Source:	**Secretary SA WG3 (M. Pope, MCC)**
Title:	**Documents approved by e-mail after SA WG3 meeting #29**
Document for:	**Information**
Agenda Item:	**5.1**

The attached documents were subject to e-mail approval after the last SA WG3 meeting and are provided here for information.

S3-030473	Reply to LS N4-030722 (=S3-030337) on adapting Cx interface protocols for security purposes	SA WG3	Approved by e-mail by 28 July 2003
S3-030474	LS on 'Effects of service 27/38 on 2G/3G Interworking and emergency call'	SA WG3 (e-mail)	Approved by e-mail 13 August 2003
S3-030475	Reply to LS on the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes	SA WG3 (e-mail)	Approved by e-mail 14 August 2003
S3-030476	Reply to LS S2-03279 (=S3-030427) Address discovery using public DNS for WLAN interworking	SA WG3 (e-mail)	Approved by e-mail 14 August 2003
S3-030477	Reply to LS on DoS attacks against the 3GPP WLAN Interworking system	SA WG3 (e-mail)	Approved by e-mail 14 August 2003
S3-030478	CR to TS 33.102: IMEISV retrieval before completion of security mode setup procedure	SA WG3 (e-mail)	Approved by e-mail 5 September 2003
S3-030479	CR to 33.102: Mitigation against a man-in-the-middle attack associated with early UE handling	SA WG3 (e-mail)	Approved by e-mail 19 September 2003
S3-030380	Pseudo-CR to NDS/AF: Fetching cross-certificates	SA WG3 (e-mail)	e-mail approval. Approved 01/08/2003. Changes incorporated into new draft TS
S3-030381	Proposal for NDS/AF draft TS v0.4.0	SA WG3 (e-mail)	e-mail approval. Approved 01/08/2003. Changes incorporated into new draft TS
S3-030384 -> (S3-030xxx_NDSAF_backward compatibilityV2_email_comments.zip)	Pseudo-CR to ab.cde (NDS/AF): Addition of a Clause on backward compatibility to NDS/IP	SA WG3 (e-mail)	e-mail approval. Approved with revisions 01/08/2003. Changes incorporated into new draft TS
S3-030385	Pseudo-CR to NDF/AF: Addition of a Clause on CRL Management within the SEG	SA WG3 (e-mail)	e-mail approval. Approved 01/08/2003. Changes incorporated into new draft TS
S3-030386	Pseudo-CR to NDF/AF: Handling critical and non critical certificate extensions	SA WG3 (e-mail)	e-mail approval. Approved 01/08/2003. Changes incorporated into new draft TS
S3-030387	Pseudo-CR to NDF/AF: Additions to the clause 5.3 on profiling of certificates	SA WG3 (e-mail)	e-mail approval. Approved 01/08/2003. Changes incorporated into new draft TS
S3-030388	Pseudo-CR to NDF/AF: Addition of text on usecases	SA WG3 (e-mail)	e-mail approval. Approved 01/08/2003. Changes incorporated into new draft TS

3GPP TSG SA WG3 Security — S3#29 **S3-030473**
15 – 18 July 2003
San Francisco, USA

Title:	Reply to LS N4-030722 (=S3-030337) on adapting Cx interface protocols for security purposes
Work Items:	Support for subscriber certificates (SEC-SC), Security issues of Presence Capability (PRESNC), MBMS
Source:	3GPP SA3
To:	3GPP CN4
Cc:	-

Contact Person:
Name: Günther Horn
Tel. Number: +49 89 636 41494
E-mail Address: guenther.horn@siemens.com

Attachments: none

SA3 thanks CN4 for their LS. CN4 had the following actions on SA3:

CN4 asked SA3 to consider

a) the synchronisation problem of authentication vectors described in CN4's LS
b) security requirements of inter domain usage of Cx protocol,

and give guidance to CN4.

SA3 would like to respond to CN4's questions as follows:

a) SA3 is aware of the synchronisation problem of authentication vectors and has agreed to address the problem in the framework of a generic authentication architecture for Release 6. Work will be progressed on this issue at the SA3 ad hoc meeting in September. SA3 will keep CN4 informed of the progress of this work.
b) SA3 does not currently envisage an inter domain usage of the Cx protocol, or Cx-like protocols.

Action on CN4:
none

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Portugal
SA3#31	18 – 21 November 2003	London

3GPP TSG SA WG3 Security — S3#29 **S3-030474**
15 – 18 July 2003
San Francisco, USA

Title: **LS on 'Effects of service 27/38 on 2G/3G Interworking and emergency call'.**
Source: 3GPP SA3
To: 3GPP T3, CN1
Cc: **-**

Contact Person:
Name: Marc Blommaert
Tel. Number: +32 14 25 3411
E-mail Address: Marc.blommaert@siemens.com

Attachments: S3-030402, S3-030465

SA3#29 have approved S3-030465: 'Clarification on the usage of the c3 conversion function'. A part of the clarification now reads: 'An ME with a USIM that does not support GSM cipher key derivation (Feature 1) …. cannot operate in any GSM BSS ***with 64-bit key ciphering enabled***'. The input document S3-030402 to the same meeting detailed many scenarios where the outcome of a call setup or 2G/3G interworking was dependent on the activation of ciphering in the BSS.

SA3 found it useful to document these scenarios and thought that T3 specification TR31.900 would be the adequate place.

Actions:

To T3:
- To check if TR 31.900 is in accordance with the CR approved by S3 (S3-030465) and adapt if not.
- To consider the incorporation of the scenarios from S3-030402 section 2 into TR 31.900.

To CN1:
- To check the scenarios from S3-030402 section 2 on completeness and correctness.
- To check if TS 24.008 is in accordance with the CR approved by S3 (S3-030465) and adapt if not.

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Povoa de Varzim, Portugal
SA3#31	18 – 21 November 2003	London, UK

3GPP TSG SA WG3 Security — S3#29 **S3-030402**
15 - 18 July 2003
San Francisco, USA

Source: **Siemens**

Title: **Effects of service 27/38 on 2G/3G Interworking and emergency call**

Document for: **Discussion and decision**

Agenda Item: **7.5 and 7.6**

Abstract

This paper discusses the use of service 27 and 38 and the effects on 2G/3G Interworking and emergency calls.

1 Introduction and overview of specifications

TS 31.102 (T3) clause 4.2.8 defines

- Service 27 as 'GSM access' which resembles feature 1 of TS 33.102 (see later paragraph). The USIM only includes the Key Kc in a 3G authentication response if service 27 is available.
- Service 38 is called ‘GSM security context’. Feature 2 of TS 33.102 (See later paragraph) requires that both Service 27 and 38 be present on the USIM.

TR 31.900 (T3) clause 5.1 specifies

“To support a 2G/3G dual mode ME in a 2G radio access network, the USIM may provide functions for 2G backward compatibility. Two particular USIM services are defined for such purposes:

1. ***Service n° 27:*** *"GSM Access". This service is essential when a 2G BSS is involved. The USIM additionally generates the 2G ciphering key Kc required by the 2G air interface. From the security point of view, this behaviour can be characterised as "**3G + Kc mode**" (see below). Further, the USIM supports some additional 2G data storage elements that are necessary for 2G radio access.*
2. ***Service n° 38:*** *"GSM Security Context". This service is required when a 2G VLR/SGSN and/or a 2G HLR/AuC is involved. The USIM performs 2G AKA, i.e. it accepts 2G input data and generates 2G output data. From the security point of view, this behaviour can be characterised as "**virtual 2G mode**" (see below).*

   *A 2G VLR/SGSN never goes with a 3G BSS. Hence when a 2G VLR/SGSN is involved, then a 2G BSS is always part of the transmission chain and service n° 27 is additionally required**, i.e. services n° 27 and n° 38 have to be available at the same time.***

If services n° 27 and n° 38 are not supported by the USIM (which the ME can detect from the USIM Service Table during the USIM activation procedure) network access is impossible in a mixed 2G/3G environment, even if a SIM application is available on the UICC. A 3G ME only accesses the USIM application on the UICC.

From the security point of view, the compatibility services are connected to up to three different operation modes (see also Annex B):

- ***Normal 3G mode:*** *The results of the 3G algorithm are sent to the ME without any change. The USIM receives RAND and AUTN and responds with RES, CK and IK. This mode applies if service n° 27 is not available.*

- ***3G + Kc mode:*** *The 2G ciphering key Kc (derived from CK, IK) is additionally included in the response. The USIM receives RAND and AUTN and responds with RES, CK, IK and Kc. This requires conversion function c3 to be supported by the USIM. If service n° 27 is available in the USIM, this mode is always active and the ME picks the relevant values from the USIM response according to the present network situation.*

- ***Virtual 2G mode:*** *The USIM receives a 2G authentication request with RAND and returns a 2G authentication response with SRES (derived from RES) and ciphering key Kc (derived from CK, IK). This requires a particular algorithm execution mode plus conversion functions c2 and c3 to be supported by the USIM. If service n° 38 is available in the USIM, this mode is not always active. The ME may switch the USIM from normal 3G mode or 3G + Kc mode to virtual 2G mode by sending a particular command parameter according to the present network situation.*

The services n° 27 and n° 38 are both optional. Network operators can decide whether to include them into their USIMs and hence to allow network access with lower security level."

Section 6.8.1.5 of TS 33.102 defines optional USIM features to enable backwards compatibility with GSM.

"The USIM shall support UMTS AKA and may support backwards compatibility with the GSM system, which consists of:

Feature 1:	*GSM cipher key derivation (conversion function c3) to access GSM BSS attached to a R99+ VLR/SGSN using a dual-mode R99+ ME;*
Feature 2:	*GSM AKA to access the GSM BSS attached to a R98- VLR/SGSN or when using R99+ ME not capable of UMTS AKA or R98- ME;*
Feature 3:	*SIM-ME interface (GSM 11.11) to operate within R98- ME or R99+ ME not capable of UMTS AKA.*

A CR to TS 33.102 has been submitted to SA3#29 to correct the inaccuracy in clause 6.8.1.5 saying that GSM access can be forbidden by not implementing Service 27. This however does only apply if that service is not implemented in the ME and if ciphering is active in the BSS. TR 31.900 includes the same inaccuracy.

This contribution focuses on the consequences to 2G/3G interworking and emergency calls.

2 2G/3G interworking and emergency call scenarios

2.1 The effects of Service 27

A serving network does currently not know anything about USIM capabilities (i.e. on the lack of, or existence of any service implemented on the USIM). The dual mode mobile will indicate support of GSM and UMTS bands in the classmark irrespective of the presence of 'service 27'. The classmark does only indicate ME capabilities.

Suppose we take a dual mode mobile and insert a USIM within it that has 'service 27' not implemented.

Some of these scenarios also apply for a R99 single mode GSM capable mobile that supports the USIM interface.

Following scenarios may happen:

SCN-1. First a connection is setup via UMTS access, thereafter a handover is started. The handover will **fail** if GSM access ciphering is **activated** by the serving network because the USIM did not generate the key Kc. The network has no indication of the error reason. The network might repetitively try to handover the mobile, which may cause unnecessary signaling load in the network. It cannot be expected that a user knowing the capabilities of his USIM (i.e. the lack of GSM access) may be able to correlate this to the failed handover after having viewed the 'GSM network ciphering indicator' on his display.

SCN-2. The mobile tries to location update while being under GSM coverage. The connection will be **rejected** if GSM access ciphering is subsequently **activated** by the serving network because the USIM did not generate the key Kc. The network has no indication of the error reason. The network might repetitively try to activate ciphering, which may cause unnecessary signaling load in the network. It cannot be expected that a user knowing the capabilities of his USIM (i.e. the lack of GSM access) may be able to correlate this to the failed connection after having viewed the 'GSM network ciphering indicator' on his display.

SCN-3. First a connection is setup via UMTS access, thereafter a handover is started. The handover will **succeed** when GSM access ciphering is **NOT activated** by the serving network.

Now let's consider following scenarios for emergency calls:

SCN-4. An emergency call will succeed while being under GSM coverage when the USIM is NOT inserted. (if the serving network allows USIM-less calls).

SCN-5. An emergency call cannot be set up while being under GSM coverage with ciphering enabled when a USIM is inserted while the USIM did not generate the key Kc.

SCN-6. An emergency call can be set up while being under GSM coverage with ciphering disabled when a USIM is inserted.

Also SCN-1 to SCN-3 applies for Emergency calls;

As can be seen from these scenarios the absence of 'service 27' on the USIM which is inserted in a dual mode ME can have some unexpected effects to the call.

The expected behavior from service 27 (i.e. GSM only access) for a user having such a USIM is similar with that of a mobile indicating MS classmark 'UMTS only'. However if the MS classmark is set to "UMTS only" then a dual mode ME with such a USIM inserted could not make an emergency call anymore over GSM (now irrespective of whether ciphering is enabled or not).

It is therefore important to discuss this first from a service point of view with following list of question that need to be answered:

1) Should an ME with a USIM without service 27 be prevented from accessing GSM systems regardless of whether or not GSM ciphering is enabled?
2) Should an ME with a USIM without service 27 be prevented from handing over from UMTS to GSM regardless of whether or not GSM ciphering is enabled?
3) Should an ME with a USIM without service 27 be prevented from making GSM emergency calls?
4) Should an ME with a USIM without service 27 be prevented from handing over emergency calls from UMTS to GSM?

2.2 The effects of service 38

Suppose we take a dual mode mobile and insert a USIM within it, that has 'service 38' not implemented. Some of these scenarios also apply for a R99 single mode GSM capable mobile that supports the USIM interface.

