3GPP TSG-SA3 Meeting #32
Edingburgh, Scotland, 9-13 February, 2004

Tdoc ⌘S3-040064

CR-Form-v7

CHANGE REQUEST

⌘ **33.220** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **1.0.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	'n' parameter in bootstrapping phase
Source:	⌘	Ericsson
Work item code:	⌘	GBA
Date:	⌘	27/01/2004
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:	⌘	The 'n' parameter is optional to be included from the BSF to the UE in the bootstrapping phase. A clarification has been added that the BSF shall always include parameter 'n' to the UE if key derivation shall take place. If the parameter *n* is not supplied then no key derivation is performed in the BSF or the UE, i.e. Ks = Ks_NAF. Also a requirement has been added that BSF shall use the same value in parameter 'n' for all NAFs. The value in parameter 'n' may be changed over time.
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.3.2

Other specs affected: ⌘	Y	N		
			Other core specifications	⌘
			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.

4.3.2 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 4)

Editor's note: 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 4.3.3).

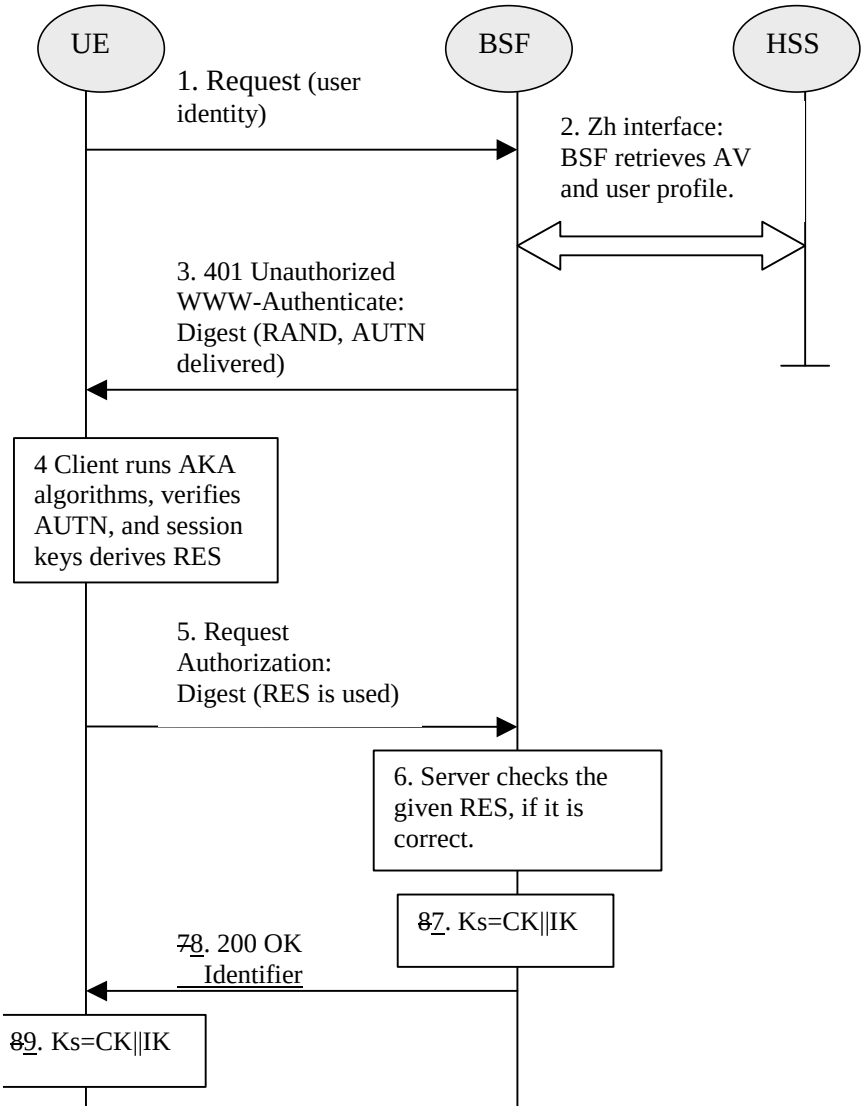

Figure 4: The bootstrapping procedure

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 to derive the key material Ks_NAF. Ks_NAF is used for securing the Ua interface.

8. The BSF shall send 200 OK message and shall supply a transaction identifier to the UE to indicate the success of the authentication. If key derivation shall be performed in the BSF and the UE, then t~~T~~he BSF shall~~may~~ also supply the parameter *n* used to determine the NAF_Id_n (cf. previous bullet) to the UE over the Ub interface. If the parameter *n* is not supplied then no key derivation is performed in the BSF and UE, i.e. Ks = Ks_NAF. BSF shall use the same value in parameter n for all NAFs. The value of parameter n may be changed over time.

9. The key material Ks is generated in UE by concatenating CK and IK. The Ks is used to derive the key material Ks_NAF. Ks_NAF is used for securing the Ua interface.

Ks_NAF is computed as Ks_NAF = KDF (Ks, key derivation parameters), where KDF is a suitable key derivation function, and the key derivation parameters include the user's IMSI, the NAF_Id_n and RAND. The NAF_Id_n consists of the n rightmost domain labels in the DNS name of the NAF, separated by dots (n= 1, ..., 7). For n = 0, NAF_Id_n equals the full DNS name of the NAF. The next bullet specifies how the UE obtains n.

NOTE: This note gives an example how to obtain the NAF_Id_n: if the DNS name of the NAF is "server1.presence.bootstrap.operator.com", and n = 3, then NAF_Id_n = " bootstrap.operator.com".

Editor's note: The definition of the KDF and the possible inclusion of further key derivation parameters is left to ETSI SAGE.