3GPP TSG SA WG3 Security — S3#28 **S3-030201**

06 - 09 May 2003

Berlin, Germany

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

Title: **NDS/AF TS**

Document for: **Information**

Agenda Item:

The latest base version of the NDS/AF specification is presented for information. This version 0.2.0 includes editorial changes and corrections to the version agreed in the S3#27 meeting.

3GPP TS ab.cde V0.~~1~~2.0 (2003-~~02~~04)

Technical Specification

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

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

Contents

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.

~~NOTE: In case two SEG's interconnect security domains 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.~~

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.

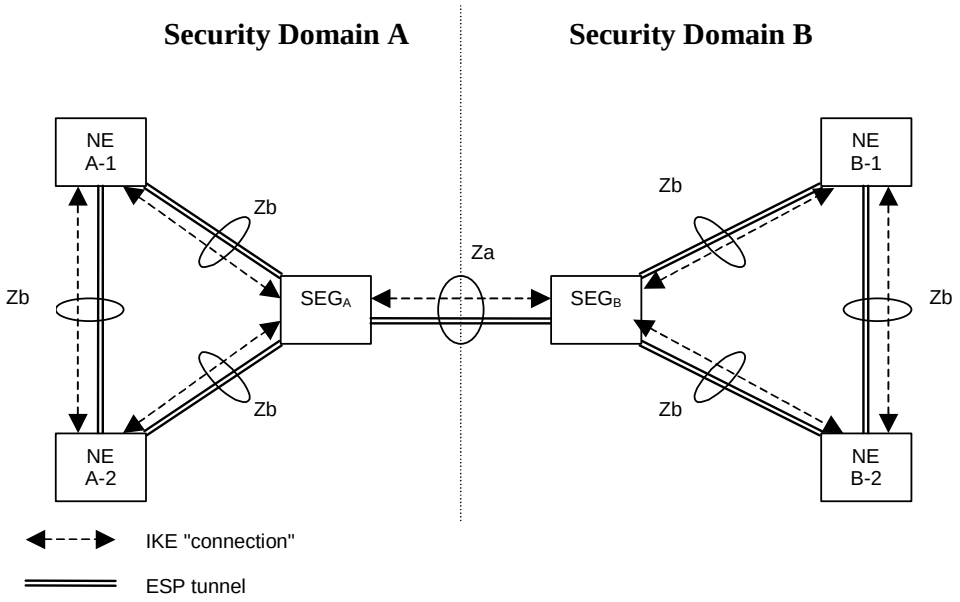

Figure 1: NDS architecture for IP-based protocols [1]

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~~2459~~: "Internet X.509 Public Key Infrastructure Certificate and CRL Profile "

3 Definitions and abbreviations

3.1 Definitions

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

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

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

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~~e~~ 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]

4.1 Cross-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 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 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 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.

5.1 PKI architecture for ~~3GPP~~NDS/AF

This chapter defines the PKI architecture for the ~~3GPP~~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 CA is called a 'roaming CA'.~~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~~entities~~ in the domain. This specification describes the profile for the roaming CA~~domain certification authority~~ and a profile for ~~the end entity certificates~~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 certificate authority which the network elements use for inter-operator authentication is called roaming CA of the domain.~~ 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 ~~in~~ Za interface ~~in~~ towards domain ~~A~~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 ~~in~~ Za interface ~~in~~ towards domain ~~B~~A.

