3GPP TSG SA WG3 Security **S3-010079**
joint S2/S3 meeting, Göteborg, 27 Feb 2001

Open issues
beyond location of security functions

Source:	**Siemens AG**
Document for:	**Discussion**
Agenda item:	**?**

Authentication - related

- **Authentication at call set-up (INVITE)**
  - Network-initiated
  - UE- initiated
- **Re-authentication during (long) calls**
  - Network initiated:
    by whom, P-CSCF, S-CSCF or HSS?
- **Re-synchronisation procedure for authentication and key agreement**
  - cf. TS 33.102, section 6.3.5
- **Periodic local authentication**
  - Cf. TS 33.102, section 6.4.7 (is this needed?)

Cryptographic mechanisms

- **Ciphering mechanism**
  - ESP or new application layer protocol
- **Integrity mechanism, including replay protection**
  - ESP or new application layer protocol

Security context management

- **Ciphering and integrity mode negotiation**
  - Cf. TS 33.102, section 6.4.2
- **Provisions for limiting the cipher key and integrity key lifetime**
  - Cf. TS 33.102, section 6.4.3
- **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

Security in roaming and handover scenarios

- **Security in roaming scenarios**
  - Between IM domains
  - Between IM domain and other domain (? CS, GSM?)

- **Security in handover scenarios**
  - Between IM domains
  - Between IM domain and other domain (? CS, GSM?)

- **Issues:** security context transfer, re-authentication, security gaps, . . .

User identity confidentiality

- **User IMS identity (NAI) in REGISTER procedure needs to be protected**

---> Solution in analogy to TMSI (Temporary Mobile Subscriber Id) required??