Technical Specification Group Services and System Aspects   **TSGS#16(02)0387**

Meeting #16, Marco Island, Florida, 10-13 June 2002

Work Item Description

Source   **SA WG3** (Modified by TSG SA #16)

Title   **Network Domain Security; Authentication Framework (NDS/AF): Feasibility Study**

1   3GPP Work Area

	Radio Access
X	Core Network
	Services

2   Linked work items

-      Network Domain Security; IP network layer security

3   Justification

For 3GPP systems there is a need for truly scaleable entity authentication framework since an increasing number of network elements and interfaces are covered by security mechanisms . The work item needs to be completed preferably in Release 6 time frame but no later than the Release 7 (more specifically, early 2004) timeframe.

4   Objective

The general objective is toof the feasibility study is to study the impacts of development of a highly scaleable entity authentication framework for 3GPP network nodes. The framework will to be developed would be in the context of the Network Domain Security work items. This effectively limits the scope to the control plane entities of the core network.

The primary objective is for the studied authentication framework to provide entity authentication for the nodes that are using NDS/IP. This means that the authentication is developed to replace the (not so scaleable) default IPsec/IKE use of pre-shared secrets to authenticate the network elements. The authentication framework will therefore be based on profiled X.509v3 type of digital certificates and of profiled public key infrastructure technology and standards.

The Feasibility Study (FS) shall indicate the domains to which the NDS/AF will apply. Furthermore, the FS will specifically show the benefits of applying NDS/AF to the current NDS/IP domain. The consequences and alternatives are to be presented along with the pro's and con's. It is included into the workstudy how actual operator CA's are organized feasibly and what are the trust relationships between them. Thus, feasible different trust models and their effects are studiedcovered more closely.

Additionally the work~~FS~~ will present ~~high level~~ requirements for the used protocols and certificate profiles, so as it is possible for operator IPsec and PKI implementations to interoperate.

~~This work may later be extended to the development of the authentication framework itself depending on the results of the feasibility study.~~

This work might also later be extended to provide entity authentication services to non-control plane nodes.

5   Service Aspects

None identified yet.

6   MMI-Aspects

None identified.

7   Charging Aspects

None identified yet.

8   Security Aspects

The work item is a security item.

9   Impacts

Affects:	USIM	ME	AN	CN	Others
Yes				X	
No	X	X			
Don't know			X		X

10   Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
SA3#25	October, 2002	Revised FS and WID approved.~~Broad agreement on TOC and scope of NDS/AF TS~~ ~~Work on NDS/AF general architecture and profiling of X509v3 certificates. Discussions on certificate distribution (and revocation) and the associated services and requirements.~~ ~~Work on trust model, CA hierarchy and RA issues.~~
SA3#26	November, 2002~~TBD~~	Work on NDS/AF general architecture and profiling of X509v3 certificates. Discussions on certificate distribution (and revocation) and the associated services and requirements.~~Work on profiling of digital certificates.~~ ~~Work on certificate distribution.~~

		Work on trust model, CA hierarchy and RA issues.
		Involve related 3GPP workgroups (if any).
SA3#27	~~TBD~~ (Feb~~ruary,~~ ~~/March~~ 2003~~?)~~	Agree on all top-level principles for the NDS/AF TS~~:~~. Work on trust model, CA hierarchy and RA issues Work on profiling of digital certificates. Work on certificate distribution (and revocation). Involve related 3GPP workgroups (if any).~~Continue work on actual specification. Finalize trust model.~~
SA3#28	~~TBD,~~ May~~,~~ ~~/June~~ 2003~~?~~	Progress work on NDS/AF TS~~:~~. Finalize trust model. Finalize certificate profile(s).
SA3#29	TBD, Aug/Sept 2003?	Finalize certificate distribution. Prepare to submit NDS/AF TS to SA for information.
SA#21?	TBD, Oct. 2003	NDS/AF TS submitted for information to SA plenary
SA3#30	TBD, Nov 2003	Resolve any remaining issues. Submit NDS/AF TS for approval.
SA#22?	Dec, 2003	NDS/AF TS submitted for approval to SA plenary
SA/CN #23?	March 2004	(if applicable) Stage-3 work approved

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
33.xxx	NDS/AF	SA3				~~Whether a new spec is created depends on the outcome of the FS.~~
Affected existing specifications						
Spec No.	CR	Subject		Approved at plenary#		Comments

11 Work item raporteurs

Tommi Viitanen, Nokia
tommi.viitanen@nokia.com
+358 40 5131090

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Nokia, Telenor, T-Mobile, Siemens, SSH Communications Security Corp

14 Classification of the WI (if known)

X	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a   The WI is a Feature: List of building blocks under this feature

14b   The WI is a Building Block: