

## CHANGE REQUEST

⌘ **33.220** CR **CRNum** ⌘ rev **-** ⌘ Current version: **6.1.0** ⌘

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

<b>Title:</b>	⌘ Clarification of the definition of a default type of NAF-specific key.		
<b>Source:</b>	⌘ Gemplus, Siemens		
<b>Work item code:</b>	⌘ SSC-GBA	<b>Date:</b>	⌘ 28/06/04
<b>Category:</b>	⌘ <b>D</b>	<b>Release:</b>	⌘ Rel-6
	Use <u>one</u> of the following categories: <b>F</b> (correction) <b>A</b> (corresponds to a correction in an earlier release) <b>B</b> (addition of feature), <b>C</b> (functional modification of feature) <b>D</b> (editorial modification) Detailed explanations of the above categories can be found in 3GPP <a href="#">TR 21.900</a> .		Use <u>one</u> 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)

<b>Reason for change:</b>	The current version of TS 33.220 proposes to use Ks_ext_NAF as default type of key to use for procedures using bootstrapping Security Association.  The UE and the NAF have to agree on the type of the key to use Ks_ext_NAF or Ks_int_NAF. It is the NAF which decides the level of security associated to the service and informs the UE of its choice. It is clarified that this decision overrules the default setting.
<b>Summary of change:</b>	Clarifying text
<b>Consequences if not approved:</b>	Unclear text

<b>Clauses affected:</b>	5.3.3		
<b>Other specs affected:</b>	Y	N	Other core specifications ⌘ Test specifications O&M Specifications
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
	<input type="checkbox"/>	<input checked="" type="checkbox"/>	
<b>Other comments:</b>			

### 5.3.3 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 5.3.1.

Once the UE and the NAF have established that they want to use GBA then every time the UE wants to interact with a NAF the following steps are executed as depicted in figure 5.3.

Next, the UE and the NAF have to agree, which type of keys to use,  $Ks_{ext\_NAF}$  or  $Ks_{int\_NAF}$ , or both. The default is the use of  $Ks_{ext\_NAF}$  only. This use is also supported by MEs and NAFs, which are GBA\_U unaware. If  $Ks_{int\_NAF}$ , or both, [Ks\\_ext and Ks\\_int](#), are to be used, this use has to be agreed between UE and NAF prior to the execution of the procedure described in the remainder of this clause 5.3.3. [Any such agreement overrules the default use of the keys.](#) How this agreement is reached is application-specific [and is not within the scope of this document.](#) ~~and is not within the scope of this document.~~

NOTE 1: [This agreement may be mandated by the specification, which defines the Ua reference point between UE and NAF, e.g. TS 33.246 for the use of GBA in MBMS, or negotiated by the NAF and the UE over the Ua reference point, or reached by configuration.](#)

~~Such an agreement could e.g. be reached by manual configuration, or by an application specific protocol step.~~

Editors' Note: The support of unaware GBA\_U MEs, which are GBA\_ME aware only is FFS.

In general, UE and NAF will not yet share the key(s) required to protect the Ua reference point. If they do not, the UE proceeds as follows:

- if  $Ks_{ext\_NAF}$  is required and a key  $Ks_{ext}$  is available in the UE, the UE derives the key  $Ks_{ext\_NAF}$  from  $Ks_{ext}$ , as specified in clause 5.3.2;
- if  $Ks_{int\_NAF}$  is required and a key  $Ks_{int}$  is available in the UICC, the ME requests the UICC to derive the key  $Ks_{int\_NAF}$  from  $Ks_{int}$ , as specified in clause 5.3.2;

NOTE 2: If it is not desired by the UE to use the same  $Ks_{ext/int}$  to derive more than one  $Ks_{ext/int\_NAF}$  then the UE should first agree on new keys  $Ks_{ext}$  and  $Ks_{int}$  with the BSF over the Ub reference point, as specified in clause 5.3.2, and then proceeds to derive  $Ks_{ext\_NAF}$  or  $Ks_{int\_NAF}$ , or both, as required.

- if  $Ks_{ext}$  and  $Ks_{int}$  are not available in the UE, the UE first agrees on new keys  $Ks_{ext}$  and  $Ks_{int}$  with the BSF over the Ub reference point, as specified in clause 5.3.2, and then proceeds to derive  $Ks_{ext\_NAF}$  or  $Ks_{int\_NAF}$ , or both, as required;
- if the NAF shares a key with the UE, but the NAF requires an update of that key, it shall send a suitable bootstrapping renegotiation request to the UE and terminate the protocol used over Ua reference point. The form of this indication depends on the particular protocol used over Ua reference point. If the UE receives a bootstrapping renegotiation request, it starts a run of the protocol over Ub, as specified in clause 5.3.2, in order to obtain new keys.

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

NOTE 4: If it is not desired by the NAF to use the same  $Ks$  to derive more than one  $Ks_{int/ext\_NAF}$  then the NAF should always reply to the first request sent by a UE by sending a key update request to the UE.

