3GPP TSG SA WG3 Security — S3#24 **S3-020358**
9 - 12 July 2002
Helsinki, Finland

Source:	**Nokia, Siemens, SSH, Telenor, T-Mobile**
Title:	**NDS/AF Feasibility Study to support the evolution of TS 33.210 NDS/IP**
Document for:	**Discussion and approval**
Agenda Item:	**7.2**

NDS/Authentication Framework (AF) Feasibility Study

to support TS 33.210 NDS/IP evolution

Contributors: Nokia, Siemens, SSH, Telenor, T-Mobile

TABLE OF CONTENTS

1. INTRODUCTION

1.1 Purpose

For the long-term evolution of 3GPP systems there is a need for truly scalable entity Authentication Framework (AF). 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.

The objective is to develop a highly scalable entity authentication framework for 3GPP network nodes. This framework will be developed in the context of the Network Domain Security work items, which effectively limits the scope to the control plane entities of the core network. Thus, *the Authentication Framework will provide entity authentication for the nodes that are using NDS/IP*.

The study will specifically show the benefits of applying NDS/AF to the current NDS/IP domain. The consequences and alternatives will be presented along with the pro's and con's. In the PKI-based alternative, this study analyzes how operator CA's can be organized and what are the trust relationships between them. Thus, different trust models and their effects will be studied. Additionally, we will present high-level requirements for the used protocols and certificate profiles, to make it possible for operator IPsec and PKI implementations to interoperate.

It should be noted that although there is a strong trend towards PKI systems, this feasibility study does not take it as a self-evident approach for NDS/AF. In other words, the non-PKI approach is also to be studied.

1.2 Scope

The scope of this feasibility study is limited to authentication of network elements which are using NDS/IP, and located in the inter-operator domain.

This means that we concentrate on authentication of Security Gateways (SEG), and the corresponding Za-interfaces. Authentication of elements in the intra-operator domain is considered as an internal issue for the operators. This is quite much in line with [6] which states that only Za is mandatory, and that the security domain operator can decide if the Zb-interface is deployed or not, as the Zb-interface is optional for implementation.

However, NDS/AF can easily be adapted to intra-operator use. This is just a simplification of the inter-operator case as all NDS/IP NEs and the PKI infrastructure belong to the same operator. Validity of certificates may be restricted to the operator's domain.

This work might also later be extended to provide entity authentication services to non-control plane nodes, but this has not been studied.

The NDS architecture for IP-based protocols is illustrated in Figure 1.

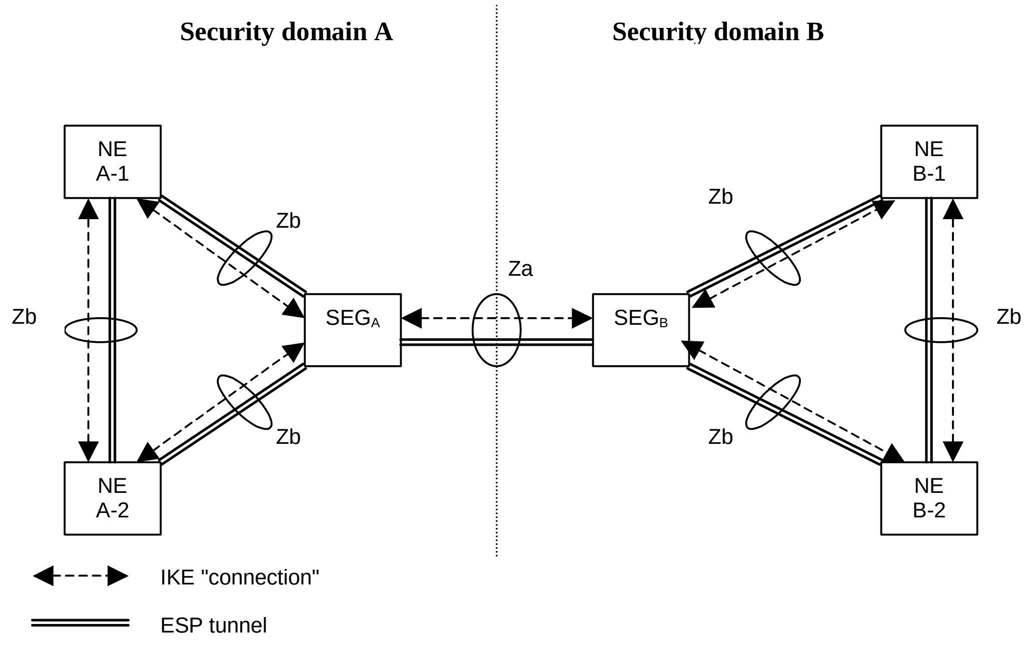

Figure 1 NDS architecture for IP-based protocols [6]

1.3 Terms, acronyms and abbreviations

AF	Authentication Framework
CA	Certification Authority
CMC	Certificate Management Messages over CMS
CMP	Certificate Management Protocol
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CTL	Certificate Trust List
DMZ	DeMilitarized Zone
EE	End Entity (synonymous for PKI-client in SEG)
HTTP	Hyper Text Transfer Protocol
IKE	Internet Key Exchange
LDAP	Lightweight Directory Access Protocol
NDS	Network Domain Security
OCSP	Online Certificate Status Protocol
Root CA	A CA that is directly trusted by an end-entity; that is, securely acquiring the value of a Root CA public key requires some out-of-band step(s). This term is not meant to imply that a Root CA is necessarily at the top of any hierarchy, simply that the CA in question is trusted directly.
SEG	Security Gateway
SOI	Son of IKE

Za Interface between SEGs belonging to different networks/security domains (A Za interface may be an intra or an inter operator interface).

