

1st edition, May 2004

Original

R

Railway Public Key Infrastructure Recommendations for Interoperability

This leaflet is to be published only in English



UNION INTERNATIONALE DES CHEMINS DE FER
INTERNATIONALER EISENBAHNVERBAND
INTERNATIONAL UNION OF RAILWAYS

Leaflet to be classified in Volume:

IX - Information Technology, Miscellaneous

Application:

With effect from 1 January 2004

All members of the International Union of Railways

Record of updates

1st edition, May 2004

First issue

The person responsible for this leaflet is named in the UIC Code

Contents

Summary	1
1 - Introduction	2
2 - A public key infrastructure.....	3
2.1 - The concept.....	3
2.2 - Key points when building a PKI	4
2.2.1 - Background.....	4
2.2.2 - X.509 Certificate Fields.....	5
2.2.3 - Identification.....	5
2.2.4 - Community and applicability	6
2.2.5 - Liability	7
2.2.6 - Financial responsibility.....	7
2.2.7 - Interpretation and enforcement.....	7
2.2.8 - Publication and repository.....	7
2.2.9 - Compliance audit	7
2.2.10 - Confidentiality	7
2.2.11 - Identification and authentication	7
2.2.12 - Certificate renewal, update and re-key	8
2.2.13 - Operational requirements	8
2.2.14 - Physical, procedural and personnel security controls.....	12
2.2.15 - Technical security controls.....	12
2.3 - Rail Certification Authority	14
3 - Specifications for interoperability	15
3.1 - Scope	15
3.2 - Levels of interoperability	15
3.2.1 - Component-level interoperability	15
3.2.2 - Application-level interoperability	17
3.2.3 - Inter-domain interoperability	18
3.2.4 - Summary of interoperability issues	19

3.3 - Multiple CA interoperability	20
3.3.1 - Bridge Certification Authority concept.....	20
3.3.2 - Technical issues	21
3.3.3 - Policy and business issues	24
3.3.4 - Legal issues	25
Appendix A - Summary of the MISR.....	26
Appendix B - The UIC as BCA	29
Glossary	32
List of abbreviations	36
Bibliography	38

Summary

The leaflet has been drawn up for UIC members who plan to implement, or have implemented, a public key infrastructure in their organisations. It provides implementers with the minimum recommended security requirements to allow interoperability between Public Key Infrastructures (PKIs).

The leaflet addresses three main points. The first describes the building of a PKI for data exchange on a domestic level between RUs, clients and IMs. The second is dedicated to the interoperability of PKIs and the minimum interoperability security requirements (MISR) to guarantee secure exchange. And the third point, comprised of appendices, summarises a recommended set of MISR to be respected and an example of a Bridge Certificate Authority (BCA) as it could be provided by the UIC.

1 - Introduction

Railways are affected by electronic commerce and the "Internet phenomenon". Many of them have their own Internet sites via which they offer their customers increasingly sophisticated services (on-line ticket sales, tracing consignments, etc.) or have already embarked on business-to-business data interchange via Internet. Of course these railways apply a certain level of data security to protect these data exchanges.

When security functions are used in information-processing applications to protect information, they must guarantee the authentication (see Glossary - page 32) and origin of a message, detect any loss of integrity (see Glossary - page 32), protect confidentiality and ensure non-repudiation (see Glossary - page 32) of an action at a given point in time. Today, public key (see Glossary - page 32) cryptography, previously restricted to military and banking fields, provides an answer to these security needs. In this technology, an electronic identity known as a public key certificate (see Glossary - page 32) represents the user.

Like many other players on the international economic scene, the railway industry will become a user of public key certificates, both in their internal relations and in the services they offer to individual customers and firms. Unfortunately commercial products, used for ensuring data security, cannot always guarantee interoperability (see Glossary - page 32). Compliance with standards alone is not sufficient to guarantee interoperability between the products and services of the different suppliers / operators / publishers.

However, for reasons of confidentiality (see Glossary - page 32) or even fraud prevention, the data interchange between railways undertakings (RUs), infrastructure managers (IMs) and customers requires a certain level of data security.

In view of the prospects for the development of electronic commerce and the key role played by security-related functions, the UIC (see List of abbreviations - page 36) has been charged with developing a security strategy for its members, not only on a domestic level but also on an international level.

