Technical Specification Group Services and System Aspects
Meeting #18, New Orleans, USA, 9-12 December 2002

**TSGS#18(02)0720**

**Source:** **SA WG3**

**Title:** **1 CR to 33.210 (Rel-6): Securing UTRAN/GERAN IP Transport interfaces and specifically the Iu interface with NDS/IP mechanisms**

**Document for:** **Approval**

**Agenda Item:** **7.3.3**

| SA doc# | Spec | CR | R | Phase | Subject | Cat | Current Version | WI | SA WG3 doc# |
|---|---|---|---|---|---|---|---|---|---|
| SP-020720 | 33.210 | 004 | | Rel-6 | Securing UTRAN/GERAN IP Transport interfaces and specifically the Iu interface with NDS/IP mechanisms | B | 5.1.0 | SEC-NDS-IP | S3-020685 |
| | | | | | | | | | |

**3GPP TSG-SA3 Meeting #26**
**Oxford, UK, 19-22 November 2002**

***Tdoc ⌘S3-020685***

*CR-Form-v7*

# CHANGE REQUEST

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ⌘ | **33.210** | **CR** | **004** | ⌘ **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:*** | UICC apps⌘ ☐ | ME ☐ | Radio Access Network ☒ | Core Network ☒ |

| | | |
|---|---|---|
| ***Title:*** | ⌘ | Securing UTRAN/GERAN IP Transport interfaces and specifically the Iu interface with NDS/IP mechanisms |
| ***Source:*** | ⌘ | SA WG3 |
| ***Work item code:*** | ⌘ | SEC1-NDS-IP |
| ***Date:*** | ⌘ | 20/11/2002 |
| ***Category:*** | ⌘ | **B** |
| ***Release:*** | ⌘ | Rel-6 |

*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)* |
| *Rel-6* | *(Release 6)* |

| | | |
|---|---|---|
| ***Reason for change:*** | ⌘ | Iu interface is carrying information that is classified as sensitive. Iu is used for conveying e.g. security keys, which are vital for the end-user security. Hence Iu interface needs to be encrypted along with the integrity check. |
| ***Summary of change:*** | ⌘ | Addition to Annex to cover the Iu interface also with NDS/IP mechanisms. |
| ***Consequences if not approved:*** | ⌘ | Security wise critical Iu interface would be left unprotected. |

| | | |
|---|---|---|
| ***Clauses affected:*** | ⌘ | Annex (normative) |

***Other specs affected:*** ⌘

| Y | N | | |
|---|---|---|---|
| X | | Other core specifications | ⌘ TS 25.412 |
| | X | Test specifications | |
| | X | 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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document.*

[1] 3GPP TS 21.133: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements".

[2] 3GPP TR 21.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Vocabulary for 3GPP Specifications".

[3] 3GPP TS 23.002: "3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Network architecture".

[4] 3GPP TS 23.060: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS); Service description; Stage 2".

[5] 3GPP TS 23.228: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2".

[6] 3GPP TS 29.060: "3rd Generation Partnership Project; Technical Specification Group Core Network; General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[7] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture".

[8] 3GPP TS 33.103: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Integration guidelines".

[9] 3GPP TS 33.120: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Principles and Objectives".

[10] 3GPP TS 33.203: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Access security for IP-based services".

[11] RFC-2393: "IP Payload Compression Protocol (IPComp)".

[12] RFC-2401: "Security Architecture for the Internet Protocol".

[13] RFC-2402: "IP Authentication Header".

[14] RFC-2403: "The Use of HMAC-MD5-96 within ESP and AH".

[15] RFC-2404: "The Use of HMAC-SHA-1-96 within ESP and AH".

[16] RFC-2405: "The ESP DES-CBC Cipher Algorithm With Explicit IV".

[17] RFC-2406: "IP Encapsulating Security Payload".

[18] RFC-2407: "The Internet IP Security Domain of Interpretation for ISAKMP".

