3GPP TSG SA WG3 Security — S3#21 **S3-010627**

November 26th– 30th, 2001

Sophia Antipolis, France

Source:	Ericsson
Title:	On defining NDS/IP traffic
Document for:	Discussion/Decision
Agenda Item:	TBD

1. Scope

This contribution tries to fix some inconsistencies of the specification while defining the kind of traffic that should be protected and/or routed through SEGs.

At the same time, issues such as references to BGs and policy discrimination of GTP traffic and some other editorial and/or TS structural issues are also discussed.

S3 members are kindly asked to review and discuss the proposed changes to 33.210 presented below and marked with change bars for an easier introduction into the spec.

2. Proposals

2.1 NDS/IP Traffic

While reviewing TS 33.210 v0.6.0, Ericsson has identified some inconsistences while specifying the kind of traffic that shall be routed through SEGs. To name a few …

> *… **All secure communication** between security domains shall take place through Security Gateways (SEGs)…*
>
> *… **All NDS/IP traffic** shall pass through a SEG before entering or leaving the security domain…*
>
> *… **All traffic** from a NE in one security domain towards a NE in a different security domain will be routed via a SEG and will afforded hop-by-hop security protection towards the final destination…*
>
> *… The Za-interface covers **all secure IP communication** between security domains …*
>
> *… **All control plane traffic** towards external destinations shall be routed via a SEG.*

It is not clear whether all traffic (control/user plane of all IP protocols), all control plane traffic or only the traffic that shall be protected shall be routed through the SEG. This contribution proposes a definition for NDS/IP Traffic in order to try to solve these inconsistencies.

While applying these changes in many different parts of the specification, some other issues are discussed and proposed in this contribution.

2.2 List of GTP interfaces and Protocols

This contribution proposes to move the list of GTP interfaces and protocols (table 2 currently in chapter 4.4.1) to chapter 6 where the rest of particularities related to NDS/IP aplication to GTP are specified.

2.3 Definition of BG

It is also proposed to remove the reference to BorderGateway in chapter 5.6.2. BG is defined in TS 23.002 …

> ### *4.1.3.3 Border Gateway (BG)*
>
> *The Border Gateway (BG) is a gateway between a PLMN supporting GPRS and an external inter-PLMN backbone network used to interconnect with other PLMNs also supporting GPRS. The role of the BG is to provide the appropriate level of security to protect the PLMN and its subscribers.*
>
> *The BG is only needed in PLMNs supporting GPRS.*

Considering this definition, it looks like BG is only applicable to GPRS NWs (only for GTP) and since we are now including NDS/IP support to IMS, mentioning BG in the definition of the generic Za interface might not be appropriate.

In line with discussions at S3#20 on Nokia's contribution S3-010489, it is also Ericsson opinion that BGs and SEGs should be defined as two separate logical entities.

Ericsson proposes S3 to give a closer look to the definition of BG in TS 23.002 related to the potential security functions it might implement. At a first sight, it might look like that BG implements some kind of FireWall functionality. However, this goes in contradiction with BG definition in the IP community where typicaly a BG is no more than a router.

2.4 Policy discrimination of GTP-C and GTP-U

Chapter 6.2 addresses in an unclear way how and where security policies are applied…

- In one sense it refers that policy discrimination of GTP-C and GTP-U shall be performed at GSNs. This is assuming then that GTP-U will not be routed through SEGs and excluding the NW configuration where GSNs route GTP traffic to SEG and then SEG applies security policies in order to determine that GTP-U shall bypass IPSec.
- While refering to the checking of the SPD it is not clear whether this check is performed at GSNs or at SEGs themselves.

Changes to chapter 6.2 tries to address these issues.

While doing this change, it was identified wrong numbering in section 5.2 which has been also fixed.

3. Proposed Changes

***************************** *FRIST CHANGE* *****************************

3.1 Definitions

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

Anti-replay protection: Anti-replay protection is a special case of integrity protection. Its main service is to protect against replay of self-contained packets that already have a cryptographical integrity mechanism in place.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

NDS/IP Traffic: Traffic that requires protection according to the mechanisms defined in this specification.

Security Association: A unidirectional logical connection created for security purposes. All traffic traversing an IPsec SA is provided the same security protection. The IPsec SA itself is set of parameters to define a unidirectional security protection between two entities. An IPsec Security Association includes the cryptographic algorithms, the keys, the duration of the keys, and other parameters.

Transport mode: Mode of operation that primarily protects the payload of the IP packet, in effect giving protection to higher level layers

Tunnel mode: Mode of operation that protects the whole IP packet by tunnelling it so that the whole packet is protected

***************************** *NEXT CHANGE* *****************************

4.3 Security for native IP based protocols

The UMTS network domain control plane is sectioned into security domains and typically these coincide with operator borders. The border between the security domains is protected by Security Gateways (SEGs). The SEGs are responsible for enforcing the security policy of a security domain towards other SEGs in the destination security domain. The network operator may have more than one SEG in its network in order to avoid a single point of failure or for performance reasons. A SEG may be defined for interaction towards all reachable security domain destinations or it may be defined for only a subset of the reachable destinations.

