3GPP TSG-SA WG3 Meeting #36
Shenzhen, China, November 23-26, 2004

Tdoc ⌘S3-041089

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.220** **CR** **043** ⌘ **rev** **1** ⌘ Current version: **6.2.0** ⌘

*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:	⌘	No GUSS/USS update procedures in Release-6
Source:	⌘	SA WG3
Work item code:	⌘	GBA-SSC
Date:	⌘	16/11/2004
Category:	⌘	**C**
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:
Ph2 (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)
Rel-7 (Release 7)

Reason for change:	⌘	The possible GUSS/USS update procedures are mentioned in editor's notes. As the Release-6 is freezing and no studies have been made regarding the details and possible implications of GUSS/USS update procedure, the update procedure is postponed to Release-7. In Release-6, the GUSS in the BSF is updated as part of the bootstrapping procedure with the BSF, and USSs in the NAF when it is fetching a new NAF specific key over Zn reference point.
Summary of change:	⌘	- 4.4.5 and 4.4.6: GUSS update in BSF and USS update in NAF are done by using the existing method, i.e., the BSF gets the updated version of the GUSS when it next time fetches the authentication vectors and GUSS from the HSS, or when NAF fetches a new USS from the BSF when it receives a new B-TID from the UE. The possible update procedure initiated by the HSS may be defined in future releases.
Consequences if not approved:	⌘	

Clauses affected:	⌘	4.4.5, 4.4.6

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

Other comments:	⌘	

==== ***BEGIN CHANGE*** ====

4.4.5 Requirements on reference point Zh

The requirements for reference point Zh are:

- mutual authentication, confidentiality and integrity shall be provided;

NOTE 1: This requirement may be fulfilled by physical or proprietary security measures if BSF and HSS are located within the same operator's network.

- the BSF shall be able to send bootstrapping information request concerning a subscriber;
- the HSS shall be able to send 3GPP AKA vectors to the BSF in batches;
- the HSS shall be able to send the complete set of subscriber's GBA user security settings needed for security purposes to the BSF;

~~Editor's note: It's ffs how to proceed in the case where GBA user security settings are updated in HSS after GBA user security settings were forwarded. The question is whether this profile change should be propagated to BSF.~~

NOTE 2: If subscriber's GUSS is updated in HSS, this is not propagated to the BSF. The GUSS in the BSF is updated when the BSF next time fetches the authentication vectors and GUSS from the HSS over Zh reference point as part of the bootstrapping procedure.

- no state information concerning bootstrapping shall be required in the HSS;
- all procedures over reference point Zh shall be initiated by the BSF;

~~Editor's note: This requirement may need to be modified depending on what happens in the case where the GBA user security settings in the HSS is updated.~~

- the number of different interfaces to HSS should be minimized.

4.4.6 Requirements on reference point Zn

The requirements for reference point Zn are:

- mutual authentication, confidentiality and integrity shall be provided;
- If the BSF and the NAF are located within the same operator's network, the Zn reference point shall be secured according to NDS/IP [13];
- If the BSF and the NAF are located in different operators' networks, the Zn' reference point between the D-Proxy and the BSF shall be secured using TLS as specified in RFC 2246 [6];

Editor's Note: The TLS Certificate profiling needs to be completed and will be added into an Annex.

- The BSF shall verify that the requesting NAF is authorised;
- The NAF shall be able to send a key material request to the BSF, containing NAF's public hostname used by the UE's corresponding request. The BSF shall be able to verify that a NAF is authorized to use this hostname, i.e. the FQDN used by UE when it contacts the NAF;
- The BSF shall be able to send the requested key material to the NAF;
- The NAF shall be able to get a selected set of application-specific user security settings from the BSF, depending on the policy of the BSF and the application indicated in the request from the NAF over Zn;
- The NAF shall be able to indicate to the BSF the single application or several applications it requires user security settings for;

NOTE 1: If some application needs only a subset of an application-specific user security setting, e.g. only one IMPU, the NAF selects this subset from the complete set of user security settings sent from BSF.

- The BSF shall be able to configure on a per NAF or per application basis if private subscriber identity and which user security settings may be sent to a NAF;

- The BSF shall be able to indicate to the NAF the lifetime of the key material. The key lifetime sent by the BSF over Zn shall indicate the expiry time of the key, and shall be identical to the key lifetime sent by the BSF to the UE over Ub.

NOTE 2: This does not preclude a NAF to refresh the key before the expiry time according to the NAF's local policy.

~~Editor's note: It is ffs which actions are to be taken over Zn when the BSF receives a user security settings update from the HSS over Zh.~~

NOTE 3: If one or more of the USSs that have been delivered to the NAF has been updated in subscriber's GUSS in the HSS, this change is propagated to the NAF the next time it fetches the USS from the BSF over Zn reference point (provided that the BSF has updated subscriber's GUSS from the HSS over Zh reference point).

==== *END CHANGE* ====