PKI Smart Card Technology

Dragan M. Spasić[1]

Abstract - **Hardware-based cryptography is more secure than software-based cryptography, because cryptographic operations are performed and private keys stored on the cryptography devices (such as smart cards). This paper provides a description of a digital ID, cryptographic keys and digital certificates, creating a digital ID, Microsoft CryptoAPI, and PKI smart card structure and operations. Included in this description is also the Philips Smart Card P8WE5032 chip.**

Keywords - **Public Key Infrastructure (PKI), digital certificate, smart card, Microsoft CryptoAPI.**

I. Introduction

Users submit transactions via the Internet only when they are confident that their personal information, such as credit card numbers and financial data, is secure. The Public Key Infrastructure (PKI) [1, 2, 3] is the basis for every e-business (e-commerce, e-banking, e-government…) trust infrastructure. PKI cryptography, digital signature, and smart card technology, applied via digital certificates, provide the authentication, data integrity, nonrepudiation and privacy (confidentiality) necessary for e-business.

PKI smart card is hardware-based cryptography device for securely generating and storing private and public keys, digital certificates and performing cryptographic operations, such as digital signing and key exchange. Only someone who possesses the smart card, the smart card reader and knows the Personal Identification Number (PIN) can use the smart card.

Smart card vendors provide interface software, such as Cryptographic service provider module (CSP), for use with Microsoft CryptoAPI, or they use a PKCS#11 module. Support for Gemplus GemSAFE smart card, and Schlumberger-Axalto Cryptoflex smart card [4] is included with the Windows 2000/XP installation. Additional smart card CSPs might be developed and certified for use with Windows 2000/XP (for example, Datakey RSA CSP).

II. A Digital ID and Media

A digital ID is a set of electronic credentials that uniquely identify a person. There are two parts to a digital ID: an asymmetric private key and a digital certificate (asymmetric public key).

Asymmetric keys come in pairs. PKI uses asymmetric keys in both encryption and digital signature operations. In the encryption operation, there is an encryption public key and a decryption private key. The decryption private key decrypts data that has been encrypted with the corresponding encryption public key.

In the digital signature operation, there is a signing private key and a verification public key. The verification public key is used to decrypt a hash value that has been encrypted with the signing private key.

PKI X.509 digital certificate is the public part of digital ID. Each digital certificate contains at least the following fields [5]:

- Version. Version of the certificate format (for example, version 3).
- Serial number. The unique serial number that is assigned by the issuing CA (the entity that issued the certificate).
- Signature algorithm. The message digest (hash) and public key cryptography algorithms that are used by the issuing CA to digitally sign the certificate.
- Issuer. The name of the issuing CA.
- Validity period. The certificate's start and expiration dates. These define the interval during which the certificate is valid, although the certificate can be revoked before the designated expiration date.
- Subject. The name of the subject (owner) of the certificate.
- Subject public key information. The public key and the public key cryptography algorithm.
- Digital signature. The CA's digital signature, which is created as the last step in generating the certificate.

The following media can be used for storing digital ID:

- Hard disk, CD-ROM, floppy disk, or other removable media.
- PKI smart card (Fig. 1.).
- PKI USB smart token (Fig. 2.). It plugs directly into a USB port (no smart card reader required).

Smart cards and USB tokens provide a number of benefits [6]:

- Security: Private key never leaves the card, and is protected by two-factor security: something that is owned (the card) and something that is known (the card PIN or PassPhrase).
- Portability: Digital ID can go wherever user (owner) go.
- Flexibility: A card can be used to store a variety of data, including private keys, public keys, digital certificates, user names and passwords, etc.
- Simplicity: Many passwords can be stored on a single card. In addition, user is less likely to lose a card than forget a password.

[1] Dragan M Spasić is with the Public enterprise of PTT communications "Srbija" (Post Serbia), Katićeva 14-18, 11000 Belgrade, SCG, E-mail: dspasic@ptt.yu

- Ease of use: A card is simply inserted into a card reader to activate an application. Also, one card can be used for several applications.

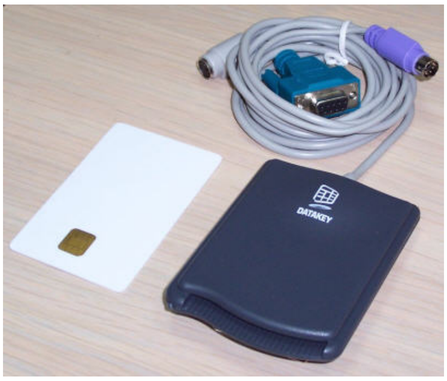

Fig. 1. Smart card and smart card reader

Fig. 2. USB smart token

III. Creating a Digital ID

Digital ID is created in a three-step process (Fig. 3.) [7]:

1. Private and public keys are generated on a smart card. This is done directly on a card. The private key is permanently stored on a card. It never leaves a card. The public key is sent to a Certificate Authority (CA).
2. The CA verifies the public key really belongs to user. If the verification succeeds, it creates a digital certificate for user and sends codes to user to download the certificate.
3. User then downloads the digital certificate on a card, completing the digital ID.