Following scenarios may happen:

SCN-7. First a connection is setup via UMTS access, thereafter a handover is started. The handover may fail if a new 2G authentication is performed within the target serving network. This may be happen during or after handover. The network might repetitively try to authenticate the mobile, which may cause unnecessary signaling load in the network. It cannot be expected that a user knowing the capabilities of his USIM (i.e. the lack of GSM security context) may be able to correlate this to the failed handover or dropped call after having viewed the 'GSM network ciphering indicator' on his display.

SCN-8. The mobile tries to location update when a pre-R99 MSC/SGSN is involved. The connection will be rejected if 2G authentication is subsequently **activated** by the serving network because the USIM does not support 2G authentication. The network has no indication of the error reason. The network might repetitively try to authenticate the mobile during the location update, which may cause unnecessary signaling load in the network. It cannot be expected that a user knowing the capabilities of his USIM (i.e. the lack of GSM security context) may be able to correlate this to the failed connection after having viewed the 'GSM network ciphering indicator' on his display.

Now let's consider following scenarios for emergency calls:

SCN-9. An emergency call will succeed while being under GSM coverage when the USIM is NOT inserted. (if the serving network allows USIM-less calls).

SCN-10. An emergency call cannot be set up while being under GSM coverage if pre-R99 MSC/SGSN is involved. The network might repetitively try to authenticate the mobile, which may cause unnecessary signaling load in the network.

Also SCN-7 to SCN-8 apply for Emergency calls;

Similar scenarios can happen if using a GSM capable mobile with a USIM that has 'service 38' not implemented, but only 'service 27'.

Similar questions as with ‘service 27’ can be asked:

5) Should an ME with a USIM without service 38 be prevented from making GSM emergency calls?
6) Should an ME with a USIM without service 38 be prevented from handing over emergency calls from UMTS to GSM?

3 Proposal

Siemens proposes to ask CN1 if TS 24.008 does cover the above described scenarios. The mentioned CR to TS 33.102 should be attached to make them aware that the result of the call or handover might depend on the ciphering status of the GSM access network. This case was not covered in TS 33.102 so far.

As the behaviour in the described scenarios (SCN-x) are a consequence of an operators decision to use USIMs with service 27 NOT-implemented respectively service 38 NOT-implemented, there may be a need to document this behaviour in detail, in order to make operators aware of the consequences.

SA1 or GSMA could be informed about this in order to find a suitable place to document this. The TR 31.900 (T3) may be a suitable place to incorporate these issues.

3GPP TSG SA WG3 Security — S3#29 **S3-030465**
15 - 18 July 2003, San Francisco, USA

CR-Form-v7

CHANGE REQUEST

⌘ **33.102** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 5.2.0 ⌘

*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 ☐

Title:	⌘	Clarification on the usage of the c3 conversion function
Source:	⌘	Siemens, Nokia, T-Mobile
Work item code:	⌘	Security ***Date:*** ⌘ 08/07/2003
Category:	⌘	**F** ***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 support of the USIM Service n° 27: called "GSM Access" is optional. With this service the USIM generates the 2G ciphering key Kc required by the 2G air interface. The Kc is derived from the CK and IK with the conversion function c3. The c3 algorithm is described in section 6.8.1.2 of TS 33.102. The function c3 may only be performed in the network and the USIM. If an operator decides to issue USIMs without USIM Service n° 27 it is the intention of the operator that *64-bit 2G ciphering* shall not be possible. Thus c3 shall not be performed in the ME if the USIM Service n° 27 is not available. This essential mandatory requirement for the ME is not explicitly stated in TS 33.102. - Erroneous sentence on the lack of c3 function on the USIM, specifying that the ME cannot operate under any BSS. - The last sentence in 6.8.1.5 has been corrected.
Summary of change:	⌘	- It is clarified that the conversion function c3 shall not be performed in the ME. - It is clarified that with the lack of c3 function on the USIM, the ME cannot operate under BSS with *ciphering enabled.* - Split of the last sentence of 6.8.1.5 to correct the logic of the sentence.
Consequences if not approved:	⌘	Risk of erroneous ME implementations which are performing the c3 in the ME, completely bypassing the operator's intentions to forbid 64-bit 2G ciphering.

Clauses affected:	⌘	6.8.1.5			
Other specs affected:	⌘	**Y** / **N**	Other core specifications	⌘	TR 31.900
		X /	Other core specifications		
		/ **X**	Test specifications		
		/ **X**	O&M Specifications		
Other comments:	⌘				

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

6.8.1.5 USIM

The USIM shall support UMTS AKA and may support backwards compatibility with the GSM system, which consists of:

Feature 1: GSM cipher key derivation (conversion function c3) to access GSM BSS attached to a R99+ VLR/SGSN using a dual-mode R99+ ME;

Feature 2: GSM AKA to access the GSM BSS attached to a R98- VLR/SGSN or when using R99+ ME not capable of UMTS AKA or R98- ME;

Feature 3: SIM-ME interface (GSM 11.11) to operate within R98- ME or R99+ ME not capable of UMTS AKA.

When the ME provides the USIM with RAND and AUTN, UMTS AKA shall be executed. If the verification of AUTN is successful, the USIM shall respond with the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM shall store CK and IK as current security context data. If the USIM supports access to GSM cipher key derivation (feature 1), the USIM shall also derive the GSM cipher key Kc from the UMTS cipher/integrity keys CK and IK using conversion function c3 and send the derived Kc to the R99+ ME. In case the verification of AUTN is not successful, the USIM shall respond with an appropriate error indication to the R99+ ME.

When the ME provides the USIM with only RAND, and the USIM supports GSM AKA (Feature 2), GSM AKA shall be executed. The USIM first computes the UMTS user response RES and the UMTS cipher/integrity keys CK and IK. The USIM then derives the GSM user response SRES and the GSM cipher key Kc using the conversion functions c2 and c3. The USIM then stores the GSM cipher key Kc as the current security context and sends the GSM user response SRES and the GSM cipher key Kc to the ME.

In case the USIM does not support GSM cipher key derivation (Feature 1) or GSM AKA (Feature 2), the R99+ ME shall be informed. An ME with a~~A~~ USIM that does not support GSM cipher key derivation (Feature 1) shall not perform the GSM cipher key derivation (conversion function c3) in the ME and therefore cannot operate in any GSM BSS with 64-bit key ciphering enabled. An ME with a~~A~~ USIM that does not support GSM AKA (Feature 2) cannot operate under a R98- VLR/SGSN. ~~-~~A USIM that does not support GSM AKA (Feature 2) cannot work within ~~or in a both~~ a ~~R99+~~ ME that is not capable of UMTS AKA ~~-~~and cannot work within a~~in~~ R98- ME.

**** end of change ****

3GPP TSG SA WG3 Security — S3#29 **S3-030475**
15 - 18 July 2003
San Francisco, USA

Title: **Reply to LS on** the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes

Response to: **S2-032746 (S3-030433)**

Release: **Rel-6**

Source: **SA3**

To: **SA2**

CC: IREG, IREG Packet Group, GSMA WLAN Task Force, GSMA Security Group

Contact Person:

Name: Sébastien Nguyen Ngoc
Tel. Number: +33 145 29 47 31
E-mail Address: sebastien.nguyenngoc@francetelecom.com

Attachments: **None**

Overall Description:

SA3 thanks SA2 for their LS on the recommendation from IREG of non publicly routable IP addresses for the GPRS nodes.

SA3 believes that hiding the IP address of the PDG on GRX using NAT or other techniques would not be useful from a security point of view. There are potential threats on the PDG, and those should be addressed so that the PDG is secured against attacks. No issues were raised in SA3 with the suggestion in SA2's liaison that a PDG address on GRX could be made visible and accessible to specific authorised UEs.

However, SA3 does not envision that NAT is a useful mechanism to meet these threats. Furthermore, NAT would add additional complexity to the system and is known to introduce incompatibilities with common tunnelling protocols like IPSec. Therefore SA3 does not recommend the use of NAT on the IP address of the PDG.

Actions:

To SA2:

SA2 is kindly asked to take above conclusion into their architectural discussions.

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Povoa de Varzim, Portugal
SA3#31	18 – 21 November 2003	London, UK

3GPP TSG SA WG3 Security — S3#29 **S3-030476**
15 - 18 July 2003
San Francisco, USA

Title: Reply to LS S2-03279 (=S3-030427) Address discovery using public DNS for WLAN interworking

Work Items: WLAN Interworking

Source: 3GPP SA3
To: 3GPP SA2
Cc:

Contact Person:
Name: Colin Blanchard
Tel. Number: +44 1473 605353
E-mail Address: colin.blanchard@bt.com

Attachments: none

SA3 thanks SA2 for their LS on Address discovery using public DNS for WLAN interworking. SA2 had asked SA3 to answer the following questions

- Is allowing IP address of the WAG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

- Is allowing IP address of the PDG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking?

SA3 would like to respond as follows:

It was not clear to SA3 about what is meant by "public DNS" and in fact the following elements need to be considered separately:

1. **DNS Client**: The UE DNS Client's resolver will use a recursive name server for its queries. The Client can get the IP address for the recursive name server via static configuration or DHCP. The DHCP occurs after authentication to the WLAN and could be configured to provide the recursive name servers to use for WLAN/3G interworking. This would require the WLAN operator to configure the DHCP to support this.

2. **Recursive Name Servers:** The Recursive Name Server answers recursive queries from the UE's on the WLAN. It performs the necessary non-recursive queries to other name servers to get the correct Resource Records. The WLAN operator or 3G operator could operate the Recursive Name Servers. These DNS servers could probably be configured to answer queries for host names on the Internet and for

host names on the PLMN. These DNS servers would have to be secured of course. **SA3 have assumed that a "public" Recursive Name Server might be considered one that can resolve names on the Internet (i.e., uses Internet DNS for resolving names) and allows all authenticated WLAN clients to use it. The Recursive Name Server should be configured so that only users on the WLAN can query it (not accessible from the Internet) and should be controlled by the operators according to the roaming agreement.**

3. **Delegated Name Servers**: These DNS servers hold the Resource Records (e.g., A records) for the WAG and/or PDG. **SA3 have assumed that these will be managed and controlled by the operators of the WAG or PDG. SA3 weren't sure whether "public" DNS referred to name servers that are accessible to queries from the Internet or perhaps sit on the Internet DNS tree?** However, it is not clear to SA3 what DNS tree will the WAG & PDG names be placed in, Internet or an alternate. For example, would it use an ICANN-assigned TLD or a special TLD (e.g.,. gprs).

On the specific question asked by SA2 on "Is allowing IP address of the PDG/WAG to be discovered by UE using public DNS satisfactory according to 3GPP security requirements applicable to 3GPP WLAN interworking" SA3 would like to make the following comments:

1. If the Internet DNS is to be used, then the Recursive Name Servers have to have access to the Internet in order to query the root servers and TLD servers. It is not necessary that the Recursive Name Servers be reachable from the Internet other than to receive replies to its queries (e.g., it should not answer queries from the Internet). The Delegated Name Servers need to be reachable from the Recursive Name Servers, but it is not then necessary that they are reachable from the Internet

2. Addresses used in the GRX should not be re-used on the Internet. However, this possibility should be considered. The Delegated Name Servers should be sure to resolve to the correct PDG addresses.

3. If DNS servers are used for determining IP addresses of WAG or PDG for tunnel establishment purposes, SA3 does not see any issues in satisfying the 3GPP security requirements, as the security threats against the DNS servers can be mitigated using existing mechanisms, as is already is the case with many current DNS server deployments. It is also recognized that more can be done to secure the DNS, such as deployment of TSIG and/or relevant aspects of DNSSEC

4. As well as protecting the DNS servers themselves, the communication between the UE and the DNS server has to be secure from modification by an attacker e.g. through the use of 802.11 security on the air interface and network security between the AP and the DNS server.

Finally, it should be noted that as an alternative it might be possible to deliver the IP address of the PDG or WAG to the UE using EAP-AKA authentication instead of using DNS. However, it is recognised that it is far from trivial to pass additional information in EAP and at the moment, SA3 see no way to provide such information in EAP-SIM or EAP-AKA. If EAP-SIM/AKA were extended to carry the Home PDG address, then this would work in any environment in which EAP-SIM or EAP-AKA would work. It should be noted that this will not hide the IP address of the tunnel endpoint, it will only make its discovery inconvenient.

Conclusion

Based on the assumptions and mechanisms described above, SA3 believes the DNS could be used for discovery of either WAG or PDG addresses by the UE.

Action on SA2:

To comment on the assumptions highlighted in bold above

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp
SA3#30	6 – 10 October 2003	Porto
SA3#31	18 – 21 November 2003	London

3GPP TSG SA WG3 Security — S3#29 **S3-030477**
15 - 18 July 2003
San Francisco, USA

Title: **Reply to LS on DoS attacks against the 3GPP WLAN Interworking system**
Response to: **S2-032730 (S3-030428)**
Release: **Rel-6**

Source: **SA3**
To: **SA2**
CC : **-**

Contact Person:
Name: Anand Palanigounder
Tel. Number: +1-972-684-4772
E-mail Address: anand@nortelnetworks.com

Attachments: **None**

Overall Description:

SA3 thanks SA2 for their LS on Denial of Service attacks against the 3GPP WLAN Interworking system. SA3 reviewed the conclusions reached in the attached paper titled "Security analysis for tunnel establishment" (S2-032483) and concluded the following:

SA3 agrees with the conclusion reached in the document except that, in case there is no WAG in the VPLMN or traffic routed through it, PDGW will be the one being affected by the Denial of Service attack.

