3GPP TSG SA WG3 Security — S3#28 **S3-030305**
6 - 9 May 2003
Berlin, Germany

Title: **Adopting Cx-based protocols for several interfaces: NAF-BSF (D interface) and BSF-HSS (C interface), the interface between Authentication Proxy and HSS, and the interface between HSS and BM-SC for MBMS**

Response to: **N/A**
Release: Rel-6
Work Item: Support for subscriber certificates (SEC1-SC), Security issues of Presence Capability (PRESNC), MBMS
Source: SA3
To: CN4
Cc: -

Contact Person:
Name: Philip Ginzboorg
Tel. Number: +358504836224
E-mail Address: philip.ginzboorg@nokia.com

Attachments: S3-030241, S3-030282

1. Overall Description of Support for subscriber certificates

SA3 are currently evaluating the architecture implementing “support for subscriber certificates” work item. It includes two new function entities BSF (bootstrapping) and NAF (network application), among the others. BSF and NAF communicate over the D interface; BSF and HSS communicate over the C interface. In their earlier LS (S3-030131) SA3 informed CN4 that SA3 consider reusing the Cx specifications in D interface. Now SA3 would like to update CN4 with the lists of identified requirements on the two interfaces, as well as the attached contributions that attempt to establish an initial studying. It should be noted that the names of the C and D interfaces are for temporary use only and proper names could be provided at later stage when concept is more mature.

Requirements on protocol C from attached S3-030241:
The BSF is able to

- Communicate securely with a HSS.
- Send Authentication Vector information request to the HSS.
- Send optional User Profile request to the HSS.
- Receive Authentication Vector information from the HSS.
- Receive User Profile from the HSS.
- Preferably the HSS does not need modifications to support bootstrapping.
- All procedures are initiated by the BSF.

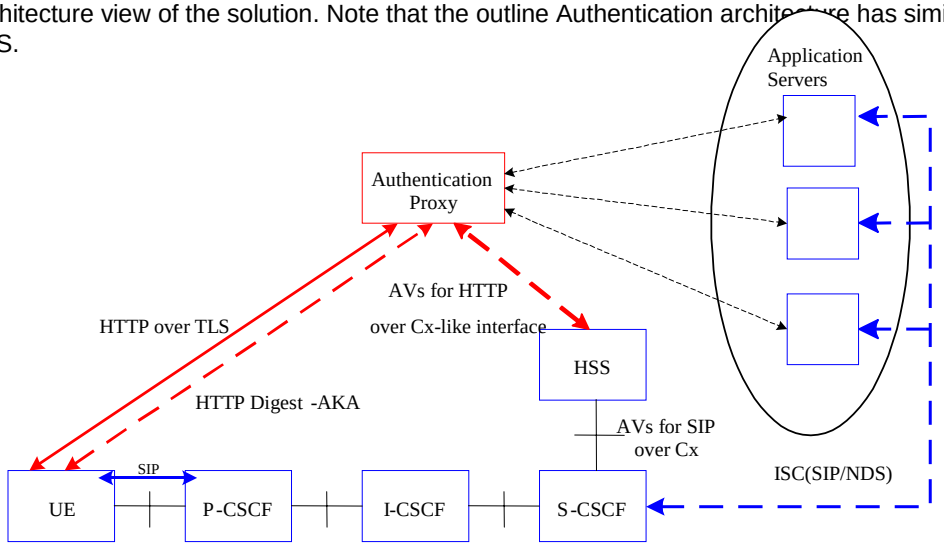
Requirements on protocol D from attached S3-030282:

- NAF is able to communicate securely with a subscriber’s BSF.
- NAF is able to send a key material request to the BSF.
- BSF is able to send the requested key material to the NAF.
- NAF is able to get the subscriber profile from BSF.

2. Overall Description of Security issues of Presence Capability

Meanwhile, SA3 work on another work item, Security issues of Presence Capability under which HTTP protocol is used over interface Mt between the UE and the SIP Application Servers cloud. This would require the UE authentication over HTTP. One potential solution introduces a new network entity that is completely trusted by the IMS sub-network, namely Authentication Prox/Authenticator, to communicate with HSS for fetching AKA Quintet challenge. The solution could also variant to fetch a subset of AKA Quintet with only one session key.

A figure is copied from an earlier contribution from earlier SA3 meeting (S3-020528) intends to give an whole architecture view of the solution. Note that the outline Authentication architecture has similarities to that of IMS.

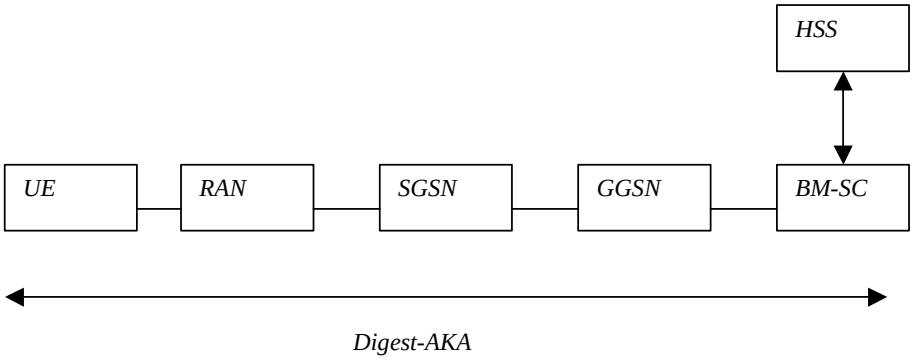


The exact requirements for Cx-like interface are for further study.

3. Overall Description of MBMS

SA3 is also working on the WI: Multimedia broadcast/multicast service (MBMS). It was proposed in SA3#28 (SA3 Tdoc S3-030248) as a conclusion that the authentication is done between the BM-SC and the UE. This implies that the Cx-interface may be utilized between the HSS and the BM-SC.

A figure is copied from proposal for SA3#28 (S3-030248) and intends to give an architecture view of the solution. Note that the use of Digest-AKA in this context has not been agreed by SA3 and is for further study. Note that the outline Authentication architecture has similarities to that of IMS.



The exact requirements for interface between HSS and BM-SC are for further study.

4. Actions to CN4

ACTION 1: **SA3 kindly ask CN4 to review the two attached contributions, and evaluate if they foresee any obstacle in reusing Cx for the C and D interface;**

ACTION 2: **SA3 kindly ask CN4 consider the feasibility of introducing Cx-like interface between Authentication Proxy and HSS, and the possibility of adopting Cx protocol for Presence service;**

ACTION 3: **SA3 kindly asks whether CN4 sees any problems with using the Cx-interface between the HSS and the BM-SC in the MBMS architecture.**

For Actions 2 and 3, CN4 is asked to comment on the expected timescales to complete the specification of new Cx-like interfaces for Presence and MBMS once the precise requirements are available.