This three-step process is very simple for end user, because, most of the details are transparent.

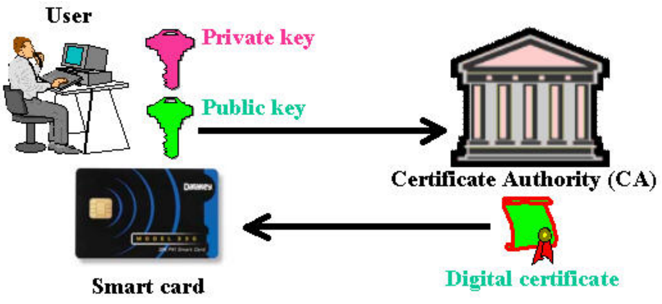

Fig. 3. Creating a digital ID

IV. Microsoft CryptoAPI

The basic cryptographic element of the Windows 2000/XP architecture is the Microsoft Cryptographic Application Programming Interface, or Microsoft CryptoAPI, or CAPI. All major application elements of Windows 2000/XP make use of the Microsoft CryptoAPI for their cryptographic services. The Microsoft CryptoAPI model consists of (Fig. 4.):

1. Applications.
2. Microsoft CryptoAPI (CAPI).
3. Cryptographic Service Provider (CSP) modules.
4. Smart cards.

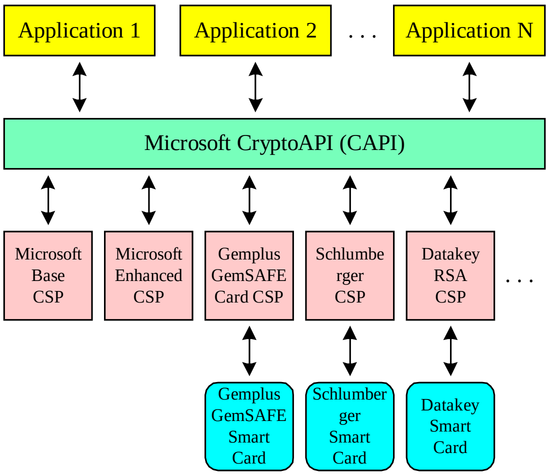

Fig. 4. Microsoft CryptoAPI model

Microsoft CryptoAPI provides a set of functions that allow applications to encrypt or digitally sign data in a flexible manner while providing protection for private keys. Cryptographic operations are performed by independent modules known as cryptographic service providers (CSPs). Any Windows 2000/XP application can request cryptographic operations from a CSP. CSPs can be implemented in software as well as in hardware (such as smart card CSPs).

Using Microsoft CryptoAPI, developers can easily integrate strong cryptography into their applications. Cryptographic service provider (CSP) modules interface with CryptoAPI and perform several functions [8]:

- Create and manage private and public keys.
- Create and manage digital certificates.
- Encrypt and decrypt messages, files, programs, passwords, forms, credit-card numbers or any other data either residing locally on a computer or being transmitted over a network, including the Internet.
- Digitally sign a message or data to ensure that a recipient knows the identity of its creator and that the data hasn't been tampered with or altered.

Microsoft provides two distinct CSP modules with Windows 2000/XP configurations:

1. Microsoft Base Cryptographic Provider, which provides basic cryptography support (RSA key length: 512 bits).
2. Microsoft Enhanced Cryptographic Provider, which provides strong cryptography support (RSA key length: 1024 bits).

For these Microsoft CSPs, all cryptographic operations are provided through software within the CSP. No cryptographic hardware, including smart cards, is supported. Both CSPs use RSA technology. Microsoft CSPs have received the Federal Information Processing Standard (FIPS) 140-1 Level 1 certification by the National Institute of Standards and Technology (NIST).

Vendors can develop hardware or software CSPs that support a wide range of cryptographic operations and technologies. However, Microsoft must certify and digitally sign all CSPs. CSPs do not work in Windows 2000/XP unless they have been digitally signed by Microsoft.

