Public Key Certification Infrastructure

Petr Hanácek
hanacek@dcse.fee.vutbr.cz

Faculty of Electrical Engineering and Computer Science
Brno University of Technology

Jan Staudek
staudek@fi.muni.cz

Faculty of Informatics
Masaryk University Brno

Abstract

The article deals with the technical and non-technical problems of the certification authorities and public key infrastructure (PKI). It explains individual technical processes and the binding of these processes to the system of appropriate documents (e.g. Certification Policy) and administrative measures. The authors will present their experiences with design of the real PKI for governement applications. The described PKI will employ public key technology at multiple levels of assurance. The fundamental objective of this PKI is to provide digital identity services. It will also support privacy services. It is the objective of the PKI to provide certification services that have the following attributes: standards-based, support multiple applications and products, provide secure interoperability throughout government and with industry, support digital signature and key exchange and encipherment, provide functional separation of keys, support key recovery and data recovery, support legal non-repudiation, commercial-based, allowing for the possible outsourcing of elements in the future. The described PKI program is committed to working with major industry application providers to ensure both short-term and long-term interoperability.

Keywords: PKI, Public Key Infrastructure, certification.

1. Introduction

Public key cryptography offers the potential to security enable a wide range of applications of interest to the Czech government. Public key cryptography potentially enables substantial improvements to business processes as well as enhanced security. Digital signatures made possible with public key techniques have the potential to replace ”handwritten” signatures on documents and make digital documents the legal equivalents of paper documents with handwritten signatures.

This paper will examine the requirements and their associated issues that are placed on the PKI to support various security services for some government applications in Czech Republic. The requirements include both technical measures (like certificate generation) and policy considerations (how to set-up a domain trust relationship).

Realization of the benefits of public key technology depends on the availability of a public key infrastructure (PKI). The PKI will establish the facilities, specifications, and policies needed by the government to use public key-based certificates for information system security, workflow processing electronic commerce, secure communications, and E-mail within the government as well as with organizations of other branches of the government. Standards will provide the basis for the facilities that the PKI provides. Standards organizations that influence the PKI include the International Standards Organization (ISO), the Telecom-

munication Standardization Sector of the International Telecommunication Union (ITU-T), the Internet Engineering Task Force (IETF), and the ETSI.

2. Purpose of PKI

The primary purpose of the PKI is to provide public key certificates. A certificate is a data structure that includes a public key and the name of the person or entity that owns the public key. Individuals or entities who own public keys contained in a certificate are subscribers. The certificate also includes the name of the certification authority (CA) who created the certificate, and the period of time for which the certificate is valid. CAs digitally sign certificates. The CA is responsible for ensuring that the public key holder is the person named in the certificate and the holder of the private key associated with the public key . The CA also publishes a certificate revocation list (CRL) that lists certificates that should not be used. For example, if a subscriber's private key is compromised, the certificate containing the associated public key would be revoked.

Parties (individuals or organizations) who use the certificates are relying parties. Relying parties use certificates to verify that a subscriber digitally signed information or to encrypt information that only the subscriber can decrypt. The PKI provides a directory service to allow relying parties to obtain subscribers' certificates. CAs make the CRL available by publishing it to the directory. The directory also includes information associated with the subscriber to allow directory users to contact subscribers. Such contact information includes e-mail addresses, telephone numbers, organizational associations, and mailing addresses.

In summary, the PKI provides the services to:

- Receive requests for certificates.
- Issue certificates and otherwise respond to requests for certificates.
- Revoke certificates.
- Publish CRLs.
- Maintain a directory service allowing users to retrieve certificates, CRLs, and subscriber contact information.

3. Supported security services and types of certificates

The PKI will provide the services and facilities needed for unclassified secure information, including:

- digital signatures for:
  - ♦ authentication;
  - ♦ integrity;
  - ♦ non-repudiation.
- management of symmetric keys for confidentiality for:
  - ♦ communications sessions;
  - ♦ e-mail messages.

When extended by Key Recovery Agents, the PKI will also provide key recovery services for encrypted data. The PKI will provide the services and facilities needed for secure information access, communication, messaging and electronic commerce with commercial and personal users employing common de facto and formal security standards and using mainstream commercial security products. The PKI will be implemented primarily with ordinary commercial security products.

End-entities and infrastructure elements use PKI differently and require unique services. Digital signature and key agreement algorithms provide different services and require different infrastructure support. Table 1 identifies the service that each application uses. When deciding on the solution to specific issues, its application must be considered.

PKI Services User	Digital Signature	Key Agreement
End User	Data Integrity Non-repudiation Data Authentication Entity Authentication Third Party Services	Confidentiality Privacy
Infrastructure	Certificate Integrity Entity Authentication Date Authentication Non-repudiation Authorization/Privilege Cross-certification Compromise Recovery	Confidentiality (private keys) Key recovery

Table 1. Services

Many applications may rely on the PKI. Not all of the applications are currently known. However, based on known and anticipated needs, the PKI shall issue standard certificates intended to meet these needs. Table 2 lists these certificates and their respective purposes and characteristics.

