BRITISH STANDARD

BS ISO 21188:2006

Public key infrastructure for financial services — Practices and policy framework

ICS 35.240.40

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Document Sharing Hub
British Standards

Full document details: BS ISO 21188:2006

National foreword

This British Standard reproduces verbatim ISO 21188:2006 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/12, Banking, securities and other financial services, which has the responsibility to:

— aid enquirers to understand the text;

— present to the responsible international/European committee any enquiries on the interpretation, or proposals for change, and keep UK interests informed;

— monitor related international and European developments and promulgate them in the UK.

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

Cross-references

The British Standards which implement international publications referred to in this document may be found in the *BSI Catalogue* under the section entitled "International Standards Correspondence Index", or by using the "Search" facility of the *BSI Electronic Catalogue* or of British Standards Online.

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

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, the ISO title page, pages ii to v, a blank page, pages 1 to 107 and a back cover.

The BSI copyright notice displayed in this document indicates when the document was last issued.

Amendments issued since publication

Amd. No.	Date	Comments

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 30 June 2006

© BSI 2006

ISBN 0 580 48787 3

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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

Reference number
ISO 21188:2006(E)

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

Contents

Page

Foreword ... iv

Introduction ... v

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? ... 9
5.3 Business requirement impact on PKI environment ... 10
5.4 Functional perspectives ... 14
5.5 Business perspectives ... 19
5.6 Certificate policy (CP) ... 21
5.7 Certification practice statement (CPS) ... 23
5.8 Relationship between certificate policy and certification practice statement ... 24
5.9 Agreements ... 25
5.10 Time-stamping ... 26

6 Certificate policy and certification practice statement requirements ... 27
6.1 Certificate policy (CP) ... 27
6.2 Certification practice statement (CPS) ... 29

7 Certification authority control objectives ... 29
7.1 General ... 29
7.2 CA environmental control objectives ... 30
7.3 CA key life cycle management control objectives ... 32
7.4 Subject key life cycle management control objectives ... 33
7.5 Certificate life cycle management control objectives ... 34
7.6 CA certificate life cycle management controls ... 36

8 Certification authority control procedures ... 36
8.1 General ... 36
8.2 CA environmental controls ... 36
8.3 CA key life cycle management controls ... 51
8.4 Subject key life cycle management controls ... 55
8.5 Certificate life cycle management controls ... 60
8.6 CA certificate life cycle management controls ... 67

Annex A (informative) **Management by certificate policy** ... 69

Annex B (informative) **Elements of a certification practice statement** ... 78

Annex C (informative) **Object identifiers (OID)** ... 94

Annex D (informative) **CA key generation ceremony** ... 96

Annex E (informative) **Mapping of RFC 2527 to RFC 3647** ... 100

Bibliography ... 106

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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*.

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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.

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.

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

blank

Documents
Document Sharing Hub

Full document details: BS 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.

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.

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*

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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)

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)

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

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

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

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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)

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

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

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

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

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

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

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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.

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

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

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

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

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**

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

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

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

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.

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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 on-line communications. A TSP is a recognized authority trusted by one or more relying parties to create and sign certificates. A TSP may also revoke certificates it has created and issued. A TSP operates one or more certification authorities (CAs) whose core functions are certificate issuing, manufacturing and certificate validation. Within a financial institution, a CA is not necessarily a business entity but may 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[1)] to a single financial institution's trust service, and must share at least one certificate policy. See Figure 1 and Table 1.

b) **Contractual environment**: certificate subjects and relying parties may 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 may use different certificate policies;

   3) accreditation bridge that may recognize different certificate policies through central organization or entity.

See Figure 2 and Table 2.

c) **Open environment**: the financial institution may act as a TSP issuing certificates to the public and permits validation of certificates in an open network environment. TSPs may operate under voluntary TSP accreditation schemes or within an indigenous regulatory framework. Typically, there is no formal contract between the subscriber's TSP and the relying party. See Figures 3 and 4 and Table 3.

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

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 may use PKI for internal purposes and to support its services and communications internally or to its customers.