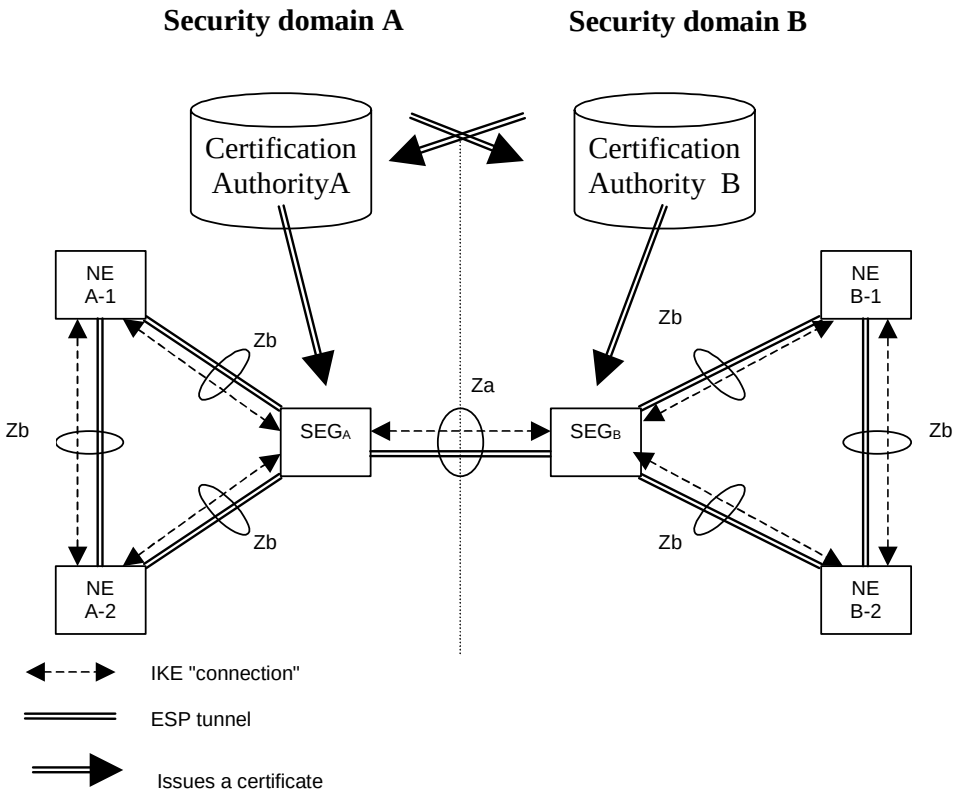

Figure ~~1~~2: Trust validation path in context of NDS/IP

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 certificatione 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, ~~for example~~ by storing the new cross-certificate into all SEGs that need to communicate with the other domain~~the device~~.

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 ~~address~~ 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.

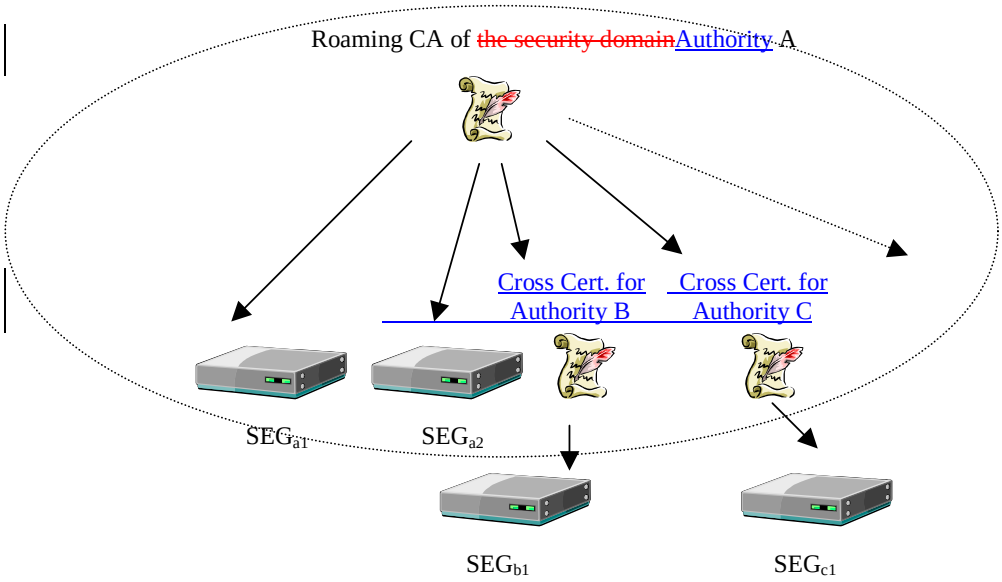

Figure 3~~2~~: Security domain A illustrated. The PKI is hierarchical inside the domain.

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 ~~IP address~~ DNS name is specified. Only local roaming CA is configured as the trusted ~~root~~ 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-~~End Entity~~ certificate and the corresponding digital signature in Main Mode message 3
- SEG A receives the remote SEG B ~~End Entity~~ 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 [xx1]as with PSK authentication.

NOTE: This specification provides authentication of SEGs in an "end-to-end" fashion as regards to roaming traffic (operator to operator). The assumption is that authentication in for example GRX (GPRS roaming network) is achieved with non-IPsec mechanisms. As long as the operators do not use the NDS/AF for getting access to GRX, the transport mechanism (inter-operator leased line, GRX or Internet) does not matter. 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 or SEG 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.

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.

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 Profiling

5.2.45.3.1 Certificate profiles

5.2.4.15.3.1.1 CA Certificate profile

5.2.4.25.3.1.2 SEG Certificate profile

5.2.4.35.3.1.3 Cross Certification between domains

~~5.2.5~~5.3.2 IKE negotiation and profiling

~~5.2.5.1~~5.3.2.1 IKE Phase-1 profiling

~~5.2.5.2~~5.3.2.2 Potential interoperability issues

~~5.2.6~~5.3.3 Path validation

~~5.2.6.1~~5.3.3.1 Path validation profiling

~~5.2.7~~5.3.4 Services 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 Security features

[Editor's note: ~~This section shall explain the provided security features in detail~~Subsections may have to be moved to suitable places.]

6.1 Repositories

6.2 Life cycle management

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.]

7.1 Authentication

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):
<~~N~~Informative annex title>

Editor's note: Topics to cover are
- Decision for simple trust model
- Decision for LDAP

Annex <B> (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