3GPP TSG SA WG3 Security **S3-030545**

6th – 10th October, 2003

Povoa de Varzim, Portugal

Agenda Item:

Source: Ericsson

Title: Initiation of bootstrapping procedure

Document for: Discussion/Decision

1. Introduction

This document suggests an enhancement on how the bootstrapping procedures currently specified in [TS 33.109] is initiated.

2. Initiation of bootstrapping

[TS 33.109] currently specifies that when UE wants to interact with a NAF, it must first contact BSF to do bootstrapping. Siemens discussed a related issue in [S3-030411] in SA3#29, and the specification was extended with a rule that also NAF can initiate the key update.

The rule of making the UE to contact BSF before NAF would propose that the use of GBA is mandatory with all applications provided by any Mobile Operator. This harms the interoperability and integration of some other applications into the Mobile Operators network. For example, in HTTP access the integration of Single-Sign On (SSO) [see e.g. Liberty-Overview] and Identity management solutions developed in Liberty Alliance and OMA to GBA would be quite difficult if the network is not able to choose between GBA and these solutions. In the current bootstrapping procedure, the UE initiates the bootstrapping without consulting NAF first. The practical consequence of this rule is that the UE will generate bootstrapped keys for every application even if NAF would not be willing to use it.

This problem can easily be avoided by using a general principle that UE must first contact NAF, instead of BSF. In case where UE really knows that bootstrapping is needed to access a specific NAF, such as PKI Portal in Subscriber Certificates, the UE could still use the current procedures of contacting BSF before NAF.

It is suggested that SA3 slightly modifies the procedure by which the bootstrapping is initiated in order to facilitate easier integration of other security solutions to GBA. It is also important that the control of chosen security mechanism is kept in the network side. The change of the requirement is demonstrated in the attached Pseudo-CR.

3. Conclusions

This documents suggests enhancement on how the general bootstrapping procedure is initiated in [TS 33.109].

It is proposed that SA3 adopts the principles described in the attached Pseudo-CR.

4. References

[Liberty-Overview] Liberty Architecture Overview, Version 1.1, Liberty Alliance, January 2003, available in http://www.projectliberty.org/specs/archive/v1_1/liberty-architecture-overview-v1.1.pdf.

[S3-030411] Siemens; Key provision in bootstrapping of application security, SA3#29, 15 – 18 July 2003, San Francisco, USA.

[TS 33.109] Bootstrapping of application security using AKA and Support for Subscriber Certificates, v0.3.0, 3GPP, SA3.

3GPP TSG SA WG3 Security — S3#30 **S3-030xxx**
6th – 10th October, 2003, Povoa de Varzim, Portugal

CR-Form-v7

CHANGE REQUEST

⌘	**33.109**	**CR**	**CRNum**	⌘**rev**	**-**	⌘	Current version:	0.3.0	⌘

*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:	⌘	Initiation of bootstrapping procedure		
Source:	⌘	Ericsson		
Work item code:	⌘	Security	***Date:*** ⌘	29/09/2003
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:	⌘	[TS 33.109] currently specifies that when UE wants to interact with a NAF, it must first contact BSF to do bootstrapping. There are cases where this general rule will harm the interoperability and integration of some other applications into the Mobile Operators network. For example, interoperability of Single-Sign On and Identity management solutions developed in Liberty Alliance and OMA to GBA is quite difficult if the network is not able to control which security mechanism is used with the UE.
Summary of change:	⌘	Introduces a general principle that UE must first contact NAF, instead of BSF. In case where UE really knows that bootstrapping is needed to access a specific NAF, such as PKI Portal in Subscriber Certificates, the UE could still use the current procedures.
Consequences if not approved:	⌘	Interoperability and integration of GBA with other applications may be difficult.

Clauses affected:	⌘					
		Y	**N**			
Other specs affected:	⌘		**N**	Other core specifications	⌘	
			N	Test specifications		
			N	O&M Specifications		
Other comments:	⌘					

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at http://www.3gpp.org/specs/CR.htm.
Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

***** Begin of Change ****

4.2 Procedures

This chapter specifies in detail the format of the bootstrapping procedure that is further utilized by various applications. It contains the AKA authentication procedure with BSF, and latter the key material generation procedure.

4.3.1a Initiation of bootstrapping

When a UE wants to interact with an NAF, but it does not know if bootstrapping procedure is required, it shall contact NAF for further instructions (see figure X).

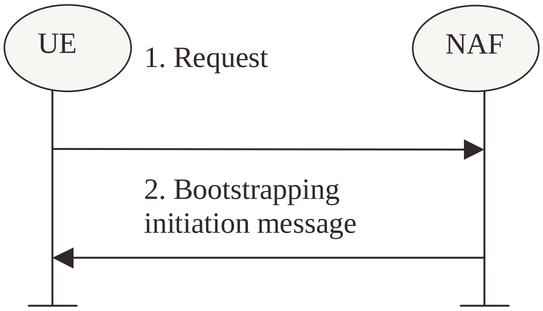

Figure x: Initiation of bootsrapping

1. UE starts protocol B with the NAF without any bootstrapping related parameters.

2. If the NAF require bootstrapping but the request from UE does not include bootstrapping related parameters, NAF replies with a bootstrapping initiation message. The form of this indication may depend on the particular protocol B and is ffs.

