3GPP TSG SA WG3 Security — S3#15 **S3-000560**

12-14 September, 2000

Washington D.C., USA

Source: Siemens AG

Title: Key management for core network security

Document for: Discussion and decision

Work item: Key management for core network security

Agenda item: tbd

Abstract

This contribution further elaborates on the conclusions of the Siemens-contribution S3-000445 presented at S3#14 and takes into account other contributions presented at S3#14. For a rationale of the conclusions, please refer to S3-000444. This contribution proposes a two-tiered key management for the UMTS core network. Text is proposed for eventual inclusion in the standards.

1. Introduction

In the Siemens contribution S3-000445 we proposed a two-tiered key management architecture for the UMTS core network. This was accepted as a working assumption by SA3. This contribution further elaborates on this. We propose to include the text of the following section 2 in the appropriate chapter on " Two-tiered key management" in the permanent document which is to be maintained on this work item. This text is meant to be eventually included in the 3GPP specification handling core network security.

The notation introduced in S3-000432 (Ericsson) which denotes the interfaces between KAC and NE entities as Z_A, Z_B and Z_C is adopted for the purpose of this document, although the definitions are slightly different.

2. Two-tiered key management

The two-tiered key management architecture consists of two types of functional entities: key administration centres (KACs) and network entities (NEs). Security Gateways are considered a special kind of NEs. Each network includes at least one KAC[1]. Communication for two-tiered key management uses two interfaces, Z_A and Z_B, where Z_A connects different KACs and Z_B connects KACs with network entities (NE). Z_C is an interface between two network entities (NEs) which is to be secured.

- KACs communicate over Z_A to establish security associations (SA) for security protocols used over Z_C between two NEs in different networks. If the two NEs reside in the same network then one KAC may establish the required SAs, and communication between two different KACs over Z_A is not needed.
- Over Z_B these SAs are securely distributed from a KAC to NEs within the same network.
- The security protocols used over Z_C protect legacy or native IP-based application layer protocols. These security protocols are specified in [doc/section, tba]. They include MAP/CAP security and IPsec.

---

[1] It is ffs whether it may be useful to have more than one KAC in a network.

- Security policy information is exchanged between KAC and NEs over Z_B. This information is required in the KAC and in the NEs, respectively, and depends on the security protocol used over Z_C. The definition of the security policy format for each security protocol can be found in [doc/section, tba].
- To secure SA negotiation and distribution, the two-tiered key management over Z_A and Z_B uses the IETF IPsec framework, cf. [IETF rfc2401, "Security architecture"].
- The KAC and all participating NEs must have an IP interface and support IPSec (AH and ESP) over the interfaces Z_A and Z_B. IPsec (AH and ESP) use the SA format described in IETF RFC 2407 when used over any of the interfaces Z_A, Z_B, or Z_C.
- A specification of the SA format for application layer security protocols over Z_C, such as MAP security (cf. [doc/section, tba]) can be found in [doc/section, tba].

Z_A interface:

SAs for Z_C shall be established with IKE/IPsec between the KACs of different networks. The exact mechanism for SA establishment is described in [doc/section, tba]. According to the SA type required by the NEs for communication over Z_C, the KACs use the respective SA format for SA negotiation.

The implementation of IKE shall conform to IETF RFC 2409. In particular, for IKE Phase 1, authentication via preshared secrets must be supported, support for other authentication methods is optional.

The KACs must be able to provide two classes of SAs to support inter- and intranetwork security over Z_C for NE and SEG entities:

- Class 1 SAs are NE-NE, SEG to NE or NE-SEG where both entities reside within the same network.
- Class 2 SAs are SEG-SEG where the SEGs reside in two different networks.

In addition, the KAC may be able to provide a third class of SAs to support inter-network security over Z_C for NEs:

- Class 3 SAs are NE-NE where the NEs reside in two different networks.

Note, that IPsec AH and ESP require an individual SA pair for each NE pair protected over Z_C. It is not possible to secure communication between more than one pair of NEs with a single SA pair. Furthermore, it is not possible to secure communication between NE pairs where NEs have more than one IP address (multi-homing), with a single SA pair.

