ETSI TS 133 204 V10.0.0 (2011-04)

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 10.0.0 Release 10)

Reference
RTS/TSGS-0333204va00

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

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.

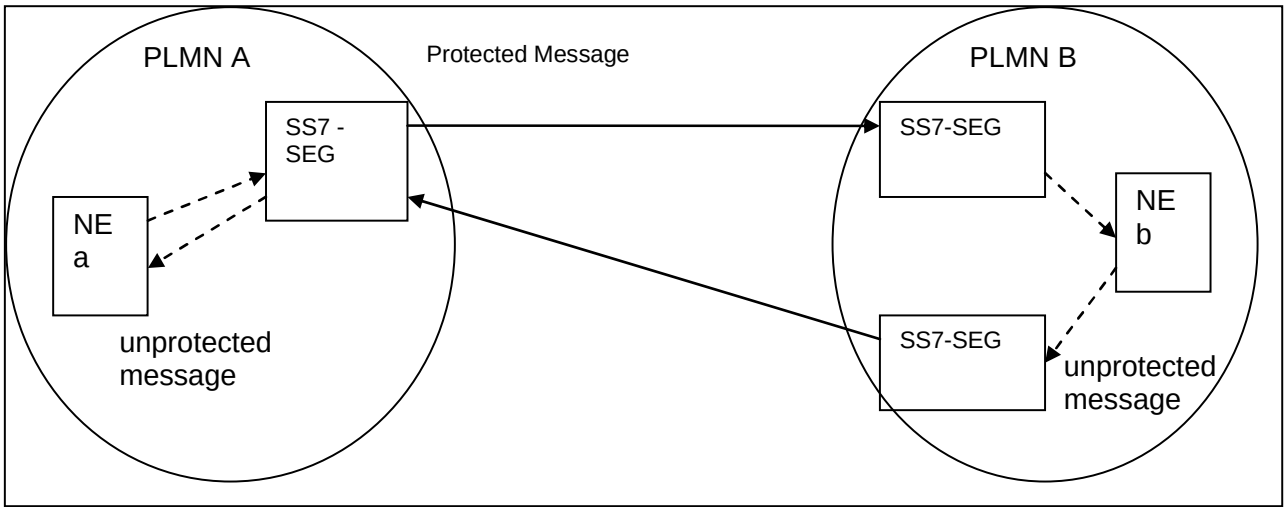

Figure 4.2-1: End-to-end SS7-Security Gateway Architecture

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.

b) The intermediate SS7-carrier performs advanced reporting.

The same considerations as for case c apply.

Figure 4.2-2 is one example of such a hub-and-spoke architecture.

NOTE: From a security point of view the number of intermediate hubs should be limited.

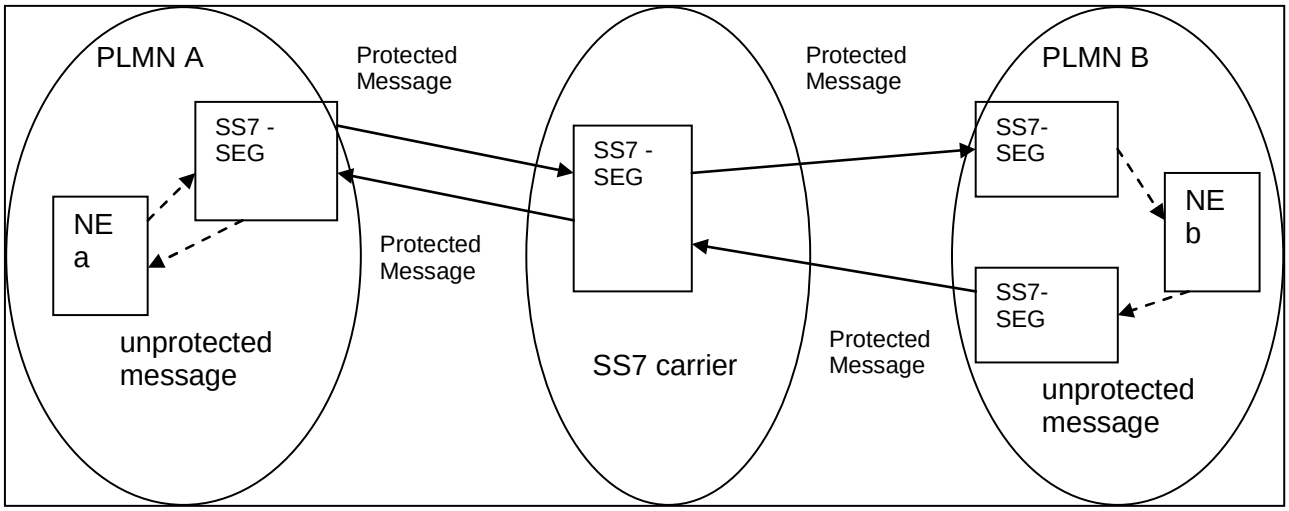

Figure 4.2-2: Example of Hub-and-Spoke SS7-Security Gateway Architecture

5 TCAP user security (TCAPsec)

5.1 Security services provided by TCAPsec

The security services provided by TCAPsec are:

- data integrity;
- data origin authentication;
- anti-replay protection;
- confidentiality (optional).

