UIC CODE 910

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

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.

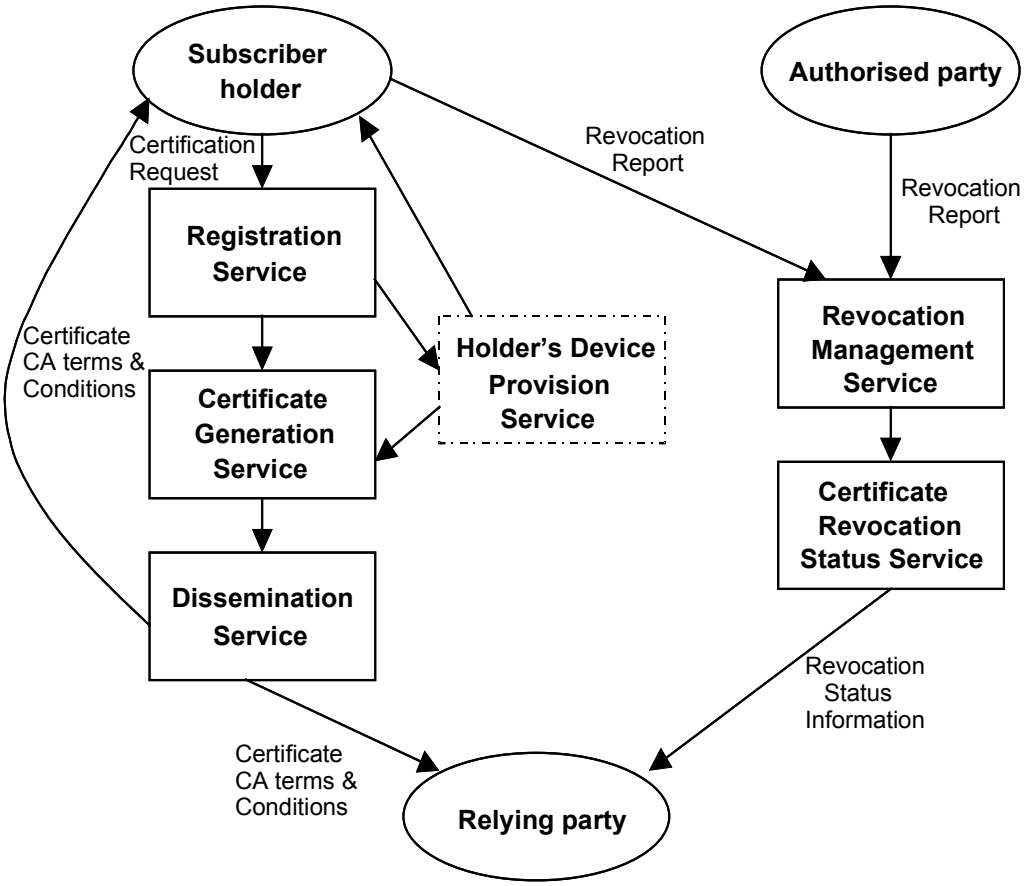

Fig. 1 - Illustration of subdivision of certification services

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.

2.2.13.7 - Records archival

CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA.

The minimum retention periods shall depend on domestic legislation. Note that if the original media cannot retain the data for the required period, a mechanism periodically to transfer the archived data to new media shall be defined by the archive site. Applications requiring processing the archive data should also be maintained for a period determined by the PAA for the CA.

Archive media shall be stored in a secure environment separated from the CA.

2.2.13.8 - Compromise and disaster recovery

If CA equipment is damaged or rendered inoperative, but the CA signature keys are not destroyed, CA operation shall be re-established as quickly as possible, giving priority to the ability to generate certificate-status information.

If the CA cannot issue a CRL prior to the time specified in the next update field of its currently valid CRL, then the PAA shall be immediately and securely notified. The PAA shall determine whether to revoke or not the root CA certificate issued to subscribers. The CA shall re-establish revocation capabilities as quickly as possible. The CA shall immediately and securely advise the PAA in the event of a disaster where the CA installation is physically damaged and all copies of the CA signature keys are destroyed.

If the CA signature keys are compromised or it is suspected that they might be compromised or lost:

- the PAA shall be immediately and securely notified (so that CAs may issue CRLs revoking any cross-certificates issued to CAs);

- any CA that has issued cross-certificates to the affected CA shall immediately publish a CRL revoking the compromised CAs certificate;

- a new CA key pair shall be generated by the CA and new CA certificates shall be issued to its subscribers and corresponding parties.

In the event of a disaster whereby the CA infrastructure is physically damaged and all copies of the CA signature key are destroyed as a result, the PAA shall be immediately and securely notified, and the PAA shall take whatever action it deems appropriate to inform its subscribers and relying parties. The PAA shall take the appropriate measures to re-establish operations, generating new key pairs and corresponding certificates and shall re-issue all cross-certificates. Relying Parties may decide whether to continue or not to use certificates signed with the destroyed private key pending re-establishment of CA operation with new certificates.

2.2.13.9 - CA termination

In the event of termination of a CA operation, certificates signed by that CA shall be revoked and the CA's PAA shall advise other Relying Parties that this CA operation has terminated so they may revoke cross-certificates they have been issued to that CA. CRL issued prior to the CA termination shall be kept available to the Relying parties.

2.2.14 - Physical, procedural and personnel security controls

Physical controls for the CA

All the physical control requirements apply to a CA.

The site location and construction, when combined with other physical security-protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorised access to the CA equipment and records.

The CA equipment shall always be protected from unauthorised access, and especially while cryptographic equipment are installed and activated. Physical access controls shall be implemented to reduce the risk of equipment tampering even when the cryptographic equipment are not installed and activated.

A CA shall have sufficient backup capability automatically to lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown.

CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contain audit, archive, or backup information shall be duplicated and stored in a separate location from the CA.

Backup systems to recover from system failure shall be checked on a periodic schedule.

2.2.15 - Technical security controls

2.2.15.1 - Key-pair generation

Cryptographic keying material for certificates issued by the CA shall be generated in evaluated cryptographic modules.

For the CA, the modules shall meet or exceed:

- the FIPS 140 Level 3 (see List of abbreviations - page 36) evaluation, or
- equivalent or higher common criteria (CC) evaluation.

2.2.15.2 - Algorithms and key sizes

All FIPS or CC-approved signature algorithms shall be considered acceptable.

2.2.15.3 - Key usage

CA signature certificate shall set two key usage bits: CRLSign and CertSign.

2.2.15.4 - Private-key protection

Use of the CA private signing key shall require action by multiple persons.

The CA private signature keys shall be backed up under the same multi-person control as the original ones.

CA private keys shall be generated by and remain in a cryptographic equipment.