5. Date of Next SA3 Meetings

SA3 #29	15th July – 18th July 2003	San Diego, U.S.A
SA2 #30	7th October – 10th October 2003	tbd

3GPP TSG SA WG3 Security — S3#28 **S3-030241**
6 – 9 May 2003
Berlin, Germany

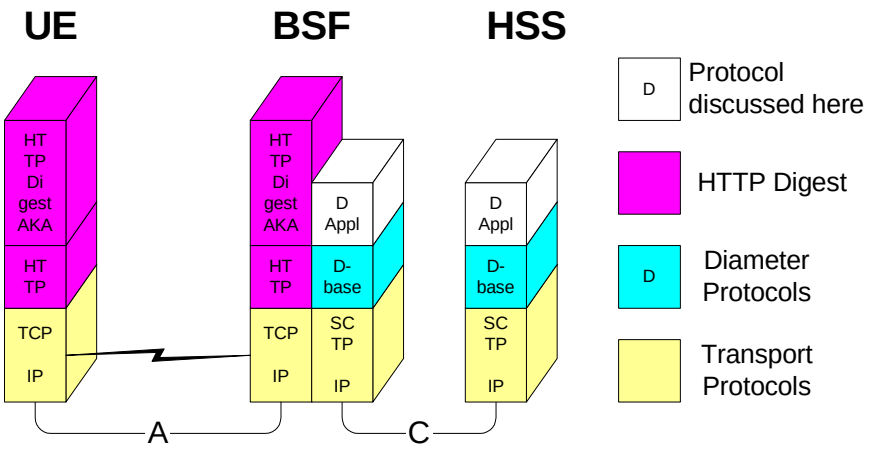
Source: **Nokia**

Title: **BSF-HSS (C interface) Bootstrapping protocol**

Document for: **Discussion and decision**

Agenda Item: **Support for subscriber certificates**

Table of Content:



1. INTRODUCTION

An adjunct contribution [S3-030203] defines the generic bootstrapping procedure. The bootstrapping procedure contains A (UE-BSF) and C (BSF-HSS) interfaces. The C interface is intra-operator interface used to fetch authentication vector and user profiles from HSS during the bootstrapping procedure.

For C interface implementation protocols two possible platforms have identified earlier:

- A Diameter application
- Revised MAP

This contribution discusses DIAMETRER based implementation of the C interface.

The study will show that the Bootstrapping C interface is possible to implement by direct reuse of 3GPP Diameter IMS Cx interface specification. This may however require existence of some IMS capabilities in the Bootstrapping implementation platform.

This discussion paper consists logically from two parts: The first part defines the general Bootstrapping C interface (chapters 3-5) with an example definition of a new Diameter application for Bootstrapping in C interface. The second part (chapter 6) basically describes the possible implementation of the C interface using unmodified 3GPP IMS Cx interface.

2. TERMINOLOGY

AUTN	Authentication token
AV	Authentication Vector. 3GPP AV=[RAND,AUTN,XRES,CK,IK].
AVP	Attribute-Value-Pair in Diameter messages.
BS	Bootstrapping
BSF	Bootstrapping Server Functionality (a network element)
CK	Confidentiality Key
IK	Integrity Key
IMPI	IMS Private Identity
IMPU	IMS Public Identity
ISIM	IMS SIM
NAI	Network Access Identifier
RAND	Challenge in authentication
SCTP	Stream Control Transmission Protocol
XRES	Response in authentication
{ }	Mandatory AVP in the Diameter messages
[ ]	Optional AVP in the Diameter messages
*	Multiple instances of the AVP possible in the Diameter messages

3. REQUIREMENTS

Figure 2 illustrates the location of the discussed protocol in an example protocol stack of bootstrapping procedure.

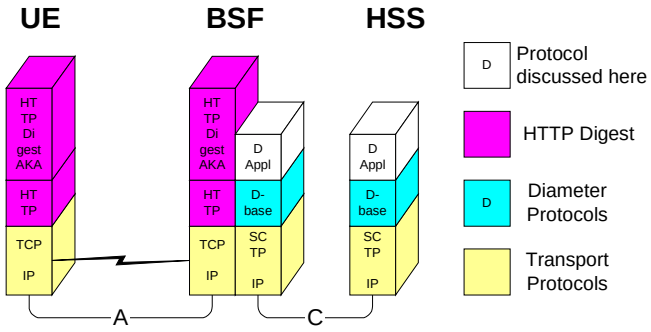


Figure 1: The Bootstrapping Procedure protocol stack

Requirements for C interface are:

- The BSF is able to communicate securely with a HSS.
- The BSF is able to send Authentication Vector information request to the HSS.
- The BSF is able to send optional User Profile request to the HSS.
- The HSS is able to send Authentication Vector information to the BSF.
- The HSS is able to send User Profile to the BSF.
- Preferably the HSS does not need modifications to support bootstrapping.
- All procedures are initiated by the BSF.

4. REQUIRED DIAMETER AVPS FOR BOOTSTRAPPING IN C

The following figure illustrates the required basic procedure in the Bootstrapping C interface.

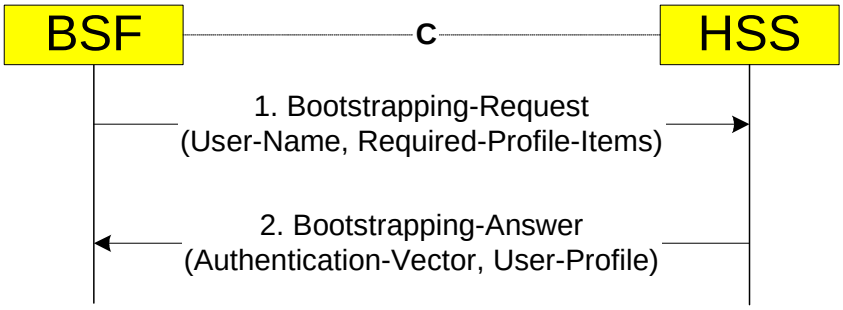


Figure 2: The Bootstrapping Procedure in C interface

Bootstrapping procedure requires following Bootstrapping specific Diameter AVPs in C interface.

4.1 In Bootstrapping-Request (BSF -> HSS)

User-Name AVP:

- Some user identity that BSF can give and HSS recognize and that needs authentication.
- Mandatory.

Required-Profile-Items AVP

- Indicates what kind of or what part of user profile is needed. Require-Profile-Items AVP may contain a code of a redefined profile or list of needed user profile information elements. The exact definition and usage is FFS. The simplest way is always order the whole user profile to the BSF. If this is true, this AVP is not needed.
- Optional.

4.2 In Bootstrapping-Answer (BSF <- HSS)

Authentication-Vector AVP:

- Contains 3GPP Authentication Vector information i.e. RAND, AUTN, XRES, CK and IK.
- Mandatory.

