3GPP TSG SA WG3 Security — SA3#28 **S3-030211**
6 - 9 May 2003
Berlin, Germany

Source: **Nokia, Siemens, SSH, T-Mobile, Verisign**

Title: **Profiling of IKE and Certificates for use within NDS/AF**

Document for: **Discussion and Decision**

Agenda Item: **TBD**

Abstract

This contribution includes contents for clauses 5.3.1/2/3 of the NDS/AF specification (S3-030150). The motivation why we made particular profile choices is included in italic text. It shall be decided whether that text is usefull to be included into the Technical Specification or not. The decision may be done on a case by case basis.

Proposed content for clauses 5.3.1/2/3

5.3.1 Certificate profiles

[Editor's note: A more detailed check on using RFC3280 and draft-ietf-ipsec-pki-profile-02.txt *as the main profiling base is needed. It needs to be assessed why and how we want to deviate from these papers]*

5.3.1.1 Common rules to all certificates

- Version 3 certificate

  Motivation: This is the current state of the art [RFC 3280].

- Hash algorithm for use before signing vertificate: Sha-1 mandatory to support, MD-5 shall not be used.

  Motivation: SHA-1, is state of the art, MD-5 shall not be used anymore as it is considered weaker

- Subject and issuer name format. Note that C is optional element. : (C=<country>), O=<Organization Name>, CN=<Some distinguishing name>. Organization and CN shall be in UTF8 format.

  Motivation: RFC3280 states in clause 4.1.2.4 Issuer that The UTF8String encoding [RFC 2279] is the preferred encoding, and all certificates issued after December 31, 2003 MUST use the UTF8String encoding of DirectoryString (except in some migration cases).

- CRLv2 support with LDAPv3 [RFC 2252] retrieval shall be supported as the primary method of certificate revocation verification.

5.3.1.2 CA Certificate profile

In addition to clause 5.3.1.1, following requirements apply:

- The RSA key length shall be at least 2048-bit

  Motivation: "RSA Laboratories currently recommends key sizes of 1024 bits for corporate use and 2048 bits for extremely valuable keys like the root key pair used by a certifying authority "

  see http://www.rsasecurity.com/rsalabs/faq/3-1-5.html

- Extensions:
  - Optionally non critical authority key identifier
  - Optionally non critical subject key identifier
  - Mandatory critical key usage: At least keyCertSign and CRL Sign should be asserted
  - Mandatory critical basic constraints: CA=True, path length unlimited or at least 2.

5.3.1.3 SEG Certificate profile

In addition to clause 5.3.4.1, following requirements apply:

- The RSA key length shall be at least 1024-bit

  Motivation: "RSA Laboratories currently recommends key sizes of 1024 bits for corporate use and 2048 bits for extremely valuable keys like the root key pair used by a certifying authority "

  see http://www.rsasecurity.com/rsalabs/faq/3-1-5.html

- Issuer name is the same as the subject name in the Domain authority cert.
- Extensions:
  - Optionally non critical authority key identifier
  - Optionally non critical subject key identifier
  - Mandatory critical key usage: At least digitalSignature shall be set.
  - Optional critical enhanced key usage: If present, at least server authentication and IKE intermediate shall be set
  - Mandatory non critical Distribution points: CRL distribution point

5.3.1.4 Cross Certificate profile

In addition to clause 5.3.1.1, following requirements apply:

- Subject name is the same, which the authority of the other domain uses in it's certificates
- Issuer Name is the same as used for signing our entities
- Extensions:
  - Optionally non critical authority key identifier
  - Optionally non critical subject key identifier
  - Mandatory critical key usage: At least keyCertSign and CRL Sign, should be asserted
  - Mandatory critical basic constraints: CA=True, path length 0.

5.3.2 IKE negotiation and profiling

[Editor's note: A more detailed check on using draft-ietf-ipsec-pki-profile-02.txt *as the main profiling base is needed. It needs to be assessed why and how we want to deviate from these papers]*

5.3.2.1 IKE Phase-1 profiling

The Internet Key Exchange protocol shall be used for negotiation of IPsec SAs. The following requirements on IKE in addition to those specified in NDS/IP [TS 33.210] are made mandatory for inter-security domain SA negotiations over the Za-interface.

For IKE phase-1 (ISAKMP SA):

- The use of RSA signatures for authentication shall be supported.
- Initiating/responding SEG are required to send certificate requests in the IKE messages

  Motivation: suggested by draft-ietf-ipsec-pki-profile-02.txt to avoid interoperability problems
- Cross-certificates shall not be send by the peer SEG as they are pre-configured in the SEG.

  Motivation: avoiding known problems (see clause 5.3.5.2)
- The SEG shall always send its own certificate in the certificate payload of the last (third) Main Mode message

  Motivation: avoids the need to cache Peer SEG certificates.
- The certificates in the certificate payload shall be encoded as type 4 (X.509 Certificate – Signature).
- The lifetime of the Phase-1 IKE SA shall be limited to at most the remaining validity time of the peer SEG certificate.

5.3.2.2 Potential interoperability issues

Some PKI-capable VPN gateways do not support fragmentation of IKE packets, which becomes an issue when more than one certificate is sent in the certificate payloads, forcing IKE packet fragmentation. This means that direct cross-certification or manually importing the peer CA certificate to the local SEG and trusting it is preferable to bridge CA systems. When IKE is run over pure IPv6 the typical MTU sizes do not increase and long packets still have to be fragmented (allowed for end UDP hosts even for IPv6, see [Path MTU Discovery for IP version 6 – RFC 1981]), so this is a potential interoperability issue.

Certificate encoding with PKCS#7 is supported by some PKI-capable VPN gateways, but it shall not be used.

5.3.3 Path validation

5.3.3.1 Path validation profiling

- Validity of certificates received from the peer SEG shall be verified by CRLs retrieved with LDAP, based on the CRL Distribution Point in the certificates.
- A SEG shall not validate received certificates from the peer SEG whose validity time has expired, but end the path validation with a negative result.
- A SEG shall not validate received certificates from the peer SEG whose CRL distribution point field is empty, but end the path validation with a negative result.
- Certificate validity calculation results shall not be cached for longer than the resulting IKE phase-1 lifetime.