Technical Specification Group Services and System Aspects Meeting #25, Palm Springs, USA

TSGS#25(04)0623

Source: **SA WG3**

Title: **CR to 33.310: Splitting the Roaming CA into a SEG CA and an Interconnection CA (Rel-6)**

Document for: **Approval**

Agenda Item: **7.3.3**

The following CR was agreed by SA WG3 and is presented to TSG SA for approval.

TSG SA Doc number	Spec	CR	Rev	Phase	Subject	Cat	Version-Current	SA WG3 Doc number	Work item
SP-040623	33.310	004	-	Rel-6	Splitting the Roaming CA into a SEG CA and an Interconnection CA	C	6.1.0	S3-040643	SEC1-NDS-AF

3GPP TSG-SA WG3 Meeting #34
Acapulco, Mexico, 6-9 July 2004

Tdoc ⌘S3-040643

CR-Form-v7

CHANGE REQUEST

⌘ **33.310** **CR** **004** ⌘**rev** **-** ⌘ Current version: **6.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: | UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network **X**

Title:	⌘	Splitting the Roaming CA into a SEG CA and an Interconnection CA
Source:	⌘	SA WG3
Work item code:	⌘	SEC1-NDS-AF
Date:	⌘	29/06/2004
Category:	⌘	**C**
Release:	⌘	Rel-6

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 *(GSM Phase 2)*
R96 *(Release 1996)*
R97 *(Release 1997)*
R98 *(Release 1998)*
R99 *(Release 1999)*
Rel-4 *(Release 4)*
Rel-5 *(Release 5)*
Rel-6 *(Release 6)*

Reason for change:	⌘	The current Roaming CA is used for issuing certificates to the operator's SEGs and to its roaming/interconnect partners. This means that other operators need to be involved every time the Roaming CA keys are renewed. If the Roaming CA is split into a SEG CA and an Interconnection CA then only renewal of SEG CA keys would require other operators to be involved. Furthermore, the SEG CA can be made more secure than a combined Roaming CA which can help reduce the need for SEG CA key renewal and thus reduce the need for inter-operator CA procedures during operation of the system.
Summary of change:	⌘	The current Roaming CA is split into a SEG CA that issues end entity certificates to SEGs within a particular operator's domain, and an Interconnection CA that issues cross-certificates on behalf of a particular operator to the SEG CAs of other domains with which the operator's SEGs have interconnection. Note that it is still optional for an operator to set up both SEG CA and Interconnection CA as a single CA.
Consequences if not approved:	⌘	Opportunities are missed to reduce the need for inter-operator CA procedures during operation of the system.

Clauses affected:	⌘	3.1, 5, 5.1.1, 5.2, 5.2.1, 5.2.2, 5.2.3, 5.2.3a (new), 5.2.3b (new), 5.2.3c (new), 5.2.3d (new), 5.2.3e (new), 5.2.4, 5.2.5, 5.2.6, 5.2.7, 5.2.8, 5.2.9, 5.2.11, 6.1, 6.1.2, 6.1.3, 6.1.4, 7.1, 7.2, 7.3, 7.4, 7.5, B.4.1, B.4.4, B.5.3

	Y	N		
Other specs affected:	⌘		**N**	Other core specifications ⌘
			N	Test specifications
			N	O&M Specifications

Other comments:	⌘	

***** Begin of Change ****

3.1 Definitions

For the purposes of the present document, the definitions given in 3GPP TR 21.905 [8] and the following definitions apply:

Interconnection CA: The CA that issues cross-certificates on behalf of a particular operator to the SEG CAs of other domains with which the operator's SEGs have interconnection.

Local CR: Repository that contains cross-certificates.

Local CRL: Repository that contains cross-certificate revocations.

PSK: Pre-Shared Key. Method of authentication used by IKE between SEG in NDS/IP [1].

Public CRL: Repository that contains revocations of SEG and CA certificates and can be accessed by other operators.

SEG CA: The CA that issues end entity certificates to SEGs within a particular operator's domain.

~~**Roaming CA:** The CA that is responsible for issuing certificates for SEG that have interconnection with another operator.~~

***** End of Change ****

***** Begin of Change ****

5 Architecture and use cases of the NDS/AF

The following types of certification authority are defined:

- SEG CA: A CA that ~~This~~ issues end entity certificates to SEGs within a particular operator's domain.
- Interconnection CA: A CA that ~~This~~ issues cross-certificates on behalf of a particular operator to the SEG CAs of other domains with which the operator's SEGs have interconnection.

The public key of the ~~roaming~~ interconnection CA ~~certificate of the owning operator~~ shall be stored securely in each~~the~~ SEG within the operator's domain. This allows the SEG to verify cross certificates issued by its operator's Interconnection CA~~It defines who is the authority that the device trusts when connecting to other devices~~. It is assumed that each operator domain could include 2 to 10 SEGs.

An operator may decide to set up both SEG CA and Interconnection CA as a single CA, i.e. separation of CAs is not required.

The NDS/AF is initially based on a simple trust model (see Annex B) that avoids the introduction of transitive trust and/or additional authorisation information. The simple trust model implies manual cross-certification.