User-Profile AVP:

- Contains the user profile information.
- Optional.

5. C INTERFACE BASED ON A NEW DIAMETER APPLICATION

Using the notation of [3GPP TS 29.229] the needed request-response message pair for the C interface can be outlined as follows. The fields specific for the bootstrapping procedure and explained in chapter 4 are marked by **bold**. Other AVPs belongs to mandatory AVPs in the Diameter Base Protocol [DIAMETER].

The following message specification is only a tentative illustration about how the C interface Diameter application messages may look like on ground the current assumption for this document.

Because this is a new diameter application, the handling behavior of the HSS can be freely defined to meet requirements of this application.

The symbol ### represents the Diameter application number to be allocated by IETF/IANA.

5.1 Bootstrapping-Request (BSR) Command

The Bootstrapping-Request (BSR) command, indicated by the Command-Code field set to 1 and the 'R' bit set in the Command Flags field, is sent by a BSF to a HSS in order to request Authentication vector and optional application user profile for user identified by User-Name. Only the mandatory AVPs from the base diameter protocol are included.

Message Format:

```
< BS-Request> ::=Diameter Header: ###: 1, REQ, PXY >
            <Session-Id >
            { Vendor-Specific-Application-Id }
            { Auth-Session-State }
            { Origin-Host }
            { Original-Realm }
            { Destination-Realm }
            { User-Name }                    # IMSI/IMPI
            [ Required-Profile-Items]
```

5.2 Bootstrapping-Answer (BSA) Command

The Bootstrapping-Answer (BSA) command, indicated by the Command-Code field set to 1 and the 'R' bit cleared in the Command Flags field, is sent by a HSS in response to the Bootstrapping-Request command.

Message Format:

```
< BS-Answer> ::=< Diameter Header: ###: 1 >
            < Session-Id >
            { Vendor-Specific-Application-Id }
            { Auth-Session-State }
            { Origin-Host }
            { Origin-Realm }
            { Authentication-Vector }
            [ User-Profile ]
```

6. C INTERFACE IMPLEMENTATION WITH EXISTING DIAMETER APPLICATIONS

There are two ways to reuse some existing Diameter application also for Bootstrapping C interface:

- **Direct reuse:**
  We can try to adapt the bootstrapping procedure so that we can use somehow the existing Diameter applications messages and especially their all ready fixed AVPs directly.

- **Adding new AVPs**:
  If the above is not possible or practical, we can extent the accepted AVP set in reused Diameter application. The alternatives for this are listed below.

Basically, we have two alternatives to extend existing Diameter applications:

1. **Standard extension** adding new AVPs:
   We may extent an existing similar Diameter application standard by adding new bootstrapping specific AVPs. This requires acceptance by IETF.
   This the clearest way, but may produce timing problems.

2. **Vendor specific extensions** adding new AVPs:
   Because the Bootstrapping C interface is operator internal interface (BSF-HSS) it is also possible to add the needed AVPs as vendor specific extension.
   IANA is already reserved Vendor identifiers 10415 for 3GPP and 5535 for 3rd Generation Partnership Project 2 (3GPP2) possible for this kind of usage. (See http://www.iana.org/assignments/enterprise-numbers).

The best case is the direct reuse. If the direct reuse is not for some reason possible the next target is the extension alternatives i.e. standard extension or the Vendor specific extension.

The following chapter will show that the reuse of 3GPP IMS Cx Diameter application may be possible with certain redefinition.

6.1 C interface based on Diameter Cx

This solution is based on a sub set of the 3GPP IMS Cx (HSS – CSCF) registration procedure from [3GPP TS 29.228] and its Diameter implementation from [3GPP TS 29.229].

6.1.1 Useful parts

There are three relevant message pairs in IMS Cx:

- **Multimedia-Authentication-Request/Answer (MAR/MAA)** that is indented to multimedia server in order to request security information from HSS. This function is similar to Bootstrapping C interface Authentication vector down loading function. The S-CSCF that corresponds the BSF initiates the procedure.
  These messages are called Cx-AuthDataReq/Cx-AuthDataResp in 3GPP TS 29.228.
- **Push-Profile-Rquest/Answer (PPR/PPA**) that is intended to update the user profile information in the S-CSCF when it changes in the HSS. The user profile push procedure is initiated by the HSS and is therefore not suitable for the bootstrapping C interface. This message pair is not apart of the Cx registration procedure. Usage of this message in the bootstrapping C interface requires probably modifications to the HSS.
- **Server-Assignment-Request/Answer (SAR/SAA)** that is indented to store the name of the server that is currently serving the user (not needed in C interface) and to down load information that the S-CSCF needs to give service to the user. The later function is similar to the Bootstrapping user profile down loading to the BSF. The S-CSCF, that corresponds the BSF, initiates the procedure.
  This message pair is called S-CSCF Registration/Deregistration-Notification in 3GPP TS 29.228.

The following AVPs are already defined for Cx:

Message	AVP	Cx usage	C interface comment
MAR, MAA, SAR, SAA	User-Name	IMPI	IMPI from HTTP Digest AKA username.
MAR	Public-Identity	This AVP contains the public identity of a user in the IMS. The syntax of this AVP corresponds either to a SIP URL [SIP],[URI] or a TEL URL [RFC 2806].	The IMPU in UE may be used if necessary. If the CX interface allows to leave it empty, it can be omitted (FFS).
MAA	SIP-Auth-Data-Item	Contains among others Confidential Key (CK) and Integrity key (IK), RAND, AUTN and XRES.	Contains all needed elements of authentication vector. This is the Authentication-Vector AVP in sect. 4.2.
SAR	User-Data-Request-Type	Indicates if Complete profile, Registered Profile or unregistered profile is required.	Probably does NOT allow selection of security association application specific subsets from user profile. Probably has always constant value of “complete profile required”.
SAA	User-Data	Relevant (in SIP point of view) user profile.	Probably will contain the complete user profile (see above comment).

Based on the above table, we can map the Bootstrapping specific application AVPs presented in chapter 4 correspondences with Cx AVPs in the table below:

interface AVP (from chapter 4).	x AVP	omment
SR User-Name	AR User-Name	k if IMPI is available for C interface n the BSF.
SR Required-Profile-Items	AR User-Data-Request-ype	robably enables only down loading he complete user profile information.
SA Authentication-Vector	AA SIP-Auth-Data-Item	k for C interface
SA User-Profile	AA User-Data	sable in C interface.

Summary:

- The Cx based transfer of authentication vector data is no problem in C interface.
- Down loading an unrestricted user profile is no problem.
- The reuse of IMS Cx user identities requires usage of IMS compatible user identities. Probably IMPI can be user as User-Name. Also identities compatibility with the Bootstrapping A interface protocol, which is selected later, is ffs. If Digest AKA is used, then IMPI can be used.
- The usage of Cx for bootstrapping as discussed earliermay cause error situation in the HSS (FFS).

