



Welcome to the World of Standards



EMBEDDED UICC: THE PATH TO A STANDARD

Standardisation of the embedded UICC for M2M/IoT

Presented by Xavier PIEDNOIR

21 March 2016 - Mainz, Germany.

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 with 5 billion+ users

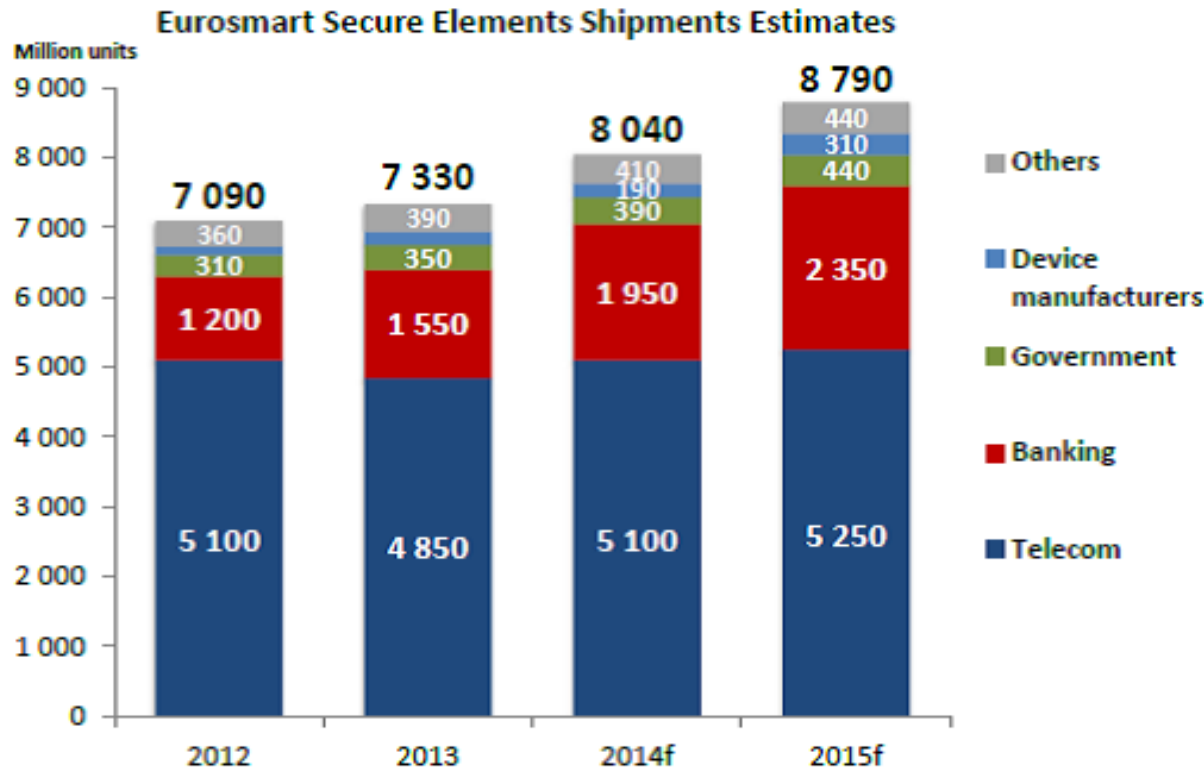
Specifies the UICC:

- A common IC Card platform for all mobile telecommunication systems
- Physical and logical interfaces enabling communication between the IC Card and the hosting device (e.g. mobile phone)
- APIs, browsers, Internet connectivity, M2M, new interfaces for high speed and NFC as well as remote management



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.

Smart card deployments



Forecast for 2016: 9800+ million of units
Pace accelerating for banking and device manufacturers (embedded secure elements).

Smart Cards: working with others



- ETSI does not work in isolation:
 - Partnerships is the preferred way
- ETSI is the largest partner in 3GPP
- GlobalPlatform and NFC Forum are longstanding working partners:
 - MoU with both of them
- MoU with SIMalliance
- Partnership with GSM Association
- ETSI and EMVCo building relationship

See portfolio at:

<http://webapp.etsi.org/AgreementView/AgreementSearch.asp>



Embedded UICC (eUICC) on the way (1/2)



- M2M applications and harsh industrial environments drive the need for non-removable or non-accessible UICCs.
 - Smart meters, vending machines, car communication modules
- No easy replacement does not have to translate into "lifetime contract with card issuer"
 - Need for a remote management technical solution for the whole eUICC, including network access applications and related credentials
- Standard mechanisms to remotely provision and manage a subscription are needed
 - Management = enabling, disabling, deleting a subscription
 - For some devices, local management may be required



Embedded UICC (eUICC) on the way (2/2)



