Smart Secure Platform

Presented by:  Klaus Vedder       For:  ETSI Security Week 2018

13 June 2018
"Today's SIM card is the most **expensive** piece of real estate on a PCB"

(OEM manufacturer in 2012)

The ID-1 Card
(1FF, 1988)

Plug-in Card
(2FF, 1989)

MFF2
(2010)

3FF (2003)

4FF (2012)

Non-standardised packages - size of the package down to chip-scale

The 4th form factor does not provide the space for the USB interface which had taken years to be approved

SWP (Single Wire Protocol) is the standardised interface for NFC-applications
Secure Elements: From Separate to Integrated

Traditional SIM needs to be re-considered in the context of new mobile communication challenges, including machine to machine communications.

Mike Walker, ETSI Security Conference January 2011

eUICC*

✔ The UICC becomes an integrated, though dedicated piece of hardware of the device (e.g., MFF2)

✔ Provides the possibility of dematerialising the issuance of the SIM

SSP (Smart Secure Platform)

✔ First informal discussions at SCP#71 in Cupertino in October 2015

✔ Idea: Get rid of UICC specific transport protocol (T=0), APDUs, …..

✔ Create a new high level interface application - independent of lower levels

* An embedded UICC or eUICC is a "UICC which is not easily accessible or replaceable, is not intended to be removed or replaced in the terminal, and enables the secure changing of subscriptions" (ETSI TS 103 383)
ETSI’s Answer to the Changing Ecosystem: The Smart Secure Platform

Objective: not standing in the way of a better integration of the UICC while retaining its characteristics

SSP: An open platform for multiple applications
- ✔️ Clear separation of layers
- ✔️ New interface(s)
- ✔️ Faster and flexible
- ✔️ Choice of hardware
- ✔️ New filesystem
- ✔️ Support of existing features
- ✔️ Contactless, Toolkit, ...

Figure taken from ETSI TS 103 465 v 1.2.0
The New SSP Specifications

The SSP “classes”

- iSSP: the UICC (and thus the SIM) becomes an integrated part of the chipset (SoC)
- eSSP: SSP version of the eUICC;
- rSSP: SSP version of the (removable) UICC

Priority on integrated SSP; eSSP and rSSP to follow

Requirements split into generic requirements for all classes and class specific requirements (currently only for iSSP)

- TS 103 465 Smart Secure Platform; Requirements
  - Status: under change control

The technical realisations

- TS 103 666-1 Smart Secure Platform; General characteristics
- TS 103 666-2 Smart Secure Platform; Integrated SSP (iSSP) characteristics
  - Status: both are approaching completion
The iSSP Concept

**Integration** of the functionality of the UICC into a System on Chip (SoC) solution. The iSSP is an independent secure processor within the SoC

**Advantage** lies in the reduction of the number of chips, deeper integration and thus reduced amount of space

**Several bundles** may co-exist in the SoC; one being executed within the Tamper Resistant Element (TRE) and the rest stored securely outside the TRE, ready to be swapped in and executed as required

*For details and a diagram depicting an SoC solution see GlobalPlatform Technology VPP –Concepts and Interfaces Version 1.0 (March 2018)
Multiple Industry Sector SSP

Device

SSP

3GPP Functions

Connections are forbidden

Connects to the enabled bundles and the active Telecom Bundle(s)**

Payment Bundle Management Entity*

Bundle 1
Family Identifier: “Payment”

Bundle 2
Family Identifier: “Payment”

Bundle 3
Family Identifier: “XYC”

Bundle 4
Family Identifier: “Telecom Bundle”

Bundle 5
Family Identifier: “Telecom Bundle”

Bundle 6
Family Identifier: “Telecom Bundle”

Telecom Bundle Management Entity*

Payment Bundle Management Entity*

Bundle 2
Family Identifier: “Payment”

Bundle 4
Family Identifier: “Telecom Bundle”

Bundle 5
Family Identifier: “Telecom Bundle”

Bundle 6
Family Identifier: “Telecom Bundle”

Primary Platform Interface

Primary Platform

*Not yet specified; rules up to the specific industry sector

** “(s)” or no “(s)” , that’s the question

© ETSI 2018
Conclusion

The **standardised** SIM packages will (largely) disappear and a new (SIM) **logical** interface will replace today’s rather old SIM-ME interface for use by all industry sectors.
Thank You

Dr. Klaus Vedder
Chairman ETSI TC SCP
Zeata Security Ltd.

ETSI TC Smart Card Platform

Home of the UICC
The most widely deployed secure element in the world

Next ETSI TC SCP Plenary Meeting
San Diego, USA
28-29 June 2018
see: www.etsi.org

Standardization has always been fun!

Find your way through the standardization maze:
Collect the technologies you need to take mobile telecommunications to the next level.