3GPP TSG SA WG3 Security — S3#35 **S3-040736**
5 - 8 October 2004
St Paul's Bay, Malta

Agenda item: 6.9.2 GBA

Title: Impact analysis -Validity condition set by NAF

Source: Huawei

Document for: Discussion and Decision

1 Introduction

In the SA3#33 meeting , the NAF set local validity condition of Transaction identity and key material according the special requirements was discussed and the method of limited number of times was thought as preferred method. But the concern rose about whether it will impact other interfaces. This paper analysis this issue.

2 Discussion

The advantage of the NAF set the local validity condition according the special requirements.:

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.

The impact on other interface:

If the local validity condition or the lifetime of key material was reached , the NAF will send the key update request to UE, just like the state in section 4.5.3 of TS33.220 "*if the NAF shares a key with the UE, but the NAF requires an update of that key, e.g. because the key's lifetime has expired, it shall send a suitable bootstrapping renegotiation request to the UE and terminates the protocol used over reference point Ua, see figure 4.5*.". There is other state in the same section of TS 33.220 to avoid the complexity and impact to other interface risen by key update request:" *when a new Ks is agreed over the reference point Ub 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*". So the NAF set local validity condition and request key update subsequently , all the procedure are in line with current TS and no any impact to other interface.

3 Conclusion

It is a useful to NAF mitigates the potential risk without any impact to other interface, so we suggest add this feature to NAF in TS body but not in NOTE'S.

4 Proposal

Approve the attached CR.

3GPP TSG-SA WG3 SECURITY Meeting #35
St Paul's Bay, Malta, 5-8 October 2004

Tdoc ⌘Att1_S3-040736

CR-Form-v7.1

CHANGE REQUEST

⌘	**33.220**	**CR**	**019**	⌘**rev**	**-**	⌘	Current version:	**6.2.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

St Paul's Bay, Malta

Proposed change affects: UICC apps⌘ □ ME □ Radio Access Network □ Core Network ☒

Title:	⌘	Local validity condition set by NAF			
Source:	⌘	Huawei			
Work item code:	⌘	GBA	***Date:***	⌘	28/09/2004
Category:	⌘	**F** *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.	***Release:***	⌘	Rel-6 *Use one of the following releases:* *Ph2 (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)* *Rel-7 (Release 7)*

Reason for change:	⌘	The key leaking out is an potential security threaten during the service, e.g. leakage of key with not well safed local connections in UE, then a frequent stolen service request may happen with a very short time. Application(NAF) should have a mechanism to limit the abnormal using of the shared secret and take action to mitigate it as much as possible.
Summary of change:	⌘	NAF set the local validity condition of the shared key material. E.g. a limited number of times that TID and key material can be used. When NAF receive the user's request including the TID, the NAF can check the local validity conditions set by itself to avoid the service stolen.
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				
		Y	**N**			
Other specs affected:	⌘		X	Other core specifications	⌘	
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘					

************************************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 acquire an (application-specific) user security setting from the HSS via the BSF;
- 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

Before communication between the UE and the NAF can start, the UE and the NAF first have to agree whether to use shared keys obtained by means of the GBA. If the UE does not know whether to use GBA with this NAF, it uses the Initiation of Bootstrapping procedure described in clause 4.5.1.

Once the UE and the NAF have established that they want to use GBA then every time the UE wants to interact with an NAF the following steps are executed as depicted in figure 4.4.

UE starts communication over reference point Ua with the NAF:

- in general, UE and NAF will not yet share the key(s) required to protect the reference point Ua. If they already do (i.e. if a key Ks_NAF for the corresponding key derivation parameter NAF_Id 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 for the selected UICC application 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 for the selected UICC application is available in the UE, the UE first agrees on a new key Ks with the BSF over the reference point Ub, and then proceeds to derive Ks_NAF;

NOTE 1: If it is not desired by the UE to use the same Ks for the selected UICC application to derive more than one Ks_NAF then the UE should agree on a new key Ks with the BSF over the reference point Ub, and then proceed to derive Ks_NAF;

- if the NAF shares a key with the UE, but the NAF requires an update of that key, 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 bootstrapping renegotiation request to the UE and terminates the protocol used over reference point Ua, see figure 4.5. The form of this indication depends on the particular protocol used over reference point Ua. If the UE receives a bootstrapping renegotiation request, it starts a run of the protocol over reference point Ub, as specified in clause 4.5.2, in order to obtain a new key Ks.

NOTE 2: To allow for consistent key derivation in BSF and UE, both have to use the same FQDN for derivation (see NOTE 2 of clause 4.5.2). For each protocol used over Ua it shall be specified if only cases (1) and (2) of NOTE 2 of clause 4.5.2 are allowed for the NAF or if the protocol used over Ua shall transfer also the FQDN used for key derivation by UE to NAF.