- Fuzzy line between M2M and consumer devices
 - Where do tablets, wearables, consumer appliances sit?
 - Are those devices actually intended to have their own mobile network connectivity or are they rather best behind a "gateway" device (e.g. smartphone)?
- Different business models for embedded UICC in M2M and in consumer markets
 - Should the constraints related to one affect the other?
 - Example of eCall



Form Factor trends (1/2)



ID-1
(ISO/IEC 7810)

ID-1 aka Credit Card
2FF aka Mini-SIM
3FF aka Micro-SIM
4FF aka Nano-SIM
MFF2 aka Black Bug

2FF

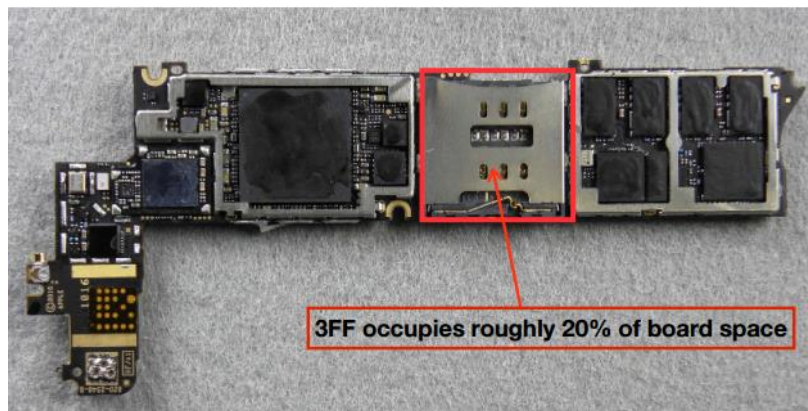
ETSI TS 102 221

3FF

4FF

□ MFF2

ETSI TS 102 671
(M2M UICC)



- Standardized form factors required for physical interoperability
 - Is that still needed when the UICC is soldered?
- Plenty more form factors still meet requirements for eUICC
 - Keeping the eUICC a dedicated piece of hardware
 - Making sure that the eUICC can be certified
- New approach in ETSI:
 - Flexible requirements for form factors
 - Discussions about allowing alternative electrical interfaces
 - Aim: not to stand in the way of better eUICC integration while retaining eUICC characteristics



Courtesy Giesecke & Devrient

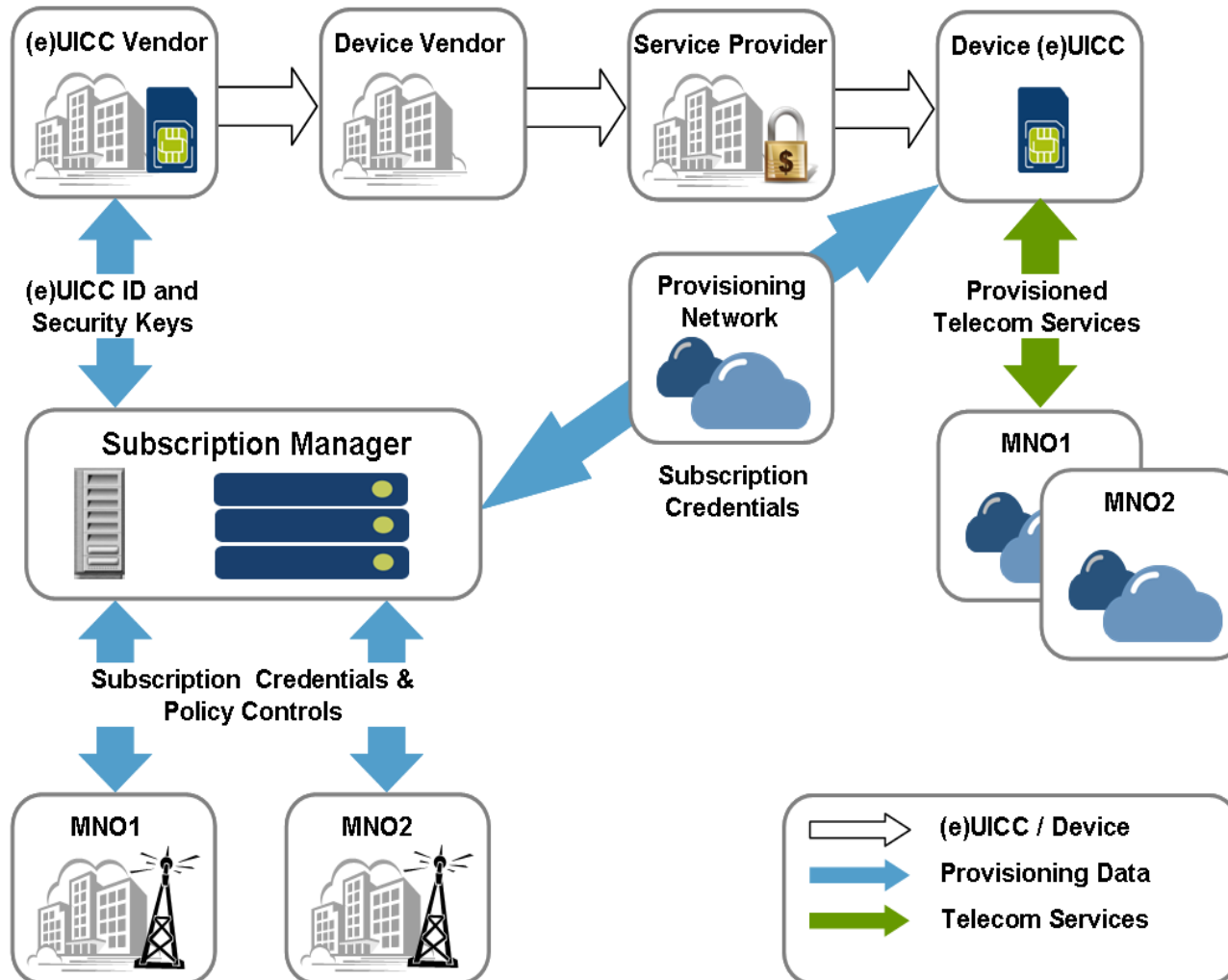
- From hard requirement (M2M) to convenience for the device manufacturer (consumer devices)
 - Thickness, battery life, screen size and feature set are key selling points. Time to market is important
 - The UICC gets in the way (too big, requires a holder/slot/tray, needs thorough device testing)
 - Handset/tablet makers would like to get rid of the removable UICC
 - Transition to eUICC.
- But there is more than overcoming technical barriers
 - Weakening the link between the MNO and the end-user is also a welcome side-effect (for the handset manufacturer)



