

Welcome to the World of Standards



Dr. Klaus Vedder
Chairman ETSI TC SCP

The UICC

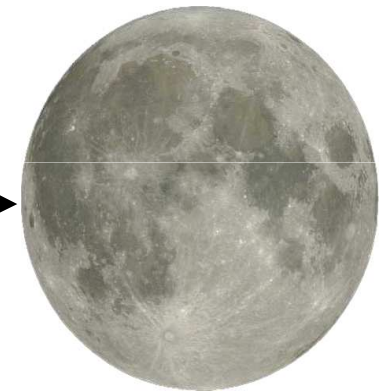
Recent Work of ETSI TC Smart Card Platform

7th ETSI Security Workshop, Sophia Antipolis, France, 18-19 January 2012

SIMs, USIMs, R-UIMs, CSIMs... in 2011



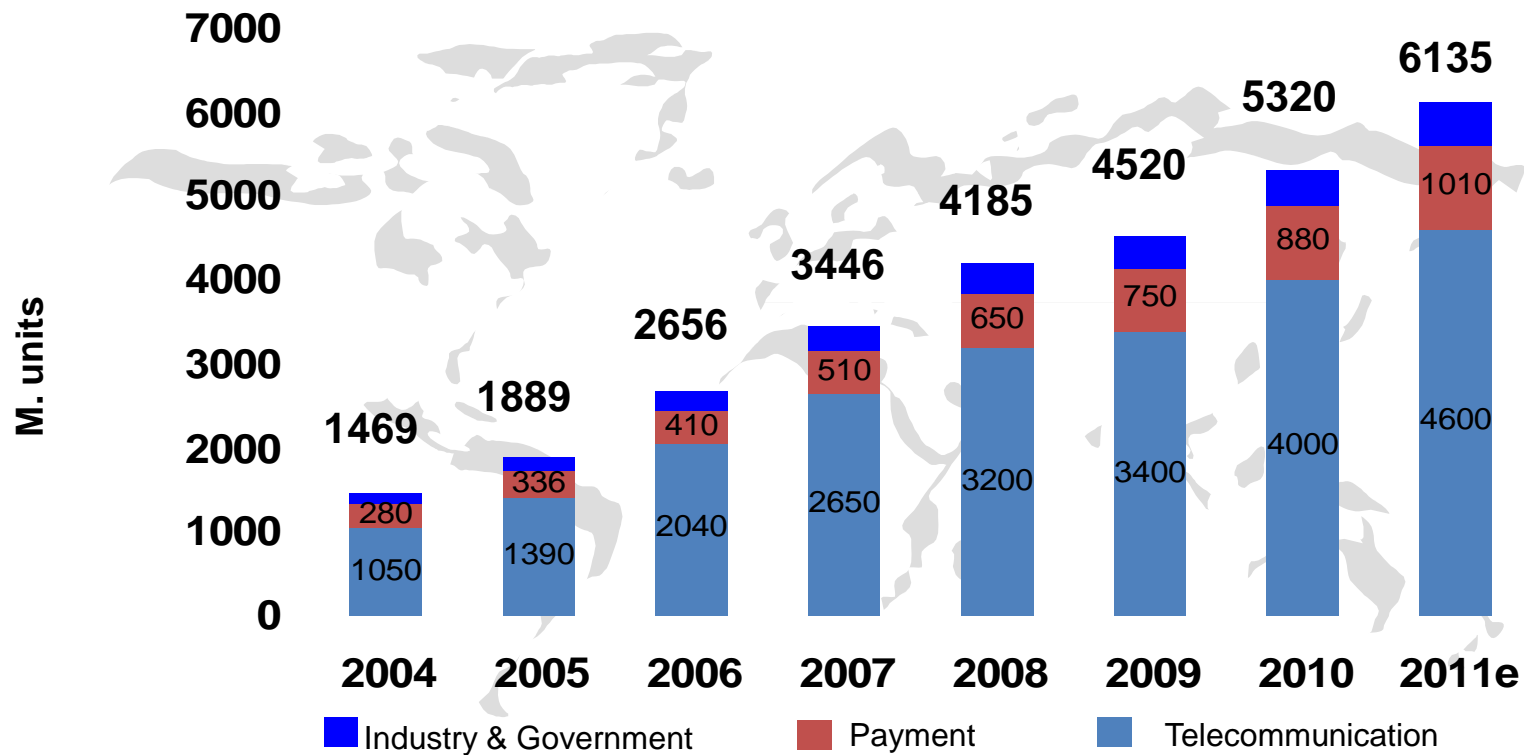
362 570 km



Missed the moon by just
20.000 km



The Smart Card Market



Source: Eurosmart



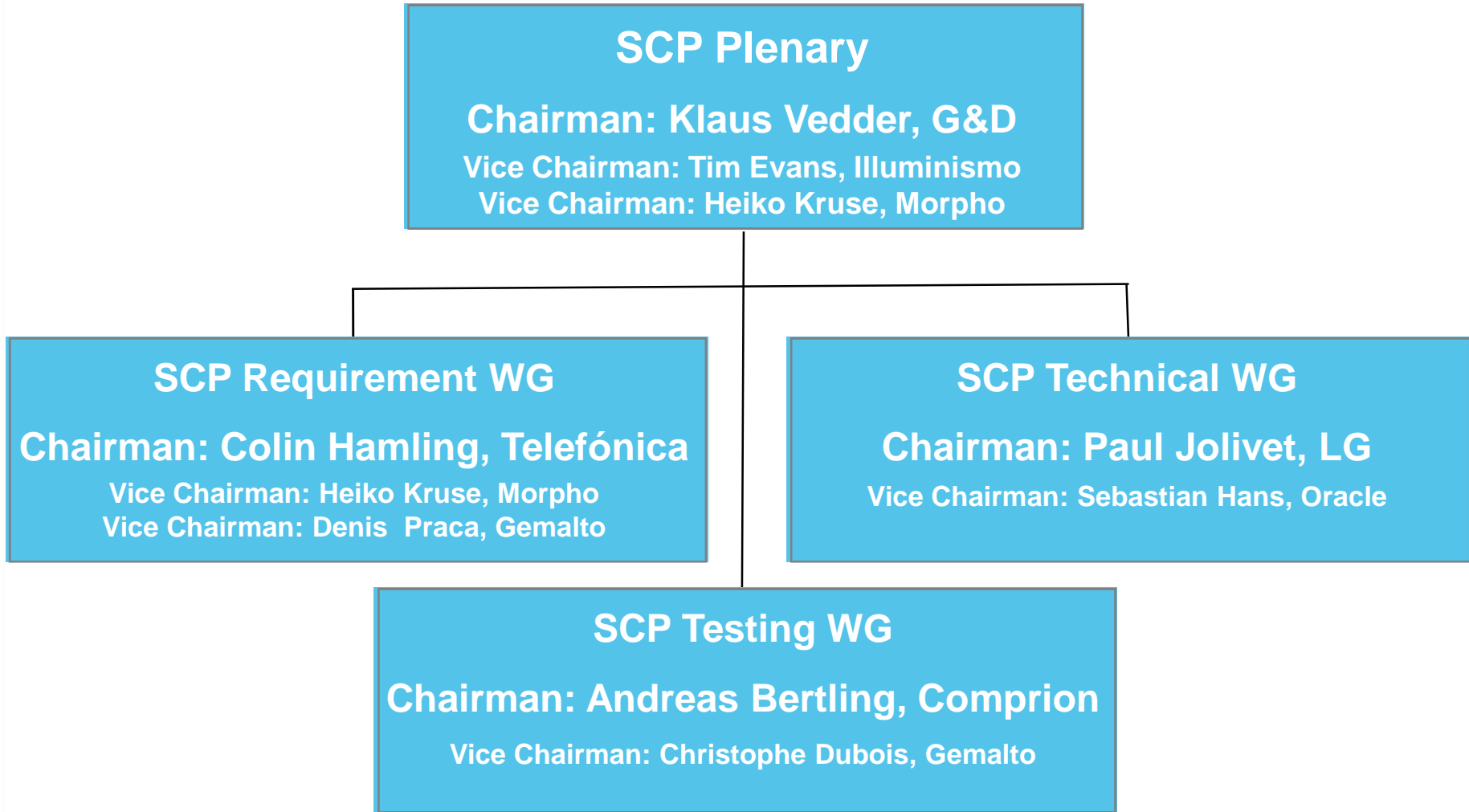
Giesecke & Devrient

- **24 Years of Dedication and Real-life Experience**
 - TC SCP was founded in March 2000 as the successor of SMG9, the people who specified the most successful smart card application ever with well over 5 billion subscribers using one or more of the over 25 billion SIMs, USIMs, R-UIMs, CSIMs, ... delivered to the market
- **ETSI TC SCP has published over fifty specifications on smart cards encompassing for every topic the whole range from requirements via the technical solution to the test specification; topics range from administrative commands to APIs, browsers, Internet connectivity, Machine-to-Machine, new interfaces for high speed and NFC as well as remote management**
 - All can be downloaded free of charge from the ETSI website

The specifications are application agnostic and are not restricted to the world of telecommunications.

They can be used as a (secure) platform for basically any application.

Structure and Officials



SCP

- Final acceptance of Work Items to be progressed by Working Groups
- Acceptance for publication of all Technical Specifications and Technical Reports as well as Change Requests to published documents
- Input to its work is received from ETSI members as well as 3GPP, 3GPP2, GlobalPlatform, GSMA, GSMA SCaG, Global Certification Forum (GCF), NFC Forum, OMA, ...

SCP REQ

- Working Group SCP REQ is responsible for developing the requirements for the Smart Card Platform

SCP TEC

- Working Group SCP TEC is responsible for the technical realisation of the requirements developed by SCP REQ and accepted by SCP

