

# **PKI tutorial**

**Description of Public Key Infrastructure**

**White paper**

---

September 2006

Copyright © Insta DefSec Oy, 2006. All rights reserved.

This document is provided only for informational purposes. It may be used according to the following conditions:

- The document may not be distributed for profit.
- Copies of this document must contain all text without modification and all pages must be included.
- All copies must include the copyright notice.
- This document is for personal use only.

Information in this document is subject to change without notice and does not represent a commitment on the part of Insta DefSec Oy.

## Table of Contents

<b>1</b>	<b>INTRODUCTION .....</b>	<b>5</b>
1.1	Purpose .....	5
<b>2</b>	<b>Description of Public Key Infrastructure (PKI).....</b>	<b>6</b>
2.1	Asymmetric encryption .....	6
2.2	PKI.....	6
2.3	The Components of PKI .....	6
2.3.1	Security Policy .....	7
2.3.2	Certificate policy .....	7
2.3.3	Certificate Practice Statement (CPS) .....	7
2.3.4	Certification Authority (CA).....	7
2.3.5	Registration Authority (RA).....	8
2.3.6	Certificate Distribution System .....	8
2.3.7	PKI-enabled applications.....	8
2.4	Advantages of PKI.....	8
2.5	Certificate types.....	9
2.5.1	Smart card (SC) certificate: .....	9
2.5.2	File certificate: .....	9
2.5.3	USB-token certificate.....	9
2.6	Cross-certification.....	10
2.7	Certificate creation process .....	10
2.8	Used standards and recommendations.....	12
2.8.1	X.500 .....	14
2.8.2	X.509 .....	14
2.8.3	RFC 1777, LDAP (Lightweight Directory Access Protocol).....	14
2.8.4	ISO/IEC 7816 .....	15
2.8.5	RFC 2527 (Internet X.509 PKI Certificate Policy and Certification Practices Framework) .....	15
2.8.6	PKCS #12.....	15
2.8.7	PKCS #15.....	15
2.8.8	S/MIME.....	15
2.8.9	PC/SC .....	15
2.9	PKI references.....	16
<b>3</b>	<b>Insta's PKI-based products and services.....</b>	<b>17</b>
3.1	Insta Certifier .....	17
3.2	Insta Managed PKI .....	18
<b>4</b>	<b>Insta Security Systems .....</b>	<b>19</b>

## DEFINITIONS, ACRONYMS AND ABBREVIATIONS

Definition	Explanation
<b>Activation data</b>	Confidential data needed in addition to the RSA key to use cryptographic modules (for example a PIN code or a password).
<b>CA</b>	Certification Authority
<b>Certificate Service Provider</b>	A provider producing the data-technological certificate services for the Certification Authority until the certificates and revocation lists have been stored in the directory.
<b>Certificate system</b>	The data-technological system of the Certification Authority for generating certificates and signing revocation lists. The use and maintenance of the Certificate System is provided by the Certificate Service Provider.
<b>CMP</b>	Card Manufacturer and Personaliser
<b>CP</b>	Certificate Policy
<b>CPS</b>	Certificate Practice Statement
<b>CRL</b>	Certificate Revocation List. A list of certificates revoked before their periods of validity have expired. A certificate which has been placed on the revocation list cannot be re-activated for use.
<b>Cross certificates</b>	The certificate of another Certification Authority certified by the Certification Authority.
<b>Directory Service Provider</b>	A provider producing the data-technological directory services.
<b>End Entity</b>	A person, role person or computer system whose public key has been certified by an enciphered key of a CA and with whose personalized data the certificate is equipped with.
<b>HST</b>	Persons electronic identification issued by the Finnish Population Register Centre
<b>IETF</b>	Internet Engineering Task Force
<b>LDAP</b>	Lightweight Directory Access Protocol
<b>PC/SC</b>	Standard for smart card reader connection.
<b>PIN</b>	Personal Identification Number
<b>PKCS</b>	Public-Key Cryptography Standards. A set of standards for public-key cryptography.
<b>PKI</b>	Public Key Infrastructure
<b>RA</b>	Registration Authority
<b>RFC</b>	Request For Comments, IETF recommendation.
<b>RSA</b>	Public key cryptographic algorithm
<b>S/MIME</b>	Secure/Multipurpose Internet Mail Extensions
<b>SC</b>	Smart Card with RSA chip
<b>X.509</b>	Standard that specifies e.g. certificate format.

