3GPP TSG SA WG3 Security — S3#13 **S3-~~00XXXX~~000356**

23-26 May, 2000

Yokohama, Japan

Source: **SA3**

To: **SA2, SA5, CN4**

CC:

Title: **Liaison Statement on Protocol Choice for Layer I of MAP Security**

Document for: **Comment**

Agenda Item:

Introduction

SA3 would like to see adequate, even if only partial, provisions for MAP security (that is, confidentiality and integrity of selected MAP messages) in R'00. One important open issue has been the protocol to be used in Layer I, the key exchange protocol between the Key Administration Centers. In TS 33.102 Version 3.4.0, one such possibility, based one ISO/IEC 11770-3, was presented. There had been arguments put forth supporting a different solution, and in S3's ad hoc meeting on MAP Security (Yokohama, May 23) the Internet Key Exchange (see RFC 2409) was considered as an alternative.

Conclusion

Some delegates were convinced of the preferability of IKE on organisational or administrative grounds, based on its de facto status as the primary internet standard for key exchange. The advantages this confers include:

- Futureproofing: this is not likely to become outmoded any time soon, and is the strongest candidate for use in an IP-based MAP system, making coming transitions easier;
- Ease of implementability: off-the-shelf software and hardware products are available; and
- Synergies: network operators are more likely to have IKE in use for other purposes than ISO/IEC 11770-3.

These advantages might be more limited than first meets the eye. For instance, with the move to an all IP-based MAP network, there will be architectural changes anyway; if network elements end up negotiating a key exchange directly with each other, then the KACs will just be eliminated, obviating any benefit that might have accrued from already having had IKE in the KACs. Still, the advantges are real, since, in the transition period from SS7 to IP, the new NE could negotiate with the KAC from a network still using SS7 using IKE.

A possible advantage of the ISO/IEC-protocol is that it has already been accepted in 3GPP and might therefore find a concensus more quickly, especially if this has already been further specified.

There were no security advantages or disadvantages of either protocol found.

S3 has decided to investigate in more detail the applicability of IKE to Layer I. As an indication of where our deliberations currently stand, the questions we have at the moment are:

- Can the IKE-negotiated key, actually intended for use in IPSec, also be used for SS7 encryption, or must a separate SS7 key be negotiated in an IPSec session?
- Can IKE support the needed negotiation for an SA (Security Association)?
- Can IKE support our needs for DoIs (Domains of Interpretation)?
- Does IKE support a client node, enabling KACs to negotiate on the behalf of NEs, thereby incorporating Layer II straightaway?

Should it turn out against all expectation that IKE does not fully support our needs on these or other points, then we will be forced to turn back to the earlier proposal.

Action requested

S3 would like a statement from the other Working Groups involved with this issue regarding their preferences between ISO/IEC and IKE. Keeping in mind that the goal is the inclusion of this functionality in R'00, the primary question is for which of the protocols under consideration is the time allowance sufficient. S3 would also like to hear of any other arguments speaking for or against one of the candidates. Furthermore, if IKE is acceptable, any support answering the questions above would be warmly received.

Contact Person

Robert Lubarsky

Tel +49 228 936 3340

Robert.Lubarsky@T-Mobil.de