5.2 Properties and tasks of an SS7-SEG

An SS7-SEG shall maintain the following databases:

- SPD-SEG: A database containing TCAPsec policy information (see clause 5.3);
- SAD-SEG: A database containing TCAPsec SA information. SS7-SEG shall monitor the SA hard expiry time and expired SAs shall be deleted from the database (see clause 5.4).

SS7-SEG shall be able to perform the following operations:

- Secure TCAP user signalling (i.e. send/receive protected or unprotected messages) according to information in SPD-SEG and SAD-SEG. The structure of protected messages is defined in clause 5.5 and the protection algorithms are defined in clause 5.6.

5.3 Policy requirements for the TCAPsec Security Policy Database (SPD)

The security policies for TCAPsec key management are specified in the SS7-SEG"s SPD. SPD entries define per peer network whether protection shall be applied, and if protection shall be applied then which protection mode shall be used. SPD entries of different SS7-SEGs within the same network shall be consistent.

Fallback to unprotected mode:

- The "fallback to unprotected mode" (enabled/disabled) is a parameter for the receiving direction per network, if enabled it allows the receiving network to accept unprotected traffic as well as protected traffic. If disabled, only protected traffic is to be accepted
- The use of the fallback indicator is specified in Annex B;
- The security measures specified in this TS are only fully useful for a particular network if it disallows fallback to unprotected mode for TCAP user messages received from any other network.

NOTE: The benefit gained for a sending operator A that applies TCAPsec for all or a subset of messages towards a peer network B is that spoofing of the SCCP calling party address for all or a subset of messages can be detected. The receiving network B is now able to reject unprotected messages for all or a subset of messages that need protection, with SCCP calling party addresses from network A.

Explicit policy configuration:

- The SPD shall contain an entry for each network the SS7-SEG is allowed to communicate with.

Protection granularity:

- SPD administration shall be allowed on TCAP user application part level for each network the SS7-SEG is allowed to communicate with.

Migration support between protection modes:

- An SPD entry may contain two protection modes for the same network. If this is the case then both protection modes shall be acceptable for incoming messages, but only one (preferred) protection mode shall be used for outgoing messages.

5.4 TCAPsec security association attribute definition

The TCAPsec security association shall contain the following data elements which can be classified in two groups

A) SA Identification attributes i.e. Network Ids and SPI:

In sending direction the SA identification is based on Destination Network Id. Per Destination Network Id more than one SA may exist. In the case where more than one valid SA is available at the SAD, the sending SS7-SEG shall choose the SA with the earliest soft expiry time.

In receiving direction the used SPI from within the TCAPsec security header can be used to retrieve the Origin Network Id.

B) Assigned cryptographic parameters per SPI:

Key and algorithm identifiers and SA lifetime.

SA Identification attributes:

- **Destination Network Id:**

  The Destination Network Id is a concatenation of the Country Code (CC) and National Destination Code (NDC) of the receiving network. The Destination Network-Id is used to identify which SAD-entry shall be used when traffic protection is needed.

- **Security Parameters Index (SPI):**

SPI is a 32-bit value that is used in combination with Destination Network Id to uniquely identify a TCAPsec SA. The SPI is used to identify which SAD entry shall be used when de-protecting traffic. Therefore the SPI needs to be assigned by the destination network.

- **Origin Network Id:**

  The Origin Network Id is a concatenation of the Country Code (CC) and National Destination Code (NDC) of the sending network.

Cryptographic parameters per SPI:

- **SS7 Security Gateway Encryption Algorithm identifier (SEA):**

  Identifies the encryption algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. Mapping of algorithm identifiers is defined in clause 5.6.

- **SS7 Security Gateway Encryption Key (SEK):**

  Contains the encryption key. The length of SEK is defined according to the algorithm identifier.

- **SS7 Security Gateway Integrity Algorithm identifier (SIA):**

  Identifies the integrity algorithm. Mode of operation of algorithm is implicitly defined by the algorithm identifier. Mapping of algorithm identifiers is defined in clause 5.6.

- **SS7 Security Gateway Integrity Key (SIK):**

  Contains the integrity key. The length of SIK is defined according to the algorithm identifier.

- **SA Hard Expiry Time:**

  Defines the actual expiry time of the SA. The Hard Expiry Time shall be given in UTC time with format YYYY-MM-DDThh:mm:ssTZD as described by W3C DTF [7].

- **SA Soft Expiry Time:**

  Defines Soft Expiry Time of the SA for outbound traffic. The format of the Soft Expiry Time is the same as the Hard Expiry Time. The SA Soft Expiry Time is determined by the Originating Network and shall expire before the SA Hard Expiry Time.

After the Hard Expiry Time has been reached, the SA shall no longer be used for inbound or outbound traffic. When the Soft Expiry Time is reached, the SA shall not be used any longer for the outbound traffic unless no other valid SA exists.