Two ways of facing the attack have been identified by SA3. Both have similar results, although different architectural implications SA2 can take into consideration:

- Firewall policies in the WAG will protect the attack in the boundaries of the GRX. In this case, suitable WAGs are needed, which are able to absorb the attack. This option has the advantage of stopping the attack in the boundaries of the backbone network, but it requires support in the VPLMN (the WAG). This option applies equally to the tunnel-switching and end-to-end tunneling approaches – in either case measures at the WAG are needed in order to block the DoS attack at the boundary of the GRX network.
- If the HPLMN does not want to rely on the fact that traffic from the WLAN AN to the PDGW is always routed through a WAG, or that the WAG performs some of the needed firewall functionality, then the PDGW may need firewall functionality (either in the same node or outside) to enforce the policies. In the same way, PDGWs which are able to absorb the attack will be required. This option has the advantage of not requiring any support in the VPLMN (for roaming cases). However, the attack has to be detected and absorbed in the PDGW of the HPLMN of the user.

SA3 also would like to point out that IP address spoofing is also possible with both end-to-end tunneling and switched tunneling approaches. In order to mitigate the DoS attacks due to address spoofing, once the attack is identified, cooperation in tracking down and terminating the attacks is needed from the operators involved (e.g., HPLMN, VPLMN, WLAN etc.). SA3 further notes that, once the DoS attack is identified, it may be easier to track down the attacker(s) at the WAG than at the PDGW. However, it is not necessarily any easier to identify such attacks on WAG as opposed to the attacks on the PDGW.

Actions:

To SA2:

SA2 is kindly asked to take above conclusions from SA3 in their architectural discussions.

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Povoa de Varzim, Portugal
SA3#31	18 – 21 November 2003	London, UK

3GPP TSG-SA3#29 **Tdoc ⌘S3-030478**

15th – 18th July, 2003 San Francisco, USA

CR-Form-v7

CHANGE REQUEST

⌘ **TS 33.102** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: **5.2.0** ⌘

*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 [X] Radio Access Network [ ] Core Network [X]

Title:	⌘	IMEISV retrieval before completion of security mode setup procedure
Source:	⌘	SA WG3
Work item code:	⌘	LATE_UE
Date:	⌘	27/08/2003
Category:	⌘	**F**
Release:	⌘	Rel-5

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 Serving Network needs to be able to retrieve the IMEISV before ciphering is started to be able to handle faulty ciphering behavior of not fully ciphering tested early UE's. TS 33.102 currently forbid the retrieval of IMEISV before completion of security mode set-up procedure. Such a restriction has not been implemented within Stage-3 specification (i.e. TS 24.008).
Summary of change:	⌘	Remove the restriction to retrieve IMEISV before security mode setup procedure has been completed.
Consequences if not approved:	⌘	The Serving Network will not be able to recognise and handle Early UE with faulty ciphering behavior when ciphering is activated.

Clauses affected:	⌘	6.4.5; 5.1.5

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

Other comments: ⌘

***** Start of change *****

5.1.5 Mobile equipment identification

~~In certain cases,~~The SN may request the MS to send it the ~~mobile equipment identity~~ IMEI or IMEISV of the terminal. ~~The mobile equipment identity shall only be sent after authentication of SN with exception of emergency calls.~~ The IMEI should be securely stored in the terminal. However, the presentation of this identity to the network is not a security feature and the transmission of the IMEI or IMEISV may~~is not~~ be unprotected. Although it is not a security feature, it should not be deleted from UMTS however, as it is useful for other purposes.

***** End of change *****

***** Start of change *****

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and VLR/SGSN. The four exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-VLR/SGSNsignalling after the initial L3 signalling message sent from MS to VLR/SGSN, i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-VLR/SGSN signalling after the initial L3 signalling message sent from MS to VLR/SGSN, and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.
- If the call is an emergency call teleservice as defined in TS 22.003, see section 6.4.9.2 below.

When the integrity protection shall be started, the only procedures between MS and VLR/SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to VLR/SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI, ~~and~~IMEI or IMEISV), and
- Authentication and key agreement.

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

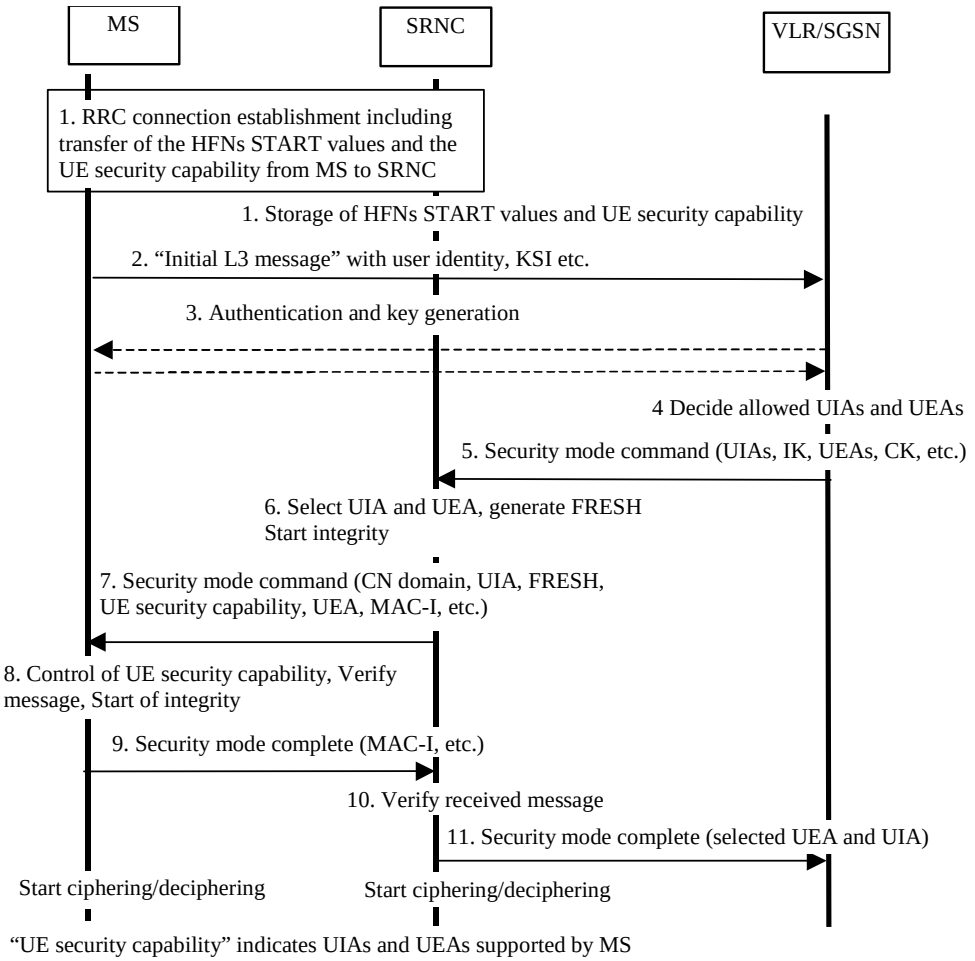

Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an unprotected message. Returning the "UE security capability" later on to the UE in a protected message will give UE the possibility to verify that it was the correct "UE security capability" that reached the network.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability optionally the GSM Classmarks 2 and 3 and the START values for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The START values and the UE security capability information are stored in the SRNC. If the GSM Clasmarks 2 and 3 are transmitted during the RRC Connection establishment, the RNC must store the GSM ciphering capability of the UE (see also message 7).

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the VLR/SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The VLR/SGSN determines which UIAs and UEAs that are allowed to be used in order of preference.

5. The VLR/SGSN initiates integrity and ciphering by sending the RANAP message Security Mode Command to SRNC. This message contains an ordered list of allowed UIAs in order of preference, and the IK to be used. If ciphering shall be started, it contains the ordered list of allowed UEAs in order of preference, and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the START value to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the START value already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the MS (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC sends a SECURITY MODE REJECT message to the requesting VLR/SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, optionally the GSM ciphering capability (if received during RRC Connection establishment), the UIA and FRESH to be used and if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the Security mode command message. Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security mode command message, the MS controls that the "UE security capability" received is equal to the "UE security capability" sent in the initial message. The same applies to the GSM ciphering capability if it was included in the RRC Connection Establishment. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the VLR/SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. this and all following downlink messages sent to the MS are integrity protected using the new integrity configuration. The Security mode complete from MS starts the uplink integrity protection, i.e. this and all following messages sent from the MS are integrity protected using the new integrity configuration. When ciphering shall be started, the Ciphering Activation time information that is exchanged between SRNC and MS during the Security mode set-up procedure sets the RLC Sequence Number/Connection Frame Number when to start ciphering in Downlink respective Uplink using the new ciphering configuration.

***** End of change *****

CR-Form-v7

CHANGE REQUEST

⌘ TS 33.102 CR 182 ⌘rev - ⌘ Current version: 5.2.0 ⌘

*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 ☒

Title:	⌘	Mitigation against a man-in-the-middle attack associated with early UE handling
Source:	⌘	SA WG3
Work item code:	⌘	LATE_UE
Date:	⌘	19/09/2003
Category:	⌘	C
Release:	⌘	Rel-5

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:	⌘	If an unprotected IMEISV is used to establish security without ciphering (i.e. with UEA0) for UEs which have faulty UEA1 implementations then a man-in-the-middle attack is possible. A mechanism to mitigate against this attack needs to be specified.
Summary of change:	⌘	Add a mechanism to mitigate against a man-in-the-middle attack associated with early UE handling.
Consequences if not approved:	⌘	A man-in-the-middle attacker would be able to disable ciphering for UEs which are capable of ciphering.

Clauses affected:	⌘	2, 6.4.5			
Other specs affected:	⌘	Y: Other core specifications	⌘	24.008, 25.413	
		N: Test specifications			
		N: O&M Specifications			
Other comments:	⌘				

***** Start of change *****

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document in the same Release as the present document.

[1] 3GPP TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Threats and Requirements".

[2] 3GPP TS 33.120: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Principles and Objectives".

[3] 3GPP TR 21.905: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications (Release 1999)".

[4] 3GPP TS 23.121: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Architecture Requirements for Release 99".

[5] 3GPP TS 31.101: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[6] 3GPP TS 22.022: "3rd Generation Partnership Project (3GPP); Technical Specification Group Services and System Aspects; Personalisation of UMTS Mobile Equipment (ME); Mobile functionality specification".

[7] 3GPP TS 23.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM application toolkit; Stage 2".

[8] ETSI GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[9] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service description; Stage 2".

[10] ISO/IEC 9798-4: "Information technology - Security techniques - Entity authentication - Part 4: Mechanisms using a cryptographic check function".

[11] 3GPP TS 35.201: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications".

[12] 3GPP TS 35.202: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification".

[13] 3GPP TS 35.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementers' test data".

[14] 3GPP TS 35.204: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data".

[15] 3GPP TS 31.111: "3rd Generation Partnership Project; Technical Specification Group Terminals; USIM Application Toolkit (USAT)".

[16] 3GPP TS 22.048: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Security Mechanisms for the (U)SIM Application Toolkit; Stage 1".

[17] 3GPP TS 25.331: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RRC Protocol Specification".

[18] 3GPP TS 25.321: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; MAC protocol specification".

[19] 3GPP TS 25.322: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; RLC Protocol Specification".

[20] 3GPP TS 31.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group Terminals; Characteristics of the USIM Application".

[21] 3GPP TS 22.101: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service aspects; Service principles".

[22] 3GPP TS 23.195 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Provision of User Equipment Specific Behaviour Information (UESBI) to network entities".

***** End of change *****

***** Start of change *****

6.4.5 Security mode set-up procedure

This section describes one common procedure for both ciphering and integrity protection set-up. It is mandatory to start integrity protection of signalling messages by use of this procedure at each new signalling connection establishment between MS and VLR/SGSN. The four exceptions when it is not mandatory to start integrity protection are:

- If the only purpose with the signalling connection establishment and the only result is periodic location registration, i.e. no change of any registration information.
- If there is no MS-VLR/SGSNsignalling after the initial L3 signalling message sent from MS to VLR/SGSN, i.e. in the case of deactivation indication sent from the MS followed by connection release.
- If the only MS-VLR/SGSN signalling after the initial L3 signalling message sent from MS to VLR/SGSN, and possible user identity request and authentication (see below), is a reject signalling message followed by a connection release.
- If the call is an emergency call teleservice as defined in TS 22.003, see section 6.4.9.2 below.

When the integrity protection shall be started, the only procedures between MS and VLR/SGSN that are allowed after the initial connection request (i.e. the initial Layer 3 message sent to VLR/SGSN) and before the security mode set-up procedure are the following:

- Identification by a permanent identity (i.e. request for IMSI), and
- Authentication and key agreement.

The message sequence flow below describes the information transfer at initial connection establishment, possible authentication and start of integrity protection and possible ciphering.

