3GPP TSG SA WG3 Security — S3#34 **S3-040487**

July 6 - 9, 2004

Acapulco, Mexico

Source: **Siemens, Nokia**

Title: **GBA: Using IPsec or TLS to secure the Zn-reference Point**

Document for: **Discussion and decision**

Agenda Item: **GBA**

1 Introduction

In the contribution S3-040224 ([1], [2]) to SA3#33 (Beijing) the contributing companies have shown that the GAA Zn-reference point can be protected with both IPsec and TLS mechanism. An open issue was the selection of the mechanism to protect the Zn-reference point i.e. the advantages and disadvantages of IPsec and TLS for that purpose should be studied further.

This paper studies further the advantages and disadvantages of IPsec and TLS for protecting the Zn reference point.

2 Zn Reference point requirements

Securing the Zn reference point requires mutual authentication, confidentiality and integrity (see Clause 4.3.6 of TS 33.220 v. 6.0.0). NAF_ID is used in Ks_NAF key derivation. For that reason the validity of the received NAF_ID shall be verified by the BSF if the NAF is connected directly to the BSF or the Diameter proxy if the NAF connects to the BSF through the Diameter proxy.

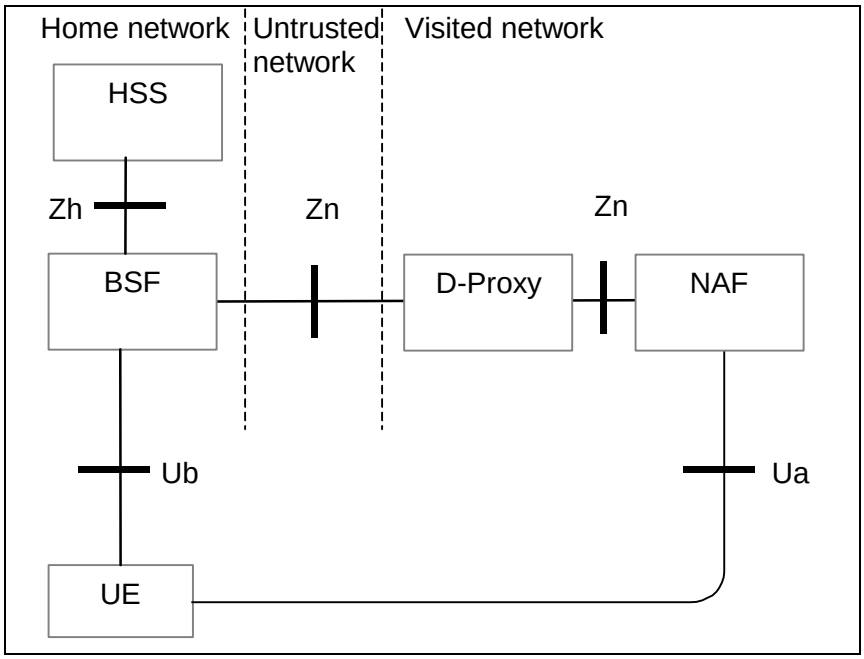

Figure 1a: Simple network model for bootstrapping in visited network

3 Comparison of security mechanisms

The NAF may be connected over Zn reference point to BSF, or to Diameter proxy, but for the sake of brevity we write "BSF" in the text below. However, the same text applies to the case in which NAF is connected to Diameter proxy.

3.1 Protected layer issues

IPsec opens a secure network layer connection between BSF and NAF. Since the IPsec mechanism operates on network layer level, all applications on NAF may communicate with all applications on BSF by default. Additional effort needs to be made to restrict the communication to the Diameter application (e.g. setting up firewall rules, or setting IPsec policies that allow only this traffic). However this effort is to be made only once.

TLS opens a secure application level connection between BSF and NAF. Only the application that opened the TLS connection may use it for communication. The BSF still needs to verify that the NAF application opening the TLS connection is indeed the Diameter application.

Conclusion: TLS+

3.2 Verification of NAF_ID

When the NAF_ID arrives to the Diameter application in BSF, the BSF needs to verify that the NAF_ID belongs to the same NAF that has opened the connection. The BSF does this by verifying the TLS received certificate identity of the TLS-layer. In case there is a D-proxy involved then the BSF needs to trust the proxy on the supplied NAF_ID.

When using IPsec a cross layer check needs to be performed, which is more complicated then the TLS check (see also section 3.3 of [1]).

