3GPP TS 29.204 V16.0.0 (2020-07)

Technical Specification

3rd Generation Partnership Project;

Technical Specification Group Core Network and Terminals;

Signalling System No. 7 (SS7) security gateway;   
Architecture, functional description and protocol details

(Release 16)

 

The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP.   
The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented.   
This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification.  
Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices.

Keywords

UMTS, GSM, SS7, Security

***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

***Copyright Notification***

No part may be reproduced except as authorized by written permission.  
The copyright and the foregoing restriction extend to reproduction in all media.

© 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).

All rights reserved.

UMTS™ is a Trade Mark of ETSI registered for the benefit of its members

3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  
LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners

GSM® and the GSM logo are registered and owned by the GSM Association

Contents

Foreword [4](#__RefHeading___Toc517479369)

Introduction [4](#__RefHeading___Toc517479370)

1 Scope [5](#__RefHeading___Toc517479371)

2 References [5](#__RefHeading___Toc517479372)

3 Definitions and abbreviations [5](#__RefHeading___Toc517479373)

3.1 Definitions [5](#__RefHeading___Toc517479374)

3.2 Abbreviations [6](#__RefHeading___Toc517479375)

4 Network architecture [6](#__RefHeading___Toc517479376)

4.1 Scenarios [6](#__RefHeading___Toc517479377)

4.1.1 Outbound traffic (not yet protected) from own to foreign NE [7](#__RefHeading___Toc517479378)

4.1.2 Inbound traffic from foreign to own NE [7](#__RefHeading___Toc517479379)

4.1.3 Inbound transit traffic [8](#__RefHeading___Toc517479380)

4.1.4 Outbound transit traffic (not relayed) [9](#__RefHeading___Toc517479381)

4.1.5 Outbound traffic from own to own NE [9](#__RefHeading___Toc517479382)

4.1.6 Inbound traffic from own to own NE [10](#__RefHeading___Toc517479383)

4.1.7 Outbound traffic from foreign to own NE [11](#__RefHeading___Toc517479384)

4.1.8 Inbound traffic from own to foreign NE [11](#__RefHeading___Toc517479385)

4.1.9 Outbound traffic (already protected) from own to foreign NE [12](#__RefHeading___Toc517479386)

4.1.10 Outbound transit traffic (relayed by SRF) [13](#__RefHeading___Toc517479387)

5 Detailed Behaviour of the SS7 Security Gateway [13](#__RefHeading___Toc517479388)

5.1 TCAP user traffic [13](#__RefHeading___Toc517479389)

5.1.1 General [13](#__RefHeading___Toc517479390)

5.1.2 Interactions with Mobile Number Portability [28](#__RefHeading___Toc517479391)

5.1.3 Interactions with SCCP segmentation [28](#__RefHeading___Toc517479392)

5.1.4 Protocol details [29](#__RefHeading___Toc517479393)

5.1.4.1 Transformation of unprotected message to protected message [29](#__RefHeading___Toc517479394)

5.1.4.2 Transformation of protected message to unprotected message [33](#__RefHeading___Toc517479395)

5.1.4.3 Handling of received XUDTS messages and UDTS messages [36](#__RefHeading___Toc517479396)

Annex A (informative): Change history [39](#__RefHeading___Toc517479397)

# 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 inter-network SS7 signalling protocols. The protection is done by security gateways which are located at the network border. As a consequence intra network SS7 signalling is not protected and network elements other than Security Gateways are not impacted.

# 1 Scope

The present document provides functional description of the SS7 Security Gateway. The document covers also network architecture, routeing considerations, and protocol details.

# 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 TS 29.002: "Mobile Application Part (MAP) specification".

[2] 3GPP TS 29.078: "Customized Applications for Mobile network Enhanced Logic (CAMEL) Phase 4; CAMEL Application Part (CAP) specification".

[3] ETSI ETS 300 358: "ISDN Completion of Calls to Busy Subscriber (CCBS) supplementary service; Functional capabilities and information flows".

[4] 3GPP TS 23.066: "Support of GSM Mobile Number Portability (MNP) stage 2".

[5] ITU-T Recommendation Q.773: "Specifications of Signalling System No.7; Transaction capabilities formats and encoding".

[6] 3GPP TS 33.200: "3G Security; Network Domain Security (NDS); Mobile Application Part (MAP) application layer security".

[7] ITU-T Recommendation E.164: " The international public telecommunication numbering plan".

[8] 3GPP TS 33.204: "3G Security; Network Domain Security (NDS); Transaction Capabilities Application Part (TCAP) user security".

[9] ITU-T Recommendations Q.711 to Q.716 (07/96), White Book Signalling Connection Control Part (SCCP).

[10] 3GPP TS 21.905: "Vocabulary for 3GPP Specifications".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [10] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [10].

TCAP user: Application Part identified by one of the following SCCP Subsystem Numbers:  
 0000 0110 HLR (MAP)  
 0000 0111 VLR (MAP)  
 0000 1000 MSC (MAP)  
 0000 1001 EIR (MAP)  
 0000 1010 is allocated for evolution (possible Authentication Centre)  
 1001 0001 GMLC (MAP)  
 1001 0010 CAP  
 1001 0011 gsmSCF (MAP) or IM-SSF (MAP) or Presence Network Agent  
 1001 0101 SGSN (MAP)  
 1001 0110 GGSN (MAP)  
 0000 1011 SSAP

## 3.2 Abbreviations

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

CC Country Code

GSMA Global System for Mobile communications Association

IV Initialisation Vector

MAC Message Authentication Code

MNP Mobile Number Portability

MSISDN Mobile Station International ISDN Number

NDC National Destination Code

NE Network Entit

PLMN Public Land Mobile Network y

RN Routeing Number

SAD Security Association Database

SEG Security Gateway

SPD Security Policy Database

SPI Security Parameter Index

SRF Signalling Relay Functio

TCAP Transcaction Capabilities Application Part

UDT SCCP Unitdata message

XUDT SCCP Extended Unitdata message n

# 4 Network architecture

In a PLMN that employs SS7 Security Gateways all TCAP user signalling messages entering or leaving the PLMN have to transit an SS7 Security Gateway which belongs to the PLMN and which performs the protection of leaving (i.e. outbound) messages and the protection checking and de-protection or blocking of entering (i.e. inbound) messages.

One or several SS7 Security Gateways may be employed within a PLMN.

