ETSI TS 133 204 V9.0.0 (2010-02)

Technical Specification

Digital cellular telecommunications system (Phase 2+);
Universal Mobile Telecommunications System (UMTS);
LTE;
3G Security;
Network Domain Security (NDS);
Transaction Capabilities Application Part (TCAP)
user security
(3GPP TS 33.204 version 9.0.0 Release 9)

Reference

RTS/TSGS-0333204v900

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

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document 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.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

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 (http://webapp.etsi.org/IPR/home.asp).

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.

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 absence of security in Signalling System No. 7 (SS7) networks is an identified security weakness in 2G systems. This was formerly perceived not to be a problem, since the SS7 networks were the provinces of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions.

For 3G systems it is a clear goal to be able to protect the core network signalling protocols, and by implication this means that security solutions shall be found for both SS7 and IP based protocols.

Various protocols and interfaces are used for control plane signalling within and between core networks. The security services that have been identified as necessary are confidentiality, integrity, authentication and anti-replay protection. These will be ensured by standard procedures, based on cryptographic techniques.

1 Scope

This technical specification covers the security mechanisms and procedures necessary to protect all TCAP user messages which are sent between different security domains. The complete set of enhancements and extensions to facilitate security protection for the TCAP protocol is termed TCAPsec and it covers transport security in the TCAP protocol itself and the security management procedures.

This technical specification contains the stage 2 specification for security protection of the TCAP protocol. The actual implementation (stage 3) specification can be found in TS 29.204 [9].

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: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 29.002: "Mobile Application Part (MAP) specification".

[3] NIST Special Publication 800-38A "Recommendation for Block Cipher Modes of Operation" December 2001.

[4] ISO/IEC 9797: "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher", Ed.1, 1999-12-16.

[5] FIPS Publication 197: "Specification for the Advanced Encryption Standard (AES)", November 26, 2001.

[6] 3GPP TS 33.210: "3G security; Network Domain Security (NDS); IP network layer security".

[7] W3C DTF profile of ISO 8601: 2000 - Data Elements and Interchange Formats - Information Interchange - Representation of Dates and Times. International Organization for Standardization. http://www.w3.org/TR/1998/NOTE-datetime-19980827.

[8] 3GPP TS 23.003: "Numbering, addressing and identification".

[9] 3GPP TS 29.204: "Signalling System No. 7 (SS7) security gateway; Architecture, functional description and protocol details "

3 Definitions, symbols and abbreviations

3.1 Definitions

In addition to the definitions included in TR 21.905 [1], for the purposes of the present document, the following definitions apply:

Anti-replay protection: Anti-replay protection is a special case of integrity protection. Its main service is to protect against replay of self-contained packets that already have a cryptographic integrity mechanism in place.

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.

Security Association: A logical connection created for security purposes. All traffic traversing a security association is provided the same security protection. The security association specifies protection levels, algorithms to be used, lifetimes of the connection etc.

SS7 Carrier: An SS7 network that is not a PLMN.

SS7 Security Gateway: A Network Node that terminates and initiates TCAPsec. Similar to a SEG (see TS 33.210 [6]), the SS7 security Gateway is used for communication between two SS7 security domains.

TCAPsec: The complete collection of protocols and procedures needed to protect TCAP user messages.

3.2 Symbols

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

f6	TCAPsec encryption algorithm.
f7	TCAPsec integrity algorithm.
Zf	TCAPsec reference point between SS7-SEGs engaged in security protected signalling.

3.3 Abbreviations

In addition to the abbreviations included in TR 21.905 [1], for the purposes of the present document, the following abbreviations apply:

AES	Advanced Encryption Standard
FALLBACK	Fallback to unprotected mode indicator
IP	Internet Protocol
IV	Initialisation Vector
MAC	Message Authentication Code
MAC-M	MAC used for TCAP user
MAP	Mobile Application Part
NDS	Network Domain Security
NE	Network Entity
PROP	Proprietary field
SA	Security Association
SAD	Security Association Database
SEA	SS7 security gateway Encryption Algorithm identifier
SEK	SS7 security gateway Encryption Key
SIA	SS7 security gateway Integrity Algorithm identifier
SIK	SS7 security gateway Integrity Key
SPD	Security Policy Database
SPI	Security Parameters Index
SS7-SEG	SS7 security gateway
TCAPsec	TCAP user security – the SS7 security gateway security protocol suite
TCAP user	Application Part identified by the SCCP Subsystem Numbers of TS 23.003 [8]
TVP	Time Variant Parameter

3.4 Conventions

All data variables in this specification are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

4 Principles of TCAP user security

4.1 Overview

This technical specification defines mechanisms for protecting all TCAP user messages called TCAPsec. Another approach which could partially achieve the same goal as TCAPsec is the use of NDS/IP [6] at the network layer when IP is used as the transport protocol. However, whenever inter-working with networks using SS7-based transport is necessary, protection with TCAPsec shall be used.

The benefit for an operator applying TCAPsec will gradually increase when more interconnected operators also apply TCAPsec. TCAPsec can be used together with TCAP handshake solutions, however when using TCAPsec for MAP SMS transfers between two PLMNs, running TCAP handshake in addition does not add more security.

NOTE 1: A limited level of MAP message authenticity can be achieved without the use of SS7-SEGs by using a TCAP handshake prior to the MAP payload exchange. Annex D describes the use of the TCAP handshake for MAP SMS transfers.

NOTE 2: TCAPsec does not validate the TCAP user payload content (e.g. SMS payload address correlation as described for TCAP handshake in Annex D). Message screening functions for particular message types may be needed on top of TCAPsec.

NOTE 3: In order to prevent all active attacks all interconnected operators shall route all SS7 traffic via SS7-SEGs.

