3GPP TSG SA WG3 Security — S3#14 **S3-000445**

2-4 August, 2000

Oslo, Norway

Source: Siemens AG[1]

Title: Key management for core network security

Document for: Discussion and decision

Work item: Key management for core network security

Agenda item: tbd

Abstract

The contribution proposes a two-tiered key management for the UMTS R'00 network domain, using the architecture – but not the protocols - described for MAP security in [1]. Key distribution will be done on layer I between key administration centres of different networks , and on layer II between the key administration center and network elements of the same network. Both layer I and layer II will be secured by means of IPSec. A possible migration path that leads towards a PKI-based key management is sketched.

1. Introduction

A key management architecture consisting of three layers was proposed in [1] for supporting MAP security in the core network. Layer III just represents the secure MAP protocol, which exchanges messages between two network entities (NE) and has a requirement for preshared symmetric keys. The distribution of these keys in a network and between different networks happens on layers I and II, where

- layer 1 exchanges symmetric keys securely between two different networks.
- layer 2 distributes these keys securely to NEs within the same network.

It should be mentioned here that the exchange of keys is only part of what needs to be agreed between the KACs and distributed to the NEs. In fact, what needs to be agreed and distributed are security associations which still have to be defined.

The KAC (key administration center) is defined as the central instance of a network for layer I and II key distribution. Each network includes one KAC, which runs layer II exchanges with the NEs within the same network and layer I exchanges with KACs of different networks.

In UMTS R'00, besides MAP, several IP-based protocols will require security services as well. Hence, IPsec[2] is likely to become part of the core network (see our companion contribution on core network security).

This contribution describes an approach for a unified key management supporting MAP security and IP security on layer III.

[1] This document is partly based on work carried out in the EU-sponsored collaborative research project USECA (http://www.useca.freeserve.co.uk/). Nevertheless, only the author is responsible for the views expressed here.

2. Two-tiered key management

The basic prerequisite for the proposed architecture is that all NEs including the KACs have an IP interface. Given this infrastructure, it can be avoided to build several independent key management solutions supporting different security protocols in the core network.

Note, that the term *network element (NE)* is not only used for end-entities (e.g. VLR, HSS), but also for intermediate entities like gateways.

The two-tiered key management architecture is basically similar to [1]. Layer I agrees security associations (SA) between different networks and layer II distributes these SAs between the KAC and all participating NEs in the same network. On layer III, MAP security and IPsec as well as other security protocols based on symmetric keys may be supported. In addition to secret keys, an SA can describe algorithms, replay protection parameters or lifetimes etc. The NEs use the layer III SAs for secure communication at layer III. For IPsec, we use the SA format as described in the IETF standards. A specification of the SA format for other security protocols, i.e. MAP on layer III will be required.

For securing transport of layer III SAs, on layer I and II SAs have to exist as well. Therefore, the different nodes must share the following SAs:

- KACs share layer I SAs with other KACs to protect layer I exchanges
- KACs share layer II SAs with each participating NE of the same network to protect layer II exchanges
- NEs share layer II SAs with the KACs of their networks
- NEs share layer III SAs with other NEs

It is proposed to use IP-based communication for layer I and II, secured by IPsec.

Only this solution seems to offer the advantages of a unified key management.

Several issues remain to be resolved if this fundamental proposal is accepted. These issues need further discussion.

LAYER I:

Protocol to agree Layer III SAs between KACs: Layer III SAs could be established in two ways:

1) using IKE between the KACs to establish layer III SAs. This would necessitate the definition of new Domains of Interpretation of IKE for all layer III protocol but IPsec.
2) using IKE to establish layer I IPsec SAs between KACs. With these SAs, IPSec secures the communication between KACs. Then a protocol to establish Layer III SAs between KACs over this secure channel would need to be defined.

In any case, choices for IKE have to be made:

Preshared secret keys vs. certificates: IKE on layer I may be – at leasts initially - based on preshared secret keys as described in [4, 5.4]. These preshared secret keys could be exchanged by any out-of-band mechanism with setting up a roaming between the networks. Alternatively, especially in later phases, certificate-based solutions for IKE could be introduced.

Mode of IKE: Since IKE phase 1 negotiation is unlikely to happen very often between KACs, IKE phase 1 may be used in main mode which has the advantage of hiding the KACs identities during negotiation.