5.5 TCAPsec structure of protected messages

TCAPsec provides following protection modes and these are defined as follows:

Protection Mode 1: Integrity, Authenticity

Protection Mode 2: Confidentiality, Integrity, and Authenticity

In case a TCAP message does not require protection (as indicated by the SPD) then the message shall be routed unchanged by the SS7-SEG.

TCAP messages protected by means of TCAPsec include a Security Header and a Protected Payload.

Secured TCAP user messages have the following structure:

Security Header	Protected Payload

For detailed message structure see TS 29.204 [9]In all protection modes, the security header is transmitted in cleartext.

The intermediate unprotected TCAP message representation is the cleartext concatenation of DialoguePortion and ComponentPortion of the original TCAP message (after message reassembly if this applies).

For protection mode 1, the protected payload is the concatenation of the intermediate unprotected TCAP message representation and the message authentication code.

For protection mode 2, the protected payload is the concatenation of the result of applying the encryption function to the intermediate unprotected TCAP message representation, and the message authentication code.

For integrity and authenticity in protection mode 1, the message authentication code is calculated on the concatenation of the security header and the intermediate unprotected TCAP message representation. The message authentication code in protection mode 2 is calculated on concatenation of the security header and the result of applying the encryption function to the intermediate unprotected TCAP message representation.

5.5.1 TCAPsec security header

For Protection Mode 1, the security header is a sequence of the following elements:

Security header = SPI || TVP

For Protection Mode 2, the security header is a sequence of the following elements:

Security header = SPI || TVP || SS7-SEG Id || Prop

where

- **Security Parameters Index (SPI):**

  See Clause 5.4

- **TVP:**

  The TVP, used for replay protection of secured TCAP user message, is a 32 bit time-stamp. The receiving network entity will accept an operation only if the time-stamp is within a certain time-window. The resolution of the clock from which the time-stamp is derived is 0.1 seconds. The size of the time-window at the receiving network entity is not standardised.

- **SS7-SEG Id:**

  1 octet used to create different IV values for different SS7-SEGs within the same TVP period. It is necessary and sufficient that *SS7-SEG Id* is unique per network. (This is sufficient because sending keys are unique per network) The SS7-SEG Id shall be a unique number within the network.

- **Proprietary field (PROP):**

  1 octet used to create different IV values for different protected TCAP user messages within the same TVP period for one network entity. The usage of the proprietary field is not standardised.

5.5.2 Protected payload

5.5.2.1 Protection Mode 1

The protected payload of secured TCAP user messages in protection mode 1 takes the following form:

Cleartext|| f7(Security Header||Cleartext)

where "Cleartext" is the concatenation of DialoguePortion and ComponentPortion of the original TCAP message (after message reassembly if this applies). Therefore, in Protection Mode 1 the protected payload is a concatenation of the following information elements:

- Cleartext

- Message authentication code (MAC-M) calculated by the function f7

Authentication of origin and message integrity are achieved by applying the message authentication code (MAC-M) function f7 with the integrity key defined by the security association to the concatenation of Security Header and Cleartext. The MAC-M length shall be 32 bits.

5.5.2.2 Protection Mode 2

The protected payload of secured TCAP user Messages in protection mode 2 takes the following form:

f6(Cleartext) || f7(Security Header|| f6(Cleartext))

where "Cleartext" is the concatenation of DialoguePortion and ComponentPortion of the original TCAP message (after message reassembly if this applies). Confidentiality is achieved by encrypting Cleartext using the encryption function f6 with the confidentiality key defined by the security association and the initialisation vector (IV). Authentication of origin and integrity are achieved by applying the message authentication code (MAC-M) function f7 with the integrity key defined by the security association to the concatenation of Security Header and ciphertext. The MAC-M length shall be 32 bits. The length of the ciphertext is the same as the length of the cleartext.

5.6 TCAPsec algorithms

5.6.1 Mapping of TCAPsec SA encryption algorithm identifiers

The SEA algorithm indication fields in the TCAPsec SA are used to identify the encryption algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below.

Table 1: SS7 Security Gateway encryption algorithm identifiers

Encryption Algorithm identifier	Description
0	AES in counter mode with 128-bit key length (MANDATORY)
1	-not yet assigned-
:	-not yet assigned-
15	-not yet assigned-

5.6.1.1 Description of SEA-0

The SEA-0 algorithm is AES [5] used in counter mode with a 128-bit key and 128-bit counter blocks as described in clause 6.5 of FIPS 800-38A Recommendation for Block Cipher Modes of Operation [3]. The initial counter block T_1 is initialized with IV. Successive counter blocks T_j (J>1) are derived by applying an incrementing function over the entire block T_{j-1} (J>=2) (see Appendix B.1: The standard incrementing function of [3]).

5.6.2 Mapping of TCAPsec SA integrity algorithm identifiers

The SIA algorithm indication fields in the TCAPsec SA are used to identify the integrity algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below.

