3GPP TSG SA WG3 Security S3-010074
Meeting S3#17

Göteborg, 27 Feb – 2 Mar, 2001

Source: Siemens AG

Title: Open issues in IM domain security beyond location of security functions

Document for: Discussion / Decision

Work item: Access security for IP-based services

Agenda item: tbd

Abstract

Much of the discussion on IM domain security in S3 so far has been focussed on security requirements and on the location of certain security functions in the network. This contribution points out that, even when these questions will have been settled, a lot of work lies ahead before the Stage 2 IM domain security architecture can be completed.

The following procedures are likely to be required. (Some of them need double-checking as they may be specific to the mechanisms of the CS and PS domain.)

1 Authentication at call set-up (INVITE)

- Network-initiated
- UE- initiated

2 Re-authentication during (long) calls

- Network initiated:
  by whom, P-CSCF, S-CSCF or HSS?

3 Re-synchronisation procedure,

- cf. TS 33.102, section 6.3.5

4 Ciphering mechanism

(ESP or new application layer protocol)

5 Integrity mechanism, including replay protection

(ESP or new application layer protocol)

6 Ciphering and integrity mode negotiation

Cf. TS 33.102, section 6.4.2

7 Provisions for limiting the cipher key and integrity key lifetime

Cf. TS 33.102, section 6.4.3

8 Security mode set-up procedure

Cf. TS 33.102, section 6.4.5

This procedure serves two purposes:

- To negotiate the security capabilities (algorithms, keys in use) between UE and network side
- To synchronise the start of confidentiality and integrity functions between UE and network side

9 Periodic local authentication

Cf. TS 33.102, section 6.4.7 (is this needed?)

10 Security in roaming scenarios

- Between IM domains
- Between IM domain and other domain (e.g. CS, GSM?)

11 Security in handover scenarios

- Between IM domains
- Between IM domain and other domain (e.g. CS, GSM?)

12 User identity confidentiality

- User IMS identity (NAI) in REGISTER procedure needs to be protected
- ---> Solution in analogy to TMSI (Temporary Mobile Subscriber Id) required??