize a message or transaction and subsequently the relying party can then rely upon the authenticated signature.

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

5.5.7 Interoperability issues

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

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

— legal jurisdiction and responsibilities;

— commercial risk management considerations;

— technical recognition of the certificate and operational processing aspects;

— policy and trust scheme obligations.

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

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

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

a) A CP can apply more broadly than to just a single organizational unit or single organization. If a particular CP is widely recognized, it has great potential as the basis of automated certificate acceptance in many systems.

b) Financial institutions that operate public or inter-organizational certification authorities shall document their own practices in CPSs. The CPS is one of the organization's means of protecting itself and positioning its relationships with subscribers and other entities.

c) Technical implementation can differ due to interpretation of standards and protocols by the PKI integrators. A technical comparison shall take place within the PKI environment to ensure technical interoperability.

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

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

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

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

or

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

5.5.8 Audit journal requirements

5.5.8.1 General

CA systems shall keep audit journals that provide sufficient detail to reconstruct events and provide "due care" requirements. All entries in audit journals shall be marked with a precise time. The time used to record events as required in the audit log shall be synchronised with UTC at least once a day. While audit journals will normally be created and maintained by the CA management system, some audit journals can out of necessity be manual. The audit requirements shall be specified in the CA's certification practice statement.

CA audit journal entries shall include all certificate and key management operations, such as key generation, backup, recovery and destruction, together with the identity of the person authorizing the operation and persons handling any key material (such as key fragments or keys stored in portable devices or media). Changes in the custody of private keys and associated parameters, and of devices or media holding keys, shall be recorded in the audit journals. Audit journals shall not record the plain text values of any private keys but can hold hash values as a means of identifying keys and validating their correctness as well as that of public keys derived from private keys by means of a one-way function.

A list of audit journal contents is provided in Annex F.

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

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

5.5.8.2 Security quality assurance

— Documented security quality assurance processes and procedures are required as part of the system of internal security control over certificate management. The audit journal shall be reviewed regularly (e.g. daily) by a security quality assurance function. In some organizations, this function can be fulfilled by the audit department. The review shall include the validation of the audit journal's integrity, and the identification and follow-up of exceptional, unauthorized or suspicious activity (e.g. digital signature failures, access at unusual times or from unusual sources, unexpected increases in volume or saturation of system resources).

— The extent and frequency of review and management escalation requirements shall be determined by a threat/risk evaluation. In high-risk applications and for legal purposes, CA systems can require end entities and relying parties to maintain an audit journal.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

5.6 Certificate policy (CP)

5.6.1 General

A CP is a common set of rules with regard to the level of trust that shall be met by associated certificates used for a particular purpose. The CP also specifies the criteria that shall be agreed upon and complied with by a certification authority before certificates issued by such a certification authority may be accepted by a relying party. It is developed by a policy authority. The policy authority writing the CP can range from a single business entity to a collection of entities such as a payment association established to interchange transactions between the member entities.

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

The purpose of a CP includes:

— to define and limit the use of certificates;

— to specify requirements and obligations of certificate subject and, where applicable, subscriber, the certification authority and relying parties;

— to define liabilities for certificate subject and, where applicable, subscriber, the certification authority and relying parties;

— to specify policy administration process;

— to specify governing law.

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

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

5.6.2 Certificate policy usage

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

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

a) certificate policy for specific functional applications (e.g. server identification certificate for customer to authenticate their online banking service provider);

b) subscription to the certificate policy that matches the business application (e.g. customer signing a purchasing order from a merchant);

c) subscription to the certificate policy that matches a generic security application with a defined environment within prespecified restrictions (e.g. providing confidentiality protection on all message types to certificate subject across the Internet).

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

5.6.3 Certificate policies within a hierarchy of trust

PKIs are commonly structured into a hierarchy with the top or apex of the hierarchy being a root. The root delegates a portion of its trust to subordinate CAs based upon the organizational needs. The root and intermediate levels primarily authenticate and sign the digital certificates of subordinate levels and provide the structuring of business requirements by differentiating between organizational needs (e.g. between geopolitical or organizational regions, countries or states, organizational units). As illustrated in Clause 6, the hierarchies permit the use of multiple certificate policies, each defining the different business requirements of facets of the business environment. With a hierarchy, each level is more granular or homogenous in its specificity of requirements to a "smaller" group of certificates issued to end-entities. Each group of certificate end-entities share a common set of certificate policies.