[19] RFC-2408: "Internet Security Association and Key Management Protocol (ISAKMP)".

[20] RFC-2409: "The Internet Key Exchange (IKE)".

[21] RFC-2410: "The NULL Encryption Algorithm and Its Use With IPsec".

[22] RFC-2411: "IP Security Document Roadmap".

[23] RFC-2412: "The OAKLEY Key Determination Protocol".

[24] RFC-2451: "The ESP CBC-Mode Cipher Algorithms".

[25] RFC-2521: "ICMP Security Failures Messages".

[26] Internet Draft: "On the Use of SCTP with IPsec ", available as "draft-ietf-ipsec-sctp-04~~3~~.txt"

[27] RFC-1750: “Randomness Recommendations for Security".

[28] 3GPP TS 25.412: "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; UTRAN Iu interface signalling transport".

------------------------------------------------------------------------------------------------------------------------------------

------------------------------------------- NEXT MODIFIED SECTION -----------------------------------------------------------

------------------------------------------------------------------------------------------------------------------------------------

# Annex D~~X~~ (normative): Security protection of UTRAN/GERAN IP transport protocols

This section details how NDS/IP shall be used to protect UTRAN/GERAN IP transport protocols and interfaces.

## D~~X~~.1 The need for security protection

The control plane in question is used to transfer signalling messages in UTRAN/GERAN IP transport network. The UTRAN IP transport option is specified in Rel5 UTRAN Technical Specifications. UTRAN Iu interface signalling transport is specified in 3GPP TS 25.412 [28]. Based on the known security threats in IP networking, the traffic shall be protected properly. This is in order not to restrict the application of IP in UTRAN and GERAN only to closed network environments.

The security solution for IP based UTRAN/GERAN transport shall follow the principles introduced in the NDS/IP since the IPSec provides application independent security solution for all IP traffic.

Iu interface is carrying information that is classified as sensitive. Iu is used for conveying e.g. subscriber specific security keys. These keys are vital for the end-user security. Hence Iu shall~~must~~ be encrypted along with the integrity check.

## D~~X~~.2 Protection of UTRAN/GERAN IP transport protocols and interfaces

IPSec ESP shall be used with both encryption and integrity protection for all RANAP messages traversing inter-security domain boundaries ~~through the Iu interface~~.

Iu control plane traffic shall be routed via a SEG when it takes place between different security domains (in particular over those interfaces that may exist between different operator domains). In order to do so, operators shall operate NDS/IP Za-interface between SEGs.

It will be for the operator to decide whether and where to deploy Zb-interfaces in order to protect the RANAP messages over the Iu interface within the same security domain.

According to TS 25.412 [28] the multi homing services of SCTP shall be required at both ends of an SCTP-association to enable transport redundancy and reliability. Additional guidelines on how to apply IPSec in SCTP are specified in [26]. This RFC shall also apply to this NDS/IP Technical Specification.

Editor's Note; The reference to I-D "draft-ietf-ipsec-sctp-04.txt" shall be replaced by the corresponding RFC reference when this draft reaches RFC status.

---------------------------------------------------------------------------------------------------------------------------------

-------------------------------------------- NEXT MODIFIED SECTION --------------------------------------------------------------

---------------------------------------------------------------------------------------------------------------------------------

# Annex E~~D~~ (informative): Change history

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 03-2002 | SA_15 | SP-020117 | - | - | Approved at TSG SA#15 and placed under change control | 2.0.0 | 5.0.0 |
| 06-2002 | SA_16 | SP-020355 | 001 | | NDS/IP Confidentiality protection for IMS session keys | 5.0.0 | 5.1.0 |
| 06-2002 | SA_16 | SP-020356 | 002 | | Strengthening the requirements on IV construction to prevent attacks based on predictable IV | 5.0.0 | 5.1.0 |
| | | | | | | | |