The first point of this leaflet focuses on the building of a Public Key Infrastructure (PKI) (see Glossary - page 32) primarily for data exchange on a domestic level between RUs, clients and IMs. After a short introduction of the concept, the leaflet describes the key points (see Glossary - page 32) to be taken into account when creating a PKI. By respecting these issues, not only a reliable domestic PKI could be created but also fair conditions for interoperable PKIs are met.

The second point of the leaflet is dedicated to interoperable PKIs. One of the major elements to allow this is to define the minimum interoperability security requirements (MISR) to guarantee secure, interoperable exchanges amongst RUs and/or IMs. These minimum-security requirements are the subject of this second point.

The Appendices A - page 26 and B - page 29 of the leaflet summarise a set of MISR to be respected and an example of a BCA as it could be provided by the UIC.

2 - A public key infrastructure

2.1 - The concept

Public Key Infrastructure is the name given to all the components, functions and procedures specifically used to manage the cryptographic keys (see Glossary - page 32) and certificates used by security systems based on public key cryptography. This infrastructure provides many functional and security services including a registration (see Glossary - page 32) service of holders, a certificate generation (see Glossary - page 32) service, a certificate distribution service, a time-stamping facility and a certificate revocation (see Glossary - page 32) service. It is assumed that, in the near future, more and more RUs and IMs will develop a kind of PKI to ensure a secure data exchange with their customers and other related organisations.

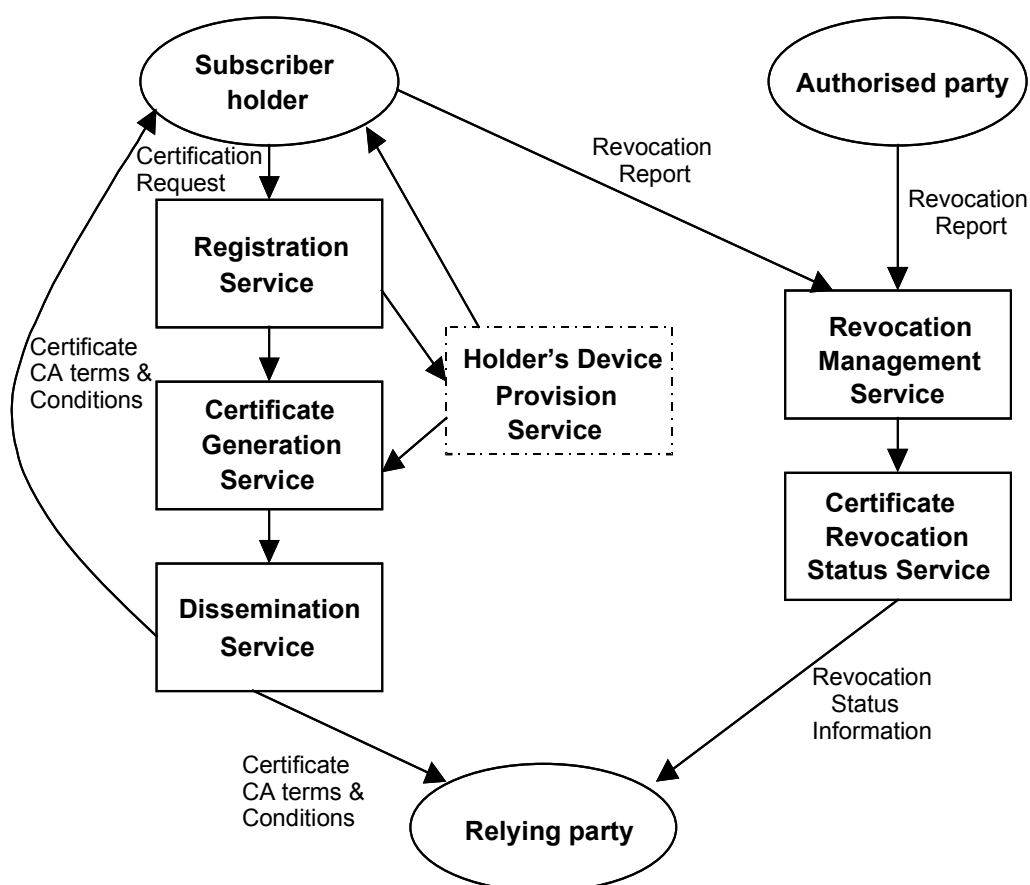


Fig. 1 - Illustration of subdivision of certification services

The subscriber or holder is the entity who receives a certificate from the certification authority. The name and the public key of this entity are contained in the certificate. Later in this document, the subscriber is called "the end-user".

