The UICC
The Security Platform for Value Added Services

Dr. Klaus Vedder
Chairman ETSI TC SCP

4th ETSI Security WS
Sophia Antipolis, France
13-14 January 2009
World Class Standards

The Most Successful Smart Card…

SIM and UICC: driving smart card technology
World Class Standards

Some Facts

Interesting SIM facts
With the amount of SIMs that were delivered in 2007 worldwide alone you could...

... stack them to a tower 1976 km high!

More interesting SIM facts
With the amount of SIMs that have ever been delivered you could...

... place them next to each other and go 20 times around the world!
ETSI TC SCP, the Smart Card Committee

- 21 Years of Dedication and Real-life Experience
  - Founded in March 2000 as the successor of SMG9, the people which specified the most successful smart card application ever with over 3 billion subscribers using one or more of the 13 billion SIMs, USIMs and R-UIMs delivered to the market.

- The Mission
  - Create a series of specifications for a Smart Card Platform, based on real-life (outside) requirements, on which other bodies can base their system specific applications to achieve compatibility between all applications resident on the smart card.
ETSI TC SCP: 21 Years of Dedication

SCP Plenary
Chairman Klaus Vedder, G&D
Vice-Chair Nigel Barnes, RIM
Vice-Chair Tim Evans, Vodafone UK

SCP Requirement WG
Chairman Ilario Macchi, TIM
Vice-Chair Heiko Kruse, Sagem Orga
Vice-Chair, Denis Praca, Gemalto

SCP Technical WG
Chairman Paul Jolivet, LG Electron.
Vice-Chair Sebastian Hans, Sun Microsystems

SCP Testing WG
Chairman Andreas Bertling, Comprion
Vice-Chair Christophe Dubois, Gemalto
The Core Specification

- **TS 102 221** *Physical and logical characteristics of the card / terminal interface*
  - the core specification which provides a multi-application platform with logical channels for smart cards - based on this platform a smart card application can be defined for any system
  - specifies the lower layers of a smart card including the electrical and mechanical interface, the logical structure, the basic commands and the intrinsic security system
  
  Test specification published as TS 102 230

- **ETSI SCP** has published over thirty specifications covering the full range from administrative commands to APIs, browsers and test specifications
  - all can be downloaded free of charge from the ETSI website
World Class Standards

The Chip

Co-processor

Operating memory

NPU
RAM

Vcc
GND

CPU
EEPROM

Non-volatile memory

I/O

CLK
RST

Operating System

Operating System

ROM
Smart Card Chip Evolution

1990  8 Bit CPU
  7 kB ROM
  3 kB EEPROM
  128 Byte RAM

2007  32 Bit CPU
  500 kB ROM
  512kB EEPROM
  16kB RAM
  or
  400 kB Flash memory
  In addition: 1GB Flash

2009  Single chip MB solutions

- CPU, RAM, ROM, EEPROM, Crypto-unit on a single piece of silicon
- structure ~1990: 1,5 µm; today: 0,09 µm
- metallised surface, sensors for Low Voltage, Frequency, Passivation Layer, Light, …
- evaluation of HW and SW against Common Criteria (CC)
Infineon Technologies SLE66CX322P with Active Shield against state of the art physical attacks: Top view (left) and underlying circuits (right)
Module and Contacts

Standard module card cross section

- ISO contacts (Cu/Ni/Au)
- FR4 substrate
- Active chip side
- Hotmelt
- Encapsulation
- Chip
- Electrical chip connection via bond wire
- Chip adhesive
- Card body

Today's layout

- VCC
- GND
- RST
- VPP
- CLK
- I/O
- AUX1
- AUX2

Standardised new layout

- VCC
- GND
- RST
- SWP
- CLK
- I/O
- USB
World Class Standards

Analysis of an OS: Looking at the Commands

Comp 128-1: 8 rounds as executed by OS 1

Comp 128-1: 2 rounds shown as executed by OS 2, which is about 5 times slower

For some recent attacks on smart cards see Springer LNCS 5189, Smart Card Research and Advanced Applications, CARDIS 2008 hosted by the Smart Card Centre, University of London