Windows 2000/XP includes smart card CSPs from two vendors: Gemplus (http://www.gemplus.com) and Schlumberger-Axalto (http://www.axalto.com). The Gemplus GemSAFE Card CSP and the Schlumberger CSP support cryptographic operations for the Gemplus and Schlumberger-Axalto smart cards, respectively. Additional smart card CSPs might be developed and certified for use with Windows 2000/XP (for example, Datakey RSA CSP).

V. Smart Card Structure

The PKI smart card is a credit card-sized device that is used to securely generate and store private and public keys, digital certificates and to perform cryptographic operations, such as digital signing and key exchange. It contains [7]:

1. Chip or integrated circuit (IC). The chip includes (for example, Fig. 5.): CPU (Central Processing Unit) - perform cryptographic operations, ROM (Read-Only Memory) - memory for containing the smart card operating system, RAM (Random Access Memory) - memory that can be read and written by the CPU, EEPROM (Electronically Erasable and Programmable Read-Only Memory) - memory to securely store private and public keys, digital certificates and other data as required, etc.
2. Smart card contact. The smart card contact has 8 contacts [9].
3. Smart card body. The smart card is credit card-sized plastic card.

The PKI smart card is protected from misuse by the Personal Identification Number (PIN) or PassPhrase, which is known only to the owner of the smart card. To use the smart card, a user inserts the card in a smart card reader that is attached to a computer and, when prompted, enters the PIN. The smart card locks after only a few failed attempts to guess the PIN.

A smart card reader (Fig. 1.) attached to the computer reads the smart card. Smart card readers attach to standard personal computer peripheral interfaces such as RS 232, PS/2, Universal Serial Bus (USB), and PCMCIA.

Each smart card vendor provides software that user must install and use to initialize and configure smart card before it can be deployed. User can use the vendor's software to configure PIN, label, inactivity timer, etc.

This section provides description of the Datakey smart card package. It includes:

1. A blank Datakey smart card.
2. A smart card reader with the selected format.
3. The Datakey CIP (Cryptographic Interface Provider) interface software (middleware) version 4.7.

There are the following Datakey smart cards (http://www.datakey.com): Model 330 Smart Card, Model 330u User PIN unblocking enabled Smart Card, Model 330i Smart Card for the Identrus System, Model 330g GSA compatible Smart Card, Model 330m Biometric-enabled Smart Card, Model 330j Java-based Smart Card.

The standard Datakey Model 330 smart card is a file-system card with an embedded chip (the Philips P8WE5032 smart card chip; see Section VI.) that contains Datakey's DKCCOS operating system. The following technical features is specific to the Datakey Model 330 smart card:

- 8-bit CPU (80C51) for performing cryptographic operations.
- DKCCOS smart card operating system (Datakey Cryptographic Card Operating System) in 32 KBytes ROM.
- 32 KBytes EEPROM for secure storage of private and public keys, digital certificates and other data such as passwords, notes, etc. Read cycles: unlimited; write/erase cycles: 100000.
- Supports both on-card key generation and key injection.
- All sensitive operations performed on-card. It means that all private key operations are performed within the smart card's chip: digital signatures and decryption of symmetric encryption keys ("unwrapping").
- Algorithms supported: RSA (key lengths: 512, 1024, 1536, 2048 bits), DSA (key lengths: 512, 1024 bits), Diffie-Hellman (primes from 512 bits to 2048 bits, and exponents from 128 bits to 256 bits), 3 DES and DES. In practice, however, 3 DES and DES are performed in the Datakey CIP software for performance reasons.
- Implements public key functions: RSA and DSA key generation, RSA and DSA for digital signature, RSA and Diffie-Hellman key exchange.
- Validated for FIPS 140-1 Level 2 (Validation Certificate No. 94).
- ISO 7816 (Identification cards - Integrated circuit(s) cards with contacts) compliant.
- PKCS#11 (Public Key Cryptographic Standard 11: Cryptographic Token Interface Standard, commonly called "Cryptoki") and Microsoft CryptoAPI

(Cryptographic Application Programming Interface) compliant.
- Supported operating systems: Windows 98, NT, 2000, XP, 2003.
- Microsoft PC/SC (Personal Computer/Smart Card specification) compliant.
- "Entrust-Ready". It can be used with Entrust applications (Entrust/Authority, Entrust/RA, Entelligence, ICE, Express, SignOn, etc).

Datakey smart cards are compliant with a wide range of smart card readers. Datakey readers are available in serial port, USB port, and PCMCIA versions.

The Datakey CIP interface software which functions as the "middleware" between a user's cryptographic smart card and their computer is designed to enhance the security of applications that support PKCS#11 (versions 1.0 and 2.01) or Microsoft CryptoAPI (version 2.0) standard cryptography.