***** End of Change ****

***** Begin of Change ****

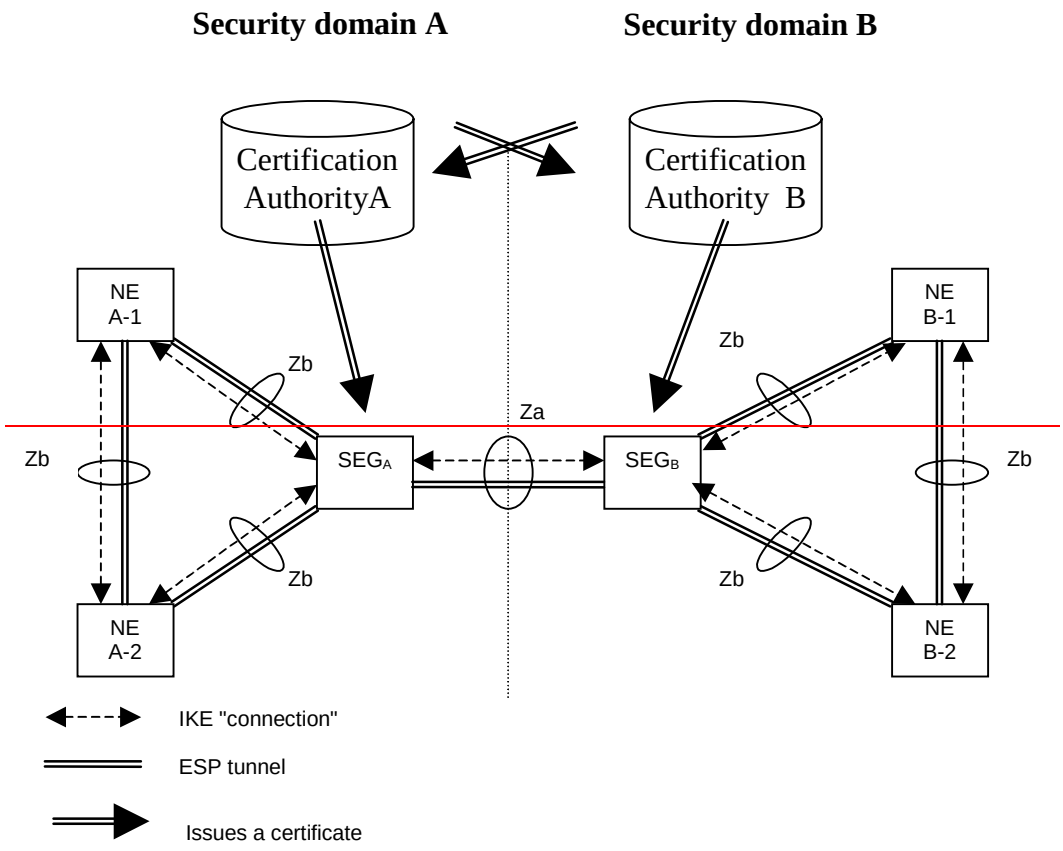
5.1.1 General architecture

Each security domain has at least one ~~certification authority~~SEG CA and one I~~i~~nterconnection CA dedicated to it. ~~The certification authority which the network elements use for inter-operator authentication is called the roaming CA of the domain.~~

The ~~roaming~~ SEG CA of the domain issues certificates to the SEGs in the domain that have interconnection with SEGs in other domains. The Interconnection CA of the domain issues certificates to the SEG CAs of other domains with which the operator's SEGs have interconnection. This specification describes the profile for the ~~roaming CA and a profile for the SEG~~various certificates that are needed. Also a method for creating the cross-certificates is described.

In general, all of the certificates shall be based on the Internet X.509 certificate profile [3].

The ~~roaming~~ SEG CA shall issue certificates for SEGs ~~in~~ that implement the Za interface. When SEG of the security domain A establishes a secure connection with the SEG of the domain B, they shall be able to authenticate each other. The mutual authentication is checked using the certificates the ~~roaming~~ SEG CAs issued for the SEGs. When a roaming agreement is established between the domains, the ~~roaming~~ Interconnection CAs cross-certify ~~with each other~~the SEG CA of the peer operator. The created cross-certificates need only to be configured locally to each domain. The cross-certificate, which Interconnection ~~roaming~~ CA of security domain A created for the SEG CA of security domain B, shall be available for the domain A SEG which provides the Za interface towards domain B. Equally the corresponding certificate, which the Interconnection ~~roaming~~ CA of the security domain B created for SEG CA of security domain A, shall be available for the domain B SEG which provides Za interface towards domain A.


Security domain A
Security domain B
Certification AuthorityA
Certification Authority B
NE A-1
NE A-2
NE B-1
NE B-2
SEG$_A$
SEG$_B$
Zb
Za
IKE "connection"
ESP tunnel
Issues a certificate

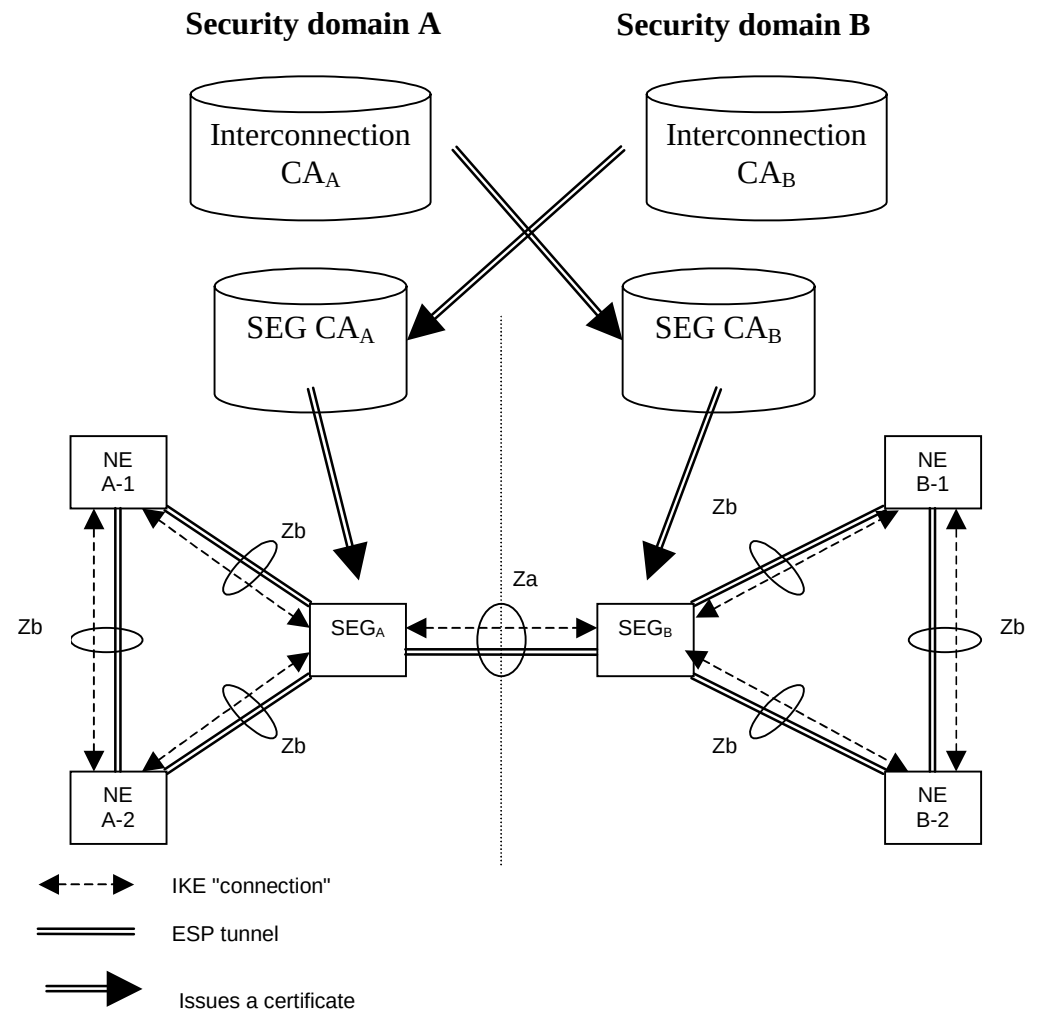


Figure 2: Trust validation path in context of NDS/IP

After cross-certification, the SEGa is able to verify the path: SEGb ->~~Authority~~ SEG CA_B~~B~~ -> ~~Authority~~ Interconnection CA_A~~A~~. Only the certificate of the Interconnection~~roaming~~ CA_A in domain A needs to be trusted by entities in security domain A.