An SS7 Security Gateway may be co-located with any TCAP user NE or it may stand alone. However, for the purpose of this document and without imposing any restrictions, it is assumed that the SS7 Security Gateways is a stand alone entity.

It is further assumed that the SS7 Security Gateways are located at the boarder of the PLMN i.e. inbound messages transit an SS7 Security Gateway before they reach any other node within the PLMN, and outbound messages transit an SS7 Security Gateway immediately before reaching a node outside the PLMN.

SS7 routeing is not impacted by the SS7 Security Gateway Architecture. As a consequence SS7 Security Gateways are stateless at TCAP level: No TCAP dialogue states are maintained in the SS7 Security Gateway since the outbound dialogue request message may transit a different SS7 Security Gateway than the corresponding inbound dialogue response message; similarly the inbound dialogue request message may transit a different SS7 Security Gateway than the corresponding outbound dialogue response message.

## 4.1 Scenarios

SS7 Security Gateways perform protection, de-protection, blocking and unmodified passing of TCAP user messages depending on the scenario as described below:

Note that scenarios 4.1.5, 4.1.6, 4.1.7, 4.1.8, and 4.1.9 are not applicable if all PLMN's TCAP user NEs are interconnected by PLMN internal signalling links and routing tables are set up not to allow these scenarios.

### 4.1.1 Outbound traffic (not yet protected) from own to foreign NE

This scenario is shown in figure 4.1.1. The message is originated at a NE inside the PLMN. It may transit several transit nodes inside the PLMN before it reaches the SS7 Security Gateway. This SS7 Security Gateway protects the message according to the relevant Security Policy with the relevant Security Association. The message may then transit several nodes outside the PLMN (including an SS7 Security Gateway) before it reaches its destination.



Figure 4.1.1: Outbound traffic (not yet protected) from own to foreign NE

### 4.1.2 Inbound traffic from foreign to own NE

This scenario is shown in figure 4.1.2. The message is originated at a NE outside the PLMN. It may transit several transit nodes (including an SS7 Security Gateway) outside the PLMN before it reaches the PLMN's SS7 Security Gateway. This SS7 Security Gateway checks whether the message is correctly protected according to the relevant security association. If it is not, the message is blocked (discarded), otherwise it is de-protected. To determine the relevant security association the fact that the message may have been relayed by an MNP-SRF in a transit network (see Clause 4.1.10 and 5.1.2) needs to be taken into account. After successful de-protection the message may then transit several nodes inside the PLMN before it reaches the TCAP user NE.



Figure 4.1.2: Inbound traffic from foreign to own NE

### 4.1.3 Inbound transit traffic

This scenario is shown in figure 4.1.3. The message is originated at a NE outside the transit PLMN. It may transit several transit nodes outside the transit PLMN before it reaches the SS7 Security Gateway in inbound direction. This SS7 Security Gateway passes the message unmodified. The message may then transit several transit nodes inside the transit PLMN, another SS7 Security Gateway of the transit PLMN in outbound direction (see Clause 4.1.4), and several transit nodes outside the transit and destination PLMN (potentially including an SS7 Security Gateway) before it reaches the destination PLMN.

Note: A PLMN operator may decide not to act as transit network for specific or all combinations of origin and destination. In this case the SS7 Security Gateway may block the inbound message.



Figure 4.1.3: Inbound transit traffic

### 4.1.4 Outbound transit traffic (not relayed)

This scenario is shown in figure 4.1.4. The message is originated at a NE outside the transit PLMN. It may transit several transit nodes outside the transit PLMN (including an SS7 Security Gateway), an SS7 Security Gateway of the transit PLMN in inbound direction (see Clause 4.1.3), and several transit nodes inside the transit PLMN before it reaches the SS7 Security Gateway in outbound direction. This SS7 Security Gateway passes the message unmodified. The message may then transit several transit nodes outside the transit and destination PLMN (potentially including an SS7 Security Gateway) before it reaches the destination PLMN.



Figure 4.1.4: Outbound transit traffic (not relayed)

### 4.1.5 Outbound traffic from own to own NE

This scenario is shown in figure 4.1.5. The message is originated at a NE inside the PLMN. It may transit several transit nodes inside the PLMN before it reaches the SS7 Security Gateway in outbound direction. This SS7 Security Gateway protects the message according to the relevant Security Association. The message may then transit several transit nodes outside the PLMN, another SS7 Security Gateway of the PLMN in inbound direction (see Clause 4.1.6) and several transit nodes within the PLMN before it reaches the destination NE inside the PLMN.



Figure 4.1.5: Outbound traffic from own to own NE

### 4.1.6 Inbound traffic from own to own NE

This scenario is shown in figure 4.1.6. The message is originated at a NE inside the PLMN. It may transit several transit nodes inside the PLMN, an SS7 Security Gateway of the PLMN in outbound direction (see Clause 4.1.5), and several transit nodes outside the PLMN before it reaches the SS7 Security Gateway in inbound direction. This SS7 Security Gateway checks whether the message is correctly protected according to the relevant Security Association. If it is not, the message is blocked (discarded), otherwise it is de-protected. The message may then transit several transit nodes inside the PLMN before it reaches the destination NE inside the PLMN.



Figure 4.1.6: Inbound traffic from own to own NE

### 4.1.7 Outbound traffic from foreign to own NE

This scenario is shown in figure 4.1.7. The message is originated at a NE outside the PLMN. It may transit several transit nodes outside the PLMN, an SS7 Security Gateway of the PLMN in inbound direction (see Clause 4.1.2), and several transit nodes inside the PLMN before it reaches the SS7 Security Gateway in outbound direction. This SS7 Security Gateway protects the message according to the reverse relevant Security Association. The message may then transit several transit nodes outside the PLMN, another SS7 Security Gateway of the PLMN in inbound direction (see Clause 4.1.2) and several transit nodes within the PLMN before it reaches the destination NE inside the PLMN.



Figure 4.1.7: Outbound traffic from foreign to own NE

### 4.1.8 Inbound traffic from own to foreign NE

This scenario is shown in figure 4.1.8. The message is originated at a NE inside the PLMN. It may transit several transit nodes inside the PLMN, an SS7 Security Gateway of the PLMN in outbound direction (see Clause 4.1.1), and several transit nodes outside the PLMN before it reaches the SS7 Security Gateway in inbound direction. This SS7 Security Gateway checks whether the message is correctly protected according to the relevant security association. If it is not, the message is blocked (discarded); otherwise it is passed unmodified. The message may then transit several transit nodes inside the PLMN, another SS7 Security Gateway of the PLMN in outbound direction (see Clause 4.1.9) and several transit nodes outside the PLMN (including an SS7 Security Gateway) before it reaches the destination NE outside the PLMN.