# 1 INTRODUCTION

## 1.1 Purpose

The rapid growth of e-business requires higher and higher levels of security and confidentiality. People involved in e-business or working remotely must be able to convince themselves not only of the identity of the other party but also of the authenticity and confidentiality of the data. This is made possible by digital certificates - data structures authenticated by a trusted party - which are used to provide proof of the identity of the person in question and to share the public key of that person. The purpose of digital certificates therefore is to increase the information security of systems as well as individuals in a public network.

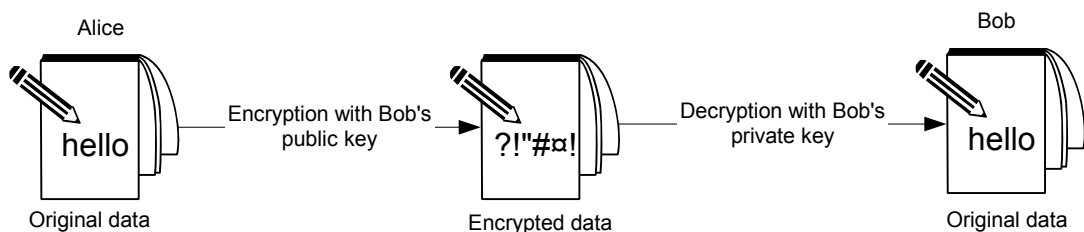
The purpose of this document is to give a basic understanding of the Public Key Infrastructure. The document concentrates on the most common features of the general PKI which is the base of Insta DefSec's Identity Management solutions.

## 2 Description of Public Key Infrastructure (PKI)

### 2.1 Asymmetric encryption

An encryption scheme, introduced by Whitfield Diffie and Martin Hellman in 1976, where each entity gets a pair of keys, called Public and Private Keys. Each entity's public-key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public-key and can only be decrypted using receiver's private key.

Public-key encryption is asymmetric because encryption and decryption use different keys.



**Figure 1: Asymmetric encryption and decryption of data**

For asymmetric encryption it is elemental that the public key management is handled efficiently. PKI offers methods for every participant's private and public key creation, public key delivery and for key revocation.

### 2.2 PKI

PKI (Public Key Infrastructure) includes a set of Public Key/Private Key algorithms that can be used for key distribution, encryption and digital signing.

Combined, all these components become an infrastructure composed of

- Certificate - a document, which ties a specific Public Key to an individual or entity
- Certification Authority - registers certificates providing assurance to the veracity of the Certificate and the relationship between the Certificate and the End Entity.
- Administrative tools - for storing, distributing, revoking, verifying status, backup and recovery of Certificates

### 2.3 The Components of PKI

A PKI consist of:

- Security Policy
- Certificate Policy (CP)
- Certificate Practice Statement (CPS)
- Certification Authority (CA)
- Registration Authority (RA)
- Certificate Distribution System
- PKI-enabled Applications

### 2.3.1 Security Policy

A security policy sets out and defines an organization's top-level direction on information security, as well as the processes and principles for the use of cryptography. Typically it will include statements on how the organization will handle keys and valuable information, and will set the level of control required to match the levels of risk.

### 2.3.2 Certificate policy

Certificate policy provides exact rules for CA operation. According to X.509, a certificate policy is "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."

Certificate policies contain specifications for security controls, CA practices, certificates, and keys, which must be implemented within the infrastructure. If there exists a possibility for cross-certification needs, it is recommended that developed policies are consistent with the IETF's framework (RFC 2527).

A certificate policy may be used by a certificate user to help in deciding whether a certificate is sufficiently trustworthy for a particular application.

CPS (Certificate Policy Statement) describes accurately how CA implements the certificate policy.

### 2.3.3 Certificate Practice Statement (CPS)

PKI systems may be operated by Commercial Certificate Authorities (CCAs) or Trusted Third Parties, and therefore require a CPS. This is a detailed document containing the operational procedures on how the security policy will be enforced and supported in practice.

CPS is a CA specific document; every CA must create its own CPS. It typically includes definitions on how the CA services are constructed and operated, how certificates are issued, accepted and revoked, and how keys will be generated, registered and certified, where they will be stored, and how they will be made available to users.

CPS is used as a tool to evaluate CA service providers. Customers evaluate the security protocols and activities used by the CA to decide if the CA meets the customers' requirements. It is recommended that CPS is based on some existing model, for example RFC 2527 (see chapter 2.8.5). It makes the service provider evaluation process easier.