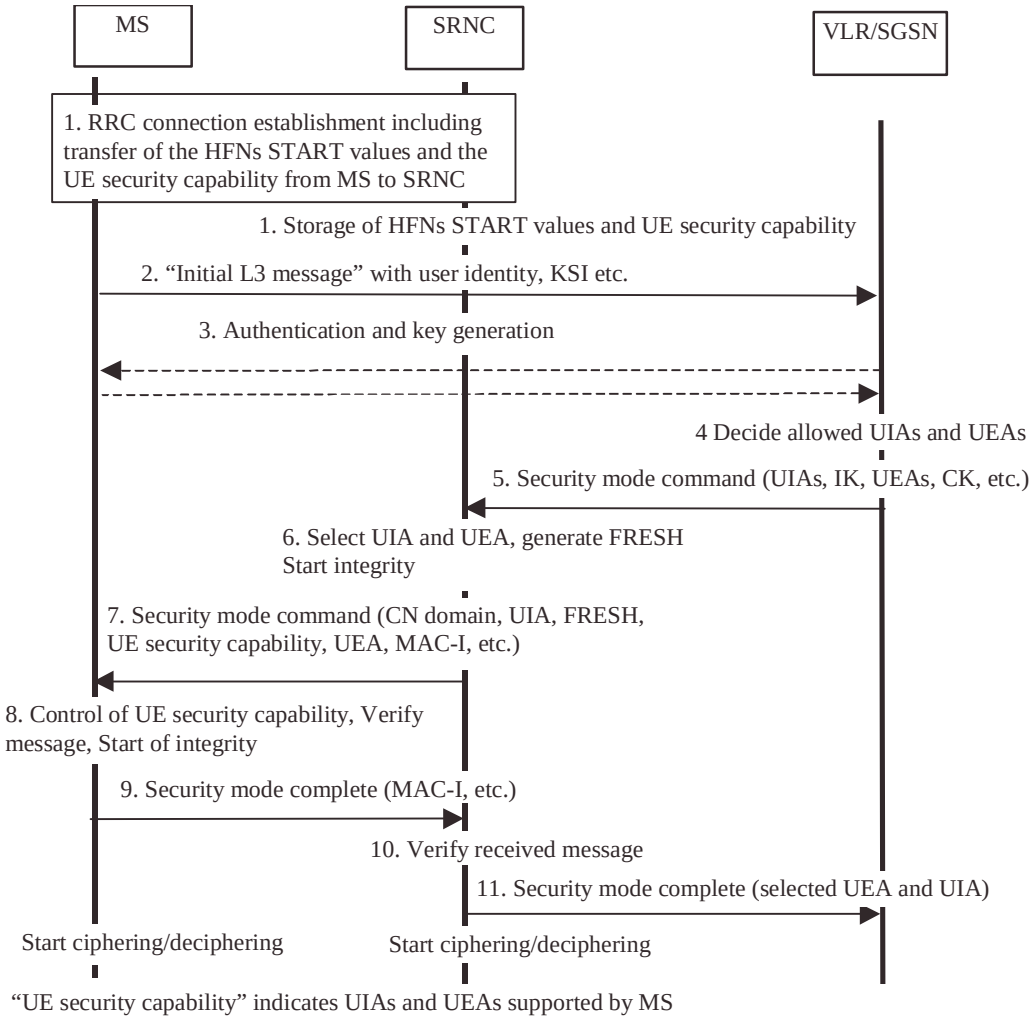

Figure 14: Local authentication and connection set-up

NOTE 1: The network must have the "UE security capability" information before the integrity protection can start, i.e. the "UE security capability" must be sent to the network in an unprotected message. Returning the "UE security capability" later on to the UE in a protected message will give UE the possibility to verify that it was the correct "UE security capability" that reached the network.

Detailed description of the flow above:

1. RRC connection establishment includes the transfer from MS to RNC of the ME security capability optionally the GSM Classmarks 2 and 3 and the START values for the CS service domain respective the PS service domain. The UE security capability information includes the ciphering capabilities (UEAs) and the integrity capabilities (UIAs) of the MS. The START values and the UE security capability information are stored in the SRNC. If the GSM Clasmarks 2 and 3 are transmitted during the RRC Connection establishment, the RNC must store the GSM ciphering capability of the UE (see also message 7).

2. The MS sends the Initial L3 message (Location update request, CM service request, Routing area update request, attach request, paging response etc.) to the VLR/SGSN. This message contains e.g. the user identity and the KSI. The included KSI (Key Set Identifier) is the KSI allocated by the CS service domain or PS service domain at the last authentication for this CN domain.

3. User identity request may be performed (see 6.2). Authentication of the user and generation of new security keys (IK and CK) may be performed (see 6.3.3). A new KSI will then also be allocated.

4. The VLR/SGSN determines which UIAs and UEAs that are allowed to be used in order of preference.

5. The VLR/SGSN initiates integrity and ciphering by sending the RANAP message Security Mode Command to SRNC. This message contains an ordered list of allowed UIAs in order of preference, and the IK to be used. If ciphering shall be started, it contains the ordered list of allowed UEAs in order of preference, and the CK to be used. If a new authentication and security key generation has been performed (see 3 above), this shall be indicated in the message sent to the SRNC. The indication of new generated keys implies that the START value to be used shall be reset (i.e. set to zero) at start use of the new keys. Otherwise, it is the START value already available in the SRNC that shall be used (see 1. above).

6. The SRNC decides which algorithms to use by selecting the highest preference algorithm from the list of allowed algorithms that matches any of the algorithms supported by the MS (see 6.4.2). The SRNC generates a random value FRESH and initiates the downlink integrity protection. If the requirements received in the Security mode command can not be fulfilled, the SRNC sends a SECURITY MODE REJECT message to the requesting VLR/SGSN. The further actions are described in 6.4.2.

7. The SRNC generates the RRC message Security mode command. The message includes the ME security capability, optionally the GSM ciphering capability (if received during RRC Connection establishment), the UIA and FRESH to be used and if ciphering shall be started also the UEA to be used. Additional information (start of ciphering) may also be included. Because of that the MS can have two ciphering and integrity key sets, the network must indicate which key set to use. This is obtained by including a CN type indicator information in the Security mode command message. Before sending this message to the MS, the SRNC generates the MAC-I (Message Authentication Code for Integrity) and attaches this information to the message.

8. At reception of the Security mode command message, the MS controls that the "UE security capability" received is equal to the "UE security capability" sent in the initial message. The same applies to the GSM ciphering capability if it was included in the RRC Connection Establishment. The MS computes XMAC-I on the message received by using the indicated UIA, the stored COUNT-I and the received FRESH parameter. The MS verifies the integrity of the message by comparing the received MAC-I with the generated XMAC-I.

9. If all controls are successful, the MS compiles the RRC message Security mode complete and generates the MAC-I for this message. If any control is not successful, the procedure ends in the MS.

10. At reception of the response message, the SRNC computes the XMAC-I on the message. The SRNC verifies the data integrity of the message by comparing the received MAC-I with the generated XMAC-I.

11. The transfer of the RANAP message Security Mode Complete response, including the selected algorithms, from SRNC to the VLR/SGSN ends the procedure.

The Security mode command to MS starts the downlink integrity protection, i.e. this and all following downlink messages sent to the MS are integrity protected using the new integrity configuration. The Security mode complete from MS starts the uplink integrity protection, i.e. this and all following messages sent from the MS are integrity protected using the new integrity configuration. When ciphering shall be started, the Ciphering Activation time information that is exchanged between SRNC and MS during the Security mode set-up procedure sets the RLC Sequence Number/Connection Frame Number when to start ciphering in Downlink respective Uplink using the new ciphering configuration.

Mechanisms are defined to allow networks to overcome early UE implementation faults [22]. A potential early UE implementation fault could be a faulty UEA1 implementation. To allow networks to handle early UEs which have faulty UEA1 implementations, the SGSN/VLR may configure the security mode command based on the UE's IMEISV so that certain UEs which claim to support UEA1 shall have security established without ciphering (i.e. with UEA0), while other UEs which claim to support UEA1 shall have security established with ciphering (i.e. with UEA1). This procedure shall involve the SGSN/VLR retrieving the IMEISV from the UE before the security mode set-up procedure has started.

If the above procedure to handle UEs which have faulty UEA1 implementations is implemented and the security mode set-up procedure results in security being established without ciphering (i.e. with UEA0) then the SGSN/VLR shall request the IMEISV from the UE for a second time immediately after the security mode set-up procedure has been completed. This second IMEISV request is integrity protected. If the IMEISV request is not successful, or if the second IMEISV received is different from the IMEISV received before the security mode set-up procedure was started then the connection shall be released.

***** End of change *****

3GPP TSG SA WG3 Security — S3#29 **S3-030380**
15 - 18 July 2003, San Francisco, USA

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 0.3.0 ⌘

*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 ☒

Title:	⌘	Fetching cross-certificates
Source:	⌘	Nokia, Siemens, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	08/07/2003
Category:	⌘	
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:	⌘	Implementing the proposal for working assumption (i.e. cross-certificates are stored into CRs, fetched with LDAP and cached in SEGs) in 'Fetching cross-certificates' discussion paper
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.2.1, 6.1, 6.3 (new), 6.4 (new), 6.5 (new), Annex X (new)

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

Other comments: ⌘

---------- FIRST CHANGED SECTION ----------

5.2 Use cases

5.2.1 Roaming agreement

Security gateways (SEG's) of two different security domains need to establish a secure tunnel, when the operators make a roaming agreement. The first technical step in creating the roaming agreement between domains is the cross-certification of the 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 CAs create a PKCS#10 certificate request, and send it to the other operator. 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 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 local Certificate Repository (CR) which all SEGs that need to communicate with the other domain shall access with LDAP.

---------- NEXT CHANGED SECTION ----------

6.1 Repositories

During VPN tunnel establishment, each SEG has to verify the validity of it's 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 CA_A is still valid

b) the certificate of SEG_A is still valid

SEG_A performs according checks from its own perspective.

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

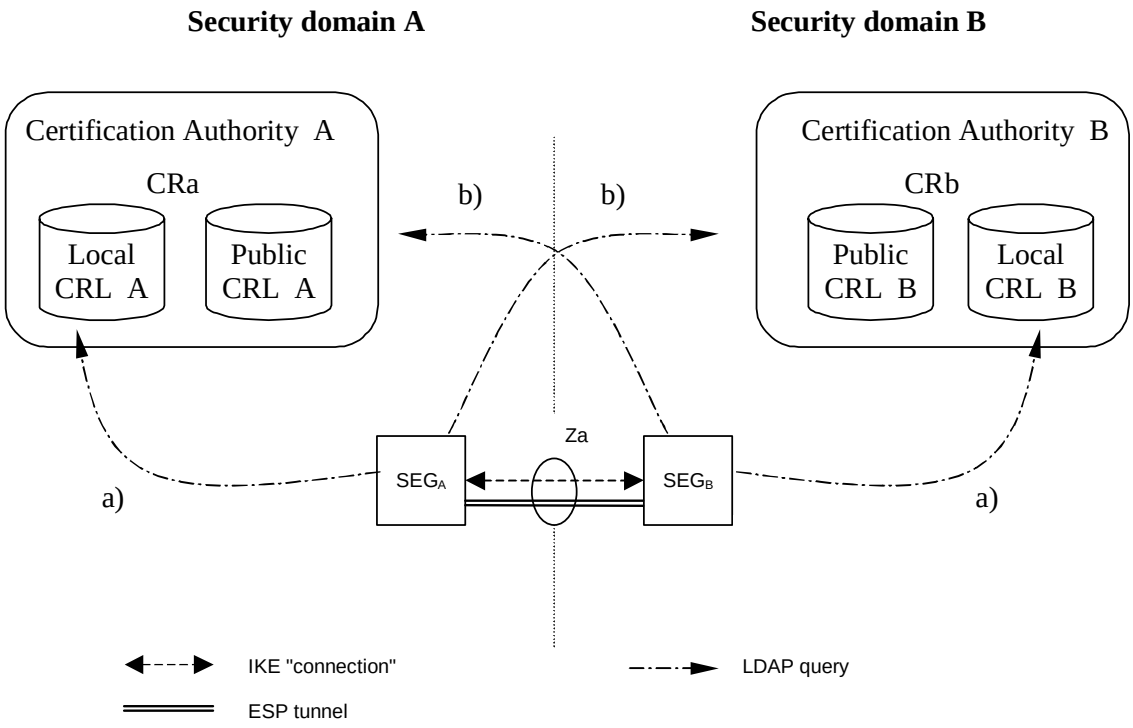

Figure 4: CRL Repositories

The public and local CRL repositories of a CA may be implemented as two 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.

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

[Editor's note: Further specification of public CRL interface and its relation to Za is ffs.]

---------- NEXT ADDED SECTIONS ----------

6.3 Cross-certification

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

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

6.4 Revoking a cross-certificate

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

1. The cross-certificate is added into the CRL.
2. The cross-certificate is removed from the CR.

6.5 Authentication during the IKE phase 1

Authentication during the IKE Phase 1 is shown in the Figure 4 above. The SEGa uses the following procedure to authenticate the 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 fetches a CRL from the (public) CRb if the locally cached CRL has not yet expired.
4. SEGa uses this CRL to verify the status of SEGb's certificate
5. SEGa uses either the locally cached cross-certificate or fetches the cross-certificate from the (local) CRa
6. SEGa fetches a CRL from the (local) CRa if the locally cached CRL has not yet expired.
7. SEGa uses this CRL to verify the status of the cross-certificate
8. SEGa verifies the status of roaming CAa certificate if roaming CAa is not a top-level CA otherwise roaming CAa is implicitly trusted.
9. SEGa authenticates the SEGb (verifies signatures)

---------- LAST ADDED SECTION ----------

Annex X <informative>:
Decision for storing the cross-certificates in CR

In order to document the decision for storing the cross-certificates in Certificate Repository, fetching those with LDAP and caching them in SEGs, this section summarises technical advantages and disadvantages of the three alternatives.