---

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 International Standard.

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

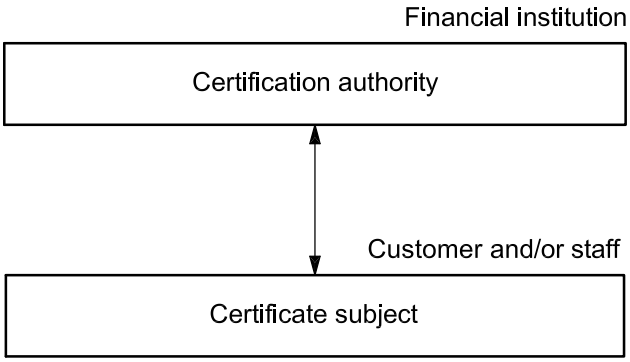

Figure 1 — Two entities in a closed environment

Table 1 — Certificate application scenarios in a closed environment

	Typical scenarios	Sample requirements	PKI operations
1	The financial institution (FI) sends an e-mail 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 e-mails between employees contained within the FI's network boundaries.	• Authentication of sender for recipient. • Message integrity for sender and recipient. • Confidentiality protection for message contents.	• Recipient validates sender's certificate. • Sender creates digital signature. • Recipient verifies digital signature. • Sender fetches recipient's certificate from directory. • Sender encrypts message with recipient's public key. • Recipient decrypts message with recipient's private key.
3	Travelling sales force with FI laptops need to exchange customer and sales information with centralized support systems.	• Mutual authentication of employee by the FI and server by employee. • Confidentiality protection for data.	• Provision of employee identification certificates. • Provision of server ID certificate. • Invoke SSL encryption. • Invoke SSL encryption.
4	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	Customer using a remote banking service where the server and browser application are provided by the FI.	• Mutual authentication of client (customer) by the FI and server by customer software. • Confidentiality protection for customer data.	• Customer authenticates to service using client certificate. • Server authenticates to customer using server certificate. • Invoke SSL encryption.

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

5.3.3 Illustration of certificate application in a contractual 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. It will provide either certificate issuance or certificate validation services, or both services, to its customers.

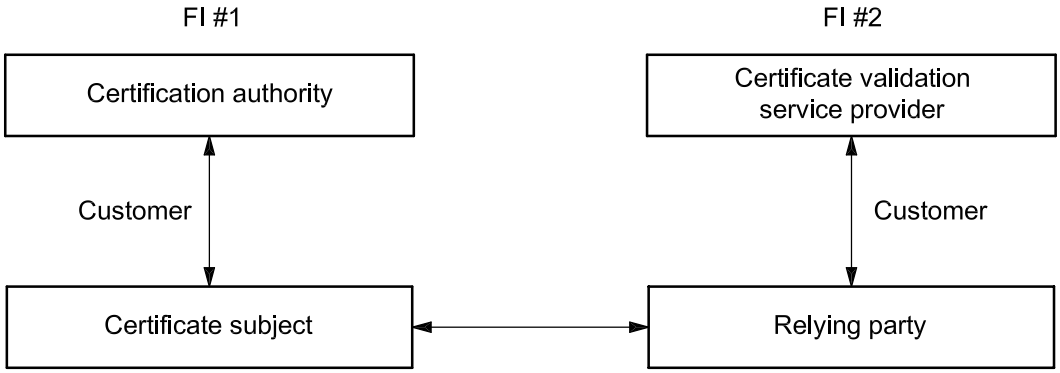

Figure 2 — Four entities in a contractual environment

Table 2 — Certificate application scenarios in a contractual environment

	Typical scenario	Sample requirements	PKI operations
1	FI employee sends an e-mail via the Internet to a customer that uses another TSP.	• Authentication of sender for recipient. • Message integrity. • Confidentiality protection for message contents.	• Recipient validates sender's certificate. • Customer checks digital signature. • 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 using certificate demonstrating mandated authority. • 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. • Sender fetches recipient's certificate from directory. • Sender encrypts message using recipient's public key. • Recipient decrypts message using recipient's private key.