Popular applications that support this standard include Microsoft applications (Internet Explorer, Outlook, Outlook Express, Word 2002/2003, Excel 2002/2003, PowerPoint 2002/2003…), Entrust applications, Netscape Communicator, etc.

VI. The Philips P8WE5032 Smart Card Chip

The Philips Smart Card Controller P8WE5032 is a single chip secured 8-bit microcontroller. It is specifically designed for secured conditional access applications and transactions in smart card environments or other security applications.

The Philips P8WE5032 chip or integrated circuit (IC) includes (Fig. 5.) [9]:

- 8-bit 80C51 CPU.
- 32 KBytes of ROM.
- 2304 bytes of RAM.
- 32 KBytes of EEPROM.
- Triple-DES co-processor:
  - 3 DES calculation time (including key load) < 200 μs.
  - DES calculation time (including key load) < 100 μs.
- Crypto co-processor Fame X (Fast Accelerator for Modular Exponentiation - eXtended) optimized for public key cryptographic calculations:
  - The major Public Key Cryptosystems like RSA, El'Gamal, DSS, Diffie-Hellmann, Guillou-Quisquater, Fiat-Shamir and elliptic curve are supported.
  - 4032 bits maximum key length for RSA with randomly chosen modulus.
  - < 450 ms typical encryption time of 1024-bit RSA with randomly chosen modulus.
  - 32-bit key length increments.
  - Boolean operations for acceleration of standard, symmetric cipher algorithms.
- True random number generator in hardware, etc.

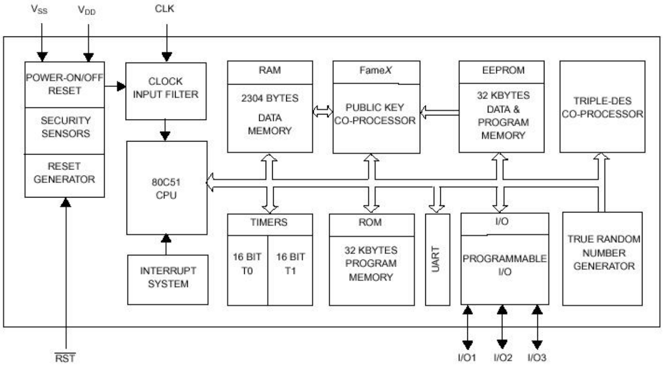

Fig. 5. The Philips P8WE5032 smart card chip diagram [9]

VII. Conclusion

Public key cryptography can be software-based, hardware-based (such as smart card), or a combination of both. For software-based cryptography, cryptographic operations occur in the computers operating system memory. Also, software-based cryptosystems store private keys on local hard disks. Attackers might be able to do memory or hard disk dumps to obtain private keys.

Hardware-based cryptography and key management is more secure than software-based cryptography and key management, because cryptographic operations are performed and private keys stored on the cryptography devices (smart cards), isolated from the operating system, computer memory and applications. On the other hand, cryptography devices store only a limited number of private and public keys and digital certificates, can take a more time to generate keys and perform cryptographic operations, and require additional costs (for smart cards, smart card readers and interface software).

References

[1] D. Spasić, "Electronic Business and PKI System of the Post Serbia", XXXIX Conference "ICEST 2004", Conference Proceedings, pp. 321-324, Bitola, Macedonia, June 2004.

[2] D. Spasić, "The Post Certification Authority", V Conference "Postfest 2004", Conference Proceedings, pp. 673-684, Zlatibor, SCG, May 2004.

[3] "Entrust Authority Security Manager Comprehensive", Entrust Technologies, 2002.

[4] D. Spasić, "Importing Entrust Web Certificate into Cryptoflex Smart Card", IX Conference "JISA 2004", Conference Proceedings (CD-ROM), Herceg Novi, SCG, June 2004.

[5] "Public enterprise of PTT communications "Srbija" Certification Practice Statement", Version 1.0 (Serbian), 8.10.2004. (http://www.cepp.co.yu/ca).

[6] Datakey CIP 4.7 User's Guide, Datakey, 2003.

[7] D. Spasić, "Digital Certificates of the Post Certification Authority on Smart Cards and USB Tokens", XXII Conference "PosTel 2004", Conference Proceedings, pp. 155-164, Beograd, SCG, December 2004.

[8] "Microsoft Releases Beta Version of CryptoAPI 2.0", Microsoft PressPass, 1996.

[9] "Secure 8-bit Smart Card Controller P8WE5032", Revision 1.0, Philips Semiconductors, July 2000.