The following table summarizes differences between alternatives:

Issue	**A) Cross-certificates are stored into SEGs:**	**B) Cross-certificates are stored into CRs:**	**C) Cross-certificates are stored into CRs and cached in SEGs upon usage:**
1) Initialization issues: storing the cross-certificate during the cross-certification	The cross-certificate is *initially* stored in several places, that is, into *all* SEGs (estimated number is between 2 and 10). Pros: - Cons: Certificate must be initially copied in several places. SEGs from different manufacturers may have other O&M interfaces to handle the certificates.	The cross-certificate is *initially* stored in CR. Pros: The handling is fully standardized. Certificate is initially copied in one place only. The operator should have the repository anyway (due to CRL handling). Cons: -	The cross-certificate is *initially* stored in CR. Pros and cons as in B).
2) Usage issues: latency during the IKE Phase 1	Pros: No extra latency Cons: -	Pros: - Cons: More latency caused by extra LDAP query (the cross-certificate is queried)	Pros & cons: as in B) at the first time, and as in A) at subsequent times
3) Cleanup issues: removing the cross-certificate NOTE: this functionality is needed only to be able to revoke cross-certificates before the next CRL gets published.	Pros: - Cons: The cross-certificate has to be removed from several places, that is, from *all* SEGs	Pros: The cross-certificate has to be removed from one single place only Cons: -	Pros: - Cons: The cross-certificate has to be removed from *both* CR *and* each SEG.
4) Security issues	Pros: No single point of failure exists. Cons: -	Pros: - Cons: CR represents a single point of failure suitable for an attacker,	Pros: Single point of failure partly mitigated Cons: -

		e.g. to submit a denial of service attack by breaking the communication at the CR.	

Analysis:

- Alternative B) requires one additional LDAP query in every IKE Phase 1 negotiation and will introduce new error cases
- Latency of LDAP: information from LDAP to local disk is cached and populating it takes some time, but in practice this time is not significant.
- The benefit of alternative B) and C) compared to alternative A) is easier management, that is, storing and removing the certificate in/from one single place only.

Conclusion: alternative C) is the most feasible choice, because it combines good points of alternatives A) and B).

3GPP TSG SA WG3 Security — S3#29 **S3-030381**

15 – 18 July 2003

San Francisco, USA

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

Title: **Proposal for NDS/AF draft TS v0.4.0**

Document for: **Discussion and decision**

Agenda Item: **7.4**

The attached proposal for new NDS/AF draft TS version 0.4.0 includes the following mainly editorial level changes agreed by the supporting companies. It is also noted that the NDS/AF draft TS has been assigned a specification number, 33.310.

- ch 4: added a reference to concise vendor neutral introduction to the PKI technology
    - changed title numbering
- ch 5: changed heading name to correspond the content
- ch 5.2.1 and 6.2: added clarification on PKCS#10 versus CMPv2 usage as requested by SA3#28
    - ch 5.2.1: deleted cross-certificate validity time example (15 years) as 3GPP does not have to give such estimations
        - deleted start time of validity as certificates are distributed in UTC
- ch 5.3 Profiling: moved to a new chapter 6 for clarity
- ch 5.3.4 Services utilising inter-domain PKI: chapter deleted as this is not a matter of NDS/AF specification
- ch 6 and 7: combined to a new chapter 6 “Detailed description of architecture and mechanisms”
- Annex A: editorial corrections

3GPP TSG SA WG3 Security — S3#29 **S3-030xxx**

15 – 18 July 2003, San Francisco, USA

3GPP TS 33.310~~ab.cde~~ V0.4~~3~~.0 (2003-07~~5~~)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Service and System Aspects;
Network Domain Security;
Authentication Framework
(Release x)

The present document has been developed within the 3rd Generation Partnership Project (3GPP ™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organizational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organizational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP ™ system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords
<keyword[, keyword]>

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

© 2002, 3GPP Organizational Partners (ARIB, CWTS, ETSI, T1, TTA, TTC).
All rights reserved.

Contents

Foreword 5

Introduction 5

1 Scope 6

2 References 6

3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7

4 Introduction to Public Key Infrastructure (PKI) 7
4.1 Cross-certification 8
4.1.1 Manual Cross-certification 8
4.1.2 Cross-certification with a Bridge CA 8

5 Use cases and profiling of the NDS/AF 8
5.1 PKI architecture for NDS/AF 8
5.1.1 General architecture 9
5.2 Use cases 10
5.2.1 Roaming agreement 10
5.2.2 VPN tunnel establishment 11
5.2.3 Operator deregistration 11
5.2.4 SEG deregistration 11
5.3 Profiling 12
5.3.1 Certificate profiles 12
5.3.1.1 Common rules to all certificates 12
5.3.1.2 CA Certificate profile 12
5.3.1.3 SEG Certificate profile 12
5.3.1.4 Cross Certificate profile 13
5.3.2 IKE negotiation and profiling 13
5.3.2.1 IKE Phase-1 profiling 13
5.3.2.2 Potential interoperability issues 14
5.3.3 Path validation 14
5.3.3.1 Path validation profiling 14
5.3.4 Services utilising inter-domain PKI 14

6 Security features 14
6.1 Repositories 14
6.2 Life cycle management 15

7 Security mechanisms 15
7.1 Authentication 16

8 Evolution path 16
8.1 Backward compatibility 16

A.1 Introduction 17

A.2 Requirements for trust model in NDS/AF 17

A.3 Cross-certification approaches 18
A.3.1 Manual Cross-certification 18
A.3.2 Cross-certification with a Bridge CA 18

A.4 Issues with the Bridge CA approach 18
A.4.1 Need for nameConstraint support in certificates or strong legal bindings and auditing 18
A.4.2 Preventing name collisions 19
A.4.3 Two redundant steps required for establishing trust 19
A.4.4 Long certificate chains connected with IKE implementation issues 20
A.4.5 Lack of existing relevant Bridge CA experiences 20

A.5 Feasibility of the direct cross certification approach 20
A.5.1 Benefits of direct cross certification 20
A.5.2 Memory and processing power requirements 21
A.5.3 Shortcomings 21
A.5.4 Possible evolution path to a Bridge CA 21

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

For 3GPP systems there is a need for truly scalable entity Authentication Framework (AF) since an increasing number of network elements and interfaces are covered by security mechanisms.

This specification provides a highly scalable entity authentication framework for 3GPP network nodes. This framework is developed in the context of the Network Domain Security work item, 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*.

Feasible trust models (i.e. how CA's are organized) and their effects are provided. Additionally, requirements are presented for the used protocols and certificate profiles, to make it possible for operator IPsec and PKI implementations to interoperate.

1 Scope

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

It means that this Specification concentrates 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 [1] 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.

NOTE: In case two SEG's interconnect separate network regions under a single administrative authority (e.g. owned by the same mobile operator) then the Za-interface is not subject to roaming agreements, but the decision on applying Za-interface is left to operators.

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

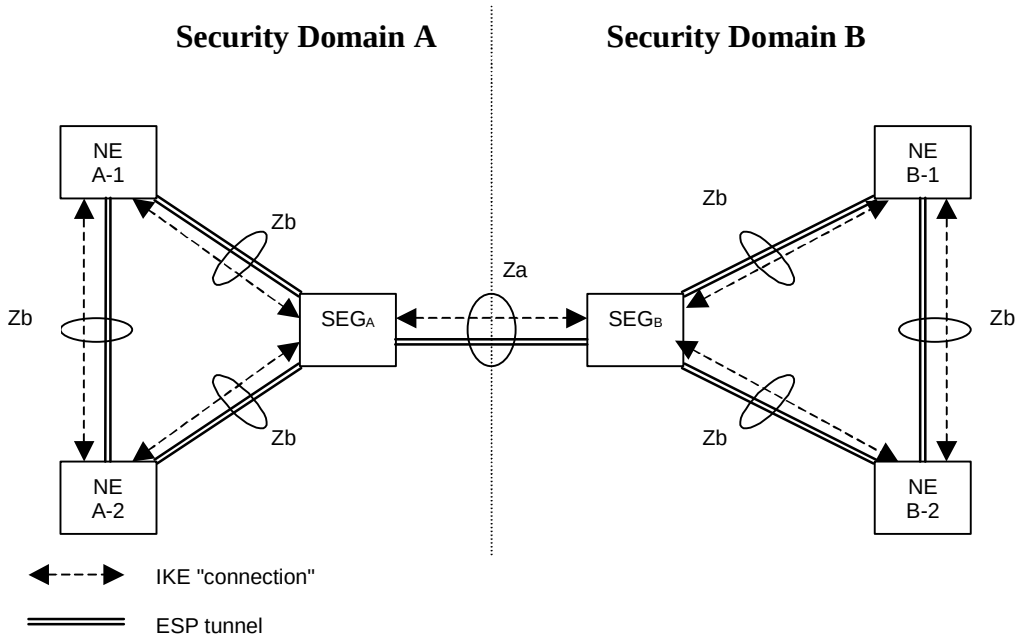

Figure 1: NDS architecture for IP-based protocols [1]

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 33.210: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Network domain security; IP network layer security".

[2] IETF RFC 2986: “PKCS#10 Certification Request Syntax Specification Version 1.7”

[3] IETF RFC 3280: “Internet X.509 Public Key Infrastructure Certificate and CRL Profile ”

[4] IETF Draft draft-ietf-pkix-rfc2510bis-08.txt: “Internet X.509 Public Key Infrastructure Certificate Management Protocol”

[5] IETF RFC 2252: “Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions”

[6] IETF RFC 1981: “Path MTU Discovery for IP version 6”

[7] PKI basics – A Technical Perspective, November 2002, http://www.pkiforum.org/pdfs/PKI_Basics-A_technical_perspective.pdf

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

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

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

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AF	Authentication Framework
CA	Certification Authority
NDS	Network Domain Security
SEG	Security Gateway
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

4 Introduction to Public Key Infrastructure (PKI)

~~*[Editor’s note: Serves as an introduction to PKI architecture and terminology. This should be kept relatively brief. Introduction of a certificate, certification authority, hierarchies, etc. Benefits of PKI: less secrets to be managed, n compared to n^2. Adding a new network element does not need configuration in other network elements. References: RFC 2459/3280]*~~ PKI Forum’s “PKI basics – A Technical Perspective” [7] provides a concise vendor neutral introduction to the PKI technology. Thus only two different cross-certification aspects are described in this introduction section.

~~4.1Cross-certification~~

Cross-certification is a process that establishes a trust relationship between two authorities. When an authority A is cross-certified with authority B, the authority A has chosen to trust certificates issued by the authority B. Cross-certification process enables the users under both authorities to trust the other authority's certificates. Trust in this context equals to being able to authenticate.

~~4.1.1~~4.1 Manual Cross-certification

Mutual cross certifications are done directly between the authorities and this approach is often called manual cross-certification. In this approach the authority does the decisions about the trust locally. When an authority A chooses to trust an authority B, the authority A signs the certificate of the authority B and distributes the new certificate (B's certificate signed by A) locally.

The down side of this approach is that it often results into scenarios where there needs to be lot of certificates available for the entities doing the trust decisions: There needs to be a certificate signed by the local authority for each security domain the local authority wishes to trust.

However, all the certificates can be configured locally and are locally signed, so the management of them is often flexible.

~~4.1.2~~4.2 Cross-certification with a Bridge CA

The Bridge CA is a concept that reduces the amount of certificates that needs to be configured for the entity that does the certificate checking. The name "bridge" is descriptive; when two authorities are mutually cross-certified with the bridge, the authorities do not need to know about each other. Authorities can still trust each other because the trust in this model is transitive (A trusts bridge, bridge trusts B, thus A trusts B and vice versa). The Bridge CA acts like a bridge between the authorities. However, the two authorities shall also trust that the bridge does the right thing for them. All the decisions about the trust can be offloaded to the bridge, which is desirable in some use cases. If the bridge decides to cross certificate with an authority M, the previously cross-certified authorities start to trust the M automatically.

The bridge-CA style cross-certifications are useful in scenarios where all entities share a common authority that everybody believes to work correctly for them. If an authority needs to restrict the trust or access control derived from the bridge-CA, it additionally needs to implement those restrictions.

5 Architecture and use cases~~Use cases and profiling~~ of the NDS/AF

[Editor's note: This section shall list the security requirements emerging from identified use cases.]

The roaming CA certificate of the owning operator shall be stored securely in the SEG. It defines who is the authority that the device trusts when connecting to the other devices. It is assumed that each operator domain could include 2 to 10 SEGs.

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

5.1 PKI architecture for NDS/AF

This chapter defines the PKI architecture for the NDS/AF. The goal is to define a flexible, yet simple architecture, which is easily interoperable with other implementations.

The architecture described below uses a simple access control method, i.e. every element which is authenticated is also provided service. More fine-grained access control may be implemented, but it is out of scope of this specification.

The architecture does not rely on bridge CAs, but instead uses direct cross certifications between the security domains. This enables easy policy configurations in the SEGs.

5.1.1 General architecture

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

The roaming CA of the domain issues certificates to the SEG's in the domain. This specification describes the profile for the roaming CA and a profile for SEG. Also a method for creating the cross-certificates is described.

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

The roaming CA shall issue certificates for SEG's in 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 CAs issued for the SEGs. When a roaming agreement is established between the domains, roaming CAs cross-certify with each other. The created cross-certificates need only to be configured locally to each domain. The cross-certificate, which roaming CA of security domain A created for security domain B shall be available for the domain A SEG which provides Za interface towards domain B. Equally the corresponding certificate, which the roaming CA of the security domain B created for security domain A shall be available for the domain B SEG which provides Za interface towards domain A.