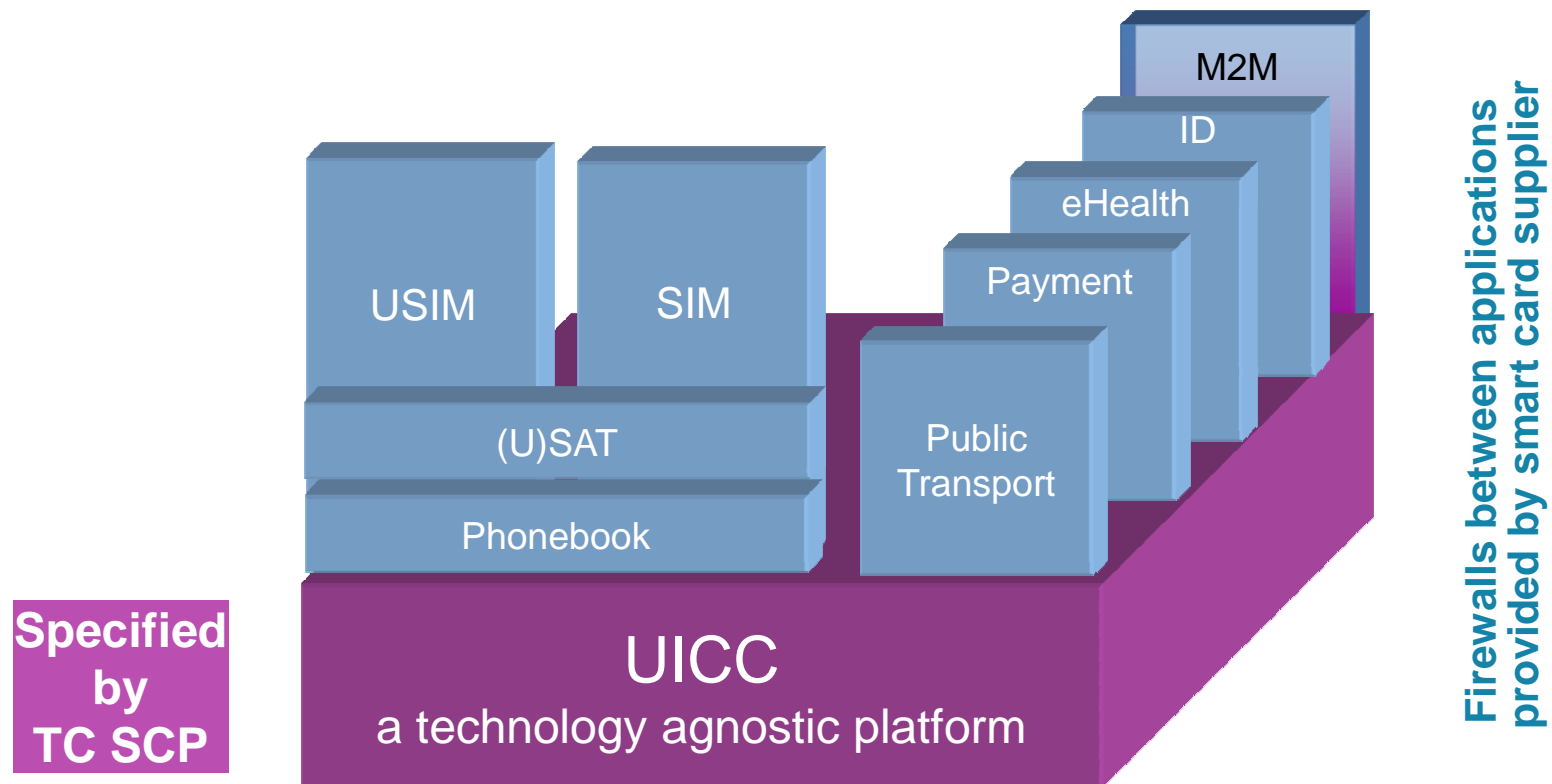
SCP TEST

- Working Group SCP TEST is responsible for the development of test specifications for deliverables produced by SCP TEC and accepted by SCP

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



A year of consolidation, after completion of eight specifications in 2010, with two exciting new topics.

The 4th Form Factor

- **Collection of use cases and requirements for a UICC form factor smaller by 25% to 40% than the one known as Mini-UICC or 3FF. While smaller, this form factor would retain the existing UICC functionalities**
- **Development of the technical specifications for a fourth UICC form factor (4FF) in accordance with the technical requirements and selection criteria**

The embedded UICC

- **A new approach for the M2M environment, revolutionizing the life of the SIM**

- **Card Application Toolkit can now be executed on composite devices (e.g., M2M module with an external display)**
- **Two customer organizations of TC SCP use the Secure Channel for the specification of their features**
 - 3GPP for secure communications between the USIM application and a Relay Node; OMA for use in the OMA BCAST specifications

Work on a related test specification started

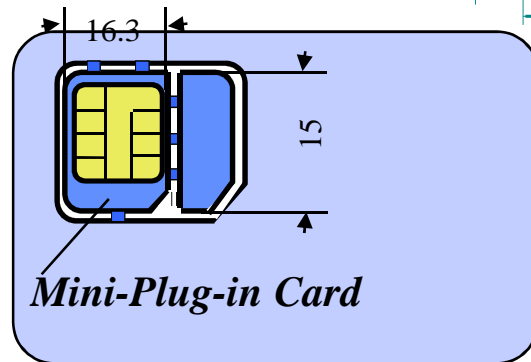
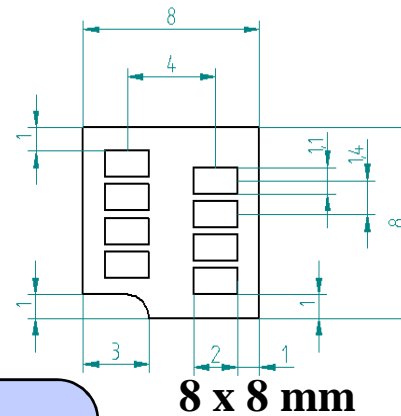
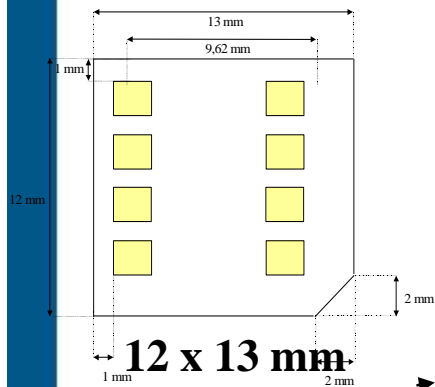
- **SCP started the following new Work Items**
 - Requirements for an embedded UICC
 - Memory integrity monitoring in M2M applications
 - Test Specification of the architecture, functional capabilities and characteristics of the Secure Channel
 - Test Specification for UICC Application Programming Interface for Java Card™ for Contactless Applications
 - Requirements and technical solution for a 4th Form Factor
 - P2P mode for contactless communications

2003: How Small is Small ?



