Technical Specification Group Services and System Aspects
Meeting #28, 06 - 09 June 2005,
Quebec, Canada

TSGS#28(05)0201

3GPP TSG-SA1 Meeting #28
Beijing, China, 04 – 08 April 2005

Tdoc S1-050537

Title: LS on service connectivity provisioning
Release: release 7

Source: 3GPP-SA1
To: OMA-DM; GSMA SCAG
Cc: 3GPP-SA

Contact Person:

Name:	Christophe DUBOIS	Chris FRIEL
Tel. Number:		
E-mail Address:	**cdubois@axalto.com**	**chris.friel@O2.com**

Attachments: S1-050527; S1-050407

---

1. Overall Description:

3GPP-SA1 has been requested by the GSMA to introduce in the 3GPP release 7 specification, requirements to provision service connectivity parameters in the UICC. These requirements have been defined in the attached CR that has been extensively discussed by SA1.

SA1 has been informed that similar work is being done on this in OMA in the Client Provisioning and Device Management activities and we therefore wish to avoid doing duplicate work in 3GPP on this subject. It is not clear, however, if the work in OMA fully meets these requirements. Could you therefore please check that your work can fulfil the requirements in the attached CR.

Specifically SA1 would like to ask the following questions:

1- What is the status of the work on provisioning within DM?
2- Is there any provisioning on the UICC already mandated in OMA-DM specifications?
3- If not, will there be any mandatory provisioning on the UICC and will this be done within 3GPP release 7 time frame?
4- In the case where provisioning on the UICC is defined, or will be defined by OMA within the release 7 time frame, could OMA-DM inform 3GPP-SA1 if the requirements in the attached CR are or will be fully covered by OMA-DM work? Otherwise could you inform us which of our requirements will not be met?

3GPP-SA1 kindly asks OMA-DM to provide answers to the above questions, and to copy them back to 3GPP-SA plenary where they will be considered together with the attached CR.

Also attached is the LS that SA1 received from GSMA SCAG and OMA DM are asked whether or not their ongoing work can fulfil these use cases.

2. Actions:

To OMA-DM group.

ACTION: 3GPP-SA1 asks OMA-DM group to answer the above question and to provide them to SA plenary in addition to SA1.

3. Date of Next TSG-SA1 Meetings:

3GPP SA1 #29 11 – 15 Jul 2005	Povoa de Varzim, PT
3GPP SA1 #30 24 – 28 Oct 2005	Vancouver, CA

3GPP TSG-SA1 Meeting #28
Beijing, China, 04 – 08 April 2005

Tdoc ⌘ S1-050527

CR-Form-v7.1

CHANGE REQUEST

⌘ **22.101** **CR** ⌘ **rev** **-** ⌘ Current version: **7.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ [X] ME [X] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Service connectivity and provisioning
Source:	⌘	Axalto, O2, Gieseke & Devrient, Swisscom, T-Mobile, Gemplus
Work item code:	⌘	TEI7
Date:	⌘	06/04/2005
Category:	⌘	**B**
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
Ph2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
Rel-4 (Release 4)
Rel-5 (Release 5)
Rel-6 (Release 6)
Rel-7 (Release 7)

Reason for change: ⌘

More and more services performed by 3G telecommunication devices require network access, whose configuration requires for examples the indication of an Access Point Name, a list of preferred data bearers with fallback order, a home page, login and password. These services generally involve a user agent or a specific application on the handset. Given the increasing variety of services requiring such network access, the provisioning of these parameters becomes a nightmare for operators when they have to be handled individually for each application, as there is no standard way in 3GPP specifications to manage such information across all possible cases.

A generic mechanism to provision terminals from the smart card is defined in OMA specifications. Provisioning based on the Smart Card is in many cases the most convenient way for the operator to configure the terminals and make them ready to use. The benefits of this mechanism are described in OMA-WAP-ProvSC.

As the USIM provides a standardized platform where provisioning data could be easily and securely managed Over The Air, it is proposed to store the connectivity and application information on the USIM according to OMA-WAP-ProvSC. To increase interoperability, this feature should be mandatory.

