3GPP TSG SA WG3 Security — S3#22 **S3-020062**

25 - 28 February 2002

Bristol, UK

Title: **Clarification of MAP security text**

Source: **Rapportuer (A. Escott)**

4 Principles of MAP application layer security

This technical specification defines mechanisms for protecting the MAP protocol at the application layer. The MAP protocol may also be protected at the network layer when IP is used as the transport protocol. However, whenever inter-working with networks using SS7-based transport is necessary, protection at the application layer shall be used.

The security measures specified in this TS are only fully useful if all interconnected operators use them. In order to prevent active attacks all interconnected operators must at least use MAPsec with the suitable protection levels as indicated in this specification and treat the reception of all MAP messages (protected and unprotected) in a uniform way in the receiving direction.

Before protection can be applied, Security Associations (SA) needs to be established between the respective MAP network elements. Security associations define, among other things, which keys, algorithms, and protection profiles to use to protect MAP signalling. The necessary MAP-SAs between networks are negotiated between the respective Key Administration Centres (KACs) of the networks. The negotiated SA will be effective PLMN-wide and distributed to all network elements which implement MAP application layer security within the PLMN. Signalling traffic protected at the application layer will, for routing purposes, be indistinguishable from unprotected traffic to all parties except for the sending and receiving entities.

Figure 1 gives an overview of the architecture used for MAPsec.

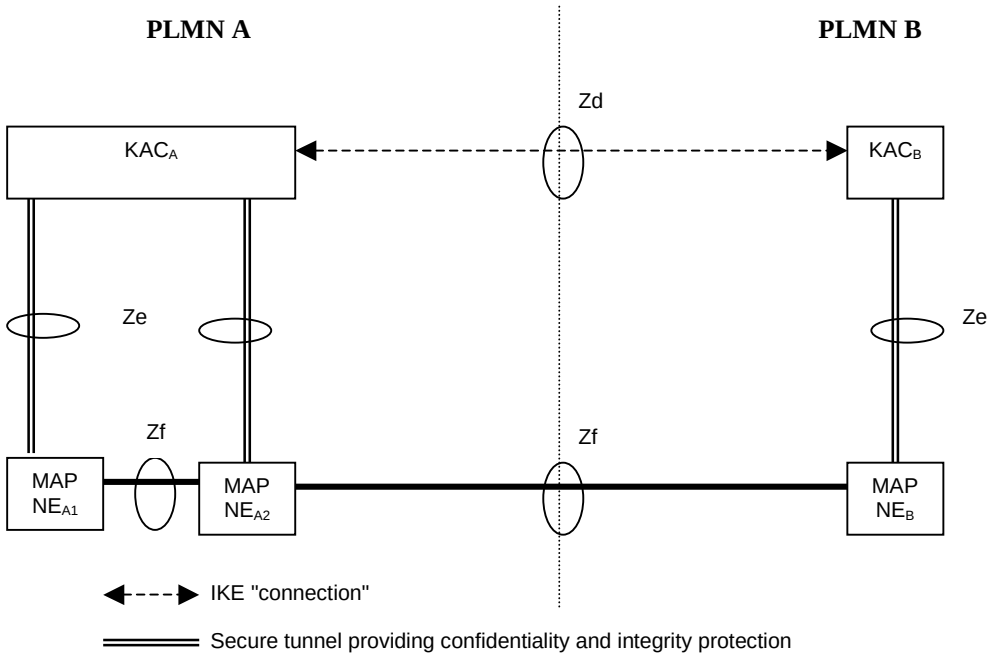

Figure 1: Overview of the Zd, Ze and Zf interfaces

The following interfaces are defined MAPsec.

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

  The Zd-interface is used to negotiate MAPsec Security Associations (SAs) between PLMNs. The traffic over Zd consists only of IKE negotiations. The negotiated MAPsec SAs are valid on a PLMN to PLMN basis.

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

  The Ze-interface is located between MAP-NEs and a KAC from the same PLMN. This interface is used for transport of MAPsec SAs and the relevant security policy information from the KAC to the MAP-NE. The KAC and the MAP-NE shall be able to communicate ~~are able to establish and maintain a~~ securely ~~tunnel between them~~. Whether the ~~tunnel~~security is established when needed or a priori is for the PLMN operator to decide.

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

  The Zf-interface is located between MAP-NEs. The MAP-NEs may be from the same PLMN or from different PLMNs (as shown in figure 1). 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 protection profile. The interface applies to all MAPsec transactions, intra- or inter-PLMN.

The security services provided by MAPsec are:

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

Annex B includes detailed procedures on how secure MAP signalling is performed between two MAP-NEs.

5 MAP security (MAPsec)

5.1 Properties and tasks of Key Administration Centres (KACs)

Key Administration Centres (KACs) are entities that are used for negotiating MAPsec SAs on behalf of MAP-NEs. The KACs are defined to handle communication over these interfaces:

- the Zd-interface, which is located between KACs from different PLMNs. The IKE protocol with support for MAPsec DoI shall be used over this interface.
- the Ze-interface, which is located between a KAC and a MAP-NE within the same PLMN is used to transfer MAPsec SAs and security policy from KACs to MAP-NEs. The SAs and security policy must be transferred in a secure manner.

