3GPP TSG SA WG3 Security — S3#21 **S3-010659**

November 26th– 30th, 2001

Sophia Antipolis, France

Source:	Ericsson
Title:	On Definition of Za/Zb/Zc Interfaces
Document for:	Discussion/Decision
Agenda Item:	7.2

1. Scope

This contribution incorporates the updates agreed during the discussion of Ericsson Tdoc S3-010626. The main difference with this contribution and the original proposal in Tdoc S3-010626 is that definition of Zb interface equals the one of Zc interface (definition of Zc interface is no longer required).

2. Proposed Changes

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

2 References

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

[1] 3G TS 21.133: Security Threats and Requirements

[2] 3G TS 21.905: 3G Vocabulary

[3] 3G TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2

[4] 3G TS 23.228: IP Multimedia (IM) Subsystem - Stage 2

[5] 3G TS 29.060: GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface

[6] 3G TS 33.102: Security Architecture

[7] 3G TS 33.103: Security Integration Guidelines

[8] 3G TS 33.120: Security Objectives and Principles

~~[9] 3G TS 33.200: Network Domain Security; MAP application layer security~~

[~~10~~9] 3G TS 33.203: Access security for IP-based services

[~~11~~10] RFC-2393: IP Payload Compression Protocol (IPComp)

[~~12~~11] RFC-2401: Security Architecture for the Internet Protocol

[~~13~~12] RFC-2402: IP Authentication Header

[~~14~~13] RFC-2403: The Use of HMAC-MD5-96 within ESP and AH

[~~15~~14] RFC-2404: The Use of HMAC-SHA-1-96 within ESP and AH

[~~16~~15] RFC-2405: The ESP DES-CBC Cipher Algorithm With Explicit IV

[~~17~~16] RFC-2406: IP Encapsulating Security Payload

[~~18~~17] RFC-2407: The Internet IP Security Domain of Interpretation for ISAKMP

[~~19~~18] RFC-2408: Internet Security Association and Key Management Protocol (ISAKMP)

[~~20~~19] RFC-2409: The Internet Key Exchange (IKE)

[~~21~~20] RFC-2410: The NULL Encryption Algorithm and Its Use With IPsec

[~~22~~21] RFC-2411: IP Security Document Roadmap

[~~23~~22] RFC-2412: The OAKLEY Key Determination Protocol

[~~24~~23] RFC-2451: The ESP CBC-Mode Cipher Algorithms

[~~25~~24] RFC-2521: ICMP Security Failures Messages

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

3.2 Symbols

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

Gi Reference point between GPRS and an external packet data network
Gn Interface between two GSNs within the same PLMN
Gp Interface between two GSNs in different PLMNs. The Gp interface allows support of GPRS network services across areas served by the co-operating GPRS PLMNs
Mm Interface between a CSCF and an IP multimedia network
Mw Interface between a CSCF and another CSCF
Za Interface between SEGs belonging to different networks/security domains
Zb Interface between NEs within the same network/security domain~~Interface between SEGs and NEs within the same network/security domain~~
~~Zc Interface between NEs within the same network/security domain~~
~~Zd MAPsec interface between KACs belonging to different networks/security domains~~
~~Ze MAPsec interface between KACs and MAP-NEs within the same network~~
~~Zf MAPsec interface between networks/security domains for secure interoperation.~~

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

4 Overview over UMTS network domain security for IP based protocols

4.1 Introduction

The scope of this section is to outline the basic principles for the network domain security architecture. A central concept introduced in this specification is the notion of a network security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks and hence separate security domains.

4.2 Protection at the network layer

For native IP-based protocols, security shall be provided at the network layer. The security protocols to be used at the network layer are the IETF defined IPsec security protocols as specified in RFC-2401 [12]. ~~All network domain entities supporting native IP-based control plane protocols shall support IPsec.~~

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 secure communication between security domains shall take place through Security Gateways (SEGs).