If 2) is used a choice of the IPSec protocol has to be made:

AH vs. ESP, mode: Confidentiality is required so ESP needs to be used. The potential additional use of AH and the mode (transport vs. tunnel) need to be decided.

LAYER II:

On layer II, IPsec AH/ESP shall be used to provide a secure channel for layer III SA transport as well.

An open issue is the IPsec SA establishment on layer II. The three possibilities are:

- Use IKE. This would require all NEs to support IKE from R‘00
- Specify another protocol for IPsec SA negotiation for layer II. This could require a large effort for specification and verification.
- Manually exchange layer II SAs. This may be acceptable in an initial phase due to the relatively small number of NEs requiring protection in a network. AH/ESP anti-replay protection cannot be used on layer II with manual keying. A proprietary mechanism for anti-replay protection would have to be specified.

Note, that with IPsec securing layer I/II, there is still no mechanism defined for negotiation and distribution of the layer III SAs. Such a mechanism is required for any two-tiered solution and affects both layer I and layer II. It has to be specified by 3GPP.

LAYER III:

Since layer III SAs are not negotiated between the NEs itself (i.e.they are manually keyed in IPsec terms), IPsec AH or ESP will not provide anti-replay protection on layer III. As for layer II, this could be solved by specifying a proprietary mechanism for anti-replay protection at layer III, or by using IKE directly between the NEs at layer III. In this case, the keys provided by Layer I/II are not used for AH/ESP, but for IKE based on preshared secret keys. IKE then dynamically negotiates IPsec SAs between the NEs and therefore supports anti-replay protection.

It needs further studywhether to use IKE on layer II or layer III.

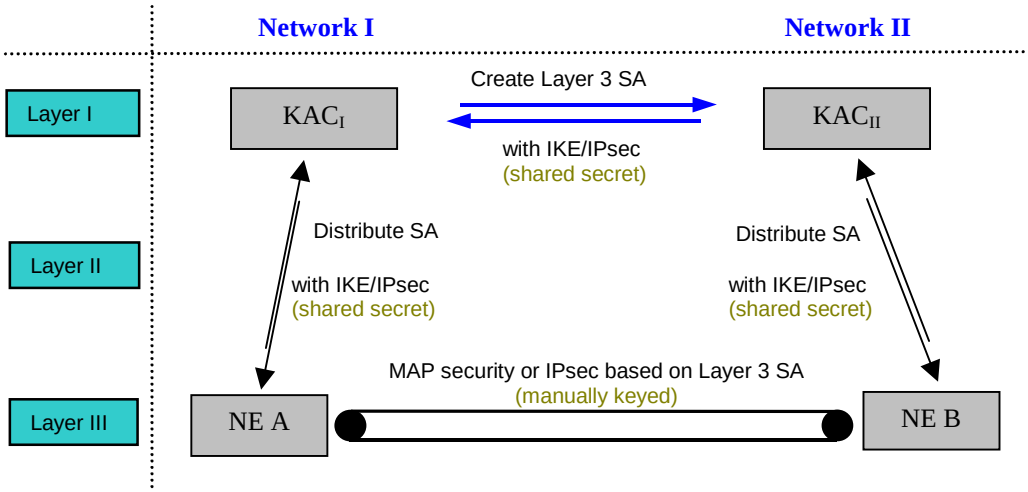

Figure 1: Proposed architecture for UMTS R’00 two-tiered core network key management

Since key management is independent from the question how exactly layer III communication can be secured, figure 1 abstracts layer III by just showing two network entities. A security gateway (SG, cf. our companion contribution on core network security protocols) is also a NE in this context, and NEs can be located in the same or in different networks. So the proposed two-tiered key management as well as the flat key management illustrated in the next section, support all possible combinations of layer III entities (e.g. end entity-to-end entity or end entity-to-SG or SG-to-SG), meaning that these entity pairs could obtain a SA from the respective KACs (two-tiered) or negotiate it directly between them using IKE (flat).

The proposed two-tiered model can be completely based on shared symmetric keys for authentication and therefore does not require the KACs or NEs to perform a large number of costly public key operations. Furthermore, no need for establishing a PKI (public key infrastructure) will arise for Release 00. A migration path to PKI-based security for later phases of UMTS development is sketched in the next section.

