ETSI STANDARDIZATION WORK

An update about the work of ETSI TC SCP

Presented by Dr. Klaus Vedder, Giesecke & Devrient, TC SCP Chairman - ETSI Security Week 2015
ETSI and TC SCP

The most deployed secure element in the world is specified in ETSI TC SCP: 25+ Years of Real-life Experience

- Founded in 2000 as the successor of SMG9, who specified the most successful smart card application ever (the SIM) with >5 billion (active) subscriptions

The UICC

- A common security platform on a dedicated piece of hardware for all (mobile telecommunication) systems
- Providing physical and logical interfaces enabling communication between the UICC and the hosting device (e.g. mobile phone)
- Over 50 specifications on APIs, browsers, Internet connectivity, M2M, new interfaces for high speed and NFC as well as remote management and test specifications

The specifications are application agnostic and therefore not restricted to the world of telecommunications. They can be used as a (secure) platform for basically any application

© ETSI 2015. All rights reserved
Smart card deployments

Pace accelerating for banking and device manufacturers

© ETSI 2015. All rights reserved
Mobile contactless services (NFC)

TC SCP delivered a widely adopted set of technical specifications enabling the use of a UICC as a Secure Element (SE) for contactless applications, e.g. turning the device hosting the UICC into a "contactless card"

- Single Wire Protocol (SWP) provides a direct physical interface
- Host Controller Interface (HCI) is the logical interface

An NFC controller may have, in the same package, its own secure element. This may result in a system with multiple Secure Elements

- Resulting challenges
  - Routing of communication to the right application in the right Secure Element, regardless of the configuration.
  - Knowledge and setup of the system
- In order to avoid fragmentation and to foster interoperability, ETSI, GlobalPlatform and the NFC Forum have teamed up to provide a single technical solution

© ETSI 2015. All rights reserved
Are multiple secure elements really needed?

Any combination of secure elements in a mobile device: 1 or 2 SIM cards, a SIM on an embedded UICC (eUICC*), an OEM specific secure element, a TPM, ....

We will see eUICCs as the platform for the SIM application(s) in consumer devices
- The OEM will be the owner of the eUICC - will that make the secure platform more open?
- MNOs and banks both become third parties
- Possibility to store derived IDs, ....
- Need for separate embedded secure element in such an environment?

Is SCP to work on such an ecosystem .... ? !

eUICCs are already happening in the M2M environment
- Automotive, IoT (e.g. remote management of sensors), smart meters, vending machines, etc.

* An 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)
M2M applications have driven the need for subscription management in eUICCs
  • SubMan is Over-The-Air management of the SIM application(s)

OTA management of the UICC is nothing new
  • Confidential management of application is available (a third party can manage its content without this being known or readable by the eUICC issuer)
  • Firewalling between application providers also exists - GlobalPlatform's security domains

A question about security of security algorithms
  • Implementation of security on an SE is SW and HW dependent
  • Applications may require specific security algorithms not provided by the eUICC by default - can they be downloaded preserving the security?
Dr. Klaus Vedder

Group Senior Vice President
Giesecke & Devrient GmbH
Prinzregentenstr. 159
81607 Munich
Germany

klaus.vedder@gi-de.com

Next TC SCP Plenary Meeting
Detroit, 09-10 July 2015
see: www.etsi.org

Standardization has always been fun!