3rd Form Factor (3FF) or mini-UICC

- May enable use of devices currently not feasible for Plug-in cards
- Backwards compatibility necessary (?)
- Also traded under the name micro-SIM



The standardised mini-UICC as part of the Plug-in card being part of the ID-1 card

3FF: A hardware “SIM-lock”?

Motivation for Yet Another Form Factor



● Nearly 8 years after the standardisation of the 3rd Form Factor (or mini-UICC, "micro SIM") Apple introduced this as a "first" mover into its devices

- Plug-in: 15x25 mm
- 3FF: 12x15 mm







● Large device manufacturers are now adopting the 3FF

BUT

Today's SIM card and connector are the most expensive piece of real estate on a PCB

A New Work Item for a Smaller SIM Card



- 
“4FF” – the 4th Form Factor
 - Smaller and thinner (than 3FF) removable SIM card
- 
Backwards compatibility
 - The new form factor should support existing functionality
- 
Adapter readiness
 - Thinner to allow adapters so that the 4FF can be "clicked" into adapters for use as a Plug-in SIM or 3FF SIM giving a kind of backward usability
- 
Supported by all BIG MNO Groups
 - AT&T, Deutsche Telekom AG, France Telecom/Orange SA, Telefonica SA, Verizon Wireless, Vodafone Group

| | | | |
|--|--|--|---|
| ETSI TC SCP #50 Marseille, France, 16 – 17 June 2011 | | SCP(11)0254r1 | |
| New Work Item Form | | Form to be used when proposing new Work Items for adoption onto the ETSI Work Programme. | |
| ATTENTION: Before starting to work on a revision of a published ETSI document, contact edithelp@etsi.org to obtain the latest Word version. In case of multi-part deliverable, please use ONE work item form for EACH part. | | | |
| Work item details | | | |
| Which Technical Body is responsible? ETSI TC Smart Card Platform (TC SCP) | | Sub Group: SCP REQ Project: | |
| WI reference number (if known) <small>(number will be allocated by Secretariat if not shown)</small> | | Will an STF be requested? [Yes / No] STF number (if known): _____ EC mandate number (if relevant): BC: _____ | |
| Formal title of deliverable: | | Use Cases and Requirements related to Fourth UICC Form Factor | |
| Working title: Fourth UICC Form Factor (4FF) | | Scope of work to be undertaken: The scope of this work item is detailed below: Development of CR(s) to 102.412 to detail the use cases, requirements and selection criteria for a new form factor which is easily removable and replaceable by the end user. It is expected that SCP REQ shall consider the following key points in this work item: <ul style="list-style-type: none"> • That the proposed size of the new form factor shall be much smaller (at least 25%–40%) than the current Mini-UICC to achieve a size optimization of terminals while allowing easy handling of the UICC by end user (i.e. without requiring specific tools) • That existing UICC functionalities as defined in ETSI specifications shall be retained in this new form factor | |
| Rapporteur (named individual person): name: Naushad Zaven _____ organization: Apple Inc _____ e-mail: Nzaven@apple.com _____ | | Supporting ETSI Member organisations: (name at least four) 1. Apple 5. Telefonica SA 2. AT&T 6. Verizon Wireless 3. Deutsche Telekom AG 7. Vodafone Group 4. France Telecom/Orange SA | |
| Deliverable document details: | | | |
| What type of document will be produced? EN [] EG [] ES [] TS [X] TR [] SR [] OS [] For EN deliverables only: – Is the draft EN to be approved by One-step Approval or Two-step Approval Procedure? [OAP / TAP] – Candidate harmonized standard? [Yes / No] – Directive: _____ | | Is it a new document or a revision of an existing one? [revision] If a revision, state the deliverable (e.g. TS 102.987 v1.1.1) being revised: TS 102.412 _____ edition / version | |
| Hierarchy: If this Work Item fits in a hierarchical tree (see TRP clause 1.6.1), its position shall then be indicated here by giving the reference of its parent node (WI reference / deliverable number / topic name): _____ | | | |
| Work schedule: | | | |
| Milestone name | | Target date | |
| • YB adoption of WI | | SCP #50 | |
| • Early Draft | | SCP REQ #32 | |
| • Stable Draft | | SCP REQ #33 | |
| • Draft for approval | | SCP REQ #33 | |
| • WI approval <small>(with min. 90%)</small> | | SCP REQ # 53 | |
| • TS approval | | SCP # 52 | |
| To be published as version: | | V. _____ | |
| Remarks: | | | |
| Environmental Aspects | | [Yes / No] | User / Consumer Aspects [Yes / No] |