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

Table 2 (*continued*)

	Typical scenario	Sample requirements	PKI operations
5	Corporate customer sends payment files directly to an automated clearing house.	• Authentication of sender (account holder) for recipient. • Message integrity and non-repudiation proof. • Confidentiality protection for message contents. • Dual customer authorization.	• Clearing house validates customer's certificate. • Clearing house verifies digital signature. • Customer fetches clearing house's certificate from directory. • Sender encrypts message using recipient's public key. • Recipient decrypts message using recipient's private key. • Two individuals digitally sign the payment files. • Clearing house verifies both digital signatures.
6	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 may offer trust services to its customers.

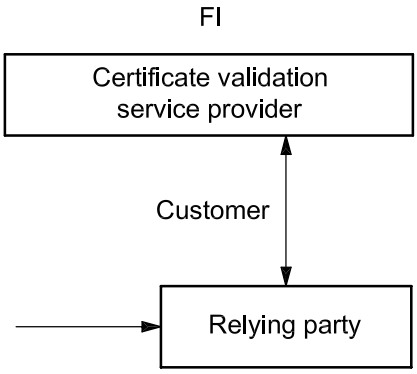

Figure 3 — FI acting as certificate validation service provider in an open environment

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

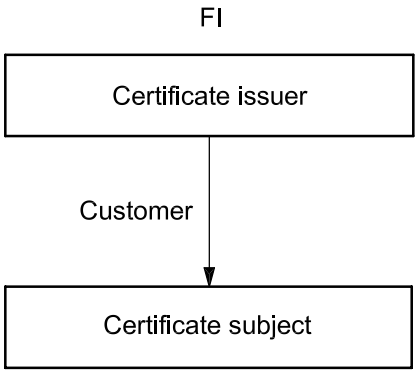

Figure 4 — FI acting as certificate issuer in an open environment

Table 3 — Certificate application scenarios in an open environment

	Scenario	Sample requirements	PKI operations
1	Web site visitor downloads executable code while browsing a financial institution's Web site.	• Authentication of FI. • Integrity of FI executable code.	• User validates FI's certificate. • User verifies FI's digital signature.
2	A customer visits an FI Web site.	• Authentication of an official FI Web site (i.e., not spoofed).	• User validates FI's server certificate.
3	Exchange of e-mails between two employees from different FIs via the Internet where there is no formal agreement in place.	• Authentication of sender for recipient. • Message integrity and non-repudiation proof. • Confidentiality protection for message contents.	• Each FI employee validates the sender's certificate. • Each FI employee verifies digital signature. • 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 e-mails between two customers using different TSPs.	• Authentication of sender for recipient. • Message integrity. • Confidentiality protection for message contents.	• Each customer validates the sender's certificate. • Each customer verifies the digital signature on the message received. • Each customer fetches the recipient's certificate from the directory.

5.4 Functional perspectives

PKI may be viewed from a number of different perspectives. The hardware, software and security procedures provide a rich set of PKI functions that can be logically grouped into PKI roles that are specified below. The subclauses that follow describe the policy authority (a), the components of a certification authority (b to g), subjects (h) and relying parties (i). A typical allocation of functions to roles is provided below though specific functions may be undertaken by different roles. Multiple roles may be undertaken by the same organization.

Figure 5 is a high-level representation of the functional elements within a PKI and their relationships.

