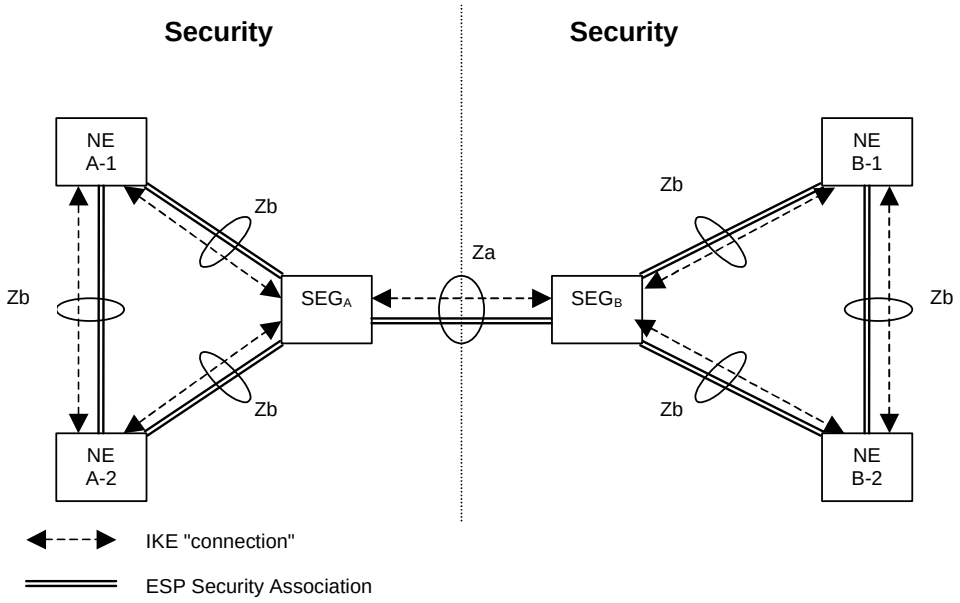
3GPP TSG SA WG3 Security — S3#28 **S3-030235**
6 - 9 May 2003
Berlin, Germany

Source:	Nokia
Title:	Openness of Rel6 IMS network: security methods required
Document for:	Discussion
Agenda Item:	7.1
WI / Topic:	IMS

1. Introduction

In 3GPP Rel5 the use of the Za interface between operators is mandatory. Thus, any traffic between operators has to use the Za interface or it is discarded. The traffic generated by the UEs has to pass through P-CSCF in their way to S-CSCF. As a direct consequence, non-protected traffic will not enter IMS.

From TS 33.210:



As the usage of the Zb interface is optional, there may be cases when some malicious users will send SIP messages directly to the S-CSCF, bypassing the P-CSCF. For these cases to be avoided some extra security mechanisms are needed in Rel5 IMS, but those can be implementation specific.

The Rel6 IMS will be a more open system and traffic arriving at the entry point of an IMS network (the I-CSCF) will be allowed to pass into IMS even in cases when it was not arriving protected on the Za interface (as it was not sent from another IMS network). This opens a hole in the IMS specification which can be easily used by hackers to masquerade IMS users identity. To prevent this some security actions has to be taken by IMS either on SIP or IPsec level:

- One possibility would be to mandate the usage of the Zb interface. In this case the CSCFs would need to know whether a packet arrived on the Za or Zb interface and process it accordingly. If it arrived protected on one of the interfaces, then it will be sent further also protected (on Za or Zb) or it will be processed as a message with a reliable identity in it. If it arrived unprotected, then it will be sent further unprotected or it will be processed as a message without a reliable identity in it.
  Mandating the usage of the Zb interface may not be feasible for some networks or in cases when the interface does not exist physically.

- Another possibility is, that the I-CSCF will forward the request to the S-CSCF without changes in case it arrived protected on the Za interface, or it will modify it in case it arrived unprotected. The modification would consist on checking the existence of the P-Asserted-Identity header in the message. If such a header is present, then it has to be either removed or a 'screening=no' parameter added to it.

The contribution was also submitted and discussed in the last CN1 meeting. The comments received from the CN1 delegates were, that this is first a security architecture problem which needs to be handled in SA3, afterwards the work can be transferred to CN1.

One other comment made by a delegate in CN1 was, that this issue may be handled by enabling the usage of TLS between the SIP proxies. In other words, the I-CSCF being at the edge of the IMS network would set up a security connection with the SIP proxy located outside the IMS domain, and the proxies would use that secure connection to transfer SIP messages. This solution solves the secure transfer of messages between proxies problem (equivalent with Network Domain Security), but does not solve the message origin verification problem: an arbitrary SIP proxy located on the Internet does not check the relation between the originator of the message and the content of the message, i.e. the I-CSCF may still receive requests containing public identities (IMPUs) of IMS users not involved in the communication, instead of the IMPU of the originator.

It is clear from the analysis made above that it is not possible to extend the trust domain concept beyond IMS networks and that at the edge of the trust domain every message must be checked and message origin verification has to be done or the IMPU must be removed from the message.

Some CN1 delegates were explicitly asking to resubmit this contribution to SA3 and that SA3 should send an LS to CN1 listing the possibilities SA3 sees to solve this problem.

2. Proposal

It is proposed to carefully study the analysis made above, reflect on the proposed alternatives and decide which kind of security mechanism is preferable, IPSec or SIP level. An LS should be sent to CN1 and possibly also to SA2.