### 2.3.4 Certification Authority (CA)

The CA system is the trust basis of a PKI as it manages public key certificates and private keys for their whole life cycle. The CA will:

- Issue certificates by binding the identity of a user or system to a public key with a digital signature
- Schedule expiry dates for certificates
- Ensure certificates are revoked when necessary by publishing Certificate Revocation Lists (CRLs)

When implementing a PKI, an organization can either operate its own CA system, or use the CA service of a Commercial CA or a Trusted Third Party.

### 2.3.5 Registration Authority (RA)

An RA provides the interface between the user and the CA. It captures and authenticates the identity of the users and submits the certificate request to the CA. The quality of this authentication process determines the level of trust that can be placed in the certificates.

### 2.3.6 Certificate Distribution System

Certificates can be distributed in a number of ways depending on the structure of the PKI environment, for example, manually by the users themselves, or through a directory service. A directory server may already exist within an organization or one may be supplied as part of the PKI solution.

### 2.3.7 PKI-enabled applications

A PKI is a means to an end, providing the security framework by which PKI-enabled applications can be confidently deployed to achieve the end benefits.

From the applications point of view other PKI components provide support functions for secure data transactions.

## 2.4 Advantages of PKI

PKI provides the core framework for a wide variety of components, applications, policies and practices to combine and achieve the four principal security functions for commercial transactions:

- Confidentiality – to keep information private
- Integrity – to prove that information has not been manipulated
- Authentication – to prove the identity of an individual or application
- Non-repudiation – to ensure that information cannot be disowned

PKI advantages:

- Use of CA offers centralized certification management
  - One authority grants certificates. This improves security and assures the participants that all certificates are handled similarly.
  - Certificate creation process is easier to handle.
- PKI improves the security of the system
  - PKI policy defines the security of the system. Participants have clear rules and they can evaluate the security by reviewing the policy.
  - Key revocation and certificate lifecycles can be used to keep the system secure and up-to-date. CRLs give means to remove endangered and expired certificates from the system.
- PKI offers a possibility to implement directory services
  - Simplifies the processes and requires less personnel for certificate management.
  - Directory services automate the CRL delivery process, which enables short CRL validity period. Old and endangered certificates are removed fast, which improves the security of the system.
  - Implemented directory service can be used also for other PKI based systems

- All participants get the certificate information (CRL, revoked keys, new participants in the system) immediately.
- PKI is a scalable system
  - Same system can be used for 1 - n certificates
- Cross-certification relationships
  - In future implementations, PKI offers a possibility to connect several CA systems by means of cross-certification.

## 2.5 Certificate types

Certificates can be stored in different medias; the used certificate storing media is application specific.

### 2.5.1 Smart card (SC) certificate:

The private key of the end entity is in the SC.

- Advantages
  - private key can not be read from the SC
  - easy to handle and deliver
  - cheap
  - secure PIN/PUK handling
- Disadvantages
  - Needs smart card reader device

### 2.5.2 File certificate:

The private key of the end entity is in encrypted file.

- Advantages
  - more flexible on target systems
  - can be used in wide variety of applications
- Disadvantages
  - secure password handling
  - can be copied

### 2.5.3 USB-token certificate

The private key of the end entity is in USB-token.

- Advantages
  - most computers have USB-port
  - easy to handel
  - cheap
  - no need for additional reader device
- Disadvantages
  - more complicated PIN/PUK handling

