3GPP TSG SA WG3 — SA 3 #17 **S3-010045**
Gothenberg, Sweden. 27 Februar-2 March 2001.

Source: **Siemens Atea**

Title: **Terminology in TS 33.102/TR 31.900**

Document for: **Discussion and decision**

Agenda item:

1. Definitions found in the different Specifications/Reports

- 3GPP TR 21.905 3.2.0 (2000-10): Vocabulary for 3GPP Specifications

User: 'An entity, not part of UMTS, which uses UMTS services. Example: a person using a UMTS mobile station as a portable telephone'.

Subscriber: 'The responsibility for payment of charges incurred by one or more users may be undertaken by another entity designated as a subscriber. This division between use of and payment for services has no impact on standardisation.'

- 3G TS 22.101 3.12.0 (2001-01): Service principles

User Equipment: is a combination of mobile equipment (ME) and SIM/USIM.

USIM: User Service Identity Module is an application residing on the IC-Card used for accessing services with appropriate security.

IC Card: a card holding an Integrated Circuit containing subscriber, end user, authentication and/or application data for one or more applications.

- 3G TR 31.900 V0.2.0 (2001-01): SIM/USIM Internal and External Interworking Aspects

2G and 3G ME have been defined:

> "A 3G ME is either a 3G single mode ME that only supports a 3G radio access network or a 2G/3G dual mode ME that supports both, a 2G radio access network (GSM) and a 3G radio access network , which ever is present. For better understanding, explicit usage of the term "2G/3G dual mode ME" shall point out particular requirements.
>
> A 2G ME does only support a 2G radio access network (GSM)."

2G and 3G AKA have been defined:

> 2G AKA is the procedure to provide authentication of an ICC to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in GSM 03.20. In a mixed 2G/3G network environment 2G AKA is performed when - except for the BSS - at least one other element is 2G.
>
> 3G AKA is the procedure to provide mutual authentication between an ICC and a serving network domain and to generate the keys CK and IK in accordance to the mechanisms specified in 3G TS 33.102. For 3G AKA all involved -elements - except for the BSS - have to be 3G.

2G and 3G Security Context have been defined:

2G Security Context is a state that is established between a user and a serving network domain (i.e. between the ICC and the VLR/SGSN) after the execution of 2G AKA, with ciphering Kc available at either side.

3G Security Context is a state that is established between a user and a serving network domain (i.e. between the ICC and the VLR/SGSN) after the execution of 3G AKA, with ciphering and integrity protection keys CK and IK available at either side. 3G Security Context is still given, if these keys are converted into Kc to work with a 2G BSS.

2G and 3G VLR/SGSN, 2G and 3G HLR/AuC have not been defined.

- 3G TS 33.102 V3.7.0 (2000-12): Security Architecture

UMTS subscriber: a mobile station that consists of user equipment with a USIM inserted.

GSM subscriber: a mobile station that consists of user equipment with a SIM inserted.

Quintet, UMTS authentication vector: temporary authentication data that enables an VLR/SGSN to engage in UMTS AKA with a particular user. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Triplet, GSM authentication vector: temporary authentication data that enables an VLR/SGSN to engage in GSM AKA with a particular user. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

User access module: either a USIM or a SIM

Mobile station, user: the combination of user equipment and a user access module.

UMTS security context: a state that is established between a user and a serving network domain as a result of the execution of UMTS AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI.

GSM security context: a state that is established between a user and a serving network domain usually as a result of the execution of GSM AKA. At both ends "GSM security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

---

2. Proposal for Specification/Report updates.

- TS 33.102 shall refer to definitions of TR 21.905 and TS 22.101 in stead of duplicating definitions.

- TS 33.102 uses ‘GSM subscriber’ and ‘UMTS Subscriber’ in another context than TR 21.905.

TS 33.102 shall note that ‘subscriber’ is used with a different meaning that the base definitions of TR 21.905.

- TS 33.102 uses ‘user‘ with 2 different meanings.
  - user as meant in 5.3 "User domain security" and 5.5 "visibility". This matches the definitions of TR 21.905: The user as being a physical person.
  - user as synonymous for ‘UMTS subscriber’ in other sections of TS 33.102.

  The term ‘user’ is here mostly synonymous to ‘UMTS subscriber’ or USIM(-application) and shall be replaced in that way depending what best fits in the context of the description.

- TR 31.900 incorrect definition:

  3G AKA is the procedure to provide mutual authentication between an ICC and a serving network domain and to generate the keys CK and IK in accordance to the mechanisms specified in 3G TS 33.102. For 3G AKA all involved -elements - except for the BSS - have to be 3G.

  → The network is not authenticated. The ICC does only know that the Serving Network has the permission from the home network and that the authentication is recent.

