EUROPEAN TELECOMMUNICATION STANDARD

FINAL DRAFT
pr **ETS 300 394-5-2**
April 1999

Source: TETRA

Reference: DE/TETRA-06009-5-2

ICS: 33.020

Key words: TETRA, security, voice, data, V+D, testing, protocol

Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 2: Protocol testing specification for TETRA security

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
Internet: secretariat@etsi.fr - http://www.etsi.org

Tel.: +33 4 92 94 42 00 - Fax: +33 4 93 65 47 16

Contents

Blank page

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by the Terrestrial Trunked Radio (TETRA) Project of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Voting phase of the ETSI standards approval procedure.

Every ETS prepared by ETSI is a voluntary standard. This ETS contains text concerning conformance testing of the equipment to which it relates. This text should be considered only as guidance and does not make this ETS mandatory.

This ETS is a multi-part standard and will consist of the following parts:

Part 1: "Radio";

Part 2: "Protocol testing specification for Voice plus Data (V+D)";

Part 4: "Protocol testing specification for Direct Mode Operation (DMO)";

Part 5: "Security".

Proposed transposition dates	
Date of latest announcement of this ETS (doa):	3 months after ETSI publication
Date of latest publication of new National Standard or endorsement of this ETS (dop/e):	6 months after doa
Date of withdrawal of any conflicting National Standard (dow):	6 months after doa

Blank page

1 Scope

This ETS contains the Test Suite Structure (TSS) and Test Purposes (TPs) to test the TETRA security protocols for Voice + Data (V+D) and Direct Mode (DM).

The TPs presented in this ETS are applicable to TETRA terminals supporting security as specified in ETS 300 392-2 [1], ETS 300 392-7 [2] and ETS 300 396-6 [3].

The objective of this test specification is to provide a basis for approval tests for TETRA equipment giving a high probability of air interface inter-operability between different manufacturer's TETRA equipment.

The ISO standard for the methodology of conformance testing, ISO/IEC 9646-1 [5] and ISO/IEC 9646-2 [6], as well as the ETSI methodology for conformance testing, ETS 300 406 [4], are used as the basis for the test methodology.

2 Normative references

This ETS incorporates by dated and undated reference, provisions from other publications. These normative references are cited at the appropriate places in the text and the publications are listed hereafter. For dated references, subsequent amendments to or revisions of any of these publications apply to this ETS only when incorporated in it by amendment or revision. For undated references the latest edition of the publication referred to applies.

[1] ETS 300 392-2: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".

[2] ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[3] ETS 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

[4] ETS 300 406: "Methods for Testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

[5] ISO/IEC 9646-1 (1994): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 1: General concepts". (See also CCITT Recommendation X.290 (1991))

[6] ISO/IEC 9646-2 (1991): "Information technology - Open Systems Interconnection - Conformance testing methodology and framework - Part 2: Abstract test suite specification". (See also CCITT Recommendation X.291 (1991))

[7] ETS 300 394-5-1: "Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 1: Protocol Implementation Conformance Statement (PICS) proforma specification".

[8] ETS 300 394-5-3: "Terrestrial Trunked Radio (TETRA); Conformance testing specification; Part 5: Security; Sub-part 3: Abstract Test Suite (ATS)".

3 Definitions and abbreviations

3.1 TETRA definitions

For the purposes of this ETS, the definitions given in ETS 300 392-7 [2] and ETS 300 396-6 [3] apply.

3.2 TETRA abbreviations

For the purposes of this ETS, the following TETRA abbreviations apply:

CCK	Common Cipher Key
DM	Direct Mode
DMO	Direct Mode Operation
ITSI	Individual TETRA Subscriber Identity
GCK	Group Cipher Key
KG	Key Generator
KH	Key Holder
KU	Key User
LA	Location Area
MAC	Medium Access Control
MM	Mobility Management
MS	Mobile Station
MSC	Message Sequence Chart
SCK	Static Cipher Key
SDS	Short Data Services sub entity within CMCE
SDU	Service Data Unit
SwMI	Switching and Management Infrastructure
V+D	Voice + Data

3.3 ISO 9646 abbreviations

For the purposes of this ETS, the following ISO 9646-1 [5] abbreviations apply:

ICS	Implementation Conformance Statement
IUT	Implementation Under Test
IXIT	Implementation eXtra Information for Testing
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement
PIXIT	Protocol Implementation eXtra Information for Testing
TP	Test Purpose
TSS	Test Suite Structure

4 Test Suite Structure (TSS)

4.1 Security TSS overview

The two security test suite, as illustrated in figure 1, are structured as a tree with a first level defined representing the V+D or DM whole test suite for TETRA security protocols.

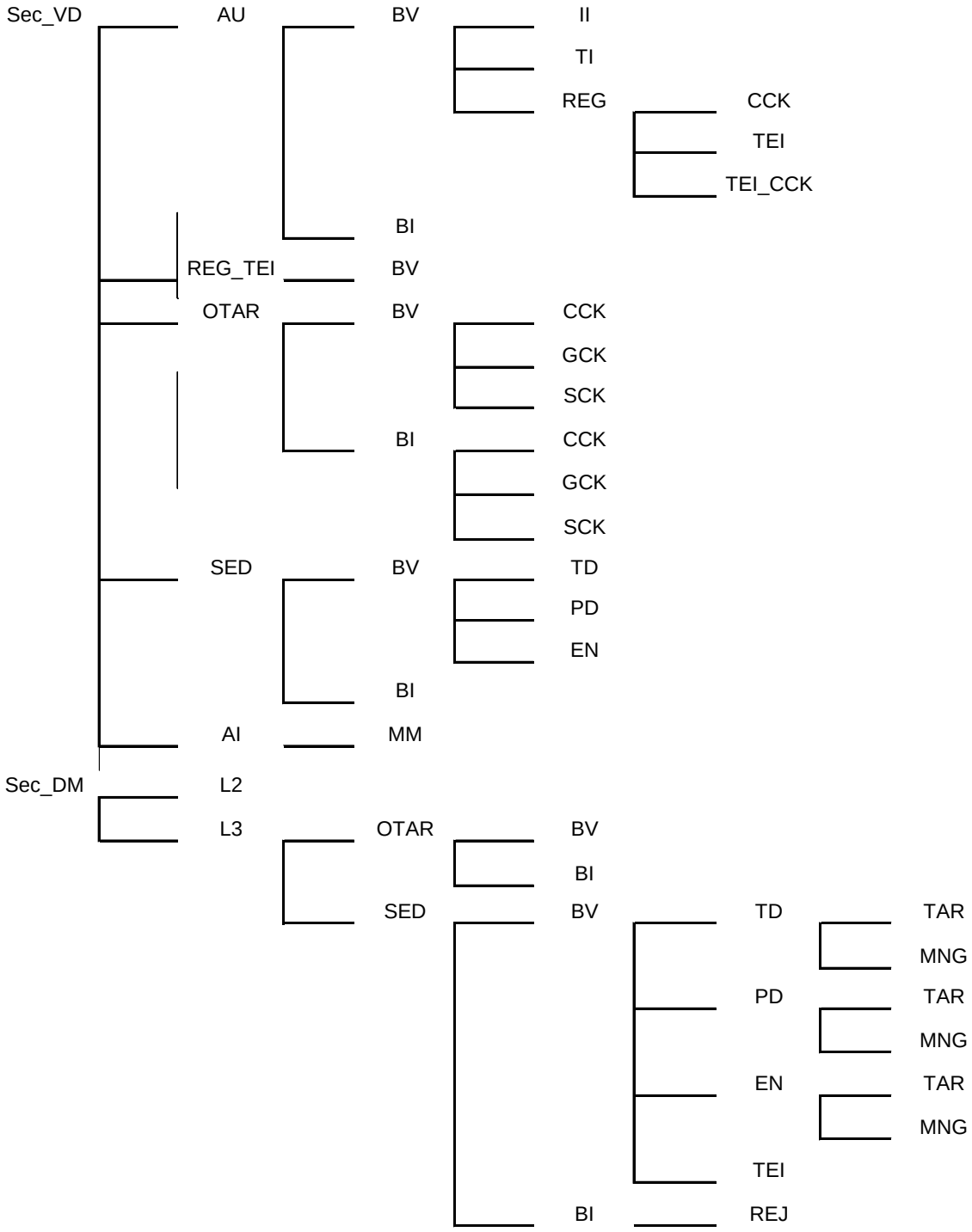

Figure 1: Security TSS

4.2 Security test groups

4.2.1 V+D Security test group

The V+D test groups are organized in several levels. The first level separates protocol test into the different functional capabilities: Authentication (AU), OTAR, Secure Enable/disable (SED) and Air Interface encryption (AI). The second level generally separates protocol test into two functional test groups according to the type of testing: Valid Behaviour (BV), and Invalid Behaviour (BI). The purpose of these test groups is explained in subclause 4.4.

The following list defines the Sec_VD layer test group names and identifiers:

= > to review

- Voice + Data (Sec_VD):
    - Authentication (AU):
        - Valid Behaviour tests (BV):
            - SwMI initiated (II);
            - Terminal initiated (TI);
            - Registration (REG)
                - CCK
                - TEI (TEI)
                - TEI_CCK
        - Invalid Behaviour tests (BI);
    - Registration with TEI (REG_TEI)
        - Valid Behaviour tests (BV):
    - Over The Air Rekeying (OTAR):
        - Valid Behaviour tests (BV):
            - Common Cipher Key (CCK);
            - Group Cipher Key (GCK);
            - Static Cipher Key (SCK);
        - Invalid Behaviour tests (BI):
            - Common Cipher Key (CCK);
            - Group Cipher Key (GCK);
            - Static Cipher Key (SCK);
    - Secure Enable/Disable (SED):
        - Valid Behaviour tests (BV):
            - Temporary disable (TD);
            - Permanent disable (PD);
            - Enable (EN);
        - Invalid Behaviour tests (BI);
    - Air Interface encryption (AI)
    - Mobility management (MM)

4.2.2 DM Security test group

The DM test groups are organized in several levels. The first level separates protocol test into the layer 2 and layer 3 configuration. The second level separates the different functional capabilities: OTAR and Secure Enable/disable (SED). The third level generally separates protocol test into two functional test groups according to the type of testing: Valid Behaviour (BV), and Invalid Behaviour (BI). The purpose of these test groups is explained in subclause 4.4.

The following list defines the S layer test group names and identifiers:

- DM (Sec_DM):
  - Layer 2 (L2):
  - Layer 3 (L3):
    - Over The Air Rekeying (OTAR):
      - Valid Behaviour tests (BV);
      - Invalid Behaviour tests (BI);
    - Secure Enable/Disable (SED):
      - Valid Behaviour tests (BV):
        - Temporary disable (TD):
          - Target role (TAR);
          - Manager role (MNG);
        - Permanent disable (PD):
          - Target role (TAR);
          - Manager role (MNG);
        - Enable (EN):
          - Target role (TAR);
          - Manager role (MNG);
        - TEI delivery (TEI);
        - ENDIS reject (REJ);
      - Invalid Behaviour tests (BI).

4.3 Test group description

The Valid Behaviour (BV) group tests an IUT in response to valid behaviour of the test system. "Valid" means that a test event is syntactically and contextually correct. All test cases in the valid behaviour group are intended to verify as thoroughly as possible the various functions of the protocol.

The Invalid Behaviour (BI) group is intended to verify that the IUT is able to react properly in case an invalid Protocol Data Unit (PDU) occurring. Invalid PDU here means syntactically or semantically invalid test events generated by the test system. A syntactically or semantically invalid test event regardless of the current state is not allowed. Inopportune test cases are also included in this test group. These are intended to verify that the IUT is able to react properly in case an inopportune test event occurs. Such an event is syntactically correct, but occurs when it is not allowed.

5 Introduction to Test Purposes (TPs)

Each TP is defined with the following assumptions:

- the Implementation Under Test (IUT) is a TETRA MS;
- for V+D tests, the test system is a simulation of the TETRA SwMI;
- for DM tests the test system is a simulation of a DM-MS;
- connection to the IUT is by either a test connector or by an RF connection.

The TPs are defined in clause 6 for TETRA V+D security and in clause 7 for DM.

5.1 TP definition conventions

The TPs are defined following particular rules as shown in table 1.

Table 1: TP definition rules

TP Id	Reference Condition Initial state Stimulus Expected behaviour of the test
TP Id:	The TP Id is a unique identifier. It shall be specified according to the TP naming conventions defined in subclause 5.2.
Reference:	The reference should contain the references of the subject to be validated by the actual TP (specification reference, clause, paragraph).
Condition:	The conditions applying to selecting the test purpose
Initial State:	Defines in which initial state the IUT has to be, in order to apply the TP.
Stimulus:	The stimulus defines the test event to which the TP is related.
Expected behaviour:	Definition of the events that are expected from the IUT to conform to the base specification. Definition of the events generated by the test system to check the behaviour of the IUT.

5.2 TP naming conventions

The identifier of the TP is built according to table 2:

Table 2: TP naming convention

TP/<ts>/<l>/<fm>/<<x>/<s>/<nn>		
<ts> = test suite	Sec_VD	Security for V+D
	Sec_DM	Security for DM
<l> = layer	L3	Layer 3 (not in the V+D part)
	L2	Layer 2 (not in the V+D part)
<fm> = functional module	For Sec layer:	
	AU	Authentication
	OTAR	Over The Air Rekeying
	SED	Secure Enable/Disable
	AI	Air Interface Encryption
x = Type of testing	BV	Valid Behaviour Tests
	BI	Invalid Behaviour Tests
s = test subgroup (as many subgroups as required)		as defined in the test suite structure
<nn> = sequential number	(01-99)	Test Purpose Number

6 Test Purposes for V+D

NOTE: The MSCs given in this clause are for information only.

6.1 Steps

The following steps are defined to check specific states of the IUT.

6.1.1 Check encryption state

There is no explicit (external observable) security protocol at layer 2 of TETRA protocol stack. Therefore the encryption state should be taken care by the test system, and a procedure is defined to check if the IUT and the test system are in the same encryption state.

Check_Encryption	Objective: to check that the IUT is in the correct encryption state The IUT is requested to initiate a CMCE call: depending on its capability it shall send a U-SETUP to initiate an individual or a group call or it shall send an U-SDS DATA to initiate an SDS call. If one of these PDUs is correctly received, this indicates that the IUT and test system are in the same encryption state.

6.1.2 Check enable state

Check_Enable	Objective: to check that the IUT is in the enabled state Depending on the capability of the IUT: If IUT is enabled and supports individual call, when it receives an individual call initiated by test system, it shall respond with U-ALERT or U-CONNECT PDU. If IUT is enabled and supports group call, when it is requested to initiate a group call, it shall send a U-SETUP PDU.

6.1.3 Check permanent disabled

Check_Permanent_Disable	Objective: to check that the IUT is permanently disabled If the IUT is permanently disabled, after receipt of a D-LOCATION UPDATE COMMAND PDU, it shall not respond.

6.1.4 Check temporary disable

Check_Temporary_Disable	Objective: to check that the IUT is temporarily disabled If the IUT is temporarily disabled, after receipt of a network initiated individual call, it shall not respond.

6.2 Authentication

Test group objective:

To test the authentication capabilities and protocol of the IUT. This test group shall test all authentication scenarios described in ETS 300 392-7 [2], clause 4, i.e. terminal initiated, SwMI initiated, and mutual.

6.2.1 Authentication initiated by the SwMI

Test group objective:

To test the authentication capabilities and protocol of the IUT when the authentication procedure is initiated by the SwMI.

6.2.1.1 SwMI authenticates MS

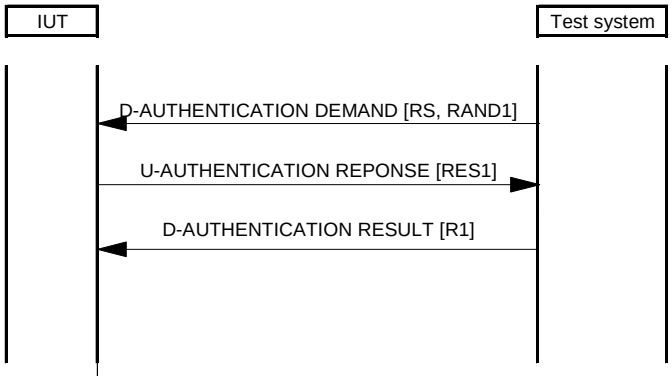

Figure 2: Authentication of MS by SwMI

Test purpose (L3):

To verify correct operation at layer 3 of MS (IUT) when subjected to an authentication demand from the SwMI (Test system).