Equally the SEGb is able to verify the path: SEGa -> SEG CA_A~~Authority A~~ -> Interconnection CA_A~~Authority B~~. The path is verifiable in ~~B~~ domain B, because the path terminates to a trusted certificate (~~roaming~~Interconnection CA_B of the security domain B in this case).

The Interconnection ~~roaming~~ CA signs the second certificate in the path. For example, in ~~A~~ domain A, the certificate for ~~roaming~~ SEG CA B is signed by the ~~roaming~~ Interconnection CA of ~~the A~~ domain A when the cross-certification is done.

5.2 Use cases

5.2.1 Operator Registration: Creation of roaming agreement

Security gateways (SEGs) of two different security domains need to establish a secure tunnel, when the operators make a roaming (or any interconnection) agreement. The first technical step in creating the roaming agreement between domains is the creation of cross-certificates~~ion of~~ by the Interconnection ~~roaming~~ CAs of the two domains.

Inter-operator cross-certification can be done using different protocols, but the certification authority shall support the PKCS#10 [2] method for certificate requests. Both ~~roaming~~ SEG CAs create a PKCS#10 certificate request, and send it to the other operator's Interconnection CA. The method for transferring the PKCS#10 request is not specified, but the transfer method shall be secure. The PKCS#10 can be transferred e.g. in a floppy disk, or be send in a signed email. The

PKCS#10 request contains the public key of the authority and the name of the authority. When the Interconnection ~~roaming~~ CA accepts the request, a new cross-certificate is created. The authority shall make that new certificate available to SEGs in his own domain by storing the new cross-certificate into a local CR (Certificate Repository) which all SEGs that need to communicate with the other domain shall access using LDAP. The cross-certification is a manual operation, and thus PKCS#10 is a suitable solution for the roaming agreement.

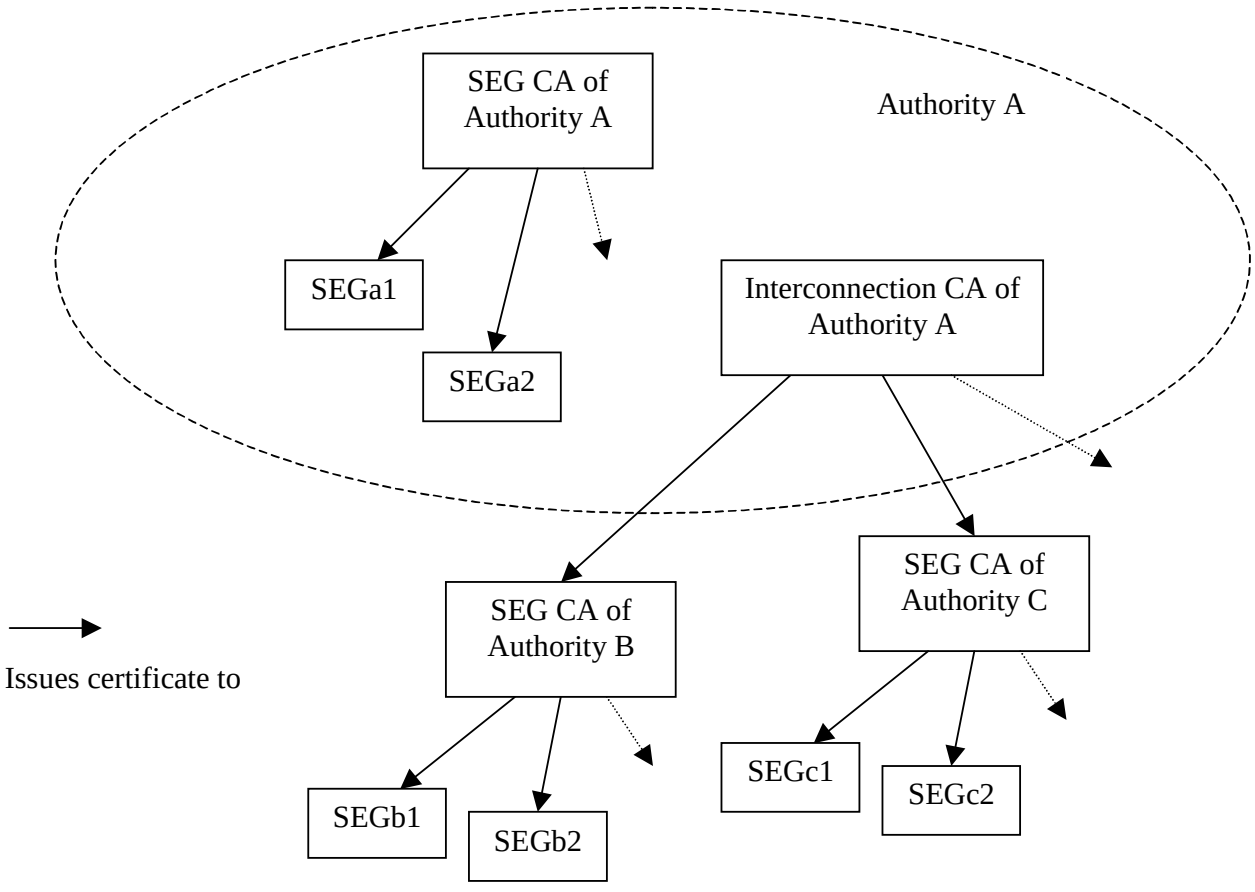
Editor's note: CMPv2 as a protocol has cross-certification capabilities as well, but that functionality is not considered to be implemented widely enough or interoperable.