Zb Interface between SEGs and NEs and interface between NEs within the same network/security domain

2. ARCHITECTURE ALTERNATIVES

This chapter describes the different architecture alternatives for NDS/AF.

2.1 Inter-operator NDS/AF with symmetric keys

In this scenario there will be no PKI involved, but each operator's SEG has to establish bilateral key agreements (i.e. share symmetric secret keys).

This has two obvious sub-scenarios which could be applied with NDS/AF:

1) mesh of direct one-to-one relationships, where each operator creates and shares a secret key with every operator with which it has a roaming agreement, and

2) hub-and-spoke approach where each SEG shares a secret key with only one intermediary security gateway, acting as a bridge between all SEGs.

These sub-scenarios are illustrated in Figure 2 and Figure 3, with the total number of operators set to 6. In the Figure 2 the total amount of keys in the system is 9, whereas the hub-and-spoke approach (in Figure 3) drops the total number of keys to 6.

Suppose that the number of operators is N, then scenario 1) described above potentially requires a total of N(N-1)/2 shared secrets to be established, whereas scenario 2) requires only N shared secrets.

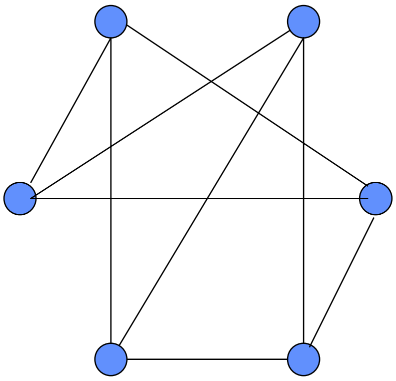

Figure 2 Partial mesh of direct trust relationships between operators

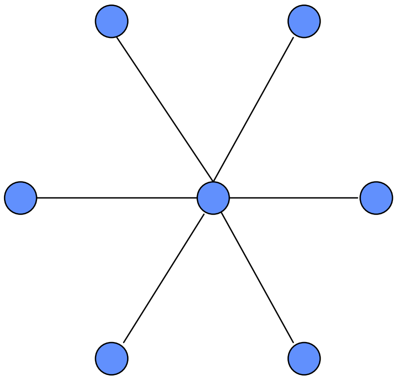

Figure 3 Hub-and-spoke approach with symmetric keys

2.2 Inter-operator NDS/AF utilizing PKI

In this scenario, each operator utilizes (its own or outsourced) PKI infrastructure to issue public-key certificates to the SEG elements to be subsequently used in IKE authentication.

This scenario has quite many variations, and the following subsections will describe them, one-by-one.

2.2.1 Trust models

We have identified three basic trust models which could be used to establish inter-operator trust relationships:

1) Strict hierarchy of operator CAs,

2) Distributed trust architecture with cross-certification, and

3) Certificate Trust Lists (CTL).

We will give the scenarios related to these trust models in the following subsections. The repository and revocation issues will be discussed separately in chapter 3.

2.2.1.1 Strict hierarchy of operator CAs

In this trust model, all entities in the hierarchy trust the single root CA.

Generally, the hierarchy may be established as follows: 1) the root CA certifies zero or more CAs immediately below it, 2) each of these CAs certify zero or more CAs immediately below it, and 3) at the second-to-last level the CAs finally certify end-entities.

For the NDS/AF, two possible sub-scenarios can be identified.

One level deep hierarchy:

There is a one master root CA, which signs the certificates of all the SEGs of every operator.

Two level deep hierarchy:

The master root CA key is used to sign the operator sub CA keys, and each operator then sign its own SEG certificates using his sub CA key. This scenario is illustrated in Figure 4.