TP/Sec_VD/AU/BV/II/01	Reference: ETS 300 392-7 [2], subclause 4.4.2.1 Condition: IUT supports SwMI initiated authentication Initial state: IUT registered (see note) Stimulus: Test system sends D-AUTHENTICATION DEMAND PDU Verify that the IUT sends the U-AUTHENTICATION RESPONSE PDU with the RES1 information element. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE: The encryption parameters established at registration shall be maintained.	

6.2.1.2 Authentication initiated by SwMI and made mutual by MS

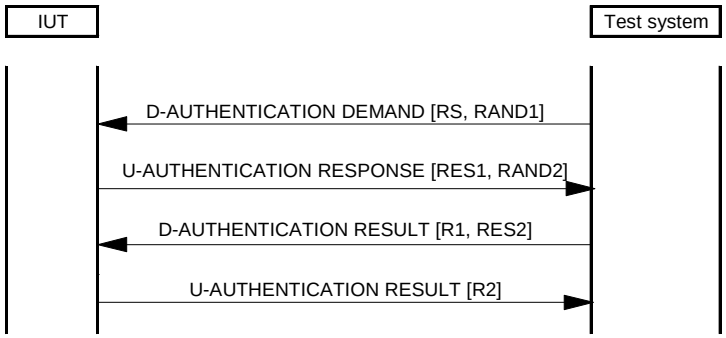

Figure 3: Authentication initiated by SwMI and made mutual by MS

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when subjected to an authentication demand from the SwMI (test system). To also verify that when the MS is configured to counter any authentication demand with a challenge that this operates correctly.

TP/Sec_VD/AU/BV/II/02	Reference: ETS 300 392-7 [2], subclause 4.4.2.3 Condition: IUT supports SwMI initiated and made mutual by MS Initial state: IUT registered (see note) Stimulus: Test system sends D-AUTHENTICATION DEMAND PDU Verify that, the IUT respond with U-AUTHENTICATION RESPONSE which contains RAND2 and RES1. Verify that after receipt of a D–AUTHENTICATION RESULT PDU, the IUT sends a U–AUTHENTICATION RESULT PDU. Verify that R1 = R2 = true. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE: The encryption parameters established at registration shall be maintained.	

6.2.2 Authentication procedures initiated by the MS

Test group objective:

To test the authentication capabilities and protocol of the IUT when it initiates the authentication procedure.

6.2.2.1 MS authenticates SwMI

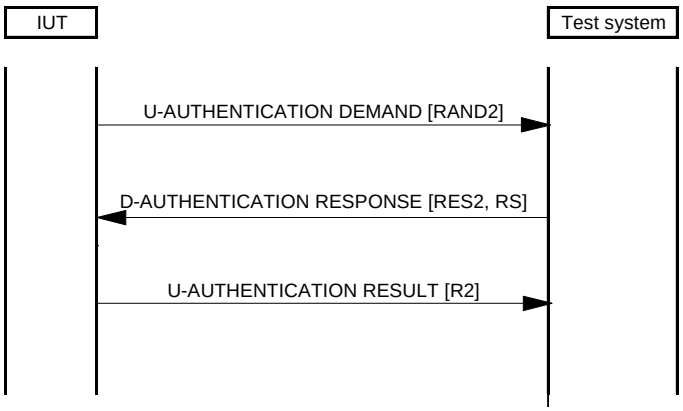

Figure 4: Authentication of the SwMI by the MS

Test purpose (L3):

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system).

TP/Sec_VD/AU/BV/TI/01	Reference: ETS 300 392-7 [2], subclause 4.4.2.2 Condition: IUT supports MS initiated authentication Initial state: IUT registered (see note) Stimulus: IUT invokes the sending of U-AUTHENTICATION DEMAND Verify that, after the test system responds with a valid response that the IUT gives result = TRUE in the U-AUTHENTICATION RESULT PDU. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE: The encryption parameters established at registration shall be maintained.	

6.2.2.2 Authentication initiated by MS and made mutual by SwMI

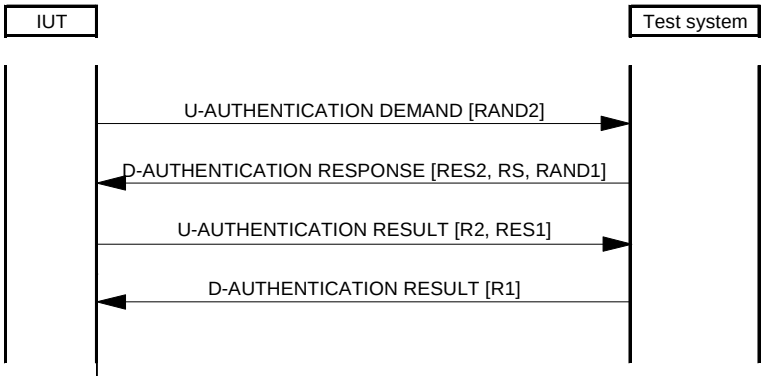

Figure 5: Authentication initiated by MS and made mutual by SwMI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system).

TP/Sec_VD/AU/BV/TI/02	Reference: ETS 300 392-7 [2], subclause 4.4.2.4 Condition: IUT supports authentication initiated by MS and made mutual by SwMI Initial state: IUT registered (see note) Stimulus: IUT invokes the sending of U-AUTHENTICATION DEMAND PDU Verify that, after receipt of a D-AUTHENTICATION RESPONSE PDU, the IUT sends a U-AUTHENTICATION RESULT. Verify that R1 = R2 = True. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE: The encryption parameters established at registration shall be maintained.	

6.2.3 Authentication procedures during registration

Test group objective:

To test the authentication capabilities and protocol of the IUT when authentication is initiated during registration.

6.2.3.1 SwMI authenticates MS during registration

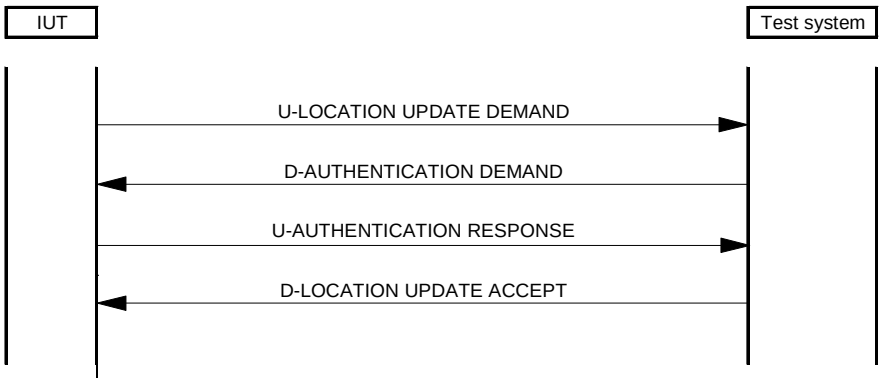

Figure 6: SwMI authenticates MS during registration procedure

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when registering to a network and being subjected to an authentication demand from the SwMI (test system).

TP/Sec_VD/AU/BV/REG/01	Reference: ETS 300 392-7 [2], subclause 4.4.2.5 Condition: IUT supports SwMI initiated authentication during registration Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU. Verify that after the receipt of the D-AUTHENTICATION DEMAND PDU, the IUT responds with the U-AUTHENTICATION RESPONSE PDU. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).

6.2.3.2 MS authenticates SwMI during registration

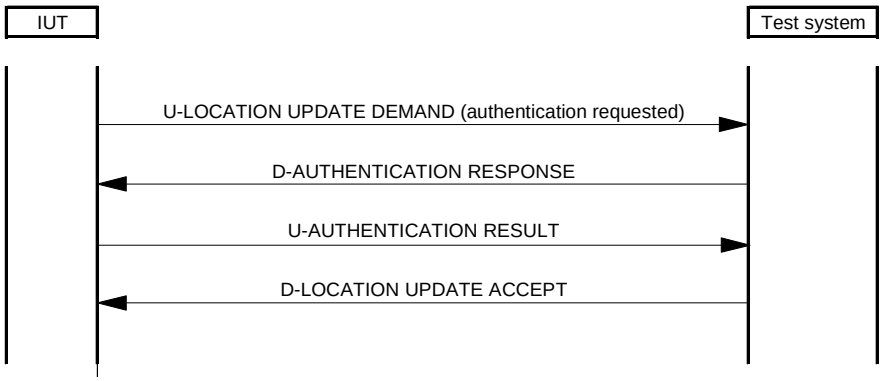

Figure 7: MS authenticates SwMI during registration

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system).

TP/Sec_VD/AU/BV/REG/02	Reference: ETS 300 392-7 [2], subclause 4.4.2.6 Condition: IUT supports MS initiated authentication during registration Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU with authentication request. Verify that after receiving the D-AUTHENTICATION RESPONSE PDU, the IUT responds with the U-AUTHENTICATION RESULT PDU with R2 = True.

6.2.3.3 Authentication initiated by MS during registration made mutual by SwMI

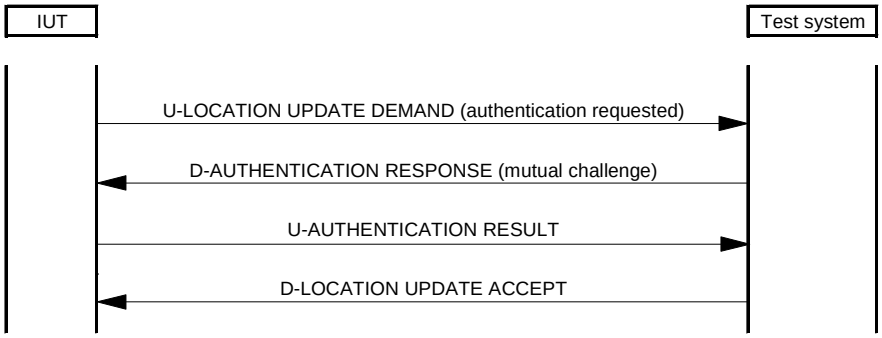

Figure 8: Authentication initiated by MS during registration made mutual by SwMI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system), which responds by a mutual authentication demand.

TP/Sec_VD/AU/BV/REG/03	Reference: ETS 300 392-7 [2], subclause 4.4.2.7 Condition: IUT supports authentication initiated by MS during registration made mutual by SwMI Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU with authentication request. Verify that after receiving the D-AUTHENTICATION RESPONSE PDU containing an authentication mutual challenge, the IUT responds with the U-AUTHENTICATION RESULT PDU with R2 = True.

6.2.3.4 SwMI authentication initiated during registration and made mutual by the MS

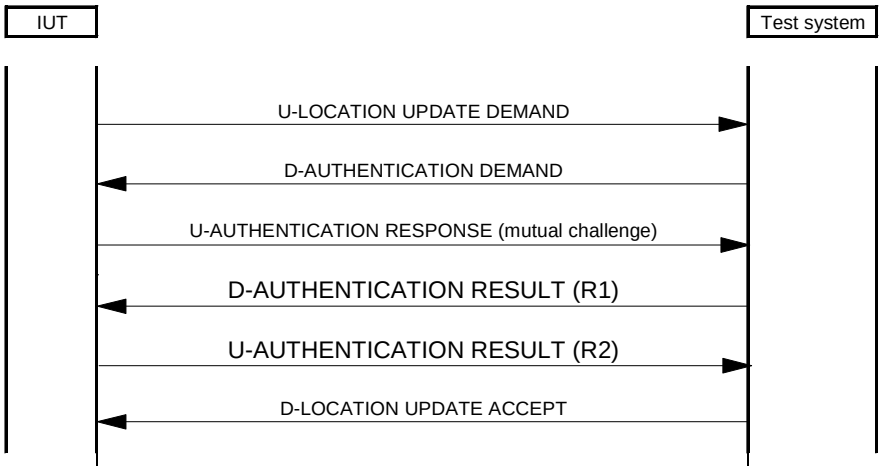

Figure 9: SwMI authentication initiated during registration and made mutual by the MS

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making a mutual authentication in a SwMI initiated authentication during registration.

TP/Sec_VD/AU/BV/REG/04	Reference: ETS 300 392-7 [2], subclause 4.4.2.8 Condition: IUT supports authentication initiated by SwMI during registration made mutual by IUT Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU without authentication request. Verify that after receiving the D-AUTHENTICATION DEMAND PDU, the IUT responds with the U-AUTHENTICATION RESPONSE PDU with a mutual authentication challenge. Verify that after receipt of the D–AUTHENTICATION RESULT with R1 = TRUE, the IUT sends the U–AUTHENTICATION RESULT with R2 = TRUE.

6.2.3.5 Authentication during registration with CCK delivery

Test group objective:

To test the authentication capabilities and protocol of the IUT when the authentication is initiated during registration with CCK delivery.

6.2.3.5.1 SwMI authenticates MS during registration and delivers CCK

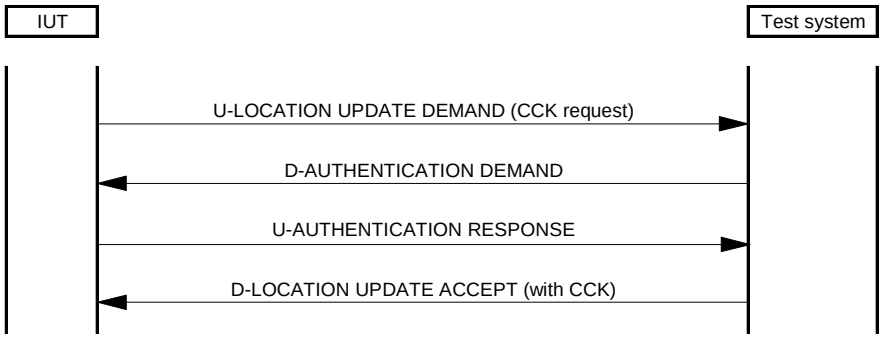

Figure 10: SwMI authenticates MS during registration and delivers CCK

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when subjected to an authentication demand from the SwMI (test system) and when requesting CCK.

TP/Sec_VD/AU/BV/REG/CCK/01	Reference: ETS 300 392-7 [2], subclause 4.4.2.5 Condition: IUT supports SwMI initiated authentication during registration and CCK delivery at registration Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU containing a CCK request type 3 element. Verify that after the receipt of the D-AUTHENTICATION DEMAND PDU, the IUT responds with the U-AUTHENTICATION RESPONSE PDU and that it accepts the CCK in the D-LOCATION UPDATE ACCEPT PDU.

6.2.3.5.2 MS authenticates SwMI during registration and request CCK

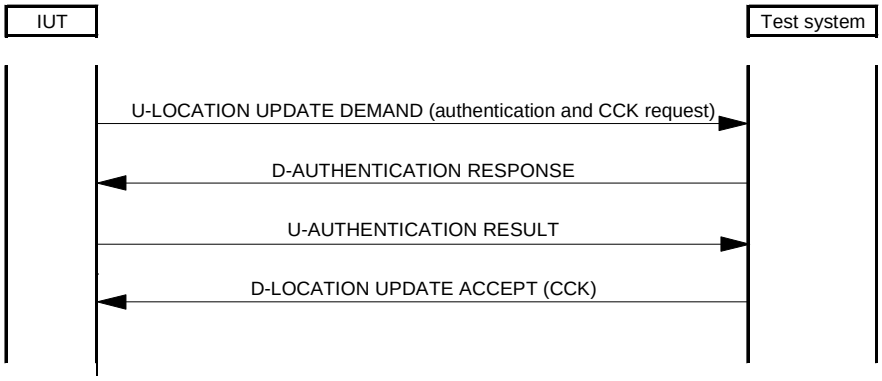

Figure 11: MS authenticates SwMI during registration and request CCK

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system) with CCK provision.

TP/Sec_VD/AU/BV/REG/CCK/02	Reference: ETS 300 392-7 [2], subclause 4.4.2.6 Condition: IUT supports MS initiated authentication during registration and CCK delivery at registration Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU with authentication and CCK request. Verify that after receiving the D-AUTHENTICATION RESPONSE PDU, the IUT responds with the U-AUTHENTICATION RESULT PDU with R2 = True.

