3GPP TSG SA WG3 Security S3-000668

Plenary meeting S3#16

Sophia Antipolis, 28-30 November, 2000

**Source:** Ericsson

**Title:** IKE negotiation of SAs over the $Z_a$ interface

**Document for:** Discussion and Decision

**Work item:** Network domain security

**Agenda item**: tbd

**Abstract**

*This contribution presents the results of an analysis of the potential problems foreseen in the contribution S3z000021 presented for the S3 Ad-hoc meeting S3#15bis held in Munich on November 8-9, 2000.*

*That contribution questioned the feasibility of IKE being used as the $Z_c$-SA negotiation protocol between KACs, i.e. over the $Z_a$ interface, in the two-tiered architecture agreed upon by S3.*

*This contribution compare the assumptions made in the S3z000021 contribution with the intended scope of the contribution originally introducing IKE negotiation to the two-tiered model (S3-000432). Furthermore, this contribution analyse the possibility to support a scope like the one described in S3z000021 using the IKE framework for $Z_c$-SA negotiation over the $Z_a$ interface, and concludes that the IKE protocol still meets the requirements imposed.*

## 1 Introduction

The two-tiered model was introduced to address the key management issue for the new version of the MAP protocol securing the transport of sensitive data over the SS7 network. It was identified that there were significant advantages of using a centralized model for the negotiation, establishment and maintenance of security associations, SA, between networks, since this would leverage potential addressing and routing problems as well as simplify the key management process. Thus the Key Administration Center, KAC, entity was introduced to take the responsibility of handling the entire key management process.

In order to enable a rapid architecture development, as well as for reasons of future migration scenarios moving the MAP traffic from the SS7 network to an IP based network, IKE was found a preferred protocol to handle the negotiation of MAP-SAs and was introduced by the Ericsson contribution S3-000432. In this contribution were also the security interfaces $Z_a$, $Z_b$ and $Z_c$ introduced (where $Z_a$ is the interface between two KACs, $Z_b$ is the interface between a KAC and a network element, and $Z_c$ is the interface between the two MAPsec enabled NEs).

In Ericsson's contribution S3-000434 it was suggested to migrate the key management concept developed for MAP security to be valid also for the more general scope of Network Domain Security. A new entity, the security gateway, SEG, was introduced (actually it was mentioned as a migrated KAC in that contribution). Later S3 has agreed that the two entities, KAC and SEG, should remain logically

separated. This requires the introduction of a new interface, $Z_d$, which is the interface between two SEGs.

