S3-000316

ETSI SMG10 (Security)

SMG10 status report to SMG#31bis

Frankfurt, Germany

17th April 2000

Dr. Stefan Pütz

(vice chair 3GPP TSG-SA WG3)

P-00-223

T-Mobil

Content of presentation

- GPRS encryption
- GEA II
- A5/3

Document list

- P-00-224: LS on GPRS ciphering (S3-000306) - *for information*
- P-00-225: LS on Introduction of rejection of non ciphered calls for GPRS (S3-000206) - *for information*
- P-00-226: LS on A5/3 (S3-000307) - *for information*
- P-00-227: A5/3 requirement specification (S3-000303) - *for approval*

T-Mobil

GPRS encryption

- SMG10 recognizes that there are practical problems making encryption mandatory for GPRS connections
- CR against GSM 03.20 (S3-000252)
  - not presented: contents agreed but wording to be confirmed by SMG10
- Support of encryption capabilities in GPRS terminals is mandatory in accordance with GSM 02.07

T-Mobil

GPRS encryption (2)

- R97/R98/R99
  - Support of ciphering indicator in GPRS terminals is mandatory in accordance with GSM 02.09/03.20 and 3G 22.101/33.102
- R00 onwards
  - Terminal/USIM shall have the ability to reject unciphered calls independent of radio access system and whether the connection is cs or ps (to counter false BTS attacks)
  - For SMG endorsement

T-Mobil

GEA 2

- SMG10 recommends that GEA 2 algorithm is deployed in GPRS systems as soon as possible
- Proposed time scales
  - Mandatory in terminals and SGSN for R99 but not before the end of 2002
  - Optional for R98
  - For SMG endorsement

GEA 2 (2)

- Requires that negotiation capabilities are supported as a mandatory requirement in GSM 04.08/3G 24.008
- From R98 onwards
  - ME must have the ability to signal its capabilities on 7 GPRS ciphering algorithms
  - To be corrected by SMG3/TSG CN1

A5/3

- GSM2000 group has produced a requirement specification for an A5/3 ciphering algorithm
  - Approved by SMG10
  - For approval by SMG
  - For approval by GSMA
  - Funding by GSMA

A5/3 (2)

- A5/3 core algorithm capable of 128 bit maximum key size
- 64 bit mode for current GSM releases
- Longer keys for future releases (R00 onwards)
- Requires that negotiation capabilities are supported as a mandatory requirement in GSM 04.08/3G 24.008 (see statement on GEA 2)

For more details on ...

- GPRS and GEA 2
  - P-00-224: LS on GPRS ciphering (S3-000306)
  - P-00-225: LS on Introduction of rejection of non ciphered calls for GPRS (S3-000206)
- A5/3
  - P-00-226: LS on A5/3 (S3-000307)
  - P-00-227: A5/3 requirement specification (S3-000303)

SMG decisions expected ...

- Rejection of unciphered GPRS calls for R00 onwards
- GEA 2 mandatory in terminals and SGSN for R99 but not before the end of 2002; optional for R98
- A5/3 ciphering algorithm requirements specification