3GPP TSG SA WG3 Security — S3#22 **S3-020116**

25 - 28 February 2002

Bristol, UK

3GPP TSG SA WG3 Security – S3#ad-hoc Antwerpen **S3z020025**

Jan 31 – Feb 01, 2002

Antwerp, Belgium

Source: Alcatel

Title: SA mode in Zb interface

Document for: Adoption

Agenda item: 6.4

1 Introduction

TS 33.210 v 082 contains misleading and contradictory statements with regards to the use of tunnel or transport mode for the Zb interface in NDS/IP. This document suggests a p-CR that aims at solving the issue, according to the solution proposed in section 4 below.

2 Contradictions

TS 33.210 currently contains contradictory statements. Indeed :

- section 5.1 states that "In the UMTS NDS…the SA mode shall always be tunnel mode";
- section 5.2 states that "NDS/IP only requires support for tunnel mode SAs";
- section 5.5 also states that "…only one ESP tunnel is used between any two NEs or SEGs…"
- figure 1 only mentions "ESP tunnel" between NE boxes
- section 5.6.2 also refers to "ESP tunnels" only.

On the other hand, section 5.3.2 states that "The operators may support transport mode to protect communications between NEs within their own network (ie for the Zb-interface).".

Section 5.3.2 is therefore in contradiction with sections 5.1 and 5.2.

For cases where the term "ESP tunnel" is used, one could argue that this is a generic term to state that the traffic is put into an ESP payload but yet no definition of such a term exists and is therefore confusing.

3 Misleading Statement

Section 5.3.2 on its own is misleading when it states that "The operators may support transport mode to protect communications between NEs within their own network (ie for the Zb-interface).".

Indeed, Zb-interface now covers both NE-NE and NE-SEG interactions. From a technical point of view, use of transport mode would only make sense for NE-NE

interactions, hence not totally for the Zb-interface as the "(ie for the Zb-interface)" may imply.

4 Solution

It is first necessary to decide whether transport mode shall be allowed for protecting NE-NE interactions in the Zb interface. An alternative is to mandate the use of tunnel mode in all situations since this is also a technically valid solution (though consuming some more bandwidth with an extra IP header).

There is no strong reason to forbid the choice between both alternatives; therefore we suggest to allow both, as currently implied by the text in section 5.3.2. Consequently, the following modifications to various sections of TS 33.210 are proposed.

5 Pseudo-CR

5.1 Security services afforded to the protocols

IPsec offers a set of security services, which is determined by the negotiated security associations. That is, the SA defines which security protocol to be used, the SA mode and the endpoints of the SA.

In the UMTS NDS the IPsec security protocol shall always be ESP ~~and the SA mode shall always be tunnel mode~~. In NDS it is further mandated that integrity protection/message authentication together with anti-replay protection shall always be used.

The security services provided by NDS/IP:

- data integrity;
- data origin authentication;
- anti-replay protection;
- confidentiality (optional);

limited protection against traffic flow analysis when confidentiality is applied;

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].

5.3 5.3.2 Support of tunnel mode

Since security gateways are an integral part of the NDS/IP architecture, tunnel mode shall be supported. For NDS/IP inter-domain communication, security gateways shall be used and consequently only tunnel mode (RFC-2401, [12]) is applicable for this case.

The operators may support transport mode to protect communications between NEs within their own network ~~(~~in the ~~for~~ context of the Zb-interface~~)~~.

5.4 5.5 Security policy granularity

The policy control granularity afforded by NDS/IP is determined by the degree of control with respect to the ESP ~~tunnels~~ Security Association between the NEs or SEGs. The normal mode of operation is that only one ESP ~~tunnel~~ Security Association is used between any two NEs or SEGs, and therefore the security policy will be identical to all secured traffic passing between the NEs.

This is consistent with the overall NDS/IP concept of security domains, which should have the same security policy in force for all traffic within the security domain. The actual inter-domain policy is determined by roaming agreements. Security policy enforcement for inter-domain communication is a matter for the SEGs of the communicating security domains.

