The UICC

Recent Work of SCP and Related Security Aspects

Dr. Klaus Vedder
Chairman ETSI TC SCP

5th ETSI Security WS
Sophia Antipolis, France
20-22 January 2010
SIMs in 2009

Interesting SIM facts
With the amount of SIMs that were delivered in 2009 worldwide alone you could ...

... fill **2165 soccer fields**!

And last but not least:
The amount of SIMs ever delivered corresponds to the weight of **413 blue whales**!
The Smart Card Market

From 2004 to 2008, the microprocessor market has grown at an annual rate of approx. 30%.

CAGR 04-08
- 25%
- 23%
- 32%

CAGR 04-09
- Telecom 26%

Source: Eurosmart (04-08)
ETSI TC Smart Card Platform

- **22 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 4 billion subscribers using one or more of the over 15 billion SIMs, USIMs, R-UIMs, ... delivered to the market.

- **SCP**
  - Create a series of specifications for a *Smart Card Platform* (for telecommunications) on which other bodies can base their system specific applications to achieve compatibility between all applications resident on the smart card.
World Class Standards

Structure and Officials

SCP Plenary
Chairman: Klaus Vedder, G&D
Vice Chairman: Tim Evans, Vodafone
Vice Chairman: Denis Praca, Gemalto

SCP Requirement WG
Chairman: Colin Hamling, Telefónica
Vice Chairman: Heiko Kruse, Sagem Orga
Vice Chairman: Denis Praca, Gemalto

SCP Technical WG
Chairman: Paul Jolivet, LG
Vice Chairman: Sebastian Hans, Sun Microsystems

SCP Testing WG
Chairman: Andreas Bertling, Comprion
Vice Chairman: Christophe Dubois, Gemalto
Description

- **SCP REQ**
  - Working Group SCP REQ is responsible for developing the requirements for the Smart Card Platform. Input is received from ETSI members as well as 3GPP, 3GPP2, GlobalPlatform, GSMA (NFC Project, ...), GSMA SCaG, NFC Forum, OMA, WiMAX Forum, ...

- **SCP TEC**
  - Working Group SCP TEC is responsible for the technical realisation of the requirements developed by SCP REQ and approved by SCP plenary in the form of Technical Specifications/Reports and Change Requests to them

- **SCP TEST**
  - Working Group SCP TEST is responsible for the development of test specifications for deliverables produced by SCP TEC and approved by SCP plenary
The Specifications

ETSI SCP has published nearly forty specifications on smart cards covering the full range from administrative commands to APIs, browsers, Internet connectivity, new interfaces for high speed and NFC as well as test specifications

- all can be downloaded free of charge from the ETSI website

The specifications are application agnostic and can be used as a (secure) platform for applications outside the world of telecommunications

The Core Specification

- TS 102 221 *Physical and logical characteristics of the card / terminal interface*
  - provides a multi-application platform with logical channels for smart cards
  - 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
The UICC - the Multi-application Platform

The UICC is *the* smart card platform providing a clear separation of lower layers and applications residing on it.

- USIM
- SIM
- (U)SAT
- Phonebook
- Public Transport
- Payment
- eHealth
- ID

Firewalls between applications provided by smart card supplier

Specified by TC SCP

UICC a technology agnostic platform

World Class Standards
The UICC

Complete revamp of the UICC, the smart card platform, in the last three years with new interfaces and shift to become part of the Internet world while retaining the security attributes

- High Speed Interface (IC_USB)
- NFC interface (SWP)
- Internet connectivity
- Smart Card Web Server
- Secure Channel
- Larger memory
- ......
World Class Standards

Convergence of security based applications

Authentication
Authenticates subscriber against network (and vice versa)

Service Platform
SIM as a platform for additional services
- SMS services
- Phonebook
- Mobile banking

Multi-Application
Near Field Communication
- Payment
- Ticketing
- Access control

IP Network Node
- Smart Card Web Server
- Machine-to-Machine
- Secure storage
- Digital identity
Contactless Mobile Terminals

The Mobile Terminal works like a contactless card for payment, personal banking, ticketing, access control, … and as a card reader for the applications on the Secure Element.

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

NFC chip for contactless transmission.