The relying party is an entity that receives a certificate from an end-user in order to verify the identity or the electronic signature of this end-user.

The service of issuing certificates is usually broken down into the following component services for the purposes of classifying requirements:

Registration service:	verifies the identity and, if applicable, any specific attributes of a subject. The results of this service are passed to the certificate generation (see Glossary - page 32) service.
Certificate generation service:	creates and signs certificates based on the identity and other attributes verified by the registration service.
Dissemination service:	disseminates certificates to subjects and, if the subject consents, to relying parties. This service also disseminates the CAs terms and conditions, and any published policy and practice information to subscribers and relying parties.
Revocation management service:	processes requests and reports relating to revocation to determine the necessary action to be taken. The results of this service are distributed through the revocation status service.
Revocation status service:	provides certificate revocation status information to relying parties. This service may be a real-time service or may be based on revocation status information, which is updated at regular intervals.

2.2 - Key points when building a PKI

The following key points have to be considered by RUs and IMs when implementing a CA for their internal needs or for interchanging with other RUs and IMs or with customers.

The structure of this overview is laid-out in accordance with the structure of a certificate policy [\(see Glossary - page 32\)](#) proposed in *Request for Comment (RFC) 2527* [\(see Bibliography - page 38\)](#).

A CA issues certificates for end-users sometimes called certificate holders. In some cases, many CAs are necessary to issue different kinds of certificates corresponding to different levels of security. When these CAs are legally subordinated to the same organisation, it is common to build a CA hierarchy where a Root CA (RCA) certifies the different subordinate CA (Sub-CA). The RCA is the top of the CA hierarchy. Sub-CAs certificates are signed by the RCA. The RCA certificate is self-signed, that means that the RCA certificate is signed by the RCA private key [\(see Glossary - page 32\)](#) (whose public key is contained in the certificate).

When the hierarchy is limited to a single CA, this CA is by nature also a RCA.

In the following points of this leaflet, the generic term "CA" will be used to name the organisation that manages the public key certificates (either as a single CA or a Sub-CA in a CA hierarchy).

2.2.1 - Background

The RCA and optional Sub-CAs have to define and publish a Certificate Policy (CP) wherein the requirements are described, which are to be fulfilled in issuance and management of certificates.

The CA shall create a Policy Approval Authority (PAA) composed of executives of the railway organisation, CA organisation and optionally Sub-CAs to define the management rules. The PAA's tasks are to ensure:

- transparency,
- co-ordination, and
- assistance to the end-users.

2.2.2 - X.509 Certificate Fields

A CP shall define the rules to be used by that CA to facilitate interoperability with other CAs.

A CA shall be able to generate and sign certificates that enforce name uniqueness and contain an X.500 (see Bibliography - page 38) Distinguished Name (DN).

The CA shall have a DN as defined in X.509 (see Bibliography - page 38), and that shall be placed in the certificate subject name field. The Common Names (CN) asserted in the CA-issued certificates shall be the official names of the end-users meeting the requirements of a DN.

Upon issuance, each certificate issued by the CA shall be manually checked to ensure that each field and extension is properly populated with the correct information, before the certificate is delivered to the end-user.

The following extension fields in an X.509 certificate are used to support the CP interpretation:

- CP's extension,
- Policy Mapping's extension, and
- Policy Constraint's extension.

The Policy Mapping information is placed into the certificates issued by the CA, or otherwise published or used by the CA Operational Authority so as to facilitate interoperability.

2.2.3 - Identification

CA certificates shall contain a registered CP Object Identifier (OID) (see Glossary - page 32), which may be used by a Relying Party to decide whether or not a certificate is trusted for a particular purpose.

If the CA wishes to define several levels of assurance in its CP, then each level of assurance should have a specific OID. The appropriate OID will be specified in certificates issued by the CA. Each CA in relationship with other CAs has to make its CP available to Relying Parties.

