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 D 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 D transaction in detail. This pseudo-CR completes the TS by adding the missing application logic description into the NAF using Bootstrapping procedure.
Summary of change:	⌘	Protocol D is given in stage 3 detail, in similar approach as that for Protocol C.
Consequences if not approved:	⌘	Implementation detail is missing.

Clauses affected:	⌘	4.3.2

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

Other comments: ⌘

4.3.2 Procedures using bootstrapped Security Association

After UE is authenticated with the BSF, every time the UE wants to interact with an NAF the following steps are executed as depicted in Figure 4:

UE starts protocol B with the NAF

- In general, UE and NAF will not yet share the key(s) required to protect protocol B. If they already do, there is no need for NAF to invoke protocol D.
- It is assumed that UE supplies sufficient information to NAF, e.g. a transaction identifier, to allow the NAF to retrieve specific key material from BSF.
- The UE derives the keys required to protect protocol B from the key material.

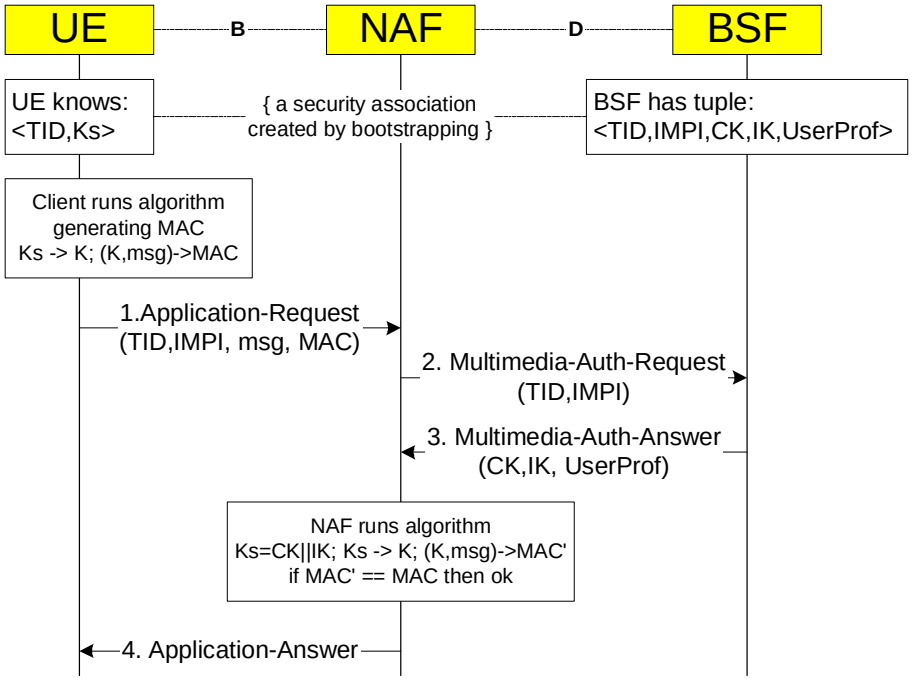
NAF starts protocol D with BSF

- The NAF requests key material corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier) in the start of protocol B.
- The BSF supplies to NAF the requested key material.
- The NAF derives the keys required to protect protocol B from the key material in the same way as the UE did.