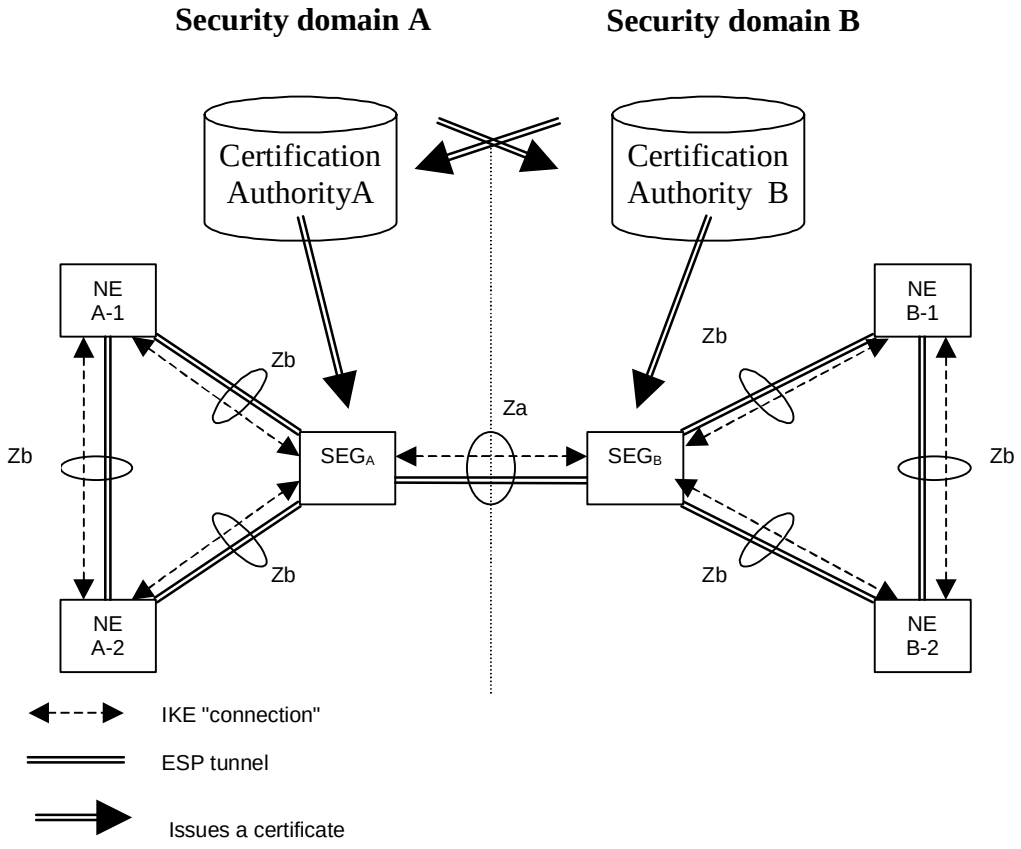

Figure 2: Trust validation path in context of NDS/IP

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

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

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

5.2 Use cases

5.2.1 Roaming agreement

Security gateways (SEG's) of two different security domains need to establish a secure tunnel, when the operators make a roaming agreement. The first technical step in creating the roaming agreement between domains is the cross-certification of the 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 CAs create a PKCS#10 certificate request, and send it to the other operator. 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 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 all SEGs that need to communicate with the other domain. 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.]

When creating the new cross-certificate, the 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. ~~The validity time could be e.g. 15 years. The start time of the validity should start e.g. a day before the actual roaming is set to start in order to avoid problems with different time zones. Problems in PKI are often due to the time differences.~~

When the new certificate is available for SEG, all that needs to be configured in SEG is the DNS name of the peering SEG gateway. The authentication can be done based on 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 roaming CA for the SEGs together with the cross certificate issued for the peering domains. The certificates of the peer domains are located under the cross-certificates of the peer domains.

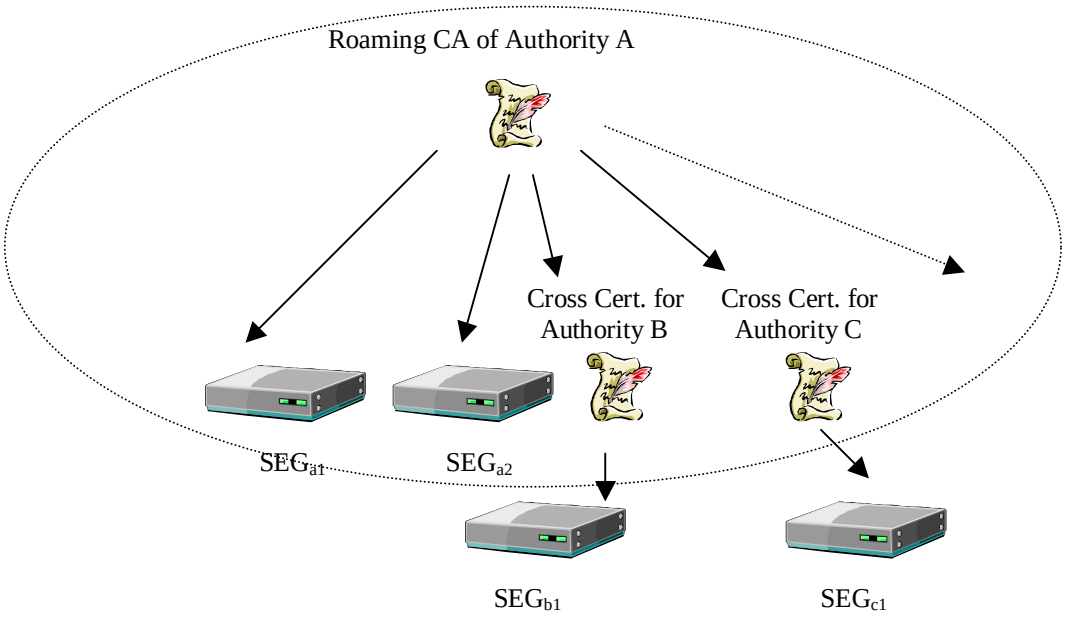

Figure 3: Security domain A illustrated. The PKI is hierarchical inside the domain.

5.2.2 VPN tunnel establishment

After establishing a roaming agreement and finishing 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 is specified. Only local roaming CA is configured as the trusted CA. Because of the cross-certification, any operator whose roaming CA has been cross-certified, can get access using this VPN connection configuration. If access to a certain local subnet is allowed for only certain operators, the VPN connection configuration shall include limitations for certificate issuer name.

[Editor's note: These limitations for certificate issuer name are ffs.]

Following is the flow of connection negotiation from the point of view of Operator A's SEG (initiator). Operator B 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 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 B CRL databases. IKE Phase-1 SA is established, and the Phase-2 SA negotiation proceeds as described with 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

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

5.2.4 SEG deregistration

If a SEG is removed from the network, the SAs shall be removed as above. The operator of the SEG shall have the certificate of the SEG listed in his CRL.

[Editor's note:

Two new paragraphs needed to describe the involved actions for revocation and check our model !?

Roaming CA certificate revocation ?

A) of the own roaming CA

B) of a partner roaming CA

SEG revocation

A) own SEG

B) SEG of a roaming partner]

~~5.3~~6 Profiling

[Editor's note: "Motivation" statements marked with italic in chapters 5.3.1 and 5.3.2 are included in the drafting stage of the TS, but will be removed before submission for approval to TSG SA.]

~~5.3.1~~6.1 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~~6.1.1 Common rules to all certificates

- Version 3 certificate

  Motivation: This is the current state of the art [3].

- Hash algorithm for use before signing certificate: 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 in 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 [5] retrieval shall be supported as the primary method of certificate revocation verification.

~~5.3.1.2~~6.1.2 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~~6.1.3 SEG Certificate profile

In addition to clause 5.3.1.1, 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~~6.1.4 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~~6.2 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~~6.2.1 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 [1] 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~~6.2.2 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 IPv6 – [6]), 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~~6.3 Path validation

~~5.3.3.1~~6.3.1 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.

~~5.3.4Services utilising inter-domain PKI~~

~~*[Editor's note: Subscriber certificates are feasible to implement without Authentication Framework (AF), but AF could help as inter-domain PKI provides the validation path for certificate usage.]*~~

~~6~~7 Detailed description of architecture and mechanisms~~Security features~~

[Editor's note: Subsections may have to be moved to suitable places.]

~~6.1~~7.1 Repositories

During VPN tunnel establishment, each SEG has to verify the validity of it's 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 CA_A is still valid

b) the certificate of SEG_A is still valid

SEG_A performs according checks from its own perspective.

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

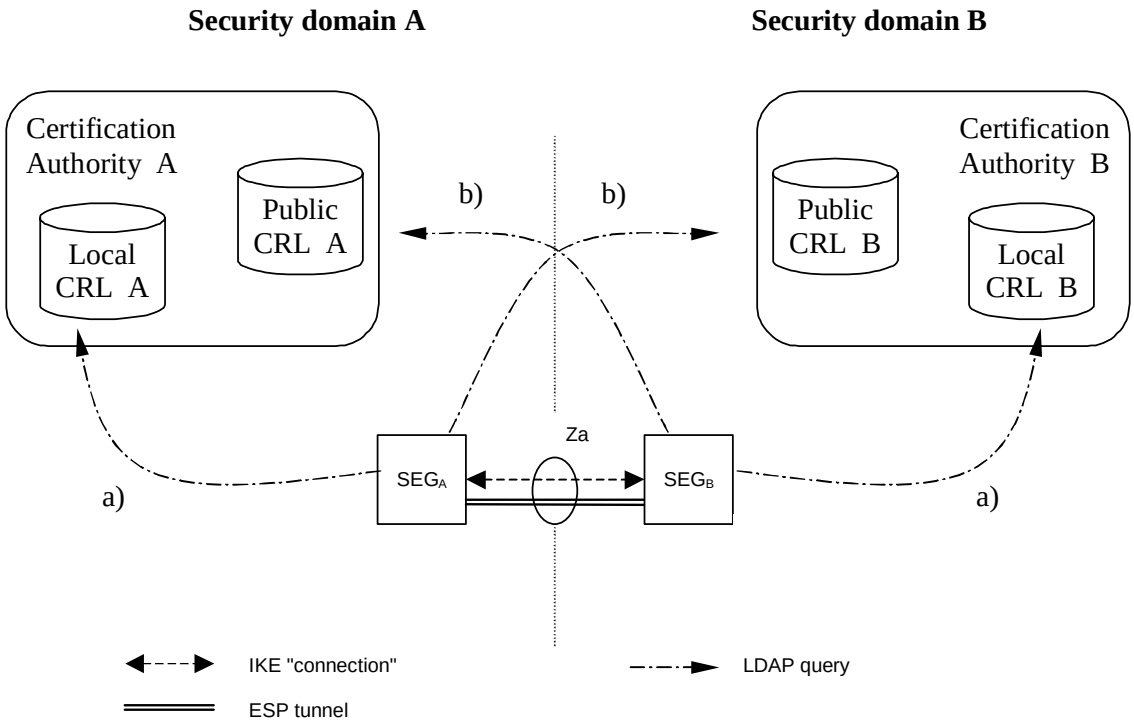

Figure 4: CRL Repositories

The public and local CRL repositories of a CA may be implemented as two 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.

SEGs shall use LDAP to access the CRL repositories.

[Editor's note: Further specification of public CRL interface and its relation to Za is ffs.]

~~6.2~~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 CAs shall support initial enrolment by SEG from CA via CMPv2, i.e. receiving a certificate from the Roaming CA, and updating the key of the certificate via CMPv2 before the certificate expires.

Enrolling a certificate to a SEG is an operation done more often than inter-operator cross-certifications, thus more automation is required than is possible with a PKCS#10 approach. It should be also noted that the lifetime of a cross-certificate is considerably longer than the lifetime of a SEG certificate. The basic CMPv2 functionalities such as enrollment 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 Security mechanisms~~

~~*[Editor's note: This section shall describe the security mechanisms that are provided for inter-domain authentication, i.e. the actual description of what the Authentication framework consists of.]*~~

~~7.1Authentication~~

8 Evolution path

[Editor's note: This chapter describes the evolution path from using NDS/IP towards optional PKI structure.]

8.1 Backward compatibility

Annex A (informative):

Decision for the simple trust model

A.1 Introduction

In order to document the decision for the "simple trust model", which requires manual cross-certification, this section discusses technical advantages and disadvantages of two basic approaches to providing inter-operator trust for purposes of roaming traffic protection, namely **cross-certification** and a **Bridge CA**. The Bridge CA is an extension of the cross-certification approach, and identified as one of the recommendable solutions for providing inter-operator trust in NDS/AF feasibility study (TR33.810). Taking into account the current state of PKI software and the general need for simple solutions when there is a choice, ~~there is pressure to make~~ the cross-certification without a Bridge CA was chosen~~as the working assumption~~ for the NDS/AF TS. This Annex~~document~~ discusses the background motivation for such direction.

The direct cross-certification without Bridge CA model is associated strongly with the current practice in the Internet IPsec world, where each IPsec connection is configured with a list of trusted CAs, and anyone with a certificate that has a trust path that can be followed up to such trusted CA (trust anchor) is allowed access. In this model, cross-certification is done at the time the roaming agreement is made. ~~We call t~~This is called the "**simple trust model**."

The Bridge CA model assumes that all operators wishing to establish a roaming agreement with other operators will first get certified by the Bridge CA for purposes of identification by other operators. This is a necessary preliminary step. Next, when the roaming agreement is done, the operators will configure their IPsec tunnels, with information about which one of the identifiable operators (who have a certificate issued by the Bridge CA) can use that tunnel. This is called the "**extended trust model**", or "separated trust and access control."

This Annex does not discuss the benefits of certificates vs. Pre-Shared Keys. The benefit of cross-certification vs. the explicit listing of roaming peer CAs includes the easier evolution path to a possible eventual Bridge CA model.

A.2 Requirements for trust model in NDS/AF

The following is a list of requirements for the trust model for NDS/AF:

A. *Simplicity and ease of deployment.* PKI brings many benefits when a large number of operators need to tunnel traffic in a mesh configuration, but its adoption should not be hindered by an unnecessarily complex technical solution. The required technical and legal operations necessary for exchanging traffic with another operator should be as easy and straightforward as possible.