Before protection can be applied, Security Associations (SA) need to be established between the respective SS7-SEG. Security associations define, among other things, which keys and algorithms to use at the SS7-SEG. The necessary SAs between networks are negotiated between the respective network operators. The negotiated SA will be effective PLMN-wide and distributed to all SS7-SEGs. Each SS7-SEG contains policy information containing the protection mode that shall be applied. Protected TCAP user signalling traffic will, for routing purposes, be indistinguishable from unprotected traffic to all parties except for the sending and receiving entities.

Annex B includes detailed procedures on how secure TCAP user signalling is performed between two SS7-SEGs.

4.2 Network architecture

4.2.1 General

TCAPsec can be applied between different types of SS7 networks:

a) between two PLMN's.

b) between a PLMN and an SS7-carrier.

c) between two SS7-carriers.

The first case is considered in the end-to-end architecture (cf. clause 4.2.2). This architecture is applied in case the communicating PLMNs do not wish to trust intermediate SS7-networks.

In a hub-and-spoke architecture, a concatenation of multiple second and third cases may happen (cf. clause 4.2.3). Using this architecture is required if certain payload related services are performed by an SS7-carrier for whom the SS7-carrier is trusted by the PLMN.

4.2.2 End-to-end architecture

In a PLMN that employs SS7-SEGs all TCAP user signalling messages entering or leaving the PLMN have to transit an SS7-SEG which belongs to the PLMN and which performs the protection of outgoing messages and the protection checking and de-protection or blocking of incoming messages. SS7-SEG shall do Global Title Translation. For all unprotected messages from network elements inside one PLMN that are destined for another PLMN, the destination point is a SS7-SEG of the originating PLMN. After the messages are protected by a SS7-SEG of the originating PLMN, this SS7-SEG shall direct the message towards the destination NE (cf. figure 4.2-1).

One or several SS7-SEGs may be employed within a PLMN.

An SS7-SEG may be co-located with any TCAP user NE or it may stand alone. However, for the purpose of this specification and without imposing any restrictions, it is assumed that the SS7-SEG is stand alone.

It is further assumed that the SS7-SEGs are located at the border of the PLMN i.e. incoming messages transit an SS7-SEG before they reach any other node within the PLMN, and outgoing messages transit an SS7-SEG immediately before reaching a node outside the PLMN.

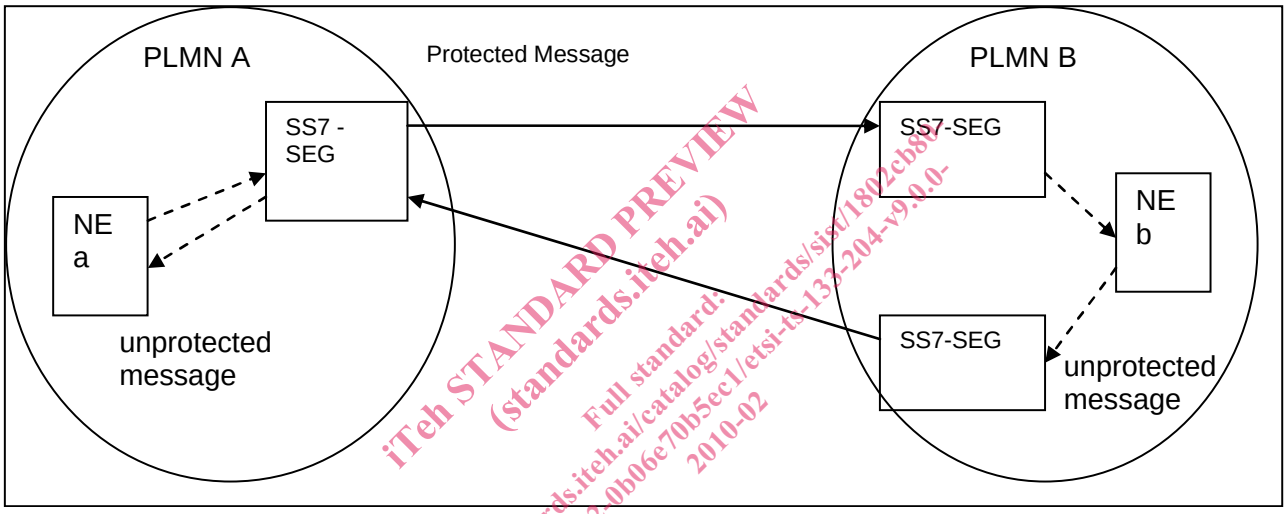

Figure 4.2-1: End-to-end SS7-Security Gateway Architecture

4.2.3 Hub-and-Spoke architecture

Using a hub-and-spoke architecture for SS7SEGs is required in following cases

a) The intermediate SS7-carrier has to perform TCAP user payload modification

An example of such a service is steering of roaming. Another example is an SMS hubbing architecture where the HUB (i.e. the SS7 carrier) has to insert a virtual SMSC-address in the MAP message.

b) The intermediate SS7-carrier needs to perfom protocol interworking.

Examples are inter-standard SMS for roaming into CDMA, and a CAMEL Gateway.

Using a hub-and-spoke architecture for SS7SEGs may be used for following cases but can also be performed in the end-to-end architecture.

a) The intermediate SS7-carrier performs message screening (e.g. SPAM control) and may have to drop messages.

If the communicating PLMNs have agreed to use protection mode 1 then using the end-to-end architecture is preferred from a security point of view.

If the communicating PLMNs have agreed to use protection mode 2 and both PLMNs find it acceptable to share the confidentiality key with the SS7 carrier then the end-to-end architecture can be used and is preferred from a security point of view. If confidentiality key sharing is not acceptable then the hub-and-spoke architecture is the only possible solution.