BRITISH STANDARD

BS ISO 15782-1:2009

Certificate management for financial services

Part 1: Public key certificates

ICS 03.060; 35.240.40

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW

Document Sharing Hub
British Standards

Full document details: BS ISO 15782-1:2009

National foreword

This British Standard is the UK implementation of ISO 15782-1:2009.

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.

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 31 December 2009

© BSI 2009

ISBN 978 0 580 59821 0

Amendments/corrigenda issued since publication

Date	Comments

Documents
Document Sharing Hub

Full document details: BS ISO 15782-1:2009

INTERNATIONAL STANDARD

ISO 15782-1

Second edition
2009-10-15

Certificate management for financial services —

Part 1: Public key certificates

Gestion de certificats pour les services financiers —

Partie 1: Certificats de clé publique

Reference number
ISO 15782-1:2009(E)

Documents
Document Sharing Hub
© ISO 2009

Full document details: BS ISO 15782-1:2009

PDF disclaimer

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

Adobe is a trademark of Adobe Systems Incorporated.

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

COPYRIGHT PROTECTED DOCUMENT

© ISO 2009

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

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

Published in Switzerland

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub

Full document details: BS ISO 15782-1:2009

Contents

Page

Foreword iv
Introduction v
1 Scope 1
2 Normative references 2
3 Terms and definitions 2
4 Symbols and abbreviations 8
5 Public key infrastructure 8
5.1 Overview 8
5.2 Public key management infrastructure process flow 9
5.3 Certification Authority (CA) 9
5.4 Registration Authority (RA) 10
5.5 End entities 10
6 Certification Authority systems 10
6.1 General 10
6.2 Responsibilities in CA systems 12
6.3 Certificate life cycle requirements 15
6.4 Security quality assurance and audit requirements 29
6.5 Business continuity planning 30
7 Data elements and relationships 30
8 Public key certificate and Certificate Revocation List extensions 30
Annex A (normative) **Certification Authority audit journal contents and use** 31
Annex B (informative) **Alternative trust models** 34
Annex C (informative) **Suggested requirements for the acceptance of certificate request data** 40
Annex D (informative) **Multiple algorithm certificate validation example** 42
Annex E (informative) **Certification Authority techniques for disaster recovery** 44
Annex F (informative) **Distribution of certificates and Certificate Revocation Lists** 47
Bibliography 48

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 15782-1:2009

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 15782-1 was prepared by Technical Committee ISO/TC 68, *Financial services*, Subcommittee SC 2, *Security management and general banking operations*.

This second edition cancels and replaces the first edition (ISO 15782-1:2003), which has been technically revised.

ISO 15782 consists of the following parts, under the general title *Certificate management for financial services*:

— *Part 1: Public key certificates*

— *Part 2: Certificate extensions*

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 15782-1:2009

Introduction

This part of ISO 15782 adopts ISO/IEC 9594-8 for the financial services industry and defines certificate management procedures and data elements.

Detailed requirements for the financial industry for the individual extensions are given in ISO 15782-2.

While the techniques specified in this part of ISO 15782 are designed to maintain the integrity of financial messages and support the service of non-repudiation, this part of ISO 15782 does not guarantee that a particular implementation is secure. It is the responsibility of the financial institution to put an overall process in place with the necessary controls to ensure that the process is securely implemented, with these controls including the application of appropriate audit tests in order to validate compliance.

The binding association between the identity of the owner of a public key and that key is documented in order to prove the ownership of the corresponding private key. This binding is called a public key certificate. Public key certificates are generated by a trusted entity known as a Certification Authority (CA).

The proper implementation of this part of ISO 15782 is intended to provide assurances of the binding of the identity of an entity to the key used by that entity to sign documents, including wire transfers and contracts.

This part of ISO 15782 defines a certificate management framework for authentication, including the authentication of keys for encryption. The techniques specified by this part of ISO 15782 can be used when initiating a business relationship between legal entities (entities).

