3GPP TSG SA WG3 Security — S3#15 **S3-000625**

12-14 September, 2000

Washington D.C., USA

Source: Ericsson

Title: Protection between the UE and the serving CSCF

Document for: Discussion / Decision

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

This contribution discusses issues related to using IPSec as protection mechanism between the UE and the serving CSCF as described in Siemens contribution S3-000561.

Protection using either TLS or IPSec

In Siemens contribution S3-000561 it is proposed to use IPSec as the working assumption for end-to-end protection of SIP messages between the UE and the serving CSCF.

In the SIP specification three options for protection of the SIP messages are given:

1. Hop-by-hop encryption to protect "who is calling whom" (e.g. using IPSec or TLS)

   This protects the users from being tracked by eavesdroppers
2. Hop-by-hop encryption of the VIA field to hide the route

   The route may give useful information for an attacker
3. End-to-end (e.g. using mechanisms defined in PGP)

   The SIP message body can be encrypted and also some certain sensitive headers as well. However some parts of the SIP-message must be in clear such as the TO and VIA field to make it possible for the proxies to route the message correctly.

It is important to note that the proxies may do changes in the SIP message.

This seems to contradict the Siemens working assumption since in e.g. a call set up scenario between UE-to-UE SIP provides either hop-by-hop protection between proxies or/and end-to-end protection between the two UEs. This is valid both for confidentiality protection and integrity protection.

References

[S3-000446] 3GPP TSG SA WG3 Security: *Requirements on access security for IP-based services*; Siemens, July 2000.

[S3-000447] 3GPP TSG SA WG3 Security: *Overview of security mechanisms for access security for IP-based services*; July 2000.

[S3-000458] 3GPP TSG SA WG3 Security: Security requirements for access to R'00 IM subsystem; Nortel, July 2000.

[Rep S3#14] 3GPP TSG SA WG3 Security: *Draft Report on S3#14, v.0.0.6*; Oslo, 1-4 August, 2000.

[TR 33.xxx] 3GPP TSG SA WG3 Security, TR 33.xxx: "Access security for IP-based services"; v0.1.0, September 2000.

[RFC 2543bis-01] IETF RFC 2543bis-01: *SIP: Session Initiation Protocol*; August 2000.

[RFC 2617] IETF RFC 2617: *HTTP authentication: Basic and digest access authentication;* June 1999.