Following are some examples of use cases using Smart Cards for provisioning:

Use case 1: Provisioning on used (mis-configured) devices

A Subscriber acquires a Device outside the operator's normal sales lines, e.g. second-hand. An inappropriate configuration in this case is very likely. The only connection to the operator is the smart card, where applicable. The Subscriber's first time use of the Device is detected automatically by the operator's infrastructure.
Alternatively the Subscriber asks explicitly for a configuration parameter set, e.g. by Customer care call or an abbreviated dialling request. The characteristics of the Device (e.g., Device capabilities, resident applications, configuration parameters) are determined and transmitted to the operator's management server. The appropriate provisioning parameters are transferred to the Device; optionally after a confirmation by the Subscriber. In addition User-specific preferences are defined by the User.
Difference to the use cases described above is that here already inserted configuration data has to be overridden; the Device is not in a 'fresh' state, but might be highly mis-configured, so standard values do not necessarily apply.

Use case 2: New hardware or application added to the device
New capabilities can be added dynamically to a device (e.g. plugging an additionnal hardware or installing new application / driver into the terminal). Access parameters may need then to be updated OTA following operator's preferences and stored in the smart card.

Example 1: PoC application downloaded into a Symbian handset.

Example 2: a WLAN module added to a standard 2G or 3G handset. As a new bearer is added for communication, the card can request an update of application parameters from a server. The parameters (e.g. list of preferred data bearers with fallback order) are sent back to the card, allowing an optimised work of the application.

Use case 3: Protect configurations
To store the provisioning parameters in the card can prevent any un-trusted access and modification from a third party.

Use case 4: Browsing optimization
A browsing application has the following fallback order: WLAN, GPRS, CSD. If the user is within a WLAN coverage area, the browser will then use WLAN (providing the handset has WLAN capability). If the user is not under WLAN coverage, the browser will still be able to work using the next bearer in fallback order, which is in this case GPRS.

Summary of change:	⌘	It is proposed to store the network access connectivity profiles on the USIM according to OMA-WAP-ProvSC.
Consequences if not approved:	⌘	

Clauses affected:	⌘	2.1 - 13.1.1 – 13.1.5				
Other specs affected:	⌘	**Y**	**N**	Other core specifications	⌘	31.102
		X				
				Test specifications		
				O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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*.

2.1 Normative references

[1] 3GPP TS 22.105 “Services and Service Capabilities”

[2] 3GPP TS 22.121: "Virtual Home Environment (VHE), Stage 1"

[3] 3GPP TS 22.038: "SIM application toolkit, stage 1"

[4] 3GPP TS 22.001: " Principles of Circuit telecommunication services supported by a Public Land Mobile Network (PLMN)".

[5] 3GPP TS 22.004: General on supplementary services"

[6] 3GPP TS 22.030: "Man-Machine Interface (MMI) of the User Equipment (UE)"

[7] 3GPP TS 22.066: "Support of Mobile Number Portability (MNP); Service description; Stage 1"

[8] 3GPP TS 22.079: " Support of Optimal Routing; Stage 1"

[9] 3GPP TS 22.129: "Handover Requirements between UTRAN and GERAN or other Radio Systems"

[10] 3GPP TS 33.102: "Security Architecture"

[11] 3GPP TS 22.011: "Service Accessibility"

[12] 3GPP TS 22.016: "International mobile Station Equipment Identities (IMEI)"

[13] 3GPP TS 24.008: " Mobile Radio Interface Layer 3 Specification"

[14] 3GPP TS 22.003: "Circuit Teleservices supported by a Public Land Mobile Network (PLMN)"

[15] 3GPP TS 21.133: "Security Threats and Requirements"

[16] 3GPP TS 33.120: "Security Principles"

[17] 3GPP TS 22.042: "Network Identity and Time Zone, Service Description, Stage 1"

[18] 3GPP TS 42.009: " Security Aspects"

[19] 3GPP TS 31.102: "USIM Application Characteristics"

[20] 3GPP TS 23.221 “Architectural Requirements”

[21] 3GPP TS 22.002: “Circuit Bearer Services (BS) supported by a Public Land Mobile Network (PLMN)”

[22] 3GPP TS 22.060: “General Packet Radio Service (GPRS)”

[23] 3GPP TS 29.002: “Mobile Application Part (MAP) specification ”

[24] 3GPP TR 23.972: "Circuit Switched Multimedia Telephony".

[25] 3GPP TS 22.140: "Multimedia messaging service; Stage 1".

[26] 3GPP TS 22.226: “Global Text Telephony, Stage 1.”

