3GPP TSG SA WG3 Security — S3#28 **S3-030282**
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.

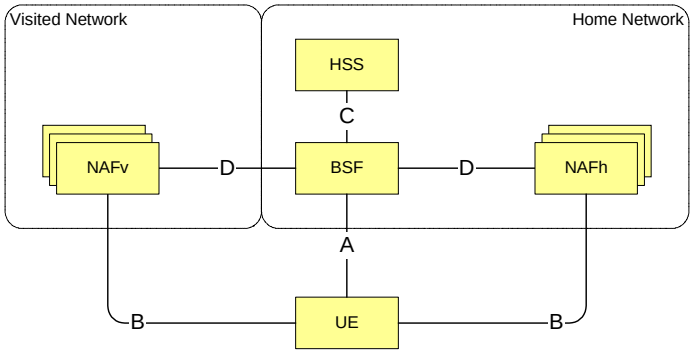


Figure 1: NAF may be in the home and in the visited network

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.

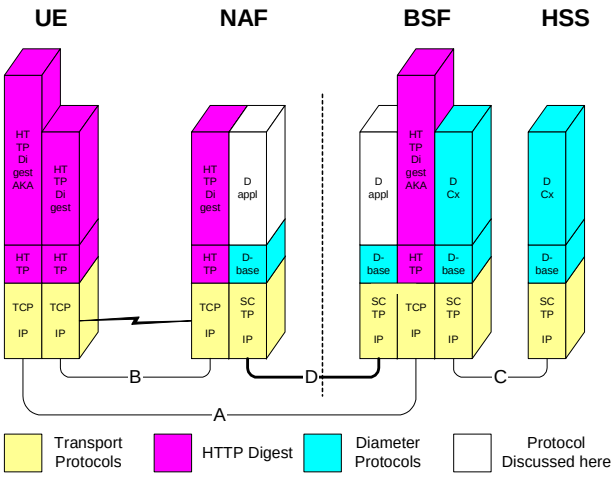
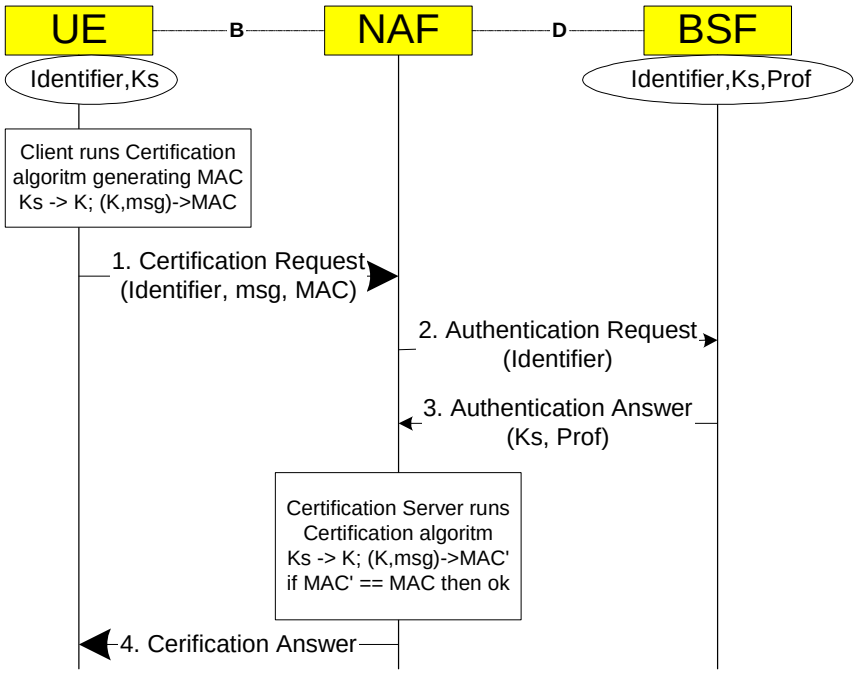