- The MNO is no longer issuing the UICC:
 - Control over the secure platform is lost
 - Legitimacy to provide secure services is lowered
 - Shift of the above to the device manufacturer
- The MNO is still the main legitimate user of the eUICC.
 - This platform has been created to secure the MNO revenue
 - What if the device manufacturers decide to provide eUICCs that are less secure than the one that the MNO would have chosen in a legacy system
 - Questions about liability
 - Questions about interferences in each other's business
- Open questions:
 - Who really owns the eUICC? The end user?
 - Will that make the secure platform really more open?



Subscription Management: ecosystem



- OTA management of the UICC is nothing new:
 - Existing secure protocols have stood the test of time and are future-proof
 - Firewalling between application providers also exists thanks to GlobalPlatform's security domains
 - Confidential management of application is also specified (a third party, in this case the MNO, can manage its content without this being known or readable from the eUICC issuer)
- Question mark about authentication algorithms:
 - Due to security and performance reasons, their support is at Platform-level. No standard way to load a new one
 - The supported set of authentication algorithms is fixed. What consequences for MNOs?
- Local Management of Profile: a threat?
- The industry is considering full eUICC firmware update, which would cover algorithms

- A number of advantages:

- Getting rid of plastic, everything handled online
- No form factor jungle anymore

- Some penalties:

- no easy SIM swap. Battery dead? Too bad..
- potential MNO grip
 - care should be taken to protect the subscriber from unnecessary/artificial lock-in, at least it should not be more than today.



When will we see this? (1/2)



- Initial work in GSMA:

- The MNO industry decided to start work there
- More MNO-friendly environment
- Tailor-made process + fewer players deciding resulted in quicker delivery
 - Two specifications: one for M2M, one for consumer devices
 - When will those two converge/merge?
 - Some requirements of the non-MNO community not addressed

- The industry wants an ETSI standard:

- Real standard with a real standards making and maintenance process
- Alignment with GSMA specifications is desired
- Question: align with which GSMA specification?
 - Potential umbrella specification by ETSI
 - Some GSMA-specific constraints may be relaxed



When will we see this? (2/2)



- The process in ETSI is open:
 - All parts of the industry represented, all players have a say. In TC SCP, handset manufacturers, MNOs, smart card manufacturers and silicon manufacturers are all present
- The process in ETSI is consensus-driven:
 - Some say "the more, the merrier"... it also means that consensus takes time to build, especially in such context
- Consensus building is slow but leads to stronger commitment
- Target date for technical spec: Q4 2016



- An embedded UICC retains its selling points:
 - The "most standard" secure element
 - Unchallenged interoperability
 - A comprehensive toolbox for remote provisioning and administration
- Still a number of open questions:
 - Technical
 - Business/Political
 - Legal/Regulatory
- It is coming, whether some like it or not
 - Let's make sure it provides a fair and level playing field for all actors
 - Let's make sure the change is not at the expense of the subscriber



Contact Details:

Xavier PIEDNOIR

Technical Officer - Smart Cards

xavier.piednoir@etsi.org

All of the ETSI deliverables for free at: <http://www.etsi.org/deliver>

Search tool at: <http://pda.etsi.org>

Thank you!