[27] 3GPP TS 22.228: "IP multimedia (IM) CN subsystem, stage 1"

[28] RFC 3261: "SIP: Session Initiation Protocol"

[29] 3GPP TR 21.905: “ Vocabulary for 3GPP Specifications”

[30] 3GPP TS 26.233: "Packet Switched Streaming Service (PSS) ; General Description"

[31] 3GPP TS 26.234: "Packet Switched Streaming Service (PSS) ; Protocols and Codecs"

[32] 3GPP TR 22.934: "Feasibility study on 3GPP system to Wireless LAN interworking"

[33] RFC 2486: "The Network Access Identifier"

[34] TS 51.011: "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface", Release 4

[35] TS22.234: "Requirements on 3GPP system to wireless local area network (WLAN) interworking"

[36] 3GPP TS 31.101: "UICC-terminal interface; Physical and logical characteristics"

[37] OMA-WAP-ProvSC: " Provisioning Smart Card Specification "

Note: http://www.openmobilealliance.org/release_program/cp_v11.htm

[…]

13 UICC, USIM and Terminal

This clause defines the functional characteristics and requirements of the User Service Identity Module (USIM) and ISIM (IM Services Identity Module). The USIM/ISIM are applications residing on a UICC.

13.1 The USIM/ISIM and User Profiles

13.1.1 The USIM

Every USIM shall have a unique identity and shall be associated with one and only one home environment.

It shall be possible for a home environment to uniquely identify a user by the USIM.

The USIM shall be used to provide security features.

For access to services, provided by PS or CS CN domains, a valid USIM shall be required. Optionally, SIM according to GSM phase 2, GSM phase 2+, 3GPP release 99, 3GPP release 4 specifications may be supported.

The USIM shall be able to support SIM Application Toolkit as specified in 3GPP TS 22.038 [3].

The USIM shall reside on a UICC. USIM specific information shall be protected against unauthorised access or alteration.

It shall be possible to update USIM specific information via the air interface, in a secure manner.

Access to the IMS services shall be possible using the USIM application in the event of no ISIM being present on the UICC. If an ISIM is present on the UICC it shall be used to access the IMS.

It shall be possible to store provisioning parameters for service connectivity in the USIM for applications known to the mobile operator (e.g. browsing, banking applications, …). The provisioning information shall be defined according to OMA-WAP-ProvSC [37] to ensure interoperability with OMA generic provisioning. A set of service connectivity parameters shall be uniquely identified in such a manner that they are associated exclusively with either one application, or a defined class or suite of applications. If provisioning parameters are present in the USIM for an application, they shall be used in priority to any other corresponding default parameters available in the UE.

Currently those parameters identified are:

- Access Point Name (APN).
- List of preferred data bearers with fallback order. The user shall be informed about application changing bearer, and be given the possibility to refuse it.

It shall be possible to define any additional provisioning parameter as required, if it has not already been identified by OMA as a mandatory parameter.

The user may modify these parameters on the USIM.

In the case where the user has entered his own value for any parameter, the user shall be informed when this parameter is to be updated by the operator, and the user shall be given the possibility to refuse this update.

Annex A describes a number of features that may optionally be supported by the UE and thus USIM.

[…]

13.1.5 The ISIM

Access to the IMS services shall be possible using an ISIM application.

The ISIM shall be sufficient for providing the necessecary security features for the IMS and IMS only.

The ISIM shall reside on a UICC. ISIM specific information shall be protected against unauthorised access or alteration.

It shall be possible to update ISIM specific information via the air interface, in a secure manner.

Note: When accessing IMS over GERAN/UTRAN or I-WLAN using ISIM, a USIM needs also be present to access the rest of the 3GPP system. Alternatively USIM could be used to access IMS.

It shall be possible to store provisioning parameters for service connectivity (as defined in section 13.1.1, above) in the ISIM for applications known to the mobile operator (e.g. browsing, banking applications, …). The provisioning information shall be defined according to OMA-WAP-ProvSC [37] to ensure interoperability with OMA generic provisioning. A set of service connectivity parameters shall be uniquely identified in such a manner that they are associated exclusively with either one application, or a defined class or suite of applications. If provisioning parameters are present in the ISIM for an application, they shall be used in priority to any other corresponding default parameters available in the UE.

It shall be possible to define any additional provisioning parameter as required, if it has not already been identified by OMA as a mandatory parameter.

The user may modify these parameters on the ISIM.

In the case where the user has entered his own value for any parameter, the user shall be informed when this parameter is to be updated by the operator, and the user shall be given the possibility to refuse this update.

