3GPP TSG-SA3 Meeting #29
San Francisco, USA, 15-18 July 2003

Tdoc ⌘S3-030342

CR-Form-v7

CHANGE REQUEST

⌘	**SpecNumber**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	**0.2.0**	⌘

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⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Protocol C in stage 3 detail		
Source:	⌘	Nokia		
Work item code:	⌘	SEC1-SC	***Date:*** ⌘	30/06/2003
Category:	⌘		***Release:*** ⌘	Rel-6

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:

2	*(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)*

Reason for change: ⌘ Current specification TS does not contain the protocol C transaction in detail. This CR completes the TS by adding the missing application logic description to the Bootstrapping procedure.

Summary of change: ⌘ Protocol C is given in stage 3 detail in following approach:

- The Cx interface Command-Codes are used. The Bootstrapping application logic, is used, instead of IMS MM application logic. Vendor-Specific-Application-Id AVPs indicates 3GPP as the vendor.
- The user's Subscriber Certificate profile is downloaded from HSS using an upgraded IMS User-Name AVP.

Consequences if not approved: ⌘ Implementation detail is missing.

Clauses affected: ⌘ 2, 3.2, 3.3, 4.3

		Y	**N**		
Other specs affected:	⌘		**X**	Other core specifications	⌘
			X	Test specifications	
			X	O&M Specifications	

Other comments: ⌘

2 References

The following documents contain provisions that, 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*.

[<seq>] <doctype> <#>[([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

[1] 3GPP TR 41.001: "GSM Release specifications".

[2] 3GPP TR 21.912 (V3.1.0): "Example 2, using fixed text".

[3] 3GPP TS 31.102: "Characteristics of the USIM Application".

[4] 3GPP TS 33.102: "Security Architecture".

[5] 3GPP TS 23.003: " Numbering, addressing and identification".

[6] 3GPP TS 29.228: "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents"; (Release 5); V5.3.0 (2003-03).

[7] 3GPP TS 29.229: "Cx and Dx interfaces based on the Diameter protocol"; Protocol details; (Release 5); V5.3.0 (2003-03).

[DIAMETER] draft-ietf-aaa-diameter-17.txt, internet draft, IETF aaa working group.

[PKCS10] "PKCS#10 v1.7: Certification Request Syntax Standard", RSA Laboratories, May 2000.

[RFC2510] Adams C., Farrell S., "Internet X.509 Public Key Infrastructure Certificate Management Protocols", RFC 2510, March 1999.

[RFC2511] Myers M., et al., "Internet X.509 Certificate Request Message Format", RFC 2511, March 1999.

[RFC2527] Chokhani S., et al, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 2527, March 1999.

[RFC2617] Franks J., et al, "HTTP Authentication: Basic and Digest Access Authentication", RFC 2617, June 1999.

[RFC3280] Housley R., et al, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC 3310] A. Niemi, et al, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)", RFC3310, September 2002.

[WAPCert] WAP-211-WAPCert, 22.5.2001: http://www1.wapforum.org/tech/terms.asp?doc=WAP-211-WAPCert-20010522-a.pdf

[WIM] WAP-260-WIM-20010712, 12.7.2001: http://www1.wapforum.org/tech/documents/WAP-260-WIM-20010712-a.pdf

[WPKI] WAP-217-WPKI, 24.4.2001: http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf

[X.509] ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8:1997, "Information Technology - Open Systems Interconnection - The Directory: Authentication Framework", 1997.

********** NEXT CHANGE ***********

3.2 Symbols

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

{ }	Mandatory AVP in the Diameter messages
[ ]	Optional AVP in the Diameter messages
*	Multiple instances of the AVP possible in the Diameter messages

3.3 Abbreviations

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

AK	Anonymity Key
AKA	Authentication and Key Agreement
AUTN	Authentication token
AV	Authentication Vector. 3GPP AV=[RAND,AUTN,XRES,CK,IK].
AVP	Attribute-Value-Pair in Diameter messages.
BSF	Bootstrapping server functionality BSF is hosted in a network element under the control of an MNO.
BSP	BootStrapping Procedure
CA	Certificate Authority
CK	Confidential Key
CMP	Certificate Management Protocols
FQDN	Full Qualified Domain Name in URI (e.g. http://FQDN:80)
HSS	Home Subscriber System
IK	Integrity Key
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
MNO	Mobile network operator
NAF	Operator-controlled network application function functionality. NAF is hosted in a network element under the control of an MNO.
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
RAND	Random challenge in authentication
REQ	In Diameter header indicates that the message is a Request.
SCP	Subscriber Certificate Procedure
UE	User Equipment
XRES	Expected response in authentication

