3GPP TSG-SA WG3 SECURITY Meeting #36 ***Tdoc ⌘ S3-040934***
Shenzhen, China, 23-26 November 2004

CR-Form-v7.1

CHANGE REQUEST

⌘ **33.220 CR 032** ⌘**rev -** ⌘ 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 **X**

Title:	⌘	Update of GUSS
Source:	⌘	Huawei
Work item code:	⌘	SEC1-SC
Date:	⌘	11/11/2004
Category:	⌘	**C**
Release:	⌘	R6

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:	⌘	In the current TS 33.220, it doesn't describe the update of GUSS. After the GUSS is updated in the HSS, it's necessary to keep consistent between the BSF and HSS to avoid to affect the service by a big delay.
Summary of change:	⌘	When the GUSS is changed in HSS, the HSS will notify the BSF, but HSS don't wait the answer from the BSF, and it's up to the BSF whether it will update the GUSS or not. Adding a procedure for the GUSS update.
Consequences if not approved:	⌘	The BSF can't update the GUSS when the GUSS is changed in the HSS. It will affect the application service.

Clauses affected:	⌘	4.2.3, 4.4.5, 4.4.6 , 4.5.5(*new*), 5.3.5(*new*)

		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	29.109
			X	Test specifications		
			X	O&M Specifications		

Other comments:	⌘	

**********Begin of change**********

4.2.3 HSS

The set of all user security settings (USSs) is stored in the HSS. There shall be at most one USS per application stored in the HSS. In the case where the subscriber has multiple subscriptions, i.e. multiple ISIM or USIM applications on the UICC, the HSS shall contain one or more subscriber profiles that can be mapped to one or more private identities, i.e. IMPIs and IMSIs.

Editor's note: Needed new subscriber profile parameters, i.e. GBA user security settings, are FFS.

The requirement on the HSS are:

- HSS shall provide the only persistent storage for GBA USSs;
- GBA USS shall be defined in such a way that interworking of different operators for standardised application profiles is possible;
- GBA USS shall be defined in such a way that profiles for operator specific applications and extensions to existing application profiles are supported without need for standardisation of these elements.
- HSS shall able to flag a GUSS which was forwarded to BSF and reset the flag in case of the BSF has not requested the GUSS for a long time.

**********End of change**********

**********Begin of 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: 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;
- the HSS shall be able to nofity the BSF the update of a GUSS if it has been sent to the BSF;
- the BSF decide whether it request the updated GUSS or not, after being notified by the HSS;
- the HSS shall be able to deal with a block update in a notification message, and BSF can also request the GUSS in a batch.

~~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.~~

- 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: 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: 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: After the GUSS is updated in BSF, NAF will update the USSs when it performs the Using Bootstrapping procedure, no extra update procedure is needed for it.

**********End of change**********

**********Begin of change**********

4.5.4 Procedure related to service discovery

To enable the bootstrapping procedure, a procedure needs to be described on how to discover the location of BSF. It shall be possible to enable the terminal to be configured either manually or automatically via one of the following approaches:

- The address information shall be published via reliable channel. Subscribers shall store all the parameters as part of the initial establishment of IP connectivity. The addresses need to be input only once;
- The address information shall be pushed automatically to the UE over the air interface when the subscription to bootstrapping service is accepted. All the parameters shall be saved in the UE and used the same manner as above. The procedure is specified in [7];
- The location information shall be discovered automatically based on DHCP, after the IP connectivity has been established. The DHCP server shall provide the UE with the domain name of a BSF and the address of a Domain Name Server (DNS) that is capable of resolving the Fully Qualified Domain Name (FQDN) of the BSF. The procedure is specified in TS 23.228 [8].

NOTE: The location of DHCP server may be pushed to UE through the procedure specified in [7].

4.5.5 Procedure of GUSS update

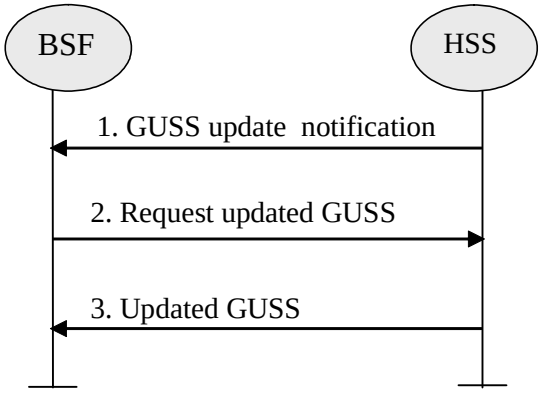

Figure 4.6: GUSS update procedure

1. After the GUSS is changed in HSS, if the GUSS has been sent to the BSF, the HSS sends a notification to BSF.
2. The BSF will make a decision according to the local configuration, to request the updated GUSS or just ignore the notification.
3. The HSS sends the updated GUSS to BSF if the request is received from step2.

**********End of change**********

**********Begin of change**********

5.3.4 Procedure related to service discovery

The text from clause 4.5.4 of this document applies also here.

5.3.5 Procedure of GUSS update

The procedure from clause 4.5.5 of this document applies also here.

**********End of change**********