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

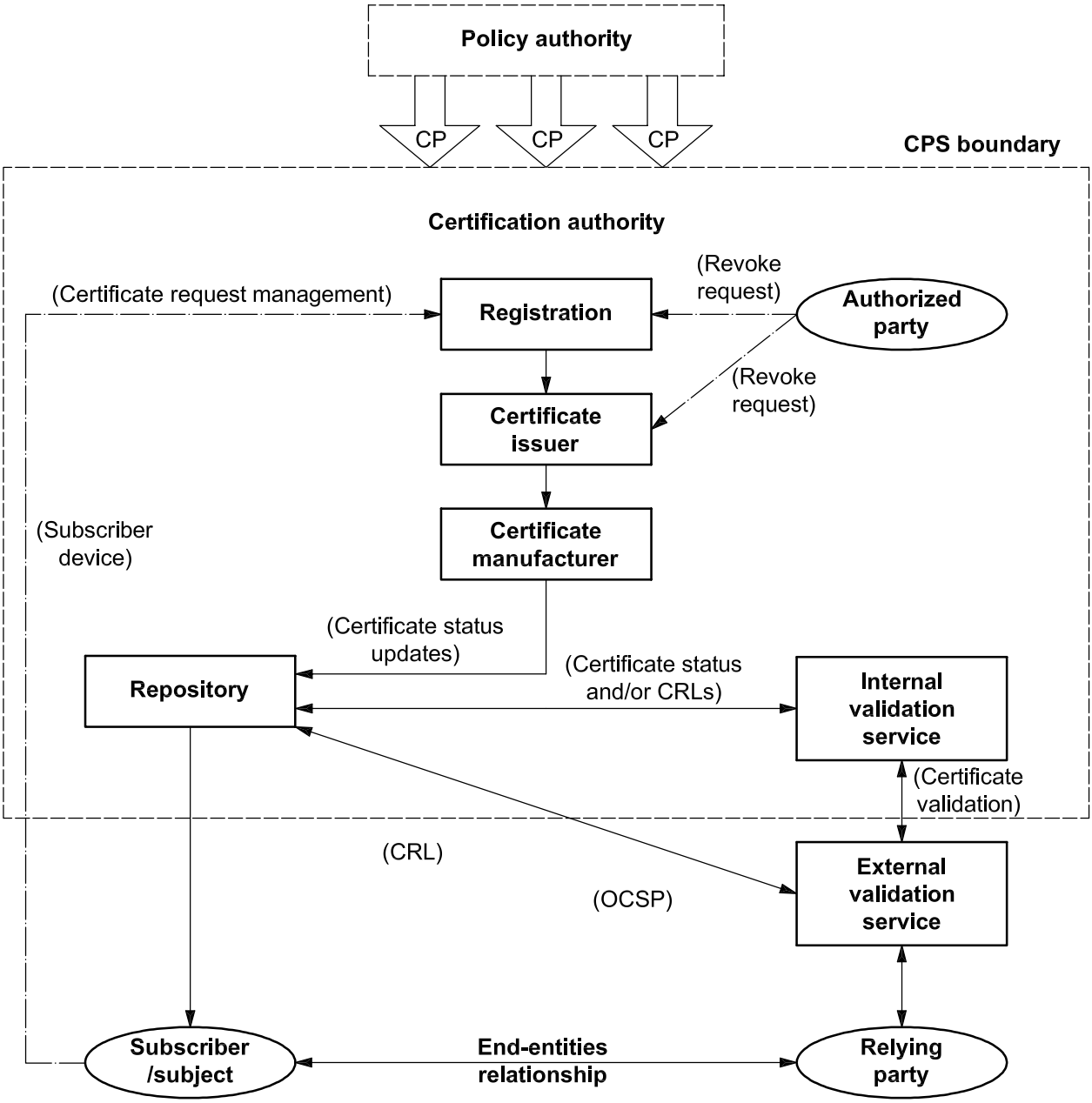

Figure 5 — Policy authority, certification authority and end-user relationships

The term “certification authority” is used in this International Standard to reflect the aggregate of the following PKI roles specified above, including: certificate issuer, certificate manufacturer, registration authority, repository, certificate validation service provider, and subject cryptographic mechanism provider. The policy authority is ultimately responsible for the effectiveness of the controls, management and operations of the CAs authorized to issue certificates under its certificate policies. The controls that the CA uses are defined within its certification practice statement.

a) **Policy authority (PA)** performs the following management functions:

— creates, maintains and approves the certificate policies;

— specifies the content of public key certificates as described by a certificate policy;

— distributes and promotes certificate policies;

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

— interprets adherence to its certificate policies;

— authorizes parties to act as certification authorities under the certificate policies;

— approves certification practice statements for authorized CAs;

