3GPP TSG SA WG3 Security — S3#23 **S3-020348**
9 - 12 July 2002
Helsinki, Finland

3GPP TSG-SA WG3 LI Meeting #11 ***Tdoc S3LI02_114 R2***
Budapest, Hungary. 04 – 06 June 2002

CR-Form-v4

CHANGE REQUEST

⌘ **33.106** **CR** **CRNum** ⌘ rev **-** ⌘ Current version: **5.1.0** ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Changes to 33.106 to clarify interception capabilities.
Source:	⌘	SA WG3-LI (Nortel Networks)
Work item code:	⌘	SEC-LI
Date:	⌘	4 June 2002
Category:	⌘	**F**
Release:	⌘	Rel-5

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:
2 (GSM Phase 2)
R96 (Release 1996)
R97 (Release 1997)
R98 (Release 1998)
R99 (Release 1999)
REL-4 (Release 4)
REL-5 (Release 5)

Reason for change:	⌘	The reference to J-STD-025 is updated to a later revision. In addition, include enhancements and clarification regarding requirements for encryption of intercepted communications, unobtrusiveness of interception, and integrity of intercepted data.
Summary of change:	⌘	Clarify the handling of interception (e.g., unobtrusiveness) and update to a Section 2 references.
Consequences if not approved:	⌘	Misalignment with J-STD-025-A.

Clauses affected:	⌘	2, 5.2.1.3, and 5.6
Other specs affected:	⌘	☐ Other core specifications ⌘ ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.

[1] European Union Council Resolution on the Lawful Interception of Telecommunications (17. January 1995)

[2] ETR 331: "Definition of User Requirements for Lawful Interception of Telecommunications; Requirements of the Law Enforcement Agencies".

[3] ES 201 158: "Lawful Interception; Requirements for network functions".

[4] ES 201 671: "Handover Interface for the lawful interception of telecommunications traffic".

[5] GSM 01.33: "Lawful Interception requirements for GSM".

[6] GSM 02.33:" Lawful Interception - stage 1".

[7] GSM 03.33: "Lawful Interception - stage 2".

[8] J-STD-025-A ~~Interim Standard~~, "Lawfully Authorized Electronic Surveillance".

5.2.1.3 Security of processes

The intercept function shall only be accessible by authorised personnel.

To be effective, interception must take place without the knowledge of either party to the communication. Therefore, decryption must also take place without either party being aware that it is happening.

No indication shall be given to any person except authorised personnel that the intercept function has been activated on a target. Authentication, encryption, audits, log files and other mechanisms may be used to maintain security in the system. Audit procedures should be capable of keeping accurate logs of administration commands.

NWOs/APs/SvPs shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of facilitating authorized communications interceptions and access to intercept related information unobtrusively and with a minimum of interference with any subscriber's telecommunications service and in a manner that protects:

(A) the privacy and security of communications and intercept related information not authorized to be intercepted; and
(B) information regarding the LEA's interception of communications and access to intercept related information.

A NWOs/APs/SvPs shall not be responsible for decrypting, or ensuring the LEA's ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the NWOs/APs/SvPs and the NWOs/APs/SvPs possesses the information necessary to decrypt the communication or the NWOs/ APs/SvPs provides encryption keys but does not provide the encryption itself. In the case that the NWOs/ APs/SvPs provides encryption keys to the subscriber or customer but does not provide the encryption itself, the NWOs/ APs/SvPs shall provide the keys to the LEA unless otherwise forbidden by national regulations.

5.6 Minimum service requirements

Quality of service, capacity, integrity, and reliability are the subject of bilateral agreement between the relevant authorities and the 3GMS operator. The QoS towards the delivery function provided by the network must be at least that the network provides to the target.