3GPP TSG SA WG3 Security — S3#17bis S3z010027

23-26 April, 2001

Madrid, Spain

Source: Nokia

Title: Proposed changes to 33.200 about KAC

Document for: Discussion and decision

Agenda Item: 7.5

This contribution proposes enhancements on the key management structure for MAPSEC. It is edited with change markers against 33.200 v. 0.4.0.

5.4 UMTS key management and distribution architecture for SS7 and mixed SS7/IP-based protocols

The following section specifies the generic parts of the key management and distribution architecture for SS7 and mixed SS7/IP-based protocols. Due to the fact that the security mechanisms are found on the application layer a number of the issues are unique to the application. Section 7 contains detailed and specific requirements for the applicable application protocols.

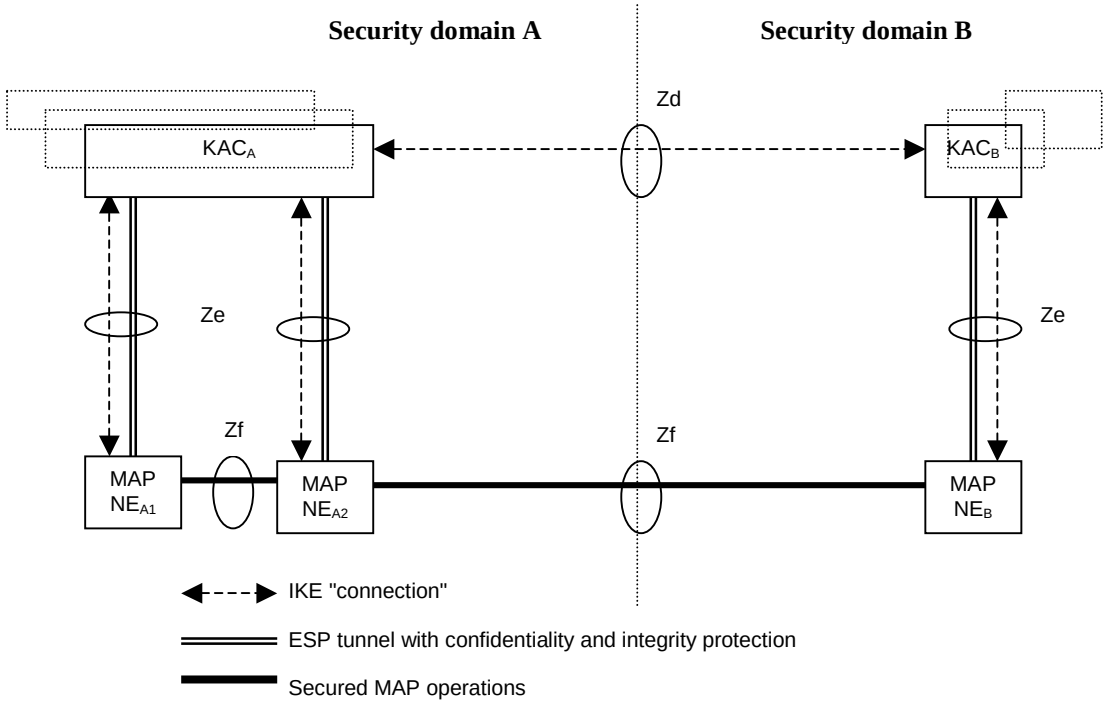

Figure 2: Overview of the Zd, Ze and Zf interfaces

For Rel4 the only SS7 protocol to be protected is the MAP protocol. References to MAP security (MAPsec) may therefore be extended to be more generic in later releases.

The following interfaces are defined MAPsec.

- **Zd-interface (KAC-KAC)**

  The Z-d-interface is used to negotiate MAPsec Security Associations (SAs) between MAP security domains. The traffic over Zd consists only of IKE negotiations. The negotiated MAPsec SAs are valid on a security domain to security domain basis.

  To avoid a single point of failure, each Zd interface can be implemented via several alternative KACs (see Figure 2). Regardless of the internal implementation (i.e. number of physical KACs), only one (logical) KAC shall be visible at each end of this interface.

- **Ze-interface (KAC-NE)**

  The Ze-interface is located between MAP-NEs and a KAC from the same MAP security domain. The KAC and the MAP-NE are able to establish and maintain an ESP tunnel between them. Whether the tunnel is established when needed or a priori is for the MAP security domain operator to decide. The tunnel is subsequently used for transport of MAPsec SAs from the KAC to the MAP-NE.

- **The Zf-interface (NE-NE)**

The Zf-interface is located between MAP-NEs. The MAP-NEs may be from the same security domain or from different security domains (as shown in figure 2). The MAP-NEs use MAPsec SAs received from a KAC to protect the MAP operations. The MAP operations within the MAP dialogue are protected selectively as specified in the applied MAPsec security profile.

NOTE: It is explicitly noted that there is no Rel4 requirements for support of KACs or the associated Zd/Ze-interfaces. KACs and its associated interfaces and protocols will only be introduced in Rel5. For Rel4 this section is only for information.