2.2.4 - Community and applicability

The CA's PAA is responsible for:

- the CP design and maintenance,
- the Certificate Practice Statement (CPS) design and maintenance,
- accepting applications seeking to interoperate by using the CA, and
- determining the mappings between certificates issued by other CAs and, if necessary, the levels of assurance set forth in the CP.

The CA's PAA will enter into a Memorandum of Agreement (MOA) with all other CA organisations in trusted communication setting forth the respective responsibilities and obligations of both parties, and the mappings between the certificate levels of assurance contained in the CA's CP and those in the other organisations' CPs.

The CA Operational Authority (OA) (see Glossary - page 32) is the entity that operates the CA. It is in charge of:

- availability of CA certificates (see Glossary - page 32),
- distribution of those certificates and Certificate Revocation Lists (CRLs) (see Glossary - page 32) into the CA repository, and
- ensuring the availability of the repository to all end-users.

As operated by a CA OA, the CA shall be responsible for all aspects of certificate life-cycle management including the following processes:

- registration of end-user's certificates,
- identification and authentication,
- publication,
- manufacturing (token, option) and revocation.

The CA will require the services of other security, community and application authorities, such as compliance auditors.

The CA Subscribers will include CA OA staff, and possibly certain network or hardware devices such as firewalls and routers when needed for infrastructure protection.

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. In our framework, the Relying Party will use the certificate to establish secure communications with the holder of the certificate.

With regard to applicability, the sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. End-users and relying parties should evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation should be done by each

end-user and is not checked by the CA CP. As a end-user or a relying party has usually no capacity to evaluate the CA security and environment, the audit report of the accredited organisation should be made available to them by the CA. To provide sufficient granularity, the CA CP shall specify security requirements with increasing, qualitative levels of assurance, corresponding to the different levels of risk identified.

2.2.5 - Liability

As far as the domestic regulations allow, a CA shall disclaim any liability that might arise from use of any certificate it issues outside the scope of its intended purpose.

2.2.6 - Financial responsibility

The CA CP shall define to what extent its financial responsibility is committed with each player (end-user, relying party, etc.).

2.2.7 - Interpretation and enforcement

The CA's PAA shall resolve any disputes associated with the use of the CA or certificates issued by the CA.

2.2.8 - Publication and repository

The CA's OA shall publish information concerning the CA necessary to support its use and operation.

The CA OA shall protect any repository information not intended for public dissemination or modification. Public keys and certificate status information in the CA repository shall be publicly available.

A CA wishing to interoperate with another CA organisation shall make its directory ([see Glossary - page 32](#)) interoperate with this CA repository, and ensure that it contains the information necessary to support interoperation with the PKI domain ([see Glossary - page 32](#)) connected to that CA.

2.2.9 - Compliance audit

A CA should have a compliance audit mechanism put in place to ensure that the requirements of their CP/CPS and the provisions of the MOA are being implemented and enforced

2.2.10 - Confidentiality

CA information not requiring protection can be made publicly available. The CA's PAA access to end-user information shall be specified in the MOA in compliance with domestic regulations regarding privacy. This end-user shall determine which part of its information can be made public.

2.2.11 - Identification and authentication

2.2.11.1 - Initial registration

Uniqueness of names across the CA PKI domain must be enforced.

A CA shall enforce uniqueness of names within the X.500 name space, which they have been authorised.

2.2.11.2 - Method to prove possession of private key

In all cases where the party named in a certificate generates its own keys, that party shall be required to prove possession of the private key corresponding to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the CA. The CA shall then verify the signature using the party's public key.

2.2.12 - Certificate renewal, update and re-key

2.2.12.1 - Certificate renewal

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number. A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged.

2.2.12.2 - Key and certificate update

Updating a certificate means creating a new certificate that has the same or a different key and a different serial number and that differs in one or more other fields from the old certificate. For example, a CA may choose to update its certificate because its characteristics have changed. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

Further, when a CA updates its private signature key and thus generates a new public key, this CA shall notify all other CAs, Registration Authorities (RAs), end-users and relying parties which rely on the CA's certificate, that it has been changed. For self-signed certificates (RCAs), such certificates shall be conveyed to end-users in a secure fashion to preclude malicious substitution attacks.