When a MAP-NE needs to establish a secure connection towards another MAP-NEs it will request a MAPsec SA from the KAC if it cannot find any appropriate MAPsec SA in its local SAD. The KAC will then either provide an existing MAPsec SA or negotiate a new MAPsec SA, before returning the MAPsec SA to the MAP-NE.

A MAPsec SA is valid for all MAP communications between the two PLMNs for which it is negotiated. That is, the same MAPsec SA shall be provided to all MAP-NEs in PLMN A for communication with MAP-NEs in PLMN B. Each PLMN can have one or more KACs. Each KAC will be responsible to define MAPsec SAs with a well-defined set of

reachable PLMNs. The number of KACs in a PLMN will depend on the need to differentiate between the externally reachable destinations, the need to balance the traffic load and to avoid single points of failure.

KACs perform the following operations:

- Negotiate SAs for MAPsec with other KACs belonging to other network operators. This action is triggered either by request for a MAPsec SA by a NE or by policy enforcement when MAPsec SAs should always be available. The negotiation of MAPsec SAs is performed at Zd-interface using IKE protocol with MAPsec DoI.
- Convert specific negotiated SA parameter so that they can be understood by NEs. In particular, the KAC shall convert negotiated SA duration in seconds as negotiated in MAPsec DoI to UTC absolute time format.
- Perform refresh of MAPsec SAs. This could be triggered internally by SA lifetime supervision depending on the policies set by the operator.
- Distribute MAPsec SAs and policy information to NEs belonging to the same PLMN as the KAC.
- KAC shall~~may~~ be able to ~~establish~~ securely ~~connections to~~ transmit MAPsec SAs and policy information to the NEs within its PLMN.

KACs are also responsible for the maintenance of the following databases:

- KAC-SPDB-MAP: Defines the scope, the security policy, in which MAP-SAs may be negotiated (e.g. allowed MAP-PPs, Algorithms, SA-lifetimes). This database is updated on operator initiative in the framework of the roaming agreements.
- NE-SPD-MAP: A database in a KAC containing the MAP security policy information that will be used by an NE in protecting MAP messages (e.g. value of “Fallback to unprotected Mode Indicator” and table of protected MAPsec operation components). This is held to update the NEs.
- NE-SADB-MAP: A database in a KAC containing MAP-SA information. This is held to allow the KAC to update the NE.

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

5.2 Properties and tasks of MAPsec enabled network elements

MAPsec MAP-NEs shall maintain the following databases:

- NE-SPD-MAP: A database in an NE containing MAP security policy information (see clause 5.3);
- NE-SADB-MAP: A database in an NE containing MAP-SA information. MAP-NEs shall monitor the SA hard expiry time and expired SAs shall be deleted from the database (see clause 5.4).

MAPsec MAP-NEs shall be able to perform the following operations:

- Secure MAP signalling (i.e. send/receive protected or unprotected messages) according to information in NE-SPD-MAP and NE-SADB-MAP. The structure of protected messages is defined in clause 5.5 and the protection algorithms are defined in clause 5.6.
- Communicate with the KAC in the same PLMN in order that the NE-SPD-MAP and NE-SADB-MAP in the NE can be updated.
- NE ~~must~~ shall be able to ~~establish a~~ securely ~~connection to~~ receive MAPsec SAs and policy information from the KAC within its PLMN.

8 Local Security Association and Policy Distribution

The KAC transmits SAs and security policy information to the NEs in the same PLMN. The method of transmitting this data to the NEs must satisfy the following requirements

- The push mechanism requires the KAC to maintain active SAs with all other networks that MAP signalling is exchanged with. The KAC internally supervises the SA lifetime and performs automatic SA renewal with all other networks that MAP signalling is exchanged with.

- If new SAs are available, the KAC distributes these SAs to the NEs that require them, according to the KAC policy. The KAC ~~must~~ shall provide fresh SAs to its NEs for a specific network in time before the soft expiry time of the current active SA has been reached.

- The NEs ~~must~~ shall ensure that only Ze-messages sent by a KAC in the same security domain are accepted. Depending on the security domain policy, the NE may only accept Ze-messages from one or more specific KACs within the domain, out of the set of KACs in that domain.

- The KAC ~~must~~ shall ensure that only Ze-messages sent by a NE in the same security domain are accepted (Otherwise an attacker could, e.g. by sending false messages, force the KAC to overload the NE's)

- The KAC shall be able to know whether the MAP-NE needs only MAP-SA's for security domain internal communication or not.

- ~~All messages over~~ The Ze interface shall~~ould be~~ provide protection against the insertion of or tampering with messages by an attacker. Furthermore messages containing sensitive information shall be protected from eavesdropping. This security could be achieved by cryptographic or other means as appropriate. ~~integrity and confidentiality protected, as they contain sensitive data or trigger messages containing sensitive data, although integrity protection may be sufficient for trigger messages.~~