## 2.6 Cross-certification

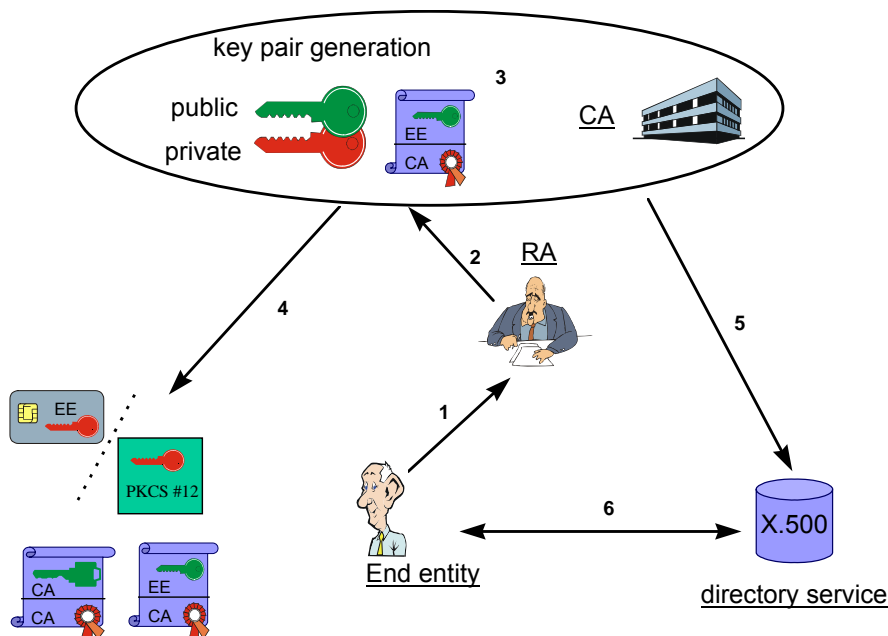
Cross-certification is a process by which two distinct CAs establish a trust relationship with each other. Cross-certified CAs agree that their respective policies and regulations are compatible, and that certificates issued by one CA may be accepted by applications who trust the certificates issued by the other CA.

Use of RFC 2527 in developing the certificate policies makes comparing of the policies easier and thus creating cross-certification relationships more straightforward.

Cross-certification is not used in existing PKI implementations. Cross-certification feature can be used in future implementations, but it is recommended that PKI implementations do not rely strongly on the cross-certification.

## 2.7 Certificate creation process

This chapter describes the typical certificate creation process.



**Figure 2: Certificate creation process**

1. End entity requests RA for a permission to order certificates from the CA.

*End entity provides all the information required in the certificate creation process. Required information is specified in the certificate policy.*

*End entity orders certificates from the RA.*

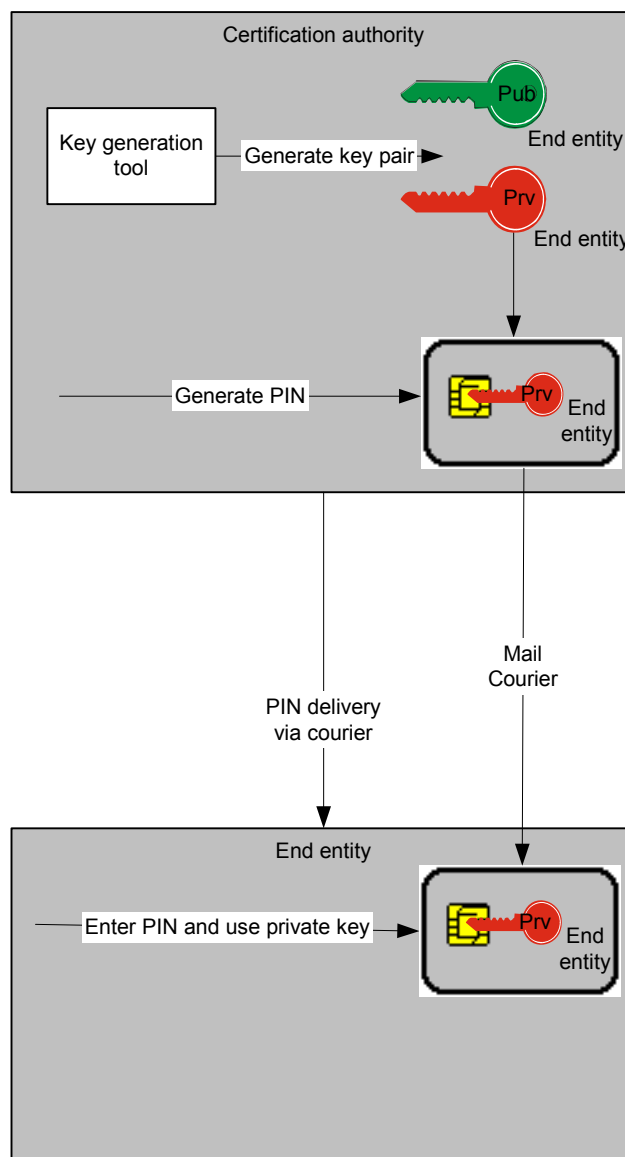
2. RA orders certificates from the CA
3. CA generates the key pair and signs the certificate.
4. CA delivers the private key, user certificate and the CA certificate to the end entity

*Using either a smart card or PKCS#12 methods (detailed description in certificate policy). SC procedure is described in Figure 3 and PKCS #12 procedure in Figure 4.*

5. CA places the certificate into the directory service.
6. The end entity queries directory service for CRL and the certificates of the intended recipients.