For example, the root level at the highest level of the hierarchy by definition shall use a self-signed certificate and can only be used to sign subordinate certificates. A subordinate CA shall be defined based upon geopolitical, organizational or other requirements. The subordinate CAs may cascade into multiple levels based upon multiple structural needs or it may issue certificates to end-entities.

In a hierarchy, the root shall be the most trusted point. Each subordinate level shares the trust between their peers, but each shall trust the superior point from which they have been delegated responsibility.

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

a) certificate policy for identifying the root CA with its implied self-signed certificate (certificates issued under Policy A in Figure 5);

b) certificate policy for identifying a subordinate CA established under the root CA or another subordinate CA. To sign the public keys of the subordinate or intermediate CAs, the root CA acting as the ultimate parent in the CA hierarchy in the FI (certificates issued under Policy B in Figure 5).

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

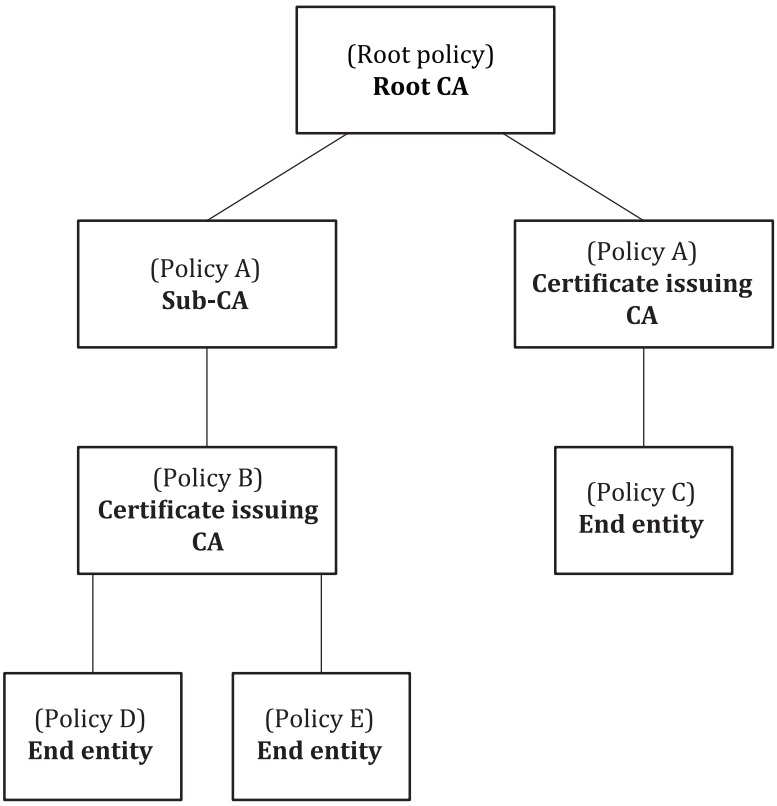

Figure 5 — Root hierarchy creates a hierarchy of trust

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

5.6.4 Certificate status

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

A certificate may be in one of the following states:

a) pre-valid – not operational;

b) live – operational;

c) suspended – not operational;

d) revoked – not operational;

e) expired – not operational.

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

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

5.7 Certification practice statement (CPS)

5.7.1 General

The certification practice statement describes the necessary and sufficient procedures and controls employed by the CA to meet the requirements of the certificate policies.

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

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

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

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

5.7.2 Authority

A policy authority specifies the certificate policy that is adopted by the certification authorities that have their controls described in certification practice statements. A CP is created, maintained, distributed and interpreted by the policy authority. The policy authority can either represent one financial institution or be shared by a number of major stakeholders. A certification authority in support of its operation prepares a CPS or an equivalent document as evidence of its ability to comply with one or many certificate policies. A formal CPS is not compulsory in a contractual PKI environment and is often determined by either the rules of the community or the policy authority. In any event, the CA shall have documented its practices. While a simple compliance statement can suffice with a contractual PKI environment, a CPS, nevertheless, provides guidance for both internal processing and processing completed by delegated roles.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

5.7.3 Purpose

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

5.7.4 Level of specificity

A certificate policy is prescriptive.