— resolves or causes resolution of disputes related to certificate policies;

— ensures regulatory compliance;

— ensures that the provisions of the CP remain valid with regard to potential security threats;

— receives and reviews reports of CA security incidents and actions taken;

— approves and documents within the CP the procedures for revocation of certificates, including:

  — who may submit revocation requests and reports;

  — how they may be submitted;

  — any requirements for subsequent confirmation of revocation reports and requests;

  — whether and for what reasons certificates may be suspended;

  — the mechanism used for distributing revocation status information;

— specifies the maximum delay between receipt of a revocation request or report and the change to the revocation status information available to all relying parties based on a risk analysis.

b) **Certificate issuer (CI)** performs the following management functions:

— manages the processes for issuing public key certificates;

— issues and manages certificate status;

— enters into a contractual arrangement with a subscriber under a subscriber agreement or banking terms and conditions;

— issues certificates to certificate subjects under one or more certificate policies;

— provides a means for subjects or, where applicable, subscribers to request revocation;

— arranges and manages the processes to revoke public key certificates;

— owns and controls its signing key(s) and therefore can switch certificate manufacturers;

— maintains ownership and control of its business records;

— subscribes to a CPS;

— processes upon receipt requests and reports relating to revocation;

— authenticates source for requests and reports of certificate revocation (i.e., checked to be from an authorized source);

— notifies the subject and, where applicable, the subscriber of a revoked or suspended certificate;

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

— provides directly or approves of the mechanisms of performing cryptographic signing and, where applicable, decipherment functionality, under the terms of the certificate policy;

— manages the obligations and liabilities as stated in the CP.

c) **Certificate manufacturer (CM)** performs the following CA operational functions:

— creates and maintains its own CPS;

— operates within the bounds of its CPS;

— generates and distributes public key certificates;

— generates and manages certificate signature asymmetric key pairs consistent with the specifications provided by a certificate issuer;

— distributes the certificate issuer's public key(s) certificates;

— generates information on certificate status (such as CRLs);

— provides out-of-band notifications of certificate issuance and revocation where required;

— maintains separation between different hosted certificate issuers;

— maintains security, availability and continuity of the certificate signing function as specified in its CPS;

— periodically demonstrates audited compliance with the certification authority control objectives specified in Clause 7;

— ensures regulatory compliance;

— ensures that the provisions of the CPS remain valid with regard to potential security threats;

— optionally generates subscriber key pairs at the request of the RA where permitted by the CP.

d) **Registration authority (RA)** performs the following operational functions:

— manages a public key certification request from a subject or, where applicable, a subscriber;

— manages the distribution of subscriber key pairs where the CM has generated the key pairs as permitted by the CP;

— performs the registration process by:

  — checking the subject's credentials evidencing claimed identity in line with regulatory know-your-customer requirements (e.g., money-laundering requirements);

  — verifying that identifying data provided by the certificate subject is valid;

  — verifying that the identifying data pertain to the certificate subject;

  — verifying that the certificate subject is entitled to obtain a public key certificate under the certificate policy;

  — verifying that the certificate subject possesses the asymmetric private key corresponding to the public key;

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

— manages the submission of certificate requests to the certificate manufacturer;

— records the binding of the certificate subject's identification data to the certificate subject's public key;

— receives and processes certificate subject or, where applicable, subscriber requests to revoke certificates, suspend certificates and reinstate suspended certificates;

— operates within the bounds of the applicable certificate policies and where applicable the CM's CPS.

e) **Repository** performs the following technological functions:

— stores and distributes public key certificates;

— stores and distributes information on certificate status (such as CRLs and/or online certificate status);

— stores and distributes PKI public information (e.g., certificate policy).

f) **Certificate validation service provider (CVSP)** performs the following functions:

— enters into a contractual arrangement with the relying PARTY, and when undertaken formally, parties sign a relying party agreement;

— enters into a contractual arrangement with the policy authority to collect information on the certificate policies and update the status of the associated certificates;

— operates within the bounds of its own organizational policies and applicable certificate policies;

