3GPP TSG SA WG3 Security — S3#31
18-21 November 2003, Munich, Germany

Tdoc ⌘S3-030728

CR-Form-v7

CHANGE REQUEST

⌘	**33.220**	**CR**	**CRNum**	⌘**rev**		⌘ Current version:	**0.1.1** ⌘

*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:	⌘	Bootstrapping procedure: merging of last two messages			
Source:	⌘	Nokia			
Work item code:	⌘	Support for Subscriber Certificates	***Date:***	⌘	29/10/2003
Category:	⌘	**F**	***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:	⌘	HTTP response cannot be sent without HTTP request. Therefore the last message supplying the transction identifier by BSF to UE (step 9) must be merged with HTTP 200 OK message (step 7).
Summary of change:	⌘	Merges last two messages sent from BSF to UE.
Consequences if not approved:	⌘	Message in step 9 cannot be sent from BSF to UE.

Clauses affected:	⌘	4.3.1				
		Y	**N**			
Other specs	⌘	**X**		Other core specifications	⌘	CN1 spec 24.def (but it already contains the change)
affected:			**X**	Test specifications		
			X	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.

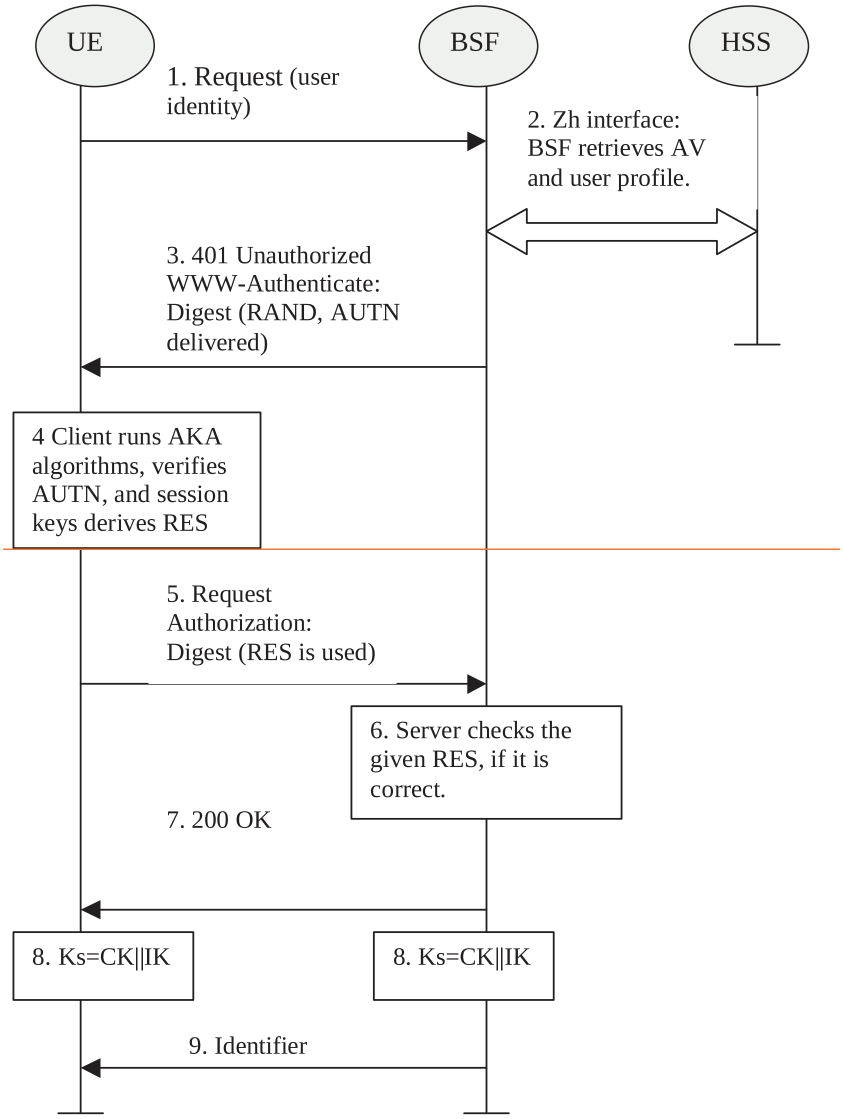
************ BEGIN CHANGE *************

4.3.1 Bootstrapping procedures

When a UE wants to interact with an NAF, and it knows that bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see Figure 1)

Editor's notes: Zh interface related procedure will be added here in future development. It may re-use Cx interface that is specified in TS 29.228.

Otherwise, the UE shall perform a bootstrapping authentication only when it has received bootstrapping initiation required message or a key update indication from the NAF (cf. subclause 4.3.2).


