3GPP TSG SA WG3 Security — S3#31 **S3-030157**
9 – 13 February, 2004, Edinburgh, Scotland

CR-Form-v7

Pseudo - 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 ☒ Radio Access Network ☐ Core Network ☒

Title:	⌘	GBA Transaction Identifier (TID) requirements		
Source:	⌘	Ericsson		
Work item code:	⌘		***Date:*** ⌘	26 January 2004
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:	⌘	GBA does not currently specify any requirements for TID. TID is a core element of GBA. It is important that TID is designed in the way that it is both secure, and useful with several using protocols in the Ua interface.
Summary of change:	⌘	Introduce requirements. See related discussion paper on the background of proposed requirements.
Consequences if not approved:	⌘	TID may not be secure, or it may not serve all potential using protocols in the Ua interface.

Clauses affected:	⌘					
		Y	**N**			
Other specs affected:	⌘	**Y**		Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

***** Begin of Change ****

4.1.6 Requirements on Zn interface

The requirements for Zn interface are:

- Mutual authentication, confidentiality and integrity shall be provided.
- The BSF shall verify that the NAF is authorised.
- The NAF shall be able to send a key material request to the BSF.
- The BSF shall be able to send the requested key material to the NAF.
- The NAF shall be able to get the subscriber profile from BSF.

Editor's note: The intention is not to send all the application-specific profile information, but only the information needed for security purposes.

Editor's note: In later phases there is an additional requirement that the NAF and the BSF may be in different operators' networks.

[Editor’s note: Relationship between TID and subscriber identity is ffs. In the case of Presence Ut interface, there are several potential identities that are related to TID, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. TID does not carry enough information on which IMPU the end-user is trying to use.]

***** End of Change ****

***** Begin of Change ****

4.1.7 Requirements on transaction identifier

Transaction identifier shall be used to bind the subscriber identity to the keying material in Ua, Ub and Zn interfaces.

Requirements for transaction identifier are:

- Transaction identifier shall be globally unique.
- Transaction identifier shall be usable as a key identifier in protocols used in the Ua interface.
- NAF shall be able to detect the home network and the BSF of the UE from the Transaction identifier.

[Editor’s note: Parallel use of GBA and non-GBA infrastructure is ffs. There are use cases when NAF may want to use GBA and non-GBA based infrastructures at the same time. For example, a NAF may want to authenticate subscribers both by using normal HTTP Digest authentication (where the usernames and passwords are distributed using some other mechanism than GBA), and by using GBA based HTTP Digest. However, it seems that in most telecommunication protocols, the server side (i.e. NAF) controls the name space related to key identifiers (cf. TID). For example, in HTTP authentication, the server issues the usernames, and does not allow the re-use of already existing usernames. The parallel use of GBA and non-GBA based infrastructures may cause conflicts on TID namespace. In particular, BSF may assign TID values that NAFs are already using with non-GBA UEs.]

Editor's note: GBA must further specify on how security associations are removed and/or updated in NAF. ~~Each bootstrapping procedure creates a new TID value even when the same UE is communicating with the same NAF. If the intend is just to update the password in HTTP Digest to a fresh one, for example, this would also mean that the identity of the end-user would need to be changed. It is not currently clear what happens to the old username and password in NAF.~~

***** End of Change ****