EUROPEAN TELECOMMUNICATION STANDARD

FINAL DRAFT

pr **ETS 300 393-7**

February 1997

Source: ETSI TC-RES

Reference: DE/RES-06004-7

ICS: 33.020

Key words: TETRA, PDO, SECURITY

Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 7: 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
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

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

Contents

Foreword 5

1 Scope 7

2 Normative references 7

3 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 8

4 Air Interface authentication and key management mechanisms 8
4.1 Air interface authentication mechanisms 8
4.1.1 Overview 8
4.1.2 Authentication of a user 9
4.1.3 Authentication of the infrastructure 10
4.1.4 Mutual authentication of user and infrastructure 11
4.1.5 The authentication key 13
4.1.5.1 Generation of K 13
4.1.6 Equipment authentication 14
4.2 Service Description and Primitives 14
4.2.1 BS Authentication primitives 14
4.2.2 MS Authentication primitives 15
4.3 Definition of Protocols 16
4.3.1 Authentication State Transitions 16
4.3.2 Overview of authentication protocol 17
4.3.2.1 Case 1: RPDI authenticates MS 17
4.3.2.2 Case 2: MS authenticates RPDI 18
4.3.2.3 Case 3: Mutual authentication initiated by RPDI 18
4.3.2.4 Case 4: Mutual authentication initiated by MS 20
4.3.2.5 Case 5: RPDI authenticates MS during registration 21
4.3.2.6 Case 6: MS authenticates RPDI during registration 22
4.3.2.7 Case 7: Mutual authentication initiated by MS during registration 23
4.3.2.8 Case 8: RPDI rejects authentication demand from MS 25
4.3.2.9 Case 9: MS rejects authentication demand from RPDI 26
4.3.3 PDU descriptions 26
4.3.3.1 D-AUTHENTICATION DEMAND 29
4.3.3.2 D-AUTHENTICATION RESPONSE 29
4.3.3.3 D-AUTHENTICATION RESULT 30
4.3.3.4 D-AUTHENTICATION REJECT 30
4.3.3.5 U-AUTHENTICATION DEMAND 30
4.3.3.6 U-AUTHENTICATION RESPONSE 31
4.3.3.7 U-AUTHENTICATION RESULT 31
4.3.3.8 U-AUTHENTICATION REJECT 31
4.3.3.9 U-TEI PROVIDE 32
4.3.4 MM PDU type 3 information elements coding 32
4.3.4.1 Authentication uplink 32
4.3.4.2 Authentication downlink 32
4.3.5 PDU Information elements coding 33
4.3.5.1 Address extension 33
4.3.5.2 Authentication result 33
4.3.5.3 Authentication reject reason 33
4.3.5.4 Mobile country code 33
4.3.5.5 Mobile network code 33
4.3.5.6 Mutual authentication flag 34
4.3.5.7 PDU type 34
4.3.5.8 Proprietary 34

4.3.5.9 Random challenge 34
4.3.5.10 Reject cause 35
4.3.5.11 Random seed 35
4.3.5.12 Response value 35
4.3.5.13 TEI 35
4.3.5.14 TEI information 35
4.3.5.15 TEI request flag 36
4.3.5.16 Type 3 element identifier 36
4.4 Boundary conditions for the cryptographic algorithms and procedures 36
4.5 Dimensioning of the cryptographic parameters 38
4.6 Summary of the cryptographic processes 39

5 Secure Enable and Disable mechanism 39
5.1 General relationships 39
5.2 Mechanisms 40
5.3 Service description and primitives 40
5.4 Definition of enable-disable protocol 41
5.4.1 Enable/Disable state transitions 41
5.4.2 Overview of enable-disable protocol 42
5.4.2.1 Disabling an MS using authentication 43
5.4.2.2 Enabling an MS using authentication 44
5.4.3 MM PDUs structures and contents 45
5.4.3.1 D-DISABLE 46
5.4.3.2 D-ENABLE 46
5.4.3.3 U-DISABLE STATUS 47
5.4.4 MM Information elements coding 47
5.4.4.1 Address extension 47
5.4.4.2 Authentication challenge 47
5.4.4.3 Disabling type 47
5.4.4.4 Enable/disable result 48
5.4.4.5 Equipment disable 48
5.4.4.6 Equipment enable 48
5.4.4.7 Equipment status 48
5.4.4.8 Intent/confirm 49
5.4.4.9 PDU Type 49
5.4.4.10 Proprietary 49
5.4.4.11 Subscription disable 49
5.4.4.12 Subscription enable 49
5.4.4.13 Subscription status 50
5.4.4.14 TETRA equipment identity 50

History 51

Foreword

This final draft European Telecommunication Standard (ETS) has been produced by the Radio Equipment and Systems (RES) Technical Committee of the European Telecommunications Standards Institute (ETSI), and is now submitted for the Vote phase of the ETSI standards approval procedure.

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

Part 1: "General network design".

Part 2: "Air Interface (AI)".

Part 7: "Security".

Part 10: "SDL Model of Air Interface", (DE/TETRA-04004-10).

Part 11: "PICS Proforma", (DE/TETRA-04004-11).

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 describes the security mechanisms in the Trans-European Trunked Radio (TETRA) Packet Data Optimized (PDO) standard. It provides mechanisms for authentication and key management mechanisms for the air interface.

Clause 4 describes the authentication and key management mechanisms for the TETRA air interface. The following two authentication services have been specified for the air-interface in ETR 086-3 [3], based on a threat analysis:

- authentication of a user by the RPDI;

- authentication of the RPDI by a user.

The use of encryption is not described in this ETS but may be provided by the application using TETRA PDO as a transport and network service.

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 300 393-1: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 1: General network design".

[2] ETS 300 393-2: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 2: Air Interface (AI)".

[3] ETR 086-3: "Radio Equipment and Systems (RES); Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".

[4] ISO 7498-2: "Information processing systems - Open Systems Interconnection - Basic reference model - Part 2: Security Architecture".

[5] ETS 300 392-7: "Radio Equipment and Systems (RES); Trans-European Trunked Radio (TETRA); Voice and Data (V+D); Part 7: Security".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this ETS, the following definitions apply:

Authentication Code (AC): A (short) key to be entered by the user into the terminal.

Authentication Key (K): The primary secret, the knowledge of which has to be demonstrated for authentication. On the infrastructure side, it is stored in a secure place of the home network. In the terminal it is generated in one of three ways: 1) the authentication key may be generated from an authentication code AC that is manually entered by the user; 2) the authentication key may be generated from a user authentication key UAK stored in a module (detachable or not); 3) the authentication key may be generated from both the UAK stored in a module and the PIN entered by the user.

Personal Identification Number (PIN): Entered by the user into the terminal and used to generate the authentication Key (K)together with the User Authentication Key (UAK).

Proprietary Algorithm: An algorithm which is the intellectual property of a legal entity.

Random challenge (RAND1, RAND2): A random value generated by the infrastructure to authenticate a user or in a terminal to authenticate the infrastructure, respectively.

Random Seed (RS): A random value used to derive a session authentication key from the authentication key.

Response (RES1, RES2): A value calculated in the terminal from RAND1 and the KS to prove the authenticity of a user to the infrastructure or by the infrastructure from RAND2 and the KS' to prove its authenticity to a user, respectively.

Session Authentication Key (KS, KS'): Generated from the authentication key and a random seed for the authentication of a user. It has a more limited lifetime than the authentication key and can be stored in less secure places and forwarded to visited networks.

Spoofer: An entity attempting to obtain service from or interfere with the operation of the system by impersonation of an authorized system user or system component.

User Authentication Key (UAK): Stored in a (possibly detachable) module within the terminal and used to derive the authentication key (with or without a PIN as an additional parameter).

3.2 Abbreviations

For the purposes of this ETS, the following abbreviations apply.

AC	Authentication code
AI	Air Interface
BS	Base Station
ITSI	Individual TETRA Subscriber Identity
K	Authentication Key
KS	Session authentication Key
LLC	Logical Link Control
MAC	Medium Access Control
MLE	Mobile Link Entity
MM	Mobility Management
MS	Mobile Station
PDU	Protocol Data Unit
PIN	Personal Identification Number
RAND1	Random challenge 1
RAND2	Random challenge 2
RES1	Response 1
RES2	Response 2
RPDI	Radio Packet Data Infrastructure
RS	Random Seed
SAP	Service Access Point
SDU	Service Data Unit
TA	TETRA Algorithm
UAK	User authentication key
XRES1	Expected response 1
XRES2	Expected response 2

4 Air Interface authentication and key management mechanisms

NOTE: The algorithms referred to in this clause may be the same as those defined in ETS 300 392-7 [5] with some outputs ignored.

4.1 Air interface authentication mechanisms

4.1.1 Overview

Authentication is optional, however if it is used it shall be as described in this clause.

The authentication method described is a symmetric secret key type. In this method one secret, the authentication key, shall be shared by each of the authenticating parties, and there should be strictly two parties with knowledge of the secret. Authentication shall be achieved by the parties proving to each other knowledge of the shared secret.

The authenticating parties shall be the authentication centre of the Radio Packet Data Infrastructure (RPDI) and the Mobile Station (MS). The MS is considered, for the purposes of authentication, to represent the user as defined by the Individual TETRA Subscriber Identity (ITSI). At the air interface the Base Station (BS) is assumed to be trusted by the RPDI and the authentication exchange proves knowledge given to the BS by the authentication centre. This knowledge shall be the session authentication key.

Authentication and provision of keys for use at the air-interface shall be linked by the use of a common algorithm set. This algorithm set shall include a means of providing keys for use in group calls. The controlling party in all authentication exchanges shall be the RPDI.

The authentication process describes a 3-pass challenge-response-result protocol.

It is assumed that the intra-system interface linking the BS to the authentication centre is adequately secure.

4.1.2 Authentication of a user

In this subclause, a mechanism is described that shall be used to achieve the authentication of a user of an MS by the RPDI. This shall be done using a challenge response protocol, with a session authentication key derived from an authentication key that shall be shared by the user and the infrastructure. The session authentication key shall be provided by an authentication centre of the home system.

The computation of the session authentication key shall be carried out by an algorithm, TA11. The computation of the response shall be done by another algorithm, TA12P.

The BS shall generate a random number as a challenge RAND1. The MS shall compute a response, RES1, and the BS shall compute an expected response, XRES1. The BS on receipt of RES1 from the MS shall compare it with XRES1. If the values are equal the result R1 shall be set to TRUE, else the result R1 shall be set to FALSE.

The process is summarized in figure 1.

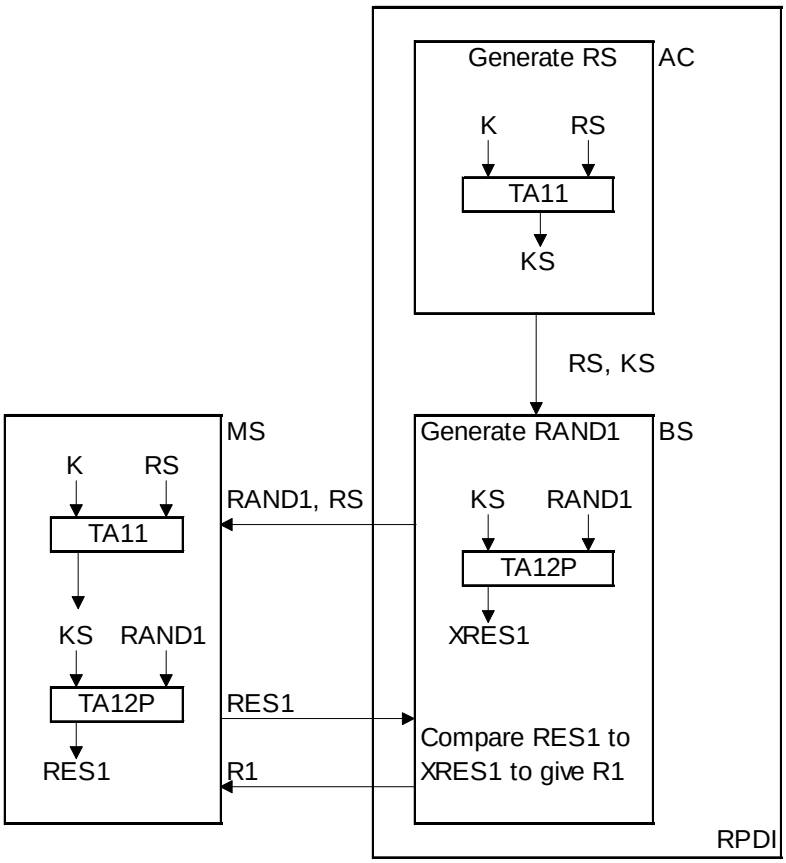


Figure 1: Authentication of a user by the infrastructure

4.1.3 Authentication of the infrastructure

Authentication of the infrastructure by a user shall be carried out in the same way as described in subclause 4.1.2 with the roles of the claimant and verifier reversed. The MS shall generate a challenge, RAND2, the BS shall generate an actual response, RES2, and the MS shall generate an expected response, XRES2. The MS on receipt of RES2 from the BS shall compare it with XRES2. If the values are equal the result R2 shall be set to TRUE, else the result R2 shall be set to FALSE.

The same authentication key K shall be used as in the case of authentication of the user by the infrastructure together with a random seed RS. However, the algorithms shall be different: TA11 shall be replaced by TA21 and TA12P by TA22P. Hence, there should also be a different value for the session authentication key, KS'. The process is summarized in figure 2.

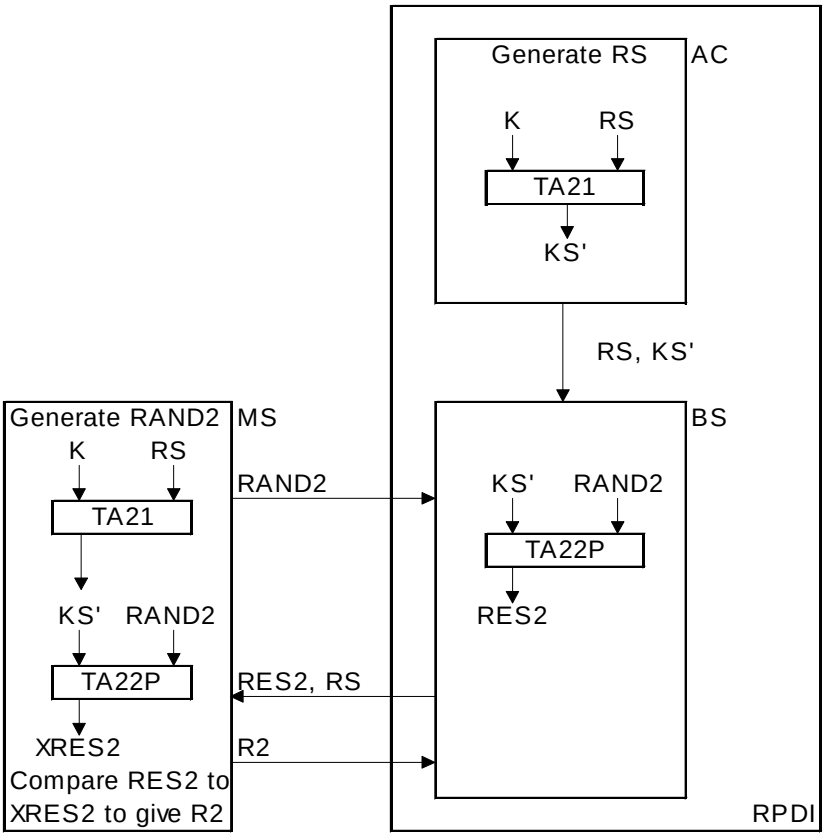


Figure 2: Authentication of the infrastructure by a user

4.1.4 Mutual authentication of user and infrastructure

Mutual authentication of user and infrastructure shall be achieved using a combined three pass mechanism. The algorithms and key K used shall be same as those used in the one way authentication described in the previous subclauses. The decision to make the authentication mutual shall be made by the first party to be challenged, not the initial challenging party. Thus mutual authentication shall be started as a one way authentication by the first challenging party, and shall be made mutual by the responding party.

If the first authentication in such a case fails the second authentication shall be abandoned.

If the authentication was initiated by the RPDI, it shall use K and one random seed RS with algorithms TA11 and TA12P to generate a session key KS. It shall then send random challenge RAND1 to the MS together with random seed RS. The MS shall run TA11 to generate session key KS, and because the authentication is to be made mutual it shall also run algorithm TA12P to generate a second session key KS'. Both MS and RPDI shall run algorithm TA12P; the MS then sends its response RES1 back to the RPDI. However, the MS also sends its mutual challenge RAND2 to the RPDI at the same time. The RPDI shall compare the response from the MS RES1 with its expected response XRES1, and because it has received a mutual challenge, it shall run TA12P to generate session key KS'. The RPDI shall then run TA22P to produce its response to the MS's challenge RES2. RES2 is sent to the MS, which shall also run TA22P to produce expected response XRES2. The MS shall compare RES2 with XRES2; and if the same, mutual authentication will have been achieved.

The process is shown in figure 3.

