Re-Trust meeting - Session 3

d'Annoville Jerome
Project Manager

12/20/06

Session 3 - Trust Model

Trust Model

TPM

Trusted Platform Module (TPM)

- Trusted Computing Group (TCG)
- Create building blocks for trusted hardware
  - Enables less vulnerable software
- Extra chip, the TPM
- Standard cryptographic algorithms
- Strong security
- Exportable
- Operating system agnostic

TPM Functions

- Random number generation
  - key creation
- Key generation
- Crypto RSA
- Hash
- Platform configuration register (PCR)
  - Platform configuration information hashed
- Non volatile storage
  - Attestation Identity Keys (AIKs)
- Management function
  - On/off, reset
- I/O

TPM: Benefits for applications

From a TCG document:

- Confidence in current state
- Trusted download of Software Updates
  - No extra crypto functions
  - Store the root of trust
- Secured Network Communications
- Reliable peripheral identification
- Local Secure Storage
- Personnel Authorization

Trust Model

Smart Card

Smart card – Hardware components

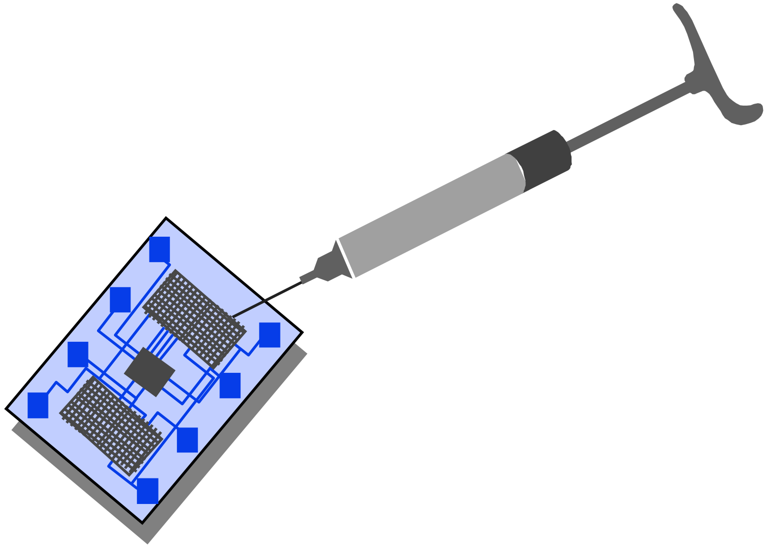
- Processor
- Cryptographic coprocessor
- Memory
  - ROM
  - EEPROM
  - RAM
- I/O in half duplex mode

Non Volatile memories

- ROM (Read Only Memory)
  - ROM is used for the “hard mask” containing the operating system, java virtual machine and APIs (Application Programmer Interfaces)
- EEPROM (Electrically Erasable and Programmable Read Only Memory)
  - EEPROM is used for “softmasks” (extensions to the above features) as well as being similar to a hard disk on the card. It contains the GSM file system and any programs written for the card.

ROM

- Operating System
  - I/O protocol
  - Chip handler
  - External commands
  - Memory management
  - Authentication algorithms
- Between 6kb and 48kb