© ISO 2009 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO 15782-1:2009

Documents
Document Sharing Hub

Full document details: BS ISO 15782-1:2009

INTERNATIONAL STANDARD ISO 15782-1:2009(E)

Certificate management for financial services —

Part 1:
Public key certificates

1 Scope

This part of ISO 15782 defines a certificate management system for financial industry use for legal and natural persons that includes

— credentials and certificate contents,

— Certification Authority systems, including certificates for digital signatures and for encryption key management,

— certificate generation, distribution, validation and renewal,

— authentication structure and certification paths, and

— revocation and recovery procedures.

This part of ISO 15782 also recommends some useful operational procedures (e.g. distribution mechanisms, acceptance criteria for submitted credentials).

Implementation of this part of ISO 15782 will also be based on business risks and legal requirements.

This part of ISO 15782 does not include

— the protocol messages used between the participants in the certificate management process,

— requirements for notary and time stamping,

— Certificate Policy and Certification Practices requirements, or

— Attribute Certificates.

While this part of ISO 15782 provides for the generation of certificates that could include a public key used for encryption key management, it does not address the generation or transport of keys used for encryption.

Implementers wishing to comply with ISO/IEC 9594-8 can utilize the certificate structures defined by that International Standard. Those wishing to implement compatible certificate and certificate revocation structures but without the overhead associated with the X.500 series can utilize the ASN.1 structures defined in ISO 15782-2. ISO 15782-2 can also be referred to for a financial services profile of certificate and CRL extensions.

ISO 21188 provides additional information for implementers on Certificate Policies, Certification Practice Statements, and PKI controls. ISO 21188 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.

NOTE The use of a bold sans serif font, such as **CertReqData** or **CRLEntry,** denotes the use of abstract syntax notation (ASN.1), as defined in ISO/IEC 8824-1 to ISO/IEC 8824-4 and ISO/IEC 8825-1 and ISO/IEC 8825-2. Where it makes sense to do so, the ASN.1 term is used in place of normal text. Refer to ISO 15782-2 for related ASN.1 modules.

Documents
Document Sharing Hub

© ISO 2009 – All rights reserved

Full document details: BS ISO 15782-1:2009

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 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

ISO/IEC 8824-2, *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification — Part 2*

ISO/IEC 8824-3, *Information technology — Abstract Syntax Notation One (ASN.1): Constraint specification — Part 3*

ISO/IEC 8824-4, *Information technology — Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications — Part 4*

ISO/IEC 8825-1, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) — Part 1*

ISO/IEC 8825-2, *Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER) — Part 2*

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

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

ISO 15782-2:2001, *Banking — Certificate Management — Part 2: Certificate extensions*

ISO 16609, *Banking — Requirements for message authentication using symmetric techniques*

ISO 21188:2006, *Public key infrastructure for financial services — Practices and policy framework*

3 Terms and definitions

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

3.1
ASN.1 module
identifiable collection of ASN.1 types and values

3.2
attribute
characteristic of an entity

3.3
audit 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

3.4
authorization
granting of rights

3.5
CA certificate
certificate whose subject is a CA, and whose associated private key is used to sign certificates

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 15782-1:2009

3.6
certificate hold
certificate suspension
temporary interruption of the validity of a certificate by the CA

3.7
certificate information
information in a certificate which is signed

3.8
certificate policy
named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements

EXAMPLE A particular Certificate Policy might indicate the applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

NOTE 1 The Certificate Policy should be used by the user of the certificate to decide whether or not to accept the binding between the subject (of the certificate) and the public key. Some of the components in the Certificate Policy framework are given concrete values and represented by a registered object identifier in the X.509, Version 3 certificate. The object owner also registers a textual description of the policy and makes it available to the Relying Parties.

NOTE 2 The Certificate Policy object identifier can be included in the following extensions in the X.509, Version 3 certificates: Certificate Policies, policy mappings, and policy constraints. The object identifier(s) may appear in none, some, or all of these fields. These object identifiers may be the same (referring to the same Certificate Policy) or may be different (referring to different Certificate Policies).

