3GPP TSG SA WG3 Security — S3#29 **S3-030340**
15 –18 July 2003
San Francisco, USA

Source:	**Nokia**
Title:	**3GPP Specifications upgrading for Bootstrapping and Subscriber Certificate**
Document for:	**Information**
Agenda Item:	**(7.9) Support for subscriber certificates**

Table of Content:

1. INTRODUCTION

This document summarises the current understanding about the possible updates needed in the 3GPP specifications for implementation of the Bootstrapping and Subscriber Certificate procedures in their C and D interfaces.

The specifications to be upgraded belong to 3GPP SA3 and CN4.

The general Bootstrapping and Subscriber Certificate procedures are currently described in a 3GPP draft TS [S3-030317].

2. TERMINOLOGY

A interface	UE – BSF
B interface	NAF – BSF
BS	Bootstrapping
BSF	Bootstrapping Server Functionality (a network element)
C interface	BSF – HSS
D interface	NAF – BSF
IANA	Internet Assigned Numbers Authority
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia Public Identity
ISIM	IMS SIM
MAA	Multimedia-Auth-Answer
MAR	Multimedia-Auth-Request
NAF	Network Application Function (a network element)
SubCert	Subscriber Certificate

3. OPEN ISSUES THAT HAVE EFFECTS TO THE FOLLOWING UPGRADINGS

The solutions for the following open issues have effects to the summary below:

- The indication method to the HSS that the Cx-like interfaces application logic is not IMS MM, but bootstrapping.
- The down loading of AVP containing Subscriber Certificate Profile (and possible other similar future application profiles) in the C and D interfaces.

4. UPGRADES TO 3GPP TS

4.1 New draft TS for bootstrapping and subscriber certificates (SA3)

4.1.1 Stage 3 description for protocols in C and D interfaces

It is planned by SA3 that the Bootstrapping C interface and the NAF-BSF D interface are based on Diameter implementation of the 3GPP IMS MM application Cx interface.

In the IMS MM case the Cx interface Diameter messages are defined in [TS 29.229]. The IMS MM application logics in S-CSCF and HSS are described in separate implementation-independent specification [TS 29.228].

The existing Diameter implementation specification [TS 29.229] is also suitable for us possibly with small additional informative reference to our TS. But the application logic specification [TS 29.228] is entirely IMS specific. For specification of detailed application logic and messages for BSF-HSS and BSF-NAF Diameter applications we have three alternatives:

1. Make a new separate application logic stage 3 specification for the BSF-HSS interface C and the NAF-BSF interface D. However, this is unpractical because the size of the new specification will be only 3-5 pages.

2. Try to include the detailed description of our C and D interfaces as annexes to the specification [TS 29.228]. Unfortunately this breaks the clear scope of the existing specification [TS 29.228]. The existing specification [TS 29.228] is totally IMS specific, and therefore it may be hard to get totally different kind of material accepted in it.

3. Include the detailed procedural descriptions to corresponding interface chapters in our current draft TS.

We propose the 3rd alternative. This avoids making separate short specification similar to [TS 29.228] for Bootstrapping and Subscriber Certificate. Also, an annex to another system's TS is not a logical solution. Therefore the draft TS "Bootstrapping of application security using AKA and Support for Subscriber Certificates" should contain also the following:

- Detailed description about the protocol in C interface including the BSF-specific usage of Multimedia-Auth-Request/Answer messages. This description is contributed in [S3-030341_A] and [S3-030342_C].

- Detailed description about the protocol in D interface including the NAF-specific usage of Multimedia-Auth-Request/Answer messages. This description is contributed in [S3-030343_D].

- New application logic for Bootstrapping Cx-like interface (C) in BSF and HSS. The description is contributed in [S3-030341_A] and [S3-030342_C].

- New application logic for Cx-like interface (D) in NAF and BSF. The description is contributed in [S3-030343_D].

We propose that the TS will only handle the intra-domain D interface case in the first phase of standardization; potential inter-domain use of D interface is not in the scope in the first phase.

