3GPP TSG SA WG3 Security — S3#22 **S3-020112**

25 - 28 February 2002

Bristol, UK

3GPP TSG SA WG3 Security — S3#21b **S3z020022**

31st January - 1st February, 2002

Antwerp, Belgium

Source:	**Telenor**
Title:	**A proposal for evolution of Network Domain Security for Release 6 – Introduction of an authentication framework**
Document for:	**Discussion**
Agenda Item:	**NDS-x.x**

Abstract

This contribution discusses the need for an authentication framework for NDS based on PKI services. This proposal also suggests that the authentication framework is defined in a separate TS instead of including the material in the current NDS/IP TS. This will allow the authentication framework to be used for MAPsec KACs as well as for NDS/IP SEGs and NEs, and at the same avoid making the NDS/IP TS unnecessarily complex.

Evolution of Network Domain Security for Release 6

As have been discussed at previous occasions in SA3, there exits a need to introduce an authentication framework in NDS. Currently, authentication of network elements is based on pre-shared secrets. The use of pre-shared secrets seems sufficient for MAPsec for the foreseeable future and it also seems sufficient for NDS/IP as long as the number of nodes don't increase too much. Having said that, a generic PKI based authentication framework should be applicable to MAPsec if the need should arise.

However, with the inevitable advent of IPv6, which will remove address space limitation and thereby remove the need for NATs etc, the possibility for real end-to-end security in NDS/IP will likely be attractive. At the same time, one can expect the number of IP addressable control plane network elements to grow rapidly.

In short, one can expect the use of pre-shared secrets not to scale too well in a few years time. At that point in time, one will need more flexible authentication methods. So, as has been suggested to SA3 in contribution S3-010622 (Nokia/Telenor), one may extend NDS with an authentication framework based on PKI services. IKE already has an option of using digital signatures and/or digital certificates as the authentication method, so there is no need to change NDS/IP to allow for a PKI-based authentication. Note that the possibility for using digital certificates does not preclude the use of pre-shared secrets.

Network Domain Security; A PKI-based authentication framework

It is possible to include the material for a PKI-based authentication framework in the NDS/IP specification. This will require the new framework to be included as a big "Release 6" CR to 33.210. As this contributor sees it, it will procedurally be both a difficult and cumbersome process to add new functionality to 33.210. In particular, it is my opinion that the addition of an authentication framework is essentially independent of NDS/IP in that NDS/IP does not require an authentication framework.

NDS/IP is flexible enough to be used with an authentication framework both with centralized SEGs and with de-centralized SEGs. One can achieve full end-to-end communication in NDS/IP for all nodes provided that one logically views all nodes as containing both the SEG and NE functionality.

So, this contributor therefore advocates that the authentication framework to be specified in a separate NDS TS. This new Release 6 TS could be named something like **Network Domain Security; A PKI-based authentication framework**.

/Geir M. Køien, Telenor R&D