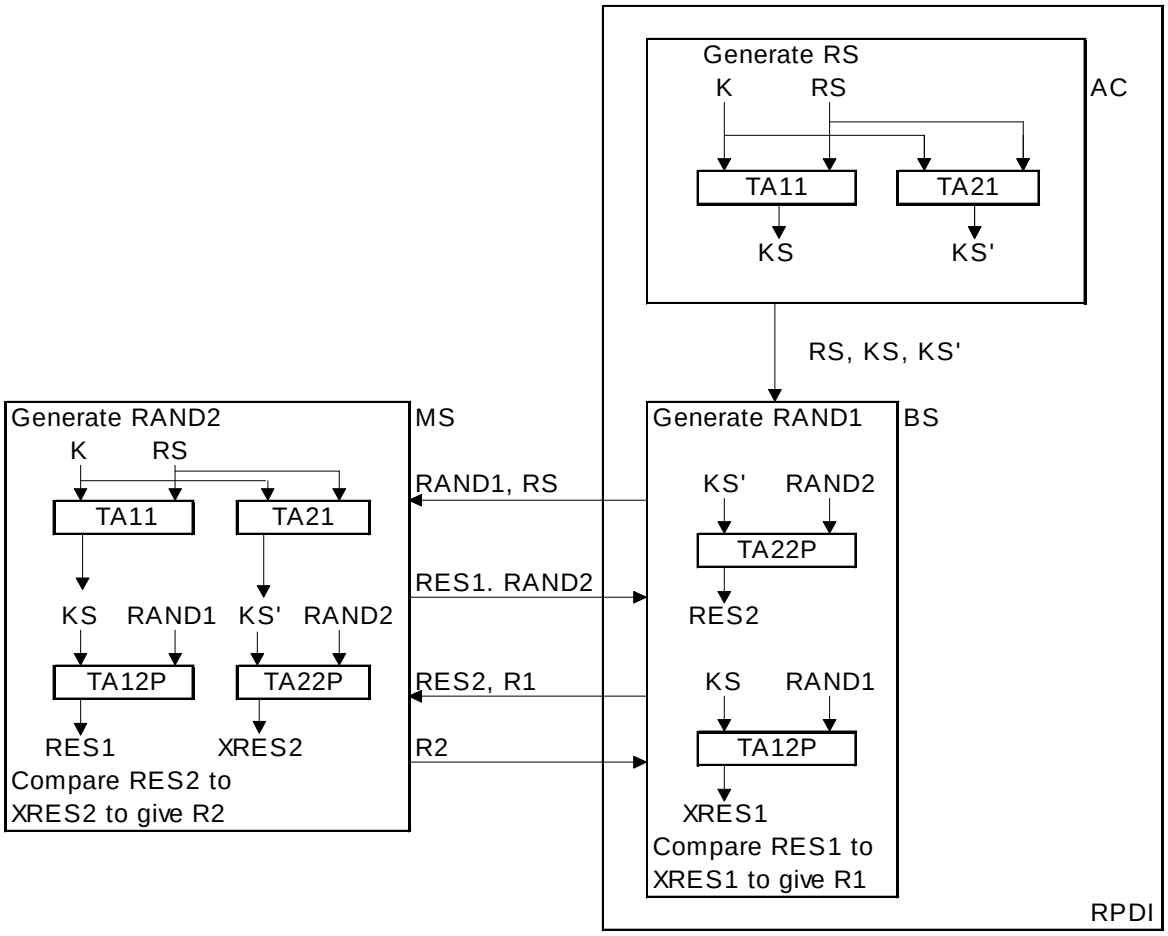


Figure 3: Mutual authentication initiated by RPDI

The mutual authentication process may also occur if a one way authentication is initiated by the MS, and then made mutual by the RPDI. In this case, the algorithms are the same, however the sequence is reversed as shown in figure 4.

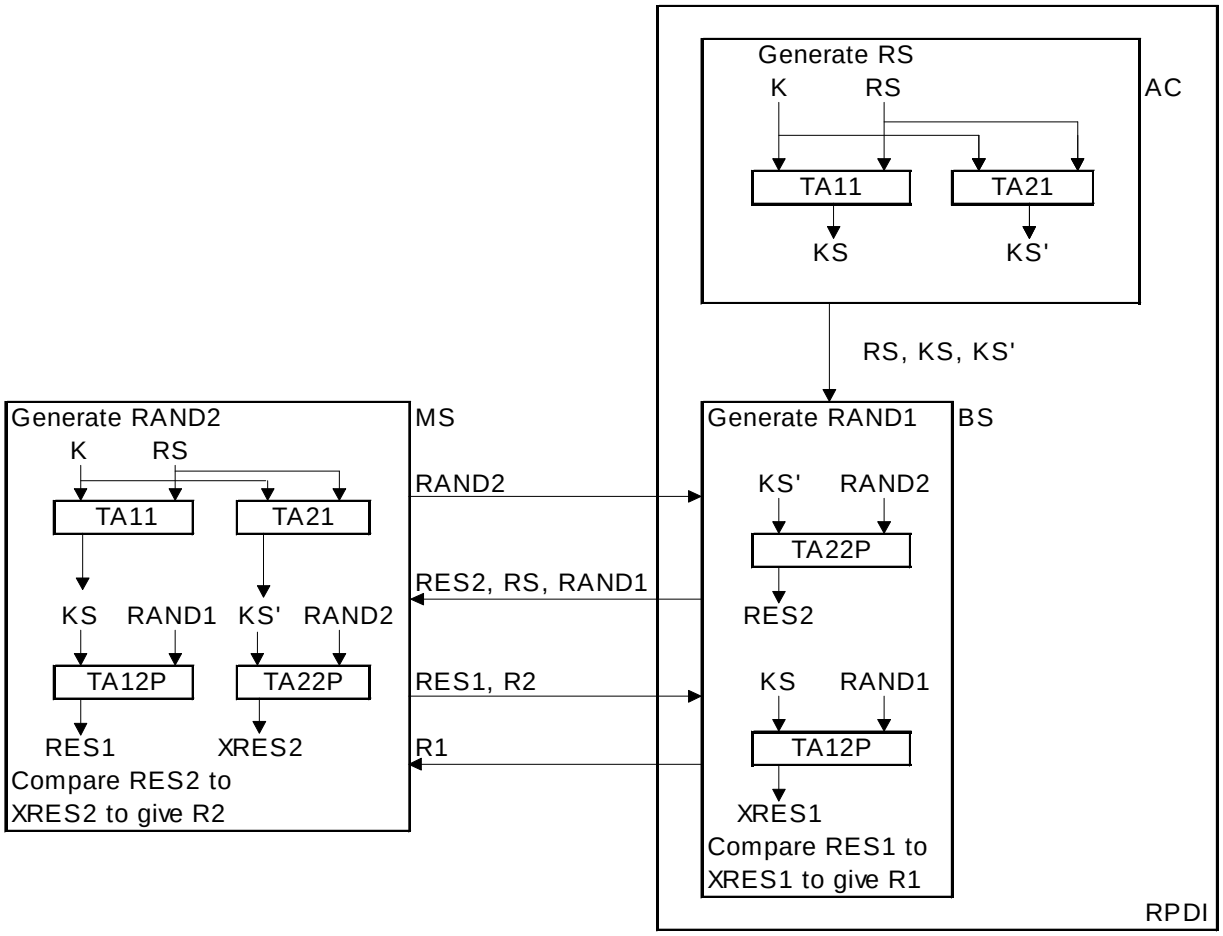


Figure 4: Mutual authentication initiated by MS

4.1.5 The authentication key

Users should be authenticated by a process that is carried out in the MS, as described in subclause 4.1.2. To provide against misuse of lost, or stolen, MS, and to authenticate the user to the MS, the user should be required to make an input before K is available and valid for use. K may be stored in a module, which may or may not be detachable, and the user may be required to make an input to this module, e.g. a personal identification number (PIN).