Smart Card creation and delivery is described in the Figure 3.

- CA creates a key pair for End Entity and places the private key into the smart card
- CA creates a PIN for smart card
- PIN and SC are delivered separately
- End Entity places the SC into the reader and enters the PIN



**Figure 3: Smart card creation and delivery process**

PKCS #12 key creation and delivery is described in the Figure 4.

- CA creates a key pair for End Entity
- CA generates a password for PKCS #12 packet and seals the private key into a PKCS #12 packet
- Password and PKCS #12 packet are delivered separately
- End Entity enters the password and unpacks the PKCS #12 packet. Private Key installation is product specific.

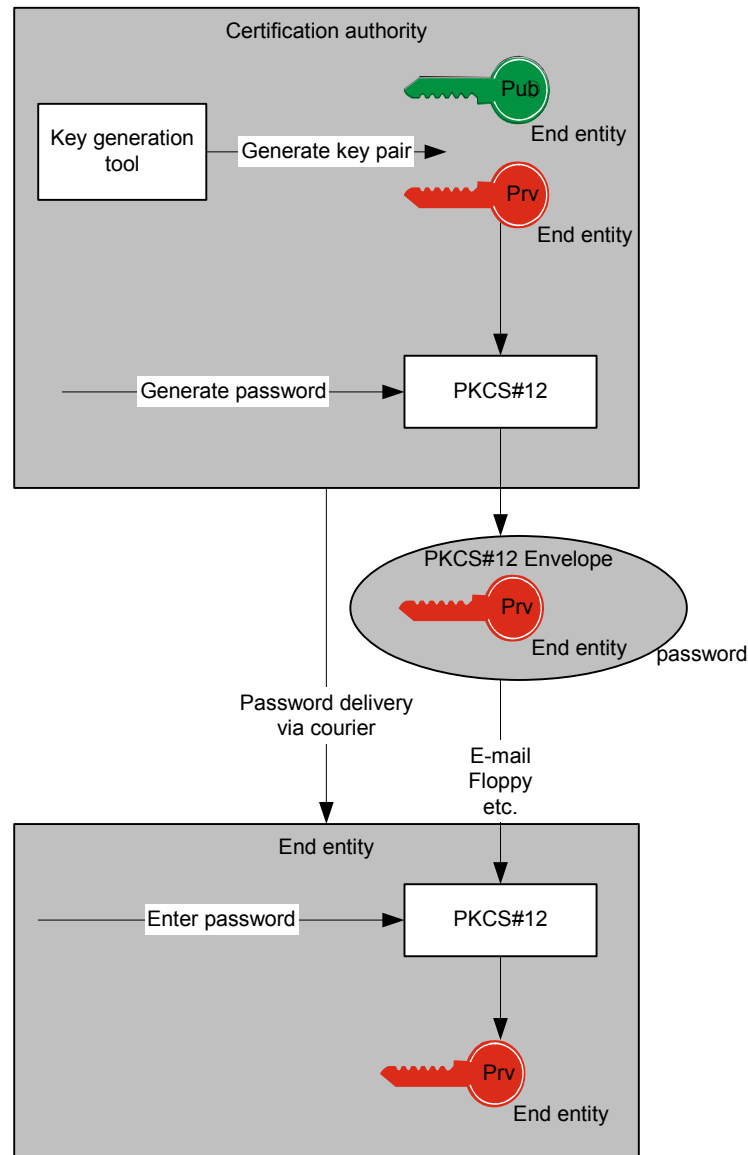
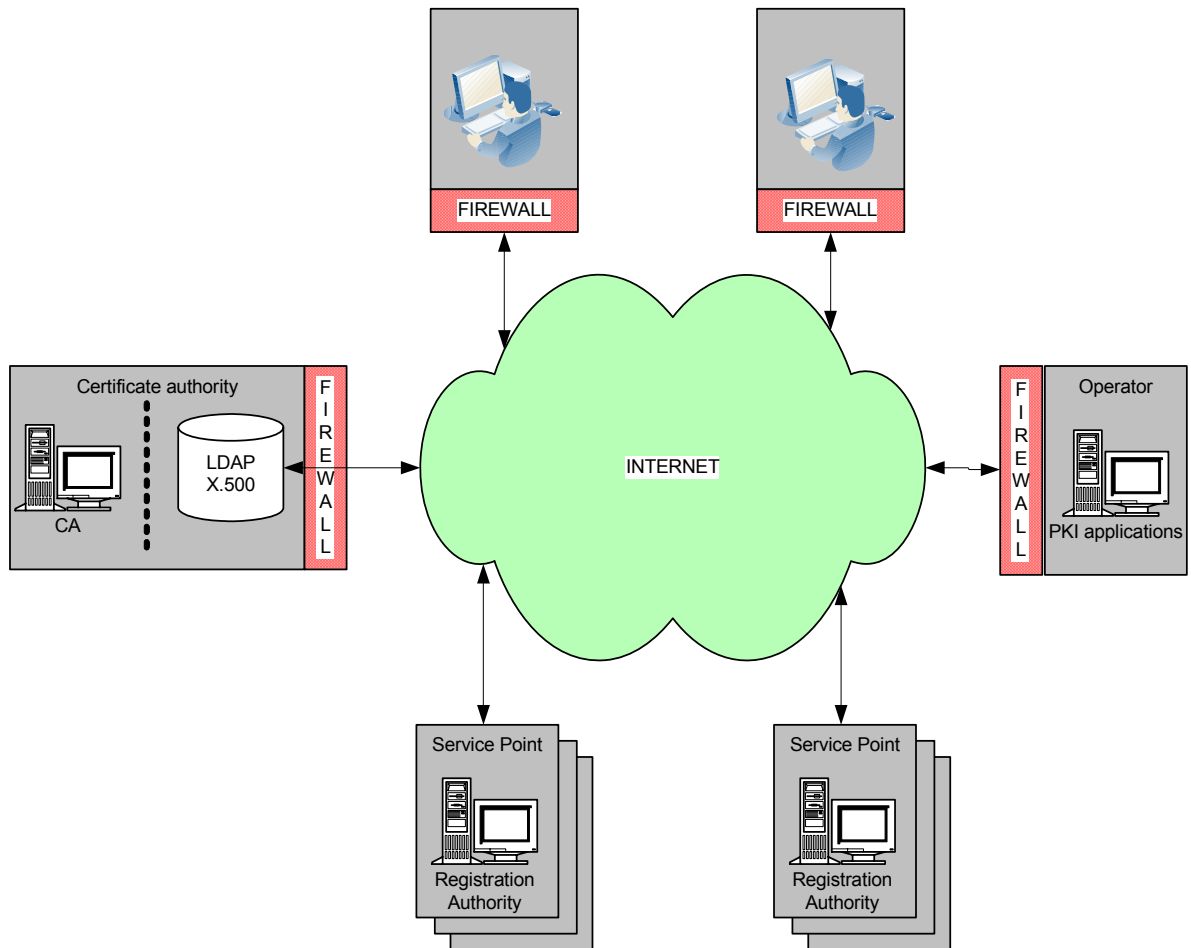