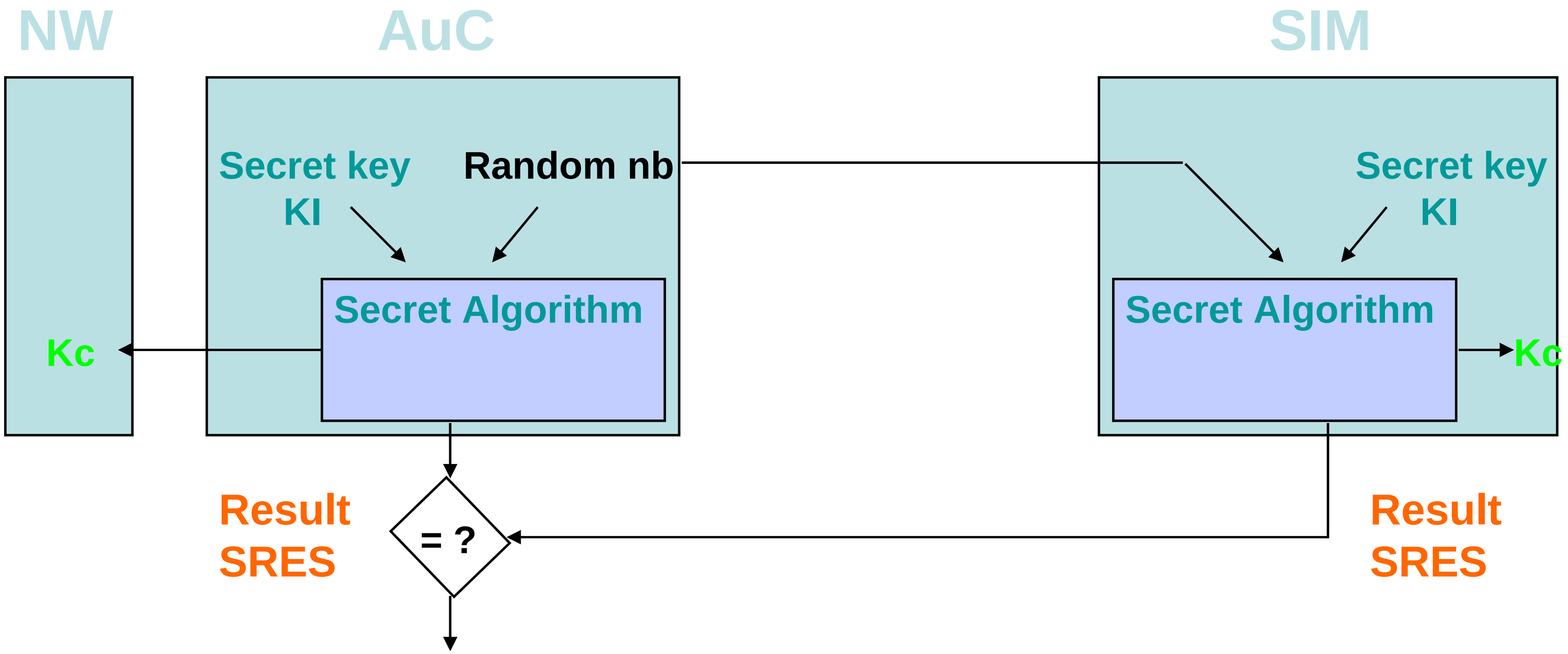
EEPROM

- Application memory
- Specific file architecture (perhaps GSM)
- Data information
- Softmask
- OS Data
- Presently up to 64kb

More on Smart card

- Communication model
  - Application Protocol Data Unit (APDU)
  - ISO 7816
- Operating System
  - File system centric
- File system
  - Master File, Dedicated File, Elementary File
  - Elementary File
    - Transparent file
    - Linear fixed
    - Linear variable
    - Cyclic fixed

Secure the usage of Network



- Yes = Subscriber recognized by the network.
  Incoming/outgoing call possible
- No = Subscriber rejected by the network.
  Incoming/outgoing call impossible