UE and NAF can now start the communication over Ua reference point using the keys  $Ks_{ext\_NAF}$  or  $Ks_{int\_NAF}$ , or both, as required. They proceed as follows:

- The UE supplies the Transaction Identifier to the NAF, as specified in clause 5.3.2, to allow the NAF to retrieve the corresponding keys from the BSF

NOTE 5: To allow for consistent key derivation in BSF and UE, both have to use the same FQDN for derivation (cf. 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 6: The UE may adapt the keys Ks\_ext\_NAF or Ks\_int\_NAF to the specific needs of the Ua reference point. This adaptation is outside the scope of this specification.

- when the UE is powered down, or when the UICC is removed, any GBA\_U keys shall be deleted from storage in the ME. There is no need to delete keys Ks\_int and Ks\_int\_NAF from storage in the UICC;

NOTE 7: After each run of the protocol over the Ub reference point, new keys Ks\_ext and Ks\_int, associated with a new transaction identifier, are derived in the UE according to clause 5.3.2, so that it can never happen, that keys Ks\_ext and Ks\_int with different transaction identifiers simultaneously exist in the UE.

- When new keys Ks\_ext and Ks\_int are agreed over the Ub reference point and new NAF-specific keys need to be derived for one NAF\_Id, then both, Ks\_ext\_NAF and Ks\_int\_NAF (if present), shall be updated for this NAF\_Id, but further keys Ks\_ext\_NAF or Ks\_int\_NAF relating to other NAF\_Ids, which may be stored on the UE, shall not be affected;

NOTE 8: This rule ensures that the keys Ks\_ext\_NAF and Ks\_int\_NAF are always in synch at the UE and the NAF.

NAF now starts communication over the Zn reference point with the BSF.

- The NAF requests from the BSF the keys corresponding to the Transaction Identifier, which was supplied by the UE to the NAF over the Ua reference point. If the NAF is GBA\_U aware it indicates this by including a corresponding flag in the request. 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 above on key derivation in this clause).
- With the keys request over the Zn reference point, the NAF shall supply NAF's public hostname that UE has used to access NAF to BSF, and BSF shall be able to verify that NAF is authorized to use that hostname.
- The BSF derives the keys Ks\_ext\_NAF, and Ks\_int\_NAF (if additionally required), as specified in clause 5.3.2. If the NAF indicated in its request that it is GBA\_U aware, the BSF supplies to NAF both keys, Ks\_ext\_NAF, and Ks\_int\_NAF, otherwise the BSF supplies only Ks\_ext\_NAF. In addition, the BSF supplies the lifetime time of these keys. 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 bootstrapping renegotiation request (See figure 4.5) to the UE.

NOTE: The NAF may adapt the keys Ks\_ext\_NAF and Ks\_int\_NAF to the specific needs of the Ua reference point in the same way as the UE did. This adaptation is outside the scope of this specification.

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

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

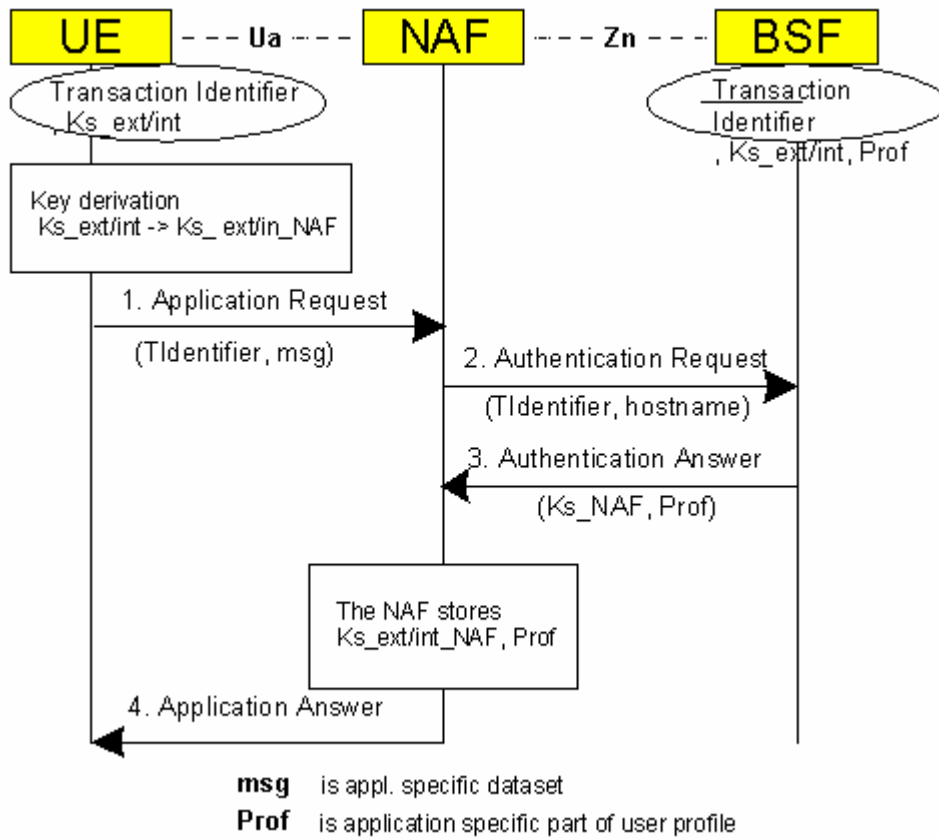


Figure 5.3: The bootstrapping usage procedure with UICC-based enhancements