3GPP TSG SA WG3 Security — S3#23 **S3-020316**

14-17 May, 2002

Victoria, B.C., Canada

From:	**SA3**
To:	**CN1**
Title:	**Secure registration of IP addresses**
Contact:	**Guenther Horn** Guenther.horn@mchp.siemens.de **Phone: +49 89 636 41494**

1. Problem description:
SA3 would like to ask for advice from CN1 regarding an IMS security issue, which is described in the following. The pertinent specification is TS 33.203.

According to a decision taken by SA3 in March 2002, IPsec ESP is used to provide the integrity for SIP messages between the UE and the P-CSCF. The integrity keys are established as part of the SIP registration procedure using the AKA protocol in SIP. The parameters for the IPsec security associations are negotiated as part of the SIP registration procedure using draft-IETF-sip-sec-agree.

IPsec security associations need to be bound to IP addresses. In particular, when the P-CSCF creates a new security association in its local database during a registration it must bind the UE’s IP address to the security association. For security reasons, an attacker must not be able to alter the IP address in the registration procedure, otherwise a wrong binding may occur. For this reason, the UE’s IP address must be communicated by the UE to the P-CSCF in an integrity-protected way during the registration procedure. But IPsec ESP does not integrity-protect the IP packet header, only information in the transport and higher layers. Therefore, the UE’s IP address has to be repeated somewhere in the integrity-protected part of the packet. SA3 currently assumes that the contact header in the integrity-protected REGISTER message, which is sent as a response to the authentication challenge, is the right place for the UE’s IP address. The contact header may contain the UE’s IP address directly, or it may contain a symbolic name. The use of symbolic names will, however, not cause problems as long as the following assumption holds:

When the P-CSCF establishes a security association with a UE as part of a registration procedure, and the contact header in the REGISTER message does not contain an IP address, but a symbolic name, then the P-CSCF is able to resolve the symbolic name to obtain a single IP address to/from which all messages protected with the security association will be sent/received.

SA3 would also like to mention that SA3 has briefly discussed the use of draft-IETF-sip-sec-agree for sending the UE’s IP address in an integrity-protected way. It appeared at first inspection, however, that such a use would require changes to draft-IETF-sip-sec-agree. But such changes may be difficult to make because draft-IETF-sip-sec-agree is already in IETF last call.

2. Actions:
2.1 SA3 would like to ask CN1 to inform SA3 whether an approach based on the above assumption is considered feasible.
2.2 If the approach was considered completely infeasible then SA3 would also greatly appreciate suggestions of alternatives from CN1 which would provide the desired secure binding of the UE’s IP address to the security association.

3. Dates of next SA3-meetings:

9-12 July, Helsinki (Nokia)

8-11 Oct, Munich (Siemens)