~~Observe that these actions~~Creation of a roaming agreement only ~~involve~~involves use of the private keys of the ~~Roaming~~Interconnection CAs. ~~;~~ T~~t~~here is no need for the operators to use the private keys of their respective SEG CAs in forming a roaming (or interconnection) agreement.

When creating the new cross-certificate, the Interconnection ~~roaming~~ CA should use basic constraint extension (according to section 4.2.1.10 of [3]) and set the path length to zero. This inhibits the new cross-certificate to be used in signing new CA certificates. The validity of the certificate should be set sufficiently long. The cross-certification process needs to be done again when the validity of the cross-certificate is ending.

When the new cross-certificate is available to the SEG, all that needs to be configured in the SEG is the DNS name or IP address of the peering SEG gateway. The authentication can be done based on the created cross-certificates.

~~When the cross-certification is implemented this way, the PKI architecture seems hierarchical to the network elements in the domain: At the very top of the hierarchy sits the roaming CA of the domain. At the second level, there are certificates directly issued by the roaming CA for the SEGs together with the cross-certificates issued for the peering domains. The certificates of the peer domains are located under the cross-certificates of the peer domains.~~



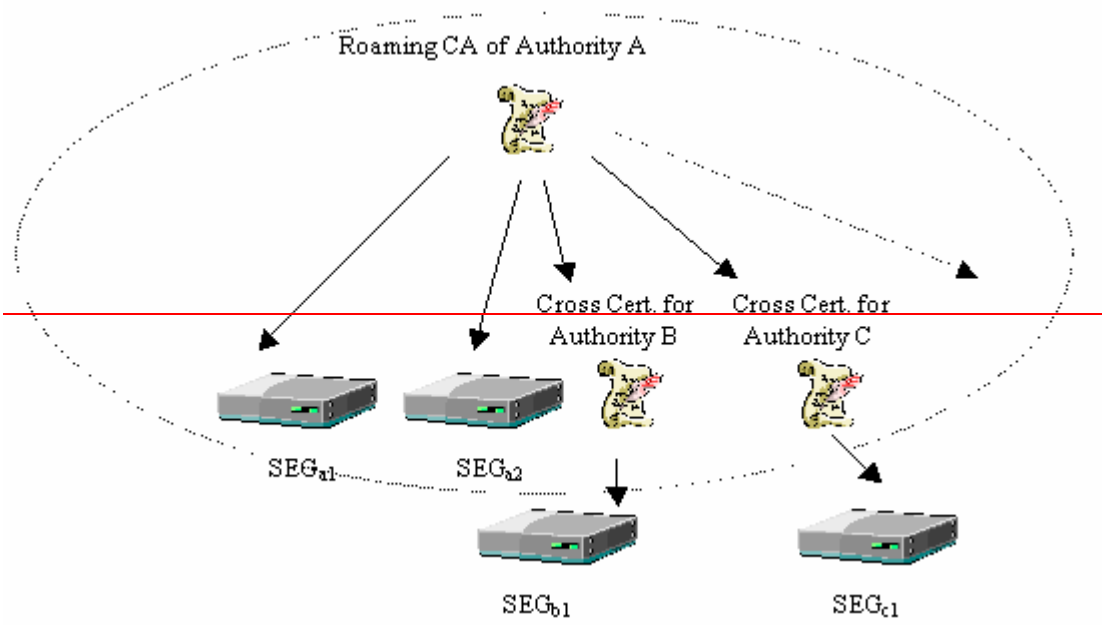


Figure 3: ~~Security domain A illustrated. The PKI is hierarchical inside the domain~~Certificate Hierarchy

5.2.2 VPN tunnel establishment

After establishing a roaming agreement and finishing the required preliminary certificate management operations as specified in the previous section, the operators configure their SEGs for SEG-SEG connection, and the SAs are established as specified by NDS/IP [1].

In each connection configuration, the remote SEG DNS name or IP address is specified. Only the local ~~roaming~~ Interconnection CA ~~is~~ and SEG CA are configured as ~~the~~ trusted CAs. Because of the cross-certification, any operator whose ~~roaming~~ SEG CA has been cross-certified can get access using this VPN connection configuration

The following is the flow of connection negotiation from the point of view of Operator A's SEG (initiator). Operator B's SEG (responder) shall behave in a similar fashion.

- During connection initiation, the initiating Operator A's SEG A provides its own SEG certificate and the corresponding digital signature in IKE Main Mode message 3;
- SEG A receives the remote SEG B certificate and signature;
- SEG A validates the remote SEG B signature;
- SEG A verifies the validity of the SEG B certificate by a CRL check to both the Operator A and Operator B CRL databases. If a SEG cannot successfully perform both CRL checks, it shall treat this as an error and abort tunnel establishment;
- - SEG A validates the SEG B certificate using the cross-certificate for Operator B's SEG CA by executing the following actions:
    - SEG A verifies the validity of the cross-certificate for Operator B's SEG CA by a CRL check to the Operator A's Interconnection CA CRL database. If a SEG cannot successfully perform the CRL check, it shall treat this as an error and abort tunnel establishment.
    - ~~o~~SEG A validates the cross-certificate for Operator B's SEG CA using its Interconnection ~~roaming~~ CA's certificate if the Interconnection ~~roaming~~ CA is not a top-level CA, otherwise the Interconnection ~~roaming~~ CA's public key is implicitly trusted.
- The IKE Phase 1 SA is established and the Phase-2 SA negotiation proceeds as described in NDS/IP [1] with PSK authentication.

NOTE: This specification provides authentication of SEGs in an "end-to-end" fashion as regards to roaming traffic (operator to operator). If NDS/AF (IKE) authentication were to be used for both access to the transport network (e.g. GRX) and for the end-to-end roaming traffic, IPsec mechanisms and policies such as iterated tunnels or hop-by-hop security would need to be used. However, it is highlighted that the authentication framework specified is independent of the underlying IP transport network.

5.2.3 Operator deregistration: Termination of roaming agreement

When a roaming agreement is terminated or due to an urgent service termination need, all concerned SEG peers shall remove the IPsec SAs using device-specific management methods. Each concerned operator shall also list the cross-certificate created for the Interconnection ~~roaming~~ CA of the terminated operator in his own local CRL.

5.2.3a Interconnection CA registration

In principle only one Interconnection CA shall be used within the operator's network, but using more than one Interconnection CA is possible (in which case the public keys of all the operator's interconnection ~~roaming~~ CAs should be installed in the operator's SEGs). The involved actions in Interconnection CA registration are those as described in the cross-certification part of clause 5.2.1: 'Operator Registration: creation of roaming agreement'. Such a situation may exist if the Interconnection CA functions are to be moved from one responsible organisation to another (e.g. outsourcing of CA services).

