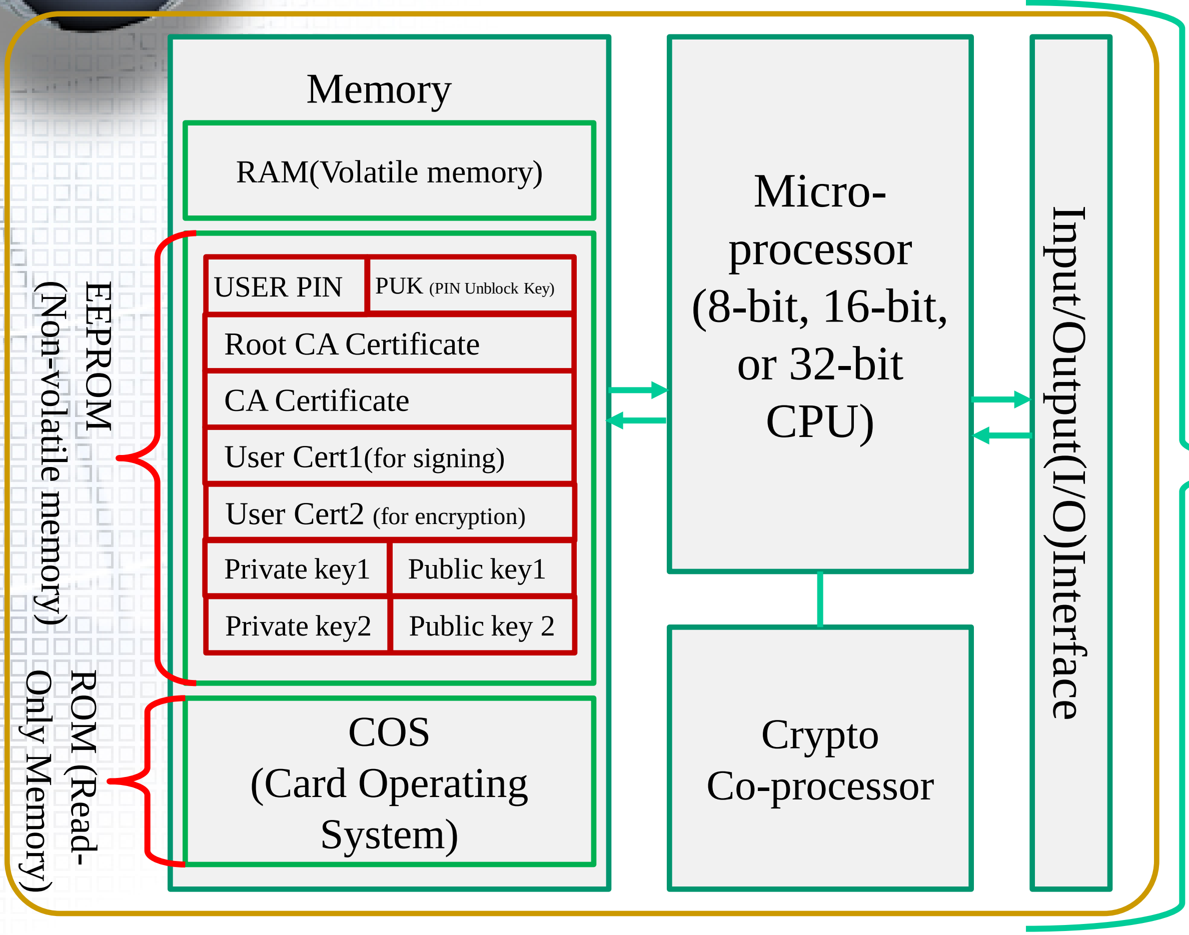
Overview of Smartcard

Wen-Cheng Wang, Ph.D., PMP,
Chief PKI Product Manager
Information and Communication Security Dept.,
Data Communications Business Group,
Chunghwa Telecom Co., Ltd.