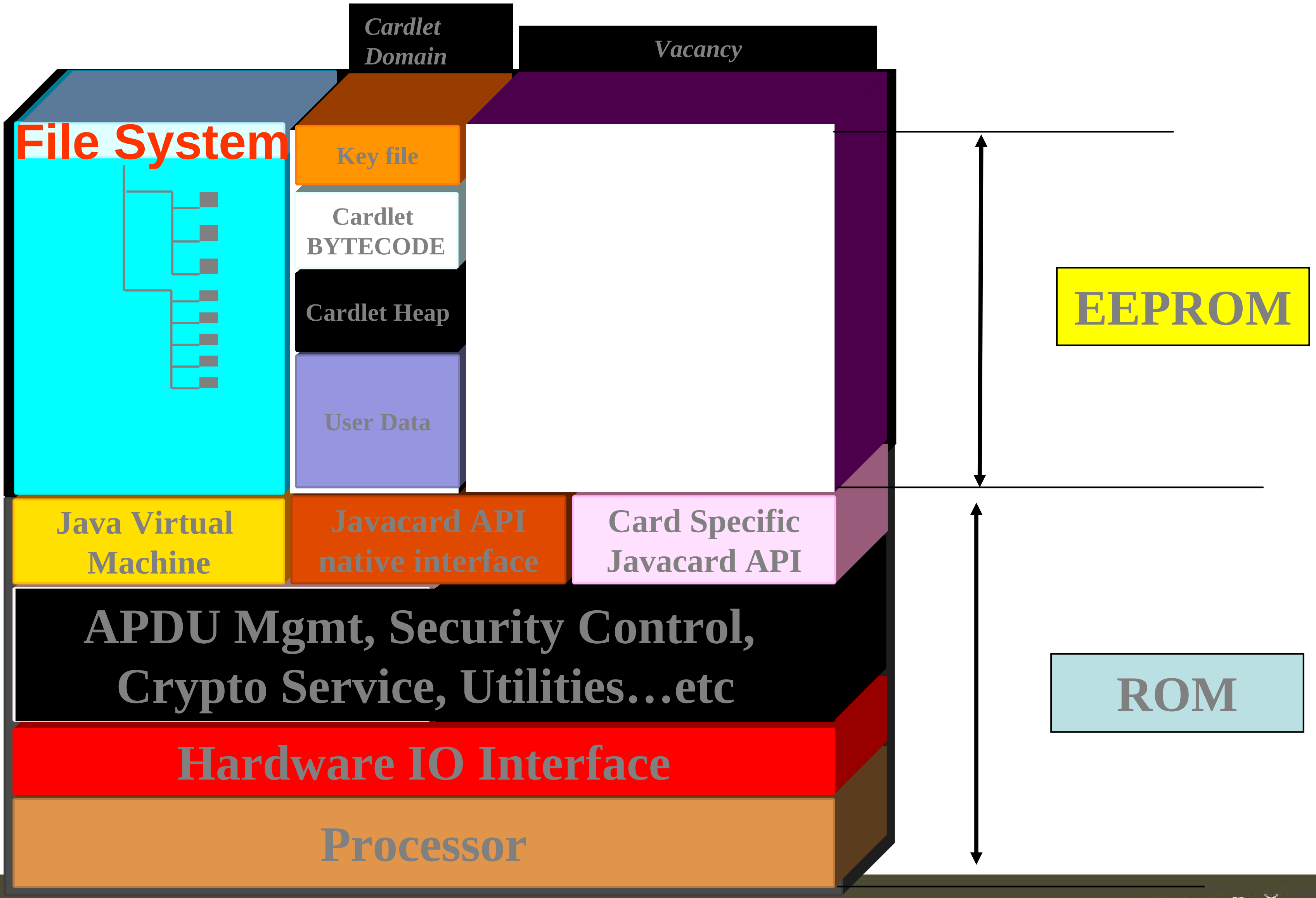
Card types

- Mono application
  - Advantage
    - lower price
  - Disadvantage
    - card features are fixed
    - proprietary implementation
    - non-portable
- Multi application
  - Java card
  - Multos

Java Card Approach

- Application should be independence to:
  - chip / card / platform
- Multiple applications on one card
- …and all the benefits from Java…...
- Card issuer & 3rd party developer are able to program the card with desired features
- applications are ‘downloadable’ after the card has been issued.
- Needs built-in security features between different applications on the same card.