5.2.3b Interconnection CA deregistration

If ~~a~~an Interconnection CA is removed from the network, it shall be assured that all certificates that have been issued by that CA to SEG CAs, and have not expired yet, shall be listed in the CRLs.

5.2.3c Interconnection CA certification creation

The Interconnection CA certificate may not be the top-level CA of the operator, which means that the Interconnection CA certificate is not self-signed. If the Interconnection CA certificate is self-signed then it needs to be securely transferred to each SEG and stored within secure memory otherwise it can be managed in the same way as a SEG certificate.

The Interconnection CA certificate shall have a 'longer' lifetime than SEG CA certificates in order to avoid the cross-certification actions that are needed each time ~~a~~an Interconnection CA certificate has to be renewed.

NOTE: There is no need to involve other operators when creating an Interconnection CA certificate.

5.2.3d Interconnection CA certification revocation

If ~~a~~an Interconnection CA key pair gets compromised then a hacker could use the keys to issue himself SEG CA certificates which in turn could be used to issue SEG certificates. Since however the trusted Interconnection CA certificates are stored locally on the SEG device or in a dedicated repository (i.e. received Interconnection CA certificates within the IKE payload shall not be accepted), the hacker also needs to compromise the SEG or the local repository to be able to set up an IPsec tunnel.

Existing IPsec tunnels need not be torn down. The old cross-certificates - and any other certificates - issued by the Interconnection CA shall be taken out of service by listing them in the Interconnection CA's CRL (provided the operator still has the key available to sign this CRL) and removing them from the dedicated repository. If the Interconnection CA certificate is self-signed then it shall be removed from each of the operator's SEGs. If the Interconnection CA certificate is issued by a higher level CA of the operator, then it shall be revoked by this higher level CA.

The operator has to create a new Interconnection CA key pair, perform the actions as described within clause 5.2.~~6~~3c for Interconnection CA certification creation, and perform the actions as described within clause 5.2.1 to generate new cross-certificates for all his interconnected networks SEG CAs. ~~load the public key part securely into all the SEGs in the operator's domain and generate new cross-certificates for all his interconnected networks SEG CAs. The old cross-certificates and certificates can be taken out of service by listing them in the CRL.~~

NOTE: There is no need to involve other operators when revoking an Interconnection CA ~~creating a new Interconnection CA key pair~~ certificate.

5.2.3e Interconnection CA certification renewal

The Interconnection CA certificate has to be renewed before the old Interconnection CA certificate expires. The renewing of an Interconnection CA certificate involves repeating the actions as described in clause 5.2.3c. This should be done before the old certificate expires.

NOTE: There is no need to involve other operators when renewing an Interconnection CA certificate.

5.2.4 ~~Roaming~~ SEG CA registration

In principle only one ~~roaming~~ SEG CA shall be used within the operator's network, but using more than one ~~roaming~~ SEG CA is possible. The involved actions are those as described in the cross-certification part of clause 5.2.1: 'Operator Registration: creation of roaming agreement'. Such a situation may exist if the ~~roaming~~ SEG CA functions are to be moved from one responsible organisation to another (e.g. outsourcing of CA services).

5.2.5 ~~Roaming~~ SEG CA deregistration

If a ~~roaming~~ SEG CA is removed from the network, it shall be assured that all ~~cross-certificates and~~ certificates that have been issued by that ~~roaming~~ CA to SEGs, and have not expired yet, shall be listed in the CRLs.

5.2.6 ~~Roaming~~ SEG CA certificate creation

The involved actions are those as described in the cross-certification part of clause 5.2.1: 'Operator Registration: creation of roaming agreement'.

The SEG CA certificate does ~~may~~ not have~~d~~ to be the top-level CA of the operator, which means that the SEG CA certificate is not self-signed. One option is to sign the operator's SEG CA with the operator's own ~~Roaming~~Interconnection CA, as this will already be a trust point established in the operator's own SEGs. If the SEG ~~roaming~~ CA certificate is self-signed then it should ~~needs to~~ be securely transferred to each of the operators's SEGs and stored within secure memory (see NOTE~~ote~~ to Section 7.5).~~otherwise it can be managed in the same way as a SEG certificate.~~

~~The roaming CA certificate may not be the top-level CA of the operator, which means that the roaming CA certificate is not self-signed. If the roaming CA certificate is self-signed then it needs to be securely transferred to each SEG and stored within secure memory otherwise it can be managed in the same way as a SEG certificate.~~

~~The roaming CA certificate shall have a 'longer' lifetime than cross-certificates and SEG certificates in order to avoid the cross-certification actions that are needed each time a roaming CA certificate has to be renewed.~~

5.2.7 ~~Roaming~~ SEG ~~-~~CA certificate revocation

This compromise is a serious event as it will require **all** the cross-certificates issued by other operators' Interconnection CAs to that SEG CA to be revoked.

Existing IPsec tunnels need not be torn down, unless they were formed very recently i.e. after the time at which the operator suspects the CA key became compromised, but before the cross-certificate used to establish the tunnel was revoked.

To restore inter-domain interoperability, the operator has to create a new SEG CA key pair and use it to issue certificates to all the SEGs in the operator's own domain. The operator shall~~must~~ then provide a ~~a~~ cross-certification request~~PKCS#10~~ (see clause 5.2.1) for the new SEG CA key-pair to the operators with whom it has roaming agreements.~~, so that they can issue new cross-certificates.~~

It is recommended that operators carefully protect their SEG CA keys to limit this knock-on effect across the operator community.

~~If a roaming CA key pair gets compromised then a hacker could use the keys to issue himself cross-certificates. Since however the trusted cross-certificates are stored locally on the device or in a dedicated repository (so received cross-~~

~~certificates within the IKE payload shall not be accepted), the hacker also needs to compromise the SEG or the local repository to be able to set up an IPsec tunnel.~~

~~Existing IPsec tunnels need not be torn down. The operator has to create a new roaming CA certificate, initiate new cross-certification and SEG certificates as if he would create new roaming agreements with all his partner networks. The old cross-certificates and certificates can be taken out of service by listing them in the CRL.~~

5.2.8 ~~Roaming~~ SEG CA certificate renewal

The ~~roaming~~ SEG CA certificate has to be renewed before the old ~~roaming~~ SEG CA certificate expires. The renewing of a ~~roaming~~ SEG CA certificate involves repeating the actions as described in the cross-certification part of clause 5.2.1: 'Operator Registration: creation of roaming agreement'.~~results in the need to renew the cross-certificates~~. This should be done before the old certificate expires.