Figure 4: PKCS #12 key pair creation and delivery process

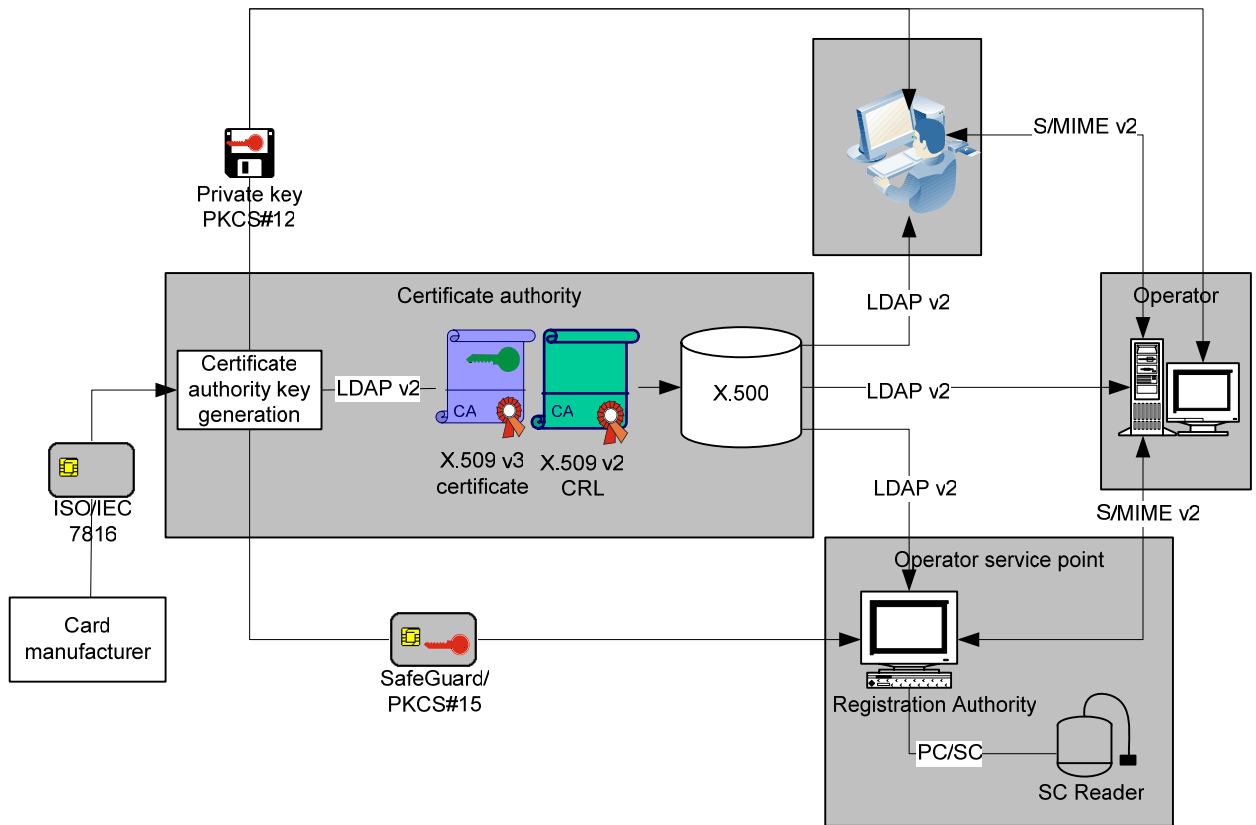
## 2.8 Used standards and recommendations

This chapter gives a short description of used standards in PKI implementation. Used standards are presented in figure 6. The arrows in the figure present the logical information flow direction.

Figure 5 presents a simplified network structure. A firewall is recommended in front of the directory service (LDAP). The network is presented in the viewpoint of one operator.



**Figure 5: Network structure**



**Figure 6: Used standards in key/certificate delivery**

### 2.8.1 X.500

An ITU-T Recommendation that is one part of a joint ITU-T/ISO multi-part standard (X.500-X.525) that defines the X.500 Directory, a conceptual collection of systems that provide distributed directory capabilities for OSI entities, processes, applications, and services. (The ISO equivalent is IS 9594-1 and related standards, IS 9594-x.)

### 2.8.2 X.509

An ITU-T Recommendation that defines a framework to provide and support data origin authentication and peer entity authentication services, including formats for X.509 public-key certificates, X.509 attribute certificates, and X.509 CRLs. (The ISO equivalent is IS 9498-4.). Use of X.509 certificates require that a CA is implemented in the system.

### 2.8.3 RFC 1777, LDAP (Lightweight Directory Access Protocol)

Framework provided by IETF, which presents a client-server protocol that supports basic use of the X.500 Directory (or other directory servers) without incurring the resource requirements of the full Directory Access Protocol (DAP).

Designed for simple management and browser applications that provide simple read/write interactive directory service. Supports both simple authentication and strong authentication of the client to the directory server.

#### 2.8.4 ISO/IEC 7816

Standard describes the hardware requirements of the SC's. For example SC manufacturer Setec conforms to the standard.

#### 2.8.5 RFC 2527 (Internet X.509 PKI Certificate Policy and Certification Practices Framework)

Framework by IETF provides a comprehensive list of topics that need to be covered in a certificate policy definition. Certificate policy can be based on structure presented in RFC 2527.

All the issues handled in RFC 2527 are not be required for PKI policy implementation, but it is recommended that all the issues covered in RFC 2527 should be handled even if all parts are not included in the final policy.

For example the HST (The persons electronic identification issued by the Finnish Population Register Centre) certification policy is done by using the RFC 2527 and ETSI's Work Item 'DES/SEC-004007-2' Policies for CSP's is based on RFC 2527.