SCaG Doc 34_021

LS on Service connectivity and provisioning

Meeting Name & Number: SCaG #34
Meeting Date: 16th – 18th March 2005
Meeting Location: GSMA London
Document Source: SCaG
Document Creation Date:

Document Status:	For Approval	
	For Information	
	For Discussion	x

Circulation Restricted *:	GSM Association:	

Document History:	

N.B. All GSM Association meetings are conducted in full compliance with the GSM Association's anti-trust compliance policy

High Level Document Summary: LS on Service connectivity and provisioning

Title: **LS on Service connectivity and provisioning**

Source: **GSMA SCaG**
To: **3GPP-SA1**

Contact Person:
Name: **Christophe DUBOIS (Axalto)**
E-mail Address: **cdubois@axalto.com**

---

1. Overall Description:

More and more services performed by 3G telecommunication devices require network access, whose configuration requires for example the indication of an Access Point Name, a list of preferred data bearers with fallback order, home page, default login and password. These services generally involve a user agent or a specific application on the handset. Given the increasing variety of services requiring such network access, the provisioning of these parameters becomes a nightmare for operators when they have to be handled individually for each application, as there is no standard way in 3GPP specifications to manage such information across all possible cases.

Following are some examples of use cases using Smart Cards for provisioning:

Use case 1 Bootstrap provisioning on new (un-configured) devices
A smart card is inserted into the Device for the first time.
The smart card contains pre-configured service parameters that enable access to a Service Provider's infrastructure and a key that allows establishing a trust connection to the Device Management system.
The User inserts the smart card into the Device and the Device is provisioned (with optional user interaction) with parameters from the smart card. Upon use, the Device then establishes a relation to the Service Provider's management server in the network.

Use case 2 New services provisioning on already bootstrapped devices
Instead of purchasing a new smart card with a Device, a Subscriber could purchase a service from a Service Provider and have their existing smart card configured with parameters or keys by an entity with Management Authority of the smart card.

Use case 3 Provisioning on used (mis-configured) devices
A Subscriber acquires a Device outside the operator's normal sales lines, e.g. second-hand. An inappropriate configuration in this case is very likely. The only connection to the operator is the smart card, where applicable. The Subscriber's first time use of the Device is detected automatically by the operator's infrastructure.
Alternatively the Subscriber asks explicitly for a configuration parameter set, e.g. by Customer care call or an abbreviated dialling request. The characteristics of the Device (e.g., Device capabilities, resident applications, configuration parameters) are determined and transmitted to the operator's management server. The appropriate provisioning parameters are transferred to the Device; optionally after a confirmation by the Subscriber. In addition User-specific preferences are defined by the User.
Difference to the use cases described above is that here already inserted configuration data has to be overridden; the Device is not in a 'fresh' state, but might be highly mis-configured, so standard values do not necessarily apply.

Use case 4 New jacket or application added to the device
New capabilities can be added dynamically to a device (e.g. plugging a jacket or installing new application / driver into the terminal). Access parameters may need then to be updated OTA following operator's preferences and stored in the smart card.

Example 1: PoC application downloaded into a Symbian handset.

Example 2: a WLAN module added to a standard 2G or 3G handset. As a new bearer is added for communication, the card can request an update of application parameters from a server. The parameters are sent back to the card, allowing an optimised work of the application.

Use case 5 Protect configurations
To store the provisioning parameters in the card can prevent any un-trusted access and modification from a third party.

Use case 6 Personalisation cost saving for handset configuration
Storing these parameters in the smart card could save memory from the handset and therefore allow to reduce its personalisation cost for each country (reducing the final cost of the handset itself).
In particular, this would be very useful considering the GSMA program about Emerging Market Handset deployment.

As 3GPP provides a standardized platform with the USIM where provisioning data could be easily and securely managed Over The Air, GSMA SCaG would like to ask 3GPP-SA1 to consider adding the possibility to store the connectivity and application information on the USIM. To increase interoperability, GSMA SCaG believe that this feature should be mandatory, parameters provisioned on the card having priority over any other contained in the handset.

GSMA SCaG thanks 3GPP-SA1 for their attention and looks forward to a fruitful cooperation with them.

2. Actions:

To 3GPP-SA1 group.

ACTION: GSMA SCaG kindly ask 3GPP-SA1 to consider the above use cases and the possibility of a requirement in 3GPP specifications to store the connectivity and application information on the USIM.

3. Date of Next GSMA SCaG Meeting:

1st -3rd June 2005