6.2.3.5.3 Authentication initiated by MS during registration including a CCK request and made mutual by SwMI

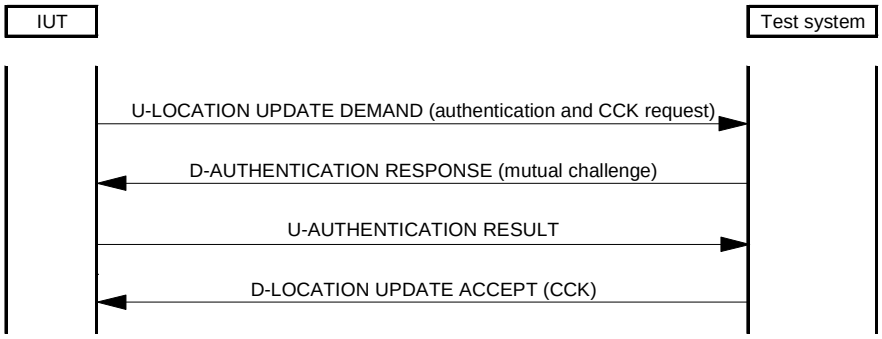

Figure 12: Authentication initiated by MS during registration including a CCK request and made mutual by SwMI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system), which responds by a mutual authentication demand and CCK exchange.

TP/Sec_VD/AU/BV/REG/CCK/03	Reference: ETS 300 392-7 [2], subclause 4.4.2.7 Condition: IUT supports authentication initiated by MS during registration made mutual by SwMI and CCK delivery at registration Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU with authentication and CCK request. Verify that after receiving the D-AUTHENTICATION RESPONSE PDU containing an authentication mutual challenge, the IUT responds with the U-AUTHENTICATION RESULT PDU.

6.2.3.5.4 SwMI authentication initiated during registration and made mutual by the MS with CCK exchange

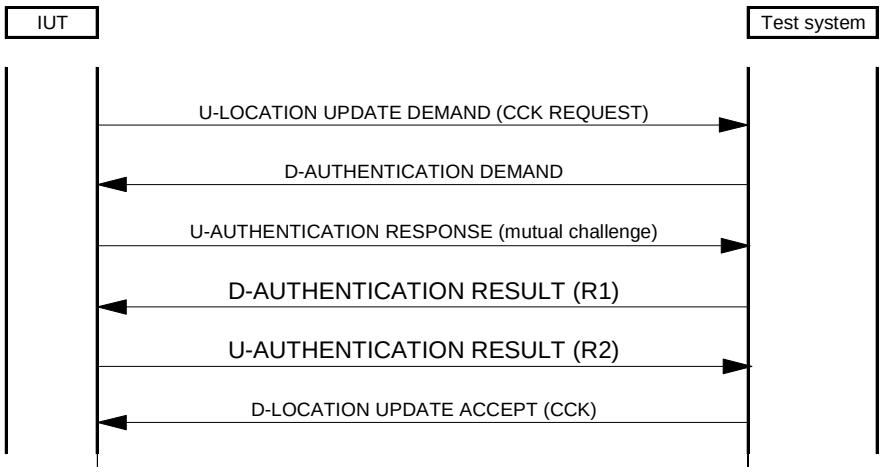

Figure 13: SwMI authentication initiated during registration and made mutual by the MS with CCK exchange

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making a mutual authentication in a SwMI initiated authentication during registration with CCK exchange.

TP/Sec_VD/AU/BV/REG/CCK/04	Reference: ETS 300 392-7 [2], subclause 4.4.2.8 Condition: IUT supports: authentication initiated by SwMI during registration made mutual by IUT and CCK delivery at registration Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU without authentication request and with CCK request. Verify that after receiving the D-AUTHENTICATION DEMAND PDU, the IUT responds with the U-AUTHENTICATION RESPONSE PDU with a mutual authentication challenge. Verify that after receipt of the D-AUTHENTICATION RESULT with R1 = TRUE, the IUT sends the U-AUTHENTICATION RESULT with R2 = TRUE.

6.2.3.6 Authentication procedures during registration with TEI exchange

Test group objective:

To test the authentication capabilities and protocol of the IUT when authentication is initiated during registration with TEI delivery.

6.2.3.6.1 SwMI authenticates MS during registration and includes a TEI request

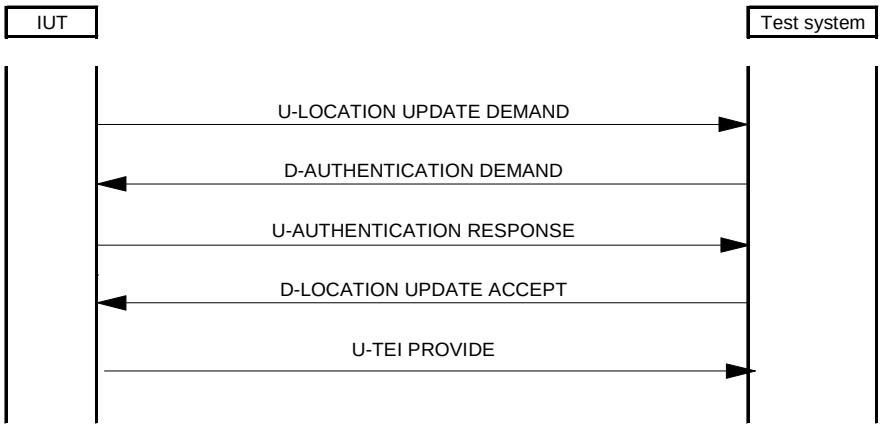

Figure 14: SwMI authenticates MS during registration and includes TEI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when subjected to an authentication demand from the SwMI (test system) with a TEI provision.

TP/Sec_VD/AU/BV/REG/TEI/01	Reference: ETS 300 392-7 [2], subclause 4.4.2.5 Condition: IUT supports SwMI initiated authentication during registration and TEI delivery Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU. Verify that after the receipt of the D-AUTHENTICATION DEMAND PDU, the IUT responds with the U-AUTHENTICATION RESPONSE PDU. Verify that after receipt of the D-LOCATION UPDATE ACCEPT PDU containing a TEI request, the IUT sends the U-TEI PROVIDE PDU.

6.2.3.6.2 MS authenticates SwMI during registration and the SwMI request TEI

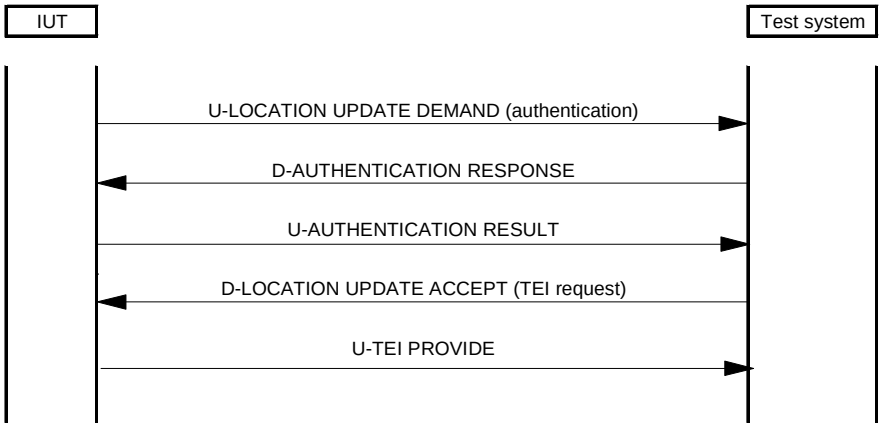

Figure 15: MS authenticates SwMI during registration and the SwMI request TEI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system) with TEI provision.

TP/Sec_VD/AU/BV/REG/TEI/02	Reference: ETS 300 392-7 [2], subclause 4.4.2.6 Condition: IUT supports MS initiated authentication during registration and TEI delivery Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU with authentication request. Verify that after receiving the D-AUTHENTICATION RESPONSE PDU, the IUT responds with the U-AUTHENTICATION RESULT PDU. Verify that after receipt of the D-LOCATION UPDATE ACCEPT PDU containing a TEI request, the IUT sends the U-TEI PROVIDE PDU.

6.2.3.6.3 Authentication initiated by MS during registration including a TEI exchange and made mutual by SwMI

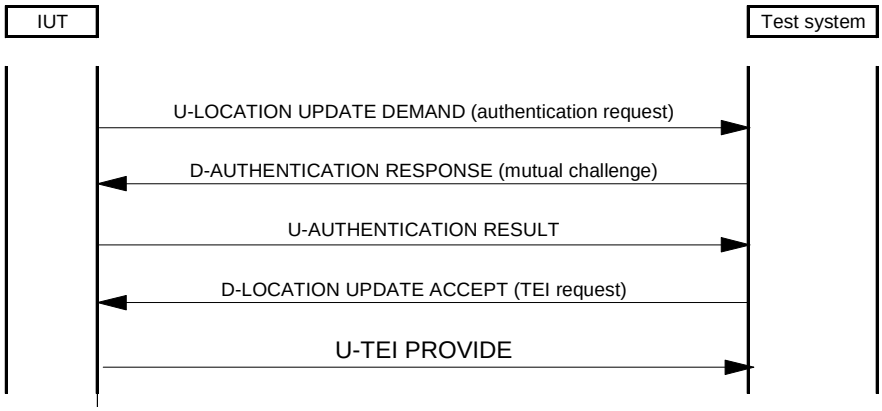

Figure 16: Authentication initiated by MS during registration including a TEI exchange and made mutual by SwMI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system), which responds by a mutual authentication demand and TEI exchange.

TP/Sec_VD/AU/BV/REG/TEI/03	Reference: ETS 300 392-7 [2], subclause 4.4.2.7 Condition: IUT supports authentication initiated by MS during registration made mutual by SwMI and TEI delivery. Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU with authentication request. Verify that after receiving the D-AUTHENTICATION RESPONSE PDU containing an authentication mutual challenge, the IUT responds with the U-AUTHENTICATION RESULT PDU. Verify that after receipt of the D-LOCATION UPDATE ACCEPT PDU containing a TEI request, the IUT sends the U-TEI PROVIDE PDU.

6.2.3.6.4 SwMI authentication initiated during registration and made mutual by the MS with TEI exchange

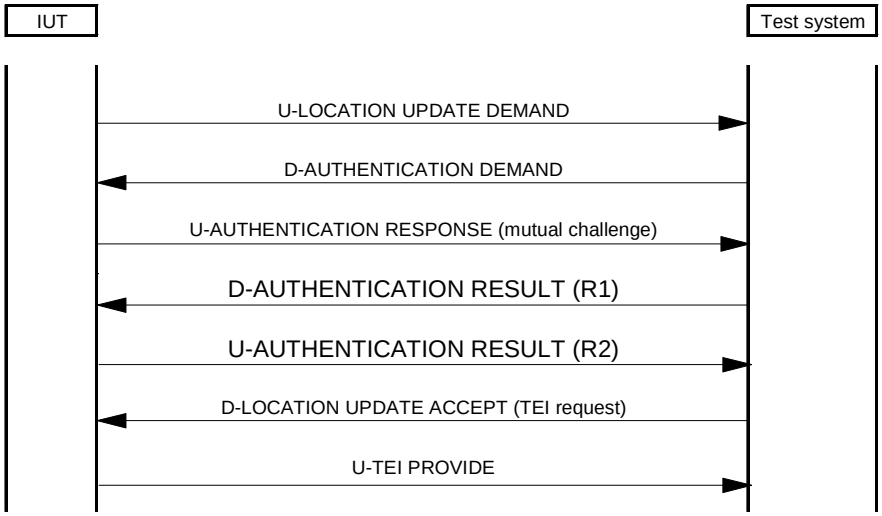

Figure 17: SwMI authentication initiated during registration and made mutual by the MS with TEI exchange

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making a mutual authentication in a SwMI initiated authentication during registration with TEI exchange.

TP/Sec_VD/AU/BV/REG/TEI/04	Reference: ETS 300 392-7 [2], subclause 4.4.2.8 Condition: IUT supports authentication initiated by SwMI during registration made mutual by MS and TEI delivery. Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU without authentication request. Verify that after receiving the D-AUTHENTICATION DEMAND PDU, the IUT responds with the U-AUTHENTICATION RESPONSE PDU with a mutual authentication challenge. Verify that after receipt of the D–AUTHENTICATION RESULT with R1 = TRUE, the IUT sends the U–AUTHENTICATION RESULT with R2 = TRUE. Verify that after receipt of the D-LOCATION UPDATE ACCEPT PDU containing a TEI request, the IUT sends the U-TEI PROVIDE PDU.

6.2.3.7 Authentication procedures during registration with TEI and CCK exchange

Test group objective:

To test the authentication capabilities and protocol of the IUT when authentication is initiated during registration with TEI and CCK delivery.

6.2.3.7.1 SwMI authenticates MS during registration, delivers CCK and receives TEI

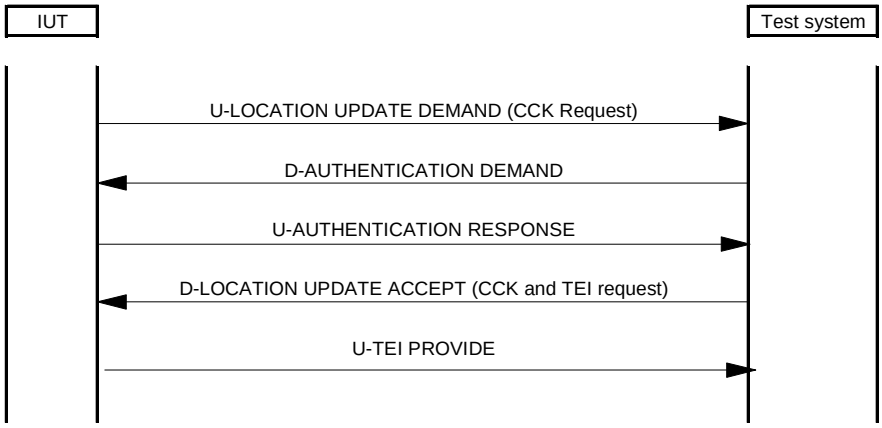

Figure 18: SwMI authenticates MS during registration, delivers CCK and receives TEI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when subjected to an authentication demand from the SwMI (test system) with a TEI and CCK provision.

TP/Sec_VD/AU/BV/REG/TEI_CCK/01	Reference: ETS 300 392-7 [2], subclause 4.4.2.5 Condition: IUT supports SwMI initiated authentication during registration and CCK delivery at registration and TEI delivery Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU containing a CCK request type 3 element. Verify that after the receipt of the D-AUTHENTICATION DEMAND PDU, the IUT responds with the U-AUTHENTICATION RESPONSE PDU. Verify that after receipt of the D-LOCATION UPDATE ACCEPT PDU containing a TEI request and the CCK information element, the IUT sends the U-TEI PROVIDE PDU.

6.2.3.7.2 MS authenticates SwMI during registration and delivers TEI and request CCK

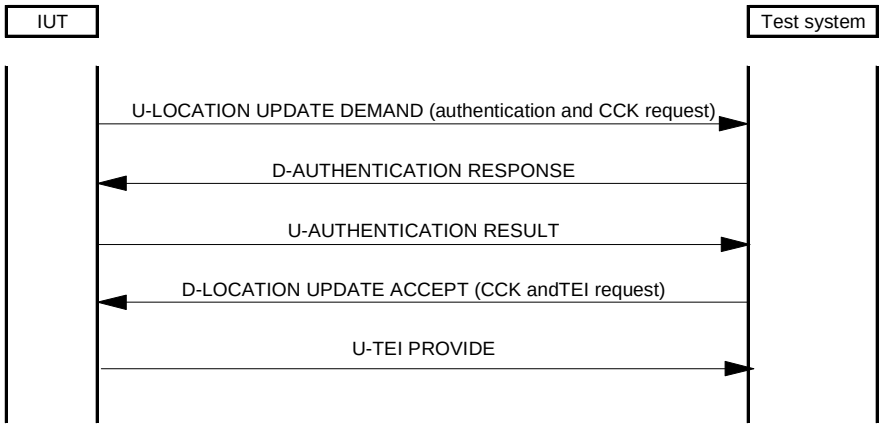

Figure 19: MS authenticates SwMI during registration and delivers TEI and request CCK

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system) with TEI provision.