— maintains the status of certificates where the CVSP holds certificates on behalf of other trust service providers in accordance with the certificate policy;

— seeks to obtain the current status on certificates from other trust service providers;

— validates the status of a certificate and provides a response to the requestor.

g) **Subject cryptographic mechanism provider (SCMP)** performs the following function:

— supplies a mechanism that consists of a physically secure-signature-creation device (e.g. an ICC) or alternatively a software emulation that provides comparable functionality in order to:

  — securely store the subject's private key and associated certificates;

  — enable secure activation and deactivation of the private key;

  — provide a secure initial activation mechanism.

h) **Subject or, where applicable, subscriber (S)** performs the following functions:

— presents their credentials as evidence for claimed identity in accordance with the relevant certificate policy;

— generates or causes to be generated one or more asymmetric key pairs;

— presents the public key certification request to the registration authority;

— complies with the asymmetric private key protection requirements (i.e., key storage and cardholder verification);

— reports loss or compromise of private key(s) and inaccuracy of certificate information;

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

— uses their key pair(s) in conjunction with authorized business applications in compliance with applicable policies and in accordance with the CP;

— uses their own private key (signing) to cryptographically sign message digests or similar data elements;

— uses their own private key (encipherment) to decrypt messages.

i) **Relying party (RP)** performs the following functions:

— validates subject public key certificates or requests the validation of certificate subject public key certificates through a CVSP;

— uses the public key in the subject's certificate for authorized business applications and appropriate cryptographic functions (e.g. digital signature verification, key exchange, etc.) in compliance with applicable policies and in accordance with the CP;

— uses the subject's public key to check the validity of the digital signature;

— uses the subject's public key (confidentiality) and appropriate cryptographic mechanism to encipher messages to provide confidentiality protection (optional).

It is possible for any or all of the certification authority roles to be delegated to one or more third party organizations, either directly or indirectly; nevertheless, it is the responsibility and liability of the certificate issuer to manage the associated CP risks.

5.5 Business perspectives

5.5.1 General

A financial institution's future ability to participate in an on-line 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 on-line 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, including the consideration of 5.5.2 to 5.5.7.

5.5.2 Business risks

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

5.5.3 Applicability

The parties involved must 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 may 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 may specify any limitations to these liabilities, such as specifying a group whose members are the only parties permitted to act as relying parties. It may 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.

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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

Optionally, under a warranty scheme, a reliance limit may be established by the CP or by separate agreement. Where this is the case, the relying party may 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 may 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, may support the same CP.

a) A CP may 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.

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

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 may differ due to interpretation of standards and protocols by the PKI integrators. A technical comparison must 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 may even involve other third party CAs that assist in providing a trusted path through a chain of cross-certificates. Care needs to be taken in the policy implications of such cross-certificates and in particular that the implied trust relationship is matched by an appropriate business relationship.

CAs may 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 must accept policies used by its own CA and that of the another CA;

or

— there must 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.

5.6 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 may 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 may 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;

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

— 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 may 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 must 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 on-line 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).

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, etc.). 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 must use a self-signed certificate and may only be used to sign subordinate certificates. A subordinate CA must be defined based upon geopolitical, organizational or other requirements. The subordinate CAs must cascade into multiple levels based upon multiple structural needs or it may issue certificates to end-entities.

In a hierarchy, the root must be the most trusted point. Each subordinate level shares the trust between their peers, but each must 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 6);

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 6).

