3GPP TSG SA WG3 Security — S3#36 **S3-040968**

23 - 26 November 2004

Shenzhen, China

Title: **Certificate management for TLS connections between IMS and non-IMS networks**

Source: **Nokia**

Document for: **Discussion/Decision**

Agenda Item: **6.4**

Work Item: **NDS/AF**

1 Introduction

NDS/AF [1] aims at complimenting NDS/IP [2] by providing a PKI that is built on top of manual cross-certifications between operators. It is envisioned that the same PKI can be extended to cover the case for establishing TLS connections between CSCFs in IMS networks and SIP Proxies in non-IMS networks.

According to Section 6.5 of TS 33.203 [3], TLS [4] may be used to protect the SIP signalling (as specified in RFC 3261 [5]) between IMS CSCF and a proxy located in a foreign network (non-IMS network). However, in Note 1 in Section 5.1.4 of TS 33.203 [3], it is also mentioned that TLS certificate management (in a fashion similar to NDS/AF) is not supported in 3GPP, and has to be solved by manual configuration of the involved operators. In the following sections several approaches of certificate management for establishing TLS connections for SIP traffic between IMS CSCFs and non-IMS SIP proxies are discussed.

2 Non-IMS operator has certificates issued by public CA

In this case, the SIP proxy of the non-IMS network presents a certificate issued by a public CA (such as Verisign) when establishing a TLS connection with an IMS CSCF. There are several issues:

1. If the IMS network happens to trust that public CA, it can be assured of the authenticity of the SIP proxy that owns that certificate. However, it does not automatically mean that the SIP proxy is authorized to forward its request to the IMS network, or vice versa. Explicit peering agreement is needed such that the CSCF knows whether such a connection is authorized.

2. How the IMS CSCF can be authenticated by the non-IMS SIP proxy is also not straightforward. The IMS CSCF may have to obtain a certificate issued by a public CA as well.

The use of public CAs allows this solution to be more scalable. Besides, existing Internet operators may have already owned certificates issued by public CAs for various purposes. They may prefer to re-use those certificates to connect to IMS networks as well. Also, this approach does not add extra requirements to non-IMS networks.

3 Manual cross-certification similar to NDS/AF

An alternative approach is by means of manual cross certification between the IMS network and the non-IMS network in a way similar to NDS/AF [1] (as discussed in [6]). The issues of this approach is:

1. Non-IMS networks need to install Interconnection CAs for manual cross-certification with IMS networks.

2. Manual cross-certification needs to be performed between every pair of networks that want to communicate.

However, manual cross-certification can be performed when two networks sign a peering agreement, in which they agree on the terms of establishing connections between the two networks (including SIP traffic and may be other traffic as well).

Although this approach may not be as scalable, it provides an option for non-IMS networks to establish secure connections for SIP traffic to IMS network. In cases where IMS networks do not want to honor certificates issued by public CA, a non-IMS network may choose to establish a peering agreement with an IMS network through this manual cross-certification procedure.

4 GRX-like exchange for SIP traffic

Another possibility is that SIP traffic between IMS network and non-IMS network can go through a third-party exchange network similar to the GPRX Roaming Exchange point (GRX) for GPRX operators. In this approach, a third party SIP network acts as an exchange point. Each participating SIP network (IMS or non-IMS) signs an agreement with this exchange network. Trust relationships are thereby established between the participating SIP networks and the exchange network. All SIP traffic from a participating IMS network to any participating non-IMS network will be proxied through a SIP server in the third-party exchange network. Two TLS connections will be established, one from the IMS CSCF to third-party SIP server, and then one from the SIP server to the destination SIP proxy of the non-IMS network. Similarly, SIP traffic from non-IMS network to IMS network goes through the same third-party SIP server.

This approach simplifies the manual cross-certification needed, and is more scalable as a result. However, a third-party SIP network has to operate this exchange network, and the SIP traffic has to go through an extra hop.

5 Conclusions

In this paper, we discussed several approaches of certificate management for establishing TLS connections for SIP traffic between IMS CSCFs and non-IMS SIP proxies. We find manual cross-certifications between the IMS and non-IMS domains, in a way similar to NDS/AF, to be a useful option for the operators. In our earlier contribution [6] we have shown the possibility of extending NDS/AF to cover the case for establishing TLS connections between CSCF in IMS network and SIP Proxy in non-IMS network for SIP signalling protection.

We propose extending the usage of NDS/AF for establishing TLS connections in Rel-7.

6 References

[1] 3GPP TS 33.310: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Network Domain Security (NDS); Authentication Framework (AF)".

[2] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[3] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services".

[4] IETF RFC 2246 (1999), Transport Layer Security version 1.0.

[5] IETF RFC 3261 (2002), SIP: Session Initiation Protocol.

[6] “Extending NDS/AF for TLS”, 3GPP, S3#35, Nokia.