4.1.2 Subscriber Certificate Profile

To enable the home operator control the applications the new TS should also contain:

- Description of Subscriber Certificate Profile (SubCert Profile) or a more general combined profile for applications, that use security association created by the bootstrapping procedure, at least in logical level. The Subscriber Data TS [TS 23.008] can then refer to this information.
- The place for the bit level description of SubCertProfile or more general profile is FFS.

4.2 TS 29.229 Cx and Dx interface based on Diameter protocol (CN4)

4.2.1 6.1.7&6.1.8 Multimedia-Auth-Request/Answer (MAR/MAA) command

Currently there is nothing mandatory to update in TS 29.229. If some upgrading is needed for the Multimedia-Auth-Request/Answer messages for Bootstrapping and the SC in Cx messages, it can be defined here.

4.2.2 “6.3 AVPs” chapter

If new AVP is defined they should be added here. The reason for new AVPs may be to transfer parts of subscriber profile from HSS to BSF. For example, if the SubCert Profile and corresponding application user profiles are not down-loaded from the HSS inside the whole XML schema for the Cx interface user profile (TS 29.228 Annex E) (see section 4.3.1), a special AVP may be needed to down load the SubCert. For example, the User-Data in the MAA message may contain a the following new User-Profile group AVP to ensure the expansibility for future applications:

```
User-Profile::=<AVP header: TBD>
         1*[SubCert-Profile]
         1*[Some-Future-Profile]
```

4.3 TS 29.228 IMS Cx and Dx Interfaces (CN4)

4.3.1 Annex E

- If the SubCert Profile is included inside the User-Data AVP in the MAA message, the SubCert Profile tag must also be added to the normative definition of XML schema for the Cx interface user profile in annex E. However, this is not needed if, as described in previous section, there is some other AVP for transferring SubCert Profile.

4.4 TS 23.008 Organization of subscriber data (CN4)

The following chapters need upgrading:

4.4.1 3.6 Data related to Core Network services Authorization

Probably this chapter, that is FFS in current 5.3.0 version of TS 23.008, is a possible place for reference to SubCert profile defined in the new [S3-030317] TS.

4.4.2 5.3 IP Multimedia Service Data Storage

This table may be also need to be upgraded.

5. POSSIBLE UPGRADES TO IETF DOCUMENTS

No updating is needed in the HTTP Digest AKA protocol for the Bootstrapping A interface.

The C and D interface potentially require following kind of upgrading to IETF Diameter and its applications specifications:

1. Currently we assume that IMS Multimedia-Auth-Request/Answer command codes will be used also for Bootstrapping-Request/Answer messages (Vendor-Specific-Application-ID is used to diffrentiate between IMS and Bootstrapping messages.) In the future it may be possible to request a new command code from IANA for Bootstrapping messages. In this case, Diameter command code lists would also need updating.

2. If new AVPs are defined (e.g. for NAF-specific parts of subscriber profile), then some Diameter specifications may need to be updated.

3. There may be need to allocate new values in existing Diameter AVPs code space (e.g. we could allocate own value for bootstrapping Vendor-Specific-Application-Id).

These potential upgrades to IETF documents are FFS.

6. REFERENCES

[3GPP TS 23.008]	Organization of subscriber data (release 5), V5.3.0 (2002-12)
[3GPP TS 23.228]	IP Multimedia Subsystem (IMS); Stage 2 (Release 6); V6.1.0 (2003-03)
[3GPP TS 29.228]	IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents; (Release 5); V5.3.0 (2003-03)
[3GPP TS 29.229]	Cx and Dx interfaces based on the Diameter protocol; Protocol details; (Release 5); V5.3.0 (2003-03)
[DIAMETER]	IETF aaa working group, draft-ietf-aaa-diameter-17.txt
[S3-030317]	Bootstrapping of application security using AKA and Support for Subscriber Certificates; System Description (Release 6)
[S3-030341_A]	Nokia CR: Protocol A in stage 3 detail.
[S3-030342_C]	Nokia CR: Protocol C in stage 3 detail.
[S3-030343_D]	Nokia CR: Protocol D in stage 3 detail.