Conclusion: TLS+

3.3 NAT traversal

Related to IPsec, the informational RFC3715 [4] describes the 'IPsec-Network Address Translation (NAT) Compatibility Requirements'. Only these issues from [4] are highlighted that are relevant in the context of Zn Reference point. If both Zn-reference end points have public IP addresses then there is no problem with the use of IPsec tunnels (TS 33.210). So the problems described below are only relevant in case at least one of the IPsec endpoint addresses of the different security domains have been taken from the private IPv4 address space.

Section 2.1 of [4] on 'Intrinsic NA(P)T Issues' highlights that **with the use of SCTP** (which is the case for Diameter on the Zn-reference point)**, there is no problem in using IPsec ESP (in both tunnel and transport mode) together with NAT.** The reason for this is that the SCTP checksum is not influenced by the changing NAT-ed IP addresses and that ESP mode does not authenticate the original IP-addresses.
For IKE it is known that where IP addresses are used as identifiers in Internet Key Exchange Protocol (IKE) Phase 1 [RFC2409] or Phase 2, modification of the IP source or destination addresses by NATs or reverse NATs will result in a mismatch between the identifiers and the addresses in the IP header. In order to avoid use of IP addresses as IKE Phase 1 and Phase 2 identifiers, FQDNs can be used instead. In that case, it is necessary to verify that the proposed identifier is authenticated as a result of processing an end-entity certificate, if certificates are exchanged in Phase 1. A second possible solution according to [3] is to perform IKE NAT detection and negotiation and the use of UDP encapsulation of IPsec packets through NAT boxes in IKE. This solution also allows the use of IPsec AH. For the Zn-reference point the IKE-NAT solution [3] is not really necessary.

If the peer entities in IPsec are identified by their IP address in certificate or pre-provisioned shared secrets are used in IKE establishment then a potential IP address change[1] may complicate establishment and management of IPsec connection between NAF and BSF. However if an IPsec certificate is used then the DNS name can be used as identification and the potential problems go away.

[1] Which should be a very rare event for the nodes that are used within inter-operator communications.

The identity of the peer entities in TLS are not tied to their IP address. A TLS client is typically identified by client certificate, while the server is typically identified with a server certificate. Therefore no extra functionality to avoid affects of NATs is needed at the BSF, the NAF and D-Proxy when selecting TLS for protection the Zn-reference point.

Conclusion: Both IPsec and TLS can work with NATs. TLS is intrinsically NAT independent, while IPsec/IKE needs to include the necessary features.

3.4 Implementation of different mechanism

Currently the protection of intra-operator IP-interfaces is specified according to TS 33.210 (NDS/IP). If TLS is accepted as the mechanism for Inter-operator Zn-reference point communication then the implementation of two different security mechanisms is needed on the Zn-reference point at the BSF and NAF.

A possible way out to avoid the implementation of both IPsec and TLS on DIAMETER-client is following proposal:

1) Distinguish a Zn and a Zn' reference point into the specification where the Zn' is a Zn-reference point that is used between operators.

2) To mandate the use of a D-Proxy for interoperator communication.

TLS would then be mandatory for use in interoperator communication and the mandatory implementation of TLS would only be necessary between a BSF and a D-proxy and not for the NAFs. In that case there would be a clean split between the use of TLS and IPsec (according to NDS/IP) for the use within GBA. NOTE that for DIAMETER [RFC3588] IPsec implementation is mandatory for DIAMETER clients, while the TLS implementation is optional. For DIAMETER server implementations both IPsec and TLS are mandatory for implementation. A NAF, which is only acting as DIAMETER-client, would not be forced to implement TLS with the above proposal.