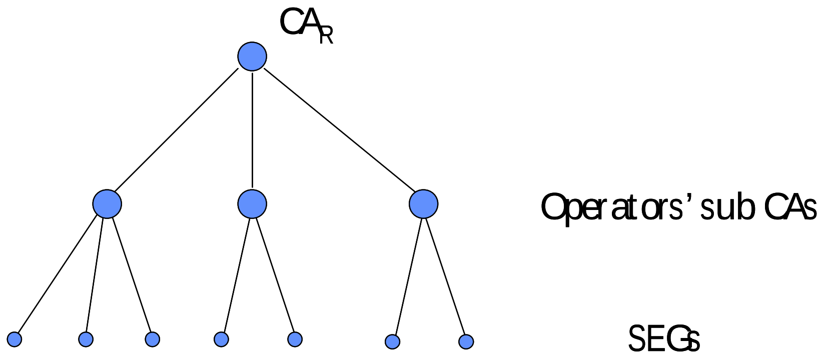

Figure 4 Strict hierarchy of CAs (2-level solution)

2.2.1.2 Distributed trust architecture

In contrast to strict hierarchy where all the operators trust a single root CA, the distributed trust architecture distributes trust among operators' own root CAs. The process of interconnecting the peer root CAs is known as cross-certification. Figure 5 illustrates one possible distributed trust architecture with cross-certification. The cross-certification and roaming agreement establishment are directly linked to each other; the cross-certificates can be created as part of the roaming agreement establishment process.

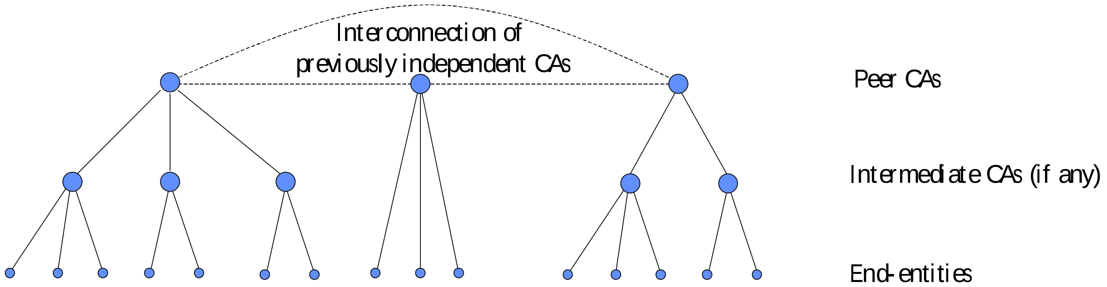

Figure 5 Distributed trust architecture (general view)

For the NDS/AF, two possible sub-scenarios can be identified. In both cases, each operator signs its own SEG certificates using his own root CA key.

Mesh

In the mesh configuration, all the operator's root CAs are potentially cross-certified with each other. If the CAs are not all connected, then we have a partial mesh. For example, Figure 5 illustrates a full mesh configuration. A *full mesh* requires *n(n-1)/2* cross-certification agreements, and a total of *n(n-1)* cross-certificates to be stored, when there are *n* root CAs.

Hub-and-spoke

Figure 6 illustrates a hub-and-spoke configuration, where each operator's root CA cross-certifies with a single central CA whose task is to facilitate this kind of interconnections. This central CA is called a hub, which spokes out to the root CAs. The central CA may also be called a *bridge CA*, bridging communication gaps between pairs of roots. The fully connected case requires only *n* cross-certification agreements for *n* root CAs.

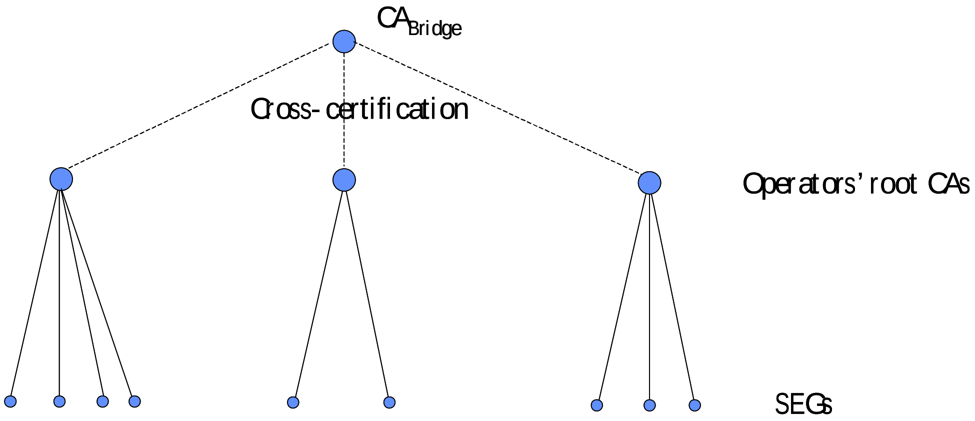

Figure 6 Bridge CA

2.2.1.3 CTL model

A Certificate Trust List (CTL) is a signed PKCS#7 data structure that can contain a list of trusted CAs. A trusted CA is identified within the CTL by a hash of the public key certificate of the subject CA. The CTL also contains policy identifiers and supports the use of extensions.

From an inter-domain interoperability perspective, the CTL essentially replaces the cross-certification. The key is that the relying party trusts the issuer of the CTL, which then allows the relying party to trust the CAs conveyed within the CTL. [1]

CTL is more like the legacy web browser trust model and it is not considered a real alternative here, but presented as it has been quite largely used.

An example, where a root CA of an operator A provides a CTL indicating unilateral trust to operators B and C is shown in Figure 7.