April 17, 2015

Inside a smartcard



Memory

RAM(Volatile memory)

EEPROM (Non-volatile memory)

USER PIN

PUK (PIN Unblock Key)

Root CA Certificate

CA Certificate

User Cert1(for signing)

User Cert2 (for encryption)

Private key1

Public key1

Private key2

Public key 2

ROM (Read-Only Memory)

COS (Card Operating System)

Micro-processor (8-bit, 16-bit, or 32-bit CPU)

Crypto Co-processor

Input/Output(I/O)Interface

The IC chip under the metal cover

Internal Architecture of the IC chip

Note: The IC chip of a smartcard is actually a micro-computer with CPU (micro-processor), RAM, ROM, EEPROM and running its own operating system (Card Operating System, COS). Usually, for speeding up the crypto computing, there will be a Crypto Co-Processor inside the IC chip if the smartcard is to be used in PKI.

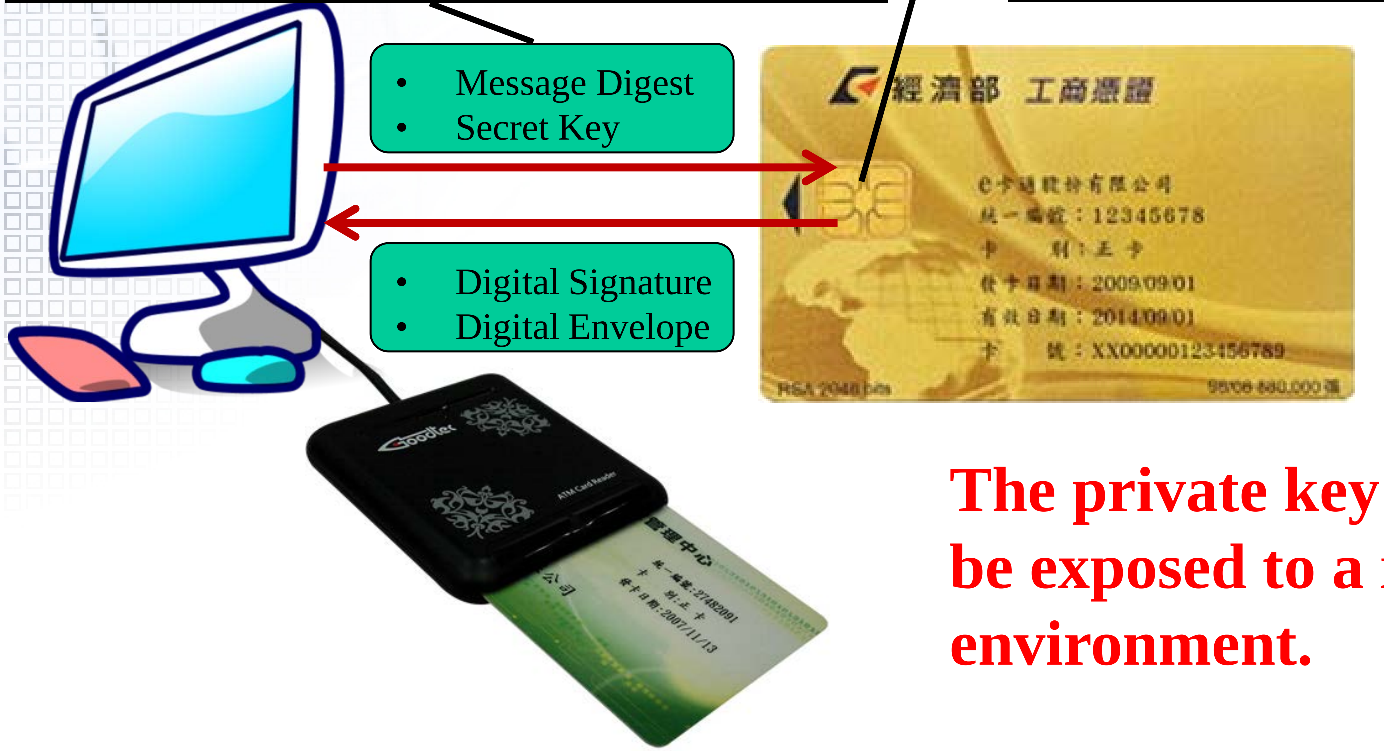
Security of smartcard

In-Chip Crypto Computation

- When the computer need to generate a digital signature or encrypt a digital envelope, the data (Message Digest or Secret Key) will be send, through a smartcard reader, into the chip for crypto computation with the private key

In-Chip Key Generation

- the public-key pair was generated inside the chip
- the private key of the key pair can not be read or exported from the chip and this is enforced by COS