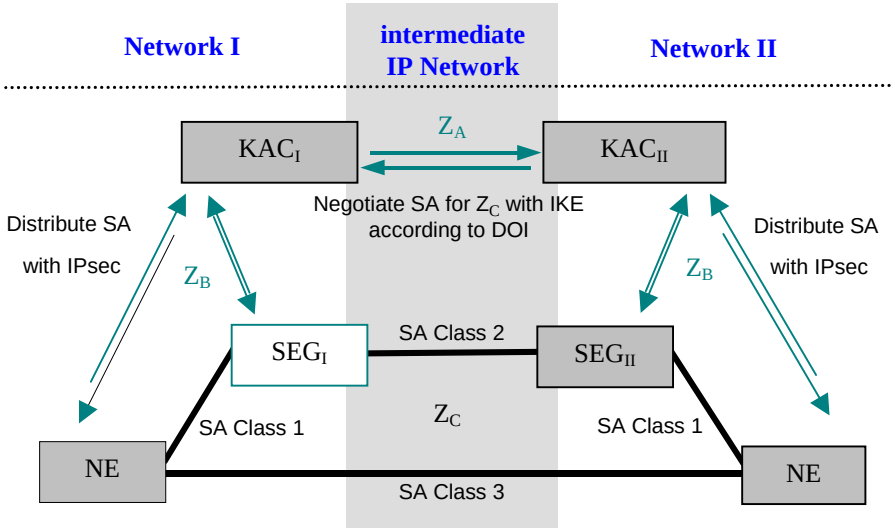

Figure 1: Two-tiered core network key management architecture

Z_B interface:

On the Z_B interface, IPsec shall be used to provide a secure channel between a KAC and an NE (or SEG) for

distribution of the SAs used to secure Z_C and for exchanging the related policy information. If an automated key management with support for replay protection in IPsec is needed, IKE should be used. The implementation of IKE for the Z_B interface shall conform to IETF RFC 2409. If IKE is used for automated key management then, for IKE Phase 1, authentication via preshared secrets must be supported. Support for other authentication methods is optional. The specification of the Z_B interface is described in [doc/section, tba].

NOTE: The proposed two-tiered model can be completely based on preshared symmetric keys for authentication or can use the public key authentication mechanisms of IKE. Using preshared symmetric keys means the KACs or NEs do not need to perform public key operations. Furthermore, no need for establishing a PKI (public key infrastructure) will arise for introducing core network security. But a smooth migration path from two-tiered to PKI-based security for later phases of UMTS development is possible.(cf. [doc/section, input from S3-000445, section3])

3. Conclusions and open issues

The following has been proposed in this contribution:

- The use of a two-tiered key management for all core network security protocols;
- The use of Key Administration Centres to establish network-internal and network-external security associations for the Z_C interface
- The use of IKE/IPsec over the Z_A interface to derive security associations for the Z_C interface between networks
- The use of IPSec to secure the Z_B interface
- The optional use of IKE to establish security associations for the Z_B interface
- The definition of a security policy format for each security protocol used over Z_C.

Furthermore, it is proposed to include the text of section 2 in the permanent document which is to be maintained on this work item. This text is meant to be eventually included in the 3GPP specification handling core network security.

The KAC mechanism to establish SAs for security protocols over Z_C is still regarded as an open issue:

- The first possibility to support IPsec replay protection for Z_C (which then requires automated keying) would be to negotiate the SAs between KACs with IKE as phase 2 SAs and pass them over Z_B to the NEs. To run IKE and the IPsec kernel (AH, ESP) on different logical entities is not the intention of the IPsec framework. It would necessitate to provide appropriate interfaces between the IKE entity, the IPsec kernel and the policy management component. Although this approach seems to be possible, it first has to be studied more careful whether it is in conflict with the IPsec RFCs and whether the implementation of such a system is possible.
- The second possibility is to establish a secure channel between the KACs and negotiate the SAs for ZC over this secure channel. This would require the specification of a new proprietary protocol for SA negotiation.

We prefer the first approach, under the reservation that the feasability of this approach can be shown and it does not offend the IPsec RFCs.