The UMTS network domain security does not extend to the user plane and consequently the security domains and the associated security gateways towards other domains do not encompass the user plane Gi-interface towards other, possibly external to UMTS, IP networks.

A chained-tunnel/hub-and-spoke approach is used which facilitates hop-by-hop based security protection.

All NDS/IP traffic shall pass through a SEG before entering or leaving the security domain.~~All secure communication between security domains shall take place through Security Gateways (SEGs).~~

***************************** *NEXT CHANGE* *****************************

4.4.1 Security domains and interfaces

The UMTS network domain shall be logically and physically divided into security domains. These control plane security domains may closely correspond to the core network of a single operator and shall be separated by means of security gateways.

The specific network domain security interfaces are found in table 1. The definitions for Zd, Ze and Zf only apply to NDS/MAP (TS33.200, [9]).

Table 1: Network domain security specific interfaces

Interface	Description	Network type
Za	Network domain security interface between SEGs. The interface is used for both the negotiation of security associations aiming at setting up ESP tunnels between SEGs and the protection of traffic within the negotiated ESP tunnels between SEGs (no third party negotiation).	IP
Zb	Network domain security interface between SEGs and NEs within the same network. The interface is used for both the negotiation of security associations aiming at setting up ESP tunnels between a NE and a SEG and the protection of traffic within the negotiated ESP tunnels.	IP
Zc	Network domain security interface between NEs within the same network. The interface is used for both the negotiation of security associations aiming at setting up ESP tunnels between NEs and the protection of traffic within the negotiated ESP tunnels.	IP

~~The interfaces, which affects/is affected by the network domain security specification, are described in the table below. Notice that when security protection is employed over an interface, this specification will refer to the Z-interface name.~~

~~Table 2: Interfaces that are affected by NDS/IP~~

~~Interface~~	~~Description~~	~~Affected protocol~~
~~Gn~~	~~Interface between GSNs within the same network~~	~~GTP~~
~~Gp~~	~~Interface between GSNs in different PLMNs.~~	~~GTP~~
~~Mw~~	~~Interface between CSCFs within the same network~~	~~SIP~~
~~Mm~~	~~Interface between CSCF and Multimedia IP network~~	~~SIP~~

***************************** *NEXT CHANGE* *****************************

5.2 Security Associations (SAs)

In the UMTS network domain security architecture the key management and distribution between SEGs is handled by the protocol Internet Key Exchange (IKE) [18,19,20]. The main purpose of IKE is to negotiate, establish and maintain Security Associations between parties that are to establish secure connections. The concept of a Security Association is central to IPsec and IKE.

To secure typical, bi-directional communication between two hosts, or between two security gateways, two Security Associations (one in each direction) are required.

Security associations are uniquely defined by the following parameters:

- A Security Parameter Index (SPI)
- An IP Destination Address (this is the address of the ESP SA endpoint)
- A security protocol identifier (this will always be the ESP protocol in NDS/IP)

With regard to the use of security associations in the UMTS network domain control plane the following is noted:

- NDS/IP only requires support for tunnel mode SAs

- NDS/IP only requires support for ESP SAs
- There is no need to be able to negotiate SA bundles as only a single ESP SA is set up to protect traffic between the nodes

The IPsec specification of SAs can be found in RFC-2401 [12].

5.2.1~~2~~ Security Policy Database (SPD)

The Security Policy Database (SPD) is a policy instrument to decide which security services are to be offered and in what fashion.

The SPD shall be consulted during processing of both inbound and outbound traffic. This also includes traffic that shall not/need not be protected by IPsec. In order to achieve this the SPD must have unique entries for both inbound and outbound traffic such that the SPD can discriminate among traffic that shall be protected by IP~~p~~sec, ~~and~~ that shall bypass IP~~p~~sec or that shall be dropped by IPsec.

The SPD plays a central role when defining security policies, both within the internal security domain and towards external security-domains. The security policy towards external security domains will be subject to roaming agreements and shall be regulated by a well-defined set of standardised NDS/IP protection profiles.

5.2.2~~3~~ Security Association Database (SAD)

The Security Association Database (SAD) contains parameters that are associated with the active security associations. Every SA has an entry in the SAD. For outbound processing, a lookup in the SPD will point to an entry in the SAD. If an SPD entry does not point to an SA that is appropriate for the packet, an SA shall be automatically created or fetched from an SEG or KAC.