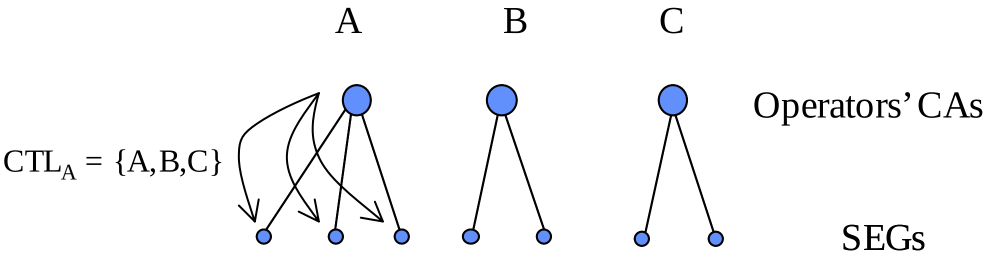

Figure 7: CTL model

3. FUNCTIONALITY AND PROTOCOLS

3.1 Minimum set of functionality

The minimum required PKI functionality may be realized by profiling the use of existing protocols to enhance interoperability between implementations: Examples are profiling of certificate fields, CRL usage, IKE Certificate handling.

The minimum set of functionality to be specified by NDS/AF will consist of:

- Certificate life cycle management method comprising
    - Certificate initial enrollment (manually assisted or automatic)
    - Key update (Key update refers to an operation where an end entity updates its private key and receives from the CA a certificate with a new public key and validity but otherwise identical contents.)
    - (Revocation requesting [might not be valid within NDS/AF])
- Certificate validation (validation of the certificate chain including the revocation data to a trusted root CA)
- Certificate dissemination method
    - IKE Peer to Peer exchange or repository access
- Revocation information dissemination method
    - IKE Peer to Peer exchange or repository access

3.2 Available protocols

Only in those cases having inter-operator operations, the protocols are an issue. These include FTP, HTTP and LDAP for repository access, OCSP [2] for certificate status checking and CMP [4,5] or CMC [6] for certificate life cycle management.

End entities (EEs) need to be able to fetch CRLs in order to check the certificate status from a PKI repository. Also, in the case of multi-level CA hierarchies and cross-certification, EEs might need to fetch the certificates between the other party and the trusted CA in the certificate path (the EE certificate itself should be sent in the IKE payload). Both LDAP (Light-weight Directory Access Protocol) and HTTP should be supported for fetching CRLs from a repository. HTTP is very widely used, easy to implement and often used to fetch CRLs. However, LDAP is more suitable for fetching other objects as CRLs.

CRL distribution point in the EE certificate or sub-CA certificate should point to the CRL issued by the CA. LDAP should be the supported mechanism to fetch certificates needed for certificate path construction. Unlike LDAP, there is no specification for HTTP for the certificate retrieval.

Additionally it should be noted that the CRL transport mechanism is depends on the trust model. Also if IKE payload can include a certificate chain then HTTP would be enough, but this subject needs further study.

3.3 Repositories

In general, repositories should be located or duplicated close to nodes that access repositories frequently. Repositories can be located outside SEGs, in DeMilitarized Zone (DMZ) or in the operator’s network. Normally repositories are located at DMZ, which is a recommended approach also in this situation.

In the chapter 2 trust models, we may have the following repository scenarios. It should be noted that if the whole certificate chain is included in the IKE payload then repository access for certificate retrieval may be omitted. However, this is dependent on the trustmodel.

Strict hierarchy of operator CAs (1-level)

Certificate repository: Not required; in IKE authentication phase 1 each SEG will exchange their own device certificates, signed by the same CA. Here we also suppose that the root CA certificate is securely pre-installed in each SEG.

CRL repository: Required; the repository can be a centralized repository co-located in the root CA.

Strict hierarchy of operator CAs (2-level)

Certificate repository: Required; in IKE authentication phase 1 each SEG needs access to intermediary certificates (i.e. peer’s sub CA certificate) if they are not sent within the certificate payload. The repository can be either a centralized repository co-located in the root CA, or it can be located within each sub CA.

CRL repository: Required; the repository can be either a centralized repository co-located in root CA, or it can be located within each sub CA.

Distributed model (mesh):

Certificate repository: Required; in IKE authentication phase 1 each SEG needs access to intermediary certificates (i.e. cross-certificates of peer CAs) if they are not sent within the certificate payload. The repository can be either a centralized repository in DMZ, or it can be located within each local CA.

CRL repository: Required; the repository can be either a centralized repository in DMZ, or it can be located within each local CA.

Distributed model (hub-and-spoke):

Certificate repository: Required; in IKE authentication phase each SEG needs access to intermediary certificates (i.e. cross-certificates of peer CAs and the Bridge CA) if they are not sent within the certificate payload. The repository can be either a centralized repository in DMZ (possibly co-located in Bridge CA), or it can be located within each local CA.

CRL repository: Required; The repository can be either a centralized repository in DMZ (possibly co-located in Bridge CA), or it can be located within each local CA.

CTL model:

Certificate repository: Required; in IKE authentication phase each SEG needs access to intermediary certificates if they are not sent within the certificate payload. The repository can be either a centralized repository in DMZ, or it can be located within each local CA.