> *Editor's notes: If the protocol B is HTTP, then NAF can initiate the bootstrapping procedure by using HTTP re-direct status codes (e.g. 302 Moved Temporarily).*

4.3.1 Bootstrapping procedures

When a UE wants to interact with an NAF, and it knows that bootstrapping procedure is needed, it shall first perform a bootstrapping authentication (see Figure 1).

~~:~~*Editor's notes: Protocol C related procedure will be added here in future development. It may re-use Cx interface that is specified in TS 29.228.*

Otherwise, the UE~~It~~ shall ~~also~~ perform a bootstrapping authentication only when it has received bootstrapping initiation message or a key update indication from the NAF (cf. section 4.3.2).

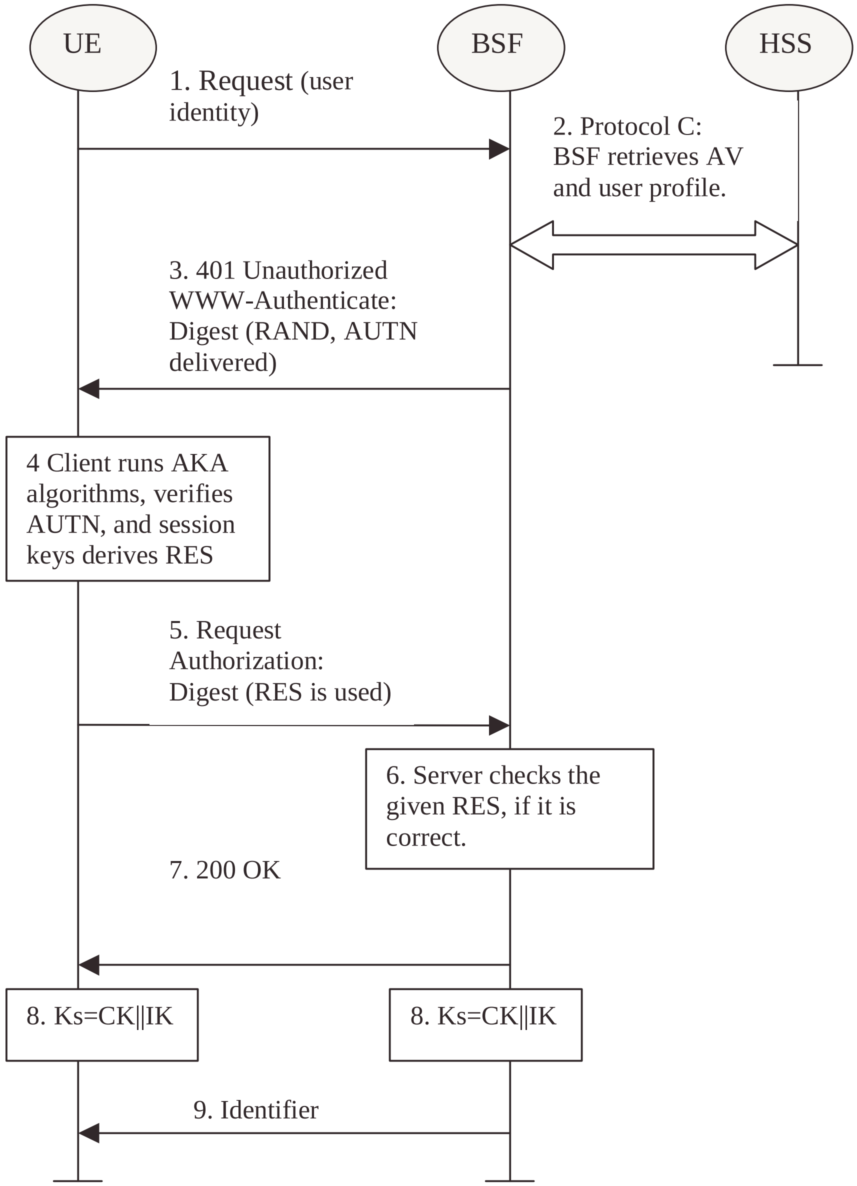
UE
BSF
HSS
1. Request (user identity)
2. Protocol C: BSF retrieves AV and user profile.
3. 401 Unauthorized WWW-Authenticate: Digest (RAND, AUTN delivered)
4 Client runs AKA algorithms, verifies AUTN, and session keys derives RES
5. Request Authorization: Digest (RES is used)
6. Server checks the given RES, if it is correct.
7. 200 OK
8. Ks=CK||IK
8. Ks=CK||IK
9. Identifier

Figure 1: The bootsrapping procedure

1: The UE sends an HTTP request towards the BSF.

2. BSF retrieves the user profile and a challenge, i.e. the Authentication Vector (AV, AV = RAND||AUTN||XRES||CK||IK) by protocol C from the HSS.

3. Then BSF forwards the RAND and AUTN to the UE in the 401 message (without the CK, IK and XRES). This is to demand the UE to authenticate itself.

4: The UE calculates the message authentication code (MAC) so as to verify the challenge from authenticated network; the UE also calculates CK, IK and RES. This will result in session keys IK and CK in both BSF and UE.

5. The UE sends request again, with the Digest AKA RES as the response to the BSF.

6: If the RES equals to the XRES that is in the AV, the UE is authenticated.

7. The BSF shall send 200 OK message to the UE to indicate the success of the authentication.

8. The key material Ks is generated in both BSF and UE by concatenating CK and IK. The Ks is used for securing the protocol B.

Editor's note: The key material Ks is 256 bits long. It is up each NAF to make the usage of the key material specifically.

9. BSF may supply a transaction identifier to UE in the cause of protocol A.

***** End of Change ****