Figure 4.1.8: Inbound traffic from own to foreign NE

### 4.1.9 Outbound traffic (already protected) from own to foreign NE

This scenario is shown in figure 4.1.9. The message is originated at a NE inside the PLMN. It may transit several transit nodes inside the PLMN, an SS7 Security Gateway of the PLMN in outbound direction (see Clause 4.1.1), several transit nodes outside the PLMN, an SS7 Security Gateway of the PLMN in inbound direction (see Clause 4.1.8), and several transit nodes inside the PLMN before it reaches the SS7 Security Gateway. This SS7 Security Gateway passes the message unmodified. The message may then transit several transit nodes outside the PLMN (including an SS7 Security Gateway) before it reaches the destination NE outside the PLMN.



Figure 4.1.9: Outbound traffic (already protected) from own to foreign NE

### 4.1.10 Outbound transit traffic (relayed by SRF)

This scenario is shown in figure 4.1.10. The message (originally destined for the PLMN) is originated at a NE outside the transit PLMN. It may transit several transit nodes outside the transit PLMN (including an SS7 Security Gateway), an SS7 Security Gateway of the transit PLMN in inbound direction (see Clause 4.1.2), several transit nodes inside the transit PLMN, and an MNP-SRF which replaces the SCCP called party address of the message before it reaches the SS7 Security Gateway in outbound direction. This SS7 Security Gateway recognizes that the message was relayed by an SRF by analyzing the SCCP called party address and protects the message with the relevant Security Association. The message may then transit several transit nodes outside the transit and destination PLMN (potentially including an SS7 Security Gateway) before it reaches the destination PLMN.



Figure 4.1.10: Outbound transit traffic (relayed by SRF)

# 5 Detailed Behaviour of the SS7 Security Gateway

## 5.1 TCAP user traffic

### 5.1.1 General

With regard to TCAP user traffic the SS7 Security Gateway performs message protection, protection checking and de-protection, transparent passing, and blocking of messages depending on the message's origin (SCCP calling party address), the message's destination (SCCP called party address), and the message's direction (inbound or outbound) as shown in figure 5.1.1.



Figure 5.1.1 Process SS7 Security Gateway (sheet 1 of 2)



Figure 5.1.1 Process SS7 Security Gateway (sheet 2 of 2)



Figure 5.1.2 Macro Check\_Direction (sheet 1 of 1)



Figure 5.1.3 Macro Inbound\_own\_to\_own (sheet 1 of 1)

The decision box "message contains protectable parameter" takes the "yes"-exit if   
user-information is present in the Dialogue Portion, or  
a parameter is present in an Invoke or ReturnError Component, or  
a result is present in a ReturnResult Component.

The decision box "message is not protected" takes the "no"-exit if  
user-information within the Dialogue Portion is identified by the object identifier ss7-ProtectedDialogueAS or  
operationCode within an Invoke or ReturnResult Component takes the global value ss7-ProtectedDialogueAS or  
errorCode within an ReturnError Component takes the global value ss7-ProtectedDialogueAS.

The decision box "message should be protected according to SPD" takes the "yes"-exit if the message's SCCP calling party address identifies a PLMN for which an SPD entry for incoming messages exists.

The decision box "fall back allowed according to SPD" takes the "yes"-exit if the SPD entry for incoming messages is marked "fall back allowed".

The decision box "calling party address consistent with SPI" takes the "yes"-exit if the SPI within the message's Security Header points to an SA that was negotiated with the PLMN derived from the message's SCCP calling party address.

The decision box "protection mode acceptable according to SPD" takes the "yes"-exit if the protection mode within the message's Security Header is found in the SPD-entry for incoming messages.



Figure 5.1.4 Macro Inbound\_own\_to\_foreign (sheet 1 of 1)

The decision box "message contains protectable parameter" takes the "yes"-exit if   
user-information is present in the Dialogue Portion, or  
a parameter is present in an Invoke or ReturnError Component, or  
a result is present in a ReturnResult Component.

The decision box "message is not protected" takes the "no"-exit if  
user-information within the Dialogue Portion is identified by the object identifier ss7-ProtectedDialogueAS or  
operationCode within an Invoke or ReturnResult Component takes the global value ss7-ProtectedDialogueAS or  
errorCode within an ReturnError Component takes the global value ss7-ProtectedDialogueAS.

The decision box "message should be protected according to SPD" takes the "yes"-exit if the message's SCCP called party address identifies a PLMN for which an SPD entry for outgoing messages exists.

The decision box "fall back allowed according to SPD" takes the "yes"-exit if the SPD entry for outgoing messages is marked "fall back allowed".

The decision box "called party address consistent with SPI" takes the "yes"-exit if the SPI within the message's Security Header points to an SA that was negotiated with the PLMN derived from the message's SCCP called party address.

The decision box "protection mode correct" takes the "yes"-exit if the presence/absence of octets 10 and 11 within the message's Security Header is consistent with the protection mode in the SPD-entry for outgoing messages. Note that octets 10 and 11 of the Security Header are only used to construct the IV which is not needed (and shall therefore be absent) if the protection mode is "authenticity and integrity".



Figure 5.1.5 Macro Inbound\_foreign\_to\_own (sheet 1 of 2)



Figure 5.1.5 Macro Inbound\_foreign\_to\_own (sheet 2 of 2)

The decision box "message contains protectable parameter" takes the "yes"-exit if   
user-information is present in the Dialogue Portion, or  
a parameter is present in an Invoke or ReturnError Component, or  
a result is present in a ReturnResult Component.

The decision box "message is not protected" takes the "no"-exit if  
user-information within the Dialogue Portion is identified by the object identifier ss7-ProtectedDialogueAS or  
operationCode within an Invoke or ReturnResult Component takes the global value ss7-ProtectedDialogueAS or  
errorCode within an ReturnError Component takes the global value ss7-ProtectedDialogueAS.

The decision box "relayed by SRF" takes the "yes"-exit if the SCCP called party address consists of a Routing Number (RN) pointing to the own network and an MSISDN pointing to a relay network within the portability cluster.

The decision box "message should be protected according to SPD (relay network)" takes the "yes"-exit if an SPD entry for incoming messages exists for the relay network.

The decision box "Fall Back allowed according to SPD (relay network)" takes the "yes"-exit if the SPD entry for incoming messages (from the relay network) is marked "fall back allowed".

