3GPP TSG SA WG3 Security — IMS Security ad-hoc **S3z010112**
14 September, 2001
Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#20 **S3-010442**
16 - 19 October, 2001
Sydney, Australia

3GPP TSG-CN-WG1, Meeting #19 ***Tdoc N1-011332***
27 – 31 August, 2001, Helsinki, Finland

From: TSG CN WG1

To: TSG SA WG3

CC: TSG SA WG2, TSG CN WG4

Title: Response to LS "On the use of Network Domain Security for protection of SIP signalling messages“ (N1-011041 or S3-010403)

Date: 27 August 2001

Contact: Apostolis Salkintzis, Motorola [mailto:salki@motorola.com]

CN1 thanks SA3 for their LS in S3-010403, which considers the problem of security protection of SIP messages in the core network.

CN1 understands that:

- The general problem is how to provide confidentiality of SIP messages between the UE and the P-CSCF, i.e. on the so-called "first-hop" (according to TS 33.203).
- From the UE to the RNC, SIP confidentiality is based on the UTRAN confidentiality mechanisms. This is specified in TS 33.203, sec. 5.1.2.
- From the GGSN to P-CSCF, i.e. across Gi interface, typical IPsec procedures can be applied, according to NDS/IP specification, TS 33.210.
- According to SA3´s LS in S3-010403, the problem exists across Gn/Gp interfaces, where SIP messages are encapsulated in GTP-U tunnels and this makes it impossible for IPsec to apply protection only to GTP-U PDUs that carry SIP messages.

From the above, and given SA3's assumption that SIP confidentiality would be based on hop-by-hop procedures in the UMTS network, CN1 observes that confidentiality issues should also be addressed on the Iu-ps interface, since no such procedures are currently defined. Even if SIP confidentiality is provided in the core network according to TS 33.210, SIP messages would still be transmitted unprotected over Iu-ps, if protection mechanisms are not defined for this interface too.

CN1 has discussed the potential solutions included in S3-010403 and believes that, if SIP protection is going to be based on NDS/IP mechanisms (i.e. not between the UE and the P-CSCF but rather within the network in a hop-by-hop fashion), then it is preferred to specify a solution that

- can be applied on both Iu-ps and Gn/Gp interfaces, and
- cause minimum or no impact on UMTS architecture and protocols.

In this context, CN1 would be interested to know if SA3 has investigated any solutions inline with the above preferences. For instance, has SA3 investigated the limitations of option 2 in S3-010403? Has

SA3 considered any potential extensions to IPsec (on Iu-ps and Gn/Gp) as alternative solutions? Such extensions wouldn´t have an impact on the UMTS architecture or protocols.