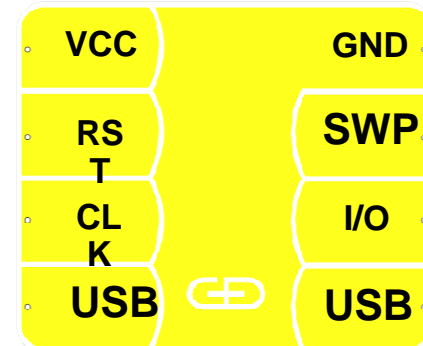


• No plastic around the contact plate

- Cutting away all "excessive" plastic around an 8 contact 3FF SIM card would give a saving in area of ~30% over the 3FF SIM - new size: 10.4x 12.2 mm
- However, a small rim of isolating material is absolutely necessary to avoid short circuits with the socket (problems with hand-made 3FFs)

• If we want to be really small

- What about contacts C4 and C8 which are used for the USB interface ?
 - ~70% of today's SIMs are delivered with a 6 pin contact plate
- How do we cater for the USB interface ?
 - Additional contact(s) in the middle of the contact plate
 - Switch of protocol from T=0 to USB during operation using the other existing contacts
 - Replace T=0 interface by USB interface and give up backwards compatibility
 - not a solution any longer



Savings by Cutting Away Plastic



| Card | Height | Width | Area | Saving wrt Plug-in |
|-------------------------|--------|-------|------|--------------------|
| Plug-in (1989) | 15 | 25 | 375 | |
| 3FF (2004) | 12 | 15 | 180 | 52% |
| 6 pin 4FF | 9* | 12* | 108 | 71% (40% wrt 3FF) |
| 8 pin 4FF "w/o plastic" | 10.4* | 12.2* | 127 | 66% (30% wrt 3FF) |

* rough figures

**In comparison:
MFF2**

5 6 30



The 10 Requirements (Agreed)



- The fourth UICC form factor shall be at least 25% smaller as compared to the Mini-UICC.
- The fourth UICC form factor should be 40% smaller as compared to the Mini-UICC.
- The fourth UICC form factor shall specify 8 contacts.
- The usage of the 8 contacts of the fourth UICC form factor shall be compliant with ETSI TS 102 221 Section 4.5.
- The fourth UICC form factor shall retain all existing UICC functionalities as specified in the existing ETSI specifications.
- It shall be possible to have a legible identifier (e.g. at least ICCID) on a UICC complying to the fourth UICC form factor.
- The fourth UICC form factor shall be easily removable and replaceable by the end user (i.e. without requiring specific tools).
- The design of the fourth UICC form factor shall prevent the 4FF from becoming jammed in a Mini-UICC reader. An example is that if the 4FF is turned 90 degrees and it fits perfectly into the Mini-UICC reader (4FF length = Mini-UICC width).
- The need for an orientation mark to prevent wrong insertion (4FF into 4FF reader) should be considered in order to prevent "electrical damage" of the UICC.
- There shall be a maximum contact pad size defined in order to prevent the contact pad metal to stretch to the 4FF card edge (e.g. min. 0.2 mm clearance towards the edge).



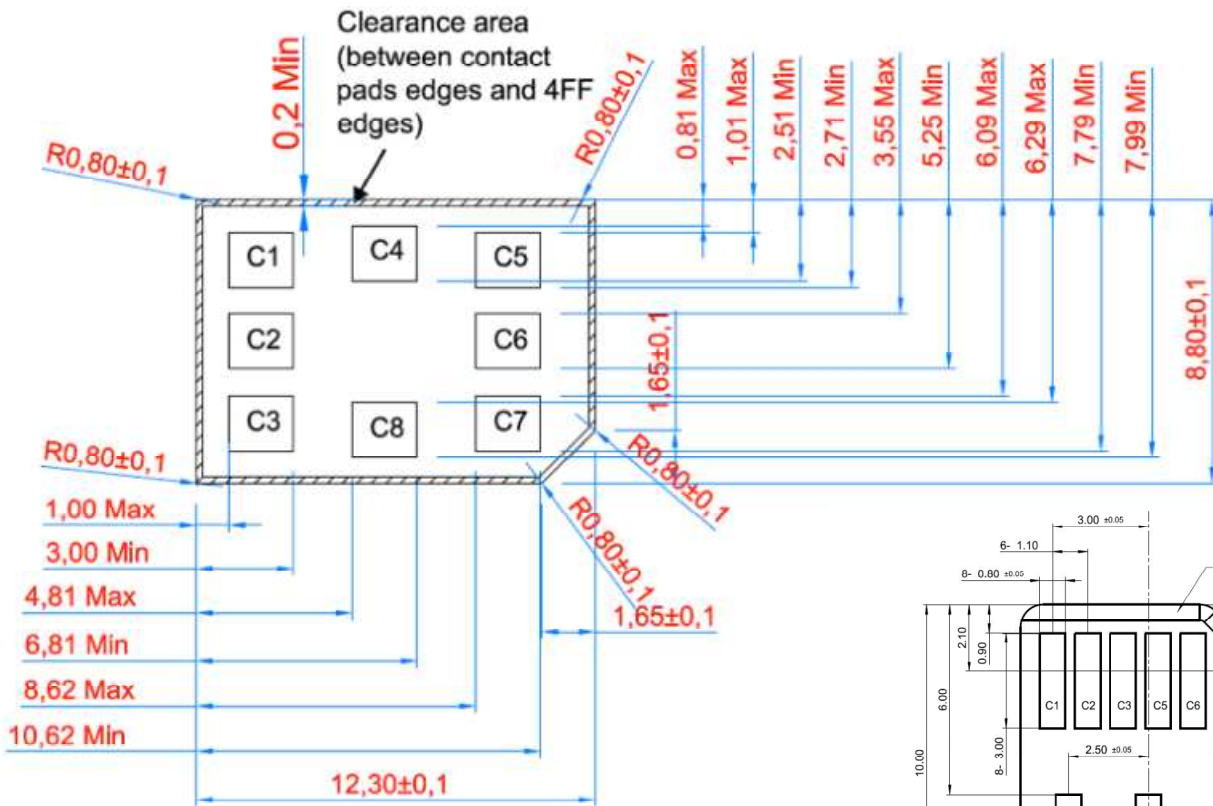
The 4 Selection Criteria (Agreed)