Table 2: SS7 Security Gateway integrity algorithm identifiers

Integrity Algorithm identifier	Description
0	AES in a CBC MAC mode with a 128-bit key (MANDATORY)
1	-not yet assigned-
:	-not yet assigned-
15	-not yet assigned-

5.6.2.1 Description of SIA-0

The SIA-0 algorithm is the ISO/IEC 9797 Part 1: padding method 2, MAC algorithm 1 (initial transformation=1, output transformation=1). No IV used. The MAC-length m is 32-bits (see clause 5.6.1). See ISO/IEC 9797 [4] for more information.

5.6.3 Construction of IV

The IV used in the encryption shall be constructed as follows:

$$IV = TVP \,||\, SS7\text{-}SEG\ Id \,||\, Prop \,||\, Pad$$

The padding field is used to expand *TVP* || *SS7-SEG Id* || *Prop* to the *IV* length required by the cryptographic scheme in use.

The IV length shall be 16 octets. The padding (Pad) shall be 10 octets with all bits set to zero.

Annex A (informative): Guidelines for manual key management

A.1 Inter-domain Security Association and Key Management Procedures

Manual Inter-domain Security Association and Key Management procedures is subject to roaming agreements.

Some important parts of an inter-domain Security Association and Key Management agreement are:

- to define how to carry out the initial exchange of TCAPsec SAs;
- to define how to renew the TCAPsec SAs;
- to define how to withdraw TCAPsec SAs (including requirements on how fast to execute the withdrawal);
- to decide if fallback to unprotected mode is to be allowed;
- to decide on key lengths, algorithms, protection mode, and SA expiry times, etc (TCAPsec SAs are expected to be fairly long lived).

An SA being used by an SS7-SEG for incoming traffic expires when it reaches its hard expiry time. When this occurs, the SS7-SEG can no longer use that SA to process incoming TCAPsec traffic. If a new additional valid SA is installed into the SS7-SEG, the "old" one shall still be kept until it reaches its hard expiry time, so as to be able to accept incoming traffic still received under the "old" SA.

An SA being used by an SS7-SEG for outgoing traffic expires when it reaches its soft expiry time. When this occurs, the SS7-SEG shall start using another valid SA. If no such valid SA exists, the SS7-SEG continues to use the "old" SA until it reaches its hard expiry time or another valid SA effectively becomes available.

In case the current SA gets compromised, a new valid SA should be made immediately available to all SS7-SEG, which should then stop using the compromised SA and delete it.

To ease SA renewal, both networks may decide to set up several TCAPsec SAs in advance so that SS7-SEGs can automatically switch from one SA to another SA. In such a situation, the TCAPsec SAs would have different soft and hard expiry times.

When more than one valid SA is available, the SS7-SEG chooses the one with the earliest soft expiry time.

A.2 Local Security Association Distribution

Manual Local Security Association Distribution is executed entirely within one network and is consequently at the discretion of the administrative authority.

The requirement on the manual distribution procedures can be summarized as follows:

- Procedures for transporting the relevant TCAPsec SA to the SS7-SEG shall be defined. In order to ensure that the TCAPsec SA are present when needed, all valid TCAPsec SA should be distributed to all SS7-SEG as soon as they are available.
- Procedures for revocation of TCAPsec SAs shall be defined.

Annex B (normative): TCAPsec message flows

Imagine a network scenario with two SS7-SEG at different PLMNs (SS7-SEGa in the sending PLMN A and a SS7-SEGb in the receiving PLMN B) willing to communicate using TCAPsec. Figure 1 presents the message flow.

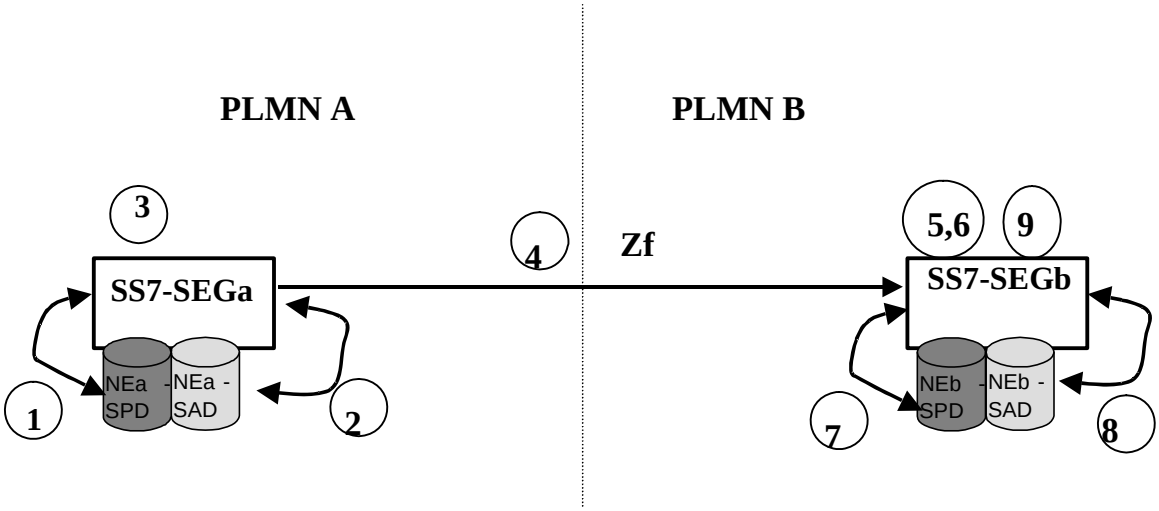

Figure B-1. TCAPsec Message Flow

NOTE: The same migrations can be applied within the Hub-and-spoke Architecture where one or both of the PLMNs take the role of an SS7 carrier.