A certification practice statement is descriptive and detailed. Such documents are generally defined as internal operating procedure documents that can describe specific tasks and responsibilities within an organization. Such documentation can be used in the daily operation of the CA and reviewed by those performing a process review or audit. In an open environment, the trusted service provider shall publicly disclose its certification practice statement through an online means that is available on a 24/7 basis.

5.7.5 Approach

The CP is based upon known business requirements.

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

5.7.6 Audience and access

In general, the CP is managed as public information in the contractual environment, and therefore widely disseminated by the PA to all participants. The CP shall clearly identify the distribution policy of public, sensitive and confidential information both within the contractual environment and to appropriate external parties.

A CPS is a statement by a CA as to the control practices it will follow in issuing and maintaining certificates and clearly defines how its practices fully support the CP identified. It is therefore by its nature a sensitive document which can be considered confidential. If the circulation of the CPS is restricted, financial institutions can use a PKI disclosure statement, indicating the type and nature of the controls without disclosing specific control details to support the CP. In an open environment, the trusted service provider shall publicly disclose its certification practice statement through an online means that is available on a 24/7 basis.

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

5.8 Agreements

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

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

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

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

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

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

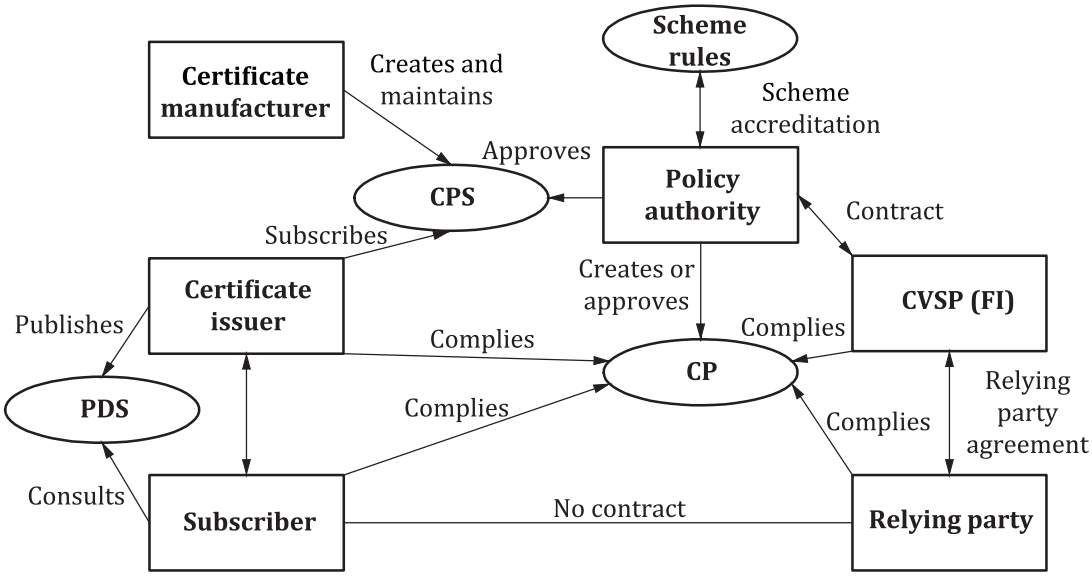

Figure 6 — Control documents within standard financial PKI model

5.9 Time-stamping

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

There are two aspects of certificate usage where timing is of particular importance. Firstly, trust services are based on certificates which have a validity period. If a signature is verified after the expiry of the signing key certificate, the validity of the certificate cannot be ensured. Secondly, if a certificate is revoked then any use of the certificate after the time that it is revoked could be considered to be invalid. Thus, if there is significant time between the application of a certificate in securing data and the checking of the validity of the protection, for example when applying a digital signature to stored data, it is important to be sure of the time at which the signature was applied. If it can be confirmed that a signature was created before the supporting certificate expired or was revoked, then the validity of the signature can be ensured long after either of those events. It is for the relying party to determine whether they accept the risk associated with a certificate that could have expired or been revoked in the interim period.