Javacard Architecture



Cardlet Domain

Vacancy

File System

Key file

Cardlet BYTECODE

Cardlet Heap

User Data

EEPROM

Java Virtual Machine

Javacard API native interface

Card Specific Javacard API

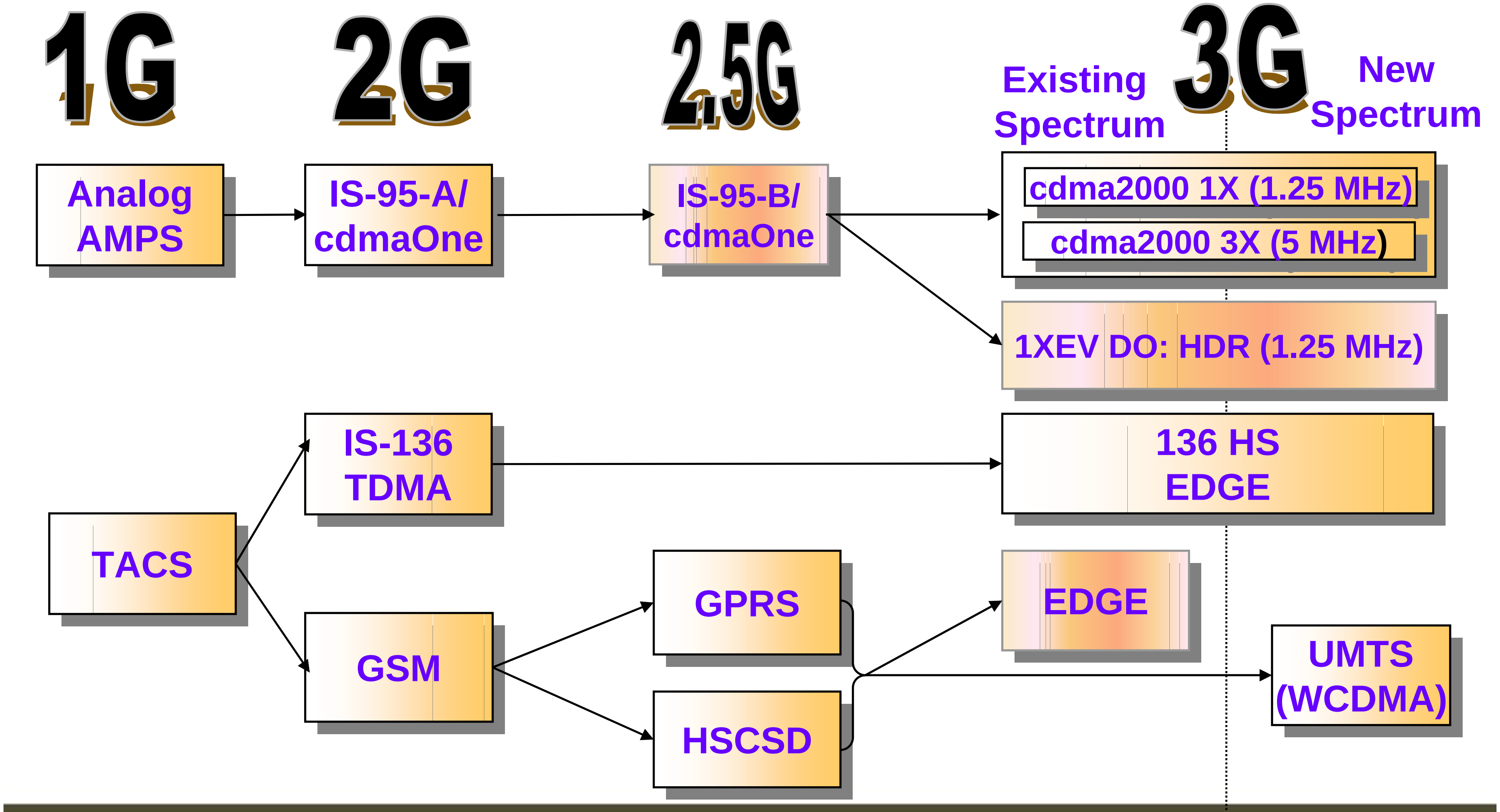
APDU Mgmt, Security Control, Crypto Service, Utilities…etc

Hardware IO Interface

Processor

ROM

Wireless Standards Evolution to 3G



Smart card use in traditional Wireless networks

- **SIM** ***User Authentication by the server only: A3/A8***
  - GSM/PTS **2 G**
  - GPRS **2.5 G**
  - EDGE **2.75G**

- **UICC/USIM** ***Mutual Authentication: AKA - Milenage***
  - WCDMA – TD SCDMA **3 G**
  - HSDPA **3.5 G**

- **R-UIM** ***User Authentication by the server only: Cave***
  - CDMA / EvDo

Technical Synthesis Of Wireless

Traditional

Emerging

4G ?

	2G	2.5G	2.75G	3G	3.5G	802. 11b	802. 11g	802. 11a	802. 16d	802. 16e
~ Rate **Kb/s**	9.6	56	200	384	9000	11000	54000	54000	75000	15000
MaxRange **Km**	0.1 - 1	0.1 - 1	0.1 - 1	0.1 - 1	0.1 - 1	0.1	0.1	0.08	50	5
Spectrum **GHz**	0.9 1.8	0.9 1.8	0.9 1.8	2.1	2.1	2.4	2.4	5	2 11	6