4.1.5.1 Generation of K

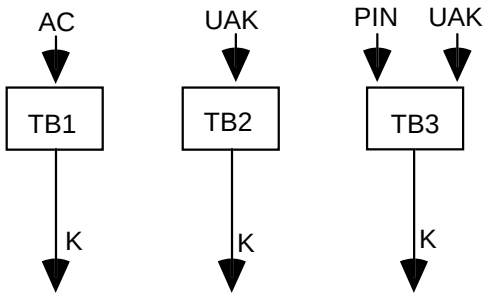


Figure 5: Generation of the authentication key

The generation of K shall be carried out using at least one of the following cases, summarized in figure 5:

1) K may be generated from an Authentication Code (AC) that is manually entered by the user. In this case AC shall be remembered by the user and should not normally be longer than a few digits. The procedure to generate K from AC is labelled TB1.

2) K may be generated from a User Authentication Key (UAK). In this case the UAK can be a random value of a desirable length (e.g. 128 bits). The procedure to generate K from UAK is labelled TB2.

3) K may be generated from both the UAK stored in a module and the PIN entered by the user. The procedure to generate K from UAK and PIN is labelled TB3. In this case the actual checking shall be carried out implicitly by the infrastructure through the authentication process.

4.1.6 Equipment authentication

The authentication of the TETRA Equipment Identity (TEI) is outside the scope of this ETS. However the protocol described in subclause 4.3 provides a mechanism whereby the BS may demand an MS to provide TEI in encrypted form as part of the registration exchange.

4.2 Service Description and Primitives

NOTE: The primitives described in this subclause are not testable and may be interpreted as for information only.

The primitives of the authentication service are shown in figure 6.

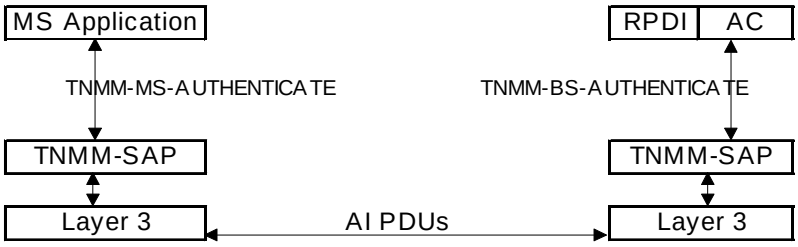


Figure 6: TNMM-AUTHENTICATE primitives

The description of the authentication mechanisms in subclause 4.1 assigns TA11 and TA21 to AC, and TA12P and TA22P to the BS for the SwMI side. The primitives in the BS and MS may be different.

The convention used in this ETS is to pair primitives as in table 1.

Table 1: Pairing of primitives across TNMM SAP

MM to Application	Application to MM
Indication	Response
Confirm	Request

4.2.1 BS Authentication primitives

At the TNMM service access point, a specific service shall be provided to allow an application to initiate an authentication exchange and to receive its result. The primitives required should be as follows (TNMM-BS-AUTHENTICATE in each case):

Indication: Used by MM to indicate to AC that a terminal is requesting authentication of the RPDI, or that in systems where authentication is required that a terminal is registering.

Response: Used by the AC to supply the session key(s) and random seed to the BS.

Request: Used by AC to request authentication of a terminal.

Confirm: Used by MM to indicate result of an authentication request.

The content of the primitives should be as shown in table 2.

Table 2: Parameters in TNMM-BS-AUTHENTICATE primitive

Parameter	Indication	Response	Request	Confirm
ITSI	M	M	M	M
Type	M	-	M	-
Session key	-	M	M	-
Random seed	-	M	M	-
Mutual authentication flag	-	M	M	-
Second session key	-	C	C	-
Result	-	-	-	M

The parameters should be coded as below:

Type =
Registration;
Authentication demand.

Result =
Success;
RPDI authentication fail;
Terminal authentication fail;
Terminal authentication reject.

Parameters ITSI, KS, RS, MF, KS', R should be coded as binary streams with maximum lengths as defined by table 32.

4.2.2 MS Authentication primitives

At the TNMM service access point, a specific service shall be provided to allow an application to initiate an authentication exchange and to receive its result. The MS-MM shall respond to an authentication demand from the RPDI. The primitives required should be as follows (TNMM-MS-AUTHENTICATE in each case):

Indication: Used by MM to indicate to the application that the RPDI is requesting the terminal to authenticate itself.

Response: Used by the application to supply the session key(s) and random seed to the terminal.

Request: Used by the application to request authentication of the RPDI.

Confirm: Used by MM to indicate result of an authentication request.

The content of the primitives should be as shown in table 3.

Table 3: Parameters in TNMM-MS-AUTHENTICATE primitive

Parameter	Indication	Response	Request	Confirm
Type	M	-	M	-
Session key	-	M	M	-
Random seed	-	M	M	-
Mutual authentication flag	-	M	M	-
Second session key	-	C	C	-
Result	-	-	-	M

The parameters should be coded as below:

Type =
Registration;
Authentication demand;

Result =
Success;
RPDI authentication fail;
RPDI authentication reject;
Terminal authentication fail;
Terminal authentication reject.

Parameters KS, RS, MF, KS', R should be coded as binary streams with maximum lengths as defined by table 32.

4.3 Definition of Protocols

4.3.1 Authentication State Transitions

Figure 7 gives an overview of the received PDUs that result in a change of authentication state. It is assumed that the initial state is Not-Authenticated and that demands for authentication may also be made when parties are in an authenticated state.