********************************** *NEXT CHANGE* *********************************

5.6 UMTS key management and distribution architecture for native IP based protocols

5.6.1 Network domain security architecture outline

The NDS/IP key management and distribution architecture is based on the IPsec IKE [12,18,19,20] protocol. As described in the previous section a number of options available in the full IETF IPsec protocol suite have been considered to be unnecessary for NDS/IP. Furthermore, some features that are optional in IETF IPsec have been mandated for NDS/IP and lastly a few required features in IETF IPsec have been deprecated for use within NDS/IP scope. Section 5.3 and 5.4 gives an overview over the profiling of IPsec and IKE in NDS/IP.

The compound effect of the design choices in how IPsec is utilized within the NDS/IP scope is that the NDS/IP key management and distribution architecture is quite simple and straightforward.

The basic idea to the NDS/IP architecture is to provide hop-by-hop security. This is in accordance with the *chained-tunnels* or *hub-and-spoke* models of operation. The use of hop-by-hop security also makes it easy to operate separate security policies internally and towards other external security domains.

In NDS/IP only the Security Gateways (SEGs) shall engage in direct communication with entities in other security domains for NDS/IP traffic. The SEGs will then establish and maintain IPsec secured ESP tunnels between security domains. ~~These SEG-SEG tunnels will normally be established and maintained to be in permanent existence.~~ SEGs will normally maintain at least one IPSec tunnel available at all times to a particular peer SEG. The SEG will maintain logically separate SAD and SPD databases for each interface.

The NEs will be able to establish and maintain ESP secured tunnels as needed towards a SEG or other NEs within the same security domain. All NDS/IP traffic from a NE in one security domain towards a NE in a different security domain will be routed via a SEG and will afforded hop-by-hop security protection towards the final destination.

Operators may decide to establish only one ESP tunnel. This would make for coarse-grained security granularity. The benefits to this is that it gives a certain amount of protection against traffic flow analysis while the drawback is that one will not be able to differentiate the security protection given between the communicating entities. It shall still be possible to negotiate different SAs for different protocols.

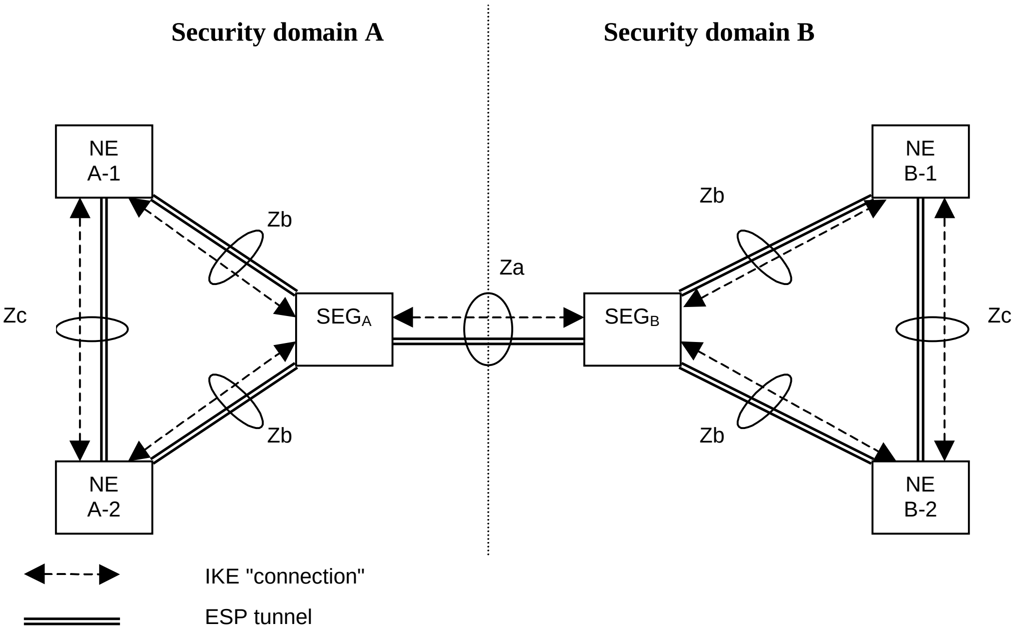

Figure 1: NDS architecture for IP-based protocols

5.6.2 Interface description

The following interfaces are defined for protection of native IP based protocols:

- **Za-interface (SEG-SEG)**

  The Za-interface covers all ~~secure~~ NDS/IP traffic ~~communication~~ between security domains. The SEGs uses IKE to negotiate, establish and maintain a secure tunnel between them. Subject to roaming agreements, the inter-SEG tunnels would normally be available at all times, but they can also be established as needed. The tunnel is subsequently used for forwarding secured traffic between security domain A and security domain B.

  One SEG can be dedicated to only serve a certain subset of all roaming partners. This will limit the number of SAs and tunnels that need to be maintained. ~~The number of SEGs within a network will normally be limited and should normally not be larger than the numer of BGs in the network.~~

  All security domains shall operate the Za-interface.

