

3G TR 33.902 V3.1.0 (2000-01)

Technical Report

**3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
3G Security;
Formal Analysis of the 3G Authentication Protocol
(3G TR 33.902 version 3.1.0 Release 1999)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) 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™ system should be obtained via the 3GPP Organisational Partners' Publications Offices.

Reference

3TR/TSGS-0333902U

Keywords

Security, Authentication

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	4
1 Scope.....	5
2 References.....	5
3 Definitions and Abbreviations	5
4 Formal analyses	5
4.1 Formal analysis of the 3G authentication protocol with modified sequence number management	5
4.2 Formal analysis of the 3G authentication and key agreement protocol	5
Annex A: Formal Analysis of the 3G Authentication Protocol with Modified Sequence Number Management	6
Annex B: Formal analysis of 3G authentication and key agreement protocol	37
Annex C: Change history.....	45

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