3GPP TSG SA WG3 Security — S3#32 **S3-040056**
9 –13 February 2004
Edinburgh, UK

Title:	Draft LS on key derivation for the Generic Bootstrapping Architecture
Release:	6
Work Items:	Support for Subscriber Certificates and Generic Authentication Architecture
Source:	Siemens
Agenda Item:	6.9.2 (GBA)

Abstract

TS 33.220 v1.0.0 specifies in section 4.3.2 the use of a key derivation function KDF. This contribution proposes to send an LS to ETSI SAGE asking SAGE if they could provide a proposal for a specification of KDF satisfying the requirements outlined in the LS.
3GPP SA3 is asked to endorse sending the LS to ETSI SAGE. The LS is to be based on the draft in this contribution and take into account possible relevant contributions and information received during SA3#32, such as the contributions on multiple key derivation and on a UICC-based Generic Bootstrapping Architecture.

3GPP TSG SA WG3 Security — S3#32 **S3-040yyy**
9 –13 February 2004
Edinburgh, UK

Title:	LS on key derivation for the Generic Bootstrapping Architecture
Release:	6
Work Items:	Support for Subscriber Certificates and Generic Authentication Architecture
Source:	3GPP SA3
To:	ETSI SAGE
Cc:	

Contact Person:
Name: tbd
Tel. Number: tbd
E-mail Address: tbd

Attachments: 3G TS 33.220 v100, S3-030552, possible further useful attachments submitted to SA3#32

Abstract

3GPP SA3 currently works on a Generic Bootstrapping Architecture. The specification is contained in TS 33.220. The current version TS 33.220 v1.0.0 (which is attached to this LS) specifies in section 4.3.2 the use of a key derivation function KDF. 3GPP SA3 kindly asks ETSI SAGE to assist in completing the specification of TS 33.220 by providing a specification for a key derivation function satisfying the requirements outlined in this LS, taking into account also new developments at SA3#32 which go beyond TS 33.220 v1.0.0.

Statement of the problem

The entities involved: a User Equipment (UE) communicates with a Bootstrapping Server Function (BSF) in the home network. The BSF has an interface with the Home Subscriber System (HSS) which contains the 3G Authentication Centre supplying authentication vectors. The UE also communicates with an application server, called Network Application Function (NAF). There may be several application servers with which a UE communicates. The situation is depicted in the figure below.

The protocol between UE and BSF over the Ub interface uses a 3G authentication vector (RAND, AUTN, CK, IK, RES) as input and results in a key Ks = CK | IK shared between UE and BSF. Ks is not tied to the use with a particular NAF. This may result in a security threat described in Tdoc S3-030552 (attached). In order to mitigate this threat and obtain a key specific to one NAF or a group of NAFs, a key derivation function is applied to Ks, using further key derivation parameters as input.

From the text of TS 33.220 v100, section 4.3.2:
" Ks_NAF is computed as Ks_NAF = KDF (Ks, key derivation parameters), where KDF is a suitable key derivation function, and the key derivation parameters include the user's IMSI, the NAF_Id_n and RAND. "

NAF_Id_n serves as an identity of the application server NAF.

New developments at SA3#32:

- In TS 33.220 v100, only one key Ks_NAF is derived from one Ks. If a Ks_NAF for a different NAF is required then first a new Ks is to be established. A contribution to SA3#32 proposed to relax this requirement and allow the derivation of multiple keys Ks_NAF for different NAFs from one Ks.

- In TS 33.220 v100, key derivation is performed on the ME (terminal), not on the UICC (smart card). At 3GPP SA3's meeting #32, it was proposed to specify a new variant of a Generic Bootstrapping

Architecture, where key derivation is performed on the UICC. For the latter variant, it was further proposed to derive two keys from Ks, namely Ks_int_NAF, which does not leave the UICC, and Ks_ext_NAF, which is transferred from the UICC to the ME. A first analysis suggests that the same key derivation function with the same key derivation parameters could be used as for TS 33.220 v100, only that the output needed to be twice as long.

(A side note: 3GPP SA3 does not intend to mandate having the key derivation on the UICC as this would require the issuing of new UICCs to all subscribers who want to participate in the Generic Bootstrapping Architecture.)

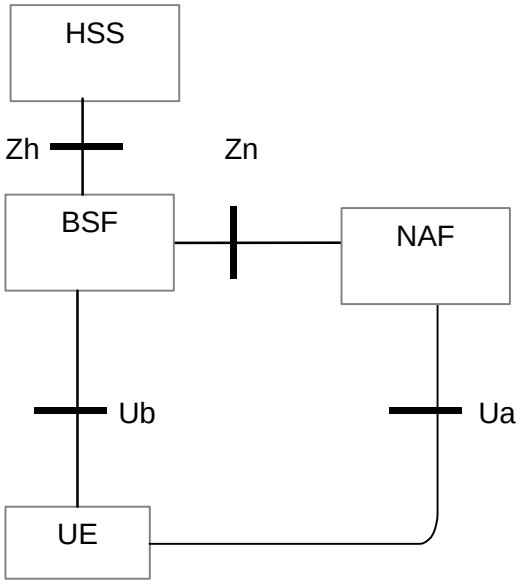

Figure 1: Simple network model for bootstrapping

Requirements on the key derivation function KDF

The following requirements have been identified so far:

1) *It shall not be possible to gain any useful knowledge about Ks from the derived keys Ks_NAF.*

2) *It shall not be possible to gain any useful knowledge about Ks1_NAFi from Ks2_NAFj for different i,j and any Ks1 and Ks2.*

3) Random input to key derivation: typically, key derivation needs random input in addition to the initial key Ks. It is suggested to use the RAND from the authentication vector, which was used to produce Ks.

4) *Identity of user and application server as input to key derivation:*
It is proposed to use IMSI and NAF_Id_n as input.

5) *It shall not be possible to gain any useful knowledge from Ks_ext_NAF about any of the other keys involved.*

ACTION:

3GPP SA3 kindly asks ETSI SAGE to assist in completing the specification of TS 33.220 by providing a specification for a key derivation function satisfying the requirements outlined in this LS.3GPP SA3 would also appreciate if SAGE could indicate a time-frame for the completion of the work. The work should be completed within the deadline for 3GPP Release 6. Unfortunately, the precise deadline is not known yet, but it is expected that it will be decided by the SA plenary in March. It will then be communicated to SAGE. Any further observations by ETSI SAGE would, of course, also be welcome. If more information is required SAGE is kindly asked to contact SA3.

Date of Next SA3 Meetings:

SA3#33	10 - 14 May 2004	Beijing
SA3#34	5 – 9 July 2004	Chicago
SA3#35	4 – 8 October 2004	tbd