3GPP-SA3 Meeting #16
Sophia Antipolis, France 28-30 November 2000

Document ***S3-000665***
e.g. for 3GPP use the format TP-99xxx
or for SMG, use the format P-99-xxx

CHANGE REQUEST

Please see embedded help file at the bottom of this page for instructions on how to fill in this form correctly.

33.102 **CR** Current Version: 3.6.0

GSM (AA.BB) or 3G (AA.BBB) specification number ↑ *↑ CR number as allocated by MCC support team*

For submission to: SA#10
list expected approval meeting # here ↑

for approval	☒	Strategic	□	*(for SMG use only)*
for information	□	non-strategic	□	

Form: CR cover sheet, version 2 for 3GPP and SMG *The latest version of this form is available from:* ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM □ ME □ UTRAN / Radio □ Core Network ☒
(at least one should be marked with an X)

Source: Nokia **Date:** 30 October 2000

Subject: Clarification of terms R99+ and R98-

Work item:

Category:	F	Correction	☒	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
(only one category	B	Addition of feature	□		Release 97	□
shall be marked	C	Functional modification of feature	□		Release 98	□
with an X)	D	Editorial modification	□		Release 99	☒
					Release 00	□

Reason for change: The following terms: - R98- and R99+ are used in the specification, but are not defined. Besides, these terms are not self evident.

This CR adds the definitions in question to the specification.

Clauses affected: 3.1

Other specs affected:	Other 3G core specifications	□	→ List of CRs:
	Other GSM core specifications	□	→ List of CRs:
	MS test specifications	□	→ List of CRs:
	BSS test specifications	□	→ List of CRs:
	O&M specifications	□	→ List of CRs:

Other comments:

help.doc

<--------- double-click here for help and instructions on how to create a CR.

3 Definitions, symbols and abbreviations

3.1 Definitions

In addition to the definitions included in TR 21.905 [3], for the purposes of the present document, the following definitions apply:

R98-: Refers to a network node or ME that conforms to R97 and R98 specifications. E.g. R98- 2G-SGSN supports Gb interface, GTPv0, etc; R98- HLR shall hold records on only GSM subscribers (SIM).

R99+: Refers to a network node or ME that conforms to R99 and newer specifications. E.g. R99+ 2G-SGSN supports Gb interface, GTPv1 and GTPv0, R99 MAP, etc; R99+ HLR shall hold records of UMTS subscribers (USIM), and optionally of GSM subscribers as well.

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities or processes.

Data integrity: The property that data has not been altered in an unauthorised manner.

Data origin authentication: The corroboration that the source of data received is as claimed.

Entity authentication: The provision of assurance of the claimed identity of an entity.

Key freshness: A key is fresh if it can be guaranteed to be new, as opposed to an old key being reused through actions of either an adversary or authorised party.

USIM – User Services Identity Module. In a security context, this module is responsible for performing UMTS subscriber and network authentication and key agreement. It should also be capable of performing GSM authentication and key agreement to enable the subscriber to roam easily into a GSM Radio Access Network.

SIM – GSM Subscriber Identity Module. In a security context, this module is responsible for performing GSM subscriber authentication and key agreement. This module is **not** capable of handling UMTS authentication nor storing UMTS style keys.

UMTS Entity authentication and key agreement: Entity authentication according to this specification.

GSM Entity authentication and key agreement: Entity authentication according to TS ETSI GSM 03.20

User access module: either a USIM or a SIM

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

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.

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.

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.

Authentication vector: either a quintet or a triplet.

Temporary authentication data: either UMTS or GSM security context data or UMTS or GSM authentication vectors.