CRL repository: Required; the repository can be either a centralized repository co-located in root CA, or it can be located within each sub CA.

3.4 Certificate revocation methods

The issues that affect in choosing the revocation mechanisms are:

- Propagation of revocation information
  - CRLs guarantee the propagation after the next update.
  - OCSP guarantees real-time propagation, but there are no strong requirements for the real-time check in NDS/IP environment
- The number of relying parties
  - In OCSP, the responder must sign each response, causing high performance requirements on the OCSP responder.
  - Only CRLs are signed, so there are no similar requirements than with OCSP.

These criteria should be discussed in every scenario.

CRLs should be used when the status of the OCSP responder certificate itself is being checked. However, this means that each EE would need to support CRLs and the CRL publishing should be deployed together with the OCSP responders. RFC2560 (OCSP) defines a certificate extension, ocsp-nocheck, which indicates that the EE can trust the certificate during its lifetime. The certification practice statement (CPS) of the operator should explicitly define whether this practice is being used as it has serious security implications to the system.

In the above trust models, we may have the following certificate revocation scenarios:

Strict hierarchy of operator CAs (1-level)

CRL distribution point is preconfigured, since there will be only one CA, only one CRL, and only one location where to get it. The CRL is located in a central repository, accessible to all the operators.

Strict hierarchy of operator CAs (2-level)

Each certificate contains CRL distribution point, pointing to the CRL of the corresponding operator, or possibly to the centralized distribution point.

Distributed model (mesh):

Each certificate contains CRL distribution point, pointing to the CRL of the corresponding operator, or possibly to the centralized distribution point.

Distributed model (hub-and-spoke):

Each certificate contains CRL distribution point, pointing to the CRL of the corresponding operator, or possibly to the centralized distribution point.

CTL model:

Each certificate contains CRL distribution point, pointing to the CRL of the corresponding operator, or possibly to the centralized distribution point.

However, the revocation of the CTL itself is a problem. Currently a CTL is valid as long as the CA certificates within the CTL. Revoking one CA from CTL means reinitialization of the infrastructure utilizing CTLs.

In all of the above scenarios the OCSP responder(s) may be located in the same domain than CRL distribution point.

3.5 Certificate and CRL profiles

In this feasibility study we suppose that the certificate and CRL profiles are as in [3].

3.6 Certificate Life Cycle Management

Certificate management protocol v2 (CMPv2 [5]) should be the supported protocol to provide certificate lifecycle management capabilities. It involves online interaction (certificate enrollment, certificate renewal, key updates, revocation requests etc) between EEs, RAs, and CAs. Inter-operator operations are involved especially when different operators trust a common CA (hosted by a third party or one of the operators).

See also Section 4.4 which describes the CMPv2 maturity level.

3.6.1 PKCS10/7 & SCEP & automatic life cycle management comparison

The initial enrollment of a certificate can be done manually by utilizing PKCS#10 certification request and PKCS#7 digital envelope syntaxes. The manual procedure includes copy-pasting certification request to a web form and manually importing the issued certificate to the end entity device. The more advanced method is to use Simple Certificate Enrollment Protocol (SCEP) [7] utilizing HTTP as a transport and PKCS#7/10 as message syntaxes. However, SCEP does not provide life-cycle management functions, especially automatic key update procedure before the certificate expires. Therefore, the initial enrollment needs to be gone through each time when the certificate expires. CMPv2 (Certificate Management Protocol version 2) [8] provides a complete lifecycle management protocol including both intial enrollment and key updates. Although there are also multiple other functions such as online revocation request and CA key roll-over in CMPv2, within NDS/AF the most relevant functions that should be supported by all implementations are initial enrollment and key update.

4. TECHNICAL BENEFITS/DISADVANTAGES OF VARIOUS ALTERNATIVES

Here all the alternatives described in sections 2.1 and 2.2 are analyzed, and their respective advantages & disadvantages are specifically shown if applied to the current NDS/IP domain.

We take various viewpoints in our analysis (as indicated by the subsection titles).

4.1 Scalability

Use of pre-shared keys with IPsec does not scale especially in mesh networks since a unique symmetric key should be generated for each IPsec connection. Adding new network element would require the generation and addition of a new key to each and every peer of the network element. Also, revocation would require similar operation. Manual effort and number of keys grow with $O(N^2)$ for the full mesh model. For the symmetric key hub-and-spoke approach, manual effort and number of keys grow with O(N) only. No standard tools exist for exchange, verification, and revocation of symmetric keys. Bandwidth and processing power of the hub SEG may prove as limiting factors because the hub must handle aggregate traffic of all connected SEGs (twice: in and out).

It is not necessary to route regular traffic through the hub SEG, but this requires additional functionality, which is not yet present in existing standards or solutions. All SEGs can share a secret key with the hub SEG and this will be used to establish a session key with any other SEG. Communication between SEGs will after this take place directly, without being routed through the hub SEG. If two SEGs have previously communicated, then they can also reuse the old session key. When adding a new SEG, both in the symmetric case and in the PKI case the new SEG must be provided with a new secret key (called private key in the PKI case). However, in the PKI case, this key can be generated locally and will not have to be distributed over the network (only the public key will have to be distributed).