5.2.9 SEG registration

If not already done, a SEG certificate has to be created (see clause 5.2.11 for a description on certificate creation).

If a SEG is added to the network, the policy database of this SEG has to be configured using device-specific management methods.

Other operators have to be informed of the new SEG: The SEG policy databases of SEGs in other networks may have to be adapted.

***** End of Change ****

***** Begin of Change ****

5.2.11 SEG certificate creation

Using device-specific management methods, the certificate creation shall be initiated. As specified in section 7.2, either the CMPv2 protocol between the ~~roaming~~ SEG CA and the SEG for automatic certificate enrolment or manual SEG certificate installation using PKCS#10 formats can be used. This is an operator decision depending for example on the number of SEG elements.

***** End of Change ****

***** Begin of Change ****

6.1 Certificate profiles

This clause profiles the certificates to be used for NDS/AF. An NDS/AF component shall not expect any specific behaviour from other entities, based on certificate fields not specified in this section.

Certificate profiling requirements as contained in this specification have to be applied in addition to those contained within RFC3280 [3]. This applies for ~~both~~ the SEG, the SEG CA and the ~~roaming~~ Interconnection CA.

Before fulfilling any certificate signing request, the ~~a roaming~~ SEG CA and Interconnection CA shall make sure that the request suits the profiles defined in this section. Furthermore, the CAs shall check the Subject's DirectoryString order for consistency, and that the Subject's DirectoryString belongs to its own administrative domain.

SEGs shall check compliance of certificates with the NDS/AF profiles and shall only accept compliant certificates.

***** End of Change ****

***** Begin of Change ****

6.1.2 Interconnection CA Certificate profile

In addition to clause 6.1.1, the following requirements apply:

- The RSA key length shall be at least 2048-bit;
- 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 1.

6.1.3 SEG Certificate profile

SEG certificates shall be directly signed by the ~~roaming~~ SEG CA in the operator domain that the SEG belongs to~~, i.e. without employing any intermediate CAs. This limits NDS/AF complexity and makes retrieval and validation of intermediate CA certificates by SEGs unnecessary~~. Any SEG shall use exactly one certificate to identify itself within the NDS/AF.

In addition to clause 6.1.1, the following requirements apply:

- The RSA key length shall be at least 1024-bit;
- Issuer name is the same as the subject name in the ~~roaming~~ SEG CA certificate.
- Extensions:
  - Optionally non critical authority key identifier;
  - Optionally non critical subject key identifier;
  - Mandatory non-critical subjectAltName;
  - Mandatory critical key usage: At least digitalSignature and keyEncipherment shall be set;
  - Optional non-critical extended key usage: If present, at least server authentication and IKE intermediate shall be set;
  - Mandatory critical Distribution points: CRL distribution point;

NOTE: Depending on the availability of DNS between peer SEGs, the following rule is applied:

- subjectAltName should contain IP address (in case DNS is not available);
- subjectAltName should contain FQDN (in case DNS is available).

6.1.4 ~~Cross~~ SEG CA certificate profile

In addition to clause 6.1.1, the following requirements apply:

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

- Subject name is the same ~~as is the same~~ as the issuer~~subject~~ name in the SEG certificate~~, which the authority of the other domain uses in its certificates~~;
- Issuer n~~N~~ame is the same as ~~is the same as~~ the subject name in the Interconnection CA certificate~~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.

***** End of Change ****

***** Begin of Change ****

7.1 Repositories

During VPN tunnel establishment, each SEG has to verify the validity of its peer SEG's certificate according to section 5.2.2. Any certificate could be invalid because it was revoked (and replaced by a new one) or a SEG or operator has been deregistered.

SEG_B has to verify that:

a) the cross-certificate ~~of~~ SEG CA_A is still valid;

b) the certificate of SEG_A is still valid,

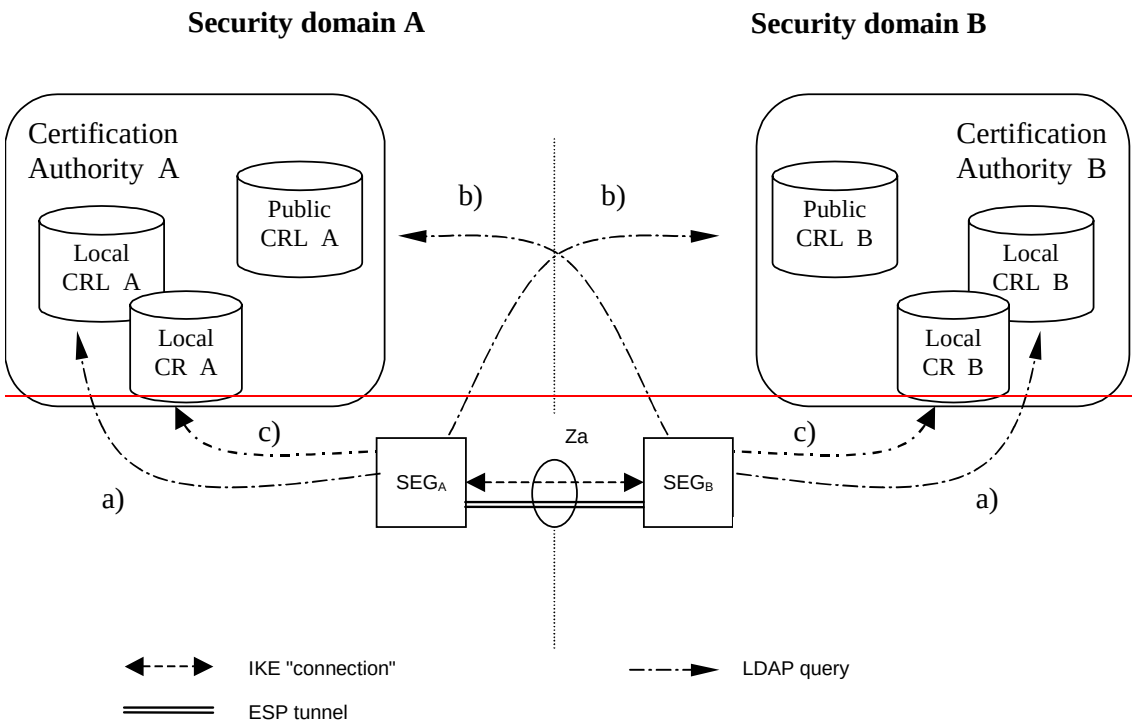
and be able to:

c) fetch the cross-certificate of SEG CA_A (if not found in SEG_B's cache).