The activation of any private key(s) by its holder (the subscriber) is required prior to a signature process. Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e. the data should not be displayed while it is entered). If the activation data must be transmitted, it shall be done via a trusted channel.

If cryptographic modules are used to store CA private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorised access. After use, the cryptographic module shall be deactivated.

End-users' private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can involve overwriting the data. For hardware cryptographic modules, this is likely to involve executing a "zero-ise" command. Physical destruction of hardware should not be required.

2.2.15.5 - Computer security controls

The CA shall include the following functionality:

- require authenticated logins;
- provide Discretionary Access Control;
- provide a security-audit capability;
- restrict access control to CA services and PKI roles;
- enforce separation of duties for PKI roles;
- require a trusted path for identification and authentication of PKI roles and associated identities;
- prohibit object re-use or require separation for CA random access memory;
- require use of cryptography (see Glossary - page 32) for session communication and database security;
- archive CA audit data;
- require self-test security related to CA services;
- require a recovery mechanism for keys and CA operation systems;
- enforce domain integrity boundaries for security-critical processes.

2.2.15.6 - Life-cycle technical controls

Hardware and software used to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with.

Hardware and software for the CA shall be developed in a controlled environment, and the development process shall be defined and documented.

All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the CA physical location.

As far as possible, the CA hardware and software shall be dedicated to performing specific processes.

Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment.

Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

The configuration of the CA system shall be documented and controlled, as well as any modifications and upgrades. There shall be a mechanism for detecting unauthorised modification to the CA software or configuration.

2.2.15.7 - Certificate and CRL profiles

A CA shall issue *X.509 v3* certificates and *X.509 v2* CRLs.

2.3 - Rail Certification Authority

Point 2.2 - page 4 addresses the key points when building a PKI for a generic organisation. In the context of this leaflet, an RU (see List of abbreviations - page 36) or an IM (see List of abbreviations - page 36) can use all these recommendations as set forth. An RU or an IM can act as a Rail Certification Authority (Rail CA) (see Glossary - page 32). A Rail CA can be a single CA or a CA hierarchy composed of an RCA (see Glossary - page 32) and many Sub CAs.

The Rail CA must define, within its general organisation, which entity takes the responsibilities and liabilities of issuing certificates for its end-users and for which target applications.

This can be an entity of the railway organisation, a dedicated subsidiary or any other kind of domestic organisation. In any cases, the PAA of this entity is liable for all the consequences following the requirements of point 2.2.

3 - Specifications for interoperability

When implementing a PKI, the designer has to decide about technical or organisational choices by following the guidelines or key points given in the previous point. Even if RUs and/or IMs decided to set in place domestic CAs, this would not guarantee interoperability between these CAs. In order to provide a basis for interoperability between PKI components possibly coming from different vendors, this leaflet specifies the Minimum Interoperability Security Requirements (MISR). This leaflet will be recommended for companies interested in offering interoperable PKI products and to RUs and/or IMs developing procurement specifications.

If ever UIC members decide to designate a hub for interoperation between the member CAs, then this leaflet could become a common specification for interoperability (see Appendix B - page 29).

3.1 - Scope

This specification supports interoperability for a large scale PKI that issues, revokes and manages digital signatures (see Glossary - page 32) and key management (see Glossary - page 32) public-key certificates. Digital signature certificates support the use of those signatures to replace hand-written signatures and to allow remote RUs or IMs, who have no previous relationship, reliably to authenticate each other and conduct business securely.

The MISR specifically addresses cross-certification between multiple CAs.

Therefore, this document is the basis for the design of a CP of CAs including the *X.509 version 3* certificate and CRL version 2 profiles.

3.2 - Levels of interoperability

Interoperability framework

Multi-vendor interoperability is a critical issue for PKI. In many cases, interoperability is used to describe the ability for one application seamlessly to communicate with another. Other aspects of interoperability include the ability to mix and match various PKI components from one vendor with those of another. Interoperability can also refer to the interaction between one enterprise domain and another. Therefore, interoperability can be classified as follows:

1. Component-Level Interoperability;

2. Application-Level Interoperability; and

3. Inter-Domain Interoperability.

3.2.1 - Component-level interoperability

As illustrated in Figure 2 - page 16, component-level interoperability addresses the interaction between systems directly supporting and/or consuming PKI-related services.

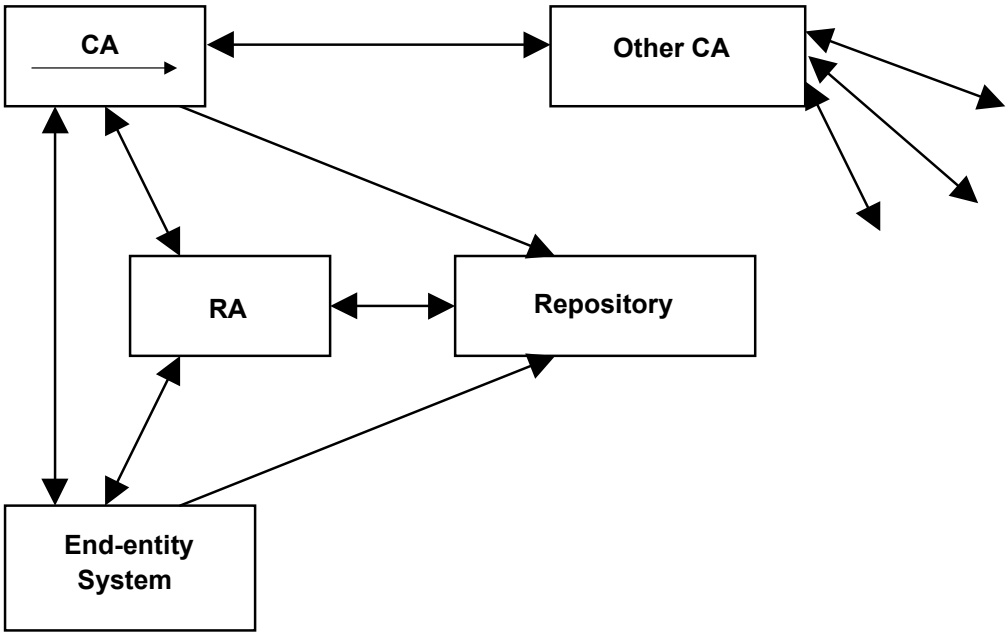

Fig. 2 - Component-level interoperability

Component-level interoperability includes the following considerations:

- Common protocols, message formats, and certificate formats must be implemented between applicable PKI components. This applies to:

  - CA-CA (and consequently to BCA-CA) (see List of abbreviations - page 36),
  - CA-RA (see List of abbreviations - page 36),
  - end-entity system-CA, and
  - end-entity system-RA.

