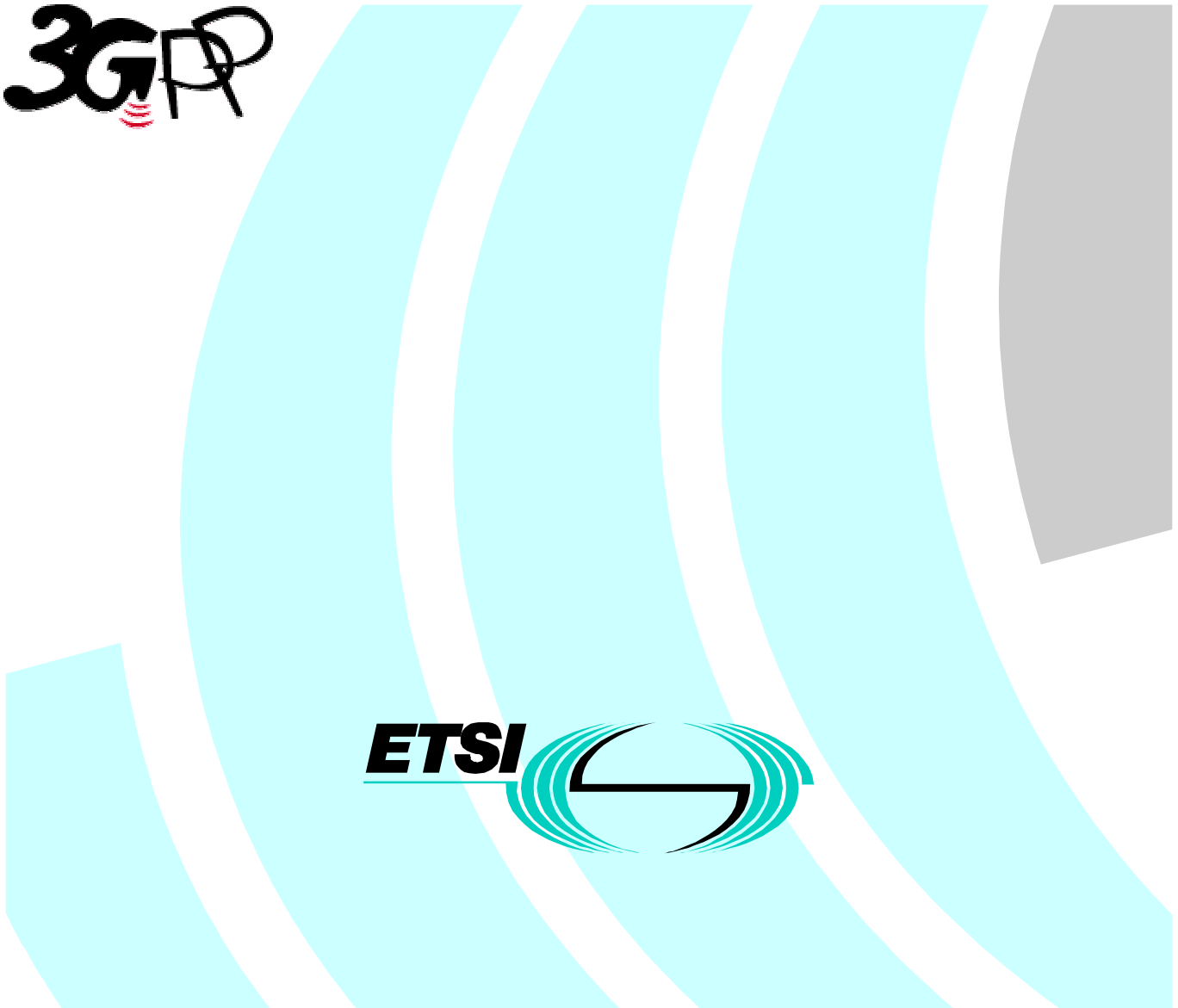
# ETSI TR 133 902 V3.1.0 (2000-01)

*Technical Specification*

**Universal Mobile Telecommunications System (UMTS);**
**Formal Analysis of the 3G Authentication Protocol**
**(3G TR 33.902 version 3.1.0 Release 1999)**



Reference
DTR/TSGS-0333902U

Keywords
UMTS

***ETSI***

Postal address
F-06921 Sophia Antipolis Cedex - FRANCE

Office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet
secretariat@etsi.fr
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

***Important notice***

This ETSI deliverable may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

***Copyright Notification***

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

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

The present document may refer to technical specifications or reports using their 3GPP identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables. The mapping of document identities is as follows:

For 3GPP documents:

3G TS | TR nn.nnn "<title>" (with or without the prefix 3G)

is equivalent to

ETSI TS | TR 1nn nnn "[Digital cellular telecommunications system (Phase 2+) (GSM);] Universal Mobile Telecommunications System; <title>

For GSM document identities of type "GSM xx.yy", e.g. GSM 01.04, the corresponding ETSI document identity may be found in the Cross Reference List on www.etsi.org/key

# Contents

# Foreword

This Technical Report has been produced by the 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 this TS, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version 3.y.z

where:

3 the first digit:

3 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 specification.

# 1 Scope

This report contains formal analyses of the authentication and key agreement (AKA) protocol specified in 3G TS 33.102. These analyses are carried out using various means of formal logic suitable for demonstrating security and correctness properties of the AKA protocol.

The structure of this technical specification is as follows:

clause 2 lists the references used in this specification;

clause 3 lists the definitions and abbreviations used in this specification;

clause 4 refers to the main body of this report. The main body is only referred to because it is not available in Word-, but only in pdf-format. The corresponding .pdf-documents are attached to this document.

# 2 References

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

All references are specific (identified by date of publication, edition number, version number, etc.) and are contained in the subsections of section 4 of this document.

# 3 Definitions and Abbreviations

All definitions and abbreviations are contained in the subsections of section 4 of this document.

# 4 Formal analyses

## 4.1 Formal analysis of the 3G authentication protocol with modified sequence number management

Annex A (TR_33902_Annex_A.pdf) contains a formal analysis of the 3GPP mechanism using a technique called Temporal Logic of Actions (TLA). The analysis seeks to prove that the 3GPP mechanism, if correctly implemented, will not "crash" or fall into failure scenarios.

## 4.2 Formal analysis of the 3G authentication and key agreement protocol

The formal analysis contained in Annex B (TR_33902_Annex_B.pdf) complements the TLA-based formal analysis contained in Annex A. An enhanced BAN logic is used to prove that the 3GPP authentication and key agreement protocol meets the required security goals.

# Annex A:
# Formal Analysis of the 3G Authentication Protocol with Modified Sequence Number Management

# Annex B:
# Formal analysis of 3G authentication and key agreement protocol

# Annex C:
# Change history

| Change history | | | | | |
|---|---|---|---|---|---|
| **TSG SA #** | **Version** | **CR** | **Tdoc SA** | **New Version** | **Subject/Comment** |
| SA#05 | 0.1.0 | | | 3.0.0 | Approved at SA#5 and placed under TSG SA Change Control |
| SA#06 | 3.0.0 | 001 | SP-99589 | 3.1.0 | Formal analysis of the 3G authentication protocol |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

# History

| Document history | | |
|---|---|---|
| V3.1.0 | January 2000 | Publication |
| | | |
| | | |
| | | |
| | | |