Chapter XL
Federal Public-Key Infrastructure

Ludwig Slusky
California State University–Los Angeles, USA

Parviz Partow-Navid
California State University–Los Angeles, USA

INTRODUCTION

All branches of federal government are required to change their business practices to a paperless operation. Privacy and information security are critical for the protection of information shared over networks internally between the U.S. government agencies and externally with nonfederal organizations (businesses; state, local, and foreign governments; academia; etc.) or individuals.

The public-key infrastructure (PKI) is the simplest, most widely used architecture for secure data exchange over unsecured networks. It integrates computer hardware and software, cryptography, information and network security, and policies and procedures to facilitate trust in distributed electronic transactions and mitigate the associated risks.

Federal PKI (FPKI) is PKI designed for implementation and use by government agencies. Federal PKI research was under way since 1991, and by the end of 2005, the federal PKI included 13 cross-certified federal entities, three approved shared service providers (SSPs; Verisign, CyberTrust, National Finance Center/U.S. Department of Agriculture [USDA]), one state, and three foreign countries (Canada, UK, and Australia; Alterman, 2005).

Initially envisioned as an interoperability mechanism for federal organizations exclusively, the federal PKI is now positioned for trust interoperability and cross-certification internally among federal agencies and externally with other organizations.

BACKGROUND

The federal PKI encompasses an interoperable public-key infrastructure that utilizes the capabilities of commercial-off-the-shelf (COTS), standard-based products and services as well as new solutions.

Both PKI and federal PKI are based on the same four fundamental principles of information security (CIA+N/R).

- **Confidentiality:** Assurance that the information has been hidden during transport.
- **Integrity:** Assurance that the information has not been altered.
- **Availability:** Assurance of reliable and timely access to data.
- **Nonrepudiation:** Assurance of irrefutable evidence that an action took place.

Implementation of federal PKI is supported by public-key encryption technology with digital signatures, cross-certification, defined assurance levels, and personal identity verification cards designed to extend the federal PKI services to end users (i.e., employees, contractors of federal agencies).

Public-Key Encryption Technology

At the core of PKI is the enabling cryptographic technology for the sharing of secure information.

Contrary to symmetric encryption schemes operating with a single key for both encryption and decryption, PKI encryption technology is based on an asymmetric encryption schema with two mathematically related keys, of which one, the public key, is used to encrypt a message and another one, the private key, is used to decrypt it (Merlow & Brethaupt, 2006; National Institute of Standards and Technology, 2001).

An asymmetric schema has an important advantage: It does not share a secret key. Public keys can be distributed and published openly. A private key, however, is only known to the owner; so, it is much easier to keep it secret.

The PKI process takes place as follows:

1. The recipient makes its public key known to others while keeping its private key secured.
2. A sender encrypts a message with the known recipient's public key.
3. The recipient decrypts the message with its secret private key.

Digital Signature

The mechanism to assure the accuracy of the public key is a public-key certificate. It binds the public-key value to the entity (also called a PKI subscriber), which owns this public key. The entity that receives the certificate (also called a PKI relying party) relies on the accuracy of the public key in that certificate. It does so by verifying the digital signature in the received subscriber's certificate (Federal Public Key Infrastructure Steering Committee, 2005). So, a public-key certificate assures that the contained public key is accurate and belongs to the subscriber.

Digital signature combines one-way secure hash functions with public-key cryptography as follows. A hash function is applied to the message to generate a fixed-length hash value (unique to the encrypted document). This value is then encrypted with the private key of the sender and attached to the message. Thus, the hash value assures data integrity of the message, and encryption of this value with the sender's private key assures nonrepudiation of the message. However, by itself, a digital signature does not protect confidentiality of the message. That is accomplished by encrypting the message as discussed above (Stewart, Tittel, & Chapple, 2005).

Upon receiving the message, the recipient validates the digital signature by generating and matching two hash values: One is produced by the hash function applied to the message, and another is produced by decrypting the digital signature with the sender's public key.

The PKI allows for multiple digital signatures on PKI transaction records representing cosigning or single signing of a part of the large document that has to be split between several transactions.

PKI Architecture

A basic PKI architecture consists of five components: the certificate authority (CA), registration authority (RA), repository, archive, and users (Microsoft, 2005).