3GPP TR 22.817 V0.~~3~~4.~~1~~0 (~~2010~~2011-~~08~~11)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on UICC/USIM enhancements
(Release ~~1~~2~~1~~)

Keywords
UICC, USIM

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP) Secretariat on behalf of the 3GPP Technical Specification Groups (TSGs).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

The present document is based ISO/IEC Directives. Most clauses of the ISO/IEC document have been retained, while some clauses have been modified or deleted. Additional material has been inserted.

Items concerning word-processor specific layout and formatting matters when using the Microsoft Word for Windows® based skeleton documents and templates are shown with shaded background. Boiler plate text (i.e. text which shall be directly used in 3GPP specifications) is represented by *italic* characters.

1 Scope

The present report identifies use cases and potential requirements for new USIM services with a focus on:

- Instances where the USIM is used inside terminals with specialised functionalities (e.g. radio modems, 3G Notebook terminals);
- Possible enhancements to facilitate USIM-UICC support for new services;
- Possible enhancements to facilitate an improved user experience when interacting with the UE; and
- Evolution from the USAT towards multimedia USIM toolkit support.

The present report covers only use cases and services that cannot be fully implemented and easily realised using the existing standards, but instead require some enhancement of the present UICC/USIM requirements. Alternative technical solutions (i.e. non USIM-based solutions) are also introduced and referenced for use cases in order to provide a more complete picture of how they might best be realised.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] GSMA Smart SIM project Technical Implementation Guide Version 1.0. Available @http://www.gsmworld.com/newsroom/document-library/technical_documents.htm;

[2] ETSI TS 102 221 v9.1.0 ”Smart Cards; UICC-Terminal Interface; Physical and logical characteristics”

[3] ETSI TS 102 600 v10.0.0 ”Smart Cards; UICC-Terminal interface Characteristics of the USB interface”

[4] 3GPP TS 31.116 v6.5.0 “Remote APDU Structure for (U)SIM Toolkit applications”

[5] ETSI TS 102 223 v9.2.0 "Smart Cards; Card Application Toolkit (CAT)"

[6] ETSI TS 102 484 v9.1.0 “Smart Cards; Secure channel between a UICC and an end-point terminal“

[7] Open Mobile Alliance “Smart Card Web Server”: OMA-TS-Smartcard_Web_Server-V1_1_1-20100910-A

[8] ETSI TS 102 613 v9.1.0 "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics (Release 9)"

[9] ETSI TS 102 622 v10.1.0 "Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) (Release 10)"

3 Definitions and Abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

BIP: Bearer Independent Protocol
CAT: Card Application Toolkit
OMA Open Mobile Alliance
OMA DM Open Mobile Alliance Device Management
SCWS: Smart Card Web Server

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

4 Use cases

4.1 Service and terminal dependent subscription parameters management

The increase number of services and capabilities of the 3GPP network may lead to a higher segmentation of the terminal market in terms of arrival of more and more terminals dedicated to specific set of services. With the arrival of this type of dedicated terminals, a need for specific subscription and subscription parameters may arise.

For example, terminals dedicated to data services may benefit from a different preferred roaming partners compared to terminals dedicated to voice services.

4.2 Activation of data access on a new device

The user purchases a new personal computer with 3GPP access capabilities not pre-configured by a specific MNO. Under the assumption that the user has a data subscription, the user shall be able to obtain 3GPP data access by simply inserting his USIM.

4.3 Delivery of MNO service as rich content

The user is used to browsing the web with his handset. He does not understand the difference between accessing third-party web content and that provided by the MNO. In order to give the user a consistent experience Operator A (his operator) makes MNO content available as web content. Some MNO content can be made available either on the Internet or locally on the UE (USIM or ME, or both). User experience of accessing MNO content is the same regardless of where the MNO content is made available.

4.4 Update of applications located on the UE

An operator wants to update a web application located on the UE (USIM or ME, or both) to a new version that will improve the user experience and provide new options for the offered service. The user is prompted that an update is available for the application. The user accepts the update and the remote server establishes a secure connection with the UE to download the data required to update the application.

4.5 Secure applications

The user accesses his private information located in the web (e.g., bank account) and performs a confidential transaction in the web (e.g. a money transfer).The user uses credentials stored on his UE (ME or USIM, or both) to access the secure service.

4.6 USAT application download reducing network traffic overload

In order to reduce the network traffic due to the establishment of GPRS connections for the SMS Push form and also to improve the user experience, some wireless technology present in the handsets (e.g. NFC, Bluetooth, WiFi) could be used.