UE
BSF
HSS
1. Request (user identity)
2. Zh interface: BSF retrieves AV and user profile.
3. 401 Unauthorized WWW-Authenticate: Digest (RAND, AUTN delivered)
4 Client runs AKA algorithms, verifies AUTN, and session keys derives RES
5. Request Authorization: Digest (RES is used)
6. Server checks the given RES, if it is correct.
7. 200 OK
8. Ks=CK||IK
8. Ks=CK||IK
9. Identifier

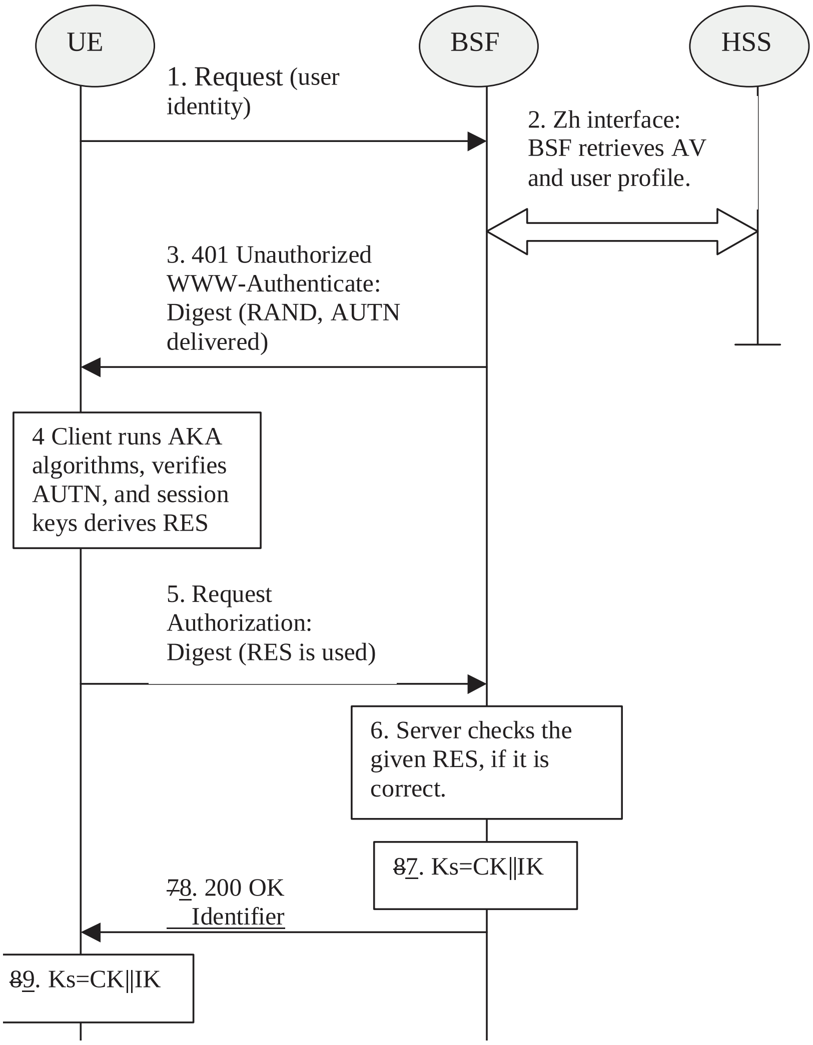

UE
BSF
HSS
1. Request (user identity)
2. Zh interface: BSF retrieves AV and user profile.
3. 401 Unauthorized WWW-Authenticate: Digest (RAND, AUTN delivered)
4 Client runs AKA algorithms, verifies AUTN, and session keys derives RES
5. Request Authorization: Digest (RES is used)
6. Server checks the given RES, if it is correct.
~~8~~7. Ks=CK||IK
~~7~~8. 200 OK Identifier
~~8~~9. Ks=CK||IK

Figure 1: The bootsrapping procedure

1. The UE sends an HTTP request towards the BSF.

2. BSF retrieves the user profile and a challenge, i.e. the Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) over Zh interface from the HSS.

3. Then BSF forwards the RAND and AUTN to the UE in the 401 message (without the CK, IK and XRES). This is to demand the UE to authenticate itself.

4. The UE calculates the message authentication code (MAC) so as to verify the challenge from authenticated network; the UE also calculates CK, IK and RES. This will result in session keys IK and CK in both BSF and UE.

5. The UE sends request again, with the Digest AKA RES as the response to the BSF.

6. If the RES equals to the XRES that is in the AV, the UE is authenticated.

7. BSF generates key material Ks by concatenating CK and IK. Ks is used for securing the Ua interface.

~~7~~8. The BSF shall send 200 OK message and shall supply a transaction identifier to the UE to indicate the success of the authentication.

~~8~~9. The key material Ks is generated in ~~both BSF and~~ UE by concatenating CK and IK. The Ks is used for securing the Ua interface.

Editor's note: The key material Ks is 256 bits long. It is up each NAF to make the usage of the key material specifically.

~~9. BSF may supply a transaction identifier to UE in the cause of Ub interface.~~

************ END CHANGE *************