2.2.12.3 - Certificate re-key

The longer and more often a key is used, the more likely it is to be subject to loss or discovery. Therefore, it is important that a end-user periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that has the same characteristics and level as the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key), a different serial number, and it may be assigned a different validity period.

Upon re-keying, the CA shall identify and authenticate the subscriber either by:

- performing the initial registration identification process, or
- using the currently valid certificate issued to the subscriber by the CA in a new certificate request.

2.2.13 - Operational requirements

2.2.13.1 - Delivery of public keys for certificate issuance

Public keys must be delivered for certificate issuance in a way that binds the applicant subscriber's identification to the public key. When the CA generates key pairs (see Glossary - page 32) centrally, it shall implement secure mechanisms to ensure that the token on which the key pair is held is securely sent to the proper Subscriber. The CA shall also implement procedures to ensure that the token is not activated by an unauthorised entity.

2.2.13.2 - Certificate issuance

The certificate request may contain an already built ("to-be-signed") certificate.

If databases are used to confirm Subscriber information, then these databases must be protected from unauthorised modification to a level commensurate with the level of assurance of the certificate being sought, if any.

Certificates, once created, shall be checked to ensure that all fields and extensions are properly populated. This may be done through software, which scans the fields and extensions looking for any evidence that a certificate was improperly manufactured.

2.2.13.3 - CA public-key delivery and use

The public key of the CA must be available for certification trust paths to be created and verified.

In order to extract the public key of the CA from that certificate with confidence that it has not been altered, the CA must ensure that its end-users have its self-signed root certificate ([see Glossary - page 32](#)) in a trustworthy fashion. Acceptable methods for RCA delivery include but are not limited to:

- the CA loading the root certificate onto tokens delivered to Relying Parties via secure mechanisms;
- secure distribution of the root certificate through secure out-of-band mechanisms;
- comparison of certificate hashes or fingerprints against the root-certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and
- loading certificates from Web-sites secured with a currently valid certificate of equal or greater assurance level than the certificate being downloaded.

2.2.13.4 - Certificate acceptance

Once the certificate has been issued by the CA, the subscriber shall notify its acceptance to the CA. From that point the certificate is considered "in use".

2.2.13.5 - Certificate revocation

Requests to revoke a certificate shall be authenticated. If the private key has not been compromised, the subscriber's private key can sign his request. When compromising of a corresponding private key is suspected, this method cannot be used. The subscriber needs to be authenticated by other means such as shared secret (grandmother's name, etc.). Authorised entities can request the OA to revoke the certificate of a subscriber.

When revocation of a certificate issued by a CA is required, it shall be done within a defined delay.

When required, the immediate generation and publication into the CA repository of status information shall be done. It declares the certificate as revoked, and the reason for the revocation. Further, and separate from the publication of the status information, prompt oral or electronic notification shall be given by the CA's OA to previously designated officials of all other CAs with which this CA interoperates.

The three main requirements regarding the repository are as follows:

- X.500 Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP);
- availability of the information;
- access control (see Glossary - page 32) mechanisms, when needed, to protect repository information.

The contents of CRLs (see List of abbreviations - page 36) shall be checked before issuance to ensure that all information is correct. This may be done using software that scans the CRLs looking for any evidence of an improperly manufactured CRL.

In addition to CRLs, CA client software may optionally support on-line status checking.

In the event of CA private key compromise or loss, the CA OA shall immediately publish a CRL.

2.2.13.6 - Security audit procedure

Audit log files shall be generated for all events relating to the key and certificate management.

All auditing capabilities of the CA operating system shall be enabled.

Each audit record shall include the following minimum data (either recorded automatically or manually for each audible event):

- type of event,
- date and time the event occurred,
- a success or failure indicator, when executing a certificate or CRL signing process,
- a success or failure indicator when performing certificate revocation,
- identity of the entity and/or operator of the CA that caused the event.

A message from any source requesting an action by the CA is an audible event. In this case, the message shall include message date and time, source, destination and contents.

All of the security audit data generated by the CA since the last review should be examined.

The audit process shall not be done by or under the control of an authority of a CA that does not belong to the OA staff.

Audit logs shall be stored in a safe, secure storage location separated from the CA equipment.

Audit logs and audit summaries shall be backed up regularly and a copy of the audit log shall be sent off-site.