3.9
certificate policy framework
comprehensive set of security- and liability-related components that can be used to define a Certificate Policy

NOTE A subset of the components in the Certificate Policy framework are given concrete values to define a Certificate Policy.

3.10
certificate re-key
process whereby an entity with an existing key pair and certificate receives a new certificate for a new public-key, following the generation of a new key pair

3.11
certificate renewal
process whereby an entity is issued for a new instance of an existing certificate with a new validity period

3.12
certificate request data
credentials
signed information in a certificate request, including the entity's public key, entity identity and other information included in the certificate

3.13
certificate revocation list
CRL
list of revoked certificates

3.14
certification
process of creating a public key certificate for an entity

3.15
certification authority
CA
entity trusted by one or more entities to create, assign, and revoke or hold public key certificates

Documents
Document Sharing Hub

© ISO 2009 – All rights reserved

Full document details: BS ISO 15782-1:2009

3.16
certification authority system
set of entities, including a CA, that manages certificates throughout the life of the certificate

NOTE The entities are responsible for

— generation,

— submission,

— registration,

— certification,

— distribution,

— use,

— renewal,

— re-key,

— revocation or hold, and

— expiry.

3.17
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

3.18
certification practice statement
CPS
statement of the practices which a Certification Authority employs in issuing and managing certificates through their life cycle

3.19
compromise
violation of the security of a system such that an unauthorized disclosure or modification of sensitive information may have occurred

3.20
confidentiality
property that information is not made available or disclosed to unauthorized individuals, entities, or processes

3.21
CRL distribution point
directory entry or other distribution source for CRLs

NOTE A CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.

3.22
cross-certification
process by which two CAs mutually certify each other's public keys

cf. **policy mapping** (3.44)

3.23
(cryptographic) key
parameter that determines the operation of a cryptographic function

NOTE Cryptographic functions include the following:

— the transformation from plain text to cipher text and vice versa;

— synchronized generation of keying material;

— digital signature generation or validation.

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 15782-1:2009

3.24
cryptographical hash
mathematical function which maps values from a large (possibly very large) domain into a smaller (fixed) range

NOTE It satisfies the following properties:

— it is computationally unfeasible to find any input which maps to a pre-specified output (i.e. pre-image resistant);

— it is computationally unfeasible to find any two distinct inputs which map to the same output (i.e. collision-resistant).

3.25
cryptographic module
device wherein cryptographic functions (e.g. encryption, authentication, key generation) are performed

3.26
cryptography
discipline which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof

3.27
cryptoperiod
time span during which a specific key is authorized for use or in which the keys for a given system may remain in effect

3.28
data integrity
property whereby data has not been altered or destroyed

3.29
delta-CRL
subset of a CRL indicating changes since the prior CRL update

3.30
(digital) signature
cryptographic transformation of data which, when associated with a data unit, provides the services of origin authentication and data integrity, and may support signer non-repudiation

3.31
directory
repository
method for distributing or making available certificates or CRLs

EXAMPLE A database or an X.500 Directory.

3.32
distinguished name
globally unique name for an entity

NOTE 1 Methods for determining global uniqueness are outside the scope of this part of ISO 15782.

NOTE 2 An entity may be issued for more than one certificate with the same distinguished name.

3.33
dual control
process of utilizing two or more separate entities (usually persons), who are operating in concert, to protect sensitive functions or information

NOTE 1 Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is able to access or to utilize the materials (e.g. cryptographic key).

NOTE 2 For manual key and certificate generation, conveyance, loading, storage, and retrieval, dual control requires split knowledge of key among the entities. Also see **split knowledge** (3.52).

Documents
Document Sharing Hub

© ISO 2009 – All rights reserved

Full document details: BS ISO 15782-1:2009

3.34
end entity
certificate subject, other than a CA, which uses its private key for purposes other than signing certificates

3.35
entity
legal (e.g. a corporation, labour union, state or nation) or natural person

EXAMPLE CA, RA or end entity.