NOTE: Comp 128-1 was successfully attacked in 1998 by a chosen plaintext-ciphertext attack, a black box attack which did not utilise any hardware or software property of the SIM.
SIM Security - a Function of Hardware and Software

Calculating the secret key from hundreds of power consumption measurements using statistical methods (DPA attacks)

Correlation on output S-box with usage of the right key

Straightforward implementation  Implementation with countermeasures
The UICC - the Multi-application Platform

The UICC consists of (all) application independent functions and features:

- clear separation of lower layers and applications
- up to 20 logical channels to access applications in parallel

Firewalls between applications provided by smart card (USIM) supplier

Specified by TC SCP

a network access technology agnostic platform
SCP Releases 7 & 8: Milestones for the UICC

The UICC has undergone a major revamp in Rel-7 (closed) and Rel-8

- **New interfaces**
  - IC_USB interface for high-speed contact communication (TS 102 600)
  - SWP (TS 102 613) and HCI (TS 102 622)
    Single Wire Protocol and Host Controller Interface specifications for contactless communication (NFC)

- **Support for large memory**
  - part of the IC_USB specification

- **A jump into the IP world**
  - IP Connectivity for the UICC (TS 102 483)
  - remote management over IP
  - migration of the toolkit framework over IP

- **API for the Smart Card Web Server (TS 102 588)**
World Class Standards

High Speed

- Current UICC-Terminal interface protocol (T=0) based on IS 7816 is not appropriate for graphical user interface, bulk data and the Internet

- IC_USB – the new high speed interface
  - Interchip (IC) USB is a modification of USB 2.0 on the physical layer for direct (non-pluggable) connections between chips; higher layers are not affected and run transparently without modifications on IC_USB.
  - nominal speed of 12 megabit per second
  - use of existing contact layout (C4 and C8)
  - IC_USB is a first step in getting rid off smart card specific protocols and turning the UICC into a real Internet platform

This will transform the SIM into a real Internet device and also allow the efficient use of high capacity SIMs in the MB and GB range
The “Contactless” USIM

- **Mobile Phones**
  - high penetration
  - personal device

- **Contactless Cards**
  - ease-of-use, convenient
  - large and growing infrastructure

The Single Wire Protocol (SWP) is the standardised I/F between (U)SIM and the Contactless Front End (CLF)

NFC chip for contactless transmission

Contactless applications on USIM (or mobile)

Mobile Phone CPU

4th ETSI Security WS

Secure Element (SE)
A New Contactless World

- The contactless interface for the (U)SIM will create a wealth of new opportunities
  - mobile phone works like a contactless card for payment, ticketing, access control, ....
  - mobile phone works as a card reader for the (U)SIM

- Management of Applications
  - secure environment on the (U)SIM dedicated to different service providers such as banks, public transport companies, ....
  - encapsulated storage areas (Trustsectors®) on the (U)SIM for secure execution of applications
  - OTA administration such as activation/de-activation or personalisation of the individual areas (Trustsectors®) via a Trusted Third Party (TTP)
  - TTP can act as a trusted “estate agent” and a broker for the memory of the (U)SIM card provided by the operator - (U)SIM becomes a piece of real estate
NFC Framework

Application Issuers
- Transport
- Payment
- Loyalty
- Events
- Governments
- Corporate ID

Mobile Network Operators
- USIM - management
- application downloads

Over-The-Air Services
- USIM / SE - management
- application downloads

Trusted Service Manager

Contactless applications on USIM (or mobile)

Mobile Phone CPU

NFC

Payment
- Transport
- Events
- Physical Access
- Identity Management

World Class Standards
Everybody is looking at Mobile NFC services with great interest
- all think NFC services and related revenue should be mostly theirs
- this created competition and this competition made its way deep down to the technical level and to the standardisation committees