- TR 31.900 shall refer to definitions of TS 33.102.

  - Option 1: Both documents shall use the same consistent set of 2G/3G definitions.

  Consequence: Big Change Request to TS 33.102. Will other 3GPP groups, that do stage 3 specification, be happy with this ?

  - Option 2: TS 33.102 shall keep using R98-/R99+ definitions, TR 31.900 the 2G/3G definitions.

  Consequence: TR 31.900 has to complete and correct his 2G/3G definitions and provide a mapping between R98-/R99+ and 2G/3G definitions.

  - Option 3: TR 31.900 shall use R98-/R99+ definitions too.

  Consequence: TR 31.900 has to be reworked completely.

  SA3 shall decide which option is preferred, given the fact that developing 2G/3G definitions for TS 33.102 are to be based on the capability of a Network Element or Mobile Equipment to perform UMTS (3G) or GSM (2G) AKA. 2G/3G definitions cannot be purely based on the attached Interfaces of a Network Element or Mobile Equipment. This is illustrated in the following set of 'draft' 2G/3G definitions.

  2G AKA: The entity Authentication and Key Agreement procedure to provide authentication of an ICC to a serving network domain and to generate the key Kc in accordance to the mechanisms specified in TS ETSI GSM 03.20.

  2G HLR/AuC: A HLR/AuC that supports triplet generation for GSM subscribers. A 2G HLR/AuC may support MAP version 3 to transport the triplets to a VLR/SGSN, but does not support quintet generation.

  ***2G ME**: Mobile Equipment that does only support 2G AKA and can only be attached to GSM BSS*

  2G security context: The state that is established between a user and a serving network domain (i.e. between the ICC and the VLR/SGSN) after the execution of 2G AKA. At both ends "2G security context data" is stored, that consists at least of the GSM cipher key Kc and the cipher key sequence number CKSN.

  ***2G VLR/SGSN**: A VLR/SGSN that supports 2G AKA and can only be attached to GSM BSS over the A/Gb-interface .*

  3G AKA: The entity Authentication and Key Agreement procedure to provide authentication of an *USIM* to a serving network domain, to check that the serving Network is allowed to authenticate and to generate the keys CK and IK in accordance with the mechanism in this specification.

  3G HLR/AuC: A HLR/AuC that supports quintet generation for UMTS subscribers. A 3G HLR/AuC shall support MAP version 3 for transporting quintets to a 3G VLR/SGSN. A 3G HLR/AuC may additionally support triplet generation for GSM subscribers.

  ***3G ME**: Mobile equipment supporting 3G AKA and 2G AKA. Either a single mode ME that only supports a 3G radio access network, a 2G/3G dual mode ME that supports both a 2G radio access network (GSM) and a 3G radio access network, or a single mode ME that only supports 2G radio access network(GSM).*

  3G security context: The state that is established between a user and a serving network domain (i.e. between the ICC and the VLR/SGSN) after the execution of 3G AKA. At both ends "UMTS security context data" is stored, that consists at least of the UMTS cipher/integrity keys CK and IK and the key set identifier KSI. 3G Security Context is still given, if the keys CK/IK are converted into Kc to work with a GSM BSS.

  ***3G VLR/SGSN**: A VLR/SGSN that supports 3G AKA and optionally supports 2G AKA. It can be attached to a GSM BSS via the A/Gb-interface and/or UTRAN via the Iu-interface.*

  The current definitions of 2G and 3G ME in TR 31.900 are based on the access capabilities (UTRAN/GSM). But what if a GSM only ME (it may support USIM-ME interface) also supports 3G AKA in a future 3GPP release?

- Proposed correction of definitions for TS 33.102: (Corrections in **bold**)

UMTS subscriber: a **Mobile Equipment** with a **UICC** inserted **and activated USIM-application**.

GSM subscriber: a **Mobile Equipment** with a SIM inserted **or a Mobile Equipment with a UICC inserted and activated SIM-application.**

Quintet, UMTS authentication vector: temporary authentication **and key agreement** data that enables an VLR/SGSN to engage in UMTS AKA with **a UMTS subscriber**. A quintet consists of five elements: a) a network challenge RAND, b) an expected user response XRES, c) a cipher key CK, d) an integrity key IK and e) a network authentication token AUTN.

Triplet, GSM authentication vector: temporary authentication **and key agreement data** that enables an VLR/SGSN to engage in GSM AKA with a **UMTS or GSM subscriber**. A triplet consists of three elements: a) a network challenge RAND, b) an expected user response SRES and c) a cipher key Kc.

- Proposed additions for TS 33.102: (in case option 2 or 3 is selected)

R99+ and R98- definitions have to be added.