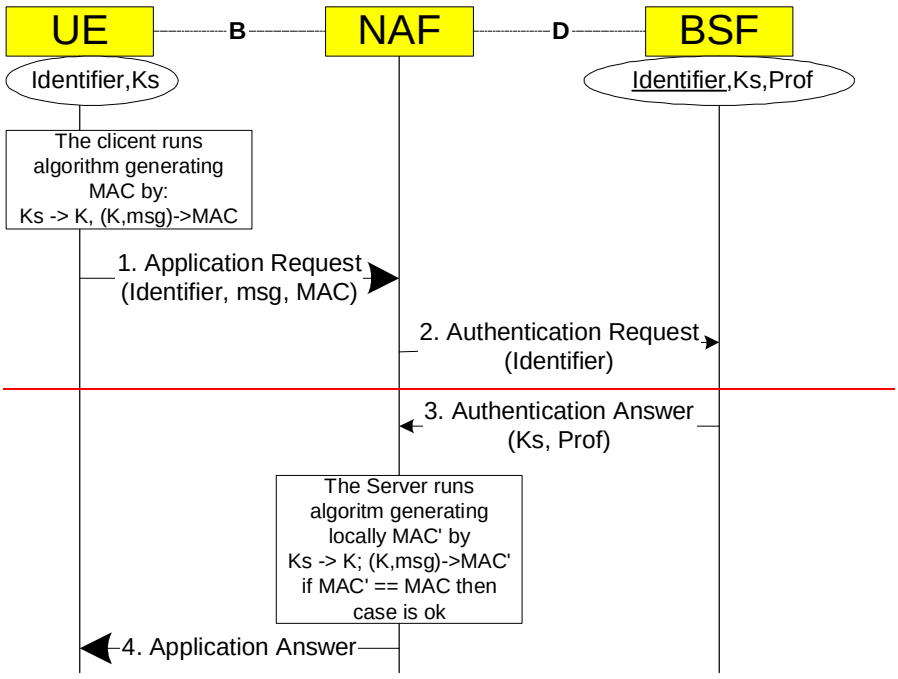
NAF continues protocol B with UE

Once the run of protocol B is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to run protocol B in a secure way.

Editor's note: Message sequence diagram presentation and its details in protocol B will be finalized later.



MAC represents all credentials **msg** is appl. specific dataset
UserProf is application specific part of user profile



MAC represents all credentials **msg** is appl. specific dataset
Prof is application specific part of user profile

Figure 1: The bootstrapping usage procedure

4.3.2.1 Protocol D

The protocol D performs the retrieval of an authentication vector and user profile data by NAF from BSF. The application procedure of protocol D part refers to step 2 and 3, which are defined in stage 3 details as below:

2. The NAF shall send Authentication Request in the format of Multimedia-Auth-Request (MAR) message to the BSF. The content of the message is given here in the same format as in [7]. The curly brackets indicate mandatory AVP. The square brackets indicate 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 NAF
                    { Origin-Realm }                        ; Realm of NAF
                    { Destination-Realm }                   ; Realm of BSF
                    [ Destination-Host ]                    ; Address of the BSF
                    { 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 appl. is FFS
      0*1 {Acct-Application-Id}                         ; Omitted
```

The User-Name is the IMPI from send by the UE.

Editor's note: The transfer of the Transaction Identity (TID) (base 64 coded octet string) is FFS. It may be sent in concatenation with the IMPI in User-Name AVP or as its own AVP.

The Destination-Realm is derived from realm part of the IMPI. When determining the value of Destination-Host AVP in home network the NAF can use redirector function (SLF) to resolve the address of the BSF if needed (see [7] section 5.5). The derivation of the Destination-Host in the visited network case is FSS.

The NAF may set the Auth-Session-State AVP to NO_STATE_MAINTAINED to inform that the BSF 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 application 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.

3. In the successful case the BSF has a tuple <TID,IMPI,CK,IK,UserProf> identified by Transaction Identity (TID). When the BSF receives the MAR it checks the existence of the tuple and matches the stored and received IMPIs. If checking fails the BSF sends Multimedia-Auth-Answer (MAA) with Result-Code set to indicate the error type. In successful case the Result-Code is set to 2xxx as defined in [DIAMETER].

The BSF derives the user authentication vector information according the IMPI and packs in into SIP-Auth-Data AVP defined in [6]. The HSS fetches also the user profile (e.g. Subscriber Certificate profile) and packs it to the IMS User-Data AVP defined in [6] and [7].

Editor's note: This requires an addition to XML schema of User-Data AVP defined in [TS 29.228]. This updating is not yet accepted or contributed. Another alternative is to define a new AVP for user profile.

After that the BSF shall send the Authentication Answer in format of the following Multimedia-Auth-Answer (MAA) message back to the NAF.

```
< Multimedia-Auth-Answer> ::= < Diameter Header: 303 >
                              < Session-Id >
                              { Vendor-Specific-Application-Id }
                              [ Result-Code ]                          ; 2xxx in successful case
                              [ Experimental-Result]
                              { Auth-Session-State }                   ; NO_STATE_MAINTAINED
                              { Origin-Host }                          ; Address of BSF
                              { Origin-Realm }                         ; Realm of BSF
                              [ 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 BSF should set the mandatory Auth-Session-State AVP to NO_STATE_MAINTAINED to inform that the BSF does not require the NAF 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).

When the MAA message is send the BSF can remove the tuple <TID,IMPU,CK,IK,UserProf> stored by bootstrapping procedure.