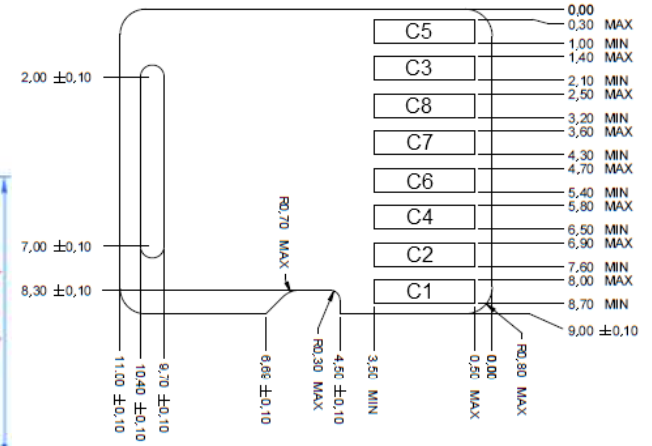
- **The following selection criteria is to be used when selecting a technical solution in case several technical solutions meet the requirements specified in the present document.**
 - **A preference is to be given to a technical solution for the 4FF that provides an overall space saving, including the mechanical reader, compared to a solution where the UICC size reduction is higher but the size reduction including the mechanical reader is less.**
 - **In case of several solutions providing similar size reduction a preference is to be given to a solution based on the existing plug-in/mini UICC contact layout (size and arrangement) compared to a solution based on a different contact layout.**
 - **In case of several solutions providing similar size reduction a preference is to be given to a solution with a shorter time to market than a solution with a longer time to market. Time to market includes availability of both UICCs and mechanical readers.**
 - **A technical solution that prevents "electrical damage" in case of wrong insertion is to be given a preference compared to a solution not providing such protection.**



