3GPP TSG SA WG3 Security – S3#ad-hoc Antwerpen **S3z020024**

Jan 31 – Feb 01, 2002

Antwerpen, Belgium

Source: Alcatel

Title: Secure connection between KAC and NE

Document for: Decision

Agenda item: 5.4

1 Introduction

This contribution discusses the mandatory need for a secure connection between the KAC and the NE when the KAC distributes MAPsec SA and SPD information to the NE, and a related ambiguity in section 5.1 of TS 33.200v5.

2 General Discussion

The MAPsec SA and SPD information distributed by the KAC towards the MAP-NE contains highly sensitive information such as the cryptographic keying material to be used by the MAP-NE when encrypting/decrypting and generating/verifying integrity of MAPsec messages. As much as the KAC and the MAP-NEs themselves must be protected against keying material leakage/stealing, the transport of any such material over the network infrastructure between the KAC and the MAP-NE must be achieved in a secure way given that this is potentially the weakest link in the chain of events.

Apart from the highly sensitive information such as secret keying material, other MAPsec information items and security policy information in general are also to be considered as sensitive information. One must indeed avoid that fake/intentionally erroneous information is given to the MAP-NE. Such information must therefore be integrity protected and authenticated as a minimum.

We will also note that if the secure transport of the MAPsec SAs and policy information is indeed optional, this is not in line with what happens in NDS/IP where, thanks to the use of IKE, every SA setup is fully secure over the network, including for intra-domain SA setup.

The fact that in MAPsec the SA setup is realized through a new non-IKE mechanism must not weaken the security level of the SA setup phase (which is here achieved through a push distribution mechanism).

3 Ambiguity

Current text in section 5.1 of TS 33.200v5 states that "The SAs and security policy must be transferred in a secure manner." Another statement in section 5.1 states that "KAC may be able to establish secure connections to transmit MAPsec SAs and policy information to the NEs within its PLMN.".

Above text can be read as the KAC is not required to make sure it uses a secure connection to transmit data to each NE. Hence, it could use a non-secure connection.

On the other hand, section 5.2 states that "NE must be able to establish a secure connection to receive MAPsec SAs and policy information from the KAC within its PLMN.".

The text above seems to correct somewhat the text in section 5.1 as it could imply that it is the responsibility of the NE to set up a secure connection towards the KAC, which can then use this secure connection to transmit data in a safe way. Yet, it is not clear what happens if such a secure connection is not present when the KAC needs to distribute data.

4 Proposed CR

In order to resolve the above perceived ambiguity, the following change is proposed to section 5.1:

- Prior to transmitting MAPsec SA and policy information to a NE within its PLMN, the KAC shall ensure that a secure connection is in place with that NE. If no such secure connection exists, the KAC may be able to establish the required secure connections ~~to transmit MAPsec SAs and policy information to the NEs within its PLMN~~.