3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010108**

14 September, 2001

Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#20 **S3-010433**

16 - 19 October, 2001

Sydney, Australia

3GPP TSG-SA WG2 meeting #19 **Tdoc S2-012311**
Sophia Antipolis, France, 27 – 31 August 2001

Source: SA2

To: SA3

Cc: CN1, CN4

Response to: LS S3-010403 on the use of Network Domain Security for protection of SIP signalling messages from WG3.

Contact Person:

Name: Farrokh Khatibi
Tel. Number: +1 858.658.3716
E-mail Address: fkhatibi@qualcomm.com

Attachments: None

SA2 thanks SA3 for the liaison on the use of Network Domain Security for protecting SIP signalling messages (S3-010403, S2-012035).

1. Overall Description:

In your liaison, you have identified five possible options to protect the IMS SIP messages:

1. To not encrypt any GTP-U messages, understanding that this means that IMS SIP messages will not be encrypted when carried by GTP-U in the core network.
2. To protect all GTP-U messages, including the small proportion that are IMS SIP messages.
3. To introduce a new sub-version of GTP for the IMS control plane (GTP-IC). This new GTP-IC would then have a unique port number assigned to it, enabling those messages to be encrypted. All IMS control plane messages would then have to be tunnelled through GTP-IC in the core network.
4. Extend GTP-C to contain all IMS control plane messages. All IMS control plane messages would then have to be tunnelled through GTP-C in the core network. Again, since GTP-C is always encrypted, the IMS SIP messages would be encrypted.

5. Introduce multiple IP addresses (multi-homing) of the CSCFs such that GTP-U containing IMS control plane messages would use a different set of IP addresses from the GTP-U containing non-IMS control plane messages.

SA3 informed that alternatives 2, 3, and 4 are feasible from security point of view. SA2 has analyzed the mentioned alternatives and the conclusion is:

Alternative 2 is inefficient since only a small percentage of the GTP-U messages are IMS SIP messages.

Solutions 3 and 4 assume that RAN has knowledge of which IP packets carry SIP signalling. Currently RAN is not aware of contents of IP packets.

SA2 would like to understand what requirements are being addressed here? It is SA2's understanding that the protection of SIP messages between the UE and P-CSCF is covered with Access Security (integrity protection) and the security between different CSCFs is covered via NDS. SA2 has difficulty understanding the security requirements to GTP-U related to IMS.

2. Actions:

To SA3 group.

ACTION:

SA2 would like to understand what security issue is being addressed here that is not already covered via SIP application level security and network domain security.

3. Date of Next SA2 Meetings:

SA2_20	29th October – 2nd November 2001	Japan
SA2_21	26th – 30th November 2001	Cancun, Mexico