TP/Sec_VD/AU/BV/REG/TEI_CCK/02	Reference: ETS 300 392-7 [2], subclause 4.4.2.6 Condition: IUT supports MS initiated authentication during registration and CCK delivery at registration and TEI delivery Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U–LOCATION UPDATE DEMAND PDU with authentication request containing a CCK request. Verify that after receiving the D-AUTHENTICATION RESPONSE PDU, the IUT responds with the U-AUTHENTICATION RESULT PDU. Verify that after receipt of the D-LOCATION UPDATE ACCEPT PDU containing a TEI request, the IUT sends the U-TEI PROVIDE PDU.

6.2.3.7.3 Authentication initiated by MS during registration including TEI, CCK exchange and made mutual by SwMI

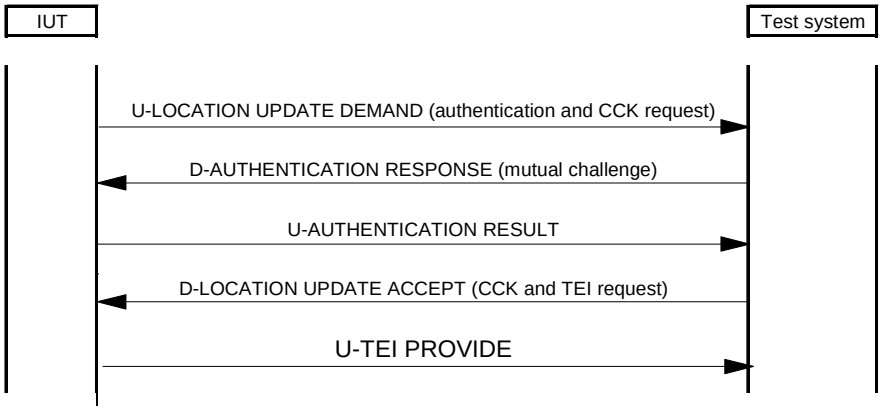

Figure 20: Authentication initiated by MS during registration including TEI, CCK exchange and made mutual by SwMI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an authentication demand of the SwMI (test system), which responds by a mutual authentication demand and CCK and TEI exchange.

TP/Sec_VD/AU/BV/REG/TEI_CCK 03	Reference: ETS 300 392-7 [2], subclause 4.4.2.7 Condition: IUT supports authentication initiated by MS during registration made mutual by SwMI and TEI delivery and CCK delivery at registration. Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU with authentication and CCK request. Verify that after receiving the D-AUTHENTICATION RESPONSE PDU containing an authentication mutual challenge, the IUT responds with the U-AUTHENTICATION RESULT PDU. Verify that after receipt of the D-LOCATION UPDATE ACCEPT PDU containing a TEI request, the IUT sends the U-TEI PROVIDE PDU.

6.2.3.7.4 SwMI authentication initiated during registration and made mutual by the MS with TEI and CCK exchange

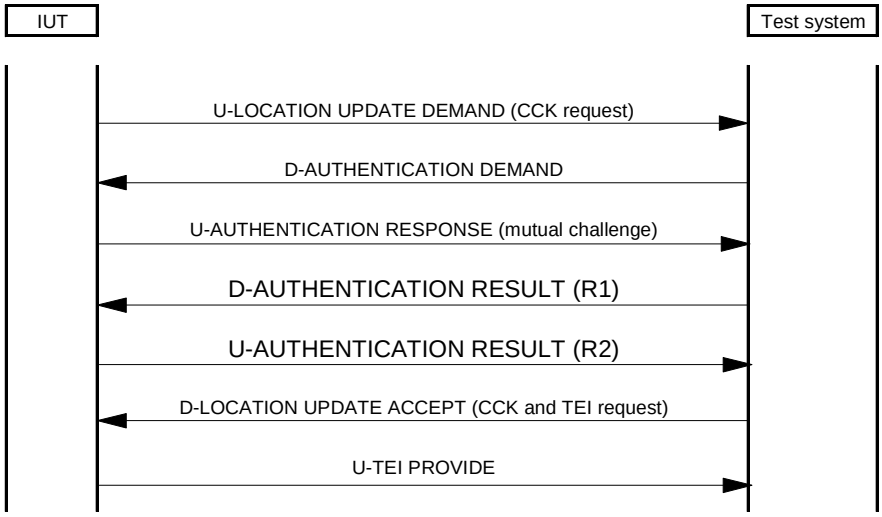

Figure 21: SwMI authentication initiated during registration and made mutual by the MS with TEI and CCK exchange

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making a mutual authentication in a SwMI initiated authentication during registration with TEI and CCK exchange.

TP/Sec_VD/AU/BV/REG/TEI_CCK/04	Reference: ETS 300 392-7 [2], subclause 4.4.2.8 Condition: IUT supports authentication initiated by SwMI during registration made mutual by MS and TEI delivery and CCK delivery at registration. Initial state: IUT camped on a cell Stimulus: IUT is made to invoke the sending of a U-LOCATION UPDATE DEMAND PDU without authentication request and with authentication and CCK request. Verify that after receiving the D-AUTHENTICATION DEMAND PDU, the IUT responds with the U-AUTHENTICATION RESPONSE PDU with a mutual authentication challenge. Verify that after receipt of the D-AUTHENTICATION RESULT with R1 = TRUE, the IUT sends the U-AUTHENTICATION RESULT with R2 = TRUE. Verify that after receipt of the D-LOCATION UPDATE ACCEPT PDU containing a TEI request and containing the CCK, the IUT sends the U-TEI PROVIDE PDU.

6.2.4 Unsuccessful authentication procedures

Test group objective:

To test the authentication capabilities and protocol of the IUT when authentication is unsuccessful.

6.2.4.1 Unsuccessful authentication initiated by MS

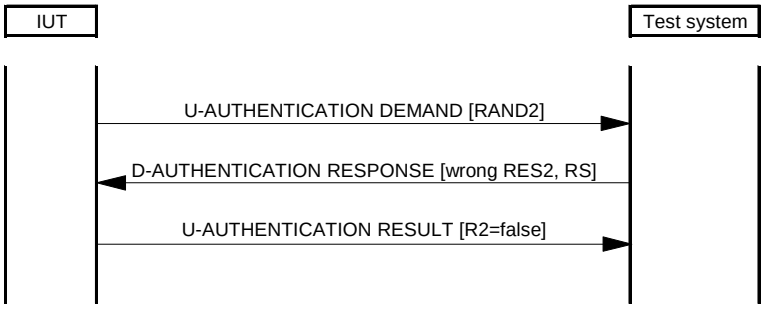

Figure 22: Unsuccessful authentication initiated by MS

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an unsuccessful mutual authentication demand of the SwMI (test system).

TP/Sec_VD/AU/BI/01	Reference: ETS 300 392-7 [2], subclause 4.4.2.2 Condition: IUT supports MS initiated authentication Initial state: IUT registered (see note) Stimulus: IUT invokes the sending of U-AUTHENTICATION DEMAND PDU Verify that, after receipt of a D-AUTHENTICATION RESPONSE PDU containing a wrong value of RES2, the IUT sends a U-AUTHENTICATION RESULT with R2 = false. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE: The encryption parameters established at registration shall be maintained.	

6.2.4.2 Unsuccessful MS authentication during mutual authentication initiated by the SwMI

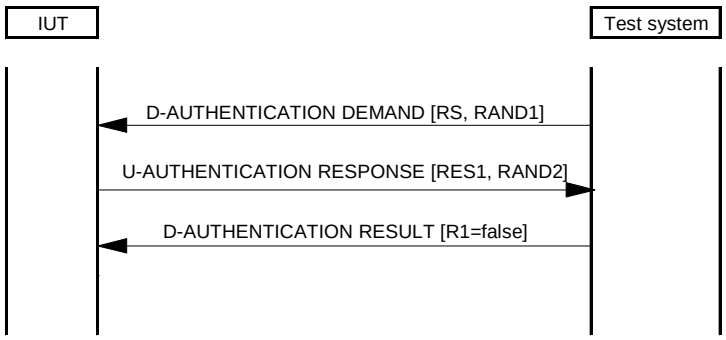

Figure 23: Unsuccessful MS authentication during mutual authentication initiated by the SwMI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when subjected to a mutual authentication failure.

TP/Sec_VD/AU/BI/02	Reference: ETS 300 392-7 [2], subclause 4.4.2.3 Condition: IUT supports authentication initiated by SwMI and made mutual by MS. Initial state: IUT registered (see note) Stimulus: Test system sends D-AUTHENTICATION DEMAND PDU Verify that, the IUT respond with the sequence: U-AUTHENTICATION RESPONSE which contains RAND2 and RES1. Verify that after receipt of a D-AUTHENTICATION RESULT PDU with R1 = false, the IUT does not send any response. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE: The encryption parameters established at registration shall be maintained.	

6.2.4.3 Unsuccessful SwMI authentication during mutual authentication initiated by the SwMI

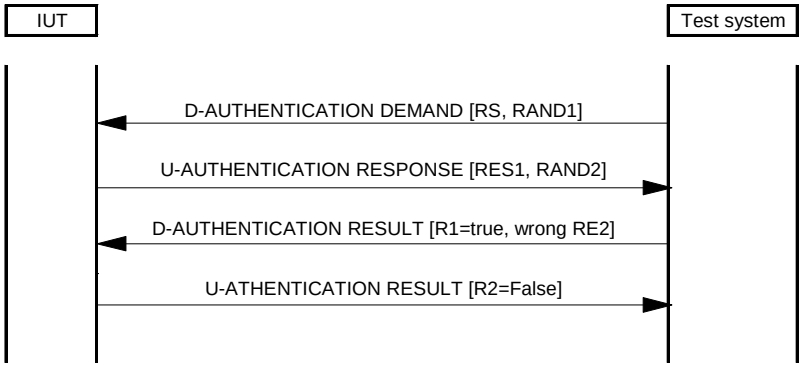

Figure 24: Unsuccessful SwMI authentication during mutual authentication initiated by the SwMI

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when subjected to a mutual authentication failure.

TP/Sec_VD/AU/BI/03	Reference: ETS 300 392-7 [2], subclause 4.4.2.3 Condition: IUT supports authentication initiated by SwMI and made mutual by MS. Initial state: IUT registered (see note) Stimulus: Test system sends D-AUTHENTICATION DEMAND PDU Verify that, the IUT respond with the sequence: U-AUTHENTICATION RESPONSE which contains RAND2 and RES1. Verify that after receipt of a D-AUTHENTICATION RESULT PDU with R1 = true and a wrong value of RES2, the IUT sends a U-AUTHENTICATION RESULT PDU with R2 = false. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE: The encryption parameters established at registration shall be maintained.	

6.2.4.4 Unsuccessful mutual authentication initiated by MS

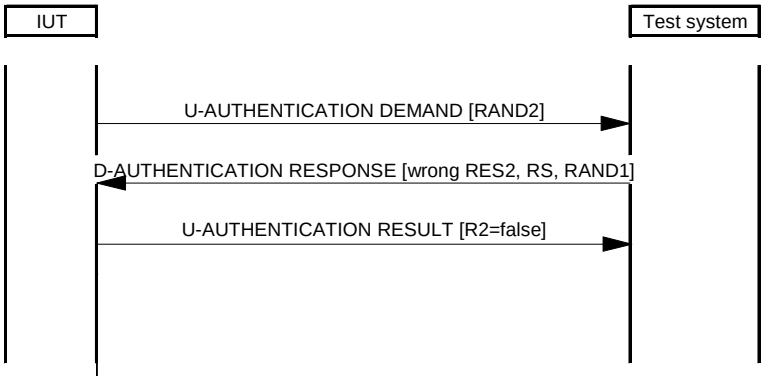

Figure 25: Unsuccessful mutual authentication initiated by MS

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when making an unsuccessful mutual authentication demand of the SwMI (test system).

TP/Sec_VD/AU/BI/04	Reference: ETS 300 392-7 [2], subclause 4.4.2.4 Condition: IUT supports authentication initiated by MS made mutual by SwMI. Initial state: IUT registered (see note) Stimulus: IUT invokes the sending of U-AUTHENTICATION DEMAND PDU Verify that, after receipt of a D-AUTHENTICATION RESPONSE PDU containing a wrong value of RES2, the IUT sends a U-AUTHENTICATION RESULT with R2 = false and RES1 shall not be included in this PDU. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE: The encryption parameters established at registration shall be maintained.	

6.3 TEI delivery during registration without authentication

Test group objective:

To test the TEI and/or CCK delivery capabilities and protocol of the IUT during registration without authentication.

6.3.1 TEI delivery during registration without authentication

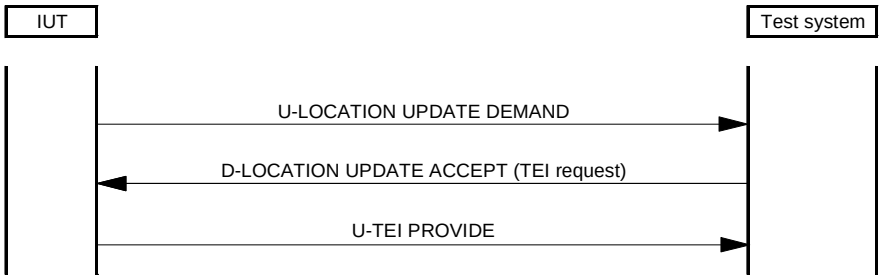

Figure 26: TEI delivery during registration without authentication

Test purpose:

To verify correct operation at layer 3 of MS (IUT) during registration without authentication with TEI delivery

TP/Sec_VD/REG_TEI/BV/01	Reference: ETS 300 392-7 [2] Condition: IUT supports TEI delivery Initial state: IUT camped on a cell. Stimulus: IUT invokes the sending of U-LOCATION UPDATE DEMAND PDU Verify that, after receipt of a D-LOCATION UPDATE ACCEPT PDU containing a TEI request, the IUT sends a U-TEI PROVIDE PDU.

6.4 OTAR

Test group objective:

To test the OTAR capabilities and protocol of the IUT. This test group shall test all OTAR scenarios described in ETS 300 392-7 [2], clause 4, i.e. for CCK, SCK and GCK for each of terminal initiated and SwMI initiated transfers.

6.4.1 CCK delivery functions

Test group objective:

To test the OTAR CCK capabilities of the IUT. This test group shall test all OTAR scenarios described in ETS 300 392-7 [2], clause 4, for CCK delivery for each of terminal initiated and SwMI initiated transfers.

6.4.1.1 SwMI-initiated CCK provision

NOTE: The selection of current and/or future CCK is identified only by the selection of parameters within each PDU.

This scenario shows SwMI providing a CCK to the MS.

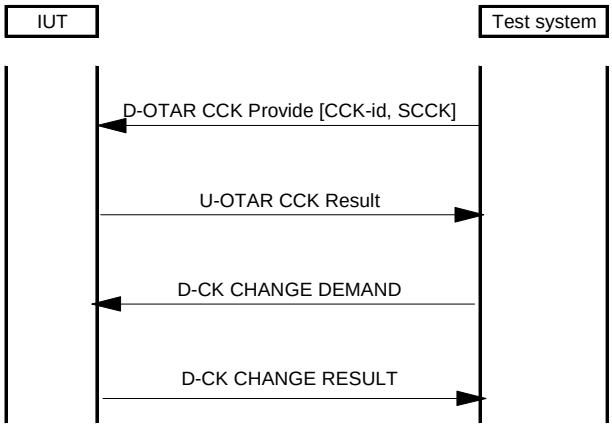

Figure 27: SwMI initiated CCK provision

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when the SwMI (test system) provides a new CCK for the current LA.