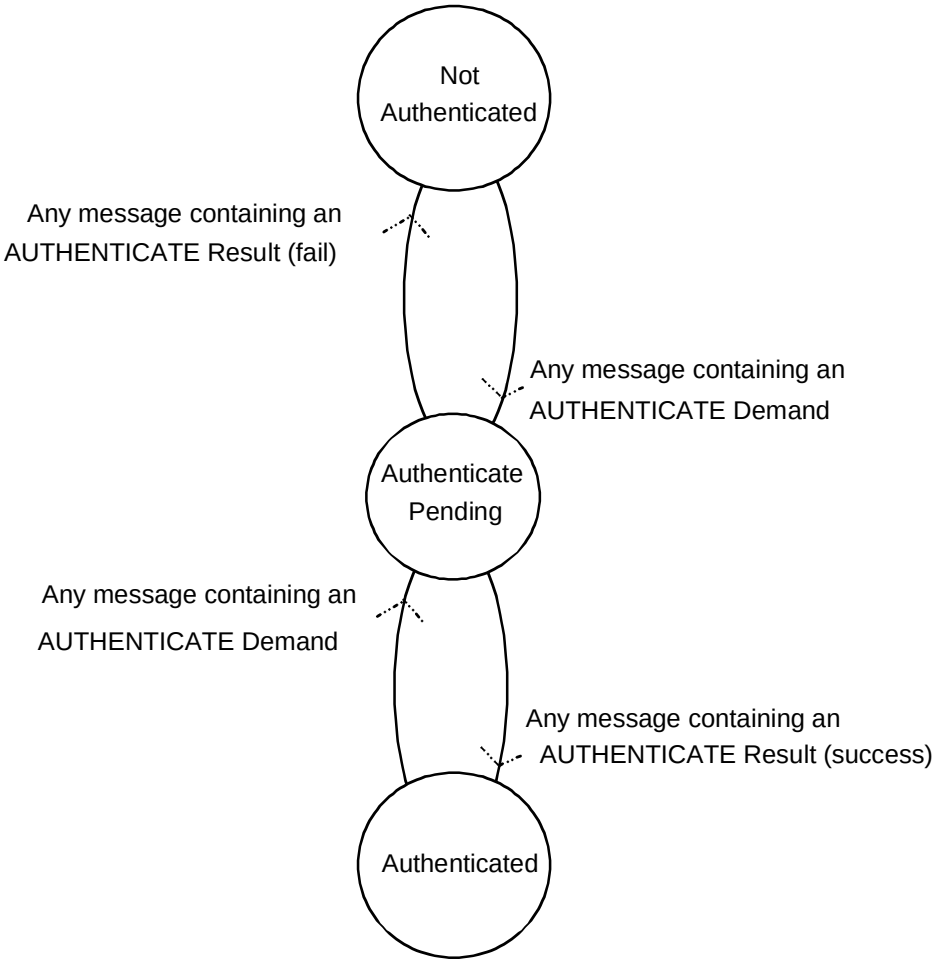


Figure 7: Authentication State transitions

4.3.2 Overview of authentication protocol

The air interface authentication protocol shall use the Mobility Management (MM) service of layer 3 in the TETRA protocol stack (see ETS 300 393-2 [2], clause 15).

An authentication exchange can be requested, either explicitly or as part of the registration procedure. It can be initiated by the MS or RPDI. The initiating side shall send an "AUTHENTICATION DEMAND" PDU that shall always be answered by the other side with an "AUTHENTICATION RESPONSE" PDU. Success or failure of the authentication shall be communicated by a specific "AUTHENTICATION RESULT" PDU.

The recipient of the first authentication demand may instigate mutual authentication by use of the mutual authentication indicator, and by sending its challenge together with the response to the first challenge. In this case, the response to this second challenge shall be sent together with the result of the first challenge. This mechanism saves signalling, as only one random seed RS is required, and the functions can be combined in PDUs requiring fewer transmissions at the air interface.

Descriptions of the protocol, together with Message Sequence Charts (MSCs), are given in subclauses 4.3.2.1 to 4.3.2.9. In each case the label in the MSC is mapped to a single statement in the text (if the same label appears on multiple diagrams the same text applies).

NOTE: In the MSCs given in subclauses 4.3.2.1 through 4.3.2.9 the position of the TNMM primitives is shown for information only.

4.3.2.1 Case 1: RPDI authenticates MS

D-AUTHENTICATION DEMAND shall contain RAND1+RS,
U-AUTHENTICATION RESPONSE shall contain RES1,
D-AUTHENTICATION RESULT shall contain R1.

The normal message sequence in this case shall be according to figure 8.

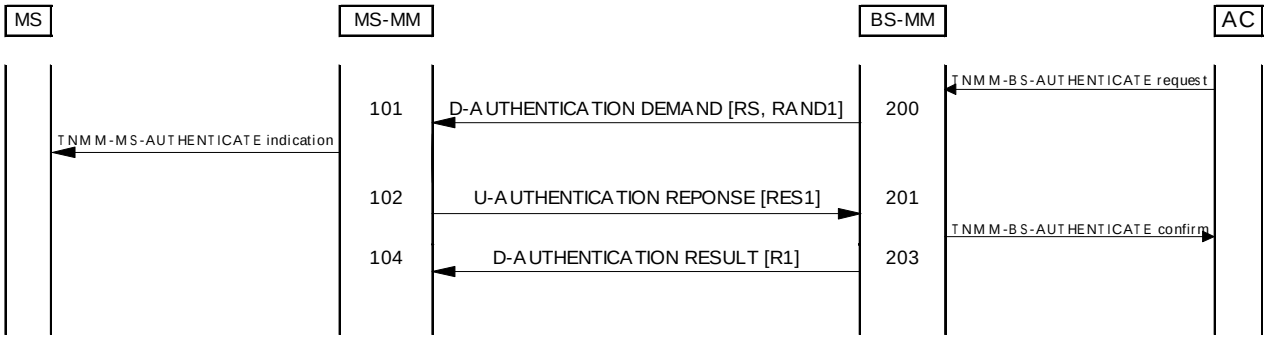


Figure 8: Authentication of MS by RPDI

200 BS-MM shall challenge MS-MM to authenticate by sending RS and RAND1. The RPDI shall also calculate XRES1 using algorithms TA11 and TA12P using RS and RAND1 as inputs.

101 MS-MM shall retrieve RS and RAND1 from the authentication challenge and shall run algorithms TA11 and TA12P to generate RES1.

102 MS-MM shall respond to the authentication challenge by sending RES1 to BS-MM. Since the MS is not configured to mutually authenticate the RPDI, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESPONSE to be false and RAND2 shall not be included in this PDU.

