3GPP TSG SA WG3 Security — S3#33 **S3-040315**
10 - 14 May 2004
Beijing, China

Agenda item: 6.9.2 GBA

Title: NAF remove the security associations

Source: Huawei

Document for: Discussion and Decision

1 Introduction

As the discussion in the last SA3 meeting, GBA shall further specify on how security associations are removed and/or updated in NAF. This contribution discuss different remove/update methods and suggest NAF remove the security association with some deletion conditions after the security association had been invalid.

2 Discussion

Method 1:

"*NAF can distinguish that different TID values are actually related to the same security association. In this way, NAF can remove old security associations (or update old ones) when new security associations are created*"

If NAF want to know that different TID values are related to the same security association, the user identity is necessary in NAF. The TID can be combined to user identity. when the new security association is created , the NAF check whether are there other TIDs relating the same IMSI, then the NAF can remove the old ones. However, it is unclear now whether the user identity is necessary in each NAF.

Method 2:

"*Each bootstrapping procedure creates new security association. NAF removes security associations only when the key can not meet the validity conditions*"

TS 33.220 shows "*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, it shall send a suitable key update request to the UE and terminates the protocol used over Ua interface*", from this point , the new security association is

created after the NAF find the key is invalid (the security association is stale), then the UE should request service with new security association. But, there maybe some problems with this method, for example , if the UE use the wrong security association or the UE use the stale security association to request the service ,the additional signal message will happened over Zn interface, because the NAF had remove that stale security association and have to retrieve it from BSF. If many UEs use the wrong TID, the result appear just like Dos attack.

Method 3:

"*NAF removes the security association with some deletion conditons after the key had been invalid*"

When the NAF find the key had been invalid, the NAF should not remove the security association immediately, it can set some deletion conditions to that security association for afterward removing. For example , the NAF can set a delay time to security association, if the security association is not visited in that setting delay time, then the security association can be removed after that delay time. If the stale security association is visited in that delay time, then NAF can extend the delay time to avoid the possible retrieve from BSF. For the consideration of saving the NAF resource, the delay time can be set flexibly e.g. only a short delay. But if the delay time had reached, the NAF will remove the stale security association ,and if NAF receive the stale TID request at this time, the NAF have to retrieve it from BSF once, so the saving resource between the NAF and Zn interface should be balanced to set the appropriate delay time.

3 Conclusion

The method1 and method3 are also potential solutions.

Before the method1 can be selected, the open issue rose by S3-040032 about the user identity in NAF should be solved, and because the method3 have no more requirements to NAF, we suggest the method3 as current solution to ensure the integral of TS. If the open issue is closed , the solution also can be update.

4 Proposal

1 NAF shall remove the security association with some deletion conditions after the key had been invalid.

2 Approve the attached CR.

5 References

[1] 3GPP TS 33.220: "Generic Authentication Architecture (GAA);Generic bootstrapping architecture"

[2] S3-040065: “Requirements for Transaction identifier in GBA” ERICSSON

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:	⌘	NAF remove the security associations
Source:	⌘	Huawei
Work item code:	⌘	GBA
Date:	⌘	17-04-2004
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:	⌘	GBA shall further specify on how security associations are removed and/or updated in NAF.
Summary of change:	⌘	Add “NAF shall be able to remove the security association with deletion conditions after the key had been invalid” to the section 4.3.7. and delete the Editor’s notes. Add corresponding describing to the Procedures using bootstrapped Security Association.
Consequences if not approved:	⌘	The TS is not integral.

Clauses affected:	⌘	4.3.7 4.5.3

		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 **********

4.3.7 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.
- NAF shall be able to remove the security association with deletion conditions after the key had been invalid.

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. Transaction Identifier). 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 Transaction Identifier namespace. In particular, BSF may assign Transaction Identifier values that NAFs are already using with non-GBA UEs.

~~Editor's note: GBA shall further specify on how security associations are removed and/or updated in NAF.~~

**********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, 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);
- If the shared key between UE and NAF is invalid ,the NAF shall set deletion conditions to the corresponding security association for afterward removing.
- 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. 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.

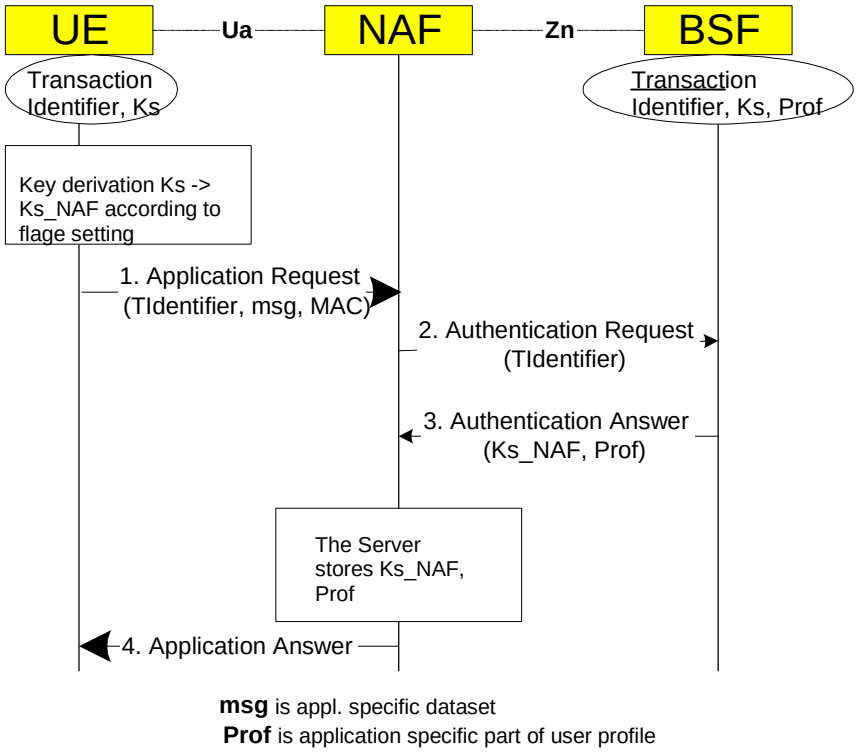

Figure 5: The bootstrapping usage procedure

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