TP/Sec_VD/OTAR/BV/CCK/01	Reference: ETS 300 392-7 [2], subclause 4.4.3.2 Condition: IUT supports CCK delivery. Initial state: IUT registered, IUT authenticated (see note 1 and note 2). Stimulus: The test system is made to invoke the sending of D-OTAR CCK Provide PDU. Verify that, the IUT sends a U-OTAR CCK Result PDU after receipt of D–OTAR CCK Provide PDU containing a valid current CCK for the current LA. Verify that after receipt of the D-CK CHANGE DEMAND PDU requesting an acknowledgement, the IUT sends a D-CK CHANGE RESULT. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

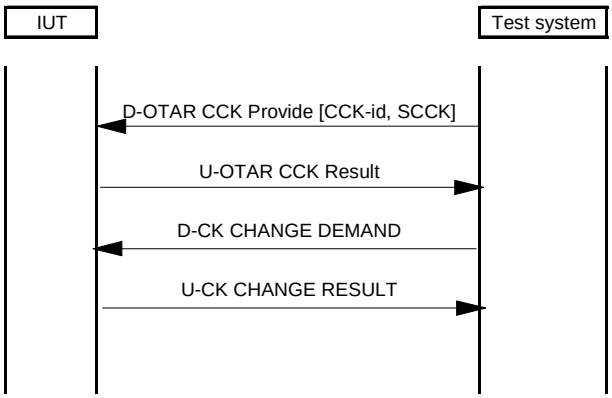

Figure 28: SwMI initiated CCK provision for other LA

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when the SwMI (test system) provides future CCK with a location area list

TP/Sec_VD/OTAR/BV/CCK/02	Reference: ETS 300 392-7 [2], subclause 4.4.3.2 Condition: IUT supports CCK delivery. Initial state: IUT registered, IUT authenticated (see note 1 and note 2). Stimulus: The test system is made to invoke the sending of D-OTAR CCK Provide PDU. Verify that, the IUT sends a U-OTAR CCK Result PDU after receipt of D–OTAR CCK Provide PDU containing a valid future CCK and the location area list. Verify that after receipt of the D-CK CHANGE DEMAND PDU requesting an acknowledgement, the IUT sends a D-CK CHANGE RESULT. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.1.2 MS-initiated CCK provision

This scenario shows MS requesting a CCK.

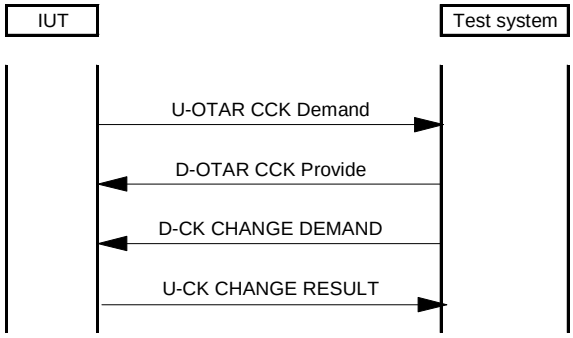

Figure 29: MS-initiated CCK provision

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when the MS initiates OTAR CCK provision.

TP/Sec_VD/OTAR/BV/CCK/03	Reference: ETS 300 392-7 [2], subclause 4.4.3.3 Condition: IUT supports OTAR CCK delivery Initial state: IUT registered, IUT authenticated (see note 1 and note 2). Stimulus: The IUT is made to invoke the request of a new CCK in the U-OTAR CCK Demand PDU. Verify that, IUT sends U-OTAR CCK Demand PDU. Test system sends D–OTAR CCK Provide PDU. Verify that after receipt of the D-CK CHANGE DEMAND PDU requesting an acknowledgement, the IUT sends a D-CK CHANGE RESULT. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.1.3 MS-initiated CCK provision in a U-PREPARE PDU

6.4.1.3.1 MS roams into a new cell in the same LA and the same registration area

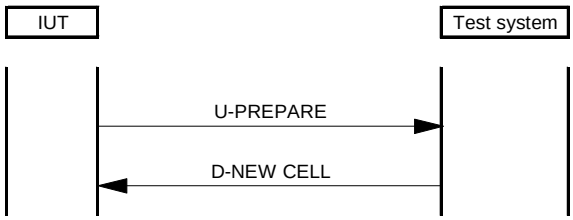

Figure 30: MS roams into a new cell in the same LA and the same registration area

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when the MS roams into a new cell in the same LA and the same registration area.

TP/Sec_VD/OTAR/BV/CCK/04	Reference: ETS 300 392-7 [2], subclause 4.4.3.3 Condition: IUT supports OTAR CCK delivery and supports announced type 1 cell reselection. Initial state: IUT registered, IUT authenticated, a CMCE call is in progress (see note 1 and note 2). Stimulus: The IUT is made to invoke the roaming in a new cell in the same LA and same registration area. Verify that, IUT sends U-PREPARE PDU without MM PDU including. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.1.3.2 MS roams into a new cell in a different LA and the same registration area

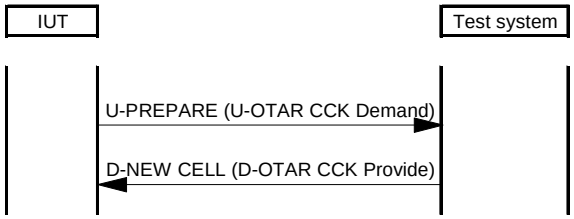

Figure 31: MS roams into a new cell in a different LA and the same registration area

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when the MS roams into a new cell in a different LA and the same registration area.

TP/Sec_VD/OTAR/BV/CCK/05	Reference: ETS 300 392-7 [2], subclause 4.4.3.3 Condition: IUT supports OTAR CCK delivery Initial state: IUT registered, IUT authenticated, a CMCE call is in progress (see note 1 and note 2). Stimulus: The IUT is made to invoke the roaming in a new cell in a different LA and same registration area. Verify that, IUT sends U-PREPARE PDU containing a U-OTAR CCK PDU. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.1.3.3 MS roams into a new cell in a different LA and different registration area

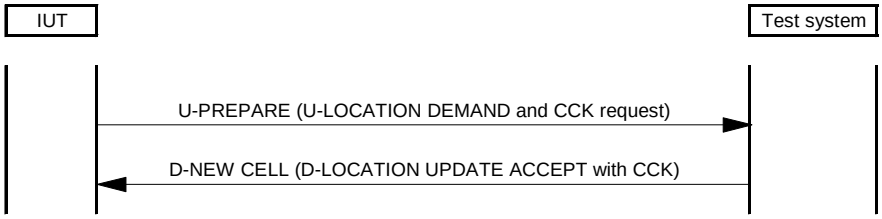

Figure 32: MS roams into a new cell in a different LA and different registration area

Test purpose:

To verify correct operation at layer 3 of MS (IUT) when the MS roams into a new cell in a different LA and different registration area.

TP/Sec_VD/OTAR/BV/CCK/06	Reference: ETS 300 392-7 [2], subclause 4.4.3.3 Condition: IUT supports CCK delivery. Initial state: IUT registered, IUT authenticated, a CMCE call is in progress (see note 1 and note 2). Stimulus: The IUT is made to invoke the roaming in a new cell in a different LA and different registration area. Verify that, IUT sends U-PREPARE PDU containing a U-LOCATION UPDATE with CCK request. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.1.4 SwMI provides an incorrect CCK to MS

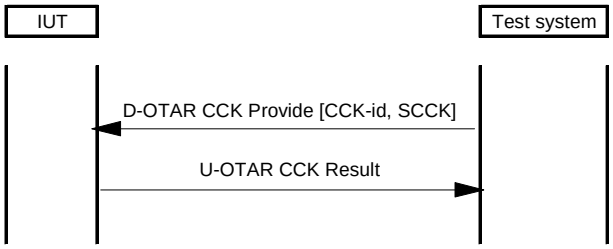

Figure 33: SwMI provides an incorrect CCK to MS

Test purpose:

To verify correct operation of MS (IUT) when the SwMI (test system) provides an incorrect CCK.

TP/Sec_VD/OTAR/BI/CCK/01	Reference: ETS 300 392-7 [2], subclause 4.4.3.2 Condition: IUT supports CCK delivery. Initial state: IUT registered, IUT authenticated (see note 1 and note 2). Stimulus: The test system is made to invoke the sending of D-OTAR CCK Provide PDU. Verify that, the IUT sends a U-OTAR CCK Result PDU including the provision result "incorrect KN" after receipt of D-OTAR CCK Provide PDU containing an invalid CCK. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.2 OTAR protocol functions SCK

Test group objective:

To test the OTAR SCK capabilities of the IUT. This test group shall test all OTAR scenarios described in ETS 300 392-7 [2], clause 4, for SCK delivery for each of terminal initiated and SwMI initiated transfers.

6.4.2.1 MS initiates provision of SCK

The MSC in figure 34 shows the case where the MS requests provision of one or more SCKs in use on a system.

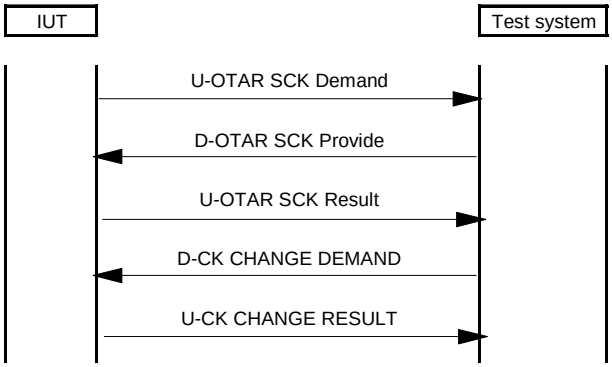

Figure 34: MS initiates provision of SCK

Test purpose:

To verify correct operation of MS (IUT) when the MS (IUT) initiates the provision of OTAR SCK.

TP/Sec_VD/OTAR/BV/SCK/01	Reference: ETS 300 392-7 [2], subclause 4.4.4.1 Condition: IUT supports OTAR SCK Initial state: IUT registered (see note 1 and note 2). Stimulus: The IUT is made to invoke a SCK demand. IUT sends U-OTAR SCK Demand PDU. Verify that after receipt of D–OTAR SCK Provide PDU, the IUT sends U-OTAR SCK Result PDU. Verify that after receipt of the D-CK CHANGE DEMAND PDU requesting an acknowledgement, the IUT sends a D-CK CHANGE RESULT. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: K is available to both the IUT and to the test system.	

6.4.2.2 SwMI initiates SCK to MS

This scenario shows the case where the SwMI provides SCK to an MS without the MS first requesting SCK provision.

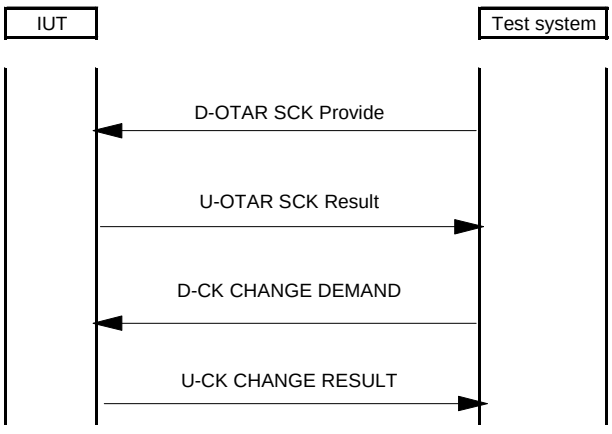

Figure 35: SwMI initiates SCK to MS

Test purpose:

To verify correct operation of MS (IUT) when the SwMI (test system) initiates the delivery of OTAR SCK.

TP/Sec_VD/OTAR/BV/SCK/02	Reference: ETS 300 392-7 [2], subclause 4.4.4.2 Condition: IUT supports OTAR SCK Initial state: IUT registered (see note 1 and note 2) Stimulus: Test system sends D-OTAR SCK Provide PDU. Verify that, after the receipt of D-OTAR SCK Provide PDU, the IUT sends U-OTAR SCK Result PDU. Verify that after receipt of the D-CK CHANGE DEMAND PDU requesting an acknowledgement, the IUT sends a D-CK CHANGE RESULT. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: K is available to both the IUT and to the test system.	

6.4.2.3 SwMI provides an incorrect SCK

The normal message sequence in the case where the SwMI provides an incorrect SCK to MS shall be according to figure 37.

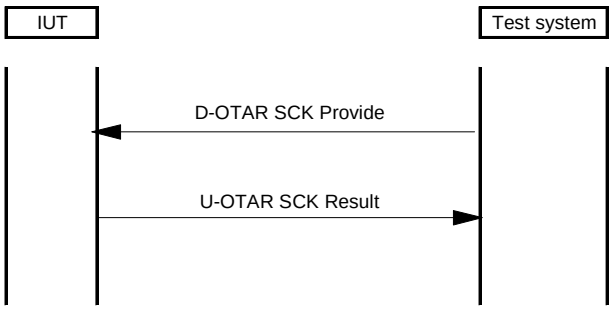

Figure 36: SwMI provides an incorrect SCK

Test purpose:

To verify correct operation of MS (IUT) when the SwMI (test system) provides an incorrect SCK.

TP/Sec_VD/OTAR/BI/SCK/01	Reference: ETS 300 392-7 [2], subclause 4.4.4.2 Condition: IUT supports OTAR SCK. Initial state: IUT registered (see note 1 and note 2). Stimulus: The test system is made to invoke the sending of D-OTAR SCK Provide PDU. Verify that, the IUT sends a U-OTAR SCK Result PDU including the provision result "incorrect KN" after receipt of D-OTAR SCK Provide PDU containing an invalid SCK. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: K is available to both the IUT and to the test system.	

6.4.3 OTAR protocol functions GCK

Test group objective:

To test the OTAR GCK capabilities of the IUT. This test group shall test all OTAR scenarios described in ETS 300 392-7 [2], clause 4, for GCK delivery for each of terminal initiated and SwMI initiated transfers.

6.4.3.1 MS requests provision of GCK

This scenario shows the case where the MS requests provision of a GCK for a group. The MS may initiate this procedure at any time.

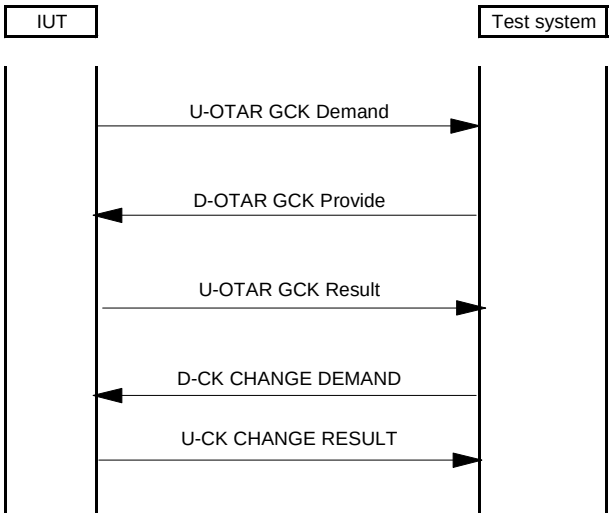

Figure 37: GCK delivery initiated by MS

Test purpose:

To verify correct operation of MS (IUT) when it requests the provision of OTAR GCK.

TP/Sec_VD/OTAR/BV/GCK/01	Reference: ETS 300 392-7 [2], subclause 4.4.5.1 Condition: IUT supports OTAR GCK Initial state: IUT registered and authenticated (see note 1 and note 2). Stimulus: IUT sends U-OTAR GCK Demand PDU. IUT sends U-OTAR GCK Demand PDU. Verify that, after receipt of D–OTAR GCK Provide PDU, the IUT sends U-OTAR GCK Result PDU. Verify that after receipt of the D-CK CHANGE DEMAND PDU requesting an acknowledgement, the IUT sends a D-CK CHANGE RESULT. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.3.2 SwMI provides GCK to MS

This scenario in figure 39 shows the case where the SwMI provides a GCK to an MS without the MS first requesting GCK provision.

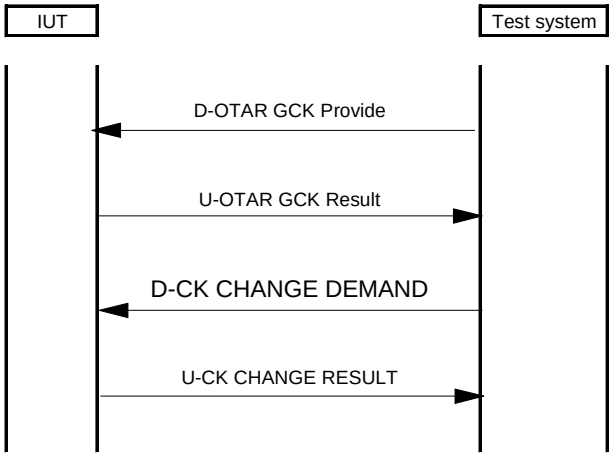

Figure 38: GCK delivery initiated by SwMI

Test purpose:

To verify correct operation of MS (IUT) when the SwMI (test system) initiate the provision of OTAR GCK.