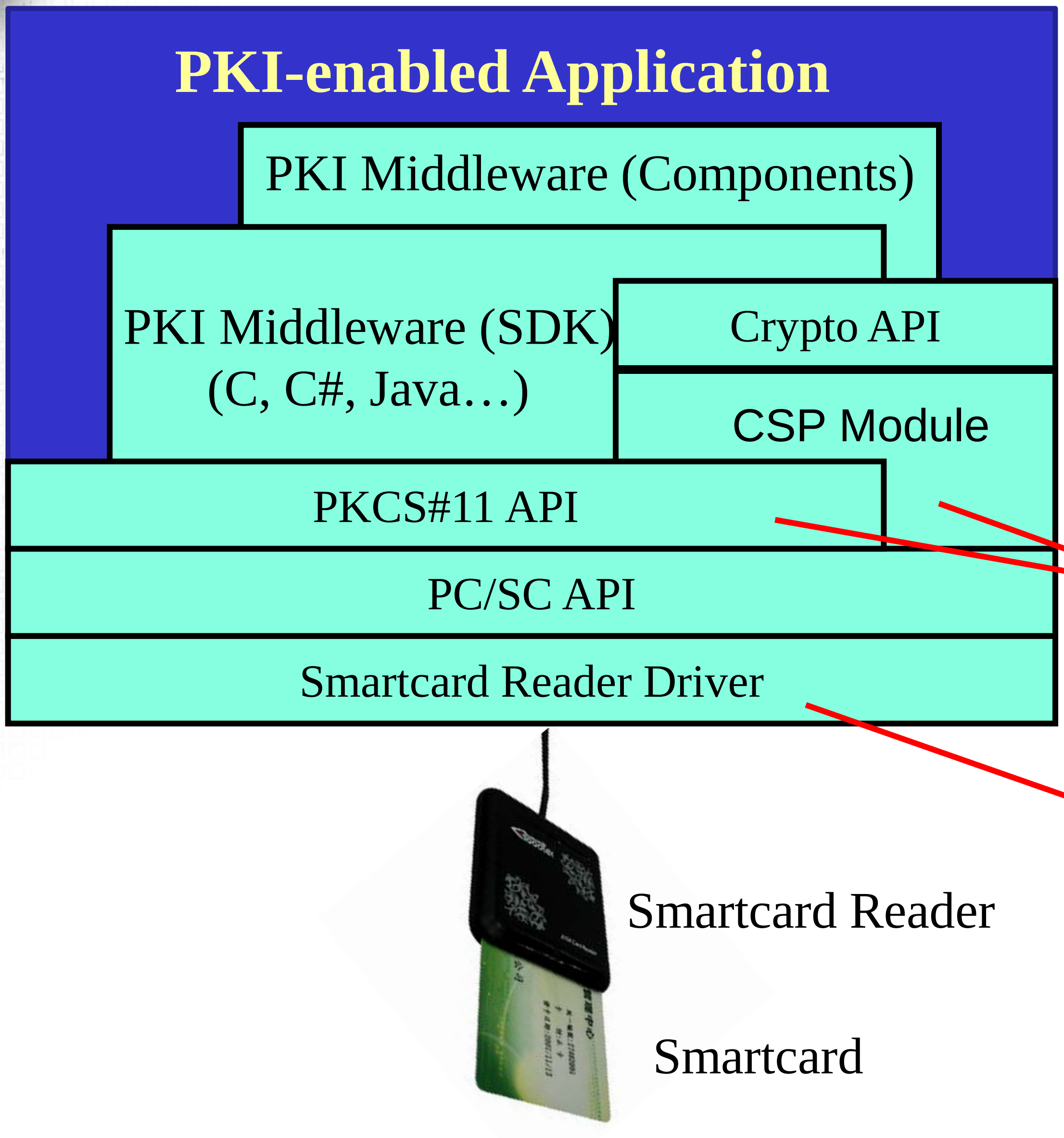


- Message Digest
- Secret Key

- Digital Signature
- Digital Envelope

The private key will never be exposed to a insecure environment.

