3GPP TSG SA WG3 Security — MAP Security ad-hoc **S3z010083**

13 September, 2001

Sophia Antipolis, France

3GPP TSG SA WG3 Security **S3-010368**
Meeting S3#19
Newbury, July 3-6 2001

Source: ALCATEL
Title: Local Security Association Distribution
Document for: Discussion / decision
Agenda item: 7.1

1 Introduction

TR 33.800 V0.4.0 contains some preliminary description of a generic automatic mechanism that could be used to distribute MAPsec SA information from some central KAC to the NEs within the same domain (section 6 of TR 33.800). This is what is specified as interface Ze, realisation of which has so far been assumed to be based on IPsec (ie the mechanism used for interactions between the KAC and the NEs should rely on IPsec for security).

This contribution discusses the generic architecture as currently described in TR 33.800 and suggests possible protocols to achieve intra-domain SA management.

2 Analysis of TR 33.800 Current Mechanism

2.1 Security Policy in NEs

Figure 2 in section 6.1 shows an SPD only in the KAC, which seems to imply that the NE contains no such policy database. The accompanying process description does not clarify this aspect as it lacks any reference to some policy information within the NE both for outgoing and incoming traffic.

This is considered incomplete: the NE needs some minimal policy information (to be distributed from the KAC). This policy information (typically whether or not to apply MAPsec with a given operator, whether fallback to unprotected mode is allowed, …) should conceptually be part of a Security Policy Database located in the NE. The contents of such a SPD should be distributed to the NE from the KAC. It is to be noted that we view such a SPD as a conceptual database. Clearly, its realization is an implementation matter. Only the policy information distribution via the Ze interface protocol needs to be fully standardized.

2.2 Pull Mechanism

The information flow and the procedure description are based on a pure pull mechanism, which requires the NE to explicitly request SA information.

This is not considered practical. The KAC is mainly responsible for setting up MAPsec SAs with remote domains. It is a therefore natural for the KAC to distribute MAPsec SAs as soon as these have been actually set up. This improves the latency in NEs when processing MAP messages to a "new" remote domain. Consequently, the architecture should allow for both push and pull mechanisms. Although a pure pull model is not efficient enough as discussed above, a pure push mechanism is not sufficient either as the KAC should always expect that a NE does receive MAP messages to process for which it currently has no MAPsec SA information.

2.3 SA Lifetime Supervision

As currently described, when the KAC supervises the SA lifetime and sets up a new SA before the old one expires, it waits for a request from a NE to distribute the new SA to the requesting NE. We believe that the KAC should have the opportunity to set up several MAPsec SAs at the same time with a remote domain and distribute this set of MAPsec SAs to its NEs without waiting for requests. The NE can determine which SA to use first as the SAs would have different (absolute) lifetimes. The SA with the shorter lifetime would be used first by the NE for outgoing traffic.

Current description covers the case where the NEs supervise SA lifetime and request a new SA from the KAC. It is not clear that this is an appropriate procedure as it may flood the KAC and it is not clear how to achieve randomization of requests. It may be better to rely on a priori distribution of new MAPsec SAs by the KAC and further on explicit requests for SA information by the NE when processing a MAP message.

Although the KAC may have negotiated two SAs, only one should be valid at a given time. For outbound traffic, the NE should always use the SA which expires the sooner. For inbound traffic, the NE should use the SA indicated in the received MAP message.

3 Possible Local SA Management Mechanisms

3.1 Management Protocol over IPsec

An IPsec SA is set up between the KAC and each NE served by the KAC (for scalability purposes, it may be appropriate to have several KACs in charge of managing MAPsec SAs with a given set of NEs – however a mechanism is then needed to manage the MAPsec SAs between the KACs themselves).

A brand new protocol can be specified for use over IPsec. Such a protocol should enable a KAC to send MAPsec SA and related policy information to a NE, a NE to request details of an SA (in relation to received MAP message), a NE to notify the KAC of security errors, …

Rather than a new protocol, existing policy protocols such as COPS may be considered.

3.2 New IKE Phase 2

In such a solution, IKE phase 1 is used to set up a secure communication channel between the KAC and the NE. A new DoI is specified in which the KAC sends the SA information together with the related policy to the NE. Such information could be under the form of an SA payload with new appropriate attributes. Request for an SA by the NE can be implemented in

a SA payload identifying the requested SA. Error/notification messages can be implemented with Notify payloads.

3.3 Secure Multicast

The IETF is currently working on future solutions for securing multicast traffic. This work includes mechanisms for managing keying material (and by extension SA information) in a multicast context.

The interaction between the KAC and the NEs presents similarities to key management in a multicast context. Solutions developed in IETF for multicast key management could be considered in the context of inter-domain SA management.

It is to be noted that security multicast solutions being developed within the IETF are not ready yet and should be expected in a timeframe of one year at the earliest.