B. *Compatibility with existing standards.* Unless there are explicit requirements why existing PKI standards should be extended to accommodate 3GPP environment, the 3GPP specifications should be accommodated to the existing standards. This allows best choice of equipment for operators and allows interoperability with non-3GPP environments.

C. *Usable by both GRX and non-GRX operators.* Both operators making use of GRX providers and those without (using leased lines or even the public Internet), should be able to make use of NDS/AF measures to exchange traffic securely.

A.3 Cross-certification approaches

A.3.1 Manual Cross-certification

The trust model of manual cross certification is characterized by the clause: “Trust nobody unless explicitly allowed”. Issuing a certificate for the authority ~~we wish~~ to be trusted creates the allowances. The manual cross certification is easy to understand. Also the security of this depends only on the decisions done locally.

A.3.2 Cross-certification with a Bridge CA

The trust model of bridge-CA can be characterized by the clauses:

“Trust everybody that the Bridge-CA trusts unless explicitly denied”. Explicit denials are handled by writing the restrictions (in the form of name constraints) to the certificate issued to the bridge.

“Trust everybody listed in the certificate which I issued to the bridge”. Explicit allowances are listed in the certificate issued to the bridge (in the form of name constraints).

Name constraint is a rarely used extension for X.509 certificates. In essence it is a clause that says who to trust or who not to trust based on names on certificates. The fact that they are relative rarely used and the fact that there is so little official documentation about them is a risk. Name constraints also require that there is some organization doing registration of names in order to avoid name collisions.

A.4 Issues with the Bridge CA approach

A.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 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 CA, O=Operator M

However, she can fabricate certificates of the following form:

Subject: CN=SEG 1, O=Operator A

Signer: CN=Roaming 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.

A.4.2 Preventing name collisions

If name constraints are used to prevent the additional "bureaucracy" involved with the Bridge CA, the names written into the certificate need to be registered with a third party to prevent two operators accidentally or on purpose using the same name in their certificates. This is in conflict with requirement B.

A.4.3 Two redundant steps required for establishing trust

As described in the introduction, with the "extended trust model", each operator shall first be certified by the bridge (authentication), and then as the second step, enumerate the trusted operators when configuring the IPSec tunnel (access control).

For the Bridge CA model to work, there is a need for organization that all the other parties involved can trust - and the trust shall be transitive! If you trust the bridge, you shall also trust the other organizations joining to the bridge via the cross certification. If Operator A and the Bridge CA cross certify with each other, Operator A will automatically trust every other certified operator to obey the rules. And this trust is not related to the roaming traffic tunnel; the tunnel has to be configured independently of the PKI.

So even if ~~we avoid~~ configuring new certificates in the SEG's is avoided when ~~we use~~ cross certification is used, the roaming information~~we~~ shall be configured and maintained ~~the roaming information~~ in the SEG some other way. And the hard part: How ~~do we combine~~ the trust provided by the PKI and the roaming agreements is combined, because clearly in this case PKI provided trust is not the same as roaming agreements.

~~We would need t~~Two steps would be needed:

1. building "trust" through Bridge CA => authenticating the peer SEG

2. specify in the tunnel configuration which peering SEGs ~~we~~ can be trusted

If the cross-certification is done without a Bridge CA, the steps can be combined into one. What is the additional value of the PKI provided trust (step 1), if the peering SEGs have to be restricted in any case?

A.4.4 Long certificate chains connected with IKE implementation issues

If Bridge CA is used, a Roaming 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.

A.4.5 Lack of existing relevant Bridge CA experiences

The Federal PKI in the USA is an example deployment where a Bridge CA is used to connect together CAs of the various federal agencies. It seems to be however the only documented one of its kind, and is connected with very heavy policy documentation and obviously heavy auditing practices, even within one organization, the federal government. The bridge approach is warranted in the case, because they want to automatically check whether some entity has legal rights to sign some document. The number of entities doing cross-domain PKI validation can be several millions, and it is impossible for one validating entity to keep count of individual signers.

In 3G roaming, the situation is in many ways different. When a new operator is born, the other ones do not automatically want to exchange roaming traffic with the new one, but a legal agreement with that operator and a technical tunnel establishment shall be done. In Federal PKI, the situation is the opposite: nothing should need to be done and still be able to trust the other.

In the Federal PKI, the paperwork and processes make name constraints in certificates unnecessary, and IKE is supposedly not used together with the Bridge CA.

A.5 Feasibility of the direct cross certification approach

This chapter discusses the direct cross certification, i.e. manual cross certification approach, where operators are doing the cross certification operation only when agreeing to set up a tunnel with another operator. This tunnel setup is a legal and technical operation in any case, so it is feasible to do also the cross-certification at this time, removing the need for the initial step to cross-certify with the Bridge CA.

There is no technical difference regarding the feasibility of direct cross certification or Bridge CA in the context of GRX or non-GRX environment. GRX might be one possible choice for providing the Bridge CA services.

A.5.1 Benefits of direct cross certification

The benefits of the direct cross certification is that as a mechanism it is well known, supported widely by current PKI products and there even exists an evolution path to a Bridge CA solution if the products come to support it adequately, a Bridge CA is established, and the number of operators becomes so large to warrant the use of the Bridge CA technology. Bridge CA uses the cross certification mechanisms in any case.

The tunnel configuration would look like the following:

Local-Subnetwork = some ipv6 subnetwork address

TrustedCA's = LocalCA

The information of which operator is allowed access is implicit in the direct cross certifications that have been done by the LocalCA, thus authentication and access control are tightly connected. If different foreign operators need to access different subnetworks, there would be separate tunnel configurations with SEG IP address for each, including an "AllowedCertificateSubject" limitation. The "AllowedCertificateSigner" limitation is not needed as necessary in this model (compared to the bridge CA model), since the set of operators which can be ~~who we are able to~~ authenticated are

only the ones, that~~we~~ have previously been agreed to trust when doing the direct cross certification. In ~~-~~the bridge CA case, the set of operators which can be~~we are able to~~ authenticated includes all operators who have joined to the bridge.

A.5.2 Memory and processing power requirements

In case of direct cross certification, each operator shall store the certificates issued for the other operators locally. They could be stored in the SEG devices, or then in a common repository.

If an operator makes roaming agreements with 500 other operators, this would require roughly 1000 kilobytes of memory, if the operator signs the certificates herself, and one certificate takes 1 kilobyte of memory. This should be quite feasible taken into account the high-end nature of SEG hardware.

Processing power benchmark for validating certificates:

Hardware: 800 MHz Pentium III, 256 MB of memory.

200 x 1024-bit RSA certificates, 1 Root CA (operator's own CA), 200 Sub CAs (other operator CAs) and 200 end entity (SEG) certificates. Also CRLs were verified. Both certificates and CRLs were loaded from disk during the test. The whole test took 3.5 seconds, with probably disk I/O taking most of the time.

In this test 200 certificate chains were validate up to the trusted root.

A.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 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.

A.5.4 Possible evolution path to a Bridge CA

If needed, it is possible to take the Bridge CA into use gradually, given that the support by PKI products becomes reality. From one operator's point of view, the bridge CA would be like any other operator so far, and a cross-certification would be made, but additionally the name constraints in the certificate issued for the Bridge CA should be updated every time a new roaming agreement is made.

Annex B (informative): Decision for the CRL repository access protocol

In order to document the decision for the protocol to access CRL repositories, this section summarises technical advantages and disadvantages of the two candidates.

LDAP

+ implemented by all PKI products (unless purely manual)

+ scalability

+ flexibility (integration possibility to other systems, automatic public key retrieval possibility)

- complexity

HTTP

+ simple

- not supported by all PKI products (although widely supported)

LDAP was chosen as the more future-proof protocol. Although more complex than HTTP, LDAP is well established amongst PKI vendors and operators.

Annex <C> (normative):
<Normative annex title>

Annex <X> (informative): Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
02-2003					TOC proposal for SA3#27		0.0.1
02-2003					Content of SA3#27 approved TDoc S3-030083 added and meeting comments incorporated	0.0.1	0.1.0
04-2003					Editorial changes and corrections	0.1.0	0.2.0
05-2003					Updated according to SA3#28 decisions	0.2.0	0.3.0
07-2003					Editorial corrections and clarification agreed by SA3#28	0.3.0	0.4.0

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ ab.cde CR CRNum ⌘rev - ⌘ Current version: 0.3.0 ⌘

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 ☒

Title:	⌘	Addition of a Clause on backward compatibility to NDS/IP
Source:	⌘	Siemens, Nokia, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	2507/07/2003
Category:	⌘	
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:	⌘	Addition of a new clause that describes how 1) NDS/IP and NDS/AF features interwork 2) How the migration can be done from PSK authentication method towards RSA signatures authentication method
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	New Clause

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

Other comments:	⌘	

8 Evolution path

[Editor's note: This chapter describes the evolution path from using NDS/IP towards optional PKI structure.]

8.1 Backward compatibility

NDS/IP describes an authentication framework whereby IKE phase 1 negotiation is based on pre-shared secrets authentication method. NDS/AF describes an optional authentication framework which enables NDS/IP SEGs to perform ~~whereby~~ IKE phase 1 negotiation ~~is~~ based on RSA Signatures authentication method. An NDS/AF compliant SEG shall also contain NDS/IP functionality. However an NDS/IP compliant SEG need not contain NDS/AF functionality.

Device specific management has to be used to reconfigure a SEG such that NDS/AF functionality will be used at the IKE initiator side for IKE phase 1 negotiation. The transition towards NDS/AF based authentication may be done on a SEG by SEG basis. Before the first NDS/AF SEG is taken into use it shall be assured that all needed NDS/AF functionality like CR, CRL's is available and working. The setting up of a NDS/AF based IPsec tunnel can be tested in parallel to the existing traffic.

A smooth migration may be done in the following way. An NDS/AF SEG shall provide several algorithm proposal's during IKE phase-1 negotiation, some based on RSA signature authentication method, others based on PSK authentication method. The responding IKE peer will select PSK authentication method if it does not support RSA signature authentication method but may select RSA signature authentication method if complies with NDS/AF. The IKE-responder policy shall be configured such that the RSA signature authentication method shall take precedence over PSK authentication method in order to ensure that it is used as soon as the IKE-initiator proposes RSA signature authentication method.

If the SEGs of both operators support NDS/AF based authentication then both SEG settings may be changed. The pre-shared secrets may then be removed from the SEGs and the IKE initiator shall only use RSA signature authentication method. However this removal of PSK is not essential as it may be used as a fallback mechanism. Only some care has to be taken that the policy between SEGs of different operators be coordinated otherwise this may result in failed tunnel set up. This would be the case if the initiating IKE peer only uses RSA signature authentication method and the responding IKE peer only accept PSK authentication method.

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 0.3.0 ⌘

*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 ☒

Title:	⌘	Addition of a Clause on CRL Management within the SEG
Source:	⌘	Siemens, Nokia, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	07/07/2003
Category:	⌘	
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:	⌘	Addition of a separate clause that collects CRL management issues according to the working assumption that CRLs shall be retrieved out-of-band via LDAP. The alternative way of handling CRLs is exchanging them during IKE Phase 1 (see also according to Section 3.3.9 of draft-ietf-ipsec-pki-profile-02.txt. recommendation). However a product survey revealed that there are still few products supporting this. This statement was confirmed by one of the authors draft-ietf-ipsec-pki-profile-02.txt.
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	New Clause 6.3

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

Other comments:	⌘	

6 Security features

[Editor's note: Subsections may have to be moved to suitable places.]

6.1 Repositories

During VPN tunnel establishment, each SEG has to verify the validity of it's 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 CA_A is still valid

b) the certificate of SEG_A is still valid

SEG_A performs according checks from its own perspective.

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

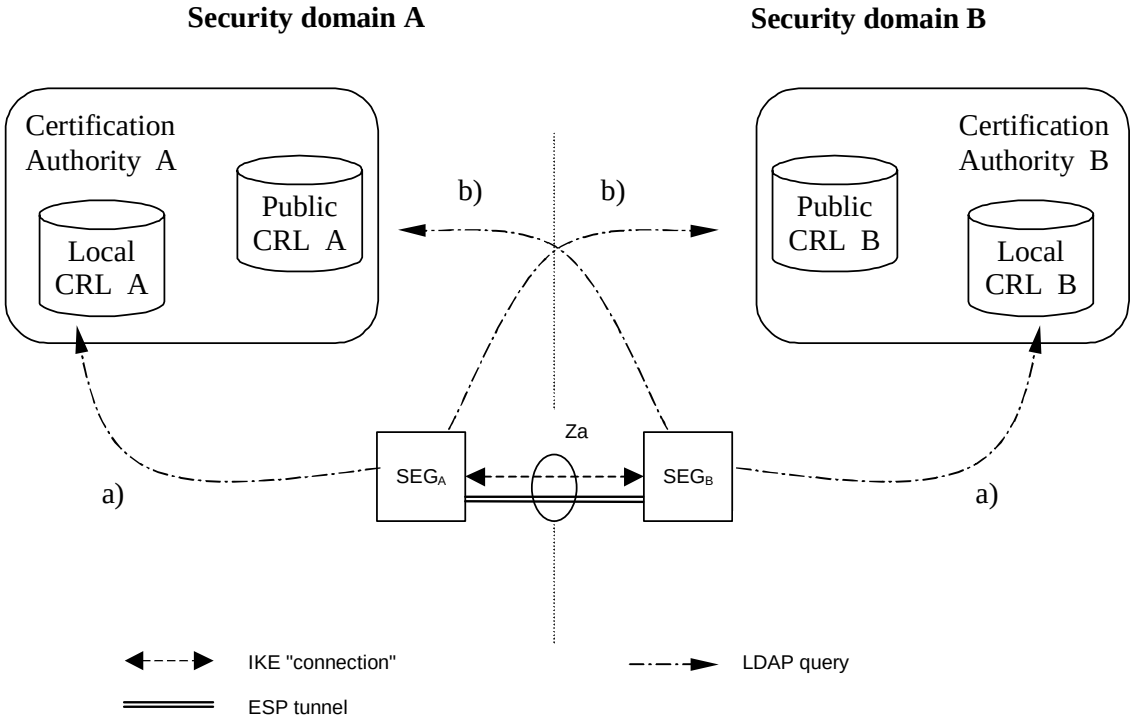

Figure 4: CRL Repositories

The public and local CRL repositories of a CA may be implemented as two 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.