Certificate Type	**Purpose and Properties**
Identity	**Purposes:** Owner authentication, Owner accountability (non-repudiation) **Characteristics:** Holds only basic, static identity information, Private key under owner's exclusive control
Privacy	**Purpose:** Encrypt information for privacy **Characteristics:** Holds only basic, static identity information, Private key subject to data recovery
E-mail	**Purposes:** Single key for dual-use (sign and encrypt S/MIME e-mail) (near term), Separate keys and certificates for signing and encrypting e-mail (mid-term) **Characteristics:** Includes e-mail address (non-static), Dual-use private key subject to data recovery (near term)
Server or device	**Purposes:** Support Secure Sockets Layer for client-server communications (authentication and privacy), Support Internet Protocol Security employment (authentication and privacy) **Characteristics:** May include host name or IP address, Private key subject to data recovery
CA, Root CA	**Purposes:** Certificate authentication and integrity, CA accountability (non-repudiation) **Characteristics:** Private key under CA's exclusive control

Table 2. Types of certificates

3.1 Certificate Assurance Levels

The X.509 standard does not associate certificate policies with particular assurance levels. However some approaches define a number certificate policies ordered by their assurance level. The proposed PKI proposes two ordered levels of assurance:

- Medium-level Assurance
- High Assurance

Certificates issued within this PKI will contain at least one of the standard assurance level policy IDs in the certificate policies extension.

3.2 Certificate Policy Field Contents

The **certificatePolicies** extension in PKI certificates will identify the policies that apply to a certificate. The **certificatePolicies** field will contain the identifier of an assurance level policy, that states the highest level of trust supported by this certificate, as determined by the issuing CA and its policy management authority.

4. PKI Structure

The structure of proposed PKI is a hierarchical architecture. In the hierarchical architecture all relying parties base their trust on the key of a single root CA. The root's public key must be distributed in some authenticated fashion to all relying parties, to "bootstrap" trust in the PKI. Trust paths descend from the root through subordinate CAs. The hierarchical certification path architecture has some advantages:

- The organizational management structure of many organizations such as the government is largely hierarchical. Trust relationships are frequently aligned with organizational structure, so it is natural to align the certification path with the organizational structure;
- The hierarchy may be aligned with hierarchical directory names;
- The strategy for searching for a certification path is straightforward;
- Important existing PKI components are designed hierarchically;
- Each user has a certification path back to the root. The user can provide his path to any other user and any user can verify the path, since all users know the root's public key.

A strictly hierarchical certification path architecture also has some disadvantages:

- It is improbable that there will be a single root CA for the world PKI;
- Commercial and business trust relationships are not necessarily hierarchical;
- Compromise of the root private key is catastrophic and recovery requires the secure distribution of the new public key to every user.

Early attempts to design PKIs, such as the Internet Privacy Enhanced Mail (PEM) standard generally featured a hierarchical structure. The principal reason for this was to facilitate the management of security policies and trust relationships: branches of the tree were aligned with security policies. The X.509 v3 certificate structure, however, introduces several extensions that allow the management of policies and trust relationships in a non-hierarchical PKI, and this rationale for a hierarchical PKI is no longer compelling.

The PKI will support secure communications with business, other branches of the government, the public, and state and local governments, as well as between departments. The PKI will therefore support and inter-operate with a broad range of technologies, as appropriate, including commonly used technologies that are not approved for use to protect communications between users.

The PMA will approve cross-certification with non-government CAs. The optional policy mapping, path length constraint, and subtrees constraint extension fields of the X.509 v3 certificates may be used by CAs to constrain the use of cross certification links with non-government CAs and infrastructures.

CAs may issue end-entity certificates to non-government users in accordance with their CPS. Name space constraints in the certificates may, however, limit propagation of trust to certificates issued to subjects with non-government names.

5. PKI Management and Policies

Certificate Policies and Certification Practice Statements are key elements in the management of the PKI. The management body for the PKI will be the Policy Management Authority. Similarly domain Policy Management Authorities will manage the policies for the CAs within individual trust domains.

The terms Certificate Policy (CP) and Certification Practice Statement (CPS) are often confused. The term certificate policy effectively has an evolving legal meaning and a more or less mechanical instantiation as a field in a certificate. However, the processing of certificate policies extension has two different modes, depending on the critical bit in the extension.

A Certification Practice Statement (CPS) is a statement of the practices that a particular CA employs in issuing certificates. A CPS describes the details of the system used and the practices employed by a CA to issue certificates. A CPS details the procedures used to implement the policies identified in the certificates issued by a CA, including the means used to identify certificate subjects. It also states the means used to protect the public key of the CA, and the other operational practices followed by the CA to ensure security.