TP/Sec_VD/OTAR/BV/GCK/02	Reference: ETS 300 392-7 [2], subclause 4.4.5.2 Condition: IUT supports OTAR GCK Initial state: IUT registered and authenticated (see note 1 and note 2). Stimulus: Test system sends U-OTAR GCK Provide PDU. Verify that, after receipt of D-OTAR GCK Provide PDU, the IUT sends U–OTAR GCK Result PDU. Verify that after receipt of the D-CK CHANGE DEMAND PDU requesting an acknowledgement, the IUT sends a D-CK CHANGE RESULT. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.3.3 SwMI unable to provide GCK requested by MS

This scenario shows the case where the MS requests provision of one GCK in use on a system and the SwMI is unable to provide it.

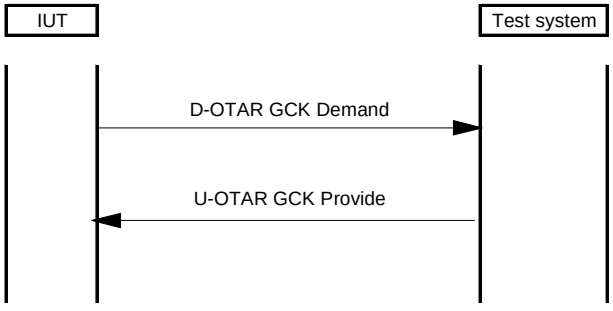

Figure 39: SwMI unable to provide GCK requested by MS

Test purpose:

To verify correct operation of MS (IUT) when IUT initiates the provision of one OTAR GCK and when SwMI (test system) is unable to provide it.

TP/Sec_VD/OTAR/BI/GCK/01	Reference: ETS 300 392-7 [2], subclause 4.4.5.1 Condition: IUT supports OTAR GCK Initial state: IUT registered. IUT authenticated (see note 1 and note 2). Stimulus: The IUT is made to invoke a GCK demand. IUT sends U-OTAR GCK Demand PDU. Verify that after receipt of D–OTAR GCK Provide PDU that does not include any GCK, the IUT does not send the U-OTAR GCK Result PDU. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.4.3.4 SwMI provides an incorrect GCK to MS

The normal message sequence for the layer 3 in the case where the SwMI provides an incorrect GCK to MS shall be according to figure 41.

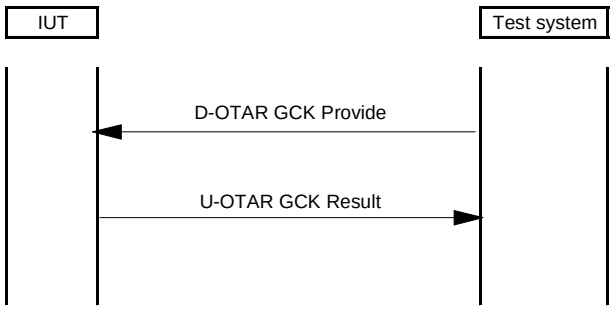

Figure 40: SwMI provides an incorrect GCK to MS

Test purpose:

To verify correct operation of MS (IUT) when the SwMI (test system) provides an incorrect GCK.

TP/Sec_VD/OTAR/BI/GCK/02	Reference: ETS 300 392-7 [2], subclause 4.4.5.2 Condition: IUT supports OTAR GCK. Initial state: IUT registered, IUT authenticated (see note 1 and note 2). Stimulus: The test system sends a D-OTAR GCK Provide PDU. Verify that, the IUT sends a U-OTAR GCK Result PDU including the provision result "incorrect KN" after receipt of D-OTAR GCK Provide PDU containing an invalid GCK. The CMCE step Check_Encryption is executed to confirm that encryption state is maintained (see subclause 6.1.1).
NOTE 1: The encryption parameters established at registration shall be maintained. NOTE 2: DCK is available to both the IUT and to the test system.	

6.5 Enable and Disable

Test group objective:

To test the enable and disable capabilities and protocol of the IUT. This group shall test all scenarios described in ETS 300 392-7 [2], subclause 5.4.

NOTE 1: In testing it is suggested that permanent disabling is performed as the final test, otherwise further testing may be invalid pending repair of the IUT.

NOTE 2: The variant of enable/disable (temporary or permanent, ITSI or TEI or both) is indicated in the DISABLE Intent PDU and test cases will be selected from declarations made in the PICS and PIXIT (see ETS 300 394-5-1 [7] and ETS 300 394-5-3 [8]).

6.5.1 Disable procedures

Test group objective:

To test the disable capabilities and protocol of the IUT.

6.5.1.1 Disable with mutual authentication

This scenario shows the case where the SwMI disables the equipment and/or the subscriber temporarily or permanently with mutual authentication.

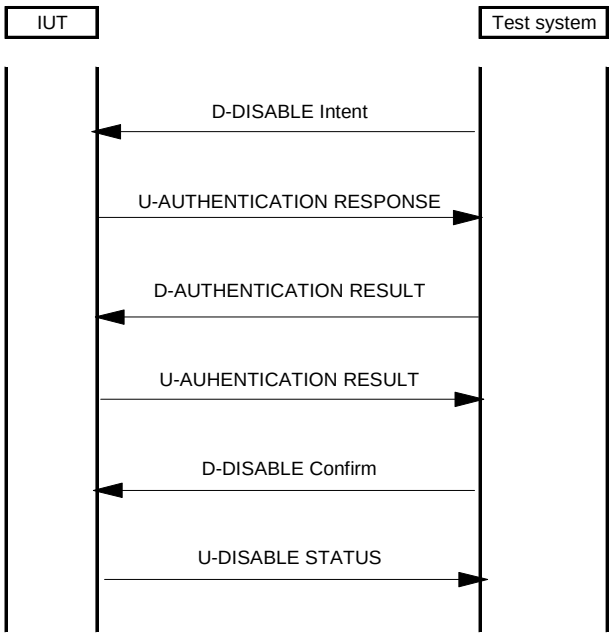

Figure 41: Disabling with mutual authentication

TP/Sec_VD/SED/TD/01	Reference: ETS 300 392-7 [2], subclause 5.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by IUT and disable TEI temporarily Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **temporarily** disable the **equipment** with authentication. Verify that after receipt of the D-DISABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D–DISABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. The CMCE step Check_Temporary_Disable is executed to confirm that IUT is temporarily disable (see subclause 6.1.4).

TP/Sec_VD/SED/TD/02	Reference: ETS 300 392-7 [2], subclause 5.4.3.1 Condition: IUT supports authentication by SwMI made mutual by IUT and disable temporarily ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **temporarily** disable the **subscriber** with authentication. Verify that after receipt of the D-DISABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D–DISABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. The CMCE step Check_Temporary_Disable is executed to confirm that IUT is temporarily disable (see subclause 6.1.4).

TP/Sec_VD/SED/TD/03	Reference: ETS 300 392-7 [2], subclause 5.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by IUT and disable temporarily TEI and disable temporarily ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **temporarily** disable the **equipment and the subscriber** with authentication. Verify that after receipt of the D-DISABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D–DISABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. The CMCE step Check_Temporary_Disable is executed to confirm that IUT is temporarily disable (see subclause 6.1.4).

TP/Sec_VD/SED/PD/01	Reference: ETS 300 392-7 [2], subclause 5.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by IUT and disable permanently TEI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **permanently** disable the **equipment** with authentication. Verify that after receipt of the D-DISABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D–DISABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. The CMCE step Check_Permanent_Disable is executed to confirm that IUT is permanently disable (see subclause 6.1.3).

TP/Sec_VD/SED/PD/02	Reference: ETS 300 392-7 [2], subclause 5.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by IUT and disable permanently ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **permanently** disable the **subscriber** with authentication. Verify that after receipt of the D-DISABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D–DISABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. The CMCE step Check_Permanent_Disable is executed to confirm that IUT is permanently disable (see subclause 6.1.3).

TP/Sec_VD/SED/PD/03	Reference: ETS 300 392-7 [2], subclause 5.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by IUT and disable permanently TEI and disable permanently ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **permanently** disable the **equipment and the subscriber** with authentication. Verify that after receipt of the D-DISABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D-DISABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. The CMCE step Check_Permanent_Disable is executed to confirm that IUT is permanently disable (see subclause 6.1.3).

6.5.1.2 Disable without authentication

This scenario in figure 44 shows the case where the SwMI disables the equipment and/or the subscriber temporarily or permanently without authentication.

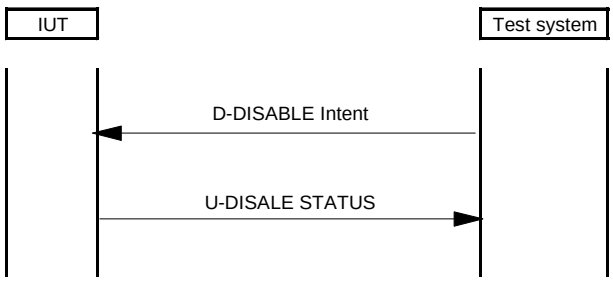

Figure 42: Disabling without authentication

TP/Sec_VD/SED/TD/04	Reference: ETS 300 392-7 [2], subclause 5.4.5 Condition: IUT supports disable temporarily TEI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **temporarily** disable the **equipment** without authentication. Verify that after receipt of the D-DISABLE Intent PDU, the IUT sends back the U-DISABLE STATUS PDU. The CMCE step Check_Temporary_Disable is executed to confirm that IUT is temporarily disable (see subclause 6.1.4).

TP/Sec_VD/SED/TD/05	Reference: ETS 300 392-7 [2], subclause 5.4.5 Condition: IUT supports disable temporarily ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **temporarily** disable the **subscriber** without authentication. Verify that after receipt of the D-DISABLE Intent PDU, the IUT sends back the U-DISABLE STATUS PDU. The CMCE step Check_Temporary_Disable is executed to confirm that IUT is temporarily disable (see subclause 6.1.4).

TP/Sec_VD/SED/TD/06	Reference: ETS 300 392-7 [2], subclause 5.4.5 Condition: IUT supports disable temporarily TEI and ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **temporarily** disable the **subscriber and equipment** without authentication. Verify that after receipt of the D-DISABLE Intent PDU, the IUT sends back the U-DISABLE STATUS PDU. The CMCE step Check_Temporary_Disable is executed to confirm that IUT is temporarily disable (see subclause 6.1.4).

TP/Sec_VD/SED/PD/04	Reference: ETS 300 392-7 [2], subclause 5.4.5 Condition: IUT supports disable permanently TEI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **permanently** disable the **equipment** without authentication. Verify that after receipt of the D-DISABLE Intent PDU, the IUT sends back the U-DISABLE STATUS PDU. The CMCE step Check_Permanent_Disable is executed to confirm that IUT is permanently disable (see subclause 6.1.3).

TP/Sec_VD/SED/PD/05	Reference: ETS 300 392-7 [2], subclause 5.4.5 Condition: IUT supports disable permanently ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **permanently** disable the **subscriber** without authentication. Verify that after receipt of the D-DISABLE Intent PDU, the IUT sends back the U-DISABLE STATUS PDU. The CMCE step Check_Permanent_Disable is executed to confirm that IUT is permanently disable (see subclause 6.1.3).

TP/Sec_VD/SED/PD/06	Reference: ETS 300 392-7 [2], subclause 5.4.5 Condition: IUT supports disable permanently TEI and ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE PDU to **permanently** disable the **subscriber and equipment** without authentication. Verify that after receipt of the D-DISABLE Intent PDU, the IUT sends back the U-DISABLE STATUS PDU. The CMCE step Check_Permanent_Disable is executed to confirm that IUT is permanently disable (see subclause 6.1.3).

6.5.1.3 Disable failure

This scenario shows the case where the SwMI disables the equipment and/or the subscriber temporarily or permanently and the MS rejects the disabling request.

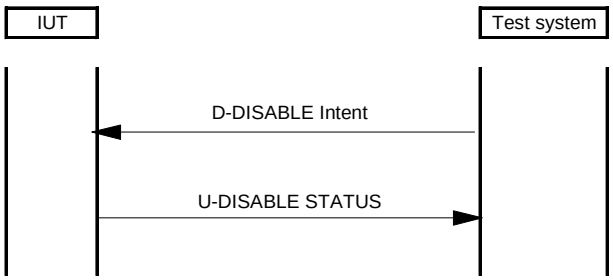

Figure 43: Disable failure

Test purpose:

To verify correct operation of MS (IUT) when the disabling request initiated by the SwMI (test system) is rejected by the IUT. ETS 300 394-5-3 [8] provides test cases for all valid error conditions described in ETS 300 392-7 [2].

TP/Sec_VD/ SED/BI/01	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports disable temporarily TEI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **temporarily** disable the **equipment** with an invalid TEI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for disabling failure. The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/SED/BI/02	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports disable temporarily ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **temporarily** disable the **subscriber** with an invalid ITSI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for disabling failure. The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/SED/BI/03	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports disable temporarily TEI and ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **temporarily** disable the **subscriber and the equipment** with invalid TEI and ITSI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for disabling failure. The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/SED/BI/04	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports disable permanently TEI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **permanently** disable the **equipment** with an invalid TEI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for disabling failure. The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/SED/BI/05	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports disable permanently ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **permanently** disable the **subscriber** with an invalid ITSI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for disabling failure. The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/SED/BI/06	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports disable permanently TEI and ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **permanently** disable the **subscriber and the equipment** with invalid TEI and ITSI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for disabling failure. The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/ SED/BI/07	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by MS and disable temporarily TEI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **temporarily** disable the **equipment** without authentication. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating "authentication is required". The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/ SED/BI/08	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by MS and disable temporarily ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **temporarily** disable the **subscriber** without authentication. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating "authentication is required". The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/ SED/BI/09	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by MS and disable temporarily TEI and disable permanently ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **temporarily** disable the **equipment** and the subscriber without authentication. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating "authentication is required". The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/ SED/BI/10	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by MS and disable permanently TEI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **permanently** disable the **equipment** without authentication. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating "authentication is required". The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/ SED/BI/11	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by MS and disable permanently ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **permanently** disable the **subscriber** without authentication. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating "authentication is required". The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/ SED/BI/12	Reference: ETS 300 392-7 [2], subclause 4.4.3.1 Condition: IUT supports authentication initiated by SwMI made mutual by MS and disable permanently TEI and disable permanently ITSI Initial state: IUT registered Stimulus: Test system sends D-DISABLE Intent PDU to **permanently** disable the **equipment** and the subscriber without authentication. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating "authentication is required". The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

6.5.2 Enable procedures

Test group objective:

To test the enable capabilities and protocol of the IUT.

6.5.2.1 Enable with mutual authentication

This scenario shows the case where the SwMI enables the equipment and/or the subscriber with mutual authentication.

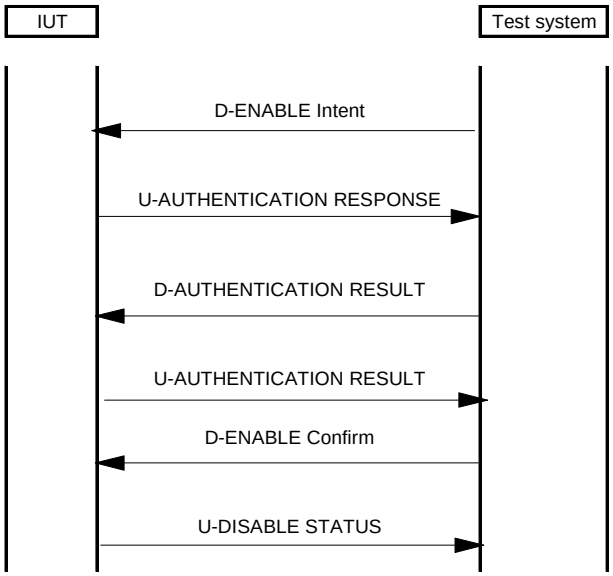

Figure 44: Enabling scenario with mutual authentication

TP/Sec_VD/SED/BV/EN/01	Reference: ETS 300 392-7 [2], subclause 5.4.3.2 Condition: IUT supports authentication initiated by SwMI made mutual by the IUT and enable TEI Initial state: IUT registered, equipment temporarily disabled. Stimulus: Test system sends D-ENABLE Intent PDU to enable the **equipment**. Verify that after receipt of the D-ENABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D–ENABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. A CMCE test is done to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/SED/BV/EN/02	Reference: ETS 300 392-7 [2], subclause 5.4.3.2 Condition: IUT supports authentication initiated by SwMI made mutual by the IUT and enable ITSI Initial state: IUT registered, subscriber temporarily disabled. Stimulus: Test system sends D-ENABLE Intent PDU to enable the **subscriber**. Verify that after receipt of the D-ENABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D–ENABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. A CMCE test is done to confirm that IUT is enabled (see subclause 6.1.2).

