3GPP TSG SA WG3 Security — S3#34 **S3-040504**
6 – 9 July 2004
Acapulco, Mexico

Source:	Siemens
Title:	Detailing of key lifetime
Work Item:	7.9.2 GBA
Document for:	Discussion and decision

Justification for attached CR to TS 33.220 v610

It was decided at SA3#32 that

“ 1. BSF shall be able to indicate to NAF the expiration time of the bootstrapping information. This should be added as a new requirement into TS 33.220 for Zn interface. . . .
It was commented that only an expiration time would be adequate and not a creation time and validity time. It was clarified that it may happen that the NAF may have a requirement on the freshness of bootstrapped keys. Proposal 1 were endorsed by SA WG3, with "bootstrapping information" replaced by "Ks".

(cf. report on SA3#32, text on discussion of S3-040077, which was later merged into S3-040191).

It seems, however, that this decision was never properly implemented in TS 33.220. In order to avoid different interpretations of the key lifetime sent over Ub and Zn by BSF, UE and NAF, the clarification proposed in the attached CR seems appropriate.

3GPP TSG SA WG3 Security — SA3#34 **S3-040xxx**
6 – 9 July 2004 **Acapulco, Mexico**

CR-Form-v7

CHANGE REQUEST

⌘ **33.220 CR** ⌘ **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 ☒

Title:	⌘	Detailing of key lifetime		
Source:	⌘	Siemens		
Work item code:	⌘	SSC-GBA	***Date:*** ⌘	29/06/2004
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:	⌘	Different interpretations of key lifetime by different entities may cause interoperability problems
Summary of change:	⌘	Clarify that key lifetime means “expiration date”.
Consequences if not approved:	⌘	Interoperability problems

Clauses affected:	⌘	4.4				
		Y	N			
Other specs affected:	⌘	X		Other core specifications	⌘	TS 24.109, TS 29.109
			X	Test specifications		
			X	O&M Specifications		
Other comments:	⌘	-				

4.4 Requirements and principles for bootstrapping

The following requirements and principles are applicable to bootstrapping procedure:

- the bootstrapping function shall not depend on the particular NAF;
- the server implementing the bootstrapping function needs to be trusted by the home operator to handle authentication vectors;
- the server implementing the NAF needs only to be trusted by the home operator to handle derived key material;
- it shall be possible to support NAF in the operator's home network and in the visited network;
- the architecture shall not preclude the support of network application function in a third network;
- to the extent possible, existing protocols and infrastructure should be reused;
- in order to ensure wide applicability, all involved protocols are preferred to run over IP;
- it shall be prevented that a security breach in one NAF who is using the GBA, can be used by an attacker to mount successful attacks to the other NAFs using the GBA.

4.4.1 Access Independence

Bootstrapping procedure is access independent. Bootstrapping procedure requires IP connectivity from UE.

4.4.2 Authentication methods

Authentication between the UE and the BSF shall not be possible without a valid cellular subscription. Authentication shall be based on the 3GPP AKA protocol.

4.4.3 Roaming

The roaming subscriber shall be able to utilize the bootstrapping function in the home network. The subscriber shall be able to utilize network application function that is in a visited network.

4.4.4 Requirements on reference point Ub

The requirements for reference point Ub are:

- the BSF shall be able to identify the UE;
- the BSF and the UE shall be able to authenticate each other based on AKA;
- the BSF shall be able to send a Transaction Identifier to the UE
- the BSF shall be able to indicate to the UE the lifetime of the key material. The key lifetime sent by the BSF over Ub shall indicate the expiry time of the key.

NOTE: this does not preclude a UE to refresh the key before the expiry time according to the UE’s local policy.

4.4.5 Requirements on reference point Zh

The requirements for reference point Zh are:

- mutual authentication, confidentiality and integrity shall be provided;

NOTE: This requirement may be fulfilled by physical or proprietary security measures if BSF and HSS are located within the same operator's network.

- the BSF shall be able to send bootstrapping information request concerning a subscriber;
- the HSS shall be able to send 3GPP AKA vectors to the BSF in batches;
- the HSS shall be able to send the subscriber's GAA profile information needed for security purposes to the BSF;

Editor's note: It's ffs how to proceed in the case where profile is updated in HSS after profile is forwarded. The question is whether this profile change should be propagated to BSF.

- no state information concerning bootstrapping shall be required in the HSS;
- all procedures over reference point Zh shall be initiated by the BSF;

Editor's note: This requirement may need to be modified depending on what happens in the case where the profile in the HSS is updated.

- the number of different interfaces to HSS should be minimized.

4.4.6 Requirements on reference point Zn

The requirements for reference point Zn are:

- mutual authentication, confidentiality and integrity shall be provided;

NOTE: This requirement may be fulfilled by physical or proprietary security measures if BSF and NAF are located within the same operator's network.

Editors' Note: In the visited NAF scenario, it should be decided how the communication between a D-Proxy and a BSF is secured. The possible solutions for securing this link include TLS and IPsec.

- The BSF shall verify that the requesting NAF is authorised;
- The NAF shall be able to send a key material request to the BSF, containing NAF's public hostname used by the UE's corresponding request. The BSF shall be able to verify that a NAF is authorized to use this hostname, i.e. the FQDN used by UE when it contacts the NAF;
- The BSF shall be able to send the requested key material to the NAF;
- The NAF shall be able to get the subscriber profile information needed for security purposes from BSF;
- The BSF shall be able to indicate to the NAF the lifetime of the key material. The key lifetime sent by the BSF over Zn shall indicate the expiry time of the key, and shall be identical to the key lifetime sent by the BSF to the UE over Ub.

NOTE: this does not preclude a NAF to refresh the key before the expiry time according to the NAF's local policy.

Editor's note: Relationship between Transaction Identifier and subscriber identity is ffs. In the case of Presence reference point Ut, there are several potential identities that are related to Transaction Identifier, i.e. IMPI and IMPUs. The subscriber may have several Presence accounts related to same IMPI. Transaction Identifier does not carry enough information on which IMPU the end-user is trying to use.

4.4.7 Requirements on Transaction Identifier

Transaction identifier shall be used to bind the subscriber identity to the keying material in reference points Ua, Ub and Zn.

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 reference point Ua;
- NAF shall be able to detect the home network and the BSF of the UE from the Transaction Identifier.

NOTE 1: NAF can remove the security association based on deletion conditions after the key has become invalid.

NOTE 2: Care has to be taken that the parallel use of GBA and non-GBA authentication between UE and NAF does not lead to conflicts, e.g. in the name space. This potential conflict cannot be resolved in a generic way as it is dependent on specific protocol and authentication mechanism used between UE and application server. It is therefore out of scope of this specification.
For the example of HTTP Digest authentication used between UE and NAF, parallel use is possible as the following applies: <username,password>-pairs must be unique to one realm only. As the NAF controls the realm names, it has to ensure that only the GBA based realm is named with the reserved 3GPP realm name. In the special case that the NAF wants to allow non GBA based authentication in the GBA realm also, it has to ensure that no usernames in the format of a Transaction Identifier are used outside GBA based authentication.