According to Figure 1, when SS7-SEGa from PLMN A on behalf of NEa needs to send a message towards NEb within PLMN B using TCAPsec, the process is the following:

The Sending Entity SS7-SEGa performs the following actions during the outbound processing of every TCAP user message:

1. SS7-SEGa checks its Security Policy Database (SPD) to check if TCAPsec mechanisms shall be applied towards PLMN B:

   a) If the SPD does not mandate the use of TCAPsec for the TCAP user application part towards PLMN B, then normal TCAP communication procedures will be used and the process continues in step 4.

   b) If the SPD mandates the use of TCAPsec for the TCAP user application part towards PLMN B, then the process continues at step 2.

   c) If no valid entry in the SPD is found for PLMN B, then the communication is aborted and the message is discarded.

2. SS7-SEGa checks its Security Association Database (SAD) for a valid Security Association (SA) to be used towards PLMN B. In the case where more than one valid SA is available at the SAD, SS7-SEGa shall choose the one, the soft expiry time of which will be reached next.

   a) In case protection of TCAPsec messages towards PLMN B is not possible (e.g. no SA available, invalid SA…), then the message is discarded.

   b) If a valid SA exists then the process continues at step 3.

3. SS7-SEGa constructs the TCAPsec message towards NEb using the parameters (keys, algorithms) found in the SA and the protection mode from the SPD.

4. SS7-SEGa either:

a) sends a TCAPsec message towards PLMN B (from step 3).

b) forwards an unprotected TCAP message in the event that the SPD towards PLMN B allowed it (step 1.a).

At the Receiving PLMN, an SS7-SEG (e.g. SS7-SEGb) performs the following actions during the inbound processing of every TCAP user message it received:

5. If a TCAP message is received for which no valid SPD entry exists (i.e. SCCP calling party address is unknown) then the message is discarded (Process goes to END).

6. If an unprotected TCAP message is received, the process continues with step 7.

   Otherwise, SS7-SEGb decomposes the received TCAPsec message and retrieves SPI from the security header.

7. The SS7-SEGb checks the SPD:

   An unprotected TCAP message is received:

   a) If an unprotected TCAP message is received and fallback to unprotected mode is allowed for the specified SCCP calling party address and TCAP user application part, then the unprotected TCAP message is simply processed (Process goes to END)

   b) If an unprotected TCAP message is received, but the SPD mandates the use of TCAPsec and fallback to unprotected mode is NOT allowed for the specified SCCP calling party address and TCAP user application part, then the message is discarded.

   A TCAPsec message is received:

   c) If a TCAPsec message is received, but the SPD indicates that TCAPsec is NOT to be used, then the message is discarded.

   d) If a TCAPsec message is received and the SPD indicates that TCAPsec is required, then the process continues at step 8.

8. The receiving SS7-SEG checks its SAD to retrieve the relevant SA information for processing of the TCAPsec message:

   a) If the received SPI does not point to a valid SA, then the message is discarded.

   b) If the received SPI points to a valid SA, and if the Source and Destination Network Id, which are retrieved via the SPI, align with those from SCCP layer, then the SS7-SEG retrieves the protection mode from the SPD and the cryptographic information (keys, algorithms) from the SAD and the process continues at step 9, otherwise the message is discarded.

9. Freshness of the protected message is checked by ensuring the Time Variant Parameter (TVP) is in an acceptable window. Integrity and encryption mechanisms are applied to the message according to the identified protection level, by using the information in the SA (keys, algorithms).

   a) If the result after applying such mechanisms is NOT successful then the message is discarded.

   b) If the result after applying such procedures is successful, then SS7-SEG has the cleartext TCAP message NEa originally wanted to send to NEb. The cleartext TCAP message can now be forwarded by the receiving SS7-SEG to NEb (Process goes to END)

END: A cleartext TCAP user message is available at the receiving SS7-SEG.

In the event the received message at NEb requires an answer to NEa (Return Result/Error), an SS7 SEG in PLMN B will, on behalf of NEb perform the process in steps 1 to 4 acting as the Sender and an SS7 SEG in PLMN A will perform the process in steps 5 to 8 acting as the Receiver and forward a successfully received message to NEa.

Annex C (informative): High level migration strategy

This Annex describes three types of protection mode changes, which each may be performed per TCAP user application part between a pair of networks.

NOTE: The same migrations can be applied within the Hub-and-spoke Architecture where one or both of the PLMNs take the role of an SS7 carrier.

C.1 Transition phase from unprotected to protected message transfer

By applying a migration strategy which is coordinated between the two PLMN operators (A and B) it can be assured that protected messages are not sent from PLMN A to PLMN B (and vice versa) before operator B confirms completion of SS7-SEG introduction in his network.