TP/Sec_VD/SED/BV/EN/03	Reference: ETS 300 392-7 [2], subclause 5.4.3.2 Condition: IUT supports authentication initiated by SwMI made mutual by the IUT and enable TEI and ITSI Initial state: IUT registered, subscriber and equipment temporarily disabled. Stimulus: Test system sends D-ENABLE Intent PDU to enable the **subscriber and equipment**. Verify that after receipt of the D-ENABLE intent PDU containing an authentication challenge, the IUT sends back a U-AUTHENTICATION RESPONSE containing a mutual authentication challenge. Then after receipt of a D-AUTHENTICATION RESULT with R2 = TRUE, verify that the IUT sends U-AUTHENTICATION RESULT. Then after receipt of D–ENABLE Confirm PDU, verify that the IUT sends U-DISABLE STATUS PDU. A CMCE test is done to confirm that IUT is enabled (see subclause 6.1.2).

6.5.2.2 Enable without authentication

This scenario shows the case where the SwMI enables the equipment and/or the subscriber without authentication.

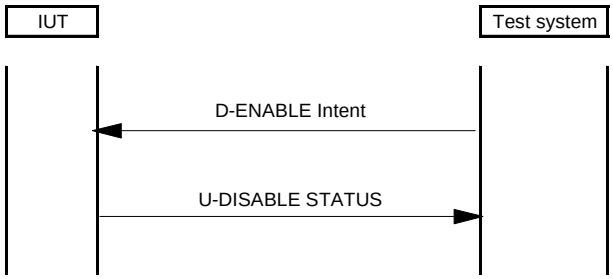

Figure 45: Enabling scenario without authentication

TP/SEC_VD/SED/BV/EN/04	Reference: ETS 300 392-7 [2], subclause 5.4.4 Condition: IUT supports enable TEI Initial state: registered, equipment temporarily disabled Stimulus: Test system sends D-ENABLE Intent PDU to enable the **equipment**. Verify that after receipt of the D-ENABLE Intent PDU, the IUT sends the U–DISABLE STATUS PDU. A CMCE test is done to confirm that IUT is enabled (see subclause 6.1.2).

TP/SEC_VD/SED/BV/EN/05	Reference: ETS 300 392-7 [2], subclause 5.4.4 Condition: IUT supports enable ITSI Initial state: registered, **subscriber** temporarily disabled Stimulus: Test system sends D-ENABLE Intent PDU to enable the subscriber. Verify that after receipt of the D-ENABLE Intent PDU, the IUT sends the U–DISABLE STATUS PDU. A CMCE test is done to confirm that IUT is enabled (see subclause 6.1.2).

TP/SEC_VD/SED/BV/EN/06	Reference: ETS 300 392-7 [2], subclause 5.4.4 Condition: IUT supports enable TEI and ITSI Initial state: registered, equipment and subscriber temporarily disabled Stimulus: Test system sends D-ENABLE Intent PDU to enable the **equipment and the subscriber**. Verify that after receipt of the D-ENABLE Intent PDU, the IUT sends the U–DISABLE STATUS PDU. The CMCE step Check_Enable is executed to confirm that IUT is enabled (see subclause 6.1.2).

6.5.2.3 Enable failure

This scenario shows the case where the SwMI disables the equipment and/or the subscriber temporarily or permanently and the MS rejects the disabling request.

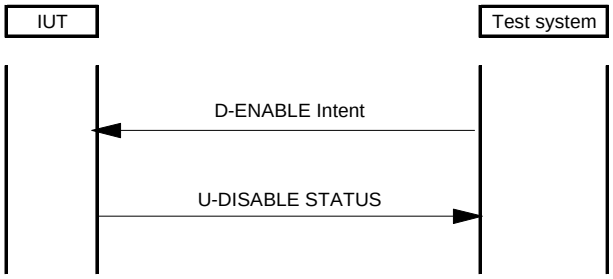

Figure 46: Enable failure

Test purpose:

To verify correct operation of MS (IUT) when the disabling request initiated by the SwMI (test system) is rejected by the IUT. ETS 300 394-5-3 [8] provides test cases for all valid error conditions described in ETS 300 392-7 [2].

TP/Sec_VD/ SED/BI/13	Reference: ETS 300 392-7 [2], subclause 4.4.3.2 Condition: IUT supports enable TEI Initial state: IUT registered, temporarily disable Stimulus: Test system sends D-ENABLE Intent PDU to enable the **equipment** with an invalid TEI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for enabling failure. A CMCE test is done to confirm that IUT is temporarily disabled (see subclause 6.1.2).

TP/Sec_VD/SED/BI/14	Reference: ETS 300 392-7 [2], subclause 4.4.3.2 Condition: IUT supports enable ITSI Initial state: IUT registered temporarily disable Stimulus: Test system sends D-ENABLE Intent PDU to enable the **subscriber** with an invalid ITSI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for enabling failure. A CMCE test is done to confirm that IUT is temporarily disabled (see subclause 6.1.2).

TP/Sec_VD/SED/BI/15	Reference: ETS 300 392-7 [2], subclause 4.4.3.2 Condition: IUT supports enable temporarily TEI and ITSI Initial state: IUT registered, temporarily disable Stimulus: Test system sends D-ENABLE Intent PDU to enable the **subscriber and the equipment** with invalid TEI and ITSI. Verify that, IUT sends U-DISABLE STATUS PDU with the enable/disable result element indicating the reason for enabling failure. A CMCE test is done to confirm that IUT is temporarily disabled (see subclause 6.1.2).

6.6 Mobility management for Air Interface Encryption

Test group objective:

To check that at initial cell selection, the MS registers and establish the security parameters advised in the cell broadcast.

6.6.1 MS registration at initial class 1 cell selection

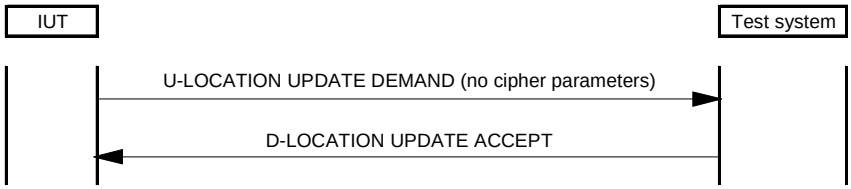

Figure 47: Initial class 1 cell selection

Test purpose:

To verify correct operation of MS (IUT) when the MS registers at a class 1 cell selection.

TP/Sec_VD/AI/MM/01	Reference: ETS 300 392-7 [2], subclause 6.5.1.1 Condition: IUT supports security class 1 Initial state: Stimulus: The IUT is made to invoke a U-LOCATION UPDATE DEMAND in a class 1 cell selection. Verify that IUT sends a U-LOCATION UPDATE DEMAND PDU without cipher parameters.

6.6.2 MS registration at initial class 2 or 3 cell selection

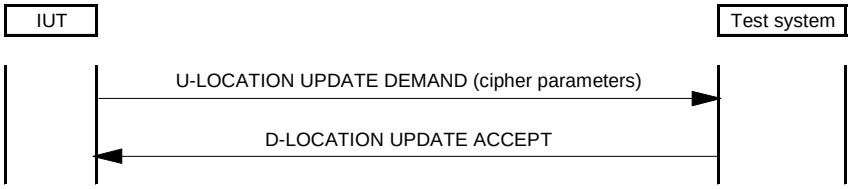

Figure 48: Initial class 2 or 3 cell selection

Test purpose:

To verify correct operation of MS (IUT) when the MS registers at a class 2 cell selection.

TP/Sec_VD/AI/MM/02	Reference: ETS 300 392-7 [2], subclause 6.5.1.1 Condition: IUT supports security class 2 Initial state: Stimulus: The IUT is made to invoke a U-LOCATION UPDATE DEMAND in a class 2 cell selection. Verify that IUT sends a U-LOCATION UPDATE DEMAND PDU with correct cipher parameters.

Test purpose:

To verify correct operation of MS (IUT) when the MS registers at a class 3 cell selection.

TP/Sec_VD/AI/MM/03	Reference: ETS 300 392-7 [2], subclause 6.5.1.1 Condition: IUT supports security class 2 Initial state: Stimulus: The IUT is made to invoke a U-LOCATION UPDATE DEMAND in a class 3 cell selection. Verify that IUT sends a U-LOCATION UPDATE DEMAND PDU with correct cipher parameters.

7 Test purposes for DMO

7.1 Layer 2

Test group objective:

To test the encryption capabilities of the Direct Mode module of the IUT at layer 2.

TP/Sec_DM/L2/01	Reference: ETS 300 396-6 [3], subclause 6.3.2.1.1 Condition: IUT supports the encryption mode 01. Initial state: Stimulus: IUT initiates a CM or SDS call. Check that the DMAC-SYNC PDU containing the DM-SETUP or DM–SETUP PRES or DM-SDS DATA or DM-SDS UDATA is sent encrypted.

TP/Sec_DM/L2/02	Reference: ETS 300 396-6 [3], subclause 6.3.2.1.1 Condition: IUT supports the encryption mode 10. Initial state: Stimulus: IUT initiates a CM or SDS call. Check that the DMAC-SYNC PDU containing the DM-SETUP or DM–SETUP PRES or DM-SDS DATA or DM-SDS UDATA is sent encrypted.

TP/Sec_DM/L2/03	Reference: ETS 300 396-6 [3], subclause 6.3.2.1.1 Condition: IUT supports the encryption mode 11. Initial state: Stimulus: IUT initiates a CM or SDS call. Check that the DMAC-SYNC PDU containing the DM-SETUP or DM–SETUP PRES or DM-SDS DATA or DM-SDS UDATA is sent encrypted.

7.2 Layer 3

NOTE: The layer 3 security protocols in DMO are dependent upon the use of SDS as a transport mechanism and can only be carried out after satisfactory testing of the SDS facility.

7.2.1 OTAR

Test group objective:

To test the OTAR capabilities and protocol of the Direct Mode module of the IUT. This test group shall test all OTAR scenarios described in ETS 300 396-6 [3].

Condition: DMO-OTAR entity supported by the IUT.

7.2.1.1 IUT requests SCK

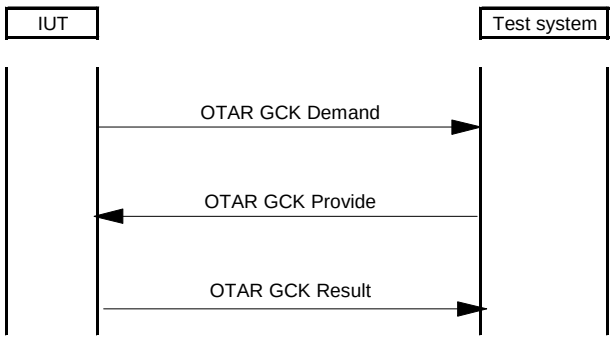

Figure 49: IUT requests provision of SCK

Test purpose:

To verify correct operation of MS (IUT) when requesting SCK.

TP/Sec_DM/L3/OTAR/BV/01	Reference: ETS 300 396-6 [3], subclause 7.5.1 Condition: IUT supports the Key User (KU) role Initial state: SCK unknown to IUT Stimulus: IUT sends the OTAR SCK Demand PDU. IUT sends an OTAR SCK Demand PDU. Verify that, after receipt of the OTAR SCK Provide PDU, the IUT sends the OTAR SCK Result PDU with provision result set to "sealed key accepted".

7.2.1.2 IUT provides SCK

This scenario shows the case when the IUT is requested to provide the SCK, i.e. the IUT acts as a Key Holder (KH) and the test system acts as a KU or as a Key Generator (KG).

7.2.1.2.1 MS as a KH provides SCK to the KU

This scenario shows the case when the IUT acts as a KH and the test system acts as a KU.

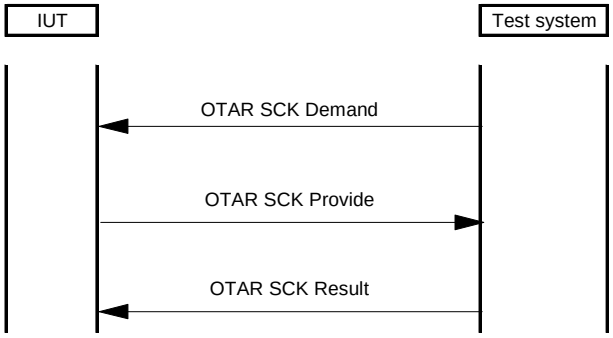

Figure 50: MS as a KH provides SCK to KU

Test purpose:

To verify normal operation of the IUT when requested by test system to provide the SCK, when the IUT acts as a KH and test system acts as a KU.

TP/Sec_DM/L3/OTAR/BV/02	Reference: ETS 300 396-6 [3], subclause 7.5.2 Condition: IUT supports the KH role Initial state: Stimulus: Test system sends the OTAR SCK Demand PDU. Test system request key from IUT acting as a key holder (as a relay for the KG). Verify that after receipt of the OTAR SCK Demand PDU, the IUT sends the OTAR SCK Provide PDU containing the requested SCK.

7.2.1.2.2 IUT as a KH requests SCK to KG

This scenario shows the case when the IUT acts as a KH and the test system acts as a KG.

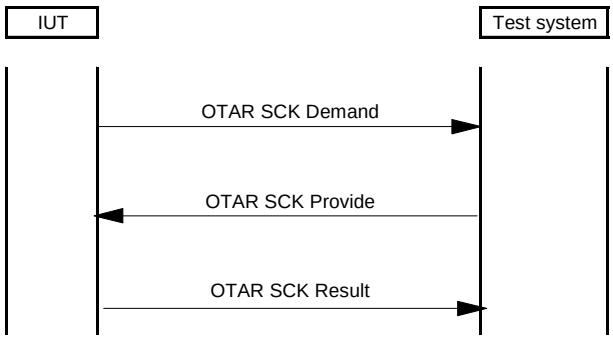

Figure 51: IUT acts as a key holder, test system as a KG

Test purpose:

To verify normal operation of the IUT as a KH when requesting provision of SCK to the test system (KG).

TP/Sec_DM/L3/OTAR/BV/03	Reference: ETS 300 396-6 [3], subclause 7.5.2 Condition: IUT supports the KH role Initial state: IUT does not have the SCK for the requested SCKN Stimulus: IUT sends the OTAR SCK Demand PDU. Test system request key from IUT acting as a key holder (as a relay for KG). Verify that after receipt of the OTAR SCK Provide PDU, the IUT sends OTAR SCK Result PDU with provision result set to "sealed key accepted". Verify that each PDU includes the ITSI of the KU.

7.2.1.3 KH distributing SCK unsolicited

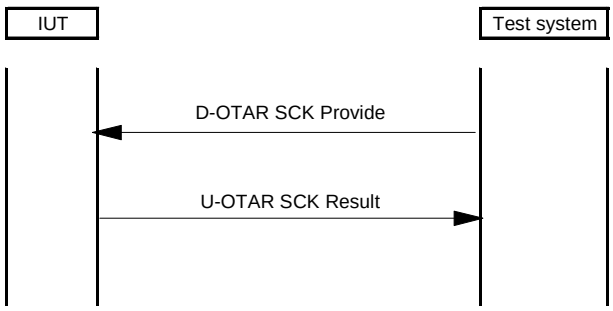

Figure 52: Test system initiates provision of SCK

Test purpose:

To verify normal operation of the IUT when test system initiates the provision of SCK.

TP/Sec_DM/L3/OTAR/BV/04	Reference: ETS 300 396-6 [3], subclause 7.5.3 Condition: IUT supports the KU role Initial state: SCK unknown to IUT Stimulus: Test system sends the OTAR SCK Provide PDU. Test system initiates provision of SCK Verify that after receipt of the OTAR SCK Provide PDU, the IUT sends the OTAR SCK Result PDU with provision result set to "sealed key accepted".

