3GPP TSG SA WG3 Security — S3#21b **S3z020029**

31st January - 1st February, 2002

Antwerp, Belgium

Source: **Nortel Networks**

Title: **Set-up Procedures for the SIP-level Security Solution**

Document for: **Discussion/Decision**

Agenda Item: **IMS-6, SIP Signalling Protection**

Abstract

This contribution proposes text for inclusion in draft TS 33.203 that describes the set-up procedures for a SIP-level security solution for the IMS in Release 5. Parameters and procedures specific to the SIP-level solution are described.

1. Introduction

As was agreed in meeting S3#20, a description is needed of the set-up procedures for SIP-level solution mechanisms for SIP confidentiality and message integrity protection in the 3GPP IMS. The editor of 33.203 has created Annex E as a placeholder for such material. The text in the next section is proposed for insertion in Annex E.

2. Proposed Text for 33.203 Annex E: Set-up Procedures for SIP-level Solution

[Editors Note: If the SIP level solution is chosen the material below shall be moved into the main body of this TS in the corresponding sections. This chapter is based on chapter 7 and provides additional specification for the support of SIP level integrity protection].

E.1 Security association parameters

As the security session keys are established by independent execution of IMS AKA in the UE and in the Home Network, the only SA attributes that must be negotiated between the UE and P-CSCF are the algorithms to use for integrity protection and encryption.

Further parameters:

- SA duration: the SA duration is based on the length of the per-subscriber registration timer as described in chapter 7. When this timer expires, the SA is declared invalid at the P-CSCF.
- Key length: the length of session keys for integrity and confidentiality protection is 128 bits.

E.2 Security Association Identifier

For each incoming message, the SIP application must apply the correct inbound SA for security services. Identification of the correct SA to apply (SA_ID) is based on the contact information (i.e. IP address or FQDN) of the partner entity. For SIP messages arriving at the P-CSCF from the UE, this information is obtained from the “Contact” header. For each message arriving at the P-CSCF destined for the UE, the SIP application must apply the correct outbound SA for security services. For outbound SIP requests, the contact information is obtained from the “Route” header. For outbound SIP responses, this information is obtained from the last address contained within the “Via” header.

3. Recommendation

It is recommended that SA3 adopt the text in section 2 of this contribution for insertion in Annex E of draft TS 33.203.