3. Migration path to PKI-based flat key management

In the Internet world, key management more and more happens within a PKI environment. Bulk data is usually encrypted by symmetric key mechanisms, but authentication and key agreement is usually based on public key schemes. In this section, we sketch a “flat” key management architecture in which there is no need for KACs any more.

Such an architecture rests on two assumptions:

- The availability of a PKI which allows to issue certificates to all NEs
- The use of IPSec between all the NEs

These assumptions make it obvious that the solution presented in this section is suitable only for the medium to long term , since MAP security on application layer is not supported by flat key management, and therefore interoperable security between MAP over IP and MAPover SS7 is not supported any more. This would still require a KAC solution as proposed in section 2.

Under the given assumptions, the NEs can directly negotiate the Layer III SAs between them, using IKE. This leads to the following architecture:

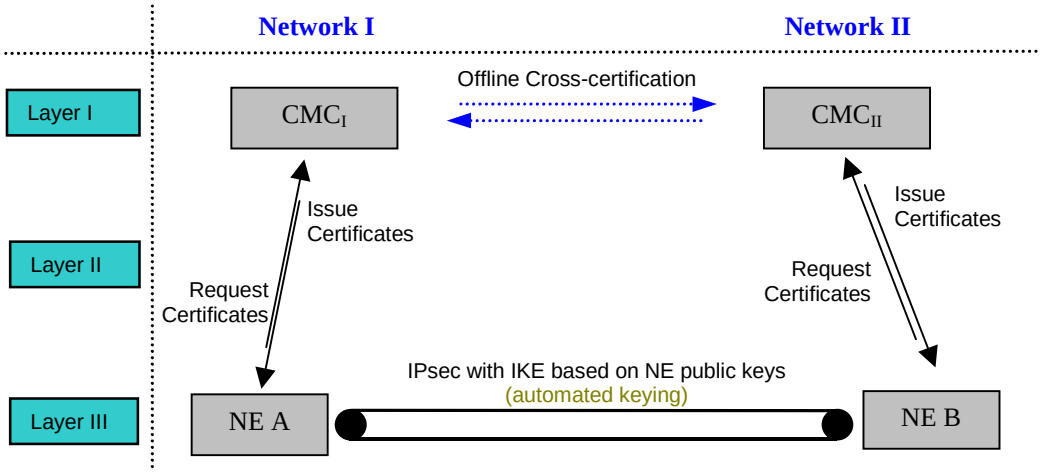

Figure 2: PKI-based key management for the core network

Instead of KACs, a certification management center (CMC) would be required which at least includes a certification authority (CA) to issue public key pairs or certificates for NEs and a repository for providing certificates to the network nodes. It would also have to provide a mechanism to revoke certificates. A trust relation between different networks could be established by a cross-certification between the networks, where the CA of network 1 issues a certificate for the CA of network 2 and vice versa. In this model, IKE will directly run between the NEs for authentication and key agreement, so layer I/II key management is not required any more. Therefore, we call this a ‘flat’ key management.

Since setting up a PKI is widely regarded as a difficult task, and since there are still legacy network entities using SS7, it seems difficult to start with a flat key management for the core network security. However, a flat key management may be an attractive solution for the medium to long term, so migration from a two-tiered to a flat key management seems desirable. And with the integration of IPsec into the core network as proposed in figure 1, this seems to be feasible.

4. Conclusions and open issues

The following principles 1) and 2) are proposed to be agreed by 3GPP S3:

1) A two-tiered key management architecture, as described in section 2, is used for the UMTS R'00 core network.

2) Layer I and II shall use IP-based communication for key negotiation, secured by IPsec AH/ESP authentication and encryption. KACs and participating NEs will have to implement an IP interface supporting IPsec AH/ESP.

The open issues listed in section 2 need to be resolved for a solution along the lines of 1) and 2). Section 3 is to show that the proposed solution allows migration to a PKI-based flat key management, but such a key management is not proposed to be included in UMTS R'00.

5. References

[1] 3G TS 33.102 v3.4.0 UMTS Security Architecture

[2] IETF RFC 2402 : IP Authentication Header (AH)

[3] IETF RFC 2406 : IP Encrypting Security Payload (ESP)

[4] IETF RFC 2409 : The Internet Key Exchange (IKE)

[5] IETF RFC 2401 : Security Architecture for the Internet Protocol