5.4.1 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~~ Security Associations in tunnel mode between security domains. 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 may be able to establish and maintain ESP ~~secured tunnels~~Security Associations 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 be afforded hop-by-hop security protection towards the final destination.

Operators may decide to establish only one ESP ~~tunnel~~ Security Association between two communicating security domains. 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. This does not preclude negotiation of finer grained security granularity at the discretion of the communicating entities.

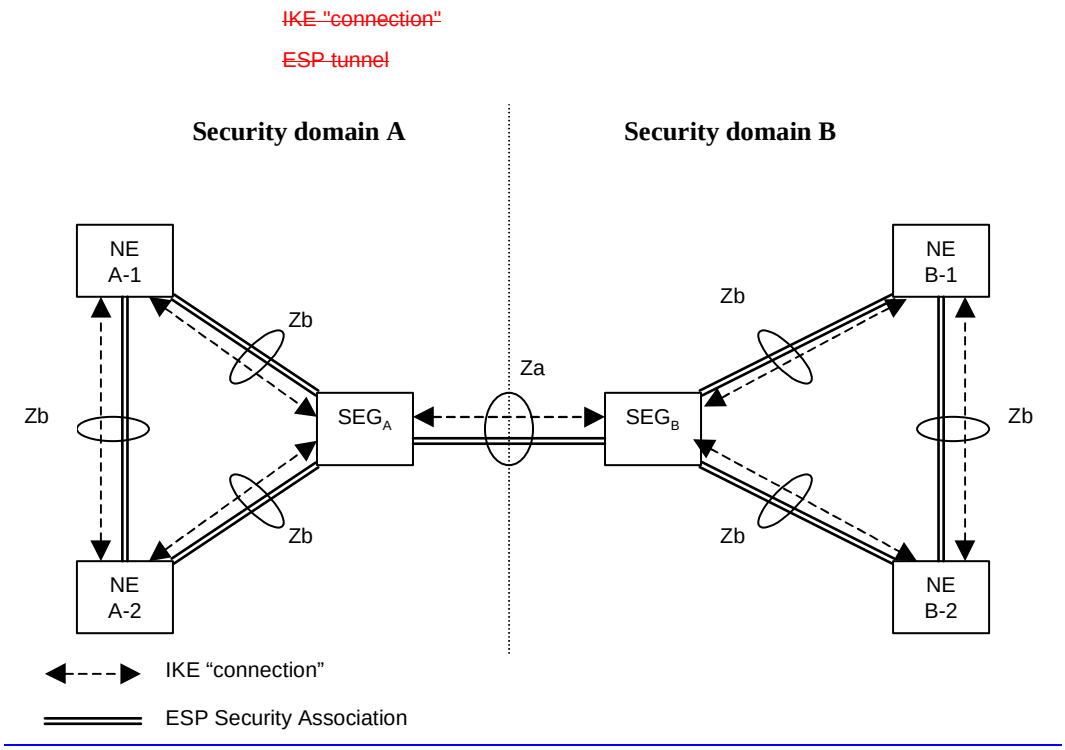

Figure 1: NDS architecture for IP-based protocols

5.4.2 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 NDS/IP traffic between security domains. The SEGs uses IKE to negotiate, establish and maintain a secure ESP 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. ESP shall be used with both encryption and authentication/integrity, but an authentictaion/integrity only mode is allowed. The tunnel is subsequently used for forwarding NDS/IP 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.

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

Editor' note: Interoperability is a primary issue over the SEG-SEG interface. It may be advantageuos to specify which IP version to use over the Za-interface in order to facilitate interoperability between security domains. This is an **open issue** which SA3 is to consider at SA3#22 (late February 2002).

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

The Zb-interface is located between SEGs and NEs and between NEs within the same security domain. The Zb-interface is optional for implementation. If implemented, it shall implement ESP+IKE.

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

Whether the ~~tunnel~~ Security Association is established when needed or a priori is for the security domain operator to decide. The ~~tunnel~~ Security Association is subsequently used for exchange of NDS/IP traffic between the NEs.~~.~~

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-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. It is observed that SEGs are responsible for enforcing security policies towards external destinations and that a combined NE/SEG would have the same responsibility towards external destinations. 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.