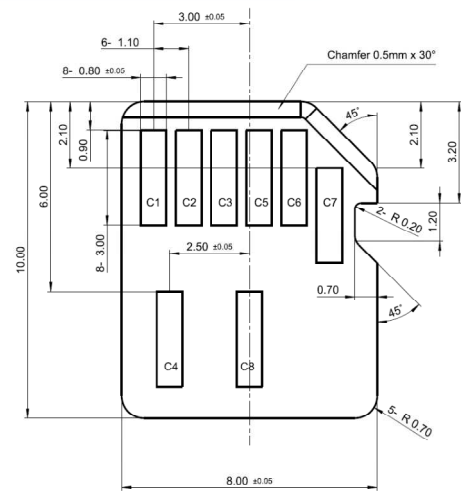
The 3 Proposals



Apple et al
12.3 mm x 8.8 mm



RIM
11 mm x 9 mm



Nokia
10 mm x 8 mm

The One Solution



Machine-to-Machine

Over-the-Air

Quality

Innovation

Flexibility

SIM

Factor Forms

Payment

Automatic

Simplicity

MINO

Trusted Service Manager

Leader

Trust

System Logic

Internet of Things

Software

Confidence

Utility

Security

Mobile Security

Responsibility

Integrity

Secure Elements

Embedded

Standardize

Subscription Management

Identity

Portability

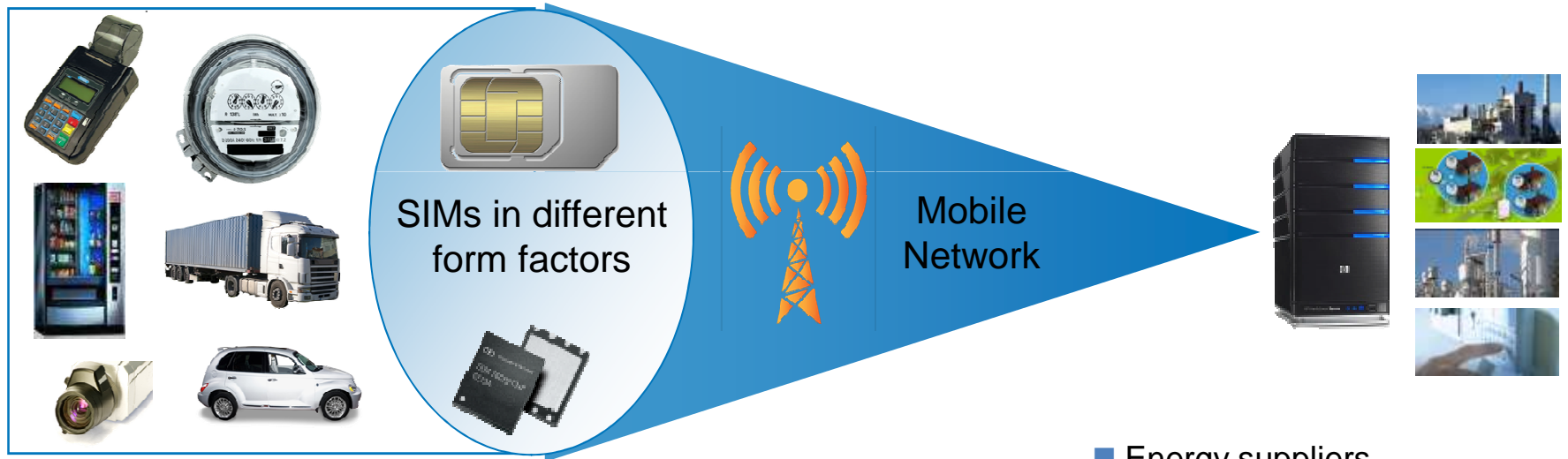
Confidentiality

ODA

Personalization

Or The Embedded UICC

M2M - Rise of the Machines



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

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

- **Mobile networks are starting to be used to connect all sorts of devices**
 - Wireless for mobility, ease of connection and remote management

- **SIMs may be embedded in devices at manufacture**
 - This may even be in advance of choice of country of use and network operator
 - Network operator may be changed during life time of the device

- **The traditional, removable SIM may not be appropriate for certain applications**

🌐 March 2010: A new specification for UICCs (SIMs) in M2M

- M2M specific constraints such as data retention, temperature, memory update cycles, vibration resistance, humidity
- MFF1 (M2M Form Factor 1) socketable 8 pin solution
- MFF2 : a non-removable, to-be-soldered housing (SON8)



What is M2M?

- **No more "plastic roaming" for the user**
 - Regulatory issues – need to change the operator
- **Ownership of an embedded SIM**
 - In some countries the end user will own the "black beetle"
- **No point in stealing a mobile device with an embedded SIM**
- **Field of usage – warranty of M2M SIM supplier**
- **Future role of the MNOs and service providers (car manufacturers, energy suppliers, ...)**
- **Lifetime issues of the chip (new SCP Work Item)**
- **Lifecycle management - personalisation and re-personalisation (OTA, OTI, ...) and distribution**

A Brief Overview of Events



- **Following some rumours about embedded SIMs in devices of some company, the GSM Association formed a Task Force on "embedded SIM" in November 2010**
- **GSMA document “Embedded SIM Task Force Requirements and Use Cases” together with a Work Item proposal given to ETSI SCP in late February 2011**
 - **GSMA Requirement Document encompasses large parts of a paper by Deutsche Telekom, Telefónica O2 UK, Vodafone Group and G&D**
- **ETSI work item on use cases and requirements agreed by ETSI SCP in early March 2011**
 - **Work on Machine-to-Machine (M2M) applications has given rise to the possibility of having a UICC that is embedded in a communication device in such a way that the UICC is not easily accessible or replaceable. The ability to change network subscriptions on such devices becomes problematic, thus necessitating new methods for securely and remotely provisioning access credentials on these Embedded UICCs (eUICC) and managing subscription changes from one operator to another**