© ISO 2018 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

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

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

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

5.10 Trust models

5.10.1 Trust model considerations

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

— first party trust model

— second party trust model

— third party trust model

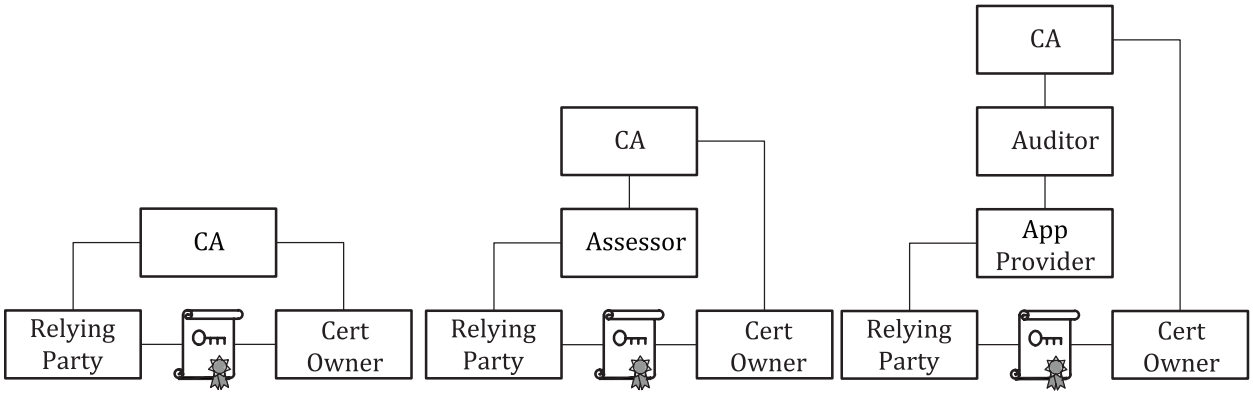

Figure 7 — CA trust models

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

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018

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

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

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

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

5.10.2 Wildcard considerations

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

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

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

5.10.3 Relying party considerations

5.10.3.1 General

Relying parties are dependent on certificates but typically do not have a direct business relationship with the certificate authority (CA). The relying party validates signatures and certificates according to a signature validation policy which can imply trust in the certificate authority itself, or as a participant in a scheme of mutual recognition (i.e. a commonly accepted "qualified level" or being certified under a bridge-CA). Another possibility is that the relying party accepts the CA's relying party agreement (RPA) explicitly or implicitly, regardless of whether the relying party has read or acknowledged the RPA. Consequently, actions taken by the relying party shall include the following.

5.10.3.2 Certificate validation

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

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

2) authorize the subject certificate;

3) authorize the trust anchor and intermediary CA certificates;

4) verify the validity dates and operation period;

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

6) verify the CA signature for each certificate;

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

The certificate validation is only successful if all of the steps have been successfully completed. Otherwise, the certificate chain is invalid and the relying party shall reject the subject certificate. The

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2018

first failure negates the need to continue processing all of the steps. Most browsers allow users to accept invalid certificates and bypass certificate validation.

5.10.3.3 Certificate revocation or suspension

Actions taken by relying parties shall include the following.

— reject any signed message received after the revocation date requiring the use of the revoked certificate;

— reject any signed message received after the suspension date and prior to its release date requiring the use of the suspended certificate;

— immediately discontinue any keying material established or protected by revoked certificate and corresponding asymmetric private key;

— update an audit journal to reflect the actions taken and the reasons for the actions.

Actions taken by relying parties shall include the following.

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

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

6 Certificate policy and certification practice statement requirements

6.1 Certificate policy (CP)

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

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

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

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

b) CP shall in accordance:

   — be uniquely identified;

   — contain its name;

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

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

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

   — identify policy authority;

   — identify procedures for publication, change and subsequent notification;

   — identify the version number and effective date;

   — include an expiry date if applicable.

© ISO 2018 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 21188:2018