3GPP TSG-SA3 Ad Hoc on ‘Network Domain Security’ **S3z010008**
Madrid 23-24 April, 2001

Agenda Item: tbd (NDS WI)

Source: Siemens

Title: Comments on MAP DoI

Document for: Discussion and Decision

1 Scope and Objectives

This contribution summarises the comments on MAPDoI v1. Attached to this contribution an edited MAPDoI RFC is provided.

SA3 haven’t still agreed on the MAPsec DoI text. Early SA3-understanding of the key and Protection Profile negotiation is necessary in order to avoid late changes on manual key management specifications.

2 Comments on MAPDoI v1.

A) The MAPsec DoI has copied a lot of text from the IPsec DoI.

Some text parts shall be deleted, because the MAPsec will never use the copied IKE options or can be referred to IPsec DoI because its use is unchanged. Other text parts leave the implementation options open, and shall be closer specified (PLMN_ID coding).

B) Network Architecture.

MAPsec DoI over ISAKMP over IP directly between the network elements is not a working assumption of 3GPP SA3.

C) Unclear status of MAPSec DoI as 3G standard.

Currently MAPsec DoI is a draft RFC and, as such, does not have a status, which would allow it to be referenced in a 3G Technical Specification. It will take quite some time for the MAPsec DoI to become an accepted RFC. But MAPSec DoI needs to be standardised in 3GPP for interoperability, probably before the IETF will have made a decision.

Siemens proposes that DoI numbers as will be specified in paragraph 6 ‘IANA considerations’ will be normative in the MAPsec DoI RFC and that all other normative parts that are currently included in the Draft RFC will be included in a separate 3GPP technical specification on MAPsec DoI. It will not only allow better change control of 3GPP initiated changes, but also a faster inclusion.

D) KINK as an alternative to IKE.

In the MAPsec DoI the use of KINK is proposed as an alternative to IKE. This is not a working assumption of SA3. KINK is an own key management protocol that is being defined at the moment, therefore does not have the mature status that IKE has. The use of KINK needs further clarification and specification before it can be used between the KAC’s. Siemens therefore proposes to use only IKE for Rel5.

E) Protection Profiles

The ‘MAPsec protection profile numbers range’ is defined in paragraph 6.8. The MAPsec DoI does not describe any restrictions on how MAP PP may be defined. Also 3GPP TS 33.200 does not include any specification rules. Only 64 identifiers are currently reserved for MAP protection profiles and a bad choice of MAP PP definition rules may lead to an early exhaustion of the identifier range. Siemens therefore proposes to define Protection Profiles in a non -overlapping way and suggests including following implementers note: ‘*A SA-proposal may contain several protection profiles. Profiles shall be defined in such a way that they do not have the same set of application context, operation mode and protection level in common’.*

F) Symmetric or asymmetric negotiation.

The current MAPsec DoI specifies a symmetric negotiation between the KACs (One KAC proposes a list of SA, the responder selects an SA-proposal that is used for the SA-Pair). This means that currently both unidirectional SA will contain the same list of supported MAP PP after a successful negotiation. Only the keys and the SPI will differ. Siemens sees currently no need for having asymmetric negotiation and hopes that there are no consequences on policy definitions. It must also be noted that an asymmetric negotiation would require a major redesign of IKE Phase 2 for use within MAPsec DoI, therefor SA3 shall be sure that symmetric negotiation is fulfilling the requirements.

G) SA duration in absolute time

The MAPsec DoI does not reflect the SA3 agreement to use absolute time for SA duration (Paragraph 4.5).

H) Inclusion of parameters for future enhancements

Siemens proposes to include additional provisions in MAPsec DoI for possible future use of AES-CBC with key lengths of 192 and 256 bit. Only 128-bit shall be mandatory for implementation for Rel5.

I) MAP SA payload specification missing

This specification text is missing and has to be included within paragraph 4.6.