3GPP TSG SA WG3 Security — S3#35 **S3-040740**

5 - 8 October 2004

St Paul's Bay, Malta

Title:	**Extending NDS/AF for TLS**
Source:	**Nokia**
Document for:	**Discussion**
Agenda Item:	**6.4**
Work Item:	**NDS/AF**

1 Introduction

NDS/AF [33.310] aims at complimenting NDS/IP [33.210] 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 [33.203], TLS [TLS] may be used to protect the SIP signalling (as specified in RFC 3261 [SIP]) 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 [33.203], 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. It is therefore desirable that in Rel7, NDS/AF could be extended to support TLS certificate management between IMS and non-IMS networks.

This paper aims at exploring this possibility.

2 Extending NDS/AF for establishing TLS connections

According to Section 6.5 of 33.203[33.203], TLS [TLS] may be used to protect the SIP signalling traffic between IMS and non-IMS networks. In this case, the same authentication framework as defined in NDS/AF could also be extended for setting up the TLS connections. Following NDS/AF, if a non-IMS network has equivalent Interconnection CA and SEG CA, the same manual cross-certifications can be achieved. This is illustrated in Figure 1, where Security Domain A is an IMS network and Security Domain B is a non-IMS network. Interconnection CA$_A$ will sign SEG CA$_B$, which is responsible for issuing certificates to SIP proxies (e.g. SIP Proxy B) in Security Domain B. Similarly, Interconnection CA$_B$ will sign SEG CA$_A$, which is responsible for issuing certificates to SEGs in Security Domain A. In this case, SEG CA$_A$ will also issue certificate to CSCF$_A$. The resulting X.509v3 certificates that CSCF$_A$ and SIP Proxy B have can then be used for establishing TLS connections between them.

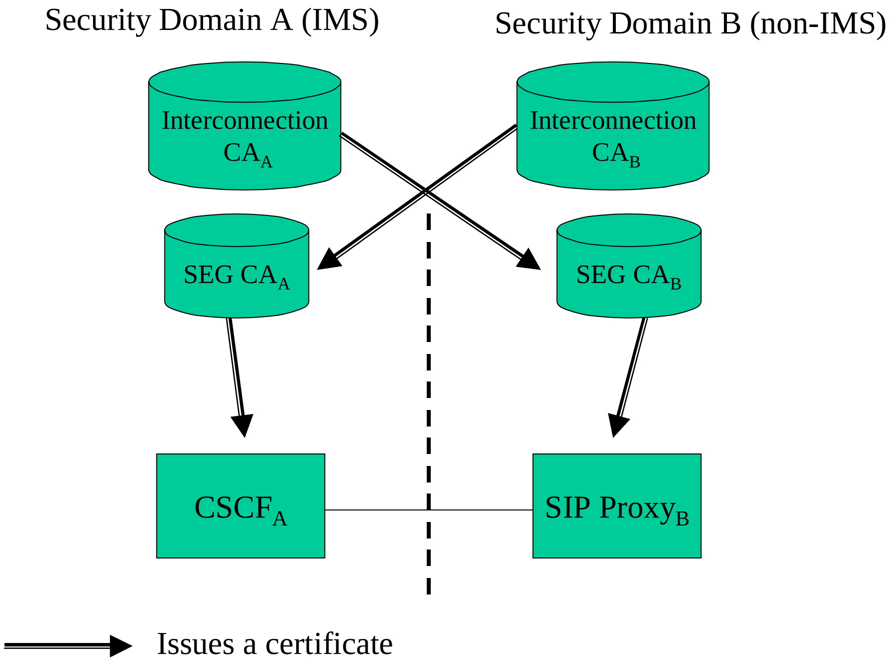

Figure 1 Manual Cross-certifications between IMS and non-IMS networks.

Similar to the case of IMS networks, an operator of the non-IMS network may decide to set up both SEG CA and Interconnection CA as a single CA.

The following figure shows an example whereby CSCF$_A$ in IMS network initiates a TLS connection with SIP Proxy$_B$ in the non-IMS network (Security Domain B), making use of the certificates discussed above.

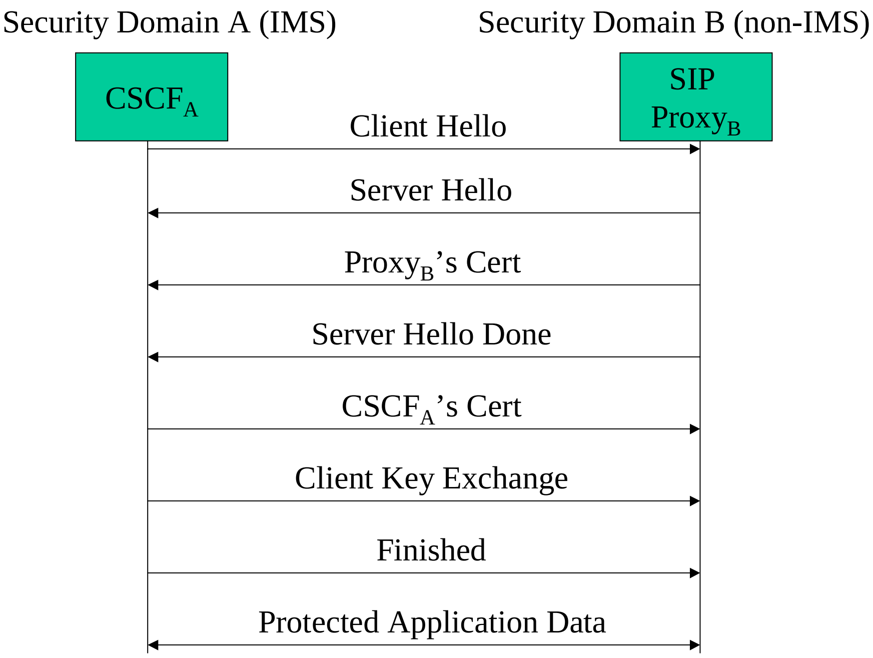

Figure 2 TLS Handshake between IMS CSCF and non-IMS SIP proxy.

In this case, the initiating CSCF ($CSCF_A$) acts as the client and initiates the TLS protocol by sending the “Client Hello” message to SIP $Proxy_B$, which acts as the server. In message 3, SIP $Proxy_B$ sends its own certificate to $CSCF_A$, which will then verify the certificate chain:

SIP $Proxy_B$’s certificate -> SEG CA_B -> Interconnection CA_A.

In message 5, $CSCF_A$ responds by sending its own certificate to SIP $Proxy_B$, which will also verify the certificate chain:

$CSCF_A$’s certificate -> SEC CA_A -> Interconnection CA_B.

Similarly, the TLS connection setup could also be initiated by the SIP Proxy in the non-IMS network.

3 Conclusions

In this paper, we discussed 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. By having a SEG CA and an interconnection CA in the non-IMS network, manual cross-certifications between the IMS and non-IMS domains can be achieved the same way as in NDS/AF. The CSCF and SIP Proxy can then use the resulting certificates for establishing TLS connections between them.

We propose that a new section will be added to NDS/AF in Rel 7 to extend the usage of NDS/AF for establishing TLS connections.

4 References

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

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

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

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

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