3.36
financial message
communication containing information which has financial implications

3.37
key agreement
method for negotiating a key value without transferring the key, even in an encrypted form

EXAMPLE The Diffie-Hellman technique.

3.38
key fragment
part of a private key which has been divided into pieces (also called shares) that are distributed amongst entities such that the pooled fragments of specific subsets of entities can reconstitute the key

3.39
key management
handling of keying material throughout its life cycle in accordance with a security policy

3.40
key pair
⟨public key cryptography⟩ public key and its corresponding private key

3.41
keying material
data, such as keys, certificates and initialization vectors, necessary to perform cryptographic operations

3.42
non-repudiation
service which provides proof of the integrity and origin of data which can be verified by a third party

NOTE The non-repudiation service protects against the signing entity falsely denying the action and can provide rebuttable presumption. It requires that appropriate processes and procedures (registration, audit journals, contractual arrangements, personnel, etc.) be in place.

3.43
out-of-band notification
notification using a communication means independent of the primary communications means

3.44
policy mapping
recognition that, when a CA in one domain certifies a CA in another domain, a particular Certificate Policy 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

cf. **cross-certification** (3.22)

3.45
policy qualifier
policy-dependent information that accompanies a Certificate Policy identifier in an X.509 certificate

3.46
private key
⟨asymmetric (public) key cryptosystem⟩ key of an entity's key pair which is known only by that entity

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 15782-1:2009

3.47
public key
⟨asymmetric (public) key cryptosystem⟩ key of an entity's key pair which is publicly known

3.48
public key 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

3.49
public key validation
PKV
process that does arithmetic tests on a candidate public key to provide assurance that it conforms to the specifications of the standard

NOTE 1 Attacks may be possible on the owner and/or user if a non-conforming public key is used.

NOTE 2 Public key validation can include arithmetic property tests (range, order, primality, etc.), canonical generation tests and consistency tests between components of a public key. Methods for public key validation are typically found in financial industry signature standards.

3.50
registration authority
RA
entity that is responsible for identification and authentication of subjects of certificates, but is not a CA and hence does not sign or issue certificates

NOTE An RA may assist in the certificate application process, revocation process or both.

3.51
relying party
user
recipient of a certificate who acts in reliance on that certificate

3.52
split knowledge
condition under which two or more entities separately have key fragments which, individually, convey no knowledge of the resultant cryptographic key

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

3.54
subject CA
CA that is certified by the issuing CA

3.55
subscriber
entity subscribing with a Certification Authority on behalf of one or more subjects

3.56
trusted CA public key
public key used to validate the first certificate in a chain of certificates as a part of certification path processing

EXAMPLE The root key in a centralized trust model or a local CA key in a decentralized trust model (see Annex B).

NOTE If an end entity validates a chain of certificates from a trusted CA public key to the end certificate, then the end certificate is considered valid.

3.57
zeroize
active destruction of electronically stored data, such as by degaussing, erasing or overwriting

Documents
Document Sharing Hub

© ISO 2009 – All rights reserved

Full document details: BS ISO 15782-1:2009

4 Symbols and abbreviations

Symbols	Meaning
X{information}	Signing of “information” by X
X_p	X's public key. (e.g. X_{1p} is X_1's public key)
X_s	X's private key
X_1«X_2»	X_2's certificate issued by the CA, X_1
X_1«X_2»X_2«X_3»X_{n-1}«X_n»	Certificate path. Each item Xi<Xi+1> in the path is the certificate for the CA which produced the next item. This path is of arbitrary length and is functionally equivalent to X_1«X_n». Possession of X_{1p} allows a user to extract the authenticated public key of X_n.
X_{1p}·X_1«X_2»	Unwrapping of a certificate or path. The public key of the leftmost CA (X_1) is used to extract the authenticated public key of the rightmost certificate (X_1«X_2») by working through the path of intervening certificates. This example extracts X_{2p}.