When the certification policy is made according to recommendation it is easier to compare separate CA-policies (cross-certification).

#### 2.8.6 PKCS #12

Specification produced by RSA Laboratories, which provides a recommendation that describes transfer syntax for personal identity information, including private keys, certificates, miscellaneous secrets, and extensions.

#### 2.8.7 PKCS #15

Specification produced by RSA Laboratories that describes the internal SC structure.

#### 2.8.8 S/MIME

Specification produced by RSA Laboratories that describes Secure/Multipurpose Internet Mail Extensions, an Internet protocol to provide encryption and digital signatures for Internet mail messages. The protocol is also suitable for similar message based systems. S/MIME standard requires a X.509 certificate structure.

#### 2.8.9 PC/SC

PC/SC is a recommendation to standardize PC interfaces to Interface Devices (IFDs) and to specify common PC programming interfaces and control mechanisms including SC's.

The PC/SC workgroup provides recommendation. The workgroup includes companies like Intel, HP, Apple, Microsoft and Toshiba.

## 2.9 PKI references

Here are few examples of existing PKI application areas around the world. Some of them are already taken in use and some are in the implementing phase.

- Microsoft Windows 2003
  - PKI support
- Governments
  - Electronic national identity card schemes
  - Smart card based secure network authentication and communications
  - Employees use smart cards for strong VPN authentication and online communications.
- Healthcare
  - Electronic prescriptions with digital signatures
  - Digital patient records
- Corporations
  - Remote work
  - Access control, authorisation
- Banking and finance
  - eBanking services

## 3 Insta's PKI-based products and services

Insta's PKI-based security products and solutions enable our customers to benefit from improved business models and to develop their operations. Efficient, secure e-business and networking solutions improve our customers' business operations, administration and utilization of modern technology.

### 3.1 Insta Certifier

Insta Certifier is a CA (Certification Authority) product for issuing and managing digital certificates in a service provider and enterprise environment. Insta Certifier enables the use of strong two-factor user authentication with smart cards and USB tokens to support secure access to enterprise applications. In addition to providing authentication management, Insta Certifier can be used as a backbone for building secure services such as Virtual Private Networks (VPNs), secure e-mail, single sign-on (SSO), and network logon based on third-party products. The integrated approach for managing identities and authentication supported by Insta Certifier allows a highly cost-effective deployment and operation of PKI in environments of all sizes.

Insta has built several identity management solutions based on Insta Certifier - product. These solutions include

- Insta ID for creating digital identities
- Insta E-mail Security for e-mail encryption and digital signing
- Insta Control for access control, digital identity management and authorisation

All Insta solutions are scalable and modular which enables the possibility also to customise our solutions according to customers' needs.

## 3.2 Insta Managed PKI

Insta can provide PKI-based certificate solutions as a managed service. Insta Service Center provides its clients with value added services of information security and user administration that support business activities professionally and cost-efficiently. Our services have been awarded the international BS7799 certificate.

Benefits of the managed service are:

- No need to bind critical resources to administration and deployment
- Service provider already has security and operations expertise and experience
- Shorter time to utilization
- Reduce investment need and establish predictable cost

PKI managed services include the whole certificate life-cycle management for the customer including:

- CA hosting and administration
- Certificate issuing and enrolling
- Certificate publishing to LDAP
- Certificate revocation list publishing to LDAP
- Certificate life-cycle management
- Supervision services
- PKI smart card, smart card reader and USB token deliveries
- Professional Services
- PKI deployment
- PKI application consultation
- PKI training
- Insta Certifier training
- Customer support services
- 24/7 Certificate revocation service

We can provide the whole certificate life-cycle management as a service or part of it can be delegated to the customer. Read more at [www.certificate.fi](http://www.certificate.fi), or contact us at [security@insta.fi](mailto:security@insta.fi).

## 4 Insta Security Systems

Insta DefSec's Security Systems is a global information security specialist developing and supplying networking and information security solutions. We focus on innovative solutions and applications for customers with high quality and security requirements.

Our product and service solutions enable our customers to benefit from improved business models and to develop their operations. Efficient, secure e-business and networking solutions improve our customers' business operations, administration and utilization of modern technology.

Our know-how, technology and processes represent the absolute top in their field, which is why we have reached an internationally recognized position in the information security market.

» *Visit our web pages to learn more about our company and resources at [www.certificate.fi](http://www.certificate.fi).*