3GPP TSG-SA3 Meeting #31
Munich, Germany, 18-21 November 2003

Tdoc ⌘S3-030704

CR-Form-v7

CHANGE REQUEST

⌘ **TS 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:	⌘	Transaction Identifier independence for different NAFs or NAF groups
Source:	⌘	Huawei Technologies Co., Ltd.
Work item code:	⌘	GBA
Date:	⌘	10/11/2003
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:
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:	⌘	[TS 33.220] The usage of the Transaction Identifier is not clear and misleading in current TS. With the bootstrapping function and utilization, after the UE successfully implements the AKA procedure with the BSF, the BSF assigns a transaction identifer (TID) to the UE. The UE includes this TID in request messages to the NAF. The NAF retrieves this TID from the BSF, and then the NAF can share the Ks with the UE. That Ks is the result of AKA between the UE and the BSF. But when the UE requests a different NAF service, the same TID will be included in the corresponding request messages. The end result is that all NAFs share the same Ks with the UE, so if one NAF is compromised, the other NAFs are in danger too. In order to eliminate this associated threat, the Transaction Identifier (and associated key) should be independent among different NAFs or NAF groups.
Summary of change:	⌘	The Transaction Identifier (and associated key) is independent among different NAFs or NAF groups. The BSFshould maintain and check the validity of transaction identifier.
Consequences if not approved:	⌘	Different UE/ NAF or UE/NAFs security threats are not independent which decreases the security of GAA.

Clauses affected:	⌘	4.1, 4.3.2			
		Y	**N**		
Other specs Affected:	⌘		**X**	Other core specifications	⌘
			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 of Change**********

4.1 Requirements and principles for bootstrapping

Editor's note: The description of AKA bootstrapping shall be added here.

- The bootstrapping function shall not depend on the particular network application function ,
- The server implementing the bootstrapping function needs to be trusted by the home operator to handle authentication vectors.
- The server implementing the network application function needs only to be trusted by the home operator to handle derived key material.
- It shall be possible to support network application functions in the operator's home network
- The architecture shall not preclude the support of network application function in the visited network, or possibly even in a third network.
- To the extent possible, existing protocols and infrastructure should be reused.
- In order to ensure wide applicability, all involved protocols are preferred to run over IP.
- The Transaction Identifier (and associated key) is independent among different NAFs or NAF groups

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

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

4.3.2 Procedures using bootstrapped Security Association

After UE is authenticated with the BSF, every time the UE wants to interact with an NAF the following steps are executed as depicted in Figure 1

UE starts communication over Ua interface with the NAF

- In general, UE and NAF will not yet share the key(s) required to protect Ua interface. If they already do, there is no need for NAF to retrieve the key(s) over Zn interface.
- If the NAF shares a key with the UE, but an update of that key it sends a suitable key update request to the UE and terminates the protocol used over Ua interface. The form of this indication may depend on the particular protocol used over Ua interface and is ffs.
- It is assumed that UE supplies sufficient information to NAF, e.g. a transaction identifier, to allow the NAF to retrieve specific key material from BSF.
- The UE derives the keys required to protect the protocol used over Ua interface from the key material.

NAF starts communication over Zn interface with BSF

- The NAF requests key material corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier) in the start of the protocol used over Ua interface.

- The BSF supplies to NAF the requested key material. If the key identified by the transaction identifier supplied by the NAF is invalid or unavailable at the BSF, the BSF shall indicate this in the reply to the NAF. The NAF then indicates a key update request to the UE.

- The BSF checks the validity of transaction identifier baseing on the status of the TID usage. For example, it only checks whether the TID is used when the NAF need exclusively use one TID; If the NAF can share one TID with other NAFs (e.g. a group of NAFs in a certain security level), more information of TID usage (e.g. numbers of NAFs have requested it, security level of these NAFs, etc.) need to be involved in the TID validity checking.

  The BSF updates the validity information of the TID after it supplied to NAF the requested key material.

- The NAF derives the keys required to protect the protocol used over Ua interface from the key material in the same way as the UE did.

NAF continues with the protocol used over Ua interface with UE

Once the run of the protocol used over Ua interface is completed the purpose of bootstrapping is fulfilled as it enabled UE and NAF to use Ua interface in a secure way.

Editor's note: Message sequence diagram presentation and its details will be finalized later.

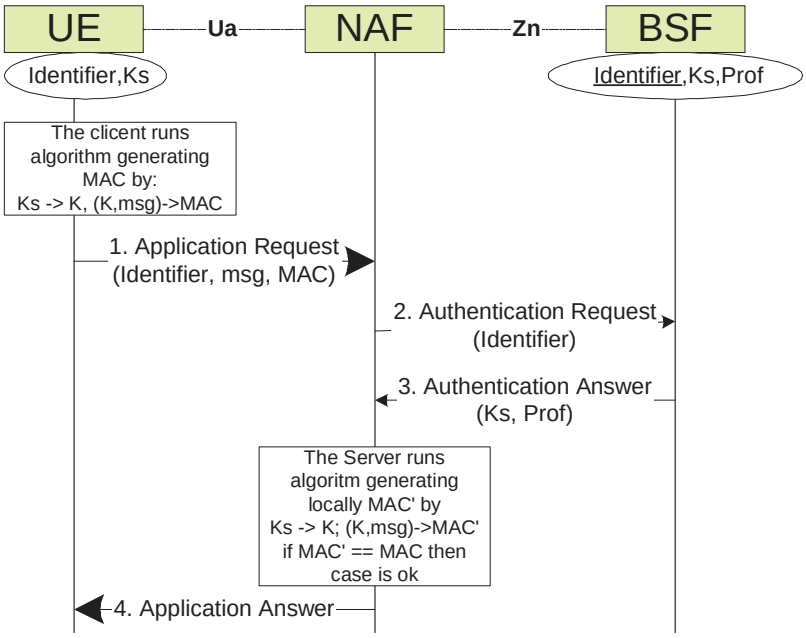

Figure 1: The bootstrapping usage procedure

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