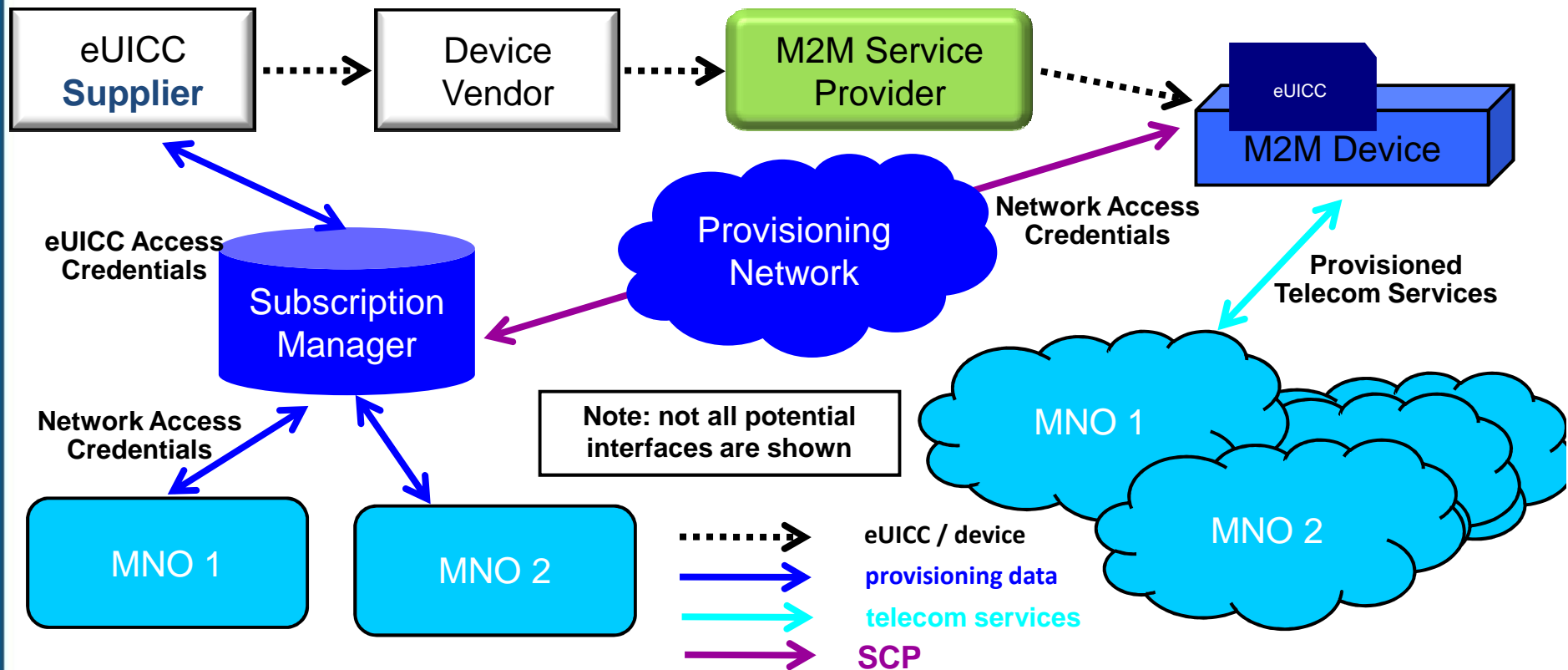




| No. | Use Case | Description |
|-----|---|---|
| UC1 | Provisioning of multiple M2M subscriptions. | A Machine-to-Machine Service Provider (M2M SP) sets-up M2M subscriptions for a number of connected M2M devices to start telecommunication services with a first MNO. Optionally, the M2M SP may later change subscriptions to a subsequent MNO. |
| UC2 | Provision of first subscription with a new connected device | A subscriber purchases a new type of communications or connected device from a device vendor together with a subscription to provide first services to this device. |
| UC3 | Subscription Change | A subscriber changes the subscription for a device to stop services with the current MNO and start services with a new MNO in accordance with policy control functions for each MNO. |
| UC4 | Stop Subscription | A subscriber sells his device and stops the subscription for services from the current MNO. |
| UC5 | Transfer Subscription | Subscriber transfers subscription between devices. |



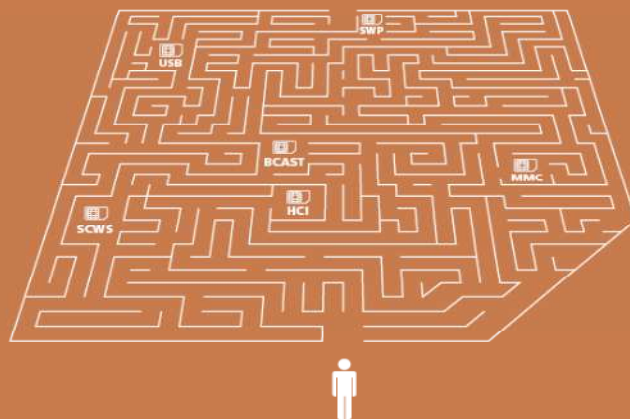
A Potential Architecture for Subscription Management



The diagram depicts roles and not entities. The architecture is still under discussion in SCP and, for instance, the role of the Subscription Manager may be split into two, one which prepares the data and one which downloads the data to the UICC



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.*

Next SCP Plenary Meeting
29-30 March in Cupertino
see: www.etsi.org

Dr. Klaus Vedder

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

klaus.vedder@gi-de.com

Requirements for an Embedded UICC

Reasoning in the Work Item

- Work on Machine-to-Machine (M2M) applications has given rise to the possibility of having a UICC that is embedded in a communication device in such a way that the UICC is not easily accessible or replaceable. The ability to change network subscriptions on such devices becomes problematic, thus necessitating new methods for securely and remotely provisioning access credentials on these Embedded UICCs (eUICC) and managing subscription changes from one operator to another
- This Work Item proposes to identify, analyse and define a representative set of use cases that will provide the key requirements for the development of a trusted framework for the management of an eUICC and for remote personalization and subscription management of such an eUICC including its integration in telecommunication network infrastructures
- It is expected that the use cases will identify aspects that need to be standardised by other organisations such as 3GPP, 3GPP2 and GlobalPlatform

Test Specification for the architecture, functional capabilities and characteristics of the Secure Channel

- This WI will provide a new conformance test specification verifying requirements specified in TS 102 484 *Secure Channel between a UICC and an end-point terminal* . This includes the architecture, functional capabilities and characteristics of the Secure Channel protocol and its associated interfaces transported over the UICC interfaces
- An STF has been formed to develop this specification

Memory integrity monitoring in M2M applications

- Applications running on an M2M UICC may need to face the degradation of non-volatile memory that usually has a limited write cycle guarantee. This work item will deliver optional extensions to the UICC API for Java Card . These extensions allow applications to be alerted if hardware performance is degrading due to its aging and support applications in reducing stress on non-volatile memory for specific data areas

Test Specification for UICC Application Programming Interface for Java Card™ for Contactless Applications; Test Environment and Annexes

- Scope: creation of a test specification covering Contactless UICC API conformance requirements specified in TSI TS 102 705

4th Form Factor (Requirements and Technical Solution)

- Scope: Collection of use cases and requirements for a UICC form factor smaller by 25% to 40% than the one known as Mini-UICC or 3FF. While smaller, this form factor would retain the existing UICC functionalities
- Scope: Development of the technical specifications for a fourth UICC form factor in accordance with the technical requirements and selection criteria

P2P mode for contactless communications

- Definition of the support of P2P mode in contactless specifications according to the agreed requirements in TS 102 412.