In the case of PKI, initialization only involves configuration of the new element to enroll certificate from the CA. Revocation can be centrally implemented with revocation lists or online certificate status responders. The number of keys grows with O(N) only. Beyond plain key numbers however, manual action is required for the new element at the most. Certificate distribution, verification, and revocation can be handled automatically.

Scalability of the distributed trust model is somewhat limited because the number of necessary cross-certifications grows with $O(N^2)$ to achieve a full mesh. However, the growth is related to the number of CAs, which is much lower than the number of SEGs.

The hub-and-spoke PKI trust model does not suffer from bandwidth and processing power limitations because the hub does not have to handle bulk traffic. The main argument for PKI is simpler key distribution. Adding a new SEG will in this case not involve distribution of secrets over the network, since the private key can be generated locally and is not shared with anyone.

4.2 Performance

The performance of the chapter 2 alternatives is analyzed (such as effects of certificate path processing to the overall performance).

The potential bottlenecks of the system are directory services and OCSP responders, since validation often requires fetching revocation information (unless a still valid CRL or OCSP response is cached). Having multiple OCSP responders, publishing CRLs into multiple directories, and implementing directory replication redundancy can be added to avoid bottlenecks. If a mesh-type of cross-certification is being deployed (meaning that each operator CA has a separate cross-certificate with each operator CA it is relying to), the certificate path construction can become a very heavy process. This is due to the fact that an EE needs to go through potentially tens of different cross-certificates in the directory before finding the correct cross-certificate for a given certificate path. Having a hub-and-spoke (bridge CA) setup, the path constructions can become more lightweight.

The potential bottleneck introduced by using directory services for certificate retrieval maybe overcome by including the whole certificate chain into the IKE payload, if the trust model allows it.

As a VPN environment is considered to be a static environment, the amount of expected revocations is not expected high. Therefore the argument that is often heard against CRL to require high bandwidth is not applicable here (is applicable for end-user certificates), making it a simple method with low bandwidth requirements.

4.3 Management issues

The management issues related to elements which fall outside of intra-operator domain, such as Bridge CA, are analyzed. Also other management aspects than just key management issues are included.

Key management is generally eased in a PKI compared to the symmetric hub-and-spoke model. In both cases a new SEG must be equipped with its own private/secret key. However, in a PKI this key can be generated locally and need not be distributed over the network since this key is not shared with anyone else. In the symmetric case, this secret key must be distributed.

The conceptually simplest trust model can be achieved if the SEGs of all operators are certified by a common CA. Every SEG can then get the certificate of all other SEGs by consulting the common CA. The management and checking of revocation status is also simplified when a common CA is in control of all the certificates.

However, it might be more realistic that we will have a structure of regional CAs. Each regional CA then needs to be part of a hierarchical structure with a common root CA or needs to be cross-certified with all other regional CAs. Combinations of hierarchical structure and cross-certifications are also possible. Management of the CAs will then be done on a regional basis. Europe (EU), Asia (ASEAN) and North America (NAFTA) could be natural regional candidates.

4.4 Re-usability

The re-usability of the current and mostly used PKI practises, products and protocols against the above solutions are analyzed.

All the technical PKI practices deployed today (LDAP, HTTP, X.509v3 profile, CRLv2 profile, OCSP) should be fully re-usable. However, there is an area that is not widely deployed today: automatic online certificate lifecycle management. Certificate lifecycle management refers to operations and online interactions between PKI entities (EEs, RAs, and CAs) that are needed for enrolling certificates (first time enrollment), updating EE private keys before certificate expiration, CA key rollover, and requesting revocation online.

Without automatic certificate lifecycle management, updating certificates before expiration would involve manual administrator involvement. Also, enrolling the first certificate for EE should be an online process. Certificate Management Protocols v2 (CMPv2) [5] is an IETF standard (draft) for implementing certificate lifecycle management. The PKI industry has expressed strong support for CMPv2, and there has been extensive interoperability testing between vendors in PKI Forum (for more info, see [9]). Already today major CA products support server-side of the CMP protocol. However, the lack of client-side implementations has slowed the adoption of certificate lifecycle management. It is suggested that CMPv2 would be specified as a mandatory mechanism for managing certificates in intra- and inter-operator PKI operations. Support for multiple mechanisms would add unnecessary complexity, so it would be preferred to have a single supported protocol for implementing lifecycle management.

4.5 Interoperability

The interoperability of the above alternatives is analyzed.

1) Interoperability towards Rel-5 SEG

Pre-shared key is the only required authentication method in NDS/IP for Rel. 5. Therefore first NDS/IP implementations will rely on symmetric keys. NDS/AF should be interoperable with those implementations. There is no way to cross-certify or establish a common hierarchy between PKI and symmetric key solutions, however. Approaches providing automatic distribution of pre-generated symmetric keys from a trusted hub using public key cryptography do not seem practicable, because they provide no easy migration path. Thus such approaches may not be worth further study. Therefore interoperability must be provided by SEGs rather than by the NDS/AF. An interoperable SEG shall support both certificate-based and pre-shared key authentication to communicate with NDS/AF capable and Rel-5 SEG, respectively.