Who is going to host the NFC services?
- mostly the battle is about contactless card emulation, which addresses transport/event ticketing and payment
- the contactless card-emulation needs a secure environment and it is all about re-using existing secure devices or deploying new ones
  - in all GSM/UMTS phones, the (U)SIM application is hosted on a secure device, the UICC
  - secure MMC, secure SD removable cards can alternatively be used
  - mobile phones may have secure devices built-in
- whoever owns the secure device has a key role
World Class Standards

Why the SIM is the Preferred Secure Element

Standardized device
- Critical success factor for global roll-out
- Globally deployed

Service delivery platform
- Storage and execution of several independent NFC apps.
- Other (non NFC) types of services

Security
- Tamper-resistant security device
- Secure loading and application management

Remote management
- OTA application management
- Flexible application download, personalization and lifecycle management

Portability
- Easy migration from one device to another
- Separation of device (selected by user) and service (e.g. by bank)

“Emergency mode”
- Power supply can be drawn from the contact-less card reader
- Enables low battery functionality

Giesecke & Devrient

4th ETSI Security WS
Principle of HCI

- The Host Controller Interface (HCI) provides the basics for high-level communication between the CLF and other hosts
  - use of hosts and gates
  - set of commands/responses
  - set of events
  - toolbox for CLF & Host configuration.

- In the ETSI context, the UICC is the only host defined in addition to the Host Controller/CLF. However, TS 102 622 includes core mechanisms that allow for extensions of the framework:
  - definition of new hosts & gates
  - definition of new commands
  - definition of new events

- ETSI’s HCI provides a basis for re-use and extension
Smart Card Web Server – SIM service portal

Concept
- (U)SIM is the secure interface to the Internet
- Web Server application on (U)SIM utilises execution environment of mobile services
- easy to use GUI for services - Web look and feel of information loaded on the (U)SIM
- the SIM portal in the hand of the subscriber
- one-button-access to the SCWS from the handset

Service categories
- hotline information services – former STK IOD services
- Phonebook/Agenda
- Java applications such as OTP
- 3rd party applications such as Google maps, Instant messenger
- access to services based on new technologies such as NFC
- filebrowser of SIM content (restricted access or free access)
- and a use case: Web Pages with FAQ to save calls to the Operator
Smart Card Web Server (SCWS)

- The device’s Internet browser accesses a WEB server located on the UICC through the high-speed interface.

Example: Protocol stack on terminal

- Internet Browser
- Socket API
- TCP/IP
- Interface Layer to IP (e.g. Ethernet Emulation Model)
- MMC 4.1 or USB 2.0 Full speed
- Connection to UICC

(U)SIM
- exclusive / concurrent operation
- IC_USB HW interface

Terminal
- MMC Host or USB Host / OTG
- 8 pin connector

WEB Services
- SCWS File System
- Configuration
- Security Layer (ACP)
World Class Standards

Machine to Machine (M2M)

- **Extended data retention time**
  - Long EEPROM life cycle
- **Quick response time**
  - HW
- **Fixed on board**
  - New form factor?
  - Packaging
  - High humidity resistant
- **New temperature range**
  - High vibration resistant
- **Dynamic provisioning**
  - Life time mngt.
  - Sales channel
  - Logistc
- **Universal profile**
  - OTA updatable (algorithms, keys, ...)
- **Network mngt.**
  - Applications
  - DRM Navigation map usage
  - Preventive Maintenance
  - Telematics
  - Meter reading

4th ETSI Security WS
M2M Status

- Requirements agreed as part of Release 8
- New form factor (MFF) required?
Dr. Klaus Vedder

Group Senior Vice President and Head of Telecommunications

Giesecke & Devrient GmbH
Prinzregentenstr. 159
81607 Munich
Germany

klaus.vedder@gi-de.com
Next SCP Plenary Meeting: Next week here at ETSI

Visit the ETSI SCP website for details on meetings, documents, ...

http://portal.etsi.org/scp/summary.asp