- Common algorithms must be implemented for entity authentication and the protection of the data exchanged between PKI components;

- A method to facilitate the storage and retrieval of certificates and certificate-status information between the repository and the PKI components must be supported (this includes the protocol(s) and any underlying authentication scheme(s));

- Private keys must be accessible by authorised end-entities in a secure manner regardless of storage method:

  - software,
  - smart card, or
  - hardware token.

- One or more certificate-status mechanisms must be supported.

3.2.2 - Application-level interoperability

The usual concept of application-level interoperability is concerned with compatibility between two peers, regardless of the supplier of the application or any auxiliary infrastructure components used to support the application.

Figure 3 illustrates application-level interoperability:

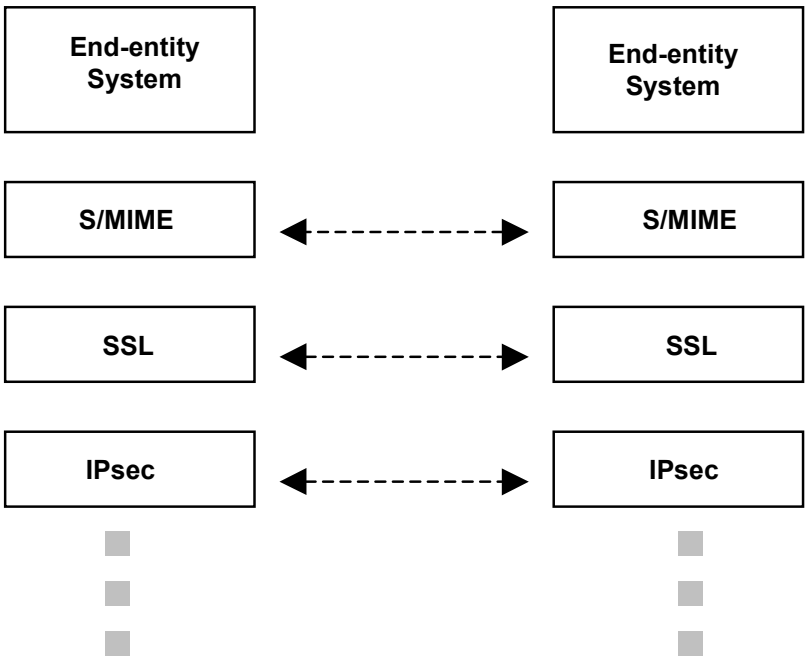

Fig. 3 - Application-level interoperability

In addition to the issues discussed in the previous point, application-level interoperability includes the following considerations:

- certificate and certificate-status information must be compatible (at least to the extent that any incompatibilities will not affect interoperability);
- business controls must be implemented to ensure certificates are being used consistently with intended key usage and any associated constraints;
- algorithms (including cryptographic algorithms (see Glossary - page 32) and key sizes) must be compatible;
- data encapsulation and encoding formats (e.g., file format, message formats, etc.) must be compatible;
- underlying communications protocols used to exchange information between peers must be compatible; and
- any in-band methods for sharing public-key related information (e.g., end-entity and CA certificates, certificate status, etc.) must be compatible.

Another aspect of application-level interoperability involves support for multiple applications from different vendors on the same end-system. This requires (often simultaneous) access to the same PKI credentials (see Glossary - page 32):

- private keys, and
- public-key certificates.

3.2.3 - Inter-domain interoperability

Inter-domain interoperability is perhaps the most complex of the three interoperability areas, since it involves, among other things, the co-operation of multiple administrative domains.

Figure 4 below helps to illustrate inter-domain interoperability. Note that the bi-directional arrow between repositories does not imply that the internal repository of one enterprise must be able to communicate directly with an internal repository of the other enterprise (although this might be a desirable option in some cases). Rather, it represents the requirement to exchange PKI-related information between the two PKI domains, which can be accomplished in a variety of ways.

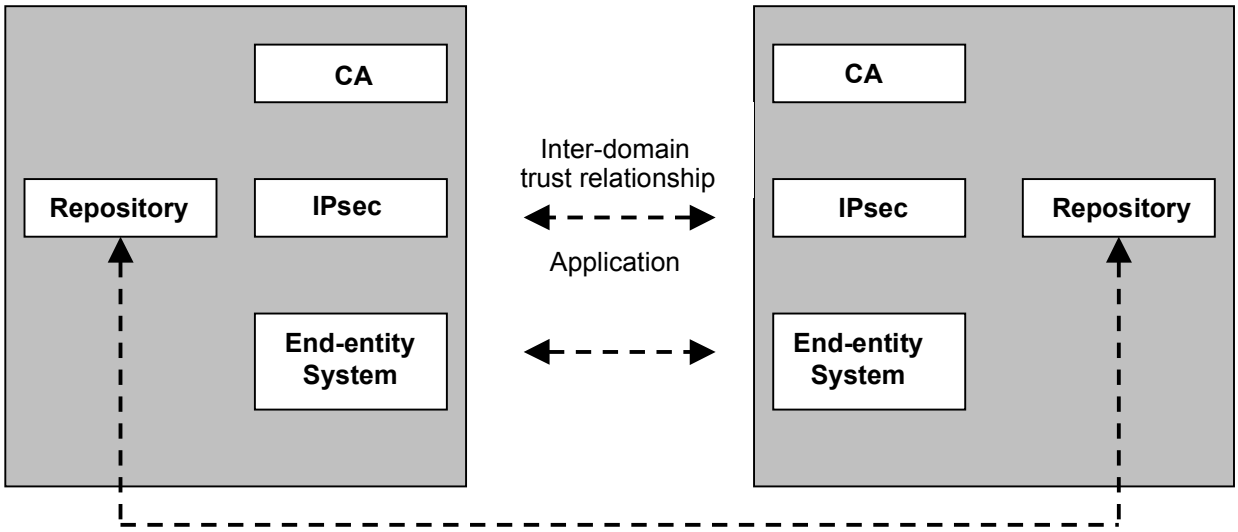

Fig. 4 - Inter-domain interoperability

Inter-domain interoperability involves a number of challenges, related to both technology and policy. All of the considerations outlined under point 3.2.2 - page 17 necessary to facilitate application-level interoperability apply here as well (i.e., it is assumed that the rationale for establishing the trust relationship is based on the need to support one or more applications between domains). In addition, the following issues must also be addressed:

- a method for establishing trust relationships between the PKI domains is required;
- appropriate PKI-related information in one domain must be made available to the other, and vice versa as applicable, based on the associated trust relationship; and
- each PKI domain must agree to adhere to certain policies (e.g., what a given certificate is to be used for), and each PKI domain needs to have mechanisms in place to enforce adherence to the agreed policies.

3.2.4 - Summary of interoperability issues

The following table summarises the technical aspects that apply to each of the interoperability areas as described previously.

Technical issues	Component-level interoperability	Application-level interoperability	Inter-domain interoperability
Common protocol, message formats and certificate formats must be implemented between applicable PKI components.	X	X	X
Common algorithms must be implemented for entity authentication and the protection of the exchanged data between PKI components.	X	X	X
Protocols and underlying authentication schemes must be supported to facilitate the storage and retrieval of certificates and certificate-status information between the repository and the PKI components.	X	X	X
Private keys must be accessible by authorised end-entities in a secure manner regardless of storage method (e.g. software, smart card or hardware token).	X	X	X
One or more certificate-status mechanisms must be supported.	X	X	X
Certificate and certificate-status information must be compatible (at least to the extent that any incompatibilities will not impact interoperability).		X	X
Business controls must be implemented to ensure certificates are being used consistently with intended key usage and any associated constraints.		X	X
Algorithms (including cryptographic algorithms and key sizes) must be compatible.		X	X
Data encapsulation and encoding formats (e.g. file format, message formats, etc.) must be compatible.		X	X
Underlying communications protocols used to exchange information between peers must be compatible.		X	X
Any in-band methods for sharing public-key related information (e.g. end-entity and CA certificates, certificate status, etc.) must be compatible.		X	X
A method for establishing trust relationship between the PKI domains is required.			X
Appropriate PKI-related information in one domain must be made available to the other.			X
Each domain must agree to adhere to certain policies, and mechanisms should be put in place to enforce adherence to the agreed-upon PKI.			X

As the interoperability between CA components is part of inter-domain interoperability, all technical issues selected in the table above should be considered as minimal requirements for PKI.

3.3 - Multiple CA interoperability

The purpose of this point is to discuss those issues associated with establishing interoperability between multiple CAs, and more generally inter-PKI domains, and to provide further recommendations. It should be noted that while standards serve a very important role in establishing compatible implementation, experience has demonstrated that standards alone are insufficient to guarantee multi-vendor interoperability. This fact is not limited to the PKI industry but the complexity within the cryptography domain increases this concern.

Within the context of the railway industry, this point addresses the interconnection between the CAs and the BCA assuming the UIC members wish to establish a BCA to facilitate interoperability between RCAs.

Of course, not all interoperability issues are directly related to the CA's interoperability. The interconnection of multiple PKI domains based on various technologies does bring almost every conceivable facet of interoperability to the forefront. While the title of this point is called "Multiple CA interoperability", emphasis is placed on what is best described as inter-domain interoperability (see point 3.2.3 - page 18).

In order to facilitate solving interoperability, the different issues are split into the following points:

- introduction to bridge CA;
- technical issues;
- policy or business relationships (organisational);
- legal considerations.

These concerns come under the jurisdiction of different managers in the organisation. Each of these managers must provide the pros and cons of the various alternatives when defining solutions for implementation.

3.3.1 - Bridge Certification Authority concept

Communication between PKI domains

In a given domain, the trust is based on the highest level, so-called the RCA (see List of abbreviations - page 36) (hereafter RCA1, RCA2, etc.). When organisations (like RUs or IMs) belonging to different trust domains need to communicate securely, they must first ensure that their respective CAs have established a trusted relationship. This trusted relationship is called a cross-certification (see Glossary - page 32). Basically, there are two ways to create this cross-certification, via a bilateral cross-certification (two by two) or via a central hub, or bridge CA (BCA).

Figure 5 illustrates these two scenarios for 6 companies:

for *n* CAs that cross-certify each other, the number of cross-certifications is *n(n*-1)/2.

for *n* CAs that can cross-certify with a BCA, the number of cross-certifications is only *n*.

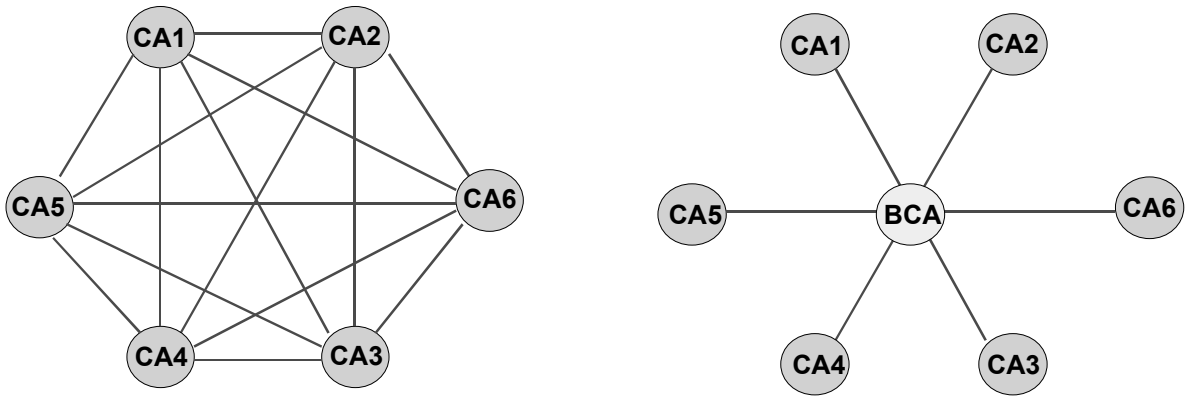

Fig. 5 - Comparison between cross-certification and BCA architecture

As can be seen, the more CAs that are involved, the more interesting the concept of BCA is. The BCA is based on the idea that a central point is used to create a community of interests between companies. To enter this community of interest, a company needs to be cross-certified with the Bridge CA.

3.3.2 - Technical issues

Essentially, this area is concerned with the protocols, data structure and other aspects (e.g., sharing certificates and certificate-revocation information) that are necessary to facilitate interoperability once all necessary business-level agreements are in place. This is probably the best standardised of the three areas.

Current PKI domain interconnection initiatives use cross-certification as the basis for inter-domain interoperability.

3.3.2.1 - Cross-certification

The fundamental purpose of cross-certification is to establish a trust relationship between two CAs and possibly between a BCA and a CA.

This is typically done to establish an interoperability path for one or more applications between two distinct PKI domains or between two CAs within the same PKI domain. The former is referred to as inter-domain cross-certification and the latter is referred to as intra-domain cross-certification. In the context of this leaflet we deal with inter-domain cross-certification.

Cross-certification may be mutual or unilateral. In the case of mutual cross-certification, a reciprocal relationship is established between the CAs - one CA issues a cross-certificate for the other, and vice versa. The cross-certificate issued by the local CA for a remote CA is referred to as a reverse cross-certificate (from the perspective of the local CA).

The cross-certificate issued by the remote CA for the local CA is referred to as the forward cross-certificate (from the perspective of the local CA). The reverse cross-certificate and the forward cross-certificate are stored in the directory as a cross-certificate pair in accordance with *X.509*. The inter-domain cross-certification between CAs should be mutual. Consequently, the requirements on the directory will really be essential (see point 3.3.2.6 - page 24).

Other key points have to be considered before cross-certifying multiple CAs. Here are the most important issues:

- encoding/decoding (see point 3.3.2.2);
- boundary and range (see point 3.3.2.3);
- naming conventions (see point 3.3.2.4 - page 23);
- certificates, CRL and certificate paths (see point 3.3.2.5 - page 23)

3.3.2.2 - Encoding/Decoding issues

Many issues related to the encoding and decoding of information can disrupt the interoperability. The following points must be considered carefully:

- inconsistent use of date formats (UTC Time versus Generalised Time) (see List of abbreviations - page 36) between CAs which can make decoding and subsequent signature verification (see Glossary - page 32) behave incorrectly;
- differences in use of Basic Encoding Rules (see Glossary - page 32) and Distinguished Encoding Rules (BER/DER) (see List of abbreviations - page 36) encoding for extensions;
- use of non-standard OIDs to denote algorithms which prevents another CAs from generating cross-certificates;
- differing assumptions about what should be supplied in the cross-certification request (e.g., one CA assumes that cross-certifying CA will determine certain values whereas the second CA assumes they will be provided in the request);
- cross-certification requests may be encoded as binary ASN.1 (see List of abbreviations - page 36) or Base64 encoded; and
- encoding of empty values (e.g., if no attributes are present in a request, some products assume that the request will contain encoding of empty set while others assume no encoding at all).

3.3.2.3 - Boundary and range issues

A number of boundary and range problems should be specified, including:

- assumptions about the maximum value of a certificate serial number (e.g., some cross-certifying CAs produce cross-certificates with a serial number greater than the cross-certified CA can handle);
- assumptions about the maximum length of names (e.g., the cross-certification request contains a distinguished name (see Glossary - page 32) longer than cross-certifying CA can handle); and
- arbitrary limits on the maximum permissible path length, which make cross-certification fail.

3.3.2.4 - Naming conventions

A number of naming-convention issues should be taken into account, including:

- use of non-standard or legacy values in distinguished names (e.g., RFC 822 (see List of abbreviations - page 36) address within Issuer Distinguished Name (DN)) has to be avoided;

- assumptions about the ordering of DN attributes (e.g., assume common name (CN) is always encoded last in sequence), or arbitrary limitations upon the number of attributes (e.g., only one organisational unit (OU) (see List of abbreviations - page 36) attribute for example); and

- where human action is required during the cross-certification process (e.g., a request and cross-certificate are transferred via floppy), file-naming conventions need to be agreed.

3.3.2.5 - Certificates, CRLs and certificate paths

A number of issues related to certificates, CRLs, and certificate paths should be addressed, including:

- some vendors implemented arbitrary path-length restrictions that would be insufficient for some environments;

- inconsistent application of key Usage and basic Constraints extensions;

- inconsistent application of issuer DN, serial number, authority Key Identifier and subject Key Identifier;

- inconsistent use of next Update field in CRLs;

- inconsistencies in creating and responding to cross-certification requests; and

- in some cases, applications do not yet possess the ability to process complex certificate paths as they have been designed with simple hierarchical trust models in mind.

When the application using the certificates allows certificate extension interpretation, the following extensions should be populated:

- Certificate Policies;

- Policy Mappings;

- Name Constraints.

These extensions are particularly valuable in preventing unwanted trust paths from being propagated through the BCA (see Glossary - page 32).

The construction of a trust between multiple domains is complex and the resolution of a trusted path can sometimes lead to an impasse. A typical case is an unsolvable path: A trusts B, B trusts C, C trust A. In this case, it is not possible to find a highest trusted point.

Each CA can enter into a cross-certification arrangement with another CA under one or more CP. Where the CPs overlap, it is considered that the CAs have established a "trusted path" to each other.

3.3.2.6 - Directory issues

The problem of multi-vendor directory interoperability must also be solved. A number of directory-related issues should be considered, including:

- in some implementations, a CA entry can only be added to the *X.500* LDAP directory when the directory is first configured in the company. Therefore, a new entry for a cross-certified CA cannot be added. Some implementations only check if the CA is bound to the directory at log-on, so errors will not be reported;

- some CAs use the same OID for different object classes.

3.3.2.6.1 - X.500 Directories

The most commonly-implemented open standards used for directory-to-directory interoperation are the *ISO/ITU X.500* standards (see Bibliography - page 38).

Several technology demonstrations have shown that *X.500* directory chaining can support multi-vendor PKIs, using a diverse array of directory systems.

Unfortunately, some of the most commonly-used commercial directory systems use proprietary protocols for inter-directory communications, so the simple approach of linking all directories via *X.500* Directory System Protocol (DSP) is not possible.

3.3.2.6.2 - LDAP referrals

The IETF (see List of abbreviations - page 36) LDAP provides for multi-directory interoperation by use of "referrals". Referrals are a way for directories to "refer" clients from the directory the client has queried to another directory that is more likely to have the information the client has requested. LDAP referrals require applications to be able to process them, and at present very few PKI-enabled clients process LDAP referrals.

3.3.2.6.3 - Border directories

The technical and policy barriers to interoperability can both be addressed to some extent by use of a concept called "border directories."

The border directory concept involves placing an *X.500*-compliant directory outside the enterprise firewall. A subset of directory information (for example, perhaps only the CA certificates and CRLs) is exported from the internal directory system to the border, and is thereafter available through the network of chained *X.500* border directories.

3.3.3 - Policy and business issues

This point encompasses non-technical details necessary to establish the relationship between two PKI domains. Ultimately, the rationale for establishing an inter-domain relationship will be based on the need to exchange information electronically. Stated another way - businesses typically establish a requirement to exchange information based on one or more applications.

This "electronic relationship" could be based on existing business requirements, or new requirements/ relationships can be forged over time. In any case, this is the application that typically drives items such as how certificates issued in a foreign domain can be used in the local domain. Naturally, these business-level agreements must be enforced technically, procedurally and legally.

3.3.3.1 - Certificate policy (CP)

The CP is a formal document that describes the requirements the CA has to comply with when operating the certificate life cycle. In particular the CP describes the interoperability requirements to allow communication with other trusted domains.

Each CP is associated with a unique identifier referred to as an OID. Certificates, cross-certificates or any other means for conveying CP information will be populated with the appropriate OIDs so that end-entity certificates are used consistently with the applicable CP(s).

The policy mapping features of the *X.509* standard allow a CA to assert in a cross-certificate that the CPs of a cross-certified PKI are equivalent to those of the local CA domain.

If a BCA is set in place, the BCA CP will indicate the applicability of its cross-certificates to the railway community including the common security requirements and, more particularly, the certificate and CRL profiles acceptable for the BCA.