2) Interoperability guarantee by profiling the selected protocols for NDS/AF

Profiling the use of certificate fields, CRL usage, IKE Certificate handling will enhance the interoperability of NDS/AF SEG of different vendors and fasten the deployment and acceptance of the choosen solutions.

Following information may help for the profiling task later on:

- The Internet IP Security PKI Profile of ISAKMP and PKIX [10]
- Requirements for Large Scale PKI-Enabled VPNs [11]

4.6 IKE

Effects of NDS/AF on IKE: what authentication methods should be supported, and what not. Also Son of IKE is discussed.

4.6.1 IKE

IKE offers the following authentication methods:

- Signatures

- Public Key Encryption
- Revised Mode of Public Key Encryption
- Pre-Shared Key

The algorithms available for asymmetric operations are Digital Signature Algorithm (DSA) and Rivest-Shamir-Adleman (RSA).

Currently the most widely used mechanisms are:

1. Pre-shared key
2. Digital signatures using the RSA algorithm

Public key encryption methods are not recommended, since initiators must determine the responder’s public key from the IP address or from other relevant information. Currently public key encryption methods do not have very wide implementation support, and they are likely to be removed from the future version of IKE.

The RSA signature method has been tested on IPsec interoperability meetings and there is wide support for it among IPsec vendors. DSA signature method has received much less testing and there have been problems withs its interoperability among vendors in the interoperability meetings.

The security level of the RSA signature method can be enchanced by increasing the key length, and using stronger hash function etc, the security level of the DSA is mostly fixed as it is designed so that all parameters of the security are same, and for example changing the hash function is not possible. The RSA key length must be minimum 1024 bits, preferably greater.

4.6.2 Son of IKE (SOI)

Currently IETF investigates a successor of IKE: The 2 current proposals are JFK and IKEv2.

It is not part of this feasibility study to investigate or mandate the support of SOI on the SEG. However, to support migration from IKE to SOI for NDS/AF, the IKE signature method that is still supported by SOI shall be choosen. The current SOI proposal does support RSA signatures, hence this will be the proposed authentication method for NDS/AF.

If a need for the pre-shared keys is seen, 3GPP should contribute to IETF about this issue, since it is still uncertain if the pre-shared keys will remain in SOI.

4.7 Effects on operator’s environment

This section analyzes the effects of above solutions on operator's environment, and especially on their existing PKI solution.

As illustrated in Figure 1, secure communication between two operators is done via the Za-interface, ie between the Security Gateways (SEGs) of the two operators. By limiting the inter-operator communications to the Za-interface, the need for certificates will be limited to the number of operators. If an operator already has a PKI implemented for intra-operator communication, then this solution can be combined with the inter-operator PKI solution. In this way secure communication will be facilitated directly between network elements of different operators. However, the focus of this document is the Za-interface.

Existing PKI solutions providing end-user security will not be influenced.

The security policy established over the Za-interface is subject to roaming agreements if the security domains belong to different operators. This is different from the security policy enforced over the Zb-interface, which is the single responsibility of the operator that controls this security domain.

Operators will have different deployment options depending on the solutions chosen for the authentication framework. Most probably they will have existing PKI solutions that they have to take into consideration.

4.7.1 Symmetric key or public key approach

We argue that this choice is primarily a question of O&M costs driven by scalability issues, and consequently a practical question. With a symmetric key solution there will be small initial costs, but the number of keys grows exponentially with the number of nodes. A PKI solution will have larger initial costs, but a growth in the number of nodes will only cause a linear growth in the number of keys.

4.7.2 In- or out-sourcing

The safest way to achieve interoperable and re-usable solutions is to conform to widely recognized standard formats and protocols. By following such an approach in this work item, operators will have better chance of utilizing the PKI investments they might already have made.

If the requirements for PKI functionality in NDS/AF will differ a lot from existing infrastructure managed by the operator, out-sourcing could be a more likely choice. In-sourcing or out-sourcing is not only a question of physical infrastructure but also a question of having administrative processes in place and operative PKI management staff with the professional skills needed.

4.7.3 Build or buy

The suggested solution should be such that buying the technology is easier and faster than building it from scratch. This aims at faster deployment of the whole PKI concept.

4.7.4 Closed or open environment

In this work item PKI for the inter-operator domain is of primary concern. However, the chosen infrastructure should not prevent evolution towards intra-operator domain PKI.
One should neither preclude an extension towards an authentication framework for non-control plane nodes. Most probably a user-plane application of PKI will have requirements that differs from NDS/AF requirements in some aspects, but elements of the infrastructure could still be re-used.