6.1.2 Two phases Cx-based C interface procedure.

No single Cx message pairs meet directly the requirements of Bootstrapping C interface alone. The sequential usage of message pairs MAR/MAA and SAR/SAA can be adapted to the Bootstrapping C interface requirements.

If one phase procedure for bootstrapping in C interface is required, we must start a standardization procedure to extend the Cx specification (i.e. adding User-Data AVP to MAA). The same holds if possibility to specially restrict the down loadable user profile is required.

From the above reasons the two phases Diameter Cx based solution is analyzed here in more details.

6.1.2.1 Procedure

The Figure 3 outlines the two phases Cx based solution for Bootstrapping C interface.

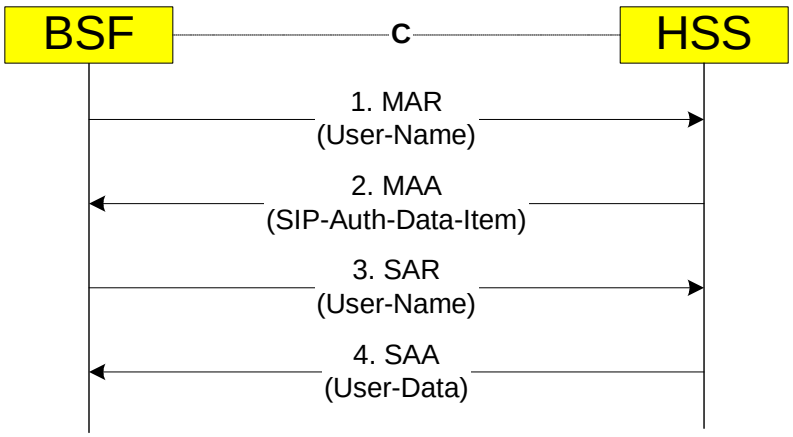


Figure 3: Two phases Cx based Bootstrapping Procedure in C interface

In the above solution the down loading of specially restricted user profiles is probably not possible. The adequacy of the IMS SIP user profile for the application that utilisates the bootstrapping procedure is FFS.

In the following two chapters the content of the messages are given in the same format as in 3GPP 29.229. The curly brackets indicate mandatory AVP. The square brackets indicate optional AVP.

6.1.2.2 MAR/MAA message pair

The Multimedia-Authentication-Request/Answer (MAR/MAA) message definition follows. The given definitions are based on the newest Diameter Cx specification [TS 28.229] that includes some changes about mandatory parameters compared to the Cx parameters defined in [TS 28.228].

The exact content of mandatory Cx AVPs is FFS. The earlier discussed AVPs are marked by bold.

```
< Multimedia-Auth-Request> ::=<Diameter Header: 303: TBD, REQ >
              < Session-Id >
              { Vendor-Specific-Application-Id }
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              { Destination-Realm }
              [ Destination-Host ]
              { User-Name }                        # IMPI of the user
              { Public-Identity }                  # IMPU of the user
              [ SIP-Auth-Data-Item ]               # Omitted
              [ SIP-Number-Auth-Items]             # value "1".
              [ Server-Name ]                      # See remarks
              *[ AVP ]
              *[ Proxy-Info ]
              *[ Route-Record ]

< Multimedia-Auth-Answer> ::= < Diameter Header: 303: TBD >
              < Session-Id >
              { Vendor-Specific-Application-Id }
              [ Result-Code ]
              [ Experimental-Result]
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              [ User-Name ]                        # IMPI
              [ Public-Identity ]                  # Omitted
              [ SIP-Number-Auth-Items ]            # value "1"
              *[ SIP-Auth-Data-Item ]              # Contains user's AV info
              *[ AVP ]
              *[ Proxy-Info ]
              *[ Route-Record ]
```

Remark on Public-Identity AVP:
The current [TS 28.229] defines Public-Identity AVP as mandatory in the MAR. The C interface does not need it. The private IMPI in User-Name AVP is logically the identity that is to be authenticated. This is the only place where Public-Identity is strictly required. According [TS 29.228] 6.3.1 the HSS may check in the IMS Cx that the private and public identities belong to the same user. One idea is to use HTTP Digest AKA realm as Public-Identity. In the IMS this public identity is called IMPU. The availability of the IMPU in the BSF is FFS, if the Public-Identifier cannot be defined as optional in the MAR.

Remark on Server-name AVP:
The current Cx specification [TS 28.228] mandates that the server name, i.e. S-CSCF name, is included into the Multimedia-Auth-Request. This is needed in IMS, e.g. in the initial registration, in order to route SIP messages to the S-CSCF.

However, in bootstrapping functionality this is not needed and therefore it may be proposed that the AP requesting authentication items shall not include the server name. In this way the HSS can decide to maintain the existing IMS registration state, e.g. the name of the S-CSCF, and shall not overwrite the S-CSCF name with the new name. In addition, the Cx specification could be modified to allow optional Server-Name AVP in the MAR/MAA commands. There are benefits also in the IMS domain. Actually the server name is already optional in current Diameter Cx specification [TS 28.229].

Remark on missing Integrity and Confidential keys:
In Cx [TS 28.228], the integrity key is mandatory and the confidentiality key optionally returned in the MAA command. Current Diameter Cx specification [TS 28.229] does not show these AVPs at all, because they are included into SIP-Auth-Data-Item AVP.

6.1.2.3 SAR/SAA message pair

The Server-Assignment-Request/Answer (SAR/SAA) message definition follows. The exact content of mandatory Cx AVPs is FFS. The earlier discussed AVPs are marked by bold.

```
<Server-Assignment-Request> ::=< Diameter Header: 301, TBD, REQ, PXY >
              < Session-Id >
              { Vendor-Specific-Application-Id }
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              [ Destination-Host ]
              { Destination-Realm }
              [ User-Name ]                          # IMPI
              *[ Public-Identity ]                   # See remarks
              [ Server-Name ]                        # See earlier remarks
              { Server-Assignment-Type }             # Probably NO_ASSIGNMENT
              { User-Data-Request-Type }             # COMPLETE_PROFILE
              { User-Data-Already-Available }        # USER_DATA_NOT_AVAILABLE
              *[ AVP ]
              *[ Proxy-Info ]
              *[ Route-Record ]

<Server-Assignment-Answer> ::=< Diameter Header: 301, TBD >
              < Session-Id >
              { Vendor-Specific-Application-Id }
              [ Result-Code ]
              [ Experimental-Result ]
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              { User-Name }                                  # IMPI
              [ User-Data ]                                  # User profile
              [ Charging-Information ]                       # See remarks
              *[ AVP ]
              *[ Proxy-Info ]
              *[ Route-Record ]
```

Remarks about Public-Identity and User-Data-Request-Type:
The definition of the SAR requires on optional set of Public-Identity AVPs. If the HSS's current definition requires at least one Public-Identity, the same Public-Identity than in the MAR request can be included. This is FFS. Probably Public-Identity is needed only in the case where the User-Data-Request-Type AVP indicates that REGISTERED/UNREGISTERED_PROFILE is needed to one or more public indentifiers. This maybe useful if it is required that the application that utilisates the security assoations established by the Bootstrapping procedure needs to user profiles spesific to public indentity. Otherwise User-Data-Request-Type has always a value of "COMPLETE_PROFILE".