The decision box "message should be protected according to SPD (orig. network)" takes the "yes"-exit if the message's SCCP calling party address identifies a PLMN for which an SPD entry for incoming messages exists.

The decision box "Fall Back allowed according to SPD (relay network)" takes the "yes"-exit if the SPD entry for incoming messages (from the network identified by the SCCP calling party address) is marked "fall back allowed".

The decision box "calling party address consistent with SPI" takes the "yes"-exit if the SPI within the message's Security Header points to an SA that was negotiated with the PLMN derived from the message's SCCP calling party address.

The decision box "protection mode acceptable according to SPD (relay network)" takes the "yes"-exit if the presence/absence of octets 10 and 11 within the message's Security Header is consistent with a protection mode found in the SPD-entry (for incoming messages from the network identified by the SPI). Note that octets 10 and 11 of the Security Header are only used to construct the IV which is not needed (and shall therefore be absent) if the protection mode is "authenticity and integrity".

The decision box "protection mode acceptable according to SPD (orig. network)" takes the "yes"-exit if the presence/absence of octets 10 and 11 within the message's Security Header is consistent with a protection mode found in the SPD-entry (for incoming messages from the network identified by the SCCP calling party address). Note that octets 10 and 11 of the Security Header are only used to construct the IV which is not needed (and shall therefore be absent) if the protection mode is "authenticity and integrity".



Figure 5.1.6 Macro Outbound\_own\_to\_own (sheet 1 of 1)

The decision box "message contains protectable parameter" takes the "yes"-exit if   
user-information is present in the Dialogue Portion, or  
a parameter is present in an Invoke or ReturnError Component, or  
a result is present in a ReturnResult Component.

The decision box "message needs to be protected according to SPD" takes the "yes"-exit if an SPD entry for outgoing messages exists (for messages sent to the own network).



Figure 5.1.7 Macro Outbound\_own\_to\_foreign (sheet 1 of 1)

The decision box "message contains protectable parameter" takes the "yes"-exit if   
user-information is present in the Dialogue Portion, or  
a parameter is present in an Invoke or ReturnError Component, or  
a result is present in a ReturnResult Component.

The decision box "message is protected" takes the "yes"-exit if  
user-information within the Dialogue Portion is identified by the object identifier ss7-ProtectedDialogueAS or  
operationCode within an Invoke or ReturnResult Component takes the global value ss7-ProtectedDialogueAS or  
errorCode within an ReturnError Component takes the global value ss7-ProtectedDialogueAS.

The decision box "message needs to be protected according to SPD" takes the "yes"-exit if an SPD entry for outgoing messages exists (for messages sent to the network identified by the SCCP called party address).



Figure 5.1.8 Macro Outbound\_foreign \_to\_own (sheet 1 of 1)

The decision box "message contains protectable parameter" takes the "yes"-exit if   
user-information is present in the Dialogue Portion, or  
a parameter is present in an Invoke or ReturnError Component, or  
a result is present in a ReturnResult Component.

The decision box "message needs to be protected according to SPD" takes the "yes"-exit if an SPD entry for incoming messages exists (for messages received from the network identified by the SCCP calling party address). If more than one acceptable protection modes are present, one may be chosen.

The task box "protect message with reverse SA" performs protection of the message with the SA that is to be used for de-protection when receiving messages from the network in question.



Figure 5.1.9 Macro Outbound\_foreign \_to\_foreign (sheet 1 of 1)

The decision box "message contains protectable parameter" takes the "yes"-exit if   
user-information is present in the Dialogue Portion, or  
a parameter is present in an Invoke or ReturnError Component, or  
a result is present in a ReturnResult Component.

The decision box "message is protected" takes the "yes"-exit if  
user-information within the Dialogue Portion is identified by the object identifier ss7-ProtectedDialogueAS or  
operationCode within an Invoke or ReturnResult Component takes the global value ss7-ProtectedDialogueAS or  
errorCode within an ReturnError Component takes the global value ss7-ProtectedDialogueAS.

The decision box "relayed by SRF" takes the "yes"-exit if the SCCP called party address consists of a Routing Number (RN) pointing to the own network and an MSISDN pointing to a relay network within the portability cluster.

The decision box "message needs to be protected according to SPD takes the "yes"-exit if an SPD entry for outgoing messages exists (for messages sent to the network identified by the SCCP called party address).

### 5.1.2 Interactions with Mobile Number Portability

In Mobile Number Portability scenarios (see 3GPP TS 23.066 [4]) a Signalling Relay Function (SRF) may relay SCCP traffic by modifying the SCCP called party address as shown in figure 4.1.10.

A relayed message's SCCP called party address consists of a Routing Number (RN) and an MSISDN (see 3GPP TS 23.066 [4]).

An SS7 Security Gateway needs to recognize (by analyzing the SCCP called party address) whether or not a message was relayed in order to

a) distinguish outbound transit traffic relayed by an SRF in the own network (which needs to be protected) from other outbound transit traffic (which needs to be passed transparently), and to

b) distinguish inbound terminating traffic relayed by an SRF within the portability cluster (where the check needs to be based on the policy identified by the MSISDN within the SCCP called party address) from other inbound terminating traffic (where the check needs to be based on the policy identified by the SCCP calling party address).

NOTE : In MNP-SRF scenarios, when the relaying PLMN does not make use of TCAP-User Security, messages sent from a source PLMN to a destination PLMN via the relaying PLMN are unprotected although protection may be desired for messages sent from the source PLMN to the destination PLMN. Network operators may therefore want to negotiate use of TCAP-User Security with all PLMNs of a portability cluster.

### 5.1.3 Interactions with SCCP segmentation

When the incoming SCCP message makes use of SCCP segmenting (i.e. several XUDT messages are received rather than one UDT or a single XUDT message) the SS7 Security Gateway has to perform reassembling before processing the message, and it may have to perform segmenting before sending the processed message.

It may happen that the received SCCP message (containing an unprotected TCAP user payload) is not segmented (UDT or single XUDT), but after security processing the message's length is increased, so that the processed message needs to be segmented before it is sent. This situation may be undesired (since transfer of XUDT messages is not guaranteed by all transit networks) but cannot be avoided by the SS7 Security Gateway (see note).

Note: The support of message segmentation at the SCCP layer in all transit networks could be enforced by mandating the usage of the White Book SCCP [9]. GSMA would work with International Carriers to ensure that fully operationally-verified support of XUDT is available before TCAPsec gateways are deployed.

