3GPP TSG SA WG3 Security — S3#32 **S3-040023**
9-13 February 2004
Edinburgh, UK

Source: **Siemens, Nokia, T-Mobile, Vodafone**

Title: **NDS/AF: pki4ipsec work within IETF**

Document for: **Information**

Agenda Item: **NDS/AF: 6.4**

1 Introduction

The goal of this contribution is to make SA3 aware of some new work that was started within the IETF. The result of this work may have implications on the NDS/AF work (TS 33.310). The supporting companies of the NDS/AF work have started monitoring this work.

2 The pki4ipsec WG

A BOF was held at IETF-58 in Nov 2003 which has resulted in a new IETF working group within the security area: **Profiling Use of PKI in IPsec (pki4ipsec)**.

The complete 'WG charter' is currently available at http://www.icsalabs.com/pki4ipsec/. The *italic* text following in this section is an extract of the charter as was available at the end of January.

The working group will focus on the needs of enterprise scale IPsec VPN deployments. Gateway-to-gateway access (tunnel and transport mode) and end-user remote access to a gateway (either tunnel or transport mode) are both in scope.

The WG will deliver

1) A standards-track document that gives specific instructions on how X.509 certificates should be handled with respect to the IKEv1 and IKEv2 protocols. This document will include a certificate profile, addressing which fields in the certificate should have which values and how those values should be handled.

2) An informational document identifying and describing requirements for a profile of a certificate management protocol to handle PKI enrolment as well as certificate lifecycle interactions between IPsec VPN systems and PKI systems. Enrolment is defined as certificate request and retrieval. Certificate lifecycle interactions is defined as certificate renewals/changes, revocation, validation, and repository lookups.

These requirements will be designed so that they meet the needs of enterprise scale IPsec VPN deployments.

Once the above two items enter WG last call, the WG will begin work on:

3) A standards-track document describing a detailed profile of the CMC protocol that meets the requirements laid out in the requirements document. Profile documents for other enrolment and/or management protocols may also be created.

The WG end date[1] *is Feb 2005.*

Two Drafts are currently available

[1] See Annex A of this contribution.

- draft-ietf-ipsec-pki-profile-03.txt: This is an in-depth document describing many aspects of IKE with potential interoperability problems. It has been available since a long time and has been used for the 3GPP NDS/AF work. This document also is based on the deploy work (available under http://www.projectdploy.com) which was also considered for NDS/AF.
- draft-hoffman-pki4ipsec-profile-00.txt : A recent draft which contains some contradictory statements with respect to the pki-profile-03. One of these contradictory areas is the need for a SEG to check if the IP-address of the IKE partner corresponds to the authenticated address of the Certificate.

3 Conclusions

TS 33.310 is a 3GPP Rel-6 specification for using certificates for the inter-operator SEG communication. The cross-certification aspects are not handled by the PKI4IPSEC WG, but the SEG-certificate profiling, IKE-handling and lifecycle management is a common area

The work initiated by the PKI4IPSEC group may consequently have some minor effects on TS 33.310, but as the NDS/AF work has been based on two of the three input documents of the IETF-group the possible effects on the specification won't be that big. According to the currently available timeline (See annex A) of the WG the main discussions on the profiling will happen before the end of March 2004, which may result in small Change Requests to TS 33.310 if alignment with 'the IETF document' is considered useful and needed. This may be decided on a case by case basis. The work on CMC is considered too late to fit within the Rel-6 deadline for NDS/AF.

Annex A : Goals and Milestones

Jan 2004	Post Certificate Profile and Use in IKE as an Internet Draft
Feb 2004	Post Management Protocol Profile Requirements as I-D
Mar 2004	Submit Certificate Profile and Use in IKE as WG last call
Apr 2004	Rev Requirements for management protocol profile as needed
May 2004	Submit Certificate Profile and Use to IESG, Proposed Standard
May 2004	Submit Requirements for Management Protocol Profile as WG last call
Jun 2004	WG decision on other Enrollment/Management protocols to profile
Jul 2004	Submit Requirements for Management protocol Profile to IESG, Informational
Jul 2004	Post CMC for IPsec VPN Profile as Internet Draft
Jul 2004	Post other enrollment/management profiles as I-D
Sep 2004	Rev CMC for IPsec VPN profile as needed
Sep 2004	Rev other enrollment/management profiles as needed
Nov 2004	CMC for IPsec VPN profile to WG last call
Nov 2004	other enrollment/management profiles to WG last call
Jan 2005	Submit CMC for IPsec VPN Profile to IESG, Proposed Standard
Jan 2005	Submit other Profiles for enrollment/management to IESG, Proposed Standard
Feb 2005	Re-charter or close