Remarks about Charging-Information:
If also Charging-Information besides the user profile is needed for application, it is also automatically available in the SAA.

6.2 C interface based on Diameter Wx

The 3GPP WLAN Wx is intended to be used between the 3GPP AAA server and the HSS. The functionality of Wx contains retrieval of authentication vector from HSS and WLAN access-related subscriber information (profile) from HSS. Both functionalities are the basic requirements for the C interface. However currently there is no protocol specification available about it [3GPP TS 23.234]. It is not yet decided is WLAN Wx MAP or Diameter-based either.

6.3 C interface based on NASREQ

Draft-ietf-aaa-diameter-nasreq-10.txt describes two diameter messages: AA-request and AA-answer. [NASREQ]

The draft species many optional AVPs for those messages for different authentication or authorization protocols. Among the mentioned protocols are:

- CHAP – PPP Challenge- Handshake Authentication Protocol (CHAP)
- ARAP
- User-Password
- Framed access authorization for PPP, SLIP, etc. support
- Login-IPv6
- VPN/Tunneling
- Accounting

It seems to be possible to reuse NASREQ messages by adding C interface-specific AVPs as one more optional extension.

These optional C interface specific AVPs are described in Chapter 4. The exact set of NASREQ AVPs to use is ffs if needed.

7. SUMMARY

The direct reuse of 3GPP IMS Cx specification may be possible and should therefore set as a target solution for further investigation for Bootstrapping C interface. The standardization of IMS Cx interface is currently more mature than the other good alternative i.e. WLAN Wx interface.

The 3GPP IMS Cx contains logically the needed information elements for the bootstrapping C interface. The exact usage of IMS identifiers in the bootstrapping and the unmodificated usage of the HSS may require some further study. There may also be some benefits if the HSS can see distinction between S-CSCF and BSF requesting the vectors.

One area where some problem in the direct reuse of 3GPP IMS Cx interfaces can appear is that can the unmodified HSS smoothly accept the proposed Cx usage as a subset of the current registration procedure. This is FFS.

The direct usage of Diameter Cx interface sets at least the following requirements to the Bootstrapping procedure:

- In order to direct reuse of 3GPP IMS Cx interface ability to use some IMS specific identifier may be required from the bootstrapping implementation platform (FFS).

- The HSS may download probably an unnecessary large user profile. The selection of needed information in the user profile must be performed in the BSF according the application that is served (FFS).

8. REFERENCES

[S3-030203] Bootstrapping of application security using AKA and support for subscriber certificates.

[DIAMETER] IETF aaa working group, draft-ietf-aaa-diameter-17.txt

[NAI] The Network Access Identifier. IETF RFC 2486. January 1999.

[NASREQ] IETF aaa working group, draft-ietf-aaa-diameter-nasreq-10.txt

[RFC 2806] URLs for Telephone Calls

[SIP] SIP: Session Initiation Protocol. IETF RFC 3261.

[URI] Uniform Resource Identifiers (URI): Generic Syntax. IETF RFC 2396

[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 29.228] Cx and Dx interfaces based on the Diameter protocol; Protocol details; (Release 5); V5.3.0 (2003-03)

3GPP TSG SA WG3 Security — S3#28 **S3-030242**
6 –9 May 2003
Berlin, Germany

Source: **Nokia**

Title: **NAF-BSF (D interface) protocol**

Document for: **Discussion and decision**

Agenda Item: **Support for subscriber certificates**

Table of Content:

1. INTRODUCTION

An adjunct contribution [S3-TS] defines a generic bootstrapping server function (BSF) that will allow a UE to mutually authenticate BSF using the AKA protocol, and agree on session keys. UE and an operator-controlled network application function (NAF) can then run some application specific protocol where the authentication of messages will be based on the session keys agreed with BSF.

This contribution discusses the D interface. The NAF uses the D interface to fetch the key material agreed during the previous Bootstrapping procedure and possibly subscriber profile information from the BSF. Such functionality is typical of AAA protocols such as RADIUS [RADIUS] or DIAMETER [DIAMETER].

This contribution discusses DIAMETRER based implementation of the D interface.The study will show that the D interface is possible to implement by reusing the 3GPP IMS Diameter Cx interface specification.

Basically the similar tasks (downloading authentication info and user profile) are performed in the C interface in the bootstrapping procedure (S-CSCF - HSS). The main differences to the requirements of C interface Diameter solution are:

- Unlike HSS, NAF and BSF are new functional elements.
- Unlike the C interface, the D interface may evolve to be inter-operator interface.

This discussion paper has logically two main parts: The first part defines the general D interface (chapters 3-5) with an example definition of a new Diameter application for D interface. The second part (chapter 6) describes a possible implementation of the D interface using 3GPP IMS Cx interface.

2. TERMINOLOGY

AVP	Attribute-Value-Pair in DIAMETER messages.
BSF	Bootstrapping Server Functionality (a network element)
BSP	Bootstrapping Procedure
CK	Confidentiality Keys
IK	Integrity Key
Ks	Session Key
NAF	Network Application Function (a network element)
SCTP	Stream Control Transmission Protocol
{ }	Mandatory AVP in the Diameter messages
[ ]	Optional AVP in the Diameter messages
*	Multiple instances of the AVP possible in the Diameter messages

3. REQUIREMENTS

BSF and NAF may be located in the same network as the HSS, or they may be located in different networks. Both possibilities are illustrated in Figure 1.

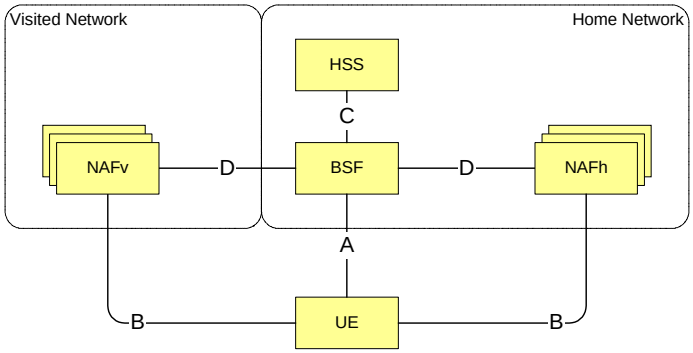


Figure 1: NAF may be in the home and in the visited network

Figure 2 illustrates a possible protocol stacks structure in network elements that are involved in bootstrapping of application security from 3G AKA and support for subscriber certificates.

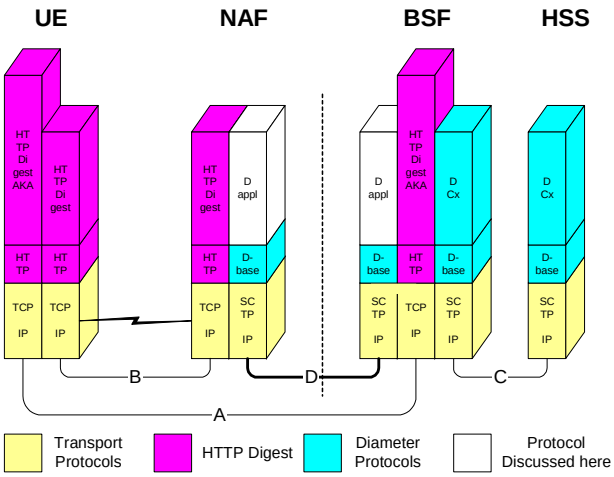
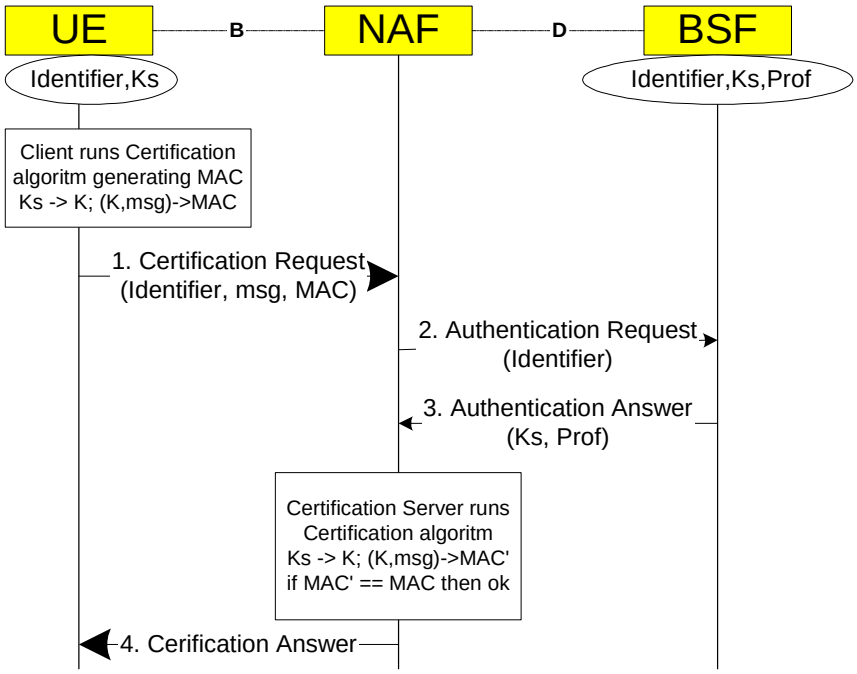


Figure 2: protocol stacks

The functionality of D interface, as outlined in [S3-030050 Nokia, Siemens] is as follows.

- After running establishing shared secret with BSF based on AKA, the UE contacts NAF
- NAF starts protocol D with BSF
- NAF requests key material corresponding to the information supplied by the UE to the NAF (e.g. a transaction identifier - TID) in the start of protocol B.
- BSF supplies to NAF the requested key material.
- NAF derives the keys required to protect protocol B from the key material in the same way as the UE did.

Figure 3 illustrates this functionality. As an example is used subscriber certification procedure. The underlying assumption in this procedure is that authentication and protection of communication between UE and NAF is based on shared symmetric key.



MAC represents all credentials **msg** is appl. specific dataset
Prof is application specific part of user profile

Figure 3: Usage procedure for Security Association created by the bootstrapping procedure

4. REQUIRED DIAMETER AVPS FOR D INTERFACE

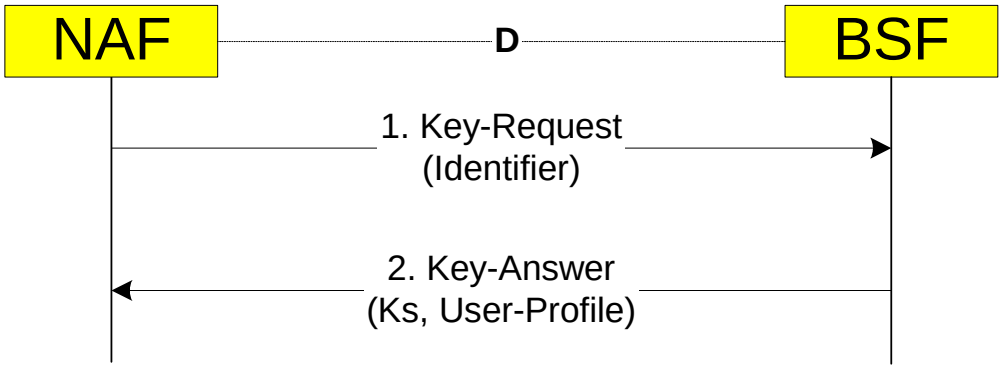


Figure 4: The Bootstrapping Procedure in D interface

4.1 In Key-Request (NAF -> BSF)

Transaction-Identity AVP:

- Temporary user transaction identity that is created during the bootstrapping procedure and stored to the BSF and the UE.
- Mandatory.

4.2 In Key-Answer (NAF <- BSF)

Derived-Key:

- Contains 256 bits long derived session key (Ks) or corresponding information for derivation.
- The derived key shall be derived from AKA key material e.g. by concatenating CK and IK
- Mandatory.

User-Profile AVP:

- Contains the required user profile information. The definition and usage of this information depens on NAF.
- Optional.

5. D INTERFACE BASED ON NEW DIAMETER APPLICATION

Using the notation of [3GPP TS 29.229] the needed request-response messages for D interface can be outlined as follows. The fields specific for this procedure and described earlier in chapter 4 are marked by **bold**. Other AVPs belong to mandatory AVPs in the diameter Base Protocol [DIAMETER].

The following message specification is only a tentative illustration about how messages in an application using security association created by the bootstrapping procedure may look like.

The symbol ### present the Diameter application number to be allocated by IETF/IANA.

5.1 Key-Request (KER) Command

The Key-Request (KER) command, indicated by the Command-Code field set to 1 and the 'R' bit set in the Command Flags field, is sent by the NAF to the BSF in order to fetch Ks and optional user profile.

Message Format

```
< Key-Request> ::=Diameter Header: ###: 1, REQ, PXY >
            <Session-Id >
            { Vendor-Specific-Application-Id }
            { Auth-Session-State }
            { Origin-Host }
            { Original-Realm }
            { Destination-Realm }
            { Transaction-Identity}
            *[ Proxy-Info ]
            *[ Route-Record ]
```

5.2 Key-Answer (KEA) Command

The Key-Answer (KEA) command, indicated by the Command-Code field set to 1 and the 'R' bit cleared in the Command Flags field, is sent by a server in response to the Key-Request command.