The user is looking for a USAT application to store in his USIM. The user is in the range of a local wireless access point (e.g. NFC, Bluetooth, WiFi). The local wireless access point is set up for provisioning USAT updates to the UICC by the operator. So, whenever the user is in the range of the local wireless access point, the USAT application can be downloaded and installed to the UICC.

5 Overall considerations

5.1 Power Consumption

As terminal complexity increases over time (e.g. with higher resolution, true colour displays, multiple bearer and dual radio capabilities, multitasking operating systems. etc) UE vendors face an increasing challenge even to maintain existing standby and operation times of their products. Device manufacturers work continuously to optimize power usage in order to reduce the overall power consumption and to maintain competitive stand-by times as functionality increases. The interface between the ME and UICC remains a significant consumer of power, and this is due to two main factors:

1. USIM Presence detection. USIM presence detection is used during calls and as required by applications on the UICC, to ensure that the UICC has not been removed during a card session. It involves the ME sending at an interval determined by the application, a STATUS command on the ME – UICC interface.

2. Proactive USIM polling. Proactive USIM polling occurs when the UE is in Idle Mode and also involves a STATUS command across the interface. In this case, the UICC requests a poll interval from the ME which responds with the maximum interval it will use that is closest to the requested interval.

In each of the above cases, the USIM is required to be active for a short time and hence consumes power. It is currently recommended in the case of Proactive USIM polling that applications on the UICC do not request short time intervals for extended periods in order to avoid an adverse impact on UE battery life. However, in the event that many SIM Toolkit applications are active in the background at the same time, the activity on the card and across the UICC-ME interface will necessarily increase.

Further, the potential use of the high speed Inter-chip USB interface to support some features would itself place an additional burden on the overall power usage of the device. This will become more significant if the interface is used in conjunction with high density memory on the UICC. In this mode typical power consumption is 45 mA (at 3.0 V) and the ME should be able to supply a maximum of 100 mA at 3.3 V [1].

It is desirable to seek to minimise the average power consumption of the USIM whilst at the same time ensuring that the performances of existing features and of any new enhancements are not unacceptably compromised. In addition, consideration will be given to the potential EMC impact that high peak current drain during active phases could have in terminals that have been optimised for lower power consumption. As such, any potential solutions for the use cases are evaluated in terms of their impact on the power usage in the terminal.

5.2 Migration from ISO to USB interface

Currently there are two interfaces defined for the UICC platform: ISO interface [2] and USB interface [3]. The "high speed" interface is currently defined as an option in TS 22.101. Considering the slow adoption of USB interface in the market the migration scenarios from the ISO interface to the USB interface might be examined.

The following migration strategies can be evaluated:

Option 1: starting from Release X and/or date dd.mm.yyyy a ME will be allowed to support all 3GPP features only via USB interface.

Option 2: for some selected 3GPP features the USIM support will only be specified via USB interface. These services should primarily be services for which it is considered that performance over the ISO interface is insufficient.

Option 3: continue to support services on both interfaces and leave the market to decide the interface to be used. For services where it is considered that performance over the ISO interface is insufficient, this should be indicated in the specification of the service.

[5.3 UICC-applications Partial Forward Compatibility

One of the main issues related to the introduction of some new UICC-based features is the need to deliver new UICC cards and the impossibility to reuse legacy cards.

A UICC-applications Partial Forward Compatible system is a system designed to be able to support some data and features included in future releases of the 3GPP standards.

Data and features can be added to legacy UICC cards by using some specific OTA mechanisms and without requiring any new UICC production and distribution. Although technically feasible (depending on the feature), the introduction of a 3GPP Release-(X+1) feature on a UICC Release-X card is currently not specified, is not interoperable and is subject to unexpected behaviour by the UICC.

In order to solve this issue, a UICC-applications Partial Forward Compatibility requirement can be evaluated.

In case the UICC-applications Partial Forward Compatibility feature will be available starting from Release-X onwards, each new 3GPP feature should be evaluated and marked as "Release-(X+N) feature potentially available on Release-X UICC cards" or as "Release-(X+N) feature-only".]

[Editor´s note: the text of this section is still under consideration]

6 Use case considerations

6.1 Service and terminal dependent subscription parameters management

Currently the USIM application provides mechanisms to indicate the Preferred PLMN list to be used with two optional lists respectively indicated as "User Controlled PLMN" and "Operator Controlled PLMN", by also indicating the Preferred Access Technologies for each PLMN. These lists have been historically designed for voice communication roaming. If available in the USIM, these lists provide the guidelines to the ME on how to manage the roaming partner selection automatically for all types of services for the subscription the USIM is linked to.

There are two existing options (1. and 2.) and a potential new solution (3.) to address the requirement:

1. Produce USIM cards specifically designed for the usage with a particular type of service (e.g. a 3G/LTE Notebook with data only subscription) containing the list of the preferred PLMNs for this service.

Formatted: Indent: Left: 0 cm

This solution has at least two drawbacks:

- it implies to produce and distribute USIMs for a dedicated type of service;

- there is no guarantee that these cards could be used for the type of services, for example, for voice communication in a traditional 3G terminal instead of a 3G/LTE Notebooks, unless the MNO blocks the voice services during the customer's provisioning.

2. Produce USIM cards with a common profile and update the USIM profile post issuance via Over-The-Air depending on the service it will preliminary be used for.

Formatted: Indent: Left: 0 cm

This solution relies on the existing technologies (e.g. OTA mechanisms for USIM management, ME features).

The benefits of the solution are:

- potential reuse of legacy USIM cards;

Formatted: Bullets and Numbering

The drawbacks of the solution are:

- need of an OTA platform for initial distribution;

Formatted: Bullets and Numbering

- need of a trigger to detect which USIM cards should be updated;

~~*[Editor's note: drawbacks and benefits FFS]*~~

3. Another solution could be to define a mechanism to store a new service dependent PLMN list on the USIM (for example, for data roaming). This list can be used by the ME for selection of a preferred roaming partner for a particular service (for example, by 3G/LTE Notebook devices, being typically oriented to data communication, or a particular IMS based service).

Formatted: Indent: Left: 0 cm

The benefits of the solution are:

- no need of any OTA platform for initial distribution;

Formatted: Bullets and Numbering

- plug-and-play solution: as soon as the USIM is inserted in the ME, the right list is immediately available;

The drawbacks of the solution are:

- the functionality is available only in new USIM cards;

Formatted: Bullets and Numbering

- new ME features should be supported;

Formatted: Indent: Left: 0 cm

~~*[Editor's note: drawbacks and benefits FFS]*~~

6.2 Delivery of MNO service as rich content

Many operators now offer rich content services (web like interface) to their mobile users. Many technologies exist that may be used by the operators depending upon their service objectives and their deployment strategies.

The options available to present the MNO services as rich content are as follows:

1. Web server on UICC
2. Web-links on the ME to the web server located on the network
3. Integrated ME based applications

Each option can be used independently or they might be combined.

1. Web server on UICC

With the evolution of technology some applications used together with a USIM like for example those based on the SCWS technology (as described in [7]) use multi-media contents to present information to the subscriber. In comparison, the classical STK technology typically presents text-based contents to the user with limited user interactions. SCWS technology based presentation is an improvement to the classical STK technology by delivering rich content to the customer using the Internet technologies.

The benefits of this solution are:

- Limited efforts for development and test of an application due to interoperability
- No expected compatibility issues with ME's in case the ME supports this technology

- Good performance due to application execution on the UE
- High security using standard mechanisms provided by USIM
- Good application portability
- Data can be accessed even without data connection (off-line access for e.g. customer support, help...)
- Fast response time even for large amount of data stored in the UICC, if high speed interface is supported by the ME (USB-IC)
- Scalable as simple applications (a WAP page) to a full-fleshed web-portal can be implemented on the same UICC
- Can be fully controlled/managed/updated by the operator (from activation and during operational phase)

The drawbacks of the solution:

- The deployment is limited to the support of the technology by the ME
- May require the support of the high speed (USB-IC) interface by the ME if large amount of data need be presented to the user, in order to provide a good display time (by reducing the transfer time).
- Technology needs to be supported by UICC
- Size and number of applications limited by available memory size of UICC.
- Frequent remote updates of the applications cause additional data traffic compared to option 2.

2. Web-like links on the ME to the web server located in the network

Another option is to locate the rich content on a central web server and access it using the Internet protocols. The UE stores locally only the links to the content.