4.4 Security domains

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 and between NEs within the same security domain. When implemented, this 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.~~Network domain security interface between SEGs and NEs within the same network. The interface is used to route NDS/IP traffic from NEs to a SEG within the same security domain.~~ ~~This interface may additionally be 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.~~ ~~When implemented, this~~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~~

4.5 Security Gateways (SEGs)

Security Gateways (SEGs) are entities on the borders of the IP security domains and will be used for securing native IP based protocols. The SEGs are defined to handle communication over ~~these interfaces:~~the Za-interface, which is located between SEGs from different IP security domains. The IKE and ESP protocols shall be used over this interface.

- ~~the Zb-interface, which is located between a SEG and an NE within the same security domain. The IKE and ESP protocols may be used over this interface.~~

All NDS/IP traffic shall pass through a SEG before entering or leaving the security domain. Each security domain can have one or more SEGs. Each SEG will be defined to handle all traffic in or out of the security domain towards a well-defined set of reachable IP security domains.

The number of SEGs in a security domain will depend on the need to differentiate between the externally reachable destinations, the need to balance the traffic load and to avoid single point of failures. The security gateways shall be responsible for enforcing security policies for the interworking between networks. The security may include filtering policies and firewall functionality not required in this specification.

SEGs are responsible for security sensitive operations and shall be physically secured. They shall offer capabilities for secure storage of long-term keys used for IKE authentication.

***************************** ***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. 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. The SEG will maintain logically separate SAD and SPD databases for each interface.

The NEs ~~will~~ may be able to establish and maintain ESP secured tunnels as needed towards a SEG or other NEs within the same 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.

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.

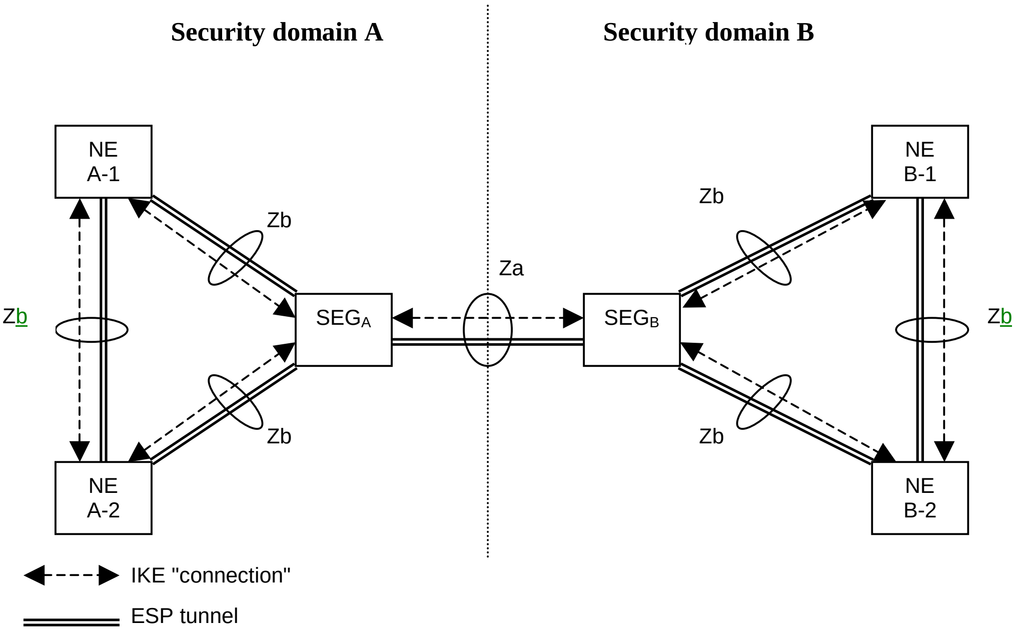

Figure 1: NDS architecture for IP-based protocols

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 IP 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 compliant with this specification 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. This interface is used to route all NDS/IP towards external destinations via a SEG.~~

~~The NE and the SEG are may be 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 traffic towards external destinations shall be routed via a SEG.~~

~~All security domains compliant with this specification shall operate the Zb-interface.~~

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

- **Zb~~c~~-interface (NE-SEG / NE-NE)**

  The Zb~~c~~-interface is located between SEGs and NEs and between NEs within ~~from~~ the same security domain.

  It is for the security domain operator to decide whether to implement Zb~~c~~-interfaces or not. If implemented, ~~T~~the NEs and SEGs~~are~~ shall be able to use IKE to negotiate, 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.