Message Format

```
< Key-Answer> ::=< Diameter Header: ###: 1 >
            < Session-Id >
            { Vendor-Specific-Application-Id }
            { Auth-Session-State }
            { Origin-Host }
            { Origin-Realm }
            { Derived-Key }            # Ks e.g. CK|IK
            [ User-Profile ]           #
            *[ Proxy-Info ]
            *[ Route-Record ]
```

Optional User-Profile AVP is sent only if there is some user profile to send.

6. D INTERFACE IMPLEMENTATION WITH EXISTING DIAMETER APPLICATIONS

There are two ways to reuse some existing Diameter application for D interface:

- **Direct reuse:**
  We can try to adapt the security association usage procedure so that we can use somehow the existing Diameter applications messages and especially their already fixed AVPs directly. If this is really possible is still FFS.

- **Adding new AVPs**:
  If the above is not possible or practical, we can extent the accepted AVP set in reused Diameter application. The alternatives for this are listed below.

Basically, we have two alternatives to extend existing Diameter applications also for D interface:

1. **Standard extension** adding new AVPs:
   We may extent an existing similar Diameter application standard by adding new bootstrapping specific AVPs. This alternative requires acceptance by IETF.
   This the clearest way, but may produce timing problems.

2. **Vendor specific extensions** adding new AVPs:
   It may be possible to add the needed AVPs as vendor specific extensions.
   IANA is already reserved Vendor identifiers 10415 for 3GPP and 5535 for 3rd Generation Partnership Project 2 (3GPP2) possibly for this kind of usage. (See http://www.iana.org/assignments/enterprise-numbers).

The best case is the direct reuse. If the direct reuse is not for some reason possible, the the possibilities to use standard extension or vendor specific extensions must be studied.

The following chapter will show that the 3GPP Cx Diameter application is possible to adapt for D interface.

6.1 D interface based on Diameter Cx

This solution is based on 3GPP IMS Cx (HSS – CSCF) registration procedure from [3GPP TS 29.228] and its Diameter implementation from [3GPP TS 29.229].

6.1.1 Useful parts

There are two relevant message pairs in Cx:

- **Multimedia-Auth-Request/Answer (MAR/MAA)** that is intended to multimedia server in order to request security information from HSS. This function is similar to D interface Authentication vector downloading function.
  These messages are called Cx-AuthDataReq/Cx-AuthDataResp in 3GPP TS 29.228.
- **Push-Profile-Request/Answer (PPR/PPA**) that is intended to update the user profile information in the S-CSCF when it changes in the HSS. The user profile push procedure is initiated by the HSS and is therefore it was not suitable for the bootstrapping C interface. This reason does not hold here, because the BSF can be defined freely.
- **Server-Assignment-Request/Answer (SAR/SAA)** that is intended to store the name of the server that is currently serving the user (not needed in D interface) and to download information that the S-CSCF needs to give service to the user. The later function is similar to the D interface user profile downloading to the NAF.
  This message pair is called S-CSCF Registration/Deregistration-Notification in 3GPP TS 29.228.

The following AVPs are already defined for Cx:

Message	AVP	Cx usage	D interface comment
MAR, PPR	User-Name	Private user identity	This is the transaction identity in username field in the HTTP digest from the B interface
MAA	SIP-Auth-Data-Item	Contains among others Confidential Key (CK) and Integrity key (IK), challenge and AUTN.	Does not directly contain Ks, but if the Ks is only a concatenation of CK and IK then this can download them and the NAF will perform the concatenation. Irrelevant fields in the AVP may be empty.
SAA, PPR	User-Data	Relevant (in SIP point of view) user profile.	Probably will contain the complete user profile(FFS).

Based on the above table, we can map the specific application AVPs presented in chapter 4 correspondences with Cx AVPs in the table below:

D interface AVP (from chapter 4)	Cx AVP	Comment
KeyReq Transaction-Identity	User-Name	Ok if transaction identifier is in same format.
KeyAns Derived-Key	UAA SIP-Auth-Data-Item	Ok for D interface, if Ks consists of concatenated CK and IK (other fields shall be empty).
KeyAns User-Profile	SAA User-Data or PPR User-Data	If the unnecessary information in user profile is emptied, this may be usable in D interface.

Summary:

- The Cx based transfer of authentication data is no problem in D interface.
- If restriction of the downloadable user profile information is needed, the BSF can empty the fields that are not needed by NAF.

6.1.2 Two phases Cx based D interface procedure.

No single Cx message pairs meet the requirements of D interface alone. The sequential usage of two message pairs can be adapted to the D interface requirements. These pairs are:

1. MAR/MAA and PPR/PPA
2. MAR/MAA and SAR/SAA

If one phase procedure for bootstrapping in C interface is required and Cx is decided to be used, we must start a standardization procedure to extent the Cx specification (adding User-Data AVP to MAA).

From the above reasons two phases Diameter Cx based solution is analyzed here in more details. Because the first PPR/PPA based alternative looks simpler and therefore more probably implementation only it further analyzed in details. The second SAR/SAA based solution is similar to the adjacent contribution [C INTERFACE] but is simpler.

6.1.2.1 Procedure

The following figures outlines the two alternatives for the two phases Cx based solution for D interface.

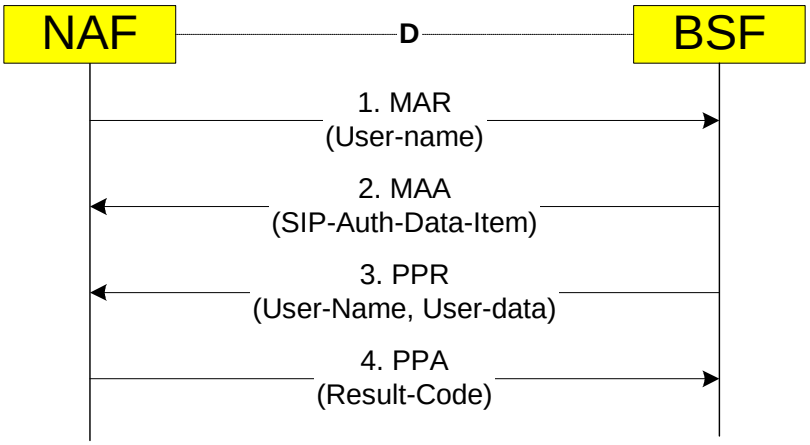


Figure 5: Two phases Cx based Bootstrapping Procedure in D interface – Alternative 1

