3GPP TSG SA WG3 Security — S3#32 **S3-040032**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda item: **6.9.2 GBA**

Title: **User identity in NAF**

Source: **Huawei Technologies Co., Ltd**

Document for: **Discussion and Approval**

1 Introduction

The user identity is a common user information which may often be needed in generic applications, so it should be provided to the NAF.

2 Discussion

The NAF can retrieve the UE TID and associated key material from the BSF after it is authorised by the BSF, so the NAF can be considered as a safe entity. The user identity in NAF is safe as its key material.

The NAF can action as various application server, application proxy etc. The user identity is a common user information which may often be needed. E.g. the second authentication according the key material coming from the BSF or NAF may request application-specific user profile information using other mechanisms e.g. GUP.

Furthermore, **the security-specific profile shall be provided to the NAF:** It is required on the Zn interface "The NAF shall be able to get the subscriber profile from BSF", and basing on the agreement in the last meeting, only the security-specific subscriber profile shall be provided,

Basing on the current procedure, the NAF can get the user identity and the corresponding security-specific profile easily. The NAF retrieves TID (comes from UE) from the BSF, and once the TID is available, the BSF return the corresponding key material. As the same time, the BSF can provide the user identity and the corresponding security-specific profile to NAF.

3 Proposal

When the BSF returns the TID corresponding key material to NAF, it may provide the user identity and corresponding security-specific profile to NAF. The attached pseudo include the required changes to TS 33.220 v0.2.0

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.220 CR CRNum** ⌘ **rev -** ⌘ Current version: **V 0.2.0** ⌘

*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:	⌘	user identity and security-specific profile in NAF
Source:	⌘	Huawei Technologies Co., Ltd.
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 user identity and corresponding security-specific profile are always necessary in NAF(Network Application Function), however, there is no text to describe how does the NAF get the it in the current TS
Summary of change:	⌘	When the BSF returns the TID corresponding key material to NAF, it should also provide the user identity and the corresponding security-specific profile to NAF
Consequences if not approved:	⌘	The NAF doesn't have the real identity of user and the corresponding security-specific profile, then the subsequent function can not be performed.

Clauses affected:	⌘	4.3.3

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

Other comments:	⌘	

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

4.3.3 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, as specified in clause 4.3.2.

NOTE: The UE may adapt the key material Ks_NAF to the specific needs of the Ua interface. This adaptation is outside the scope of this specification.

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 derives the keys required to protect the protocol used over Ua interface from the key material and the key derivation parameters, as specified in clause 4.3.2, and supplies to NAF the requested key material, the user identity and corresponding security-specific profile. If the key identified by the transaction identifier supplied by the NAF is not available 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.

NOTE: The NAF may adapt the key material Ks_NAF to the specific needs of the Ua interface in the same way as the UE did. This adaptation is outside the scope of this specification.

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.

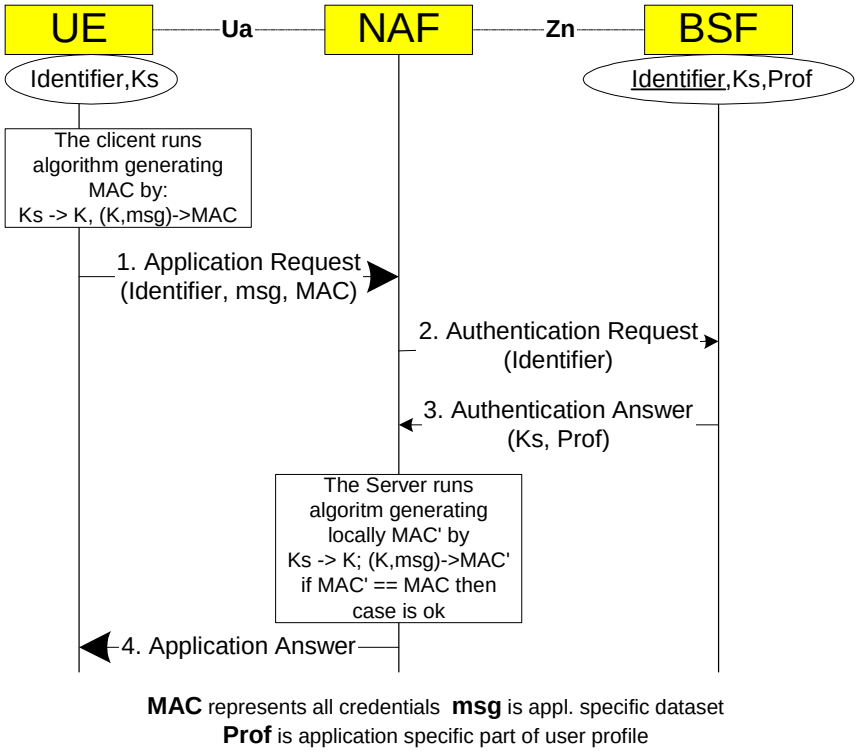

Figure 1: The bootstrapping usage procedure

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