3GPP TSG SA WG3 Security — SA3#33 **S3-040224**
10-14 May 2004
Beijing, China

Source: **Siemens, Ericsson, Nokia**

Title: **GBA: Support of NAFs within the Visited Network**

Document for: **Discussion and decision**

Agenda Item: **GBA, MBMS**

1 Introduction

The GBA specification TS 33.220 v6.0.0 currently specifies: "*For this specification release, only the case is considered where bootstrapping server functionality and network application function are located in the same network as the HSS. In further specification release, other configurations may be considered*." It was pointed out during SA3#32 that a GBA-based key management solution for MBMS needs a solution for a BM-SC located within the visited network according to a service requirement from specification TS 22.146 v6.4.0 (MBMS stage 1) section 5.3: '*In case of roaming a user should also be able to subscribe and join Multicast Services that are provided locally in the visited network, as allowed by the user's home environment*'.

This contribution analyses the possible GBA-solutions to fulfil the MBMS-service requirement, with the aim to select an MBMS independent solution. The main conclusions of this paper are

(1) The BSF that receives authentication vectors from HSS shall reside within the same operator's network as the HSS (see section 2)

(2) That IPsec and TLS mechanism can both be used for protecting the GBA-interface Zn (see section 3). The use of a DIAMETER proxy within the Visited Network (trusted by the Home network) is advantageous to keep low the amount of needed security associations between the two networks.

2 GBA-configurations

Within this paper we call BSF in the home network BSF_H and BSF in the Visited Network BSF_V. Home network is abbreviated as HN and visited network as VN. Two types of solutions can be distinguished for allowing a NAF in the VN to use bootstrapped secrets. **The first type relies on a BSF_H, getting authentication vectors from HN HSS, and allowing NAFs from the VN to interwork with the BSF_H. A second type allows a BSF_V to get authentication vectors from HN HSS**. Within this context it is irrelevant whether the NAF resides at an Application Server or within an Authentication Proxy. The latter one is anyhow not applicable for MBMS as the BM-SC (acting as a NAF), uses the Ks_NAF for other purposes than authentication only.

The approach with a BSF_V accessing HN HSS via Zh interface has following disadvantages:

- The amount of Zh-interfaces towards the HSS increases drastically (i.e. equally with the amount of Visited networks). This approach goes against one of the guidelines developed for the GBA-architecture (see TS 33.220 clause 4.3.5): '*The number of different interfaces to HSS should be minimized'*.

- UE's will have to discover, manage and select the BSF-addresses for each BSF_v.

- The Zh-interface will become an inter-operator interface: An attack on the Zh-interface has more widespread consequences than an attack on a particular Zn-interface. The Zh-interface transports AV while a particular Zn-interface transports Ks_NAF. The attacker having obtained a 3GPP authentication vector is able to derive many Ks_NAF from it.

- AVs intended for bootstrapping purposes are handled within different servers (many BSF_V in addition to one BSF_H) which may lead to AV-resynchronizations.

It is therefore proposed to allow interconnection of NAFs from the VN to BSF$_H$ via Zn interface in order to provide a solution that is suitable for MBMS Rel-6.

The next section focuses on securing the Zn-interface if running between different operator networks. The same techniques could be used for securing the Zh-interfaces as it runs over the same protocols. But when approving the above proposal to connect from VN to BSF$_H$, the Zh-interface will always be an intra-operator interface such that the NDS/IP mechanisms according to TS 33.210 apply for Zh.

3 Securing Zh and Zn interfaces

3.1 Requirements

The existing requirements on the Zn-interface listed by TS 33.220 section 4.6.3 are:

The requirements for Zn interface are:

- *“mutual authentication, confidentiality and integrity shall be provided;*

NOTE: This requirement may be fulfilled by physical or proprietary security measures if BSF and NAF are located within the same operator’s network.

- *The BSF shall verify that the requesting NAF is authorised;*
- *The NAF shall be able to send a key material request to the BSF;*
- *The BSF shall be able to send the requested key material to the NAF;*
- *The NAF shall be able to get the subscriber profile information needed for security purposes from BSF;*
- *The BSF shall be able to indicate to the NAF the lifetime of the key material.”*

When the NAF is placed within the VN and the BSF within the HN, then the first requirement cannot be fulfilled anymore by using physical or proprietary measures. However NDS/IP mechanism could then be used to protect the Zn-interface when extended over the border between two operators. This allows providing **confidentiality and integrity protection** of the IP-messages. The Zn/Zh-interface both run Cx-interface like-protocols based on DIAMETER according to TS 29.109 (Bootstrapping and subscriber certificates; Diameter protocols; Stage 3 ; cf N4-040253 for the latest version) ‘. The specification TS 33.210 (NDS/IP) already covers a similar case i.e. the Cx-interface protection in Annex C.