201 BS-MM shall retrieve RES1 and compare it with the previously calculated XRES1 (as described in 200) to decide whether or not authentication was successful.

203 BS-MM shall send the result R1 of the MS-MM authentication to MS-MM to indicate whether or not authentication was successful.

If authentication was successful, BS-MM shall set authentication result to TRUE and shall send D-AUTHENTICATION RESULT to MS-MM. Since, in this case, there is no mutual authentication, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be false and RES2 shall not be included in this PDU.

If authentication was not successful, BS-MM shall instead set authentication result to FALSE and shall send D-AUTHENTICATION RESULT. The "Mutual authentication flag" in D-AUTHENTICATION RESULT shall be set to false and RES2 shall not be included in this PDU.

104 MS-MM shall retrieve R1.

4.3.2.2 Case 2: MS authenticates RPDI

U-AUTHENTICATION DEMAND shall contain RAND2,
D-AUTHENTICATION RESPONSE shall contain RES2+RS,
U-AUTHENTICATION RESULT shall contain R2.

The normal message sequence in this case shall be according to figure 9.

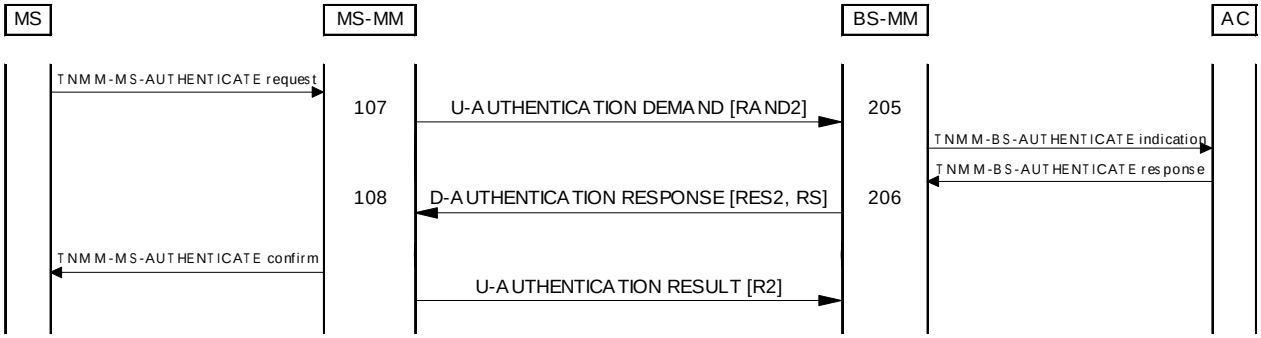


Figure 9: Authentication of the RPDI by the MS

107 MS-MM shall challenge BS-MM to authenticate by sending the challenge, RAND2.

205 BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22P to generate RES2.

206 BS-MM shall send the authentication response to MS-MM containing RES2 and RS. Since, in this case, the RPDI is not configured to mutually authenticate the MS, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESPONSE to be false and RAND1 shall not be included in this PDU.

108 MS-MM shall retrieve RES2 and RS, and run algorithms TA21 and TA22P to generate XRES2. MS-MM shall compare XRES2 and RES2 to decide whether or not authentication of the RPDI was successful.

109 MS-MM shall send the authentication result, R2, to BS-MM to indicate whether or not authentication was successful.

If authentication was successful, MS-MM shall send U-AUTHENTICATION RESULT. Since, in this case, there is no mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU.

208 BS-MM shall retrieve R2.

4.3.2.3 Case 3: Mutual authentication initiated by RPDI

D-AUTHENTICATION DEMAND shall contain RAND1+RS;
U-AUTHENTICATION RESPONSE shall contain RES1+RAND2;
D-AUTHENTICATION RESULT shall contain RES2+R1;
U-AUTHENTICATION RESULT shall contain R2.

The normal message sequence in this case shall be according to figure 10.

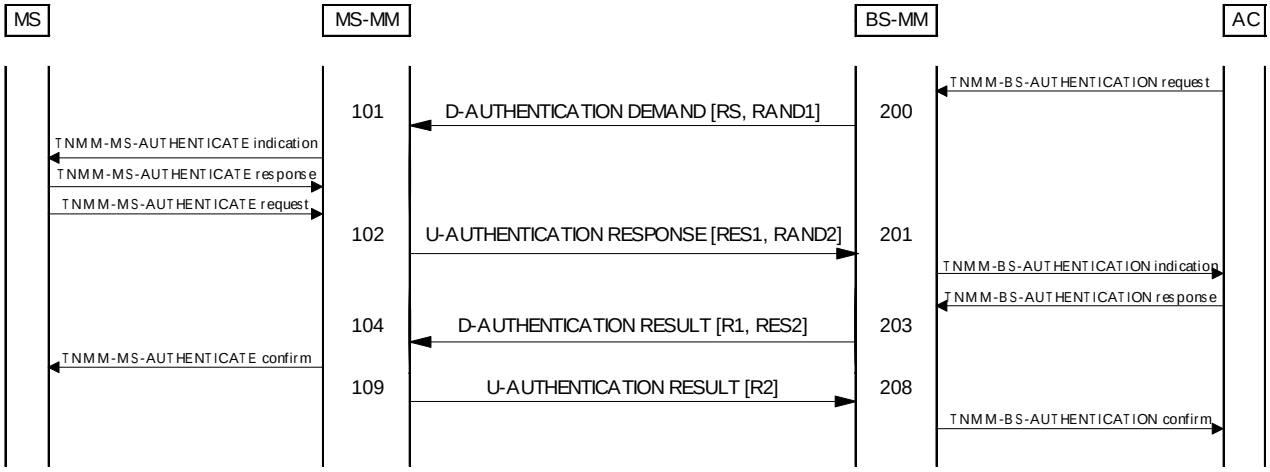


Figure 10: Mutual Authentication initiated by RPDI

200 Refer to case 1 in subclause 4.3.2.1

101 Refer to case 1 in subclause 4.3.2.1

102 MS-MM shall respond to the authentication challenge by sending RES1 to BS-MM. Since, in this case, the MS is configured for mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESPONSE to be true and RAND2 shall be included in this PDU.