- □ Faster
- □ Bigger range

Stronger need for authentication

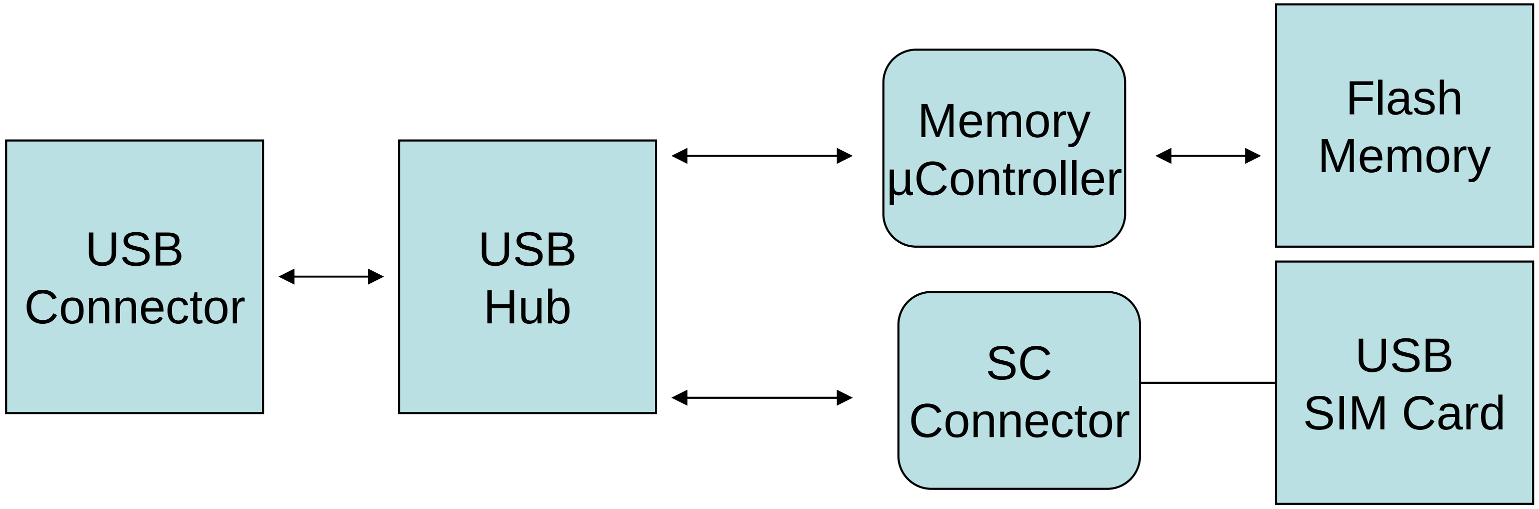
Trust Model

Dongle – USB Token

Features

- Work on any PC without installation
- Device Login Screen to authenticate the user
- Automatically loaded specific GUI to start the application
- VoIP client
- Remote administration

Hardware architecture



Functionnal Architecture

- USB SIM Card:
  - SIM Java Card:
    - SIM, USIM, OTP, TTF, ISIM application
    - GSM 3G and EAP SIM/ AKA authentication scheme.
    - No need to install a card driver (ICCD)
  - Memory access protected by PIN, contains:
    - User settings for the different applications
    - User private and secured data
- Flash Memory:
  - Application launcher
  - Various applications
  - Data

Smart Card & usual PC Applications

PKCS#11 & MS Crypto API

Purpose

- Sign email
- Encrypt a message
- Receive signed and encrypted email messages
- Smart Card Logon
- SSL
- …

Smart card applications environment

- Application
- Smart card library
- Middleware
- Driver

Smart card applications environment

- Application
- Smart card library
  - RSA PKCS#11 (Cryptoki)
  - MS Crypto API (CAPI)
- Middleware
  - PC/SC - Windows
  - pcsc-lite - Linux
- Driver provided by reader manufacturer

Windows Crypto API

- CryptoAPI has been designed by Microsoft
- Native Windows applications use the Crypto API interface
  - IE
  - MS Office

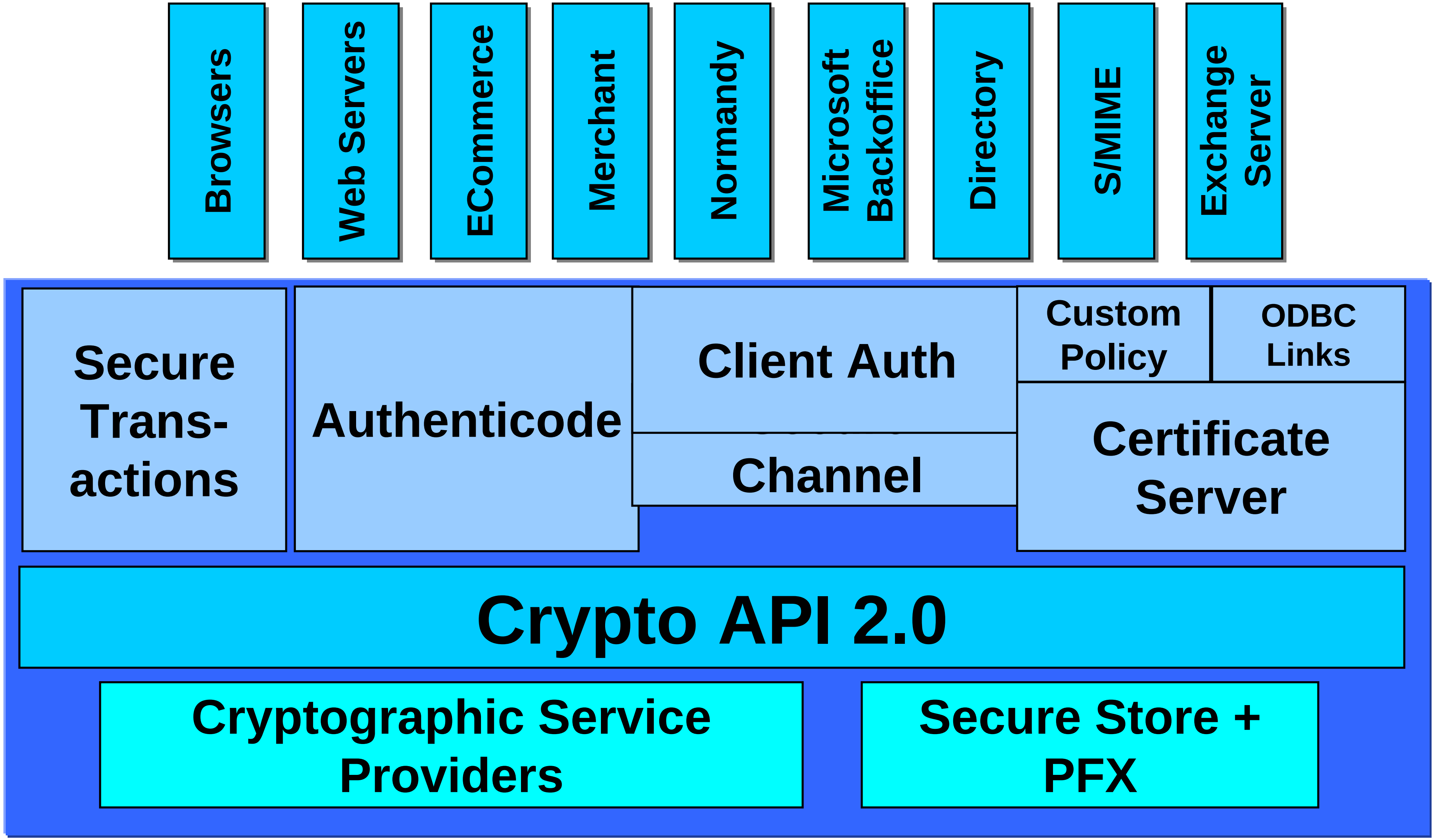
- It helps application developers to add cryptography to Win32 applications
- It consists of a set of functions to perform cryptographic operations
- With CAPI/CSP
  - No extra application required
  - Access to card is automatic

- Small MS guide (Microsoft Excel 2002)
  - Get a digital certificate
  - Install the certificate (Add)
  - Save As (must be a book)

CSP

- The cryptographic operations are performed by separate modules, called cryptographic service providers (CSPs).
- One of these, Microsoft's RSA Base Provider, comes with the operating system
- CSPs differ from each other, with some providing stronger algorithms while others contain hardware such as smartcards