4.8 Major technical and political risks

This section analyzes the technical and political risks of above solutions. At least the arrangement of CAs is a political issue, and agreeing on e.g. total hierarchy of CAs (or even Bridge CA trust model) may be difficult.

4.8.1 PKI recognition

Although PKI systems have been on the market for several years, PKI has not yet gained the widespread acceptance that some had expected. The most basic standards have been available for years. Nevertheless, there have also been expressed some opposing views on whether the PKI approach is a success.

The political reasons for opposition are mostly related to privacy concerns. This argument is only relevant for individual authentication and does not apply to our case. There might be a need for placing trust in a third party, but that does not necessarily apply to PKI only. Also in a symmetric key case one might need a third party in order to improve scalability.

4.8.2 Trust model

The choice of trust model is perhaps the most basic decision one has to make when designing an authentication framework for network domain security (NDS/AF).

A scalable solution can be obtained by introducing a CA level above the operator level CA, either a bridge CA or a master root CA.

A starting point could also be a one level deep hierarchy with all SEGs certified by a common CA. However, it is not obvious who should take the role of a master CA. It could be outsourced from the operator community, the operators could form a CA owned and operated jointly or one operator might own and/or operate it on behalf of the others.

The trust models that most probably could gain support from all operators are the distributed trust model and the hub-and-spoke model or a combination of these. A simple way of implementing the first case would be to require that each peer CA (see Figure 5) to be trusted should be directly cross-certified, thus no transitive trust relationships would be necessary. However, the case with a bridge CA is based on the use of transitive trust through the bridge CA, ie each CA will trust each CA to which the bridge CA connects.

The problem with the bridge model is that everyone must trust the bridge, just like everyone has to trust the root CA in a pure hierarchic model. The question then arises, which organization should run the bridge CA? In a distributed trust architecture, with regional CAs cross-certifying each other, then each operator only has to trust the regional CA.

In a strict hierarchic model all end-entities will store the public key of the root CA. This model is therefore very vulnerable for attacks on the root CA. If the private key of the root CA is compromised, then each node in the hierarcy must be updated with the new public key of the root CA. In the distributed trust model and the hub-and-spoke model then only other CAs will be influenced by the compromise of the keys of some central node.

4.8.3 Revocation methods

A possible approach could be a stepwise introduction of revocation mechanisms. Initially, it could be a very simple solution e.g. manual revocation. At later phases, periodic checking of CRLs may be used. Optionally, OCSP (Online Certificate Status Protocol) may replace or supplement the process of CRL checking.

4.8.4 Standard vs. proprietary solutions

It has to be sorted out whether NDS/AF has specific needs that call for non-standard PKI -solutions. It would clearly be an advantage to adhere to accepted standards. This will both ease interoperability and reduce the need for in-house software development.

4.8.5 Legal issues

The process of establishing trust relations involves legal issues. Both in the case of cross-certification and in the case of a common root CA detailed agreements has to be set up. It has to be settled what shall be the responsibility for each of the partners.

5. SUMMARY AND CONCLUSIONS

These are the current working assumptions according to the Feasibility Study work.

- It is feasible to apply NDS/AF to the current NDS/IP domain
- A PKI-based system has clear benefits compared to a symmetric approach: scalability and more simple key distribution
- The trust model is open, but different alternatives are analyzed in the FS
- Automatic certificate life cycle management is preferred over PKCS#10/7 and SCEP approaches
- CRL's are preferred over OCSP
- FS does not cover the actual protocol profling
- IKE including certificate chain in payload is preferred to repository access if the trust model allows this

6. REFERENCES

[1] PKI Forum, "CA-CA Interoperability", March 2001:
< http://www.pkiforum.org/pdfs/ca-ca_interop.pdf >

[2] Manyfolks, "RFC 2560: Online Certificate Status Protocol – OCSP", June 1999.

[3] Manyfolks, "RFC 2459: Certificate and CRL Profile", January 1999

[4] C. Adams & S. Farrell, "RFC2510: Certificate Management Protocols", March 1999

[5] C. Adams & S. Farrell, "Internet draft: Certificate Management Protocols", December 2001
< draft-ietf-pkix-rfc2510bis-06.txt >

[5] Manyfolks, "RFC 2797: Certificate Management Messages over CMS", April 2000

[6] 3GPP TS 33.210 NDS/IP v5.1.0 (2002-06)

[7] Simple Certificate Enrollment Protocol, SCEP:
< http://search.ietf.org/internet-drafts/draft-nourse-scep-06.txt >

[8] Certificate Management Protocol version 2:
< http://www.ietf.org/internet-drafts/draft-ietf-pkix-rfc2510bis-06.txt >

[9] Extensive interoperability testing between vendors in PKI Forum:
< http://www.pkiforum.org/news/ 2001/CMP_FINAL3.htm >

[10] The Internet IP Security PKI Profile of ISAKMP and PKIX (June 2002):
< http://www.ietf.org/internet-drafts/draft-ietf-ipsec-pki-profile-00.txt >

[11] Requirements for Large Scale PKI-Enabled VPNs:
< draft-dploy-requirements-00.doc at http://www.projectdploy.com/ >