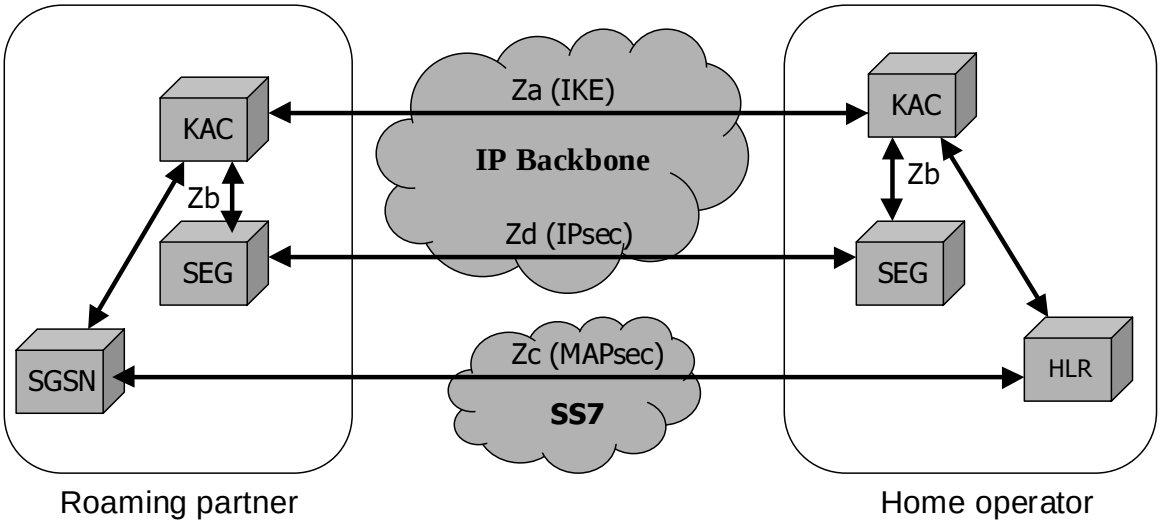


Fig 1. Proposed reference model for security interfaces

S3 has also stated that it should be possible for an operator to allow security connections directly between network elements without passing through the SEG. Since such a connection does not imply new entities in the transportation path, all modifications (such as adding the appropriate security protocol etc) should be included in the original specifications defining the relevant interface.

Should a problem using a separate KAC for such a connection arise, it has to be clarified that the current security architecture does not prohibit the functional entity KAC (or functional entity SEG for that matter) to be co-located with (distributed to) the network elements.

## 2 The intended scope of IKE in the two-tiered model

The SEG was originally introduced in order to leverage the key management required for the scope of WI Network Domain Security, by acting as an aggregation point for all IP traffic passing the network border and enforce the SAs negotiated with other networks.

Just as the solution for MAP security is built on the notion of a single network-wide SA, the SEG was introduced to achieve that very same thing for the more general case when IPsec is applied.

Ericsson appriciate, though, that there might be a desire to set up parallel SAs (IPsec tunnels), for example to separate different types of traffic. Such separation is likely to be based on either the interface (Gi, Gp…) or the protocol (GTP, CAP…).

## 3 Some IKE negotiation parameters

The *Situation* field in the ISAKMP header is used to define what type of information should be used to identify the Security Association being negotiated. When the KAC is negotiating a SA it should set the *Situation* field to the value SIT_IDENTITY_ONLY.

This indicates that the source identity information provided in an ISAKMP *Identification payload* will be used to identify the SA. The *Identification payload* esentially consist of the *Identification type* parameter, a payload length parameter and the *Identification data* field.

Allowed values of the *Identification type* parameter is defined in the Domain of Interpretation, DOI, used. The KAC should typically use either the value ID_IPV4_IP_ADDR_SUBNET or ID_IPV6_ADDR_SUBNET depending on the IP version use. The *Identification data* will then consist of an IP address and a network mask. One alternative way is to set the Identification type field to ID_FQDN, which indicates that the Identification data field consists of a Fully Qualified Domain Name, FQDN, (e.g. GTP.OPERATOR_A.NET or GP.OPERATOR_B.COM), which could be used in conjunction with the DNS system.

At the end of the SA negotiation each KAC assigns an unique Security Parameter Index, SPI, connected to the inbound SA and forwards it to the other KAC as part of the SA itself. The SPI should be sufficient identification of the SA, unless otherwise is stated in the DOI.

## 4 The capability of IKE to support the extended scope of S3z000021

In the contribution S3z000021 a new aspect/flexibility is introduced to the original concept of the two-tiered model, allowing the two KACs to negotiate SAs unique for a specific network entity pair.

This will not cause the IKE negotiation mechanism to fail, though. The only real difference from the original case briefly discussed in chapter 3 is that the KACs should choose to set the ISAKMP *Identification type* field to either ID_IPV4_ADDR, or ID_IPV6_ADDR, as appropriate. This will mean that the *Identification data* field of the ISAKMP *Identification payload* will consist of just a single IP address, i.e. the address of the network entity that will ultimately use the SA being negotiated.

Even though this type of SA setup is fully supported by the IKE based key management scheme, it should be pointed out that such a strategy will significantly increase the total number SAs required for a system.

## 5 Conclusion

Ericsson propose to denote the IPsec (IP/ESP) based SEG-to-SEG interface, $Z_d$, in order to separate it from the MAPsec/SS7 based NE-to-NE interface $Z_c$.

Furthermore, Ericsson believes it has been shown in this contribution that IKE still seems well suited to handle the $Z_c$ and $Z_d$ SA negotiation between KACs (over the $Z_a$ interface), and therefore proposes that IKE should remain the main mechanism to use for this task.