Secure Element (SE)
NFC Framework

World Class Standards

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

Mobile Phone CPU

Contactless applications on USIM (or mobile)

Payment
- Transport
- Events
- Physical Access
- Identity Management

Giesecke & Devrient

5th ETSI Security WS
Mobile NFC Services: a Big Pie but Many Shares

- Where will the NFC services be residing?
  - 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 μSD cards provide another solution
    - mobile phones may have secure devices built-in
  - whoever owns the secure device has a key role

- Management the applications
  - secure environment on the UICC dedicated to different service providers such as banks, public transport companies, ....
  - encapsulated storage areas (Trustsectors®) on the UICC 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 UICC card provided by the operator - UICC becomes a piece of real estate
The UICC (SIM) in an NFC Environment

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

ISO/IEC 14443 A
ISO/IEC 14443 B
FeliCa/MIFARE®

Giesecke & Devrient
5th ETSI Security WS
Smart Card Web Server – SIM service portal

Concept
- UICC 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 UICC
- 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
- filebowser of SIM content (restricted access or free access)
- Web Pages with FAQ to save calls to the Operator
World Class Standards

Tomorrow in my Mobile Wallet

Giesecke & Devrient

5th ETSI Security WS
Advancing Tomorrow’s Solution

TC SCP will participate in a joint initiative of GlobalPlatform, the GSMA and EMVCo (supported by AFOM, ETSI, EPC and the SIMalliance) aiming at delivering a new certification process for smart cards which will enable **certified** applications to co-exist on a **certified** UICC alongside other applications with less stringent requirements.

… “When fully developed and operational, these schemes will work together to ensure that any certified payment application will work with any certified UICC platform, reducing the incidence of certification failures when new application / platform combinations are subsequently added for testing. The result will be significantly reduced testing and development costs and a faster time to market. Additionally, no further certifications will be necessary when loading applications with less stringent security requirements onto new UICC platforms.”… (from the press release of 17 November 2009)

This topic has a huge significance for the deployment of applications and the advancement of the NFC ecosystem.
World Class Standards

Machine-to-Machine (M2M)

A sensor inside a machine

Over a network

Into a business system

SIMs in different form factors

Network

- Smart metering
- Vending machines
- Security
- Fleet management
- Telematics

- Energy suppliers
- Automotive industry
- Environmental monitoring
- Administration
- Reports

Giesecke & Devrient

5th ETSI Security WS
World Class Standards

M2M Requirements and Challenges

- **Extended data retention time**
  - Long EEPROM life cycle

- **Quick response time**
  - New temperature range

- **Integrated into modem**
  - New form factors
  - High vibration resistant
  - High humidity resistant

- **Dynamic provisioning**
  - Life time mngt.
  - Sales channel

- **Universal profile**
  - OTA management (subscriptions, algorithms, keys, …)

- **Fleet mngt.**
  - Preventive Maintenance
  - Telematics
  - Meter reading

- **Logistics**

- **Applications**
  - DRM Navigation map usage

Giesecke & Devrient

5th ETSI Security WS
M2M Status of Standardisation

- Requirements agreed as part of Release 8 (see TS 102 412)
- New M2M Form Factors (MFF) to be agreed in March by SCP Plenary
  - MFF1: socketable 8 pin solution
  - MFF2: SON8 (denoted by QFN8 below)

For details see the to-be-approved Technical Specification TS 102 671 (draft)
Work Completed

- UICC-Terminal Applicative Protocols over USB. Requirements for service migration to the USB interface
- Realisation of use cases and requirements for RFID services based on UICC requirements
- Classification and testing of UICCs in terminals with “reduced” capabilities such as M2M modems
- Remote management of the UICC over IP instead of using APDUs
- SCWS API to allow applications on the UICC to interact with the user in an ongoing web session
- Three test specifications for the Single Wire Protocol (SWP) interface and the Host Controller Interface (HCI)
  - The remaining test specification on the terminal features of the HCI is expected to be finalised by March this year
SCP: Current and Future Work

- Contactless API for the Host Controller Interface (HCI) to support NFC applications
- CAT (Card Application Toolkit) access on Modem interface. Extension of CAT to clients interfacing with the modem
- Confidential Applications: allows 3rd party applications to be loaded and executed within a secure and private environment
- API for secure channels
  - Definition of an API for the secure channel for the APDU protocol based on the secure channel API requirements added in TS 102 240. This additional API will extend the “UICC API for Java Card™” defined in TS 102 241
- UICC in notebooks
  - Technical report of specific aspects and requirements related to the use of a UICC in a notebook
- AT Commands for UICC interaction
  - Description of AT commands that can be issued to a terminal and that are specifically for use with the UICC to better facilitate communication between a UICC and applications on a laptop via a built in modem
- Support of P2P mode in contactless interface specifications
  - Specification of requirements and use cases for Peer to Peer contactless mode support in the UICC
  - To facilitate communication between applications on different UICCs
- UICC next generation Run Time Environment (RTE) to support multi-tasking of the UICC with more than one interface
- Test specifications to be realised this year
  - Test specifications for the USB interface
  - Evolution the test specification for UICC API for Java Card™ to Rel-7
  - Smart Card Web Server API
Dr. Klaus Vedder

Group Senior Vice President and Head of Telecommunications

Giesecke & Devrient GmbH
Prinzregentenstr. 159
81607 Munich
Germany

klaus.vedder@gi-de.com
The UICC is everywhere
(in the form of the SIM)