There is a standardized outline and list of factors to be considered in writing a CPS or CP The basic list of topics to be covered are the same for both a certificate policy and a CPS. The outline addresses the following major subject areas:

1. *Introduction:* Identifies who operates and manages the CA (or the certificate policy), the users it serves and how to contact it.
2. *General Provisions:* covers liability, fiscal responsibility, governing law, fees and similar considerations
3. *Identification and Authentication*: deals with how names are assigned and identities proofed.
4. *Operational Requirements*: describes the process for issuing and revoking certificates, the records that are kept the audits that are performed, and CA compromise, disaster recovery and termination provisions;
5. *Physical, Procedural and Personnel Security Controls*: describes the physical facilities, the trusted roles in operating the CA and issuing certificates, and the personnel controls on CA/RA personnel;
6. *Technical Security Controls*: covers cryptographic issues, key pair generation, the algorithms used, how private keys are activated, protected, and managed, and the technical security considerations for CA, RA and end entity systems;
7. *Certificate and CRL Profile*: states the rules for the use of certificate and CRL extensions;
8. *Specification Administration*: states how the CP or CPS is administered and maintained.

The example contents of CP and CPS is in the following table:

1. INTRODUCTION	
	OVERVIEW
	IDENTIFICATION
	COMMUNITY AND APPLICABILITY
	CONTACT DETAILS
2	**GENERAL PROVISIONS**
	OBLIGATIONS
	LIABILITY
	FINANCIAL RESPONSIBILITY
	INTERPRETATION AND ENFORCEMENT
	PUBLICATION AND REPOSITORY
	COMPLIANCE AUDIT
	CONFIDENTIALITY
	INTELLECTUAL PROPERTY RIGHTS
3	**IDENTIFICATION AND AUTHENTICATION**
	INITIAL REGISTRATION
	CERTIFICATE RENEWAL, UPDATE, AND ROUTINE RE-KEY
	RE-KEY AFTER REVOCATION
	REVOCATION REQUEST
4	**OPERATIONAL REQUIREMENTS**
	CERTIFICATE APPLICATION
	CERTIFICATE ISSUANCE
	CERTIFICATE ACCEPTANCE
	CERTIFICATE SUSPENSION AND REVOCATION
	SECURITY AUDIT PROCEDURES
	RECORDS ARCHIVAL
	KEY CHANGEOVER
	COMPROMISE AND DISASTER RECOVERY
	CA TERMINATION
5	**PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS**
	PHYSICAL CONTROLS
	PROCEDURAL CONTROLS
	PERSONNEL CONTROLS
6	**TECHNICAL SECURITY CONTROLS**
	KEY PAIR GENERATION AND INSTALLATION
	PRIVATE KEY PROTECTION
	OTHER ASPECTS OF KEY PAIR MANAGEMENT
	ACTIVATION DATA
	COMPUTER SECURITY CONTROLS
	LIFE CYCLE TECHNICAL CONTROLS
	NETWORK SECURITY CONTROLS
	CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS
7	**CERTIFICATE AND CRL PROFILES**
	CERTIFICATE PROFILE
	CRL PROFILE
8	**SPECIFICATION ADMINISTRATION**
	SPECIFICATION CHANGE PROCEDURES
	PUBLICATION AND NOTIFICATION POLICIES
	CPS APPROVAL PROCEDURES

6. Certificate Revocation List (CRL)

Certificate Revocation Lists (CRL) list unexpired certificates that have been revoked or placed on ”hold.” In the general case, certificates may be revoked for a variety of reasons; however, a CRL entry shall be issued only for situations where the private key has been (or is suspected of being) compromised or malfeasance is suspected.

The X.509 v2 certificate revocation list format adds several optional extensions to the v1 format, similar in concept to those defined for certificates. CAs shall initially generate only version 1 CRLs but shall migrate to version 2 over time. In the future, the CA that issues a CRL is not necessarily the CA that issued the revoked certificate, and some CAs may issue only CRLs. Introduction

7. Conclusions

This paper, which is based on work performed for the Czech government by both authors, presents several perspectives and addresses several issues, which will be incorporated in some part of government PKI in Czech Republic. The work assumes use of the X.509 Version 3 certificate format and associated standard extensions, resulting in a more flexible and powerful architecture than was possible with earlier certificate formats. Attention is given to issues of how a government PKI would interoperate with PKIs of other national governments, of other tiers of government, and of private industry. Substantial consideration is given to the full set of functions needed in hardware/software implementations of the PKI components and the end-user encryption and digital signature devices they would support.

8. References

[1] ISO 7498-2: 1989, Information processing systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture.

[2] ISO/IEC 9594-8: 1990, Information technology - Open Systems Interconnection - The Directory - Part 8: Authentication framework.

[3] FIPS1401 Security Requirements for Cryptographic Modules, 1994-01.

[4] The Department of Defense (DOD) Public Key Infrastructure (PKI) And External Certification Authorities (ECAs), July 13, 1998.

[5] Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile, January 4, 1999.

[6] RFC 2459, Internet X.509 Public Key Infrastructure Certification and CRL Profile, January 1999.

[7] RFC 2527, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, March 1999