********** NEXT CHANGE ***********

4.3.1.2 Protocol C

The Bootstrapping C interface performs the retrieval of an authentication vector and user profile data by BSF from the HSS. The procedure corresponds to the step 3 to 5 in Figure 3, and is defined in detail as below:

3. The BSF shall send the following Bootrstrapping request to the HSS in format of Multimedia-Auth-Request (MAR) message. The content of the message is given below in the same format as in [7]. The curly brackets indicate it is a mandatory AVP. The square brackets indicate it is an optional AVP. The address refers to the Fully Qualified Host Name (FQDN).

```
< Multimedia-Auth-Request> ::=<Diameter Header: 303, REQ >
                              < Session-Id >
                              { Vendor-Specific-Application-Id }
                              { Auth-Session-State }                   ; NO_STATE_MAINTAINED
                              { Origin-Host }                          ; Address of BSF
                              { Origin-Realm }                         ; Realm of BSF
                              { Destination-Realm }                    ; Realm of HSS
                              [ Destination-Host ]                     ; Address of the HSS
                              { User-Name }                            ; IMPI from UE
                              { Public-Identity }                      ; Empty value
                              [ SIP-Auth-Data-Item ]                   ; Omitted
                              [ SIP-Number-Auth-Items]                 ; value "1".
                              [ Server-Name ]                          ; Omitted
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

The content of Vendor-Specific-Application-ID according [DIAMETER] section 6.11 is:

```
<Vendor-Specific-Application-Id>::=<AVP header: 260>
        1*  [Vendor-Id]                              ; 3GPP is 10415
        0*1 {Auth-Application-Id}                    ; value for BS is FFS
        0*1 {Acct-Application-Id}                    ; Omitted
```

When determining the value of Destination-Host AVP the BSF can use redirector function (SLF) to resolve the address of the HSS if needed (see [7], section 5.5). The BSF may set the Auth-Session-State AVP to NO_STATE_MAINTAINED to inform that the HSS does not need to maintain any status information for this session according [7] section 5.3. The User-name is the IMS Private User Identity (IMPI) as required in [6] section 6.1.3. The mandatory Public-Identity may be set to contain non-meaningful "empty" value because the HSS application logic of the Bootstrapping does not check, as IMS MM application does, coherence of the IMPI and the User Public Identity (IMPU). Because the bootstrapping procedure requires only one authentication vector the SIP-Number-Auth-Items AVP may be omitted or set to 1 (default) according [7] section 6.3.12. The optional Server-Name AVP may be omitted.

4. When the HSS receives the MAR message, the HSS shall derive the user Authentication Vector (AV) information according the IMPI and populates into SIP-Auth-Data AVP defined in [6]. The HSS shall also fetch the user profile (e.g. Subscriber Certificate profile) and populates it to the IMS User-Data AVP defined in [6] and [7].

Ecditor's note: This requires an addition to XML schema of User-Data AVP defined in [6]. This updating is not yet accepted or contributed. Another alternative is to define a new AVP for user profile.

5. The HSS shall send the following Bootstrapping response in format of Multimedia-Auth-Answer (MAA) message back to the BSF.

```
< Multimedia-Auth-Answer> ::= < Diameter Header: 303 >
                              < Session-Id >
                              { Vendor-Specific-Application-Id }
                              [ Result-Code ]
                              [ Experimental-Result]
                              { Auth-Session-State }                  ; NO_STATE_MAINTAINED
                              { Origin-Host }                         ; Address of HSS
                              { Origin-Realm }                        ; Realm of HSS
                              [ User-Name ]                           ; IMPI
                              [ Public-Identity ]                     ; Omitted
                              [ SIP-Number-Auth-Items ]               ; value "1"
                              *[ SIP-Auth-Data-Item ]                 ; Contains one user's AV info
                              [ User-Data ]                           ; User profile
                              *[ AVP ]
                              *[ Proxy-Info ]
                              *[ Route-Record ]
```

The HSS shall set the mandatory Auth-Session-State AVP to NO_STATE_MAINTAINED to inform that the HSS does not require the BSF to maintain any status information. The User-name AVP (IMPI) may be sent back for checking. The only required authentication vector is send in the SIP-Auth-Data-Items AVP and the AVP SIP-Number-Auth-Items AVP may be omitted or set to 1 (default).

The MAR/MAA sequence in the C interface must not change possible status information of the possible simultaneously ongoing IMS MM application sessions.

When the BSF receives the MAA message, the BSF stores temporarily the tuple <IMPI,XRES,CK,IK,UserProfile> for further use inside the bootstrapping procedure.