The benefits of this solution are:

- Limited efforts for development and test of an application due to interoperability
- Good performance due to application execution on the UE
- Good application portability
- Centralised content management
- Scalable
- No support by USIM mandated

The drawbacks are:

- Response time will depend on the amount of data to be presented and the downlink speed
- Need for development and test of a service to ensure its compliancy with various models of handsets (operator controlled distribution)
- Risk of compatibility issues if a service is accessed from an untested ME (open market)
- Some limitations caused by ME OS and/or application execution platform may arise depending on the complexity of service
- Limited options to develop secure applications

3. ME-based service

The approach to develop dedicated service in form of an application located on the ME or to customize an application available from ME vendors is already being used by some MNO for branded handsets.

The benefits of this solution are:

- No compatibility issues with a selected ME
- High performance due to service execution on the ME
- Data throughput depends only on the communication protocol supported by network and ME

The drawbacks are:

- Availability of handsets will be a direct function of the operator's effort to develop the handsets
- Continuous development and test of a service to make it compliant with various and new models of handsets
- Limited service portability

6.3 Update of applications located on the UE

In the case an application is located on the USIM, the following options are available:

1. "Classical" OTA mechanisms based on SMS bearer as specified in TS 31.116 [4].

   The benefits of this solution are:

   - This mechanism is very well standardized and is widely used

   The drawbacks are:

   - It has some throughput limitation due to its nature (SMS based).
   - With increase of application size this limitation may disturb a MNO service requiring remote management of that application(s).

2. "New" mechanisms

   There are various standardised protocols e.g. BIP/CATP [5] or SCWS "Full Administration Protocol" [7]. Compared with classic OTA, they offer faster mechanisms with at least the same level of security.

   The benefits of this solution are:

   - These protocols allow transfer of a much higher amount of data in a significantly shorter time frame compared to "classical" OTA.

   The drawbacks are:

   - These protocols rely on the high speed interface between ME and USIM which is currently not widely supported by MEs on the market
   - This solution requires either direct IP connectivity with a remote management server or establishment of this connectivity via a gateway on the ME.

   In case an application is located on the ME, standard mechanisms (e.g., OMA DM) can be used to address the application update. These mechanisms are out of scope of this study.

6.4 Secure applications

Applications such as mobile commerce, banking, or access to corporate resources, since they operate with sensitive or confidential data, require an end-to-end encryption between the client and the server.

Currently there are various security mechanisms and secure transport protocols used in the market to protect application data. Some of these mechanisms are standardized by 3GPP (for example GAA), while some are specified by other organisations (OMA, SIMalliance, etc.). Still others are proprietary implementations.

Additionally, the Secure Channel mechanism to secure communication between ME and UICC is specified by ETSI (see [6]).

To provide end-to-end encryption for applications between a server and the UE (consisting of the USIM and the ME) the UE can provide the necessary security features and a secure storage for the related security credentials.

3GPP defined mechanisms for network security (e.g. user authentication) residing on a USIM for the purpose of network (internal) security. There is no standard mechanism defined in 3GPP for secure communication between a UE and an external application, be it on protocol and/or application layer. Such external secure applications, if residing on a USIM, may use any of the available secure communication protocols, commensurate with the type of application involved.

Alternatively the ME could be extended to provide the necessary security functions, but this is out of scope of this study

6.5 USAT application download reducing network traffic overload

The use of contactless interface defined in ETSI TS 102 613 [8] and TS 102 622 [9] for handset capable of some wireless access technology (e.g. NFC, Bluetooth, WiFi) can be useful within the 3GPP framework in order to reduce network traffic for:

- SMS Push for OTA sessions
- Download of Handset configuration parameters

Formatted: Bullets and Numbering

Formatted: Bullets and Numbering

7 Potential requirements

8 Conclusions

8.1 Migration from ISO to USB interface

(Editor´s note – the following text should be reviewed) Currently all the 3GPP features are available both on the ISO interface [2] and USB interface [3], the only difference consisting on the different speed the features are experienced. Up to now, the market has not considered the different user experience as a valuable reason to introduce handsets and/or UICCs supporting both the interfaces. This trend is expected to continue longer and longer.

Formatted: Font: Italic

Annex A (informative): Change history

Change history							
Date	TSG #	TSG Doc.	CR	Rev	Subject/Comment	Old	New
Feb 2011		S1-110294			/tsg_sa/WG1_Serv/TSGS1_53_Nashville/docs/ 14th – 18th February 2011		0.4.0
Aug 2011		n/a			Added info in Change History. Flagged as Rel-12	0.4.0	0.4.1

Formatted Table

Annex B