But providing mutual authentication of the NAF and the BSF can not be fulfilled if NDS/IP is used in a hop-by-hop approach (e.g. Zb/Za/Zb-interface over the network border). The BSF needs a NAF authenticated identity before the requirement: ‘*The BSF shall verify that the requesting NAF is authorised’* can be fulfilled.

3.2 Available protection mechanisms

According to [RFC3588] there exist three possibilities to protect the DIAMETER messages:

A) Application type of protection (End-to-End).

Use of CMS on AVP level provides the possibility to sign/encrypt sensitive data (see section 2.9 of [RFC3588] on end-to-End security framework). Such a solution could be used to authenticate the DIAMETER identities which need to be authorized at the BSF. Confidentiality could be provided by a transport type mechanism (e.g. IPsec). The referenced [AAACMS] "Diameter CMS Security Application” however has **expired** and is not available as RFC.

B) Transport type of protection (Hop-by-hop).

a. TLS-mechanism is recommended to be used for **inter-domain** communication [RFC3436]. TLS support is mandatory for DIAMETER servers. In this case DIAMETER protected by TLS run over SCTP. TLS certificates are used then used for the BSF$_H$ and the many NAFs.

b. IPsec-mechanism is recommended to be used for **intra-domain**[1] communication [RFC3436]. IPsec support is mandatory for DIAMETER servers. If applying NDS/IP then the operator has to trust the SEGs security and trust the IP-layer security of the path between the NAF and the BSF (NDS/IP mechanism with hop-to-hop Zb/Za/Zb where Zb now needs to be mandated for Zn). As indicated before, the BSF cannot authorize the NAF identity anymore, so the NDS/IP domain approach cannot be used. However IPsec mechanism could still be used i.e. an IPsec End-to-End tunnel between the NAF and the BSF_H can be used.

The use of options included in B) to protect Diameter messages between BSF and NAF is preferred. The advantages and disadvantages of TLS (option B.a) and IPsec (option B.b) need to be studied further.

3.3 Optimized NAF-VN configuration

Figure 1 shows a simple configuration with direct connection from NAF_V to $BSF_{H.}$

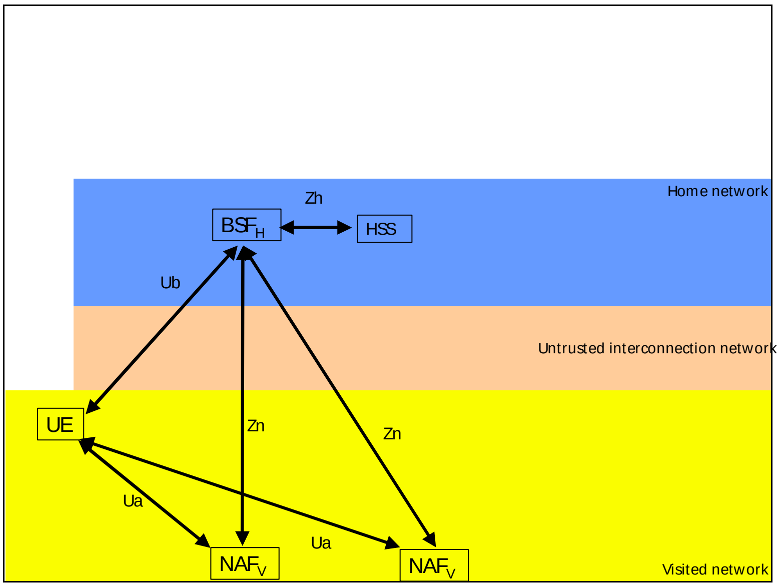

Figure 1: Simple configuration with direct connection from NAF_V to BSF_H

In this configuration adding a NAF in the Visited Network will require that the Visited Network operator contacts each GBA-roaming partner to administrate a security association, which includes either a public key or shared secret of that NAF, in their respective BSF. It should be noted that for the purposes of profile forwarding from the BSF to the NAF (cf SA3 email exploder discussions) some administration could be necessary in the BSF to explicitly allow the forwarding of some profile parameters. Without this administrative action NAF in the Visited Network cannot be used by roaming subscribers.

The configuration using a DIAMETER-proxy (hereafter called D-proxy) placed between the BSF_H and $NAF_{v,}$ as presented in Figure 2, provides some operational advantages for the topics mentioned above.

[1] It is unclear why the mechanism which is most suitable for inter-domain transport protection is not also recommended for intra-domain transport protection.

