3GPP TSG SA WG3 Security — S3#17bis S3z010026

23-26 April, 2001

Madrid, Spain

Source: Nokia

Title: Proposed changes to 33.200 about Za, Zb, Zc interfaces

Document for: Discussion

Agenda Item: 8

This contribution proposes enhancements on the key management structure for IPSEC. It is edited with change markers against 33.200 v. 0.3.5.

.

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

5.3.1 Network domain security architecture outline

The UMTS key management and distribution architecture is based on the IPsec IKE [13,19,20,21] 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 the UMTS network domain control plane. Furthermore, some features that are optional in IETF IPsec have been mandated for NDS and lastly a few required features in IETF IPsec have been deprecated for use within NDS scope. Annex A gives an overview over the usage of IPsec in NDS.

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

The basic idea to the NDS 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 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 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.

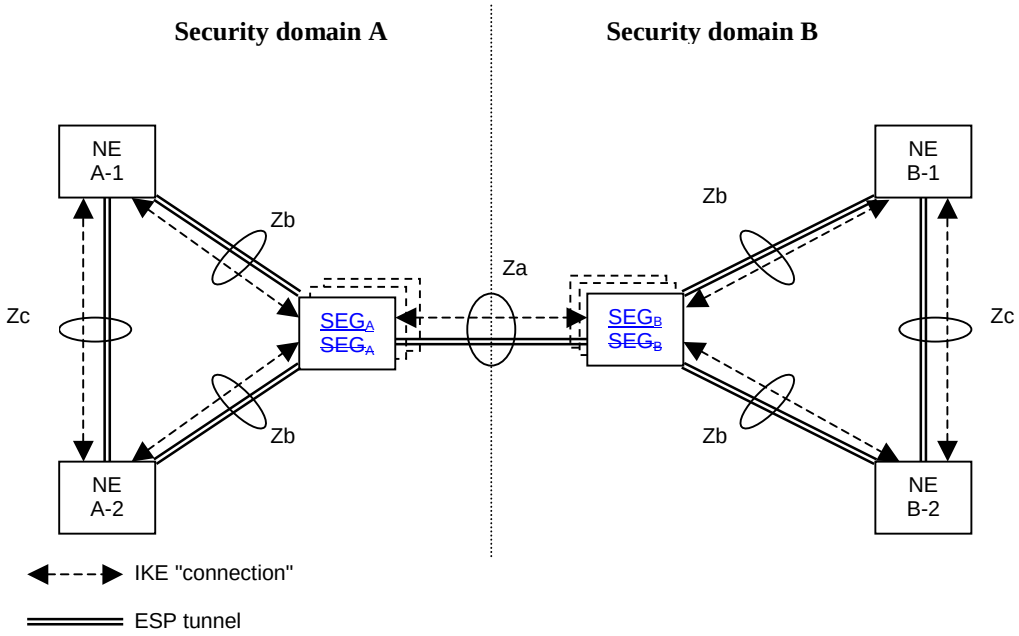

Figure 1: NDS architecture for IP-based protocols

5.3.2 Interface description

The following interfaces is 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. This tunnel is subsequently used for forwarding secured traffic between security domain A and security domain B.

  To avoid a single point of failure, each Za interface can be implemented via several alternative SEGs (see Figure 1). Regardless of the internal implementation (i.e. number of physical SEGs), only one (logical) SEG shall be visible at each end of this interface.

  ~~One~~To balance the overall load, each SEG can also 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.

- **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 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 between security domains (e.g. 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 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. 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.~~

.