**S3-000701**

# 3G TS 33.2xx V0.1.~~0~~1 (2000-~~10~~11)

*Technical Specification*

## 3rd Generation Partnership Project;
## Technical Specification Group SA3;
## Access security for IP-based services
## (Release ~~4~~5)

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented.
This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification.
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organisational Partners' Publications Offices.

Keywords

Access security, IP Multimedia

***3GPP***

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

# Contents

# Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

# Introduction

*This clause is optional. If it exists, it is always the third unnumbered clause.*

# 1 Scope

The scope for this technical specification is to specify the security features and mechanisms for secure access to the IM CN subsystem for the 3G mobile telecommunication system.

The IM CN SS in UMTS will support IP Multimedia applications such as video, audio and multimedia conferences. 3GPP has chosen SIP, Session Initiation Protocol as the signalling protocol for creating and terminating Multimedia sessions. This specification only deals with how the SIP signalling is protected, how the subscriber is authenticated and how the subscriber authenticate the IM CN SS network.

# 2 References

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

[1] 3G TS 33.102: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; 3G Security; Security Architecture".

[2] 3G TS 22.228: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Service Requirements for the IP Multimedia Core Network".

[3] 3G TS 23.228: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; IP Multimedia (IM) Subsystem".

[4] 3G TS 21.133: "3rd Generation Partnership Project (3GPP); Technical Specification Group (TSG) SA; Security Threats and Requirements ".

[5] IETF RFC 2246 (1999) “The TLS Protocol Version 1.0”

[6] IETF RFC 2402 (1998) “IP Authentication Header”

[7] IETF RFC 2406 (1998) “IP Encapsulating Security Payload (ESP)”

[8] IETF RFC 2409 (1998) “The Internet Key Exchange (IKE)”

[9] IETF RFC 2440 (1998) “Open PGP Message Format”

[10] IETF RFC 2543bis-02 (2000) “SIP: Session Initiation Protocol”

[11] IETF RFC 2617 (1999) “HTTP Authentication: Basic and Digest Access Authentication”

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply.

**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.

## 3.2 Symbols

For the purposes of the present document, the following symbols apply:

## 3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| AAA | Authentication Authorisation Accounting |
| AKA | Authentication and key agreement |
| CSCF | Call State Control Function |
| GGSN | Gateway GPRS Support Node |
| HSS | Home Subscriber Server |
| HTTP | Hypertext Transfer Protocol |
| IM | IP Multimedia |
| MAC | Message Authentication Code |
| ME | Mobile Equipment |
| PS | Packet Switched |
| SGSN | Serving GPRS Support Node |
| SIP | Session Initiation Protocol |
| UE | User Equipment |
| UICC | UMTS IC Card |
| USIM | User Services Identity Module |

# 4 Overview of the security architecture

*[Editor’s note This section shall have a figure of the overall architecture for the IM CN SS and explaining text on the trust relations, possible threats and a brief overview of the provided security features.]*

# 5 Security features

*[Editor’s note: This section shall explain the provided security features in detail]*

## 5.1 Secure access to IM CN SS

### 5.1.1 Authentication of the subscriber and the network

*[Editor’s note: This section shall deal with subscriber identity and authentication of the subscriber and Home Network/Serving Network]*

### 5.1.2 Confidentiality protection

*[Editor's note: This section shall deal with what confidentiality protection that is provided between different nodes both inter domain, intra domain and the UE]*

### 5.1.3 Integrity protection

*[Editor's note: This section shall deal with what integrity protection that is provided between different nodes both inter domain, intra domain and the UE]*

### 5.1.4 Visibility and configurability

*[Editor's note: This section shall contain what the subscriber shall be able to configure and what is visible for the subscriber regarding the actual protection the subscriber is provided with.]*

# 6 Security mechanisms

*[Editor's note: This section shall describe the security mechanisms that are provided inter domain, intra domain and to the UE.]*

## 6.1 Authentication and key agreement

*[Editor's note: This section shall describe in detail how the authentication is performed and how the keys are derived and delivered to the different nodes.]*

## 6.2 Confidentiality mechanisms

*[Editor's note: This section shall deal with cipher algorithms]*

## 6.3 Integrity mechanisms

*[Editor's note: This section shall deal with integrity algorithms]*

# 7 Security mode set-up

*Annexes are only to be used where appropriate:*

# Annex <A> (normative): <Normative annex title>

# Annex <X> (informative): Change history

*It is usual to include an annex (usually the final annex of the document) for specifications under TSG change control which details the change history of the specification using a table as follows:*

| Change history | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **Old** | **New** |
| 2000-10 | SA3#15bis | 33.2xx | | 0.1.0 | Initial version of the specification | | |
| 2000-11 | SA3#16 | | | 0.1.1 | Input from AdHoc meeting | | |
| | | | | | | | |
| | | | | | | | |
| Editor Krister Boman, Ericsson<br>Email: krister.boman@emw.ericsson.se<br>Telephone: +46 31 747 6045/ +46 70 604 0564 | | | | | | | |