In order to avoid traffic interruption during the transition phase from unprotected to protected message transfer between tw" operators' PLMNs the following course of action is recommended:

Precondition: It is assumed that neither operator A, nor operator B have activated TCAPsec for the TCAP user application part(s) that needs protection and now are going to set up use of TCAP user security for traffic to and from each other.

1. Operator A negotiates Security Associations with operator B and stores the SAs in the SAD. Both operators also agree on the policy that shall be applied for the different TCAP user application parts of the messages that needs to be exchanges between the PLMNs.

2. Operator A modifies the Security Policy in his gateways as follows: Messages received from operator B"s PLMN should be protected according to the indicated protection mode by the SPD; however fallback to unprotected mode is allowed, i.e. unprotected messages received from"operator B's PLMN are not blocked. This means that incoming messages with an SCCP calling party address pointing to operator B are accepted by PLMN A. Operator A does not send protected messages yet.

NOTE 1: When fallback to unprotected mode is allowed then other security measures may be used that assist in identifying the origin of the message to a certain trust level, e.g. TCAP handshake for MTforwardSM (see Annex D).

NOTE 2: As the fallback indicator can be specified per TCAP user application part between a pair of PLMN, this allows a gradual security upgrade.

3. When Operator A has completed step 2 in all his SS7-SEGs, he informs Operator B.

4. When Operator A receives confirmation that operator B also has performed step 2, Operator A modifies the Security Policy in his gateways as follows: Outgoing messages sent to operator B"s PLMN shall be protected as indicated by the SPD.

5. When Operator A has completed step 4 in all his SS7-SEGs, he informs Operator B which can then perform step 4 and 6 towards Operator A.

6. When Operator A receives confirmation from Operator B that he has performed step 4, Operator A modifies the Security Policy in his gateways as follows: Fallback to unprotected mode is not allowed, i.e. unprotected messages received from"operator B's PLMN will be blocked.

NOTE 3: After disabling fallback to unprotected mode then other security measures that are in use and that assist in identifying the origin of the message to a certain trust level, e.g. TCAP handshake for MTforwardSM (see Annex D), can be disabled.

C.2 Transition phase from protected message transfer to unprotected message transfer.

In order to avoid traffic interruption during the transition phase from protected to unprotected message transfer between two operators' PLMNs, the following course of action is recommended:

Precondition: It is assumed that operator A has already successfully set up the use of TCAP user security for traffic to and from operator B and is now going to remove use of TCAP user security for traffic to and from operator B.

1) Operator A modifies the Security Policy in his gateways as follows: Messages received from operator B's PLMN may still be protected according to the stored SA, however fallback to unprotected mode is allowed.

NOTE: Before setting fallback to unprotected mode to allowed, other security measures may be activated that assist in identifying the origin of the message to a certain trust level, e.g. TCAP handshake for MTforwardSM (see Annex D).

2) When Operator A has completed step 1 in all his SS7-SEGs, he informs Operator B.

3) When Operator A receives confirmation from Operator B that all SS7-SEGs in Operator B's PLMN have been set up to allow fallback to unprotected mode, Operator A changes the SPD entries to send unprotected outgoing messages via his SS7-SEGs, but allow the reception of protected messages from network B.

4) When Operator A has completed step 3 in all his SS7-SEGs, he informs Operator B.

5) When Operator A receives confirmation from Operator B that the SPD entries were changed to unprotected in all SS7-SEGs of Operator B's network, Operator A performs the similar change in his SS7-SEGs.

C.3 Transition phase from protected mode to another protected mode

In order to avoid traffic interruption during the phase where the used protection mode is modified in the SS7-SEGs' SPDs, the following course of action is recommended:

Precondition: It is assumed that operator A's policy is to protect all messages exchanged with operator B's PLMN with protection mode "integrity+authenticity"; now both Operators are going to modify the policy to protect messages sent to the other PLMN with protection mode "integrity+authenticity+confidentiality".

NOTE: The transition from protection mode "integrity+authenticity+confidentiality" to protected mode "integrity+authenticity" is similar as described below but with the protection modes reversed.

1) Operator A and B both modify the SPD by adding "integrity+authenticity+confidentiality" to the acceptable protection modes, i.e. they will now allow both "integrity+authenticity+confidentiality" and "integrity+authenticity" as acceptable protection modes, but outgoing messages are still sent with "integrity+authenticity".

2) When step 1 is completed in all SS7-SEGs of Operator B's PLMN, Operator A is informed. Similarly Operator A will inform Operator B after performing the actions of Step 1.

3) When Operator A (or Operator B) receives confirmation from Operator B (or Operator A) that the SPDs in all SS7-SEGs have been updated to accept the new protection mode in addition to the old one, Operator A (or operator B) modifies the SPD such that outgoing messages in his SS7-SEGs towards Operator B (or operator A) are send with only with protection mode "integrity+authenticity+confidentiality".

4) When step 3 is completed in all SS7-SEGs of Operator A's (or Operator B"s) PLMN, he informs Operator B (or Operator A).