3.3.3.2 - Certification Practice Statements (CPS)

The purpose of a CPS is to document the operational aspects of a CA. The CPS describes how the requirements stated in the CP have been implemented. Specifically, the CPS would not be disclosed to the public, nor would it be disclosed in the context of an inter-domain interoperability arrangement with a partner or affiliate, i.e. in the context of a cross-certification between multiple CAs.

3.3.4 - Legal issues

One of the most fundamental interoperability issues rests on the acceptance of digital signatures in a multi-jurisdictional environment.

The Electronic Signature (see Glossary - page 32) legislation (European Directive) adopted in Europe in December 1999 (see Bibliography - page 38) is one attempt to help in this regard. Similar legislation has also been adopted within the United States. This legislation aims to recognise the electronic signatures at the same level as handwritten signatures.

Issues associated with responsibilities and liability need to be addressed. Some of the methods for facilitating inter-domain interoperability attempt to limit the liability of the CA by placing additional burden on the relying party.

Obligations related to the requirements of an end-user notice need to be considered. This notice must be considered as a contract with the end-user and the CA must obtain some guarantees that the end-user has been informed and has taken this notice in consideration (by some kind of scrolling screen with an acceptance button at the bottom).

Appendix A - Summary of the MISR

This Appendix lists the Minimum Interoperability Security Requirements to establish a trusted relationship between multiple CA, either by two-by-two-cross-certification or using a bridge CA.

MISR 1 The profile of certificates (see Glossary - page 32) must be *X.509 version 3* and the profile of CRLs is version 2.

MISR 2 Common protocols, message formats, and certificate formats must be implemented between applicable PKI components. This applies to:
- CA-CA (and consequently to BCA-CA),
- CA-RA,
- end-entity system-CA, and
- end-entity system-RA.

MISR 3 Common algorithms must be implemented for entity authentication and the protection of the data exchanged between PKI components.

MISR 4 A method to facilitate the storage and retrieval of certificates and certificate-status information between the repository and the PKI components must be supported (this includes the protocol(s) and any underlying authentication scheme(s)).

MISR 5 Private keys must be accessible by authorised end-entities in a secure manner regardless of storage method:
- software,
- smart card, or
- hardware token.

MISR 6 One or more certificate-status mechanisms must be supported.

MISR 7 Certificate and certificate-status information must be compatible (at least to the extent that any incompatibilities will not affect interoperability).

MISR 8 Business controls must be implemented to ensure certificates are being used consistent with intended key usage and any associated constraints.

MISR 9 Algorithms (including cryptographic algorithms and key sizes) must be compatible.

MISR 10 Data encapsulation and encoding formats (e.g., file format, message formats, etc.) must be compatible.

MISR 11 Underlying communications protocols used to exchange information between peers must be compatible.

MISR 12 Any in-band methods for sharing public-key related information (e.g., end-entity and CA certificates, certificate status, etc.) must be compatible.

MISR 13 Access (often simultaneously) to the same PKI credentials (private keys and certificates).

MISR 14 A method for establishing trust relationships between the PKI domains is required.

MISR 15 Appropriate PKI-related information in one domain must be made available to the other, and vice versa (as applicable based on the associated trust relationship).

MISR 16 Each PKI domain must agree to adhere to certain policies (e.g., what a given certificate is to be used for), and each PKI domain needs to have mechanisms in place to enforce adherence to the agreed-upon policies.

MISR 17 The inter-domain cross-certification between the BCA and CAs should be mutual.

MISR 18 The date format must be consistent (UTC Time or GeneralisedTime) between CAs in order to make decoding and subsequent signature verification possible.

MISR 19 There must not be any differences in use of BER/DER (see List of abbreviations - page 36) encoding for extensions.

MISR 20 Only standard OIDs must be used to denote algorithms.

MISR 21 Equivalent assumptions about what should be supplied in the cross-certification requests.

MISR 22 Cross-certification requests may be encoded as binary ASN.1 or Base64 encoded.

MISR 23 The encoding of empty values (e.g., if no attributes are present in a request, some products assume that the request will contain encoding of empty set while others assume no encoding at all) should be a common assumption for the cross-certification requests.

MISR 24 The BCA should state a maximum value of a certificate serial number.

MISR 25 The BCA should state a maximum length of names.

MISR 26 The BCA should not allow arbitrary limits on maximum permissible path length, as this will lead to cross-certification failure.

MISR 27 Use of non-standard or legacy values in distinguished names (e.g., RFC 822 address within Issuer Distinguished Name (DN)) must be avoided.

MISR 28 There should be assumptions about the ordering of DN attributes (e.g., assume common name (CN) is always encoded last in sequence), or arbitrary limitations upon the number of attributes (e.g., only one organisational unit (OU) attribute for example).

MISR 29 Where human intervention is required in cross-certification process (e.g., a request and cross-certificate are transferred via floppy), file naming conventions need to be agreed.

MISR 30 There should be a common assumption about path-length restrictions.

MISR 31 The use of keyUsage and basicConstraints extensions should be consistent.

MISR 32 The use of issuer DN, serial number, authorityKeyIdentifier and subjectKeyIdentifier should also be consistent.

MISR 33 Moreover, the use of nextUpdate field in CRLs should be coherent.

MISR 34 There should not be any inconsistencies in creating and responding to cross-certification requests.

MISR 35 Except the certificate extensions mentioned above, there are other important extensions such as certificatePolicies, policyMappings, nameConstraints, policyConstraints or path length constraints (found in basicConstraints extension).

MISR 36 The use of the same OID for different object classes should be avoided.

MISR 37 The implementation must check to see if CA is bound to the directory at log on and regularly.

MISR 38 A cross-certified CA entry may be added to the X.500 LDAP directory when the directory is first configured or before.

MISR 39 Only *ISO/ITU X.500* standards must be used for directories.

MISR 40 The link of all directories via *X.500* Directory System Protocol (DSP) should be possible so the use of proprietary protocols for inter-directory communications is not allowed.

MISR 41 The access protocol to the directories must be LDAP.

MISR 42 There should be a border directory.

MISR 43 Each CP must be associated with a unique identifier referred to as an OID. Certificates, cross-certificates or any other vehicle for conveying CP information must be populated with the appropriate OIDs so that end-entity certificates are used consistent with the applicable CP(s).

MISR 44 The BCA CP must indicate the applicability of its cross-certificate to the railway community including the common security requirements and, more particularly, the certificate and CRLs profiles acceptable for BCA.

MISR 45 The legislation on signature and cryptography all around the world should be considered.

Appendix B - The UIC as BCA

If a business case for interconnection of Railways were adopted, a Bridge CA scenario would be best suited due to the significant numbers of RUs and IMs. In this case, the UIC could serve as the BCA due to its role as a neutral association of RUs and IMs.

