ETSI TS 133 259 V14.0.0 (2017-04)

TECHNICAL SPECIFICATION

Digital cellular telecommunications system (Phase 2+) (GSM);
Universal Mobile Telecommunications System (UMTS);
LTE;
Key establishment between a UICC hosting device and a remote device
(3GPP TS 33.259 version 14.0.0 Release 14)

Reference

RTS/TSGS-0333259ve00

Keywords

GSM,LTE,SECURITY,UMTS

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - 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

Important notice

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 ETSI 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 (https://ipr.etsi.org/).

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 ETSI 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 Specification (TS) has been produced by ETSI 3rd Generation Partnership Project (3GPP).

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

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

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

The need to establish a secure channel between a UICC Hosting Device and a Remote Device connected via a local interface has been identified by the Personal Network Management work (see TS 22.259 [4]), in order to protect the communication between the UICC Hosting Device and the Remote Device.

This document describes key establishment between a UICC Hosting Device and a Remote Device.

1 Scope

The present document describes the security features and mechanisms to provision a shared key between a UICC Hosting Device and a Remote Device connected via a local interface. The shared secret is then intended to be used to secure the interface between the Remote Device and the UICC hosting device. Candidate applications to use this key establishment mechanism include but are not restricted to Personal Network Management (see TS 22.259 [4]).

The scope of this specification includes an architecture overview and the detailed procedure how to establish the shared key between the UICC Hosting Device and the Remote Device. This is different from the Technical Specification TS 33.110 [5] that describes an architecture overview and the detailed procedure how to establish the shared key between the UICC itself and the terminal hosting the UICC. The use cases utilizing the mechanisms described in this specification are seen to be different to the use cases where "Key establishment between a UICC and a terminal", PSK TLS as specified in TS 33.310 [19], is utilized.

The solution described in this document is built on the existing infrastructure defined in "GBA", TS 33.220 [3].

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

[2] 3GPP TS 31.101: "3rd Generation Partnership Project; Technical Specification Group Terminals; UICC-terminal interface; Physical and logical characteristics".

[3] 3GPP TS 33.220: "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture".

[4] 3GPP TS 22.259: "Service Requirements for Personal Network Management; Stage 1".

[5] 3GPP TS 33.110: "Technical Specification Group Services and System Aspects; Key establishment between a UICC and a terminal".

[6] Void.

[7] Void.

[8] Void.

[9] 3GPP TS 29.109: "Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3".

[10] 3GPP TR 33.905: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Recommendations for trusted open platforms".

[11] 3GPP TS 24.008: "Mobile radio interface Layer 3 specification; Core network protocols; Stage 3".

[12] NIST, FIPS PUB 180-2: "Secure Hash Standard (SHS)".

[13] IETF RFC 4634 (2006): US Secure Hash Algorithms (SHA and HMAC-SHA).

[14] IETF RFC 2104 (1997): "HMAC: Keyed-Hashing for Message Authentication".