201 BS-MM shall retrieve RES1 and compare it with the previously calculated XRES1 (as described in 200) to decide whether or not authentication of the MS was successful.

If authentication of the MS was successful and, since, in this case, authentication is mutual, BS-MM shall also retrieve RAND2 from U-AUTHENTICATION RESPONSE and the RPDI shall generate RES2 using algorithms TA21 and TA22P.

If authentication of the MS was not successful, BS-MM shall not calculate RES2.

203 BS-MM shall send the MS authentication result, R1 (success or failure), to MS-MM to indicate whether or not authentication of the MS was successful.

If authentication of the MS was successful, and, since the MS has requested mutual authentication, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be true and the response, RES2, shall be included in this PDU.

If authentication of the MS was not successful, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be false and the response, RES2, shall not be included in this PDU.

104 MS-MM shall retrieve R1.

If R1 indicates successful authentication, MS-MM shall retrieve RES2 and the MS shall run algorithms TA21 and TA22P to generate and XRES2. MS-MM shall then compare XRES2 and RES2 to decide whether or not authentication of the RPDI was successful.

If R1 does not indicate successful authentication of the MS, the MS shall not calculate XRES2.

109 If authentication of the MS was successful as indicated by R1, MS-MM shall send the authentication result, R2, to BS-MM in U-AUTHENTICATION RESULT. Since this is the final stage of the mutual authentication procedure, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and RES1 shall not be included in this PDU.

If authentication of the MS was successful but authentication of the RPDI was not successful, MS-MM shall instead send U-AUTHENTICATION RESULT to indicate the result, R2.

If authentication of the MS was not successful, MS-MM shall not send U-AUTHENTICATION RESULT.

208 BS-MM shall retrieve R2.

4.3.2.4 Case 4: Mutual authentication initiated by MS

U-AUTHENTICATION DEMAND shall contain RAND2;
D-AUTHENTICATION RESPONSE shall contain RES2+RS+RAND1;
U-AUTHENTICATION RESULT shall contain RES1+R2;
D-AUTHENTICATION RESULT shall contain R1.

The normal message sequence in this case shall be according to figure 11.

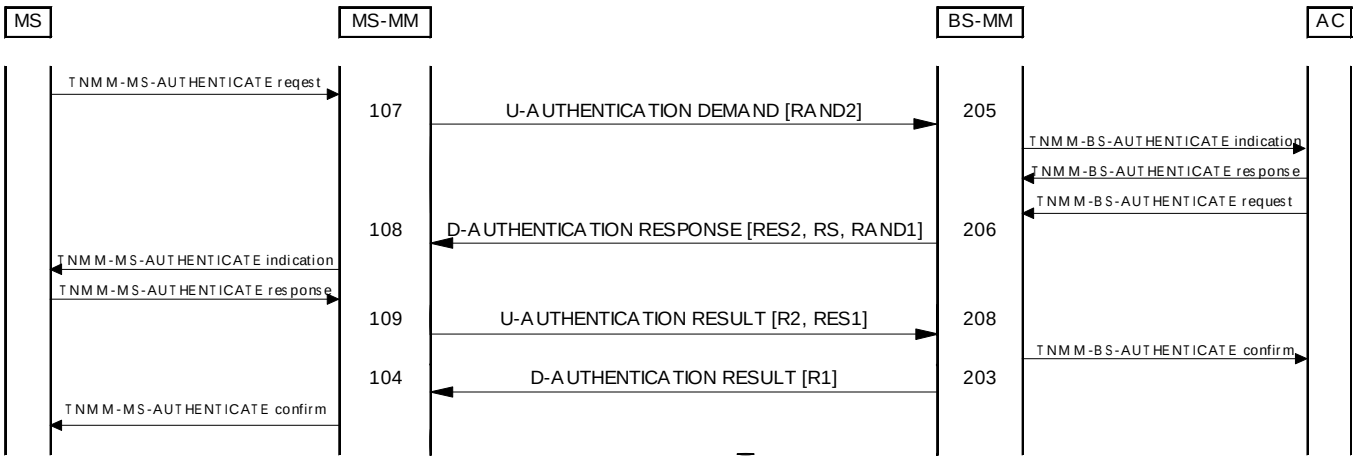


Figure 11: Mutual authentication initiated by MS

107 Refer to case 2 in subclause 4.3.2.2

205 Refer to case 2 in subclause 4.3.2.2

206 BS-MM shall respond to the authentication challenge by sending RES2 and RS to MS-MM. Since, in this case, the RPDI is configured for mutual authentication, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESPONSE to be true and RAND1 shall be included in this PDU.

108 MS-MM shall retrieve RES2 and RS, and run algorithms TA21 and TA22P to generate XRES2. MS-MM shall compare XRES2 and RES2 to decide whether or not authentication of the RPDI was successful.

If authentication of the RPDI was successful and, since, in this case, authentication is mutual, MS-MM shall also retrieve RAND1 from D-AUTHENTICATION RESPONSE and the MS shall generate RES1 using algorithms TA11 and TA12P.

If authentication of the RPDI was not successful, MS-MM shall not calculate RES1.

109 MS-MM shall send the authentication result, R2 (success or failure), to BS-MM to indicate whether or not authentication of the RPDI was successful.

If authentication of the RPDI was successful, and, since the RPDI has requested mutual authentication, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be true and the response, RES1, shall be included in this PDU.

If authentication of the RPDI was not successful, MS-MM shall set the "Mutual authentication flag" in U-AUTHENTICATION RESULT to be false and the response, RES1, shall not be included in this PDU.

208 BS-MM shall retrieve R2.

If R2 indicates successful authentication, BS-MM shall retrieve RES1 and the RPDI shall run algorithms TA11 and TA12P to generate and XRES1. BS-MM shall then compare XRES1 and RES1 to decide whether or not authentication of the MS was successful (R1).

If R2 does not indicate successful authentication of the RPDI, the RPDI should not attempt to retrieve RES1 or calculate XRES1.

203 If authentication of the RPDI was successful as indicated by R2, BS-MM shall send the authentication result, R1, using D-AUTHENTICATION RESULT. Since this is the final stage of the mutual authentication procedure, BS-MM shall set the "Mutual authentication flag" in D-AUTHENTICATION RESULT to