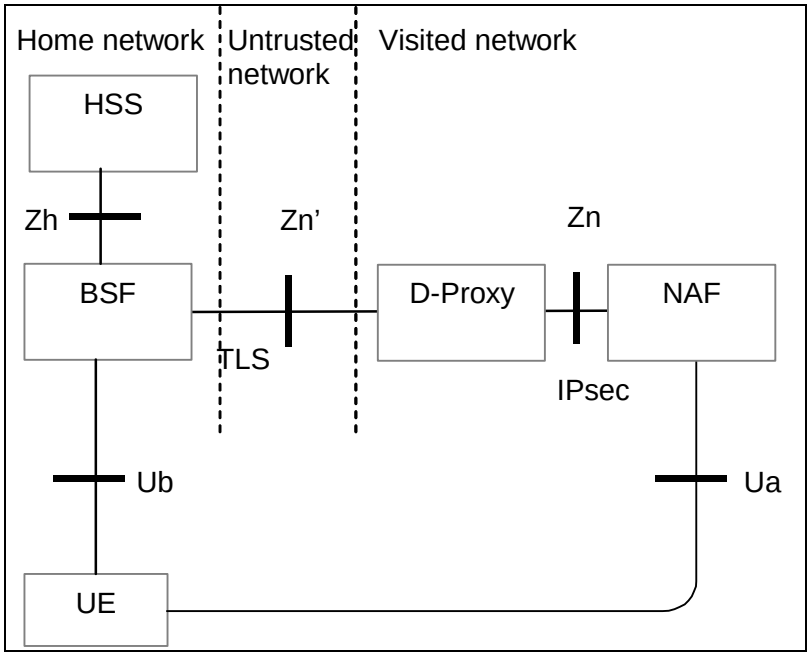

Figure 1b: Simple network model for bootstrapping in visited network

Conclusion: IPsec +

3.5 Provided security level

TLS is NAT and IP-address agnostic which cannot be said for the IKE/IPsec protocol. When a NAT is on the communication path, the IKE/IPsec solution needs to adhere to extra requirements [4] to have a workable solution. The policy database (and firewalls) needs to be configured accordingly. In case of IPsec, the chance of an insecure configuration is higher than with TLS (where such administration is not needed and therefore cannot go wrong). As the Zn-reference point is handling secrets this is an important advantage of TLS.

Conclusion: TLS +

3.6 Limitation of mechanism and migration paths

In the TLS solution peer certificates need to be manually configured in Zn end point nodes, as for 3GPP Release 6 there is no inter-operator TLS certificate enrollment and revocation infrastructure available. Whether NDS/AF can be adapted and used, needs to be studied. The IPsec solution can make use of both shared secrets (for small scale configurations) and certificates. TS 33.310 provides the means to automate the IPsec certificate enrollment and revocation. The use of TLS with trusted peer list certificates still requires more administration then IPsec certificates use, but the frequency of the key pair renewal is lower than the IPsec shared secret solution. For TLS there is some outstanding work: A TLS certificate profile needs to be selected. Having a full-blown Interoperator PKI solution ready within Rel-6 timeframe for TLS seems unrealistic, so only the trusted certificates list solution may be considered.

Conclusion: IPsec +

4 Conclusions

This contribution analyzed the advantages and disadvantages of IPsec and TLS for protecting the GBA Zn reference point. Pro's and cons of both mechanisms seem to be balanced. The use of IPsec puts some extra requirements on the Network nodes to be able to cope with NAT-traversal, which is not the case for the TLS solution.

The use of TLS used in a trusted list PKI-model is proposed under the conditions as described in Figure 1b. An open issue is to define a TLS profile.

5 References

[1] S3-040224, “GBA: Support of NAFs within the Visited Network”, Siemens, Ericsson, Nokia.

[2] S3-040432, “Support for NAF in visited network”, CR to TS 33.220, SA3#33.

[3] T. Kivinen et al., Negotiation of NAT-Traversal in the IKE, 10 Feb 2004, http://www.ietf.org/internet-drafts/draft-ietf-ipsec-nat-t-ike-08.txt

[4] RFC 3715, Informational RFC; ‘IPsec-Network Address Translation (NAT) Compatibility Requirements’. March 2004.

[5] RFC 3554, Standard RFC,” On the Use of Stream Control Transmission Protocol (SCTP) with IPsec”, July 2003

6 ANNEX A: How to use TLS on the Zn-reference point

6.1 Terminology and notation

We shall call the initiating side of TLS session ‘A’ and the responding side ‘B’. A NAF is always A, and a BSF is always B. When Diameter proxy opens a TLS session to BSF it plays the role of A and when a NAF in visited network opens a TLS session to Diameter proxy, then the proxy plays the role of B. The following symbols are used in the text: CA_A is the certification authority in A’s network and CA_B is the certification authority in B’s network. C_A is the certificate of A and C_B is the certificate of B. I_A is the set of identifiers that A may use as NAF_ID. T_B is the set of peers trusted by B.