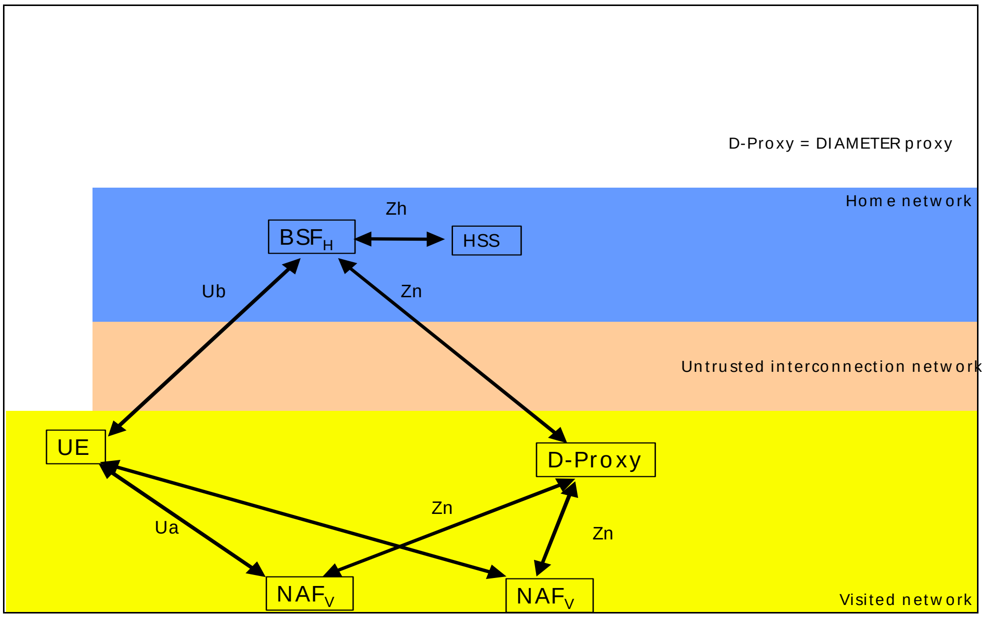

Figure 2: NAF in the Visited Network communicate with BSF_H via D-Proxy

Figure 2 provides a solution to keep the inter-operator security associations manageable, i.e. the BSF_H has to trust a Visited Network D-proxy only, and the D-proxy itself is trusted by the NAFs. Only one security association – that of D-proxy - needs to be checked in the BSF_H for each Visited Network. This requires that all DIAMETER requests towards the BSF_H shall be routed via the D-proxy. The identity of the originating NAF is available for the BSF_H via the 'Origin-Host[2] field and can be used to derive Ks_NAF at the BSF_H. Notice that D-Proxy does not have to be a new network element, but the D-Proxy functionality could be on any node supporting DIAMETER protocols (e.g. a BSF residing in the same network as the NAF).

With a use of a D-proxy the amount of security associations that need to be managed in the BSF_H can be kept low. However, D-proxy needs to check that the NAF_ID sent to BSF_H, and the identity used by NAF_V in its communications with D-proxy match to prevent one NAF_V posing as another NAF_V.

For example, if IPsec with shared secrets is used to secure the interfaces between NAF_V and BSF_H

- on the NAF to D-proxy link, it is required that the D-proxy in the VN perform a cross-layer check, i.e. D-proxy checks that the DIAMETER 'Origin-Host' Field matches with the authenticated IP or DNS-name used at IKE.
- on the D-proxy to BSF_H link, it is required that the BSF_H checks that the diameter-identity provided by the D-proxy within the Route-Record-field matches with the authenticated IP or DNS-name of D-Proxy used at IKE.

As another example, if TLS with certificates is used to secure the interfaces between NAF_V and BSF_H

- on the NAF to D-proxy link, it is required that the D-proxy in the VN performs a cross-layer check, i.e. D-proxy checks that the Diameter 'Origin-Host' Field matches the certificate identity.
- on the D-proxy to BSF_H link, it is required that the BSF_H checks that the Diameter-identity provided by the D-proxy within the Route-Record-field matches the certificate identity.

[2] Please note that it is assumed that the proxy keep the origin-host field fixed.

4 Conclusions

This paper has analysed and shown how the Zn-interface can be protected such that a solution can be provided for MBMS. Following conclusion can be made from the paper:

1. The authentication vectors used by GBA shall not leave the Home Network i.e. the BSF shall be placed within the HN.

2. IPsec and TLS mechanism can both be used for protecting the GBA-interface Zn.

3. For scalability reasons, NAFs in the visited network shall communicate with the BSF in the Home Network through Diameter proxy. In that case the Diameter proxy needs to check that the NAF_ID sent to BSF, and the identity used by NAF in its communications with Diameter proxy match.

An open issue is the selection of the mechanism to protect the Zn-interface i.e. the advantages and disadvantages of IPsec and TLS for that purpose should be studied further. The contributing companies solicit for comments/preferences on this particular issue before the comments deadline of MBMS (i.e. 26/4 16.00 CET). Further contributions to SA3#33 will be made, to be able to make a choice at SA3#33.

Note also that the conclusions of this paper also seem to apply to the Gmb-interface (also running diameter protocols) when running between a BM-SC in the VN and a GGSN in the HN, but no detailed study was done on this.