It may also happen that the received (protected) message is segmented (several XUDTs), but after security processing the message's length is decreased, so that the processed message does not need to be segmented before it is sent. In this case the de-protecting SS7 Security Gateway needs to know some SCCP-details of the original unprotected message as sent from the originating NE to the protecting SS7 Security Gateway. These original SCCP information needs to be transported within the TCAP-user parameter of the protected message. Depending on this information the de-protecting SS7-Security Gateway can decide whether to send a UDT or a single XUDT message towards the destination. .

In cases where the received unprotected message is not segmented but the (to be) sent protected message needs to be segmented, the SS7 Security Gateway has to replace the message's SCCP calling party address with its own address. This is to guarantee uniqueness of the combination of the SCCP calling party address and the Segmentation local reference in the (to be) sent message. The original SCCP calling party address needs to be transported within the TCAP-user parameter of the (first segment of the) protected message.

If the received protected message contains an original SCCP calling party address within the TCAP-user parameter, the de-protecting SS7 Security Gateway has to replace the SCCP calling party address with the original SCCP calling party address before forwarding the de-protected message to the destination.

An SS7 Security Gateway that has sent a segmented, protected message with a replaced SCCP calling party address may receive an SCCP XUDTS message with its own address as called party address. In this case the SS7 Security Gateway shall retrieve the original SCCP calling party address, the original TCAP Message type and TCAP transaction id from the data parameter of the received XUDTS message and construct a UDTS message with unmodified Return cause, called party address replaced with the retrieved original calling party address, unmodified calling party address, and Data parameter containing the retrieved TCAP message type and TCAP transaction id, and forward it to the destination.

### 5.1.4 Protocol details

#### 5.1.4.1 Transformation of unprotected message to protected message

The unprotected TCAP-user message is either transported within an SCCP UDT message or it is transported within a single SCCP XUDT message or it is segmented over several SCCP XUDT messages. Other SCCP message types are not subject to protection.

The transformation process is done in 3 steps:

**Step 1: SCCP re-assembly of the unprotected message**

In a first step the unprotected message is transformed into an intermediate unprotected representation which is made up of the following parameters:

SCCP Message type  
SCCP Protocol class  
SCCP Hop counter (optional)  
SCCP Called party address  
SCCP Calling party address  
SCCP Segmentation local reference (optional)  
SCCP Importance (optional)  
SCCP Data (made up of the following parameters: TCAP Message type  
 TCAP orig. Transaction Id (optional)  
 TCAP dest. Transaction Id (optional)  
 TCAP Dialogue Portion (optional)  
 TCAP Component Portion (optional))

If the unprotected message was transported within an SCCP UDT message, the intermediate unprotected representation of the message takes the following values:

SCCP Message type UDT  
SCCP Protocol class same as in the received UDT message  
SCCP Hop counter absent  
SCCP Called party address same as in the received UDT message  
SCCP Calling party address same as in the received UDT message  
SCCP Segmentation local reference absent  
SCCP Importance absent  
SCCP Data same as in the received UDT message

If the unprotected message was transported within a single SCCP XUDT message, the intermediate unprotected representation of the message takes the following values:

SCCP Message type XUDT  
SCCP Protocol class same as in the received XUDT message  
SCCP Hop counter same as in the received XUDT message   
SCCP Called party address same as in the received XUDT message  
SCCP Calling party address same as in the received XUDT message  
SCCP Segmentation local reference absent  
SCCP Importance same as in the received XUDT message  
SCCP Data same as in the received XUDT message

If the unprotected message was segmented over several SCCP XUDT messages, the intermediate unprotected representation of the message takes the following values:

SCCP Message type XUDT  
SCCP Protocol class same as in the first received XUDT message  
SCCP Hop counter same as in the first received XUDT message   
SCCP Called party address same as in the first received XUDT message  
SCCP Calling party address same as in the first received XUDT message  
SCCP Segmentation local reference same as in the first received XUDT message  
SCCP Importance same as in the first received XUDT message  
SCCP Data concatenation of the received segments (for details of the re-  
 assembly procedure see ITU-T Q.714 [9])

**Step 2: Protection**

In a second step the intermediate unprotected representation is transformed into an intermediate protected representation which is made up of the following parameters:

SCCP Hop counter (optional)  
SCCP Called party address  
SCCP Calling party address  
SCCP Segmentation local reference (optional)  
SCCP Importance (optional)  
Original SCCP info (made up of the following parameters: Original SCCP Calling party address (optional)  
 Original SCCP Message type  
 Original SCCP Protocol class)  
Original TCAP info (made up of the following parameters: Original TCAP Message type  
 otid (optional)  
 dtid (optional))  
TCAPsec Security header  
TCAPsec Cipher- or Cleartext  
TCAPsecMAC

The intermediate unprotected representation of the message takes the following values:

SCCP Hop counter same as SCCP Hop counter in the intermediate   
 unprotected representation  
SCCP Called party address same as in the intermediate unprotected representation  
SCCP Calling party address same as in the intermediate unprotected representation  
SCCP Segmentation local reference same as in the intermediate unprotected representation  
SCCP Importance same as SCCP Importance in the intermediate  
 unprotected representation  
Original SCCP info made up of the following parameters:  
 Original SCCP Message type same as SCCP Message type in the intermediate   
 unprotected representation  
 Original SCCP Protocol class same as SCCP Protocol class in the intermediate   
 unprotected representation  
Original TCAP info made up of the following parameters:  
 Original TCAP Message type same as TCAP Message type in the intermediate   
 unprotected representation  
 TCAP otid same as TCAP orig. Transaction Id in the intermediate   
 unprotected representation  
 TCAP dtid same as TCAP dest. Transaction Id in the intermediate   
 unprotected representation  
TCAPsec Security header See 3GPP TS 33.204 [8]  
TCAPsec Cipher- or Cleartext result of applying the encryption function to the   
 concatenation of Dialogue Portion and Component   
 Portion of the intermediate unprotected representation  
 (ciphertext), or concatenation of Dialogue Portion and   
 Component Portion of the intermediate unprotected   
 representation(cleartext)  
TCAPsec MAC result of applying the integrity function to the   
 concatenation of Security header and Cipher- or   
 Cleartext of the intermediate protected representation.