7.2.1.4 Error scenario with SDS time-out from KH

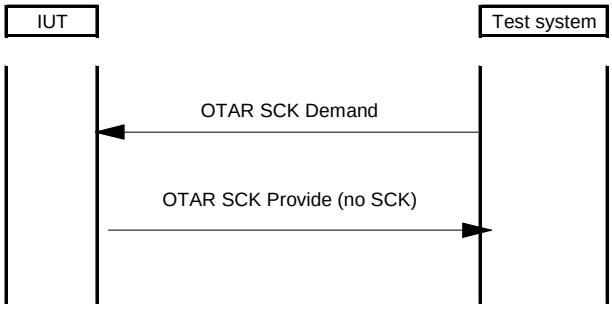

Figure 53: Error scenario with SDS time-out from KH (IUT)

Test purpose:

To verify normal operation of the IUT when acting as a KH when KG is unavailable.

TP/Sec_DM/L3/OTAR/BI/01	Reference: ETS 300 396-6 [3], subclause 7.5.4 Condition: IUT supports the KH role and IUT does not have the SCK for the requested SCKN. The KG is unavailable. Initial state: Stimulus: Test system sends the OTAR SCK Provide PDU. IUT acts as a KH when KG is unavailable Verify that after receipt of the OTAR SCK Demand PDU and after time-out of the timer T316, the IUT sends OTAR SCK Provide PDU containing no SCK and the result reason "Key sealer unavailable".

7.2.1.5 KG provides an incorrect SCKN

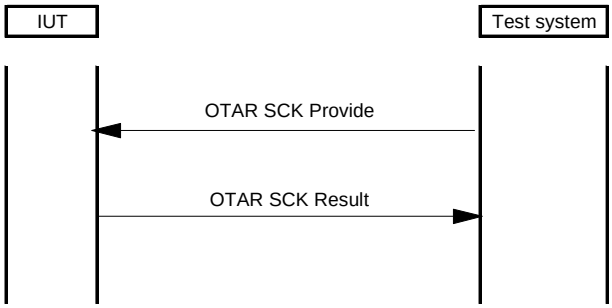

Figure 54: KG (test system) provides an incorrect SCK to MS

Test purpose:

To verify correct operation of MS (IUT) when KG (test system) provides an incorrect SCKN.

TP/Sec_DM/L3/OTAR/BI/02	Reference: ETS 300 396-6 [3], subclause 7.5.1 Condition: IUT supports the KU role Initial state: SCK unknown to IUT Stimulus: Test system sends the OTAR SCK Provide PDU. Verify that after receipt of the OTAR SCK Provide PDU containing an incorrect SCKN, the IUT sends the OTAR SCK Result PDU including result "incorrect SCKN".

TP/Sec_DM/L3/OTAR/BI/03	Reference: ETS 300 396-6 [3], subclause 7.5.1 Condition: IUT supports the KU role Initial state: SCK unknown to IUT Stimulus: Test system sends the OTAR SCK Provide PDU. Verify that after receipt of the OTAR SCK Provide PDU containing an incorrect SCK-VN, the IUT sends the OTAR SCK Result PDU including the result "incorrect SCK-VN".

7.2.2 Enable and disable

Test group objective:

To test the enable and disable capabilities and protocol of the IUT. This test group shall test all scenarios described in ETS 300 396-6 [3].

NOTE 1: All scenarios described in ETS 300 396-6 [3] follow the same generic protocol sequence with the content of the command PDU defining the particular operation and test.

NOTE 2: In testing it is suggested that permanent disabling is performed as the final test, otherwise further testing may be invalid pending repair of the IUT.

Condition: IUT supports secure enable/disable procedures.

7.2.2.1 Disable

7.2.2.1.1 MS supports the target role

This scenario shows the case where the test system disables the equipment and/or the subscriber.

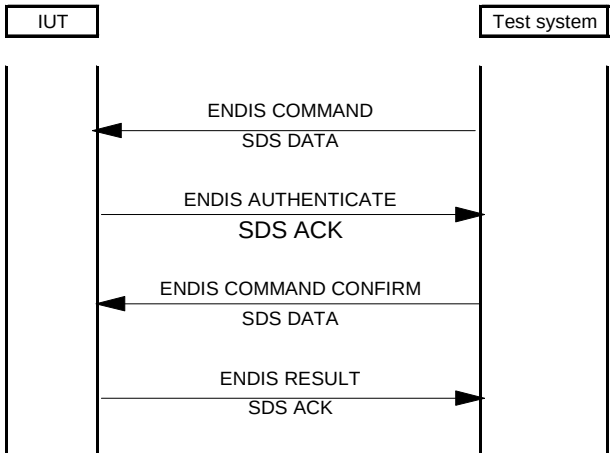

Figure 55: Disable procedure - IUT supports the target role

Test purpose:

To verify correct operation of MS (IUT) during the disabling procedure.

TP/Sec_DM/L3/SED/BV/TD/TAR/01	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the target role. Initial state: Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to **temporarily** disable the **equipment**, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

TP/Sec_DM/L3/SED/BV/TD/TAR/02	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the target role. Initial state: Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to **temporarily** disable the **subscribe**r, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

TP/Sec_DM/L3/SED/BV/TD/TAR/03	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the target role. Initial state: Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to **temporarily** disable the **equipment and subscriber**, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

TP/Sec_DM/L3/SED/BV/PD/TAR/01	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the target role. Initial state: Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to **permanently** disable the **equipment**, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

TP/Sec_DM/L3/SED/BV/PD/TAR/02	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the target role. Initial state: Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to **permanently** disable the **subscribe**r, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

TP/Sec_DM/L3/SED/BV/PD/TAR/03	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the target role. Initial state: Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to **permanently** disable the **equipment and subscriber**, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

7.2.2.1.2 MS supports the manager role

This scenario shows the case where the IUT disables the equipment and/or the subscriber.

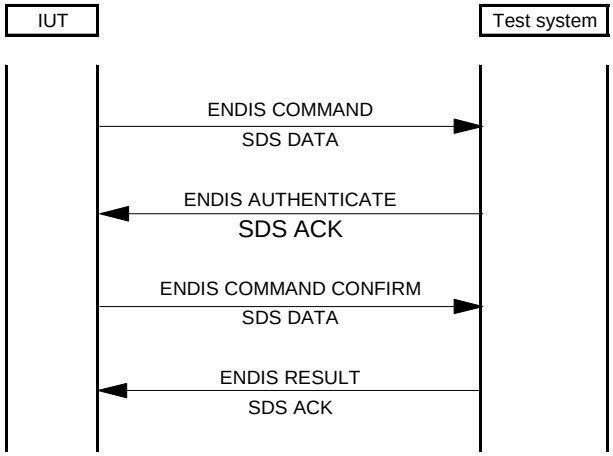

Figure 56: Disable procedure - IUT support the manager role

TP/Sec_DM/L3/SED/BV/TD/MNG/01	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the manager role. Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to **temporarily** disable the **equipment**. Verify that after receipt of the ENDIS AUTHENTICATE PDU, IUT sends the ENDIS COMMAND CONFIRM PDU.

TP/Sec_DM/L3/SED/BV/TD/MNG/02	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the manager role. Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to **temporarily** disable the **subscriber**. Verify that after receipt of the ENDIS AUTHENTICATE PDU, IUT sends the ENDIS COMMAND CONFIRM PDU.

TP/Sec_DM/L3/SED/BV/TD/MNG/03	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the manager role. Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to **temporarily** disable the **equipment and subscriber**. Verify that after receipt of the ENDIS AUTHENTICATE PDU, IUT sends the ENDIS COMMAND CONFIRM PDU.

TP/Sec_DM/L3/SED/BV/PD/MNG/01	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the manager role. Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to **permanently** disable the **equipment**. Verify that after receipt of the ENDIS AUTHENTICATE PDU, IUT sends the ENDIS COMMAND CONFIRM PDU.

TP/Sec_DM/L3/SED/BV/PD/MNG/02	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the manager role. Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to **permanently** disable the **subscriber**. Verify that after receipt of the ENDIS AUTHENTICATE PDU, IUT sends the ENDIS COMMAND CONFIRM PDU.

TP/Sec_DM/L3/SED/BV/PD/MNG/03	Reference: ETS 300 396-6 [3], subclause 8.7.3.1 Condition: IUT supports the manager role. Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to **permanently** disable the **equipment and subscriber**. Verify that after receipt of the ENDIS AUTHENTICATE PDU, IUT sends the ENDIS COMMAND CONFIRM PDU.

7.2.2.2 Enable

7.2.2.2.1 MS support the target role

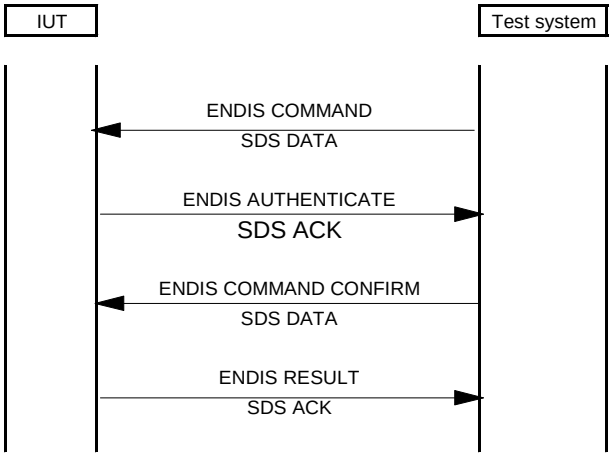

Figure 57: Enable procedure

Test purpose:

To verify the correct operation of the enabling equipment procedure.

TP/Sec_DM/L3/SED/BV/EN/TAR/01	Reference: ETS 300 396-6 [3], subclause 8.7.3.2 Condition: IUT supports the target role Initial state: equipment is in a temporarily disabled state. Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to enable the equipment, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

TP/Sec_DM/L3/SED/BV/EN/TAR/02	Reference: ETS 300 396-6 [3], subclause 8.7.3.2 Condition: IUT supports the target role Initial state: subscriber is in a temporarily disabled state. Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to enable the subscriber, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

TP/Sec_DM/L3/SED/BV/EN/TAR/03	Reference: ETS 300 396-6 [3], subclause 8.7.3.2 Condition: IUT supports the target role Initial state: IUT is in a temporarily disabled state. Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request to enable the equipment or subscriber, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS RESULT PDU with correct Equipment status, Subscription status and Enable/Disable result.

7.2.2.2.2 MS support the manager role

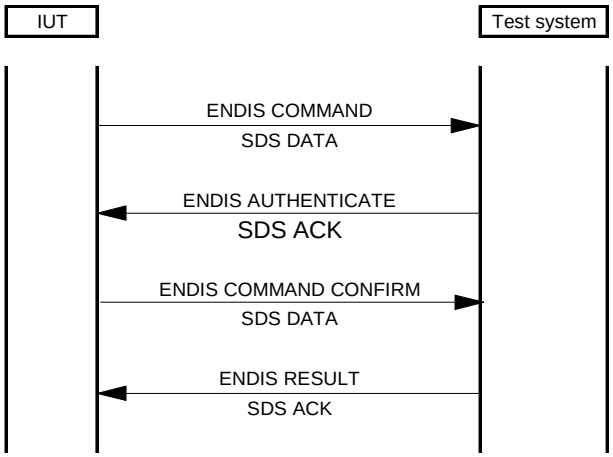

Figure 58: Enable procedure

Test purpose:

To verify the correct operation of the enabling equipment procedure.

TP/Sec_DM/L3/SED/BV/EN/MNG/01	Reference: ETS 300 396-6 [3], subclause 8.7.3.2 Condition: IUT supports the manager role Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to enable the equipment. Verify that, after receipt of ENDIS AUTHENTICATE PDU the IUT sends ENDIS COMMAND CONFIRM PDU.

TP/Sec_DM/L3/SED/BV/EN/MNG/02	Reference: ETS 300 396-6 [3], subclause 8.7.3.2 Condition: IUT supports the manager role Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to enable the subscriber. Verify that, after receipt of ENDIS AUTHENTICATE PDU the IUT sends ENDIS COMMAND CONFIRM PDU.

TP/Sec_DM/L3/SED/BV/EN/MNG/03	Reference: ETS 300 396-6 [3], subclause 8.7.3.2 Condition: IUT supports the manager role Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request to enable the equipment or subscriber. Verify that, after receipt of ENDIS AUTHENTICATE PDU the IUT sends ENDIS COMMAND CONFIRM PDU.

7.2.2.3 TEI delivery

Test purpose:

To verify the correct operation of the TEI request and delivery procedure.

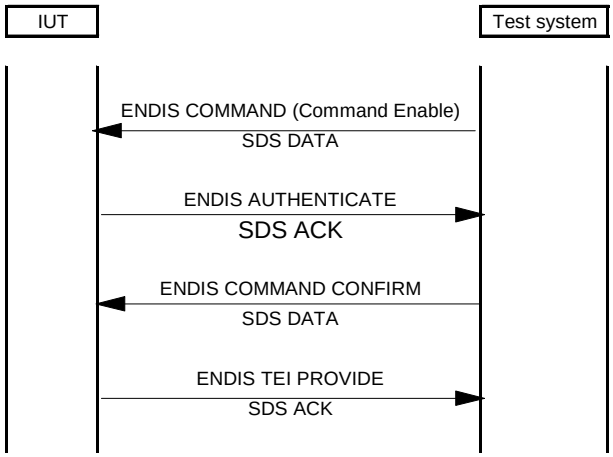

Figure 59: TEI delivery procedure

TP/Sec_DM/L3/SED/BV/TEI/01	Reference: ETS 300 396-6 [3], subclause 8.7.3.3 Condition: IUT supports the ENDIS procedures of the equipment, IUT supports the target role Initial state: Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a request for the IUT to deliver the TEI, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU, verify that IUT sends the ENDIS TEI PROVIDE PDU with the correct TEI.

TP/Sec_DM/L3/SED/BV/TEI/02	Reference: ETS 300 396-6 [3], subclause 8.7.3.3 Condition: IUT supports the ENDIS procedures of the equipment, IUT supports the manager role Initial state: Stimulus: IUT sends ENDIS COMMAND information element in an SDS-DATA PDU. IUT sends ENDIS COMMAND PDU including a request for the IUT to deliver the TEI. Verify that after receipt of ENDIS AUTHENTICATE PDU, the IUT sends the ENDIS COMMAND CONFIRM PDU.

7.2.2.4 Authentication failure in ENDIS exchange

Test purpose:

To verify the correct operation of the ENDIS REJECT procedure when the authentication procedure fails.

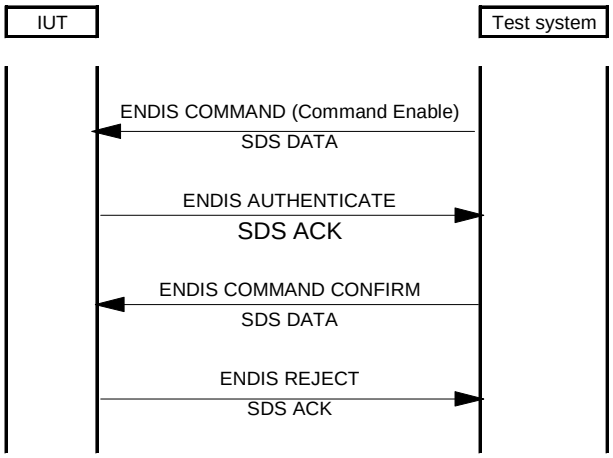

Figure 60: Authentication failure in ENDIS exchange

TP/Sec_DM/L3/SED/BI/REJ/01	Reference: ETS 300 396-6 [3], subclause 8.7.3.5 Condition: IUT supports target role Initial state: Stimulus: Test system sends ENDIS COMMAND information element in an SDS-DATA PDU. Test system sends ENDIS COMMAND PDU including a valid command, verify that IUT sends ENDIS AUTHENTICATE PDU. After receipt of the ENDIS COMMAND CONFIRM PDU containing an incorrect RES2 parameter value, verify that IUT sends the ENDIS REJECT PDU with reason set to indicate authentication error.

History

Document history			
January 1998	Public Enquiry	PE 9822:	1997-01-30 to 1997-05-29
April 1999	Vote	V 9925:	1999-04-20 to 1999-06-18