NOTE The notation used in this part of ISO 15782 is a variant of the X.509 notation for certificates, certification paths and related information.

Abbreviations	Meaning
ASN.1	Abstract syntax notation
BER	Basic encoding rules
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DER	Distinguished encoding rules
DSA	Digital signature algorithm
ECDSA	Elliptic curve digital signature algorithm
PKI	Public key infrastructure
RA	Registration Authority
RSA	Rivest Shamir Adleman algorithm
SHA-1	Secure hash algorithm-1
URI	Uniform resource identifier

5 Public key infrastructure

5.1 Overview

Public key infrastructure (PKI) is a term used to describe the technical, legal and commercial infrastructure that enables the wide deployment of public key technology.

Public key technology is used for creating digital signatures and for managing symmetric keys. With public key cryptography, two keys are used: one is kept private with the user, the other is made publicly available. That which is signed or processed with one key (public or private) may be validated with its complement (public or private). Revealing the public key does not in any way compromise the private key.

The authentication of public keys is an essential requirement and, for this reason, public keys are housed in public key certificates. A certificate contains the public key and its identifying data and is digitally signed by a

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 15782-1:2009

Certification Authority (CA). This part of ISO 15782 is based on the ISO/IEC 9594-8 format for public key certificates.

As described in ISO 21188, the term “Certification Authority” reflects the aggregate of the following PKI roles including

— Certificate Issuer,

— Certificate Manufacturer,

— Registration Authority,

— Repository,

— Certificate Validation Service Provider, and

— Subject Cryptographic Mechanism Provider.

In this part of ISO 15782, we focus on the CA as a whole and on the RA function.

5.2 Public key management infrastructure process flow

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

— key generation;

— registration;

— certification;

— distribution;

— usage;

— revocation hold;

— expiry;

— renewal;

— re-key.

The main steps involved in certification are shown in Figure 1.

5.3 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 as described in 6.3.1. The certificate(s) and proof of validation shall be maintained by the validator in an audit journal. A CA may issue certificates to any entities, including CAs.

Entities (including CAs) can use these certificates to authenticate themselves to Relying Parties. Hence, authentication may involve a chain of certificates. The verification of a chain of certificates begins with the

Documents
Document Sharing Hub

© ISO 2009 – All rights reserved

Full document details: BS ISO 15782-1:2009

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 6.3.1, Annex C and ISO/IEC 9594-8.

Once a certificate has been generated, the integrity of its contents is protected. This part of ISO 15782 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 information needed.

Two general architectures may be configured for certification paths: hierarchical and non-hierarchical. In a hierarchical architecture, authorities are arranged under a “root” CA that issues certificates to subordinate CAs. These subordinate CAs may 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 may 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 may 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, which is a common non-hierarchical architecture, a central CA cross-certifies to the other CAs. The public key of the central bridge CA is known to all other trusted CAs and the public key of each trusted CA is known to the bridge CA. The certification path consists of two certificate chains, Subject to Subject's trusted CA and Relying Party to Relying Party's trusted CA, interconnected by the bridge CA-certificates.

A compromise of the private key of a CA compromises all users of certificates of the 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 of transactions in a financial network can have catastrophic effects on financial institutions and their customers.

Figure 1 summarizes the life cycle of an end-entity certificate.

5.4 Registration Authority (RA)

An RA is an entity that is responsible for identification and authentication of the subjects of certificates, but is not a CA, and hence does not sign or issue certificates. An RA may assist in the certificate application process, revocation process, or both. The RA does not need to be a separate body, but can be part of the CA.

5.5 End entities

An end entity is a certificate subject which uses its private key for purposes other than signing certificates.

6 Certification Authority systems

6.1 General

A CA and one or more RAs may be configured as a CA system, and the functional allocation between CAs and RAs will vary, based on implementation.

© ISO 2009 – All rights reserved
Documents
Document Sharing Hub
Full document details: BS ISO 15782-1:2009