**Step 3: SCCP segmentation of the protected message**

In a third step the intermediate protected representation is transformed into a single SCCP UDT message, a single SCCP XUDT message, or several SCCP XUDT messages depending on the Original SCCP Message type of the intermediate protected representation and the need for segmentation as follows:

If the Original SCCP Message type in the intermediate protected representation takes the value "UDT" and the message need not be segmented, it is transformed into a single SCCP UDT message with following parameter values:

Message Type UDT  
Protocol class same as Original SCCP Protocol class in the intermediate protected representation  
Called party address same as SCCP Called party address in the intermediate protected representation  
Calling party address same as SCCP Calling party address in the intermediate protected representation  
Data (see below)

If the Original SCCP Message type in the intermediate protected representation takes the value "XUDT" and the message need not be segmented, it is transformed into a single SCCP XUDT message with following parameter values:

Message Type XUDT  
Protocol class same as Original SCCP Protocol class in the intermediate protected representation  
Hop counter same as Original SCCP Hop counter in the intermediate protected representation  
Called party address same as SCCP Called party address in the intermediate protected representation  
Calling party address same as SCCP Calling party address in the intermediate protected representation  
Data (see below)  
Segmentation absent  
Importance same as Original SCCP Importance in the intermediate protected representation

If the Original SCCP Message type in the intermediate protected representation takes the value "UDT" and the message needs to be segmented, it is transformed into several SCCP XUDT message with following parameter values:

Message Type XUDT  
Protocol class first segment: class 1 (in sequence delivery), return option: same as in Original SCCP Protocol class in the intermediate protected representation  
 subsequent segment: class 1 (in sequence delivery), return option: no special options  
Hop counter absent  
Called party address same as SCCP Called party address in the intermediate protected representation  
Calling party address the SS7 Security Gateway's own address  
Data (segment of see below)  
Segmentation see [9]  
Importance absent

If the Original SCCP Message type in the intermediate protected representation takes the value "XUDT" and the message needs to be segmented, it is transformed into several SCCP XUDT message with following parameter values:

Message Type XUDT  
Protocol class first segment: class 1 (in sequence delivery), return option: same as in Original SCCP Protocol class in the intermediate protected representation  
 subsequent segment: class 1 (in sequence delivery), return option: no special options  
Hop counter same as Original SCCP Hop counter in the intermediate protected representation  
Called party address same as SCCP Called party address in the intermediate protected representation  
Calling party address if SCCP Segmentation Local reference is present in the intermediate protected representation: same as SCCP Calling party address in the intermediate protected representation;  
 otherwise: the SS7 Security Gateway's own address  
Data (segment of see below)  
Segmentation see [9]; if SCCP Segmentation Local reference is present in the intermediate protected representation, the same value shall be used.  
Importance same as Original SCCP Importance in the intermediate protected representation.

The SCCP Data parameter (re-assembled) shall take the following value:

TCAP Message type unidirectional  
 TCAP DialoguePortion absent  
 TCAP ComponentPortion one invoke component with:  
 invokeId (any legal value)  
 linkedId absent  
 operationCode local value 90 (secureTransport)  
 parameter ANY DEFINED BY operationCode

**.$SS7-Secure-Transport-Operation-and-DataTypes** {

itu-t identified-organization (4) etsi (0) mobileDomain (0)

gsm-Network (1) modules (3) ss7-Secure-Transport-Operation-and-DataTypes (27) version1 (1)}

DEFINITIONS

IMPLICIT TAGS

::=

BEGIN

EXPORTS

secureTransport

;

IMPORTS

OPERATION

FROM Remote-Operations-Information-Objects {

joint-iso-itu-t remote-operations(4)

informationObjects(5) version1(0)}

;

secureTransport OPERATION ::= {

ARGUMENT

SecureTransportArg

CODE local:90 }

SecureTransportArg ::= SEQUENCE {

originalSCCP-Info [0] OriginalSCCP-Info OPTIONAL,

originalTCAP-Info [1] OriginalTCAP-Info,

protectedPayload [2] ProtectedPayload

}

OriginalSCCP-Info ::= SEQUENCE {

originalSCCP-MessageType [0] OriginalSCCP-MessageType OPTIONAL,

-- original SCCP-MessageType shall be present if it is different from the actual

-- SCCP-Message type; otherwise it may be absent

originalSCCP-ProtocolClass [1] OriginalSCCP-ProtocolClass OPTIONAL

-- originalSCCP-ProtocolClass shall be present if it is different from the actual

-- SCCP-Protocol class (first segment); otherwise it may be absent.

originalSCCP-CallingPartyAddress [2] OriginalSCCP-CallingPartyAddress OPTIONAL,

-- originalSCCP-CallingPartyAddress shall be present if and only if the actual

-- SCCP Calling party address is the SS7 Security Gateway's own address

}

OriginalSCCP-MessageType ::= ENUMERATED {

udt (9),

xudt (17) }

-- this parameter shall take the value of the Original SCCP Message type from the

-- intermediate protected representation

OriginalSCCP-ProtocolClass ::= OCTET STRING(SIZE(1))

-- coded according to ITU-T Q.713

OriginalSCCP-CallingPartyAddress ::= OCTET STRING(SIZE(3..18))

-- coded according to ITU-T Q.713

-- Octet 1: Address indicator

-- Octets 2 - n: Address

OriginalTCAP-Info ::= SEQUENCE {

originalTCAP-MessageType OriginalTCAP-MessageType,

otid OTID OPTIONAL,

dtid DTID OPTIONAL

}

OriginalTCAP-MessageType ::= ENUMERATED {

unidirectional (97),

begin (98),

end (100),

continue (101),

abort (103)}

-- this parameter shall take the value of the Original TCAP Message type from the

-- intermediate protected representation

OTID ::= OCTET STRING(SIZE(1..4))

-- OTID shall take the value of the TCAP otid from the intermediate protected

-- representation

DTID ::= OCTET STRING(SIZE(1..4))

-- DTID shall take the value of the TCAP dtid from the intermediate protected

-- representation

ProtectedPayload ::= OCTET STRING(SIZE(13..3438))

-- The protected payload is the concatenation of

-- 9 or 11 octets SecurityHeader,

-- n octets ciphertext or cleartext, and

-- 4 octets MAC

-- The SecurityHeader is coded as follows (see 3GPP TS 33.204 [8]):

-- Octets 1-4: SPI

-- Octets 5-8: TVP. The TVP is a 32 bit time stamp. Its value is binary coded

-- and indicates the number of intervals of 100 milliseconds

-- elapsed since 1st January 2002, 0:00:00 UTC

-- Octet 9: Indicator Byte with bits 7-1 spare and bit 0 if set indicates presence of

-- Octets 10-11

-- Octet 10: SS7 SEG-Id

-- Octet 11: Prop

.#END

#### 5.1.4.2 Transformation of protected message to unprotected message

The protected TCAP-user message is either transported within an SCCP UDT message or it is transported within a single SCCP XUDT message or it is segmented over several SCCP XUDT messages. Other SCCP message types are not subject to protection.