6.2 General TLS questions

6.2.1 Which mechanisms (and protocols) will be used for enrolling the TLS certificates ?

The mutual authentication in TLS is achieved based on public key technology and certificates. We assume that both A and B contain a certificate store and that there is at least one certification authority CA that can issue certificates in the system. A’s certificate is C_A. That certificate contains the set I_A of A’s identifiers. Each identifier is in the form of fully qualified domain name (FQDN). Similarly, B’s certificate is C_B.

The certificates in the store of B define the group T_B of peers trusted by B. There are several options for creation and enrollment of certificates, three of which are described below.

1. In one option there is a certification authority, CA_B, only in the network of B. CA_B issues a certificate C_B to B and a certificate C_A to A. The certificates are delivered from CA_B to A and B in a secure way ‘out of band’. Both A and B then add their peer into the group of their trusted peers by inserting that peer’s certificate into the certificate store: A inserts C_B into A’s certificate store and B inserts C_A into B’s certificate store. This insertion is typically manual and the details depend on the implementation of the management interface to the certificate store.

2. In another option both A’s and B’s networks contain certification authorities, CA_B and CA_A, respectively. CA_B issues a certificate C_B to B and CA_A issues a certificate C_A to A. The certificates are delivered from C_B to A and from C_A to B in a secure way ‘out of band’. Both A and B then add their peer into the group of their trusted peers by inserting that peer’s certificate into the certificate store: A inserts C_B into A’s certificate store and B inserts C_A into B’s certificate store.

3. In a third option the CA certificates of both sides are exchanged: the certificate of CA_B is delivered to A and the certificate of CA_A is delivered to B in a secure way ‘out of band’, inserted to the certificate store, and marked trusted. Afterwards the validation of C_A and C_B that are exchanged during TLS handshake is based on the presence of the corresponding CA certificates in the certificate store.

(In options 1 and 2 the need for certification authority may be avoided if the peers generate self signed certificates and exchange them in a secure way, 'out of band'. Also, instead of certificates themselves, certificate fingerprints may be exchanged 'out of band' in those options.)

6.2.2 Which mechanisms (and protocols) will be used for checking the certificate revocation?

The revocation operation involves the removal of A from the group T_B of peers trusted by B. In the first two enrollment options described above the revocation happens by B removing the certificate of A, C_A, from its certificate store. This removal can be done manually. In the third option the certificate of A, C_A, is not in B's certificate store. For that reason B has to have a way to check the validity of C_A with the issuer of the certificate. (Also in the first two enrollment options the amount of manual maintenance operations will decrease if B can check the validity of C_A with the issuer of the certificate.) This check can be done by using Online Certificate Status Protocol (OCSP) [RFC 2560] or by using Certificate Revocation Lists (CRLs) [RFC 3280] published by the issuer of C_A. Thereafter A's attempts to establish a TLS session with B will fail.

6.2.3 What profile will be used for the TLS certificate?

This needs to be studied. SA3 needs has to choose whether to refer to an existing TLS profile or to create an own TLS profile.

6.3 Diameter application behavior (over TLS)

TLS session establishment: When the Diameter application in A starts a TLS session with B, the TLS handshake and mutual authentication is based on certificates C_A and C_B. In this way B verifies the membership of A in the set of B's trusted peers and similarly A verifies the membership of A in its group of trusted peers.

Access to the set of identifiers I_A: After the session with the peer is successfully established the TLS implementation has the certificate of the peer. The Diameter application in B can extract the set of A's identities I_A from the certificate of A, C_A, and store it in its memory. As an example, if OpenSSL TLS implementation is used, then the Diameter application can access server certificate (and client certificate if used) through SSL_SESSION structure:

http://www.openssl.org/docs/ssl/ssl.html#DATA_STRUCTURES.

As another example, if Java Secure Socket Extension[2] (JSSE) implementation is used, then the Diameter application can access server certificate (and client certificate if used) through javax.net.ssl.SSLSession:

http://java.sun.com/j2se/1.4.2/docs/api/javax/net/ssl/SSLSession.html.

6.3.1 When a Diameter message with NAF_ID arrives from A to B, how does B check that A is authorized to use that NAF_ID?

When the Diameter application in B receives an Authentication request from A, which contains a NAF_ID, it verifies if that NAF_ID is in I_A. If the received NAF_ID is in I_A, then the Diameter application continues the processing of the Authentication request. If the received NAF_ID is not in I_A, then the Diameter application indicates an error in Authentication answer to its peer in A.

[2] JSSE is included in standard java package (i.e., J2SE - Java 2 Standard Edition).