3GPP TSG SA WG3 Security — S3#23 **S3-020278**

14-17 May, 2002

Victoria, Canada

Work Item Description

Source **Telenor**

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

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

- Network Domain Security; IP network layer security

3 Justification

For the long-term evolution of 3GPP systems there is a need for truly scaleable entity authentication framework. The work item needs to be completed preferably in Release 6 time frame but no later than the Release7 (more specifically, early 2004) timeframe.

4 Objective

The general objective is to develop a highly scaleable entity authentication framework for 3GPP network nodes. This framework will be developed 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 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. ~~An important aspect of this work item is to make sure that transition from entity authentication based on pre-shared secrets towards entity authentication based on NDS/AF can take place in phases. The phases should allow an operator to use NDS/AF internally, while still using the default pre-shared secret method towards roaming partners that does not support NDS/AF.~~

The Feasibility Study (FS) shall indicate the domains to which the NDS/AF will apply. Furthermore, the FS will specificly 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 study how operator CA's are organized feasibly and what are the trust relationships between them. Thus, different trust models and their effects are studied more closely. Additionally the 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.

~~The authentication framework may also be applicable for the KAC nodes of the MAPsec standard, but the requirements and applicability in that domain remains to be investigated by SA3.~~

~~A secondary objective is to provide entity authentication services also for control plane nodes in UTRAN.~~

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#23	May, 2002	SA3 approval of WID Initiate feasibility study (some work already done in context of NDS/IP)
SA#16	June, 2002	WID approved
SA3#24	July, 2002	Feasibility study concluded. Initiate discussions on TOC and scope of new NDS/AF TS. This includes requirements capture. Work on phased introduction/migration scenarios.

SA3#25	October, 2002	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	TBD	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/March 2003?)	Agree on all top-level principles for the NDS/AF TS. Continue work on actual specification. Finalize trust model.
SA3#28	TBD, May/June 2003?	Progress work on NDS/AF TS. 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				

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments

11 Work item raporteurs

~~TBD~~
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)
X	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: