TSG CORRESPONDENCE

Mr. Nick Yamasaki
Chair, 3GPP2 TSG-S
KDDI
GARDEN AIR TOWER
3-10-10, Iidabashi, Chiyoda-ku
Tokyo 102-8460 Japan

tsgs_chair@3gpp2.org

26 May 2011

Dr. Klaus Vedder
Chair, ETSI SCP
klaus.vedder@gi-de.com

c/o Mr. Xavier Piednoir
Support Officer, ETSI SCP
xavier.piednoir@etsi.org

RE: New Work Item for eUICC

Dear Dr. Vedder,

As a follow-up to our earlier response correspondence on the same subject dated 31 March, 2011, upon completing a more detailed analysis, we have the following questions:

1. Is the eUICC intended to be a new physical platform or form factor (in addition to the UICC and Machine to Machine (M2M) UICC [ETSI TS 102 671])?
2. Does ETSI SCP intend to differentiate the eUICC from other UICC types such as M2M UICC and removable UICC?
    a. If yes, how does ETSI SCP intend to differentiate the eUICC
    b. If no, would any smart card with the proposed subscription download capability be differentiated from smart cards that do not have this capability
3. Is it ETSI SCP's intent to replace existing OTA card management technologies, enhance those technologies, or create a new technology to manage subscriptions?

Regarding the question 3, we attach at the end of this correspondence an outline of existing capabilities for the storage of credentials on the mobile station and the Over-the-Air (OTA) management of them along with the reference to the related specifications published by 3GPP2.

Though OTA management of credentials is possible in cdma2000 networks using OTASP, IOTA & CCAT, 3GPP2 acknowledges their limitations in supporting some of the emerging use cases and deployment needs identified for embedded devices (e.g., need for manual intervention, OTASP does not work when roaming, impossibility to download credential application(s) used for access authentication, etc.).

3GPP2 will keep you informed of any specific requirements as we continue to address this work. A Work Item has been initiated to develop the system requirements.

Please also note that, having completed the detailed analysis of the set of requirements drafted by GSMA, we are forwarding some questions and comments, as well as editorial suggestions to GSMA Task Force, on which you are copied. We generally consider the GSMA document comprehensive and have not identified any additional use cases at this time. If we do identify any additional use cases or requirements as part of the progress of the agreed 3GPP2 Work Item regarding system requirements development for downloadable credentials, we will provide that information to you.

We look forward to continued collaboration with this work, and would appreciate getting apprised of any further developments.

Regards,

Nick Yamasaki
Chair, 3GPP2 TSG-S

cc:	Ms. Cheryl Blum	Chair, 3GPP2 SC	cblum@tiaonline.org
	Ms. Victoria Mitchell	3GPP2 Senior Manager	vmitchell@tiaonline.org
	Dr. Frankle Zhao	Chair, 3GPP2 TSG-A	tsga_chair@3gpp2.org
	Dr. Edward Tiedemann	Chair, 3GPP2 TSG-C	tsgc_chair@3gpp2.org
	Dr. Marvin Bienn	Chair, 3GPP2 TSG-X	tsgx_chair@3gpp2.org
	Mr. Enrico Scarrone	Chair, 3GPP TSG-SA1	enrico.scarrone@TELECOMITALIA.IT
	Mr. Balazs Bertenyi	Chair, 3GPP TSG-SA	balazs.bertenyi@nsn.com
	Mr. Heiko Kruse	Chair, 3GPP TSG-CT6	Heiko.Kruse@morpho.com
	<GSMA Embedded SIM Task Force Representative>		prd@gsm.org

Attachment

This attachment provides an outline of existing capabilities for the storage of credentials on the mobile station (MS) and the Over-the-Air (OTA) management of them along with references to the related specifications published by 3GPP2.

Storage of cdma2000 Credentials

Two options for storage of credentials are supported in cdma2000 standards:

Option 1: In non-volatile memory within the mobile station (sometimes referred to as User Identity Module or UIM), which is an integral part of the mobile station and is non removable. The credentials can be one or more of the following:

- cdma2000 1x and HRPD credentials
    - For cdma2000 1x: MIN/IMSI, A-key for CAVE authentication, K key for AKA authentication.
    - For HRPD: NAI (Network Access Identifier), shared secret associated with NAI, and the authentication algorithms.
- eHRPD (Evolved HRPD) credentials
    - USIM credential equivalents, such as Ki & IMSI, "f" functions required for AKA, etc.
    - eHRPD credentials required for 3GPP AKA authentication to 3GPP EPC (Evolved Packet Core).

  Note that an eHRPD device may not support UICC. In that case the 3GPP AKA profile required by the device is specified in cdma2000 specifications, e.g., X.S0057.
- IMS Credentials on UIM (e.g., equivalent to ISIM/USIM credentials required for IMS access or SIP Digest/ TLS credentials)

Option 2: In a removable smartcard module

- R-UIM (Removable UIM) or CSIM on UICC (cdma2000 Application)
- USIM on UICC for eHRPD access
- ISIM on UICC

OTA Management of cdma2000 Credentials

The cdma2000 credentials on the MS can be managed using one of the following:

(1) Over-the-Air Service Provisioning Protocol (OTASP) specified in C.S0016
(2) IP OTA-Device Management (IOTA-DM) specified in C.S0064
(3) IP OTA-Handset Configuration Management (IOTA-HCM), specified in C.S0040

(1) OTASP

OTASP uses cdma2000 1x as the transport to manage credentials and other information on the MS, on the smartcard (R-UIM or CSIM on UICC), or both.

OTASP does not require any pre-provisioned credentials specific to cdma2000 network on the MS, in contrast to the R-UIM/CSIM or equivalent in the UIM. Device specific credentials (e.g., MEID, Service Programming Code, etc.) are used to open the cellular channel necessary for provisioning. Until the device is provisioned with the necessary subscription information, the MS can not use any other service.

(2) and (3) IOTA-DM and IOTA-HCM

IOTA-DM and IOTA-HCM use IP transport to manage credentials and other information on the MS or the smartcard (R-UIM or CSIM on UICC, or both).

OTAPA messages are encapsulated as OMA-DM messages over IP transport. This does not require any pre-provisioned credential application on the MS such as R-UIM/CSIM or equivalent in the UIM. Device can use any available IP connection (e.g., HRPD or 1x data).

In addition to the above, cdma2000 Card Application Toolkit (CCAT defined in C.S0078 / C.S0079) supports managing information on removable smartcards (i.e., R-UIM or UICC). However, CCAT cannot be used to manage information on the UIM/MS.

Further Information

The specifications referenced here are available at:
http://www.3gpp2.org/Public_html/specs/alltsgscfm.cfm