Smartcard Programming Interface



PKI-enabled Application

PKI Middleware (Components)

PKI Middleware (SDK)
(C, C#, Java…)

Crypto API

CSP Module

PKCS#11 API

PC/SC API

Smartcard Reader Driver

Smartcard Reader

Smartcard

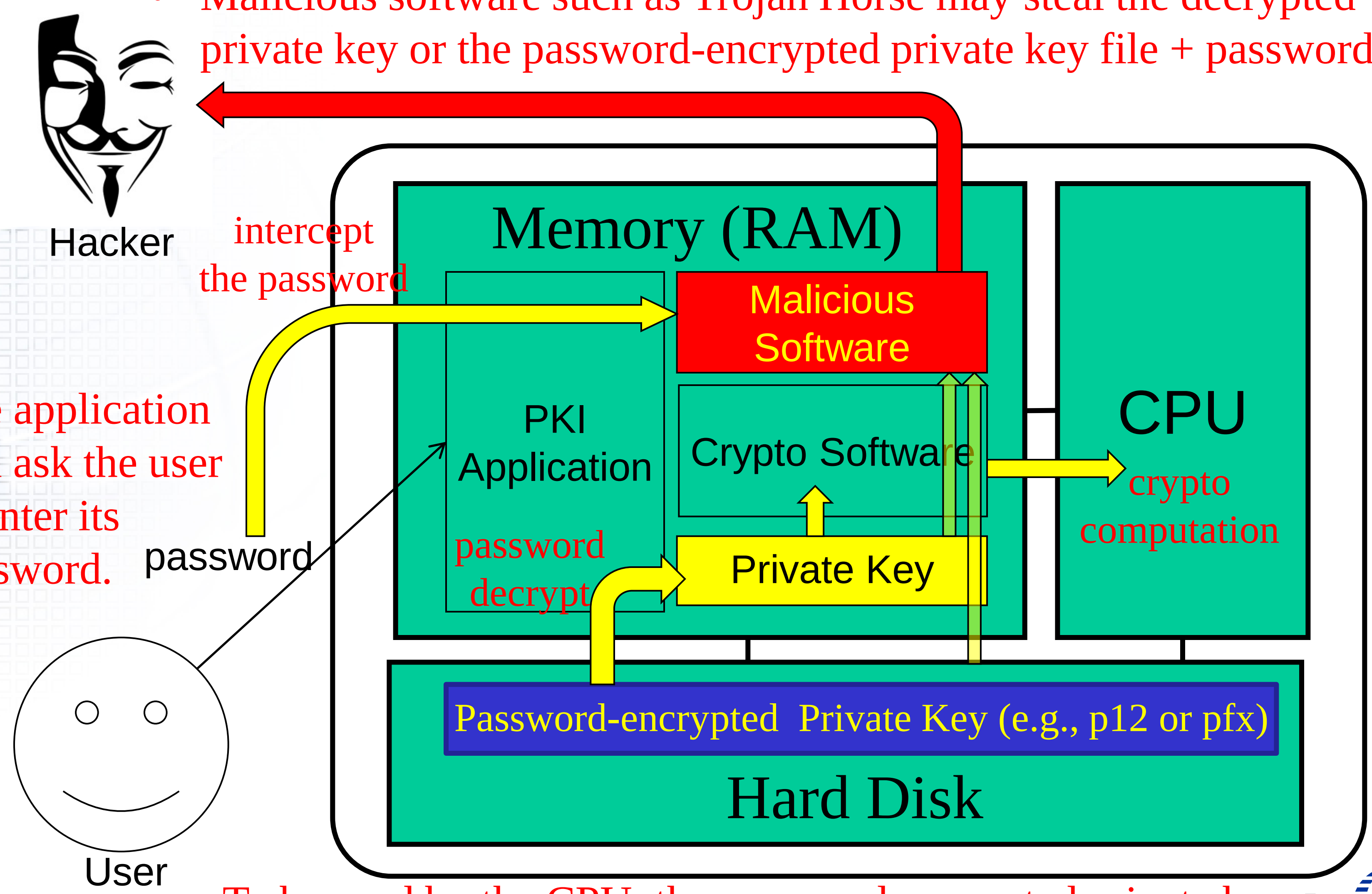
The Crypto API and Crypto Service Provider (CSP) Module is specific to Microsoft Windows.

The PKCS#11 API and CSP Module are specific to the smartcard.

The Driver is specific to the smartcard reader.

Security compared to software key

- Malicious software such as Trojan Horse may steal the decrypted private key or the password-encrypted private key file + password.



- The application will ask the user to enter its password.

- To be used by the CPU, the password-encrypted private key file in the hard disk needs to be decrypted into the memory.

中華電信股份有限公司
Chunghwa Telecom Co., Ltd.

Thank You