CryptoAPI Architecture



Browsers

Web Servers

ECommerce

Merchant

Normandy

Microsoft Backoffice

Directory

S/MIME

Exchange Server

Secure Trans-actions

Authenticode

Client Auth

Channel

Custom Policy

ODBC Links

Certificate Server

Crypto API 2.0

Cryptographic Service Providers

Secure Store + PFX

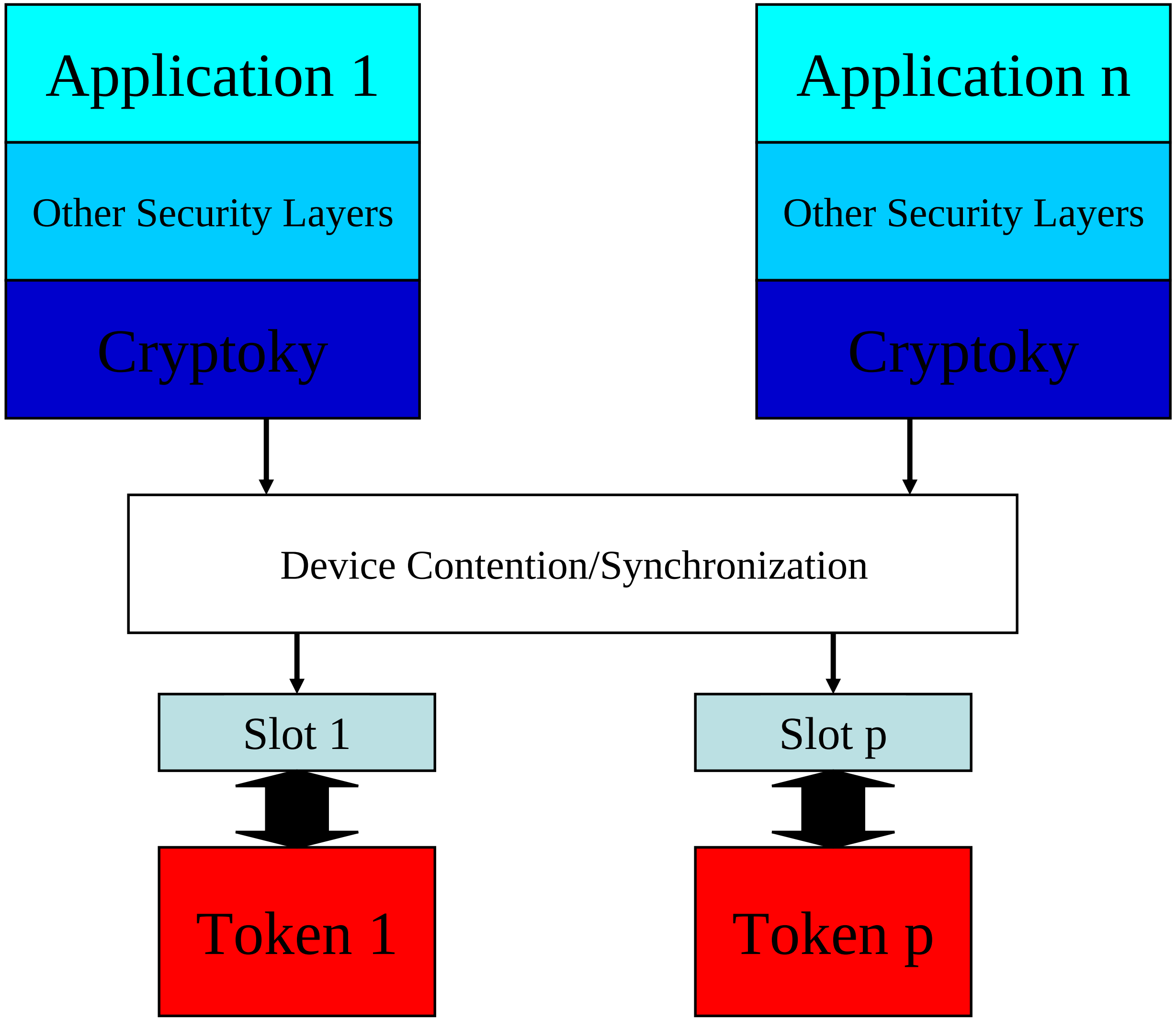
PKCS#11

- Standard interface
- Available on both MS Windows & Linux
- Firefox, Thunderbird

PKCS#11 (2)

- PKCS#11 is a standard issued by RSA Data Security
- It specifies an API, called Cryptoki, to devices which
  - hold cryptographic information
  - perform cryptographic functions
- Cryptoki follows a simple object-based approach, addressing the goals of
  - technology independence (any kind of device)
  - resource sharing (multiple applications accessing multiple devices)
  - presenting to applications a common, logical view of the cryptographic token.

PKCS#11 Architecture


Application 1
Other Security Layers
Cryptoky
Application n
Other Security Layers
Cryptoky
Device Contention/Synchronization
Slot 1
Slot p
Token 1
Token p