The transformation process is done in 3 steps:

**Step 1: SCCP re-assembly of the protected message**

In a first step the protected message is transformed into the intermediate protected representation (see chapter 5.1.4.1):

If the protected message was transported within an SCCP UDT message, the intermediate protected representation of the message takes the following values:

SCCP Hop counter absent  
SCCP Called party address same as in the received UDT message  
SCCP Calling party address same as in the received UDT message  
SCCP Segmentation local reference absent  
SCCP Importance absent  
Original SCCP info  
 Original SCCP Calling party address absent  
 Original SCCP Message type UDT  
 Original SCCP Protocol class same as SCCP Protocol class in the received UDT message  
Original TCAP info   
 Original TCAP Message type same as Original TCAP Message type in the TCAP-invoke   
 component parameter of the received message  
 otid same as otid in the TCAP-invoke component parameter of the   
 received message  
 dtid same as dtid in the TCAP-invoke component parameter of the   
 received message  
TCAPsec Security header same as received in the TCAP-invoke component parameter of the  
 received message  
TCAPsec Cipher- or Cleartext same as received in the TCAP-invoke component parameter of the  
 received message  
TCAPsec MAC same as received in the TCAP-invoke component parameter of the  
 received message

If the protected message was transported within a single SCCP XUDT message, the intermediate protected representation of the message takes the following values:

SCCP Hop counter same as in the received XUDT message  
SCCP Called party address same as in the received XUDT message  
SCCP Calling party address same as in the received XUDT message  
SCCP Segmentation local reference absent  
SCCP Importance same as in the received XUDT message  
Original SCCP info  
 Original SCCP Calling party address absent  
 Original SCCP Message type same as OriginalSCCP-MessageType in the TCAP-invoke   
 component parameter of the received message  
 Original SCCP Protocol class same as OriginalSCCP-ProtocolClass in the TCAP-invoke   
 component parameter of the received message  
Original TCAP info   
 Original TCAP Message type same as Original TCAP Message type in the TCAP-invoke   
 component parameter of the received message  
 otid same as otid in the TCAP-invoke component parameter of the   
 received message  
 dtid same as dtid in the TCAP-invoke component parameter of the   
 received message  
TCAPsec Security header same as received in the TCAP-invoke component parameter of the  
 received message  
TCAPsec Cipher- or Cleartext same as received in the TCAP-invoke component parameter of the  
 received message  
TCAPsec MAC same as received in the TCAP-invoke component parameter of the  
 received message

If the protected message was transported within several SCCP XUDT message, the intermediate protected representation of the message takes the following values:

SCCP Hop counter same as in the first received XUDT message  
SCCP Called party address same as in the first received XUDT message  
SCCP Calling party address same as in the first received XUDT message  
SCCP Segmentation local reference same as in the first received XUDT message  
SCCP Importance same as in the first received XUDT message  
Original SCCP info  
 Original SCCP Calling party address same as OriginalSCCP-CallingPartyAddress in the TCAP-invoke   
 component parameter of the received reassembled message  
 Original SCCP Message type same as OriginalSCCP-MessageType in the TCAP-invoke   
 component parameter of the received reassembled message  
 Original SCCP Protocol class same as OriginalSCCP-ProtocolClass in the TCAP-invoke   
 component parameter of the received reassembled message  
Original TCAP info   
 Original TCAP Message type same as OriginalTCAP-MessageType in the TCAP-invoke   
 component parameter of the received reassembled message  
 otid same as otid in the TCAP-invoke component parameter of the   
 received reassembled message  
 dtid same as dtid in the TCAP-invoke component parameter of the   
 received reassembled message  
TCAPsec Security header same as received in the TCAP-invoke component parameter of the  
 received reassembled message  
TCAPsec Cipher- or Cleartext same as received in the TCAP-invoke component parameter of the  
 received reassembled message  
TCAPsec MAC same as received in the TCAP-invoke component parameter of the  
 received reassembled message

**Step 2: De-Protection**

In a second step the intermediate protected representation is transformed into an intermediate unprotected representation (see chapter 5.1.4.1):

The intermediate unprotected representation of the message takes the following values:

SCCP Message type same as OriginalSCCP-MessageType from the TCAP-invoke   
 component's parameter of the intermediate protected   
 representation  
SCCP Protocol class same as OriginalSCCP-ProtocolClass from the TCAP-invoke   
 component's parameter of the intermediate protected   
 representation  
SCCP Hop counter same as SCCP Hop counter in the intermediate protected   
 representation  
SCCP Called party address same as SCCP Called party address in the intermediate   
 protected representation  
SCCP Calling party address if OriginalSCCP-CallingPartyAddress is present in the   
 intermediate protected representation, its value is taken;   
 otherwise same as SCCP Calling party address of the   
 intermediate protected representation  
SCCP Segmentation local reference if SCCP Message type in the intermediate unprotected   
 representation is XUDT, then same as in the intermediate protected representation; otherwise absent.  
SCCP Importance same as in the intermediate unprotected representation  
SCCP Data :  
 TCAP Message type same as OriginalTCAP-MessageType in the intermediate   
 protected representation  
 TCAP orig. Transaction Id same as otid in the intermediate protected representation  
 TCAP dest. Transaction Id same as dtid in the intermediate protected representation  
 TCAP Dialogue Portion (optional) First part of the cleartext (as indicated by TAG and LENGTH   
 according to BER). If encryption was applied then ciphertext   
 needs to be converted first to cleartext  
 TCAP Component Portion (optional)) second part of the cleartext (as indicated by TAG and   
 LENGTH according to BER). If encryption was applied then   
 ciphertext needs to be converted first to cleartext

**Step 3: SCCP segmentation of the unprotected message**

In a third step the intermediate unprotected representation is transformed into a single SCCP UDT message, a single SCCP XUDT message, or several SCCP XUDT messages depending on the SCCP Message type of the intermediate unprotected representation and the need for segmentation as follows:

If the SCCP Message type in the intermediate unprotected representation is "UDT", it is transformed into a single SCCP UDT message with following parameter values:

Message Type UDT  
Protocol class same as SCCP Protocol class in the intermediate unprotected representation  
Called party address same as SCCP Called party address in the intermediate unprotected representation  
Calling party address same as SCCP Calling party address in the intermediate unprotected representation  
Data same as SCCP Data in the intermediate unprotected representation

If the SCCP Message type in the intermediate unprotected representation is "XUDT" and the message does not need to be segmented, it is transformed into a single SCCP XUDT message with following parameter values:

Message type XUDT  
Protocol class same as SCCP Protocol class in the intermediate unprotected representation  
Hop counter same as SCCP Hop counter in the intermediate unprotected representation  
Called party address same as SCCP Called party address in the intermediate unprotected representation  
Calling party address same as SCCP Calling party address in the intermediate unprotected representation  
Data same as SCCP Data in the intermediate unprotected representation  
Segmentation absent  
Importance same as SCCP Importance in the intermediate unprotected representation

If the SCCP Message type in the intermediate unprotected representation is "XUDT" and the message needs to be segmented, it is transformed into several SCCP XUDT message with following parameter values:

Message type (all segments) XUDT  
Protocol class (first segment) class 1 (in sequence delivery), return option: same as in SCCP Protocol   
 class of the intermediate unprotected representation  
 (subsequent segments) class 1 (in sequence delivery), return option: no special options  
Hop counter (all segments) same as SCCP Hop counter in the intermediate unprotected representation  
Called party address (all segments) same as SCCP Called party address in the intermediate unprotected   
 representation  
Calling party address (all segments) same as SCCP Calling party address in the intermediate unprotected   
 representation  
Data segment of SCCP Data from the intermediate unprotected representation  
 (see ITU-T Q.714 [9])  
Segmentation see [9]. Local reference shall be taken from the intermediate unprotected   
 representation   
Importance (all segments) same as SCCP Importance in the intermediate unprotected representation

#### 5.1.4.3 Handling of received XUDTS messages and UDTS messages

An SS7 Security Gateway shall not try to re-assemble XUDTS messages, since the SCCP option "return on error" is not set for subsequent XUDT segments. As a consequence the SS7 Security Gateway shall not try to protect or de-protect XUDTS messages (fragments) or UDTS messages. However, special handling of XUDTS messages and UDTS messages is required as follows:

**Outbound direction**

Instead of re-assembling and protecting the XUDTS messages or protecting UDTS messages, the SS7 Security Gateway shall remove the TCAP Dialogue Portion and the TCAP Component Portion from the SCCP Data parameter before sending the XUDTS message or UDTS message. This is in order not to pass the cleartext (or fragment of the cleartext) in outbound direction. SCCP message type and addresses shall not be changed.

An example is shown in figure 5.1.4.3-1: A transit node in PLMN 2 cannot deliver the UDT message and therefore returns an UDTS message. SS7 Security Gateway 2 in PLMN 2 removes the cleartext (TCAP dialogue portion and TCAP component portion) from the SCCP data parameter. SS7 Security Gateway 1 in PLMN 1 recognizes that the received UDTS message does not contain a TCAP unidirectional message with a secure transport invoke component and therefore it does not modify the SCCP message.



Figure 5.1.4.3-1: XUDTS messages and UDTS messages (Outbound direction)

**Inbound direction**

Instead of re-assembling and de-protecting the XUDTS messages or de-protecting UDTS messages, the SS7 Security Gateway shall analyze the SCCP Called party address. If it matches with the SS7 Security Gateway's own address, it shall recover the OriginalSCCP-CallingPartyAddress from the (fragment in the) data parameter and replace the SCCP Called party address with the recovered value. In any case the SS7 Security Gateway shall recover and analyze the TCAP Message type from the (fragment in the) data parameter. If the recovered value is "unidirectional" and a invoke component with operation code "secure transport" is included, the SS7 Security Gateway shall recover the originalTCAP-MessageType, otid, and dtid from the OriginalTCAP-Info, replace the TCAP Message type with the original TCAP-MessageType, insert otid and dtid and remove the remaining material from the SCCP data parameter. If the received message is an XUDTS message and the original SCCP Message type was UDT then the SS7 Security shall modify the SCCP Message type to UDTS.

An example is shown in figure 5.1.4.3-2: A transit node in a transit network cannot deliver the XUDT messages and therefore returns an XUDTS message (note that the second XUDT does not have the SCCP return option set). SS7 Security Gateway 1 in PLMN 1 recognizes that the received XUDTS message does contain a TCAP unidirectional message with a secure transport invoke component and therefore, since the original SCCP-MessageType is UDT, modifies the SCCP Message type from XUDTS to UDTS. Furthermore, the TCAP MessageType is modified from unidirectional to the original TCAP-MessageType, the Transaction Ids are inserted, and the remaining material (fragment of the ciphertext) is removed.  
In addition the SS7 Security Gateway 1 in PLMN 1 recognizes that the received XUDTS message does contain SS7 Security Gateway 1's own address as SCCP Called party address and therefore replaces it with the original SCCPCalling party address.



Figure 5.1.4.3-2: XUDTS messages and UDTS messages (inbound direction)

Annex A (informative):  
Change history

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Date** | **TSG #** | **TSG Doc.** | **CR** | **Rev** | **Subject/Comment** | **New** |
| 2006-06 | CT#32 | CP-060320 |  |  | Approved as version 7.0.0 | 7.0.0 |
| 2006-09 | CT#33 | CP-060413 | 0001 |  | Addition of abbreviations and correction of a note | 7.1.0 |
| 2008-12 | CT#42 |  |  |  | Upgraded unchanged from Rel-7 | 8.0.0 |
| 2009-12 | - | - | - | - | Update to Rel-9 version (MCC) | 9.0.0 |
| 2011-03 | - | - | - | - | Update to Rel-10 version (MCC) | 10.0.0 |
| 2012-09 | - | - | - | - | Update to Rel-11 version (MCC) | 11.0.0 |
| 2014-09 | - | - | - | - | Update to Rel-12 version (MCC) | 12.0.0 |
| 2015-12 | CT#70 | - | - | - | Update to Rel-13 version (MCC) | 13.0.0 |
| 2017-03 | CT#75 | - | - | - | Update to Rel-14 version (MCC) | 14.0.0 |
| 2018-06 | CT#80 | - | - | - | Update to Rel-15 version (MCC) | 15.0.0 |
| 2020-07 | CT#88e | - | - | - | Update to Rel-16 version (MCC) | 16.0.0 |