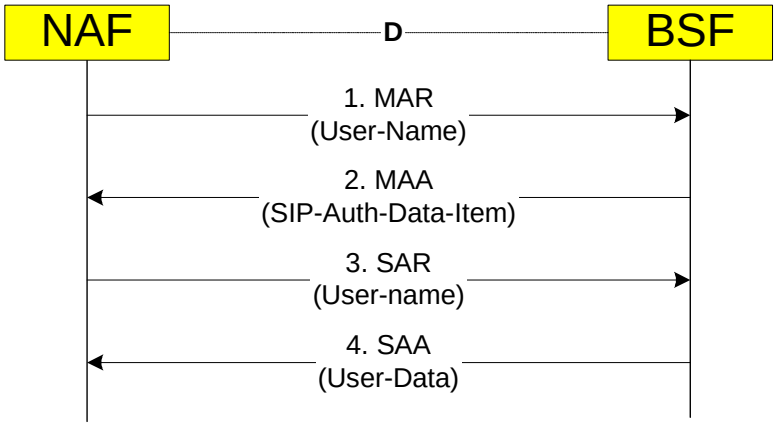


Figure 6: Two phases Cx based Bootstrapping Procedure in D interface – Alternative 2

The downloading of partial user profiles is probably not possible. The not needed user profile elements should be emptied in the BSF.

The content of the messages are given in following sections for alternative 1.The content of the messages are given in the same format as in 3GPP 29.229. The curly brackets indicate mandatory AVP. The square brackets indicate optional AVP.

6.1.2.2 MAR/MAA message pair

The UAR/UAA message definition follows. The exact content of mandatory Cx AVPs is FFS. The earlier discussed AVPs are marked by bold.

```
< Multimedia-Auth-Request> ::=<Diameter Header: 303: TBD, REQ >
              < Session-Id >
              { Vendor-Specific-Application-Id }
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              { Destination-Realm }
              [ Destination-Host ]
              { User-Name }                        # Transaction identity
              { Public-Identity }                  # May be empty.
              [ SIP-Auth-Data-Item ]               # Omitted
              [ SIP-Number-Auth-Items]             # value "1".
              [ Server-Name ]                      # Omitted, see remarks
              *[ AVP ]
              *[ Proxy-Info ]
              *[ Route-Record ]

< Multimedia-Auth-Answer> ::= < Diameter Header: 303: TBD >
              < Session-Id >
              { Vendor-Specific-Application-Id }
              [ Result-Code ]
              [ Experimental-Result]
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              [ User-Name ]                        # Transaction identity
              [ Public-Identity ]                  # Omitted
              [ SIP-Number-Auth-Items ]            # value "1"
              *[ SIP-Auth-Data-Item ]              # Contains CK and IK
              *[ AVP ]
              *[ Proxy-Info ]
              *[ Route-Record ]
```

Remark about Server-name AVP:
The current Cx specification [TS 28.228] mandates that the server name, i.e. S-CSCF name, is included into the Multimedia-Auth-Request. This is needed in IMS, e.g. in the initial registration, in order to route SIP messages to the S-CSCF. This kind of functionality is probably not needed in the D interface. Actually the server name is already optional in current Diameter Cx specification [TS 28.229].

Remark about missing Integrity and Confidentiality keys:
In Cx [TS 28.228], the integrity key is mandatory and the confidentiality key optionally returned in the MAA command. Current Diameter Cx specification [TS 28.229] does not show these AVPs at all, because they are included into SIP-Auth-Data-Item AVP.

6.1.2.3 PPR/PPA message pair

The Push-Profile-Request/Answer (PPR/PPA) message definition follows. The exact content of mandatory Cx AVPs is FFS. The earlier discussed AVPs are marked by bold.

```
<Push-Profile-Request> ::=< Diameter Header: 302, TBD, REQ >
              < Session-Id >
              { Vendor-Specific-Application-Id }
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              { Destination-Host }
              { Destination-Realm }
              { User-Name }                    # Transaction Identity
              [ User-Data ]                    # User Profile
              *[ AVP ]
              *[ Proxy-Info ]
              *[ Route-Record ]

<Push-Profile-Answer> ::=< Diameter Header: 302, TBD>
              < Session-Id >
              { Vendor-Specific-Application-Id }
              [ Result-Code ]                  # Result code of operation
              [ Experimental-Result ]
              { Auth-Session-State }
              { Origin-Host }
              { Origin-Realm }
              *[ AVP ]
              *[ Proxy-Info ]
              *[ Route-Record ]
```

6.2 D interface based on Diameter Wx

The 3GPP WLAN Wx is indented to be used between the 3GPP AAA server and the HSS. The functionality of Wx contains retrieval of authentication vector and WLAN access-related subscriber information (profile). Both functionalities are the basic requirements for the D interface. However currently there is no protocol specification available about it [3GPP TS 23.234]. It is not yet decided is WLAN Wx MAP or Diameter-based either.

6.3 D interface based on NASREQ

Draft-ietf-aaa-diameter-nasreq-10.txt describes two diameter messages: AA-request and AA-answer. [NASREQ]

The draft specifies many optional AVPs for those messages for different authentication or authorization protocols. Among the mentioned protocols are:

- CHAP – PPP Challenge- Handshake Authentication Protocol (CHAP)
- ARAP
- User-Password
- Framed access authorization for PPP, SLIP, etc. support
- Login-IPv6
- VPN/Tunneling
- Accounting

It seems to be possible to reuse NASREQ messages by adding the D interface AVPs as one more optional extension. These optional D interface specific AVPs are described in Chapter 4. The exact set of NASREQ AVPs to use is ffs if needed.

7. SUMMARY

The direct reuse of 3GPP IMS Cx specification seems to be possible and should therefore set as a target solution for the D interface. The standardization of IMS Cx interface is currently more mature than the other good alternative – WLAN Wx interface.

Compared to the similar Bootstrapping C interface [C INTERFACE] the IMS Cx implementation of the D interface is simpler because unlike the HSS the corresponding BSF can be specially defined for D interface.

The direct usage of Diameter Cx interface sets only the following requirements to the Security Association usage procedures:

- The transaction identity from the B interface should be in compatible format with IMS Cx diameter User-Name AVP format.
- The selection of downloadable information for the NAF from the user profile must be performed in the BSF, not in HSS, according to the needs of NAF by emptying the unnesessary information elements.

8. REFERENCES

[S3-030050]	Nokia, Siemens, Bootstrapping of application security from 3G AKA and support for subscriber certificates.
[C INTERFACE]	S3-030241, Nokia, BSF-HSS (C interface) Bootstrapping protocol.
[S3-TS]	S3-030202, Nokia, Bootstrapping of application security using AKA and Support for Subscriber Certificates.
[RADIUS]	IETF RFC 2865
[DIAMETER]	IETF aaa working group, draft-ietf-aaa-diameter-17.txt
[NASREQ]	IETF aaa working group, draft-ietf-aaa-diameter-nasreq-10.txt
[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)