SEGs shall use LDAP to access the CRL repositories.

[Editor's note: Further specification of public CRL interface and its relation to Za is ffs.]

6.2 Life cycle management

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

[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.]

6.3 CRL management

NDS/AF compliant SEGs shall not sent an ISAKMP CERTREQ where the Certificate Type is "Certificate Revocation List (CRL)". Receiving SEGs may ignore this request as section 5.3.1.3 specifies that CRLs shall be retrieved via CRL distribution point.

The CRL issuer (which is in most cases the CA) shall only issue full CRLs. The use of delta CRLs is not forbidden but is not encouraged because of possible interoperability problems. The full CRL shall only contain revoked certificates applicable for use within NDS/AF. The CRL issuer shall issue a CRL also in cases there are no revoked certificates. A SEG is not obliged to query for a CRL via the CRL Distribution Point, if a cached one is still available and valid. If no valid cached CRL is available, the SEG shall fetch a new CRL. If no valid CRL can be fetched, the SEG shall treat this as an error and cancel tunnel establishment.

[Editor's note: It is for ffs whether the ISAKMP SA lifetime shall be restricted to at most the remaining time+ delta defined within the CRLs NextUpdate field. This might result in following guideline
min(Cert. chain lifetime, CRLs lifetimes) >= IKE SA lifetime >= IPsec SA lifetime]

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 0.3.0 ⌘

*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 ☒

Title:	⌘	Handling critical and non critical certificate extensions
Source:	⌘	Siemens, Nokia, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	07/07/2003
Category:	⌘	
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:	⌘	Addition of explanation on how the specification text on mandatory and optional implementation (within the profiling clause 6.2) of critical and non-critical extensions has to be interpreted i.e. how to handle a mandatory critical extension, a optional critical extension, …
Summary of change:	⌘	
Consequences if not approved:	⌘	Implementers have to interpret this from RFC3280. <draft-ietf-ipsec-pki-profile-02.txt> contains similar explanations see 4.1.3. X.509 Certificate Extensions

Clauses affected:	⌘	New Annex C

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

Other comments:	⌘	

Annex B (informative):
Decision for the CRL repository access protocol

In order to document the decision for the protocol to access CRL repositories, this section summarises technical advantages and disadvantages of the two candidates.

LDAP

+ implemented by all PKI products (unless purely manual)

+ scalability

+ flexibility (integration possibility to other systems, automatic public key retrieval possibility)

- complexity

HTTP

+ simple

- not supported by all PKI products (although widely supported)

LDAP was chosen as the more future-proof protocol. Although more complex than HTTP, LDAP is well established amongst PKI vendors and operators.

Annex C (normative):
Critical and non critical Certificate Extensions.

According to RFC3280 section 4.2 a certificate extension can be designated as either critical or non-critical.

"A certificate using system MUST reject the certificate if it encounters a critical extension it does not recognize; however, a non-critical extension MAY be ignored if it is not recognized."

Optional and mandatory support statements (e.g. Clause 5.3 profiling) are being made with respect to implementation requirements. A receiving SEG shall be able to process an extension marked as critical that is mandatory to support in NDS/AF. When optional to support, a received extension marked as critical shall lead to an error according to RFC3280.

Annex <DC> (normative):
<Normative annex title>

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 0.3.0 ⌘

*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 ☒

Title:	⌘	Additions to the clause 5.3 on profiling of certificates
Source:	⌘	Siemens, Nokia, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	08/07/2003
Category:	⌘	
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: ⌘ Addition of review remarks and insights delivered from draft-ietf-ipsec-pki-profile-02.txt according to following guidelines:

- Do not refer to draft-ietf-ipsec-pki-profile-02.txt but copy the relevant information to the NDS/AF spec. draft-ietf-ipsec-pki-profile-02.txt will probably not make it to RFC in the short term if it will make it at all!
- Do not include error case descriptions from draft-ietf-ipsec-pki-profile-02.txt if due to interworking with non-compliant NDS/AF SEG.

Details of changes:

- Incorporation of the JNSA lessons from PKI interoperability testing 2001: See attachment or *http://www.jnsa.org/english/e_result.html* (also presented at IETF-55= Nov 2002).
- Adding text on the role of the roaming CA/SEG with respect to the Certificate profiling verification.
- Adding text on relation with RFC3280.
- Correcting inaccurate naming of certificate fields.
- SEG certificates shall be directly signed by the roaming CA.
- Adding an editors note on identities and outstanding profiling work

		- Adding subjectAltName to the SEG certificate profile
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.3			
		Y	**N**		
Other specs affected:	⌘		**N**	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	
Other comments:	⌘				

5.3 Profiling

[Editor's note: "Motivation" statements marked with italic in chapters 5.3.1 and 5.3.2 are included in the drafting stage of the TS, but will be removed before submission for approval to TSG SA.]

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.* draft-ietf-ipsec-pki-profile-02.txt will not be referenced from this specification, but valuable profiling statements will be copied to the NDS/AF specification*]*

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. This applies for both the SEG and the roaming CA.

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

Motivation: This addresses lesson from http://www.jnsa.org/english/e_result.html

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

Motivation: This addresses lesson from http://www.jnsa.org/english/e_result.html

[Editor's note: the relationship between a) ID's includes within the certificate, B) used at the transport layer and C) IKE ID available within the IKE policy; and their effects on the profiling needs further investigation]

5.3.1.1 Common rules to all certificates

- Version 3 certificate according to RFC3280.

  Motivation: This is the current state of the art [3].

- Hash algorithm for use before signing certificate: 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 in 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 [5] retrieval shall be supported as the primary method of certificate revocation verification.

- Certificate extensions mentioned within RFC3280 but not in NDS/AF are optional for implementation.

SerialNumber shall have a length of exactly 20 octets

Motivation: *This addresses lesson from http://www.jnsa.org/english/e_result.html*

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

SEG certificates shall be directly signed by the roaming CA, i.e. without employing any intermediate CAs. This limits NDS/AF complexity and makes retrieval and validation of intermediate CA certificates by SEGs unnecessary.

In addition to clause 5.3.1.1, 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 roaming CA~~Domain authority~~ cert.
- 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 critical ~~enhanced~~ extended 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 [1] 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.
- The identity of the CERT payload (including the SEG certificate) shall be used for policy checks.

  Motivation: ISAKMP contains two different payloads that allow the specification of the endpoint identity, the ID payload and the CERT payload. Within the NDS/AF framework only the SEG certificate is sent within IKE Phase 1 so there will be no ambiguity is selecting the peer ID from the received certificates. See also section 3.1.2 of draft-ietf-ipsec-pki-profile-02.txt on Endpoint identification.
- 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 IPv6 – [6]), 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.

3GPP TSG SA WG3 Security — S3#29 **S3-030388**
15 - 18 July 2003, San Francisco, USA

CR-Form-v7

PSEUDO CHANGE REQUEST

⌘ **ab.cde** **CR** **CRNum** ⌘**rev** **-** ⌘ Current version: 0.3.0 ⌘

*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 ☒

Title:	⌘	Addition of text on usecases
Source:	⌘	Siemens, Nokia, SSH, T-Mobile
Work item code:	⌘	NDS/AF
Date:	⌘	07/07/2003
Category:	⌘	
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:	⌘	Inclusion of missing operational usecases for various scenarios
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	5.2

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

Other comments:	⌘	

5.2 Use cases

5.2.1 Operator Registration: Creation of r~~R~~oaming agreement

Security gateways (SEG's) of two different security domains need to establish a secure tunnel, when the operators make a roaming agreement. The first technical step in creating the roaming agreement between domains is the cross-certification of the 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 CAs create a PKCS#10 certificate request, and send it to the other operator. 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 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 all SEGs that need to communicate with the other domain.

When creating the new cross-certificate, the 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. The validity time could be e.g. 15 years. The start time of the validity should start e.g. a day before the actual roaming is set to start in order to avoid problems with different time zones. Problems in PKI are often due to the time differences.

When the new certificate is available for SEG, all that needs to be configured in SEG is the DNS name of the peering SEG gateway. The authentication can be done based on 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 roaming CA for the SEGs together with the cross certificate issued for the peering domains. The certificates of the peer domains are located under the cross-certificates of the peer domains.

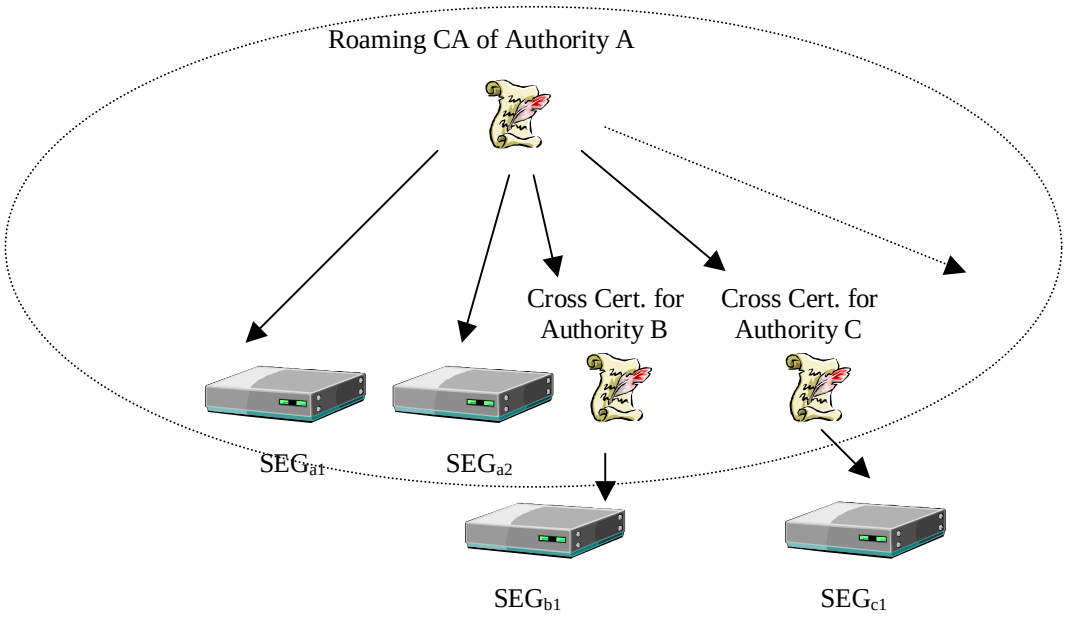

Figure 3: Security domain A illustrated. The PKI is hierarchical inside the domain.

5.2.2 VPN tunnel establishment

After establishing a roaming agreement and finishing 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 is specified. Only local roaming CA is configured as the trusted CA. Because of the cross-certification, any operator whose roaming CA has been cross-certified, can get access using this VPN connection configuration. If access to a certain local subnet is allowed for only certain operators, the VPN connection configuration shall include limitations for certificate issuer name.

[Editor's note: These limitations for certificate issuer name are ffs.]

Following is the flow of connection negotiation from the point of view of Operator A's SEG (initiator). Operator B 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 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 B CRL databases. If a SEG cannot successfully perform both CRL checks, it shall treat this as an error and abort tunnel establishment. IKE Phase-1 SA is established, and the Phase-2 SA negotiation proceeds as described with 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 peers shall remove the SAs using device-specific management methods. Each concerned operator shall also list the cross-certificate created for the roaming CA of the terminated operator in his own local CRL.

5.2.4 Roaming CA registration

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

5.2.5 Roaming CA deregistration

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

5.2.6 Roaming CA certificate creation

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 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 CA certificate revocation

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 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 to 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 CA certificate renewal

The Roaming CA certificate has to be renewed before the old roaming CA certificate expires. The renewing of a roaming CA certificate results in the need to renew the cross-certificates. This should be done before the old expire.

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 adapted

~~5.2.4~~5.2.10 SEG deregistration

If a SEG is removed from the network, the SAs shall be removed using device-specific management methods.~~as above~~. The operator of the SEG shall have the certificate of the SEG listed in his CRL. The SPD of partner network may have to be adapted.

5.2.11 SEG certificate creation

Using device specific management methods, the certificate creation is initiated. The CMPv2 protocol is used between the roaming CA and the SEG for automatic certificate enrolment.

5.2.12 SEG certificate revocation

If a SEG key pair gets compromised then the existing SAs shall be removed using device-specific management methods. The operator of the SEG shall have the certificate of the SEG listed in his CRL.

5.2.13 SEG certificate renewal

A new SEG certificate needs to be in place before the old SEG certificate expires. The procedure is similar to the SEG certificate creation and if fully automated by CMPv2.

~~*[Editor's note:*~~

~~*Two new paragraphs needed to describe the involved actions for revocation and check our model !?*~~

~~*Roaming CA certificate revocation ?*~~

~~*A)of the own roaming CA*~~

~~*B)of a partner roaming CA*~~

~~*SEG revocation*~~

~~*A)own SEG*~~

~~*B)*~~*A)* ~~*SEG of a roaming partner]*~~