SEG_A performs the same checks from its own perspective.

Check a) can be performed by querying the local CRL. For check b), a CRL of the peering SEG CA shall be queried. At this point of time, the VPN tunnel is not yet available, therefore the public CRL of the peering SEG CA shall be accessible for a SEG without utilising the Za interface.

Figure 4 illustrates the repositories and the above-mentioned steps a) – c). The local CR contains cross-certificates for SEG CAs, the local CRL contains SEG~~F~~ CA cross-certificate revocations, and the public CRL contains revocations of SEG and SEG CA certificates, and can be accessed by other operators.



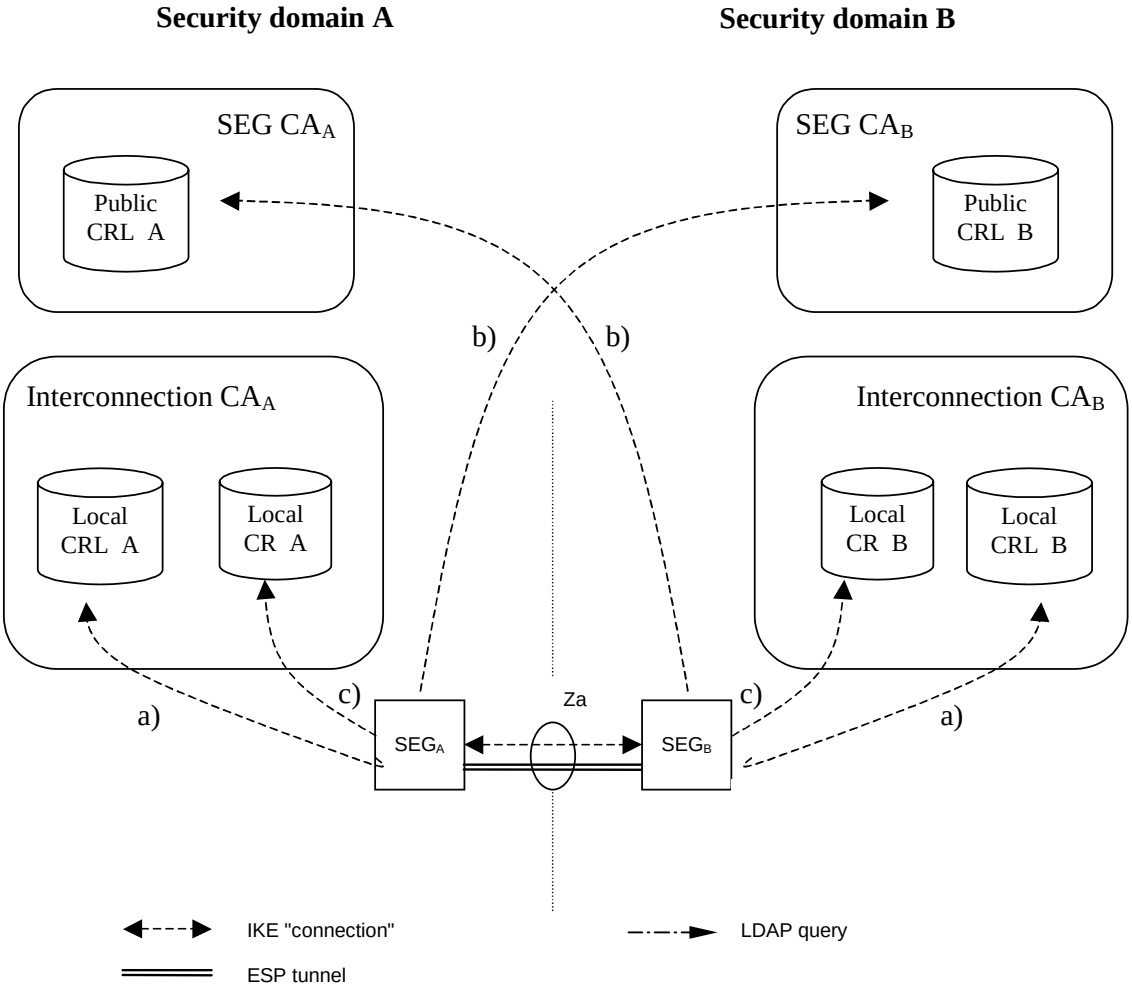


Figure 4: Repositories

If the SEG CA and Interconnection CA are combined then t~~T~~he public and local repositories of the~~a~~ CA may be implemented as separate databases or as a single database which is accessible via two different interfaces. Access to the "public" CRL is public with respect to the interconnecting transport network (e.g. GRX). The public CRL should be adequately protected (e.g by a firewall) and the owner of the public CRL may limit access to it according to his roaming agreements. Access to a public CRL database shall not be done via the ESP tunnel of the Za-interface.

NOTE: First this is not necessary as the retrieved CRL is integrity protected and contains no confidential information. Secondly access via an unprotected interface is anyhow necessary in case no currently valid security association is available to access the public CRL database and would require a dynamic behaviour of the IPsec policy database.

SEGs shall use LDAP to access the CRL and cross-certificate repositories.

NOTE: Interfaces a) and c) for locating the data used for functions in Za interface belong to the scope of NDS/AF (in addition to public b) interface) as the purpose is to guarantee the interoperability between different SEG and repository implementations. The possible migration to the cross-certification with a Bridge CA would also require these interfaces to be specified.

7.2 Life cycle management

Certificate Management Protocol v2 (CMPv2) [4] shall be the supported protocol to provide certificate lifecycle management capabilities. All SEGs and ~~Roaming~~ SEG CAs shall support initial enrolment by SEG ~~from~~ to the SEG CA via CMPv2, i.e. receiving a certificate from the ~~roaming~~ SEG CA, and updating the key of the certificate via CMPv2 before the certificate expires.

Enrolling a certificate to a SEG is an operation that may be done more often than inter-operator cross-certifications, thus more automation could be required by the operator than is possible with a PKCS#10 approach. However, also manual SEG certificate installation using PKCS#10 formats shall be supported. It should be also noted that the lifetime of a SEG CA cross-certificate is considerably longer than the lifetime of a SEG certificate. The basic CMPv2 functionalities such as enrolment and key update are widely implemented and interoperable.