5) When receiving confirmation that the SPDs have been updated in all SS7-SEGs of Operator A (or Operators B's) PLMN, Operator B (or Operator A) modifies the SPD by removing "integrity+authenticity" from the acceptable protection modes.

Annex D (normative): Using TCAP handshake for SMS transfer

The SMS Gateway/Interworking MSC operator and the serving node (MSC or SGSN) operator may agree to use the TCAP handshake as a countermeasure against SMS fraud for messages exchanged between their networks (for detailed message flows see TS 29.002 [2]). A limited level of authenticity is provided by the following mechanisms.

D.1 Mobile Terminated SMS

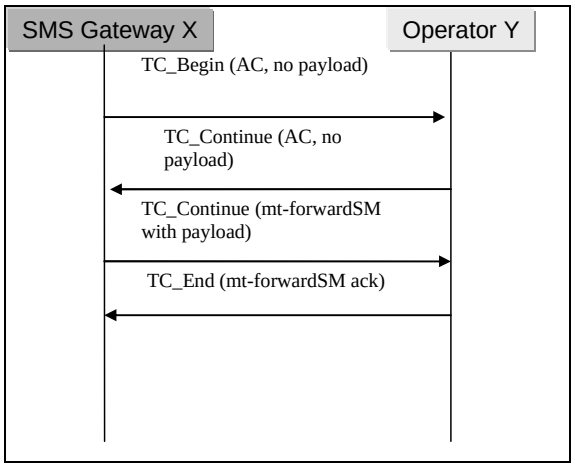

Figure D.1: MAP mt-Forward-SM messages using a TCAP Handshakes

If the serving network receives an mt-forward-SM MAP message which uses the TC_Continue to transfer the MAP payload then it is guaranteed that the SCCP calling party address of the (empty) TC_Begin message is authentic, otherwise the first TC-continue message would be sent to the falsified address. The correct message flow is guaranteed by the TCAP transaction capabilities (use of Transaction ID).

Unfortunately there are some ways in which a fraudulent SMS Gateway operator (called the originator in bullets (a) and (b)) may try to circumvent the implicit SCCP address authentication provided by the TCAP handshake.

(a) The originator includes a falsified SMS-GMSC address as SM-RP-OA in the mt-forward-SM payload carried by the TC-continue (third message in figure D.1)

(b) The originator tries to predict the TCAP transaction ID assigned by the serving node, which is to be used within the third message, and spoofs the third message without waiting for the second message. This attack has to be carried out within the right time window.

If TCAP handshake is to be used, the following measure shall be taken within the network of the serving node in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator.

MEAS-1: The receiving network shall verify if the received SMS-GMSC address (as SM-RP-OA in the third message) may be used from the SCCP Calling Party Address. Some operators use a single SMS-GMSC address for a range of SCCP Calling Party Addresses and this will need to be taken into consideration.

If TCAP handshake is to be used, at least one of the following measures shall be taken within the network of the serving node in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator.

MEAS-2a: The receiving node shall use mechanisms to ensure that the destination TCAP transaction ID which needs to be used within the third message is predictable with a probability of less than $1 / 2^{10}$ for a third party knowing all previous TCAP transaction ID values.

MEAS-2b: The receiving network shall wait n seconds before it processes the third message (TC-continue(mt-forwardSM with payload)). This should ensure that the TC_abort from the spoofed network is processed at the destination node earlier than a TC_continue including a successfully guessed TCAP Transaction ID value.

The following grouping method may be used for an operator to gradually introduce the TCAP handshake for mt-Forward-SM messages. Define an "operator group-1" as a trusted operator group and "operator group-2" as an un-trusted operator group. Agree that group-1 uses the TCAP handshake, while group-2 does not use the TCAP handshake. As specified by TS 29.002 [2] this requires that the SMS Gateway operators belonging to group-1 shall either use application context2 or 3 for mt-Forward-SM. The management of the two groups requires that the serving network shall implement a policy table of SCCP Calling Party Addresses for which a TCAP handshake is required.

If the above described grouping method is used then the following measure shall be taken at the serving network in order to counteract the spoofing possibilities of a malicious mt-Forward-SM originator that tries to circumvent the policy table checks.

MEAS-3: The serving network shall verify that the SCCP Calling Party Address of a first message with a payload (i.e. not using the TCAP handshake) is not from an SMS-GMSC-address as SM-RP-OA that shall use the TCAP handshake.

The benefit gained for operators that belong to group-1 is that spoofing of their SMS-GMSC-addresses is practically difficult if the policy table has been administrated accurately.

