3GPP TSG SA WG3 Security — S3#33 **S3-040316**
10 - 14 May 2004
Beijing, China

Agenda item: 6.9.2 GBA

Title: Validity condition set by NAF

Source: Huawei

Document for: Discussion and Decision

1 Introduction

In TS 33.220, The BSF shall be able to indicate to the NAF the lifetime of the key material. The NAF shall be able to check the lifetime of the key material set by BSF, and if the lifetime has expired, the NAF shall send key update request to UE. That lifetime of key material is set by BSF, but with some special applications , the NAF may have strict requirements on the freshness of bootstrapping information. We suggest NAF can further set the validity condition with it's special requirement.

2 Discussion

The NAF may act as various applications e.g. gaming , browsing, e-commerce etc. It's obvious the security requirements of browsing service and e-commerce service are absolutely different. The lifetime of key material set by BSF may meet the browsing service, but for the e-commerce there may be more security requirements than key lifetime , e.g. the shorter lifetime than set by BSF, a limited number of times that key can be used.

Shorter lifetime:

The NAF may set the shorter lifetime to key material than the BSF. That makes key material keep more fresh with NAF special strict requirement. This enhance the security at a certain extend, but the effect maybe not very significant.

A limited number of times:

The NAF may set a limited number of times that TID and key material can be used. This validity condition can avoid the risk of key material use frequently and some vicious attacks. For example, the key materials in UE have been leaked out, but the user doesn't know about it. The attacker may use victim's TID and key material frequently to peculate the service in a short period. If the NAF set a limited number of times that TID and key material can be used, the attack can be hold back in a limited level. It is very useful to the NAF with high security level, e.g. e-commerce .

3 Conclusion

It is necessary that NAF can set the validity condition according the local special requirements. With the analysis in section 2, the method of a limited number of times is more effective than shorter lifetime.

4 Proposal

1 NAF can set local validity condition of TID and key material according the special requirements.

2 The limited number of times is a preferred method.

3 Approve the attached CR.

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.220 CR CRNum** ⌘ **rev -** ⌘ Current version: **V 6.0.0** ⌘

*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:	⌘	Validity condition set by NAF
Source:	⌘	Huawei
Work item code:	⌘	GBA
Date:	⌘	16-04-2004
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:

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 lifetime of key material is set by BSF, but it is necessary that some high level NAFs can set local validity conditions with their local requirements
Summary of change:	⌘	Add the requirement ”NAF shall be able to set the local validity condition of the shared key material”. When NAF receive the user’s request including the TID, the NAF can check the local validity conditions set by itself.
Consequences if not approved:	⌘	The NAF miss the important feature that can avoid the some possible attacks

Clauses affected:	⌘	4.2.2 4.5.3			
Other specs Affected:	⌘	**Y**	**N**		
			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 **********

4.2.2 Network application function (NAF)

After the bootstrapping has been completed, the UE and an operator-controlled NAF can run some application specific protocol where the authentication of messages will be based on those session keys generated during the mutual authentication between UE and BSF.

General assumptions for the functionality of an operator-controlled NAF are:

- there is no previous security association between the UE and the NAF;
- NAF shall be able to locate and communicate securely with the subscriber's BSF;
- NAF shall be able to acquire a shared key material established between UE and the BSF during the run of the application-specific protocol;
- NAF shall be able to set the local validity condition of the shared key material.
- NAF shall be able to check lifetime and local validity condition of the shared key material.

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

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

4.5.3 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 5.

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 (i.e. if a key Ks_NAF for the corresponding key derivation parameter NAF_Id_n is already available),, the UE and the NAF can start to securely communicate right away. If the UE and the NAF do not yet share a key, the UE proceeds as follows:
  - if a key Ks is available in the UE, the UE derives the key Ks_NAF from Ks, as specified in clause 4.5.2;
  - if no key Ks is available in the UE, the UE first agrees on a new key Ks with the BSF over the Ub interface, and then proceeds to derive Ks_NAF;

- if the NAF shares a key with the UE, but an update of that key is needed, e.g. because the key's lifetime has expired or the key can not meet the NAF local validity condition, it shall send 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 (cf. 4.5.1);

- the UE supplies Transaction Identifier to the NAF, in the form of 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 shall adapt the key material Ks_NAF to the specific needs of the Ua interface. This adaptation is outside the scope of this specification.

- when the UE is powered down, or when the UICC is removed, any keys Ks and Ks_NAF shall be deleted from storage;

- when a new Ks is agreed over the Ub interface and a key Ks_NAF, derived from one NAF_Id, is updated, the other keys Ks_NAF, derived from different values NAF_Id, stored on the UE shall not be affected;

NAF starts communication over Zn interface with BSF

- The NAF requests key material corresponding to Transaction Identifier supplied by the UE to the NAF used over Ua interface;

- The BSF derives the keys required to protect the protocol used over Ua interface from the key material Ks and the key derivation parameters, as specified in clause 4.5.2, and supplies to NAF the requested key material Ks_NAF, as well as the lifetime time of that key material. The NAF can further set the local validity condition of the Ks_NAF, for example a limitation of reuse times of a Ks_NAF. 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 shall 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 the Ua interface with the 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.

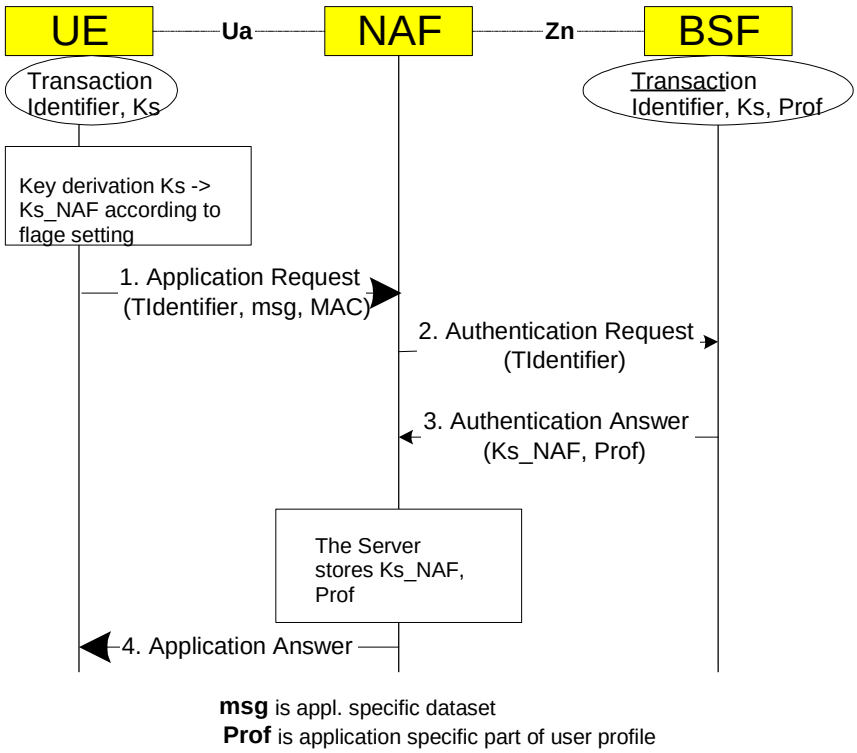

Figure 5: The bootstrapping usage procedure

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