Figure 2: protocol stacks

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

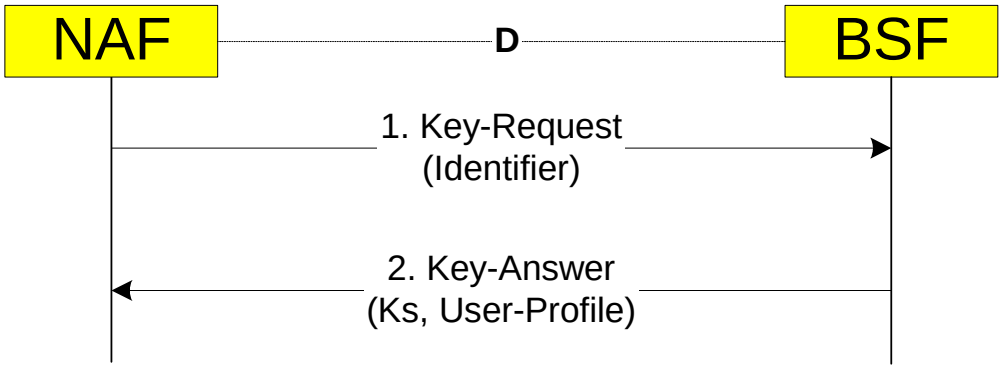


Figure 4: The Bootstrapping Procedure in D interface

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.

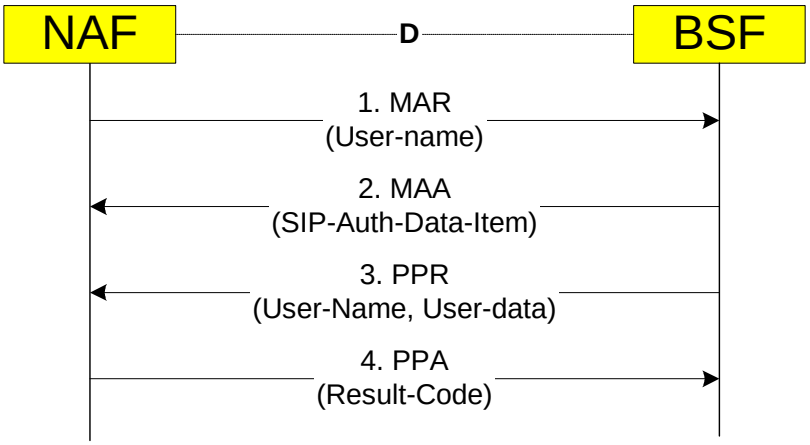


Figure 5: Two phases Cx based Bootstrapping Procedure in D interface – Alternative 1

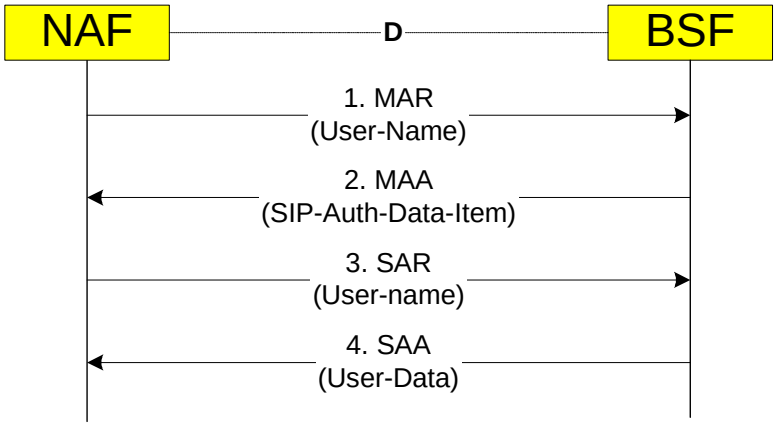


Figure 6: Two phases Cx based Bootstrapping Procedure in D interface – Alternative 2

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)