NOTE 3: If the shared key between UE and NAF is invalid , the NAF can set deletion conditions to the corresponding security association for subsequent removal.

- the UE supplies the B-TID to the NAF, in the form as specified in clause 4.3.2, to allow the NAF to retrieve the corresponding keys from the BSF;

NOTE 4: The UE may adapt the key material Ks_NAF to the specific needs of the reference point Ua. 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 reference point Ub 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 reference point Zn with BSF

- The NAF requests key material corresponding to the B-TID supplied by the UE to the NAF over reference point Ua. If the NAF has several FQDNs, which may be used in conjunction with this specification, then the NAF shall transfer in the request over Zn the same FQDN, which was used over Ua (see NOTE 2 on key derivation in this clause);

- The NAF may also request application-specific user security settings for the applications, which the request received over Ua from UE may access;

- With the key material request, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able verify that NAF is authorized to use that hostname;

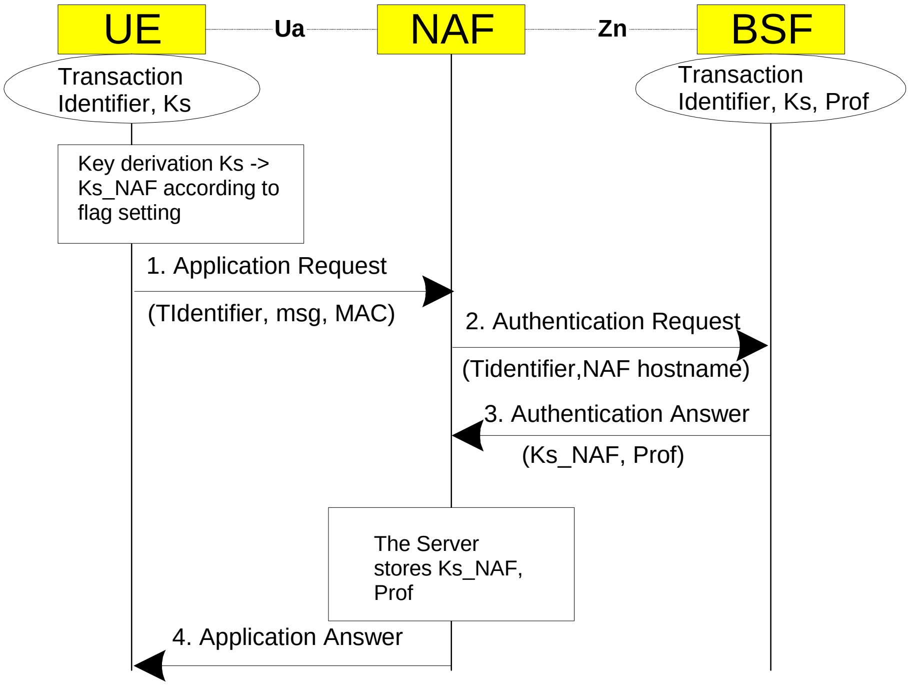
- The BSF derives the keys required to protect the protocol used over reference point Ua from the key Ks and the key derivation parameters, as specified in clause 4.5.2, and supplies to NAF the requested key Ks_NAF, as well as the lifetime of that key. The NAF can further set the local validity condition of the Ks_NAF, for example a limitation of reuse times of a Ks_NAF. If the key identified by the B-TID 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 bootstrapping renegotiation request to the UE.

NOTE 5: The NAF shall adapt the key material Ks_NAF to the specific needs of the reference point Ua in the same way as the UE did. This adaptation is outside the scope of this specification.

- The BSF may also send the private user identity (IMPI) and requested user security settings to NAF according to the BSF's policy;

NAF continues with the protocol used over the reference point Ua with the UE.

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


UE
Ua
NAF
Zn
BSF
Transaction Identifier, Ks
Transaction Identifier, Ks, Prof
Key derivation Ks -> Ks_NAF according to flag setting
1. Application Request
(TIdentifier, msg, MAC)
2. Authentication Request
(Tidentifier,NAF hostname)
3. Authentication Answer
(Ks_NAF, Prof)
The Server stores Ks_NAF, Prof
4. Application Answer

msg	is appl. specific dataset
Prof	is application specific part of user profile

Figure 4.4: The bootstrapping usage procedure

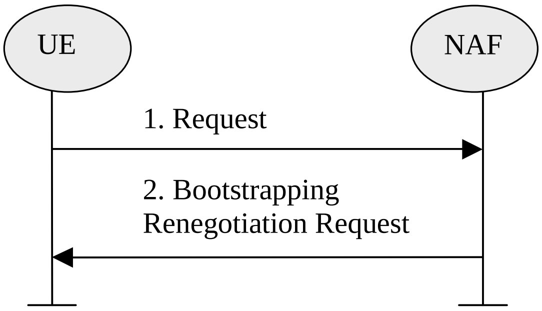


Figure 4.5: Bootstrapping renegotiation request

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