[Editor's note: The intention here is to make Za mandatory provided that an operator has decided to implement NDS/IP. This I believe captures the current agreement in S3.]

- **Zb-interface (NE-SEG)**

  The Zb-interface is located between NEs and a SEG from the same security domain. The NE and the SEG are able to establish and maintain ESP-tunnels between them. Whether the tunnel is established when needed or a priori is for the security domain operator to decide. The tunnel is subsequently used for exchange of secured traffic between the NE and the SEG. Normally ESP shall be used with both encryption and authentication/integrity, but an authentication/integrity only mode is allowed. All ~~control plane~~NDS/IP traffic towards external destinations shall be routed via a SEG.

  It is for the security domain operator to decide whether to implement Zb-interfaces or not.

- **Zc-interface (NE-NE)**

  The Zc-interface is located between NEs from the same security domain. The NEs are able to establish and maintain ESP-tunnels between them. Whether the tunnel is established when needed or a priori is for the security domain operator to decide. The tunnel is subsequently used for exchange of secured traffic between the NEs.

  Normally ESP shall be used with both encryption and authentication/integrity, but an authentictaion/integrity only mode is allowed. The ESP tunnel shall be used for all control plane traffic that needs security protection.

  It is for the security domain operator to decide whether to implement Zc-interfaces or not.

NOTE-1: The security policy established over the Za-interface is subject to roaming agreements. This differs from the security policy enforced over the Zb- and the Zc-interface, which is unilaterally decided by the security domain operator.

NOTE-2: There is normally no NE-NE interface for NEs belonging to separate security domains. This is because it is important to have a clear separation between the security domains. This is particularly relevant when different security policies are employed whithin the security domain and towards external destinations.

The restriction not to allow secure inter-domain NE-NE communication does not preclude a single physical entity to contain both NE and SEG functionality. A combined NE/SEG entity need not support an external Zb-interface provided that the entity itself is physically secured. The exact SEG functionality required to allow for secure inter-domain NE←→NE communication will be subject to the actual security policies being employed. Thus, it will be possible for roaming partners to have secure direct NE←→NE communication within the framework of NDS/IP.

***************************** ***NEXT CHANGE*** *****************************

6 Security protection for GTP

This section details how NDS/IP shall be used when GTP is to be security protected.

6.1 The need for security protection

The GPRS Tunnelling Protocol (GTP) is defined in 3G TS 29.060 [5]. The GTP protocol includes both the GTP control plane signalling (GTP-C) and user plane data transfer (GTP-U) procedures. GTP is defined for Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs.

GTP-C is used for traffic that that is sensitive in various ways including traffic that is:

- critical with respect to both the internal integrity and consistency of the network
- essential in order to provide the user with the required services
- crucial in order to protect the user data in the access network and that might compromise the security of the user data should it be revealed

Amongst the data that clearly can be considered sensitive are the mobility management messages, the authentication data and MM context data. Therefore, it is necessary to apply security protection to GTP signalling messages (GTP-C).

Network domain security is not intended to cover protection of user plane data and hence GTP-U is not protected by NDS/IP mechanisms.

Table x presents a list of GTP interfaces that shall be considered by NDS/IP.

Interface	Description	Affected protocol
Gn	Interface between GSNs within the same network	GTP
Gp	Interface between GSNs in different PLMNs.	GTP

Table X: GTP Interfaces that are affected by NDS/IP

6.2 Policy discrimination of GTP-C and GTP-U

~~SGNs~~ It must must be posible ~~able~~ to discriminate between GTP-C messages, which shall receive protection, and other messages, including GTP-U, that shall not be protected. Since GTP-C is assigned a unique UDP port-number in (TS29.060, [5]) IPsec can easily distinguish GTP-C datagrams from other datagrams that may not need IPsec protection.

~~As discussed in section 5.2.2 the~~ Security Policies shall be checked~~y Database (SPD) is consulted~~ for all traffic (both incoming and outgoing) so datagrams can be processed ~~and it processes the datagrams~~ in the following ways:

- discard the datagram
- ~~bypass the datagram (~~do not apply IPsec~~)~~
- apply IPsec

Under this regime GTP-U will simply bypass IPsec while GTP-C will be further processed by IPsec in order to provide the required level of protection. The SPD has a pointer to an entry in the Security Association Database (SAD) which details the actual protection to be applied to the datagram.

NOTE: Selective protection of GTP-C relies on the ability to uniquely distinguish GTP-C datagrams from GTP-U datagrams. For R99 and onwards this is achieved by having unique port number assignments to GTP-C and GTP-U. For previous version of GTP this is not the case and provision of selective protection for GTP-C for pre-R99 versions of GTP is not possible.