D.2 Mobile Originated SMS

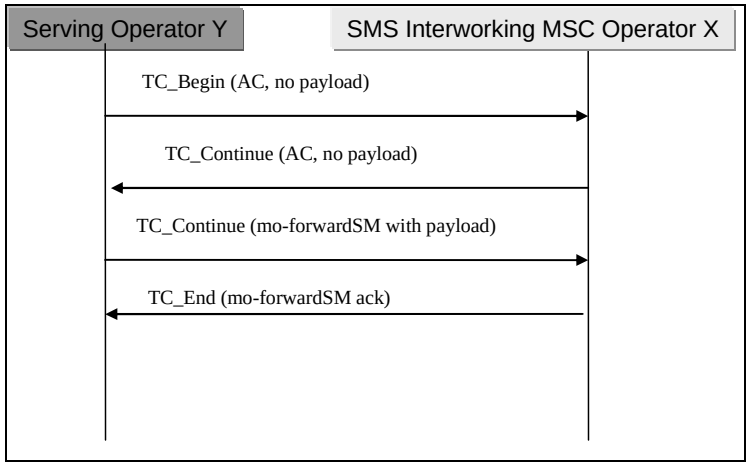

Figure D.2: MAP mo-Forward-SM messages using a TCAP Handshakes

If the serving network sends an mo-forward-SM MAP message which uses the TC_Continue to transfer the MAP payload then it is guaranteed that the SCCP calling party address of the (empty) TC_Begin message is authentic, otherwise the first TC-continue message would be sent to the falsified address. The correct message flow is guaranteed by the TCAP transaction capabilities (use of Transaction ID).

Unfortunately there are some ways in which a fraudulent serving (MSC or SGSN) operator (called the originator in bullets (a) and (b)) may try to circumvent the implicit SCCP address authentication provided by the TCAP handshake.

(a) The originator includes a falsified MSISDN as SM-RP-OA within the mo-forward-SM payload carried by the TC-continue (third message in figure D.2)

(b) The originator tries to predict the TCAP transaction ID assigned by the serving node, which is to be used within the third message, and spoofs the third message without waiting for the second message. This attack has to be carried out within the right time window.

If TCAP handshake is to be used, the following measure may be taken within the network of the SMS Interworking MSC in order to counteract the spoofing possibilities of a malicious mo-Forward-SM originator.

MEAS-1: The receiving node (i.e. SMS interworking MSC) may query the HLR to verify if the received SCCP Calling Party Address of the mo-forward-SM is from the same network which is currently serving the subscriber (MSISDN contained in SM-RP-OA in the third message).

If the TCAP handshake is to be used, then at least one of MEAS-2a and MEAS-2b of clause D.1 shall also be applied.

The following grouping method may be used for an operator to gradually introduce the TCAP handshake for mo-Forward-SM messages. Define an 'operator group-1' as a trusted operator group and 'operator group-2' as an un-trusted operator group. Agree that group-1 uses the TCAP handshake, while group-2 does not use the TCAP handshake. As specified by TS 29.002 [2] this requires that the MSC operators belonging to group-1 shall either use application context2 or 3 for mo-Forward-SM. The management of the two groups requires that the network of the SMS Interworking MSC shall implement a policy table of originating SCCP-addresses for which a TCAP handshake is required.

If the above described grouping method is used then the following measure shall be taken at the network of the SMS Interworking MSC in order to counteract the spoofing possibilities of a malicious mo-Forward-SM originator that tries to circumvent the policy table checks.

MEAS-3: The SMS Interworking MSC shall verify that the SCCP Calling Party address of a first message with a payload (i.e. not using the TCAP handshake) is not from an address that shall use the TCAP handshake.

The benefit gained for operators that belong to group-1 is that mo-Forward-SM spoofing for their subscribers, while roaming within group-1, becomes practically difficult if the policy table has been administrated accurately.

Annex E (informative): Change history

Change history									
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Cat**	**Subject/Comment**	**Old**	**New**	**WI**
06-2005	SA3-39		-	-	-	First version of TCAP user security based on TS33.200 V6.1.0	0.0.0	0.1.0	
09-2005	SA3-40		-	-	-	Documents S3-050551,561,562,563,564	0.1.0	0.2.0	
11-2005	SA3-41		-	-	-	Documents S3-050699,700,701	0.2.0	1.0.0	
02-2006	SA3-42		-	-	-	Documents S3-050052,53,54,55,56,57	1.0.0	2.0.0	
02-2006	Post SA3#42		-	-	-	Editorial corrections	2.0.0	2.0.1	
2006-03	SP-31	SP-060210	-	-	-	Approved at SA #31	2.0.1	7.0.0	
2006-06	SP-32	SP-060385	0001	-	F	Remove detailed SSN numbering	7.0.0	7.1.0	SEC7-NDS-TCAPsec
2006-06	SP-32	SP-060385	0002	-	F	Updating references to Stage 3 (removing Editor"s Note)	7.0.0	7.1.0	SEC7-NDS-TCAPsec
2006-06	SP-32	SP-060385	0003	-	F	Clarification of message routing between PLMNs	7.0.0	7.1.0	SEC7-NDS-TCAPsec
2006-09	SP-33	SP-060661	0004	1	B	Using TCAPsec within a hub-and-spoke architecture	7.1.0	7.2.0	SEC7-NDS-TCAPsec
2008-12	--	--	--	--	--	Upgrade to Release 8	7.2.0	8.0.0	--
2009-12	--	--	--	--	--	Upgrade to Release 9	8.0.0	9.0.0	--
2011-03	-	--	--	--	--	Upgrade to Release 10	9.0.0	10.0.0	--

History

Document history		
V10.0.0	April 2011	Publication