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

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

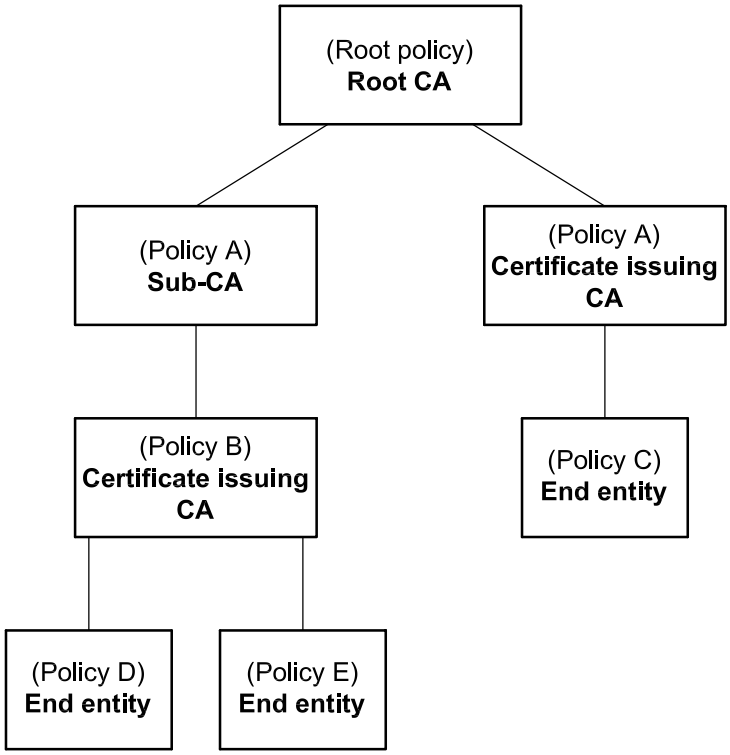

Figure 6 — Root hierarchy creates a hierarchy of trust

5.6.4 Certificate status

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

As defined in ISO 15782-1, a certificate may be in one of the following states:

a) live – operational;

b) suspended (state called “on hold” in ISO 15782-1);

c) revoked;

d) expired.

Once a certificate is revoked or expired it cannot return to a live state. Refer to ISO 15782-1 for further discussion of certificate management.

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)

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

Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

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 may 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 may 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 may also be part of the contract between the CA and the subscriber. When the legal relationship between a CA and subscriber is consensual, (e.g. in a case of a home banking relationship between a consumer or corporation and a bank), a contract, such as a subscriber or account agreement, would be a means of giving effect to the contents of the CPS.

5.8 Relationship between certificate policy and certification practice statement

5.8.1 General

The roles of the certificate policy and certification practice statement are illustrated in 5.8.2 to 5.8.6.

5.8.2 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 may 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 may suffice with a contractual PKI environment, a CPS, nevertheless, provides guidance for both internal processing and processing completed by delegated roles.

5.8.3 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.

5.8.4 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 may describe specific tasks and responsibilities within an organization. Such documentation may be used in the daily operation of the CA and reviewed by those performing a process review or audit.

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

5.8.5 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.

5.8.6 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 should 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 may be considered confidential. If the circulation of the CPS is restricted, financial institutions may use a PKI Disclosure Statement, indicating the type and nature of the controls without disclosing specific control details to support the CP.

For example, the CP may 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 may 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 may 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.

5.9 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.

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 may be used for this purpose or alternatively an independent assessment may be used to determine the suitability of the controls described in the CPS. However, at its discretion, the certification authority may 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 may be made available to the respective CAs prior to cross-certification.

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006

Figure 7 provides an overview of the typical control documents within the standard financial PKI model.