Editor's note: CMPv2 is still at draft status, but is already widely supported (see 'CMP Interop Project': http://www.ietf.org/proceedings/00dec/slides/PKIX-4/), and expected to move to Draft Standard status in the near future. Thus it is expected that CMPv2 receives a RFC status before the NDS/AF specification is completed. Additionally, CMPv2 is preferred to CMPv1(RFC2510), because of the interoperability issues with CMPv1.

7.3 Cross-certification

Both operators use the following procedure to create a SEG CA cross-certificates:

1. The ~~roaming~~ SEG CA creates a PKCS#10 certificate request, and sends it to the other operator;
2. The Interconnection ~~roaming~~ CA receives a similar request from the other operator;
3. The Interconnection ~~roaming~~ CA accepts the request and creates a new cross-certificate;
4. The SEG CA cross-certificate is stored once into the local CR of the Interconnection CA and LDAP is used to fetch cross-certificates.

7.4 Revoking a SEG CA cross-certificate

The following procedure is used to revoke a cross-certificate:

1. The cross-certificate is added into the Interconnection CA's CRL;
2. The cross-certificate is removed from the Interconnection CA's CR.

7.5 Authentication during the IKE phase 1

Authentication during IKE Phase 1 is shown in Figure 4 above. The SEGa uses the following procedure to authenticate SEGb:

1. SEGa requests SEGb's certificate using the IKE certificate request payload;
2. SEGa receives SEGb's certificate inside the IKE certificate payload;
3. SEGa authenticates SEGb (verifies signatures);
4. SEGa fetches a CRL from the (public) CRL database of SEG CAb if the locally cached CRL has not yet expired;
5. SEGa uses this CRL to verify the status of SEGb's certificate;
6. SEGa uses either the locally cached cross-certificate or fetches the cross-certificate from the (local) Interconnection CAa CR~~a~~;
7. SEGa fetches a CRL from the (local) Interconnection CAa CRL~~a~~ if the locally cached CRL has not yet expired;
8. SEGa uses this CRL to verify the status of the SEG CA cross-certificate;
9. SEGa verifies the status of the Interconnection ~~roaming~~ CAa certificate if the ~~roaming~~ Interconnection CAa is not a top-level CA, otherwise Interconnection ~~roaming~~ CAa is implicitly trusted.~~;~~

NOTE: If the local SEG CA public key is securely installed on every SEG within an operator's domain, then a cross-certificate does not need to be checked when SEGa and SEGb belong to the same operator's domain~~A cross-certificate only needs to be checked if SEGa and SEGb belong to different Cas~~.

***** End of Change ****

***** Begin of Change ****

B.4.1 Need for nameConstraint support in certificates or strong legal bindings and auditing

If no precautions are taken, it is possible that an operator (M) whose ~~Roaming~~ SEG CA has been signed by the Bridge CA (= certified by the Bridge), creates certificates that resemble another operator's (A) certificates, letting M access to operator (B)'s network, even without authorization.

Let's say operator B has the following configuration for access to her subnetwork reserved for handling roaming traffic:

- Local-Subnetwork = some ipv6 subnetwork address;
- TrustedCA's = BridgeCA;
- AllowedCertificateSubject = O=Operator A or O=Operator C or O=Operator D.

NOTE: The IP addresses of the remote SEGs are not limited, as authentication is done based on certificates, and all trusted operators are allowed similar access. If different foreign operators would require to access different subnetworks, there would be several configuration blocks like the above, with the IP addresses appropriately specified.

Such "AllowedCertificateSubject" feature (the term name is imaginary) is widely supported by PKI-capable IPSec devices.

If Operator M used certificates of the following form for her certificates, she would not be allowed in:

- Subject: CN=SEG 1, O=Operator M;

- Signer: CN=~~Roaming~~ SEG CA, O=Operator M.

However, she can fabricate certificates of the following form:

- Subject: CN=SEG 1, O=Operator A;
- Signer: CN=~~Roaming~~ SEG CA, O=Operator M.

Using such certificates would allow full but illegitimate access to Operator B's network revealed for use by Operator A.

Now, there are the following possibilities to circumvent the problem:

1. checking also the Signer name when authenticating foreign operators, either by a) a proprietary "AllowedCertificateSigner" property or b) support for nameConstraints in the Bridge CA certificate issued to operator M;
2. establishing strong legal bindings and auditing that would discourage Operator M from such illegitimate fabrication of Operator A certificates.

The problem with solution 1.a is that such "AllowedCertificateSigner" is not commonly supported by current PKI end-entity products, being in conflict with requirement B.

The problem with solution 1.b is that such "nameConstraints" attribute in certificates is not commonly supported by current PKI CA or end-entity products, being in conflict with requirement B.

The problem with solution 2 is that first of all, an organization willing to run a Bridge CA has to be found before any pair of operators can exchange roaming traffic with NDS/AF mechanisms. Next, there shall be established paperwork and auditing procedures to make sure that the exploit described here can be detected. This is in conflict with requirement A. Also, the illegitimate act described could not be technically prevented beforehand.

If name constraints are used, every time a new roaming agreement is made, each operator shall update the certificate they issue for the Bridge, adding the new roaming partner's name into the certificate. From the point of view of one operator, the number of new certificate signing operations is the same whether a Bridge CA or a direct cross-certification model is in use.

***** End of Change ****

***** Begin of Change ****

B.4.4 Long certificate chains connected with IKE implementation issues

If Bridge CA is used, a ~~Roaming~~ SEG CA certificate has to be sent in the certificate payload in addition to the local end entity (SEG) certificate. This leads in Ethernet environments to the fragmentation of the IKE packet, which some current IKE implementations do not support. It is a problem in the implementation, not the protocol. Even in IPv6, the IKE UDP packets need to be fragmented, posing a potential interoperability problem. Clearly it is not a solution to use a different protocol, but instead the current implementations should be fixed. Still, taking into account requirement B, it is safer to avoid the problem altogether by not forcing the fragmentation of IKE packets by not using a Bridge CA.

***** End of Change ****

***** Begin of Change ****

B.5.3 Shortcomings

As discussed in the previous section, the Bridge CA approach saves memory or storage space in SEGs, because all the other operators ~~Roaming~~ SEG CA certificates do not need to be stored with other operators. Just the Bridge CA certificate would be stored, and other certificates retrieved during IKE negotiation.

***** End of Change ****