B.1 - Recognition of the UIC as BCA

If the UIC has to act as a BCA, its members should officially nominate UIC for this role.

The role of the UIC to act as a BCA would mandate the establishment of a specific structure that will serve as the Policy Approval Authority (PAA).

B.2 - Role of the PAA

The PAA is an approval board whose charge is to establish, monitor and maintain policies related to the integrity of the policy infrastructure of the UIC BCA. The authority to constitute a PAA comes from the UIC steering committee. The PAA is made up of Core Members and Operational Members.

B.3 - Structure of the PAA

The core members of the UIC PAA are:

UIC staff

- PAA chairman;
- a UIC steering committee person able to make decisions and transmit PAA decisions to all UIC executives;
- a permanent UIC person able to do the current tasks during the lifecycle of the cross-certification between the BCA and the member railway CAs (i.e. someone who ensures a permanence to answer the daily problems of management and organisation related to the BCA).

Equity UIC BCA members

- at least one executive of each UIC member who is connected to the UIC BCA.

The operational members of the UIC PAA make up a working-group set of:

Permanent members

- the administrators of each Certification Authority (CA) (see Glossary - page 32) already connected to the UIC BCA;
- UIC legal employee.

Provisional members (advisers)

- technical experts;
- legal experts;
- such other persons as the PAA core members may deem appropriate.

B.4 - The role of the UIC as BCA

The PAA is in charge of:

- operating the PKI infrastructure of the BCA;
- maintaining, auditing, modifying, clarifying and replacing the existing policies and procedures;
- approving the new policies and procedures, their conformance with the document including the Minimum Interoperability Security Requirements;
- providing advice for drafting policies and procedures in order to maintain interoperability;
- publishing policies and procedures in accordance with their level of confidentiality and informing the potential candidate to join UIC BCA of the T&C (terms and condition) (see List of abbreviations - page 36);
- verifying the accurate operation of the UIC PKI in accordance with the procedures; this includes the creation and maintenance of the Quality Assurance Plan and the (technical and organisational) audit plan.
- releasing audits and the interface with the auditors;
- considering the importance of alarms generated by exceptional events such as the root-key compromise or suspicion of compromise, and starting the emergency procedures, if necessary;
- deciding what to do in case of activity termination or transfer;
- managing the application of a UIC member candidate to join the UIC BCA;
- appointing appropriate organisations to assess the level of consistency of the candidate member's PKI against the UIC requirements (audits);
- analysing results of the assessment report elaborated by the PAA working group;
- considering the risks and impacts of welcoming the PKI candidate into the existing UIC BCA network;
- voting for the admission of the new candidate into the UIC BCA network;
- following-up the legal aspects (T&C) of the new UIC BCA member.

In addition, the PAA can also:

- register the set of all the member railways' CP OIDs;
- develop the minimum interoperability criteria included in the MISR document;
- ensure the coherence between all naming plans;
- oversee any modifications (addition or deletion) of CAs.

At a minimum, the PAA has authority over the following documents:

- Certification Policy (CP) model which has been given by UIC (document CP type);
- Certificate Practice Statements (CPS) and the set of organisational and operational procedures;
- Technical and organisational audit plan;
- Quality Assurance Plan;
- Various contractual elements such as terms and conditions (T&C).

Moreover, the PAA has a role of adviser:

- Providing references and documentation;
- Mediating in technical and/or organisational choices.

Glossary

Access control	The prevention of unauthorised use of a resource, including the prevention of use of a resource in an unauthorised manner. [ISO 7498-2: 1989]
Asymmetric Key Pair	A pair of related keys where the private key defines the private transformation and the public key defines the public transformation. [ISO/IEC 9798-1: 1977, 2nd edition]
Authentication	Measures designed to provide against fraudulent transmission and imitative communications deception by establishing the validity of transmission, message, station or individual.
Basic Encoding Rules	BER was created in the early 1980s and is used in a wide range of applications, such as Simple Network Management Protocol (SNMP) for management of the Internet.
Certificate	A data structure containing the public key of an entity, together with associated information, and rendered unforgeable through being digitally signed by the certification authority, which issued it. [ISO/IEC 9594-8]
Certificate Generation	Certificate generation is the process of creating a certificate from inputs specific to the application and the end-user.
Certificate Policy	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range. [ISO/IEC 9594-8]
Certificate Revocation List	A signed list of the certificates, which have been revoked by a certification authority.
Certification Authority	An entity trusted by one or more entities to create, assign and revoke or hold public-key certificates. [ISO/IEC 9594-8: 1990]
Confidentiality	The property that information is not made available or disclosed to unauthorised individuals, entities, or processes. [ISO 7498-2: 1989]
Credentials	Data that is transferred to establish the claimed identity of an entity. [ISO 7498-2: 1989]
Cross-Certification	Certificates generated for Certification Authorities other than an immediate parent.

Cryptographic Algorithm	A set of rules specifying the procedures required performing encipherment and decipherment of data. The algorithm is designed so that it is not possible to determine the control parameters (e.g. Keys) except by exhaustive search. [ISO 11568-1]
Cryptographic Key	A parameter used in conjunction with an algorithm for the purpose of validation, authentication, encipherment or decipherment. [ISO 8732: 1988]
Cryptography	The discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use. [ISO 7498-2: 1989]
Digital Signature	Data appended to, or a cryptographic of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO 7498-2: 1989]
Directory	A collection of open systems cooperating to provide directory services. [ITU-T Recommandation X.500]
Distinguished Name	A unique, unambiguous name a particular Certification Authority assigns to a digital certificate subscriber for use within that Certification Authority's environment
Distinguished Encoding Rules	DER is a specialised form of BER that is used in security-conscious applications. These applications, such as electronic commerce, typically involve cryptography, and require that there be one and only one way to encode and decode a message.
Domain	A group of entities subject to the same security policy and under the jurisdiction of a domain authority that is responsible for enforcing the policy.
Electronic signature	Data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication. [European Directive 98/0191]
FIPS 140-1	FIPS 140-1 is a U.S. Government standard for implementations of cryptographic modules, that is, hardware or software that encrypts and decrypts data or performs other cryptographic operations (such as creating or verifying digital signatures). The FIPS 140-1 standard was created by the National Institute of Standards and Technology (NIST); it specifies requirements for the proper design and implementation of products that do cryptography.
Integrity	Integrity refers to the correctness of information, of originator of the information, and the functioning of the system that processes it.
Interoperability	Interoperability implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.