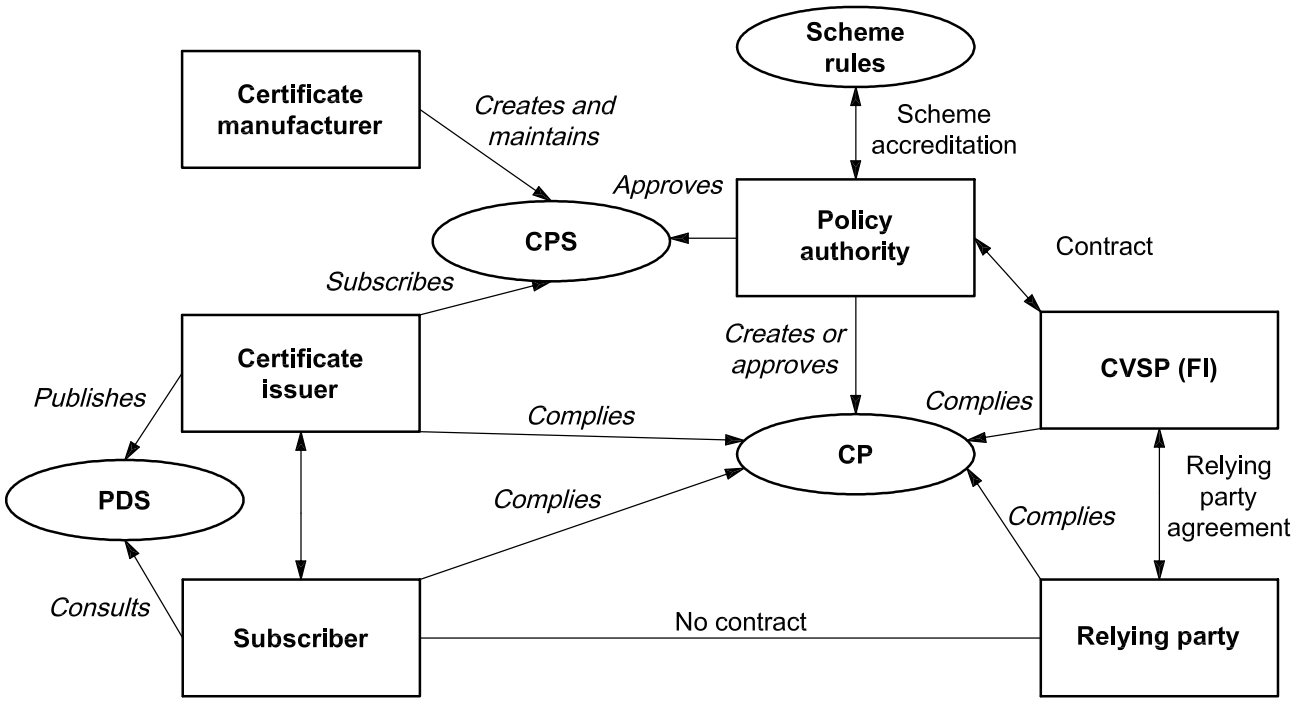

Figure 7 — Control documents within standard financial PKI model

5.10 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 certificate is used to protect data outside that period then the validity of the certificate cannot be assured. Secondly, if a certificate is revoked then any use of the certificate after the time that it is revoked may be considered to be invalid. Thus, if there may be a significant time between the application of a certificate in securing data and the checking of the validity of the protection, e.g. when applying a digital signature to stored data, it is important to be assured of the time at which the signature was applied. If it can be assured that a signature was created before the supporting certificate had expired or was revoked, then the validity of signature can be assured long after either of those events. It is for the relying party to determine whether they accept the risk associated with a certificate that may have expired or may have been revoked in the interim period.

A method of providing assurance of the time that a signature was created is to employ a trusted third party, commonly called a time-stamping authority (TSA) to bind a time to the digital signature on or near the time that the signature was created. This technique is commonly called time-stamping. An example time-stamping protocol is defined in ISO 18014-2. 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 may be applied to ensure the ongoing protection of the signed data.

Documents
Document Sharing Hub
Full document details: BS ISO 21188:2006

Such an application of time-stamping may 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 be valid at that time even though the certificate may subsequently have been revoked.

A variation of the time-stamping mechanism described above 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 18014-3). Another variation is to employ several independent time-stamping authorities and so avoid dependence on a single trusted authority.

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 or more certificate policies as defined in 8.2.6 of ISO 15782-1:2003.

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 may be acquired (e.g. URL, e-mail address, OID, etc.).

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.

e) CP shall include disclosure of governing law or how the governing law is determined.

f) CP shall identify subscriber obligations and liabilities. CP should include subscriber obligations and liabilities in order to:

— provide information in certificate request that is accurate and that the act of accepting the certificate guarantees that information contained is accurate;

— guarantee that if the subscriber or the certificate subject generates the public key pairs, it will be done in a manner appropriate to the control objectives specified (see 8.3.4);

— protect the access to the private key associated with certificate;

AVA Documents
Document Sharing Hub

Full document details: BS ISO 21188:2006