3GPP TSG SA WG3 Security — S3#32 **S3-040114**
09 - 13 February 2004
Edinburgh, Scotland, UK

Agenda Item:	GBA
Source:	Nokia
Title:	Remarks on S3-040042
Document for:	Discussion/Decision

This is a response contribution to previously submitted Tdoc S3-040042:” Multiple key derivation in a Generic Bootstrapping Architecture - Pseudo-CR”, by Siemens.

The previous discussion of the key derivation

The basic idea in S3-040042 was seen in previous meeting. The discussion raised two open issues:

(1) The key-synchronization problem: The key lifetime for different NAFs should not be mandated equal due to the individual nature of each service. For instance, currently e-commerce often uses one-time-password for one session, but for some other services there is never need to change the access secret or password. It is not good principle that lifetime of the key must be equal to all NAFs.

(2) Different key stored in UE and NAF: how to handle, for instance, the case that UE’s battery is brutely removed, or dropped, so the Ks is still valid in NAFs, but not in UE. Then UE would trigger a new round of bootstrapping procedure after re-power-on. On the other hand, the NAF who stores the old but yet still valid key would not need to communicate the BSF for retrieve another key material.

The previous discussion of the n value as the input parameter to key derivation

During the Berlin meeting, Siemens contributed S3-030042, where it was proposed to define a n value as the input parameter of key derivation algorithm. During the discussion, people criticized that the fixed n value to all NAFs would bring inflexibility to the deployment of the operator’s network. For example, there are 2 NAFs, but 3 servers in operator1’s network:
Server1.presence.operator1.com
Server2.conferencing.operator1.com
Server3.mbms.operator1.com

Suppose server 1 and 2 are configured behind a common Authentication Proxy, and they utilize the same TLS connection, the NAF_id_n for them should be the identical, thus n=2. On the other hand, for MBMS server3, a different NAF_n should be created due to residing in the different domain, so n value should be preferrable 4 (though 3 permitted also), but not 2 or 1.

Siemens argueed in SA3#31 that the n value as the input parameter of the key derivation algorithm, is associated to only ONE NAF. Since the default value is n=0, i.e. FQDN of NAF will be used, the NAF and UE can generate an identical key. Therefore at least in case of default n value, the proposal works. But the paper did not solve this issue: if the n value is not 0 for a NAF, how does the UE learn it, and how can the BSF tell the UE?

Another alternative removes this drawback. It was contributed in SA3#31 in TD S3-030729. The UE pushes the NAF names to BSF during bootstrapping procedure, so after the successful authentication, the BSF can indicate each different n value for key generation for the intended NAFs.

Below texts are exempted from SA3#31 meeting minutes (Draft_report_s3_v005):

“TD S3-030743: Key separation in a Generic Bootstrapping Architecture. This was introduced by Siemens and proposes some changes to the draft TS and a Pseudo-CR was attached to implement the proposed changes. A parameter n is proposed for use to generate keys based upon parts of the DNS name of the NAF, allowing differentiation from the full DNS name to up to the rightmost 7 parts of the DNS name. **It was clarified that AKA is always run once to derive Kc and then once again to provide the differentiable Key and that only one key is distributed to an individual NAF.”**

Remarks to S3-040042 regarding to the two issues

Regarding to issue (2), the pseudo-CR in S3-0400042 attempts to answer with new added texts: “if no key Ks is available in the UE, the UE fetches a key Ks from the BSF over the Ub interface, it then proceeds to derive Ks_NAF.”

There is no text to explain how to protect the retrieval of Ks without a new authentication procedure. It’s was criticized in SA3#31, regarding to TD S3-030729.

Remarks to S3-040042 regarding to n value

The S3-040042 brings up the above discussion again. When key derivation is applied to BSF, multiple Ks_NAF must be able to generated from one Ks, the only default n value does not work for all NAFs any more.

To provide a flexible n value for each bootstrapping procedure, n value as the input parameter of key derivation should be delivered to UE after the successful bootstrapping procedure, so BSF can inform different n value associated to each NAF to the UE. Without a flexible method, we have to re-visit the decision made for S3-030743.