Key	A sequence of symbols that controls the operation of a cryptographic transformation (e.g. encipherment, decipherment, cryptographic check function computation, signature generation, or signature verification). [ISO/IEC 9798-1: 1997, 2nd edition] [ISO/IEC 11770-1: 1997]
Key Management	The administration and use of the generation, registration, certification, deregistration, distribution, installation, storage, archiving, revocation, derivation and destruction of keying material in accordance with a security policy. [ISO/IEC 11770-1: 1997]
Key Pair	The keys in an asymmetric cryptosystem having the property that one of the pair will decrypt what the other encrypts.
Non-Repudiation	The generation, verification and recording of evidence, and the subsequent retrieval and re-verification of this evidence in order to resolve disputes. [ITU-T Rec. X.813 (1996)] [ISO/IEC 10181-4]
Object Identifier (OID)	An unambiguous string or "label" that references an entity. OIDs are registered by ISO organisation. As an example the OID string of RSA algorithm is: (1.2.840.113549.1.1) {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1)}
Operational Authority	Entity that operates the CA.
Private Key	That key of an entity's asymmetric key pair which shall normally only be known by that entity. [ISO/IEC 11770-3, (2nd DIS 08/1997)]
Public Key	That key of an entity's asymmetric key pair that can be made public. [ISO/IEC 9798-1: 1977, (2nd edition)] [ISO/IEC 11770-1: 1997] [ISO/IEC 11770-3 (2nd DIS 08/1997)]
Public Key Certificate	A security certificate that binds unforgeably the public key of an entity to the entity's distinguishing identifier, and which indicates the validity of the corresponding private key. [ISO/IEC 13888-1: 1997]
Public Key Infrastructure (PKI)	The infrastructure needed to generate, distribute, manage and archive keys, certificates and certificate-revocation lists and the repository to which certificates and CRLs are to be posted. [ISO/IEC 11770-3 (2nd DIS 08/1997)]

Rail Certification Authority (Rail CA) The railway organisation in charge of the PKI that issues certificates to its end-users.
A Rail CA can be a single CA or a CA hierarchy composed of a Root CA and many Sub CAs.

Root Certificate The Root certificate is self-signed, which means that the Root certificate is signed by the RCA private key (whose public key is contained in the certificate).

Root Certification Authority (RCA) The CA at the top of a CA hierarchy (ANSI X9.79-1)
The "Level 0" national apex element of a PKI hierarchy. It is the central government or Organisational facility that provides centralised key management services for all forms of key. In the hierarchical model, the Root CA maintains the established "community of trust" by ensuring that each entity in the hierarchy conforms to a minimum set of practices.

Registration Registration is the assignment of identities (IDs) to PKI elements and the association of administrative data and configuration attributes with each element. Either management nodes or local registration authorities can perform registration of end entities.

Registration Authority (RA) An entity who is responsible for identification and authentication of 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.
[ISO CD 15782-1]

Revocation To suspend temporarily a certificate or make a certificate ineffective from a specified time and forward. Revocation is effective by notation or inclusion in a set of revoked certificates often termed a certificate revocation list (CRL), and does not imply that a revoked certificate is destroyed or made illegible.

Signature Verification Process of verifying an electronic signature operation using the signer public key and the appropriate cryptographic algorithm.

Verification Process A process which takes as input the signed message, the verification key and the domain parameters, and which gives as output the result of the signature verification: valid or invalid.
[FCD ISO/IEC 14888-1 (12/1997)]

List of abbreviations

ANSI	American National Standard Institute
ASN	Abstract Syntax Notation
BCA	Bridge Certification Authority
BER/DER	Basic Encoding Rules/Distinguished Encoding Rules
CA	Certification Authority
CC	Common Criteria
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statements
CRL	Certificate Revocation List
DIS	Draft International Standard
DN	Distinguished Name
DSP	Directory System Protocol
FIPS	Federal Information Processing Standard
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IPsec	Internet Protocol - security protocol charter
IM	Infrastructure Manager
ISO	International Organization for Standardization
ITU	International Telecommunication Union
LDAP	Lightweight Directory Access Protocol
MIME	Multipurpose Internet Mail Extensions
MISR	Minimum Interoperability Security Requirements
MOA	Memorandum Of Agreement
OA	Operational Authority

OID	Object Identifier
OU	Organisation Unit
PAA	Policy Approval Authority
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certification Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (asymmetric cryptographic algorithm that bears the name of its inventors)
RU	Railway Undertaking
S/MIME	Secure Socket Layer
SSL	Secure Socket Layer
T&C	Terms and Conditions
UIC	International Union of Railways (Union Internationale des Chemins de fer)
UTC	coordinated universal time (Unité de temps coordonnée)

Bibliography

1. Minutes of meetings

International Union of Railways (UIC)
Preliminary Study Report On The Establishment Of Public Key Infrastructure or the UIC, Electronic Commerce Working Party, Version 1.3, March 2000

2. International standards

S. Chokhani and W. Ford
RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999

International Organization for Standardization (ISO)
ISO 11568-1:1994 : Banking - Key management (retail) - Part 1: Introduction to key management, 1994

ISO 8732:1988 : Banking - Key management (wholesale), 1988

International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC)
ISO/IEC 7498-2:1994 : Second Edition - Information technology - Open Systems Interconnection - Basic Reference Model: Part 2, Security architecture, 1994-11-15 (actual version ISO 7498-2: 1989)

ISO/IEC 9798-1:1997 : Information technology - Security techniques - Entity authentication - Part 1: General (available in English only), 1997

ISO/IEC 9594-8:1998 : Information technology - Open Systems Interconnection - The Directory: Authentication framework, 1998

ISO/IEC 9594-8:2001 : Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks, 2001

ISO/IEC 11770-1:1996 : Information technology - Security Techniques - Key management - Part 1: Framework (available in English only), 1996

ISO/IEC 10181-4:1997 : Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework, 1997

ISO/IEC 11770-3:1999 : Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques, 1999

ISO/IEC 13888-1:1997 : Information technology - Security techniques - Non-repudiation - Part 1: General, 1997

International Telecommunication Union (ITU-T)
Recommendation X.500 (02/01) - Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services, 2001

Recommendation X.509v3 (ISO/IEC 9594-8) - Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 97 (actual version: 03/2000)

Recommendation X.813 (10/96) - Information technology - Open Systems Interconnection - Security frameworks for open systems: Non-repudiation framework, 1996

3. European standards

European Parliament and Council
Directive 1999/93/EC on a Community framework for electronic signatures, 13 December 1999 - Official Journal L 013, 19/01/2000 P. 0012-0020

4. Miscellaneous

National Institute for Standards and Technology
Public Key Infrastructure (PKI) Technical Specifications: Part A - Technical Concept of Operations, September 1998

D. Crocker
RFC0822 - Standard for the format of ARPA Internet text messages, August 1982

Warning

Printed by the International Union of Railways (UIC)
16, rue Jean Rey 75015 Paris - France, May 2004
Dépôt Légal May 2004

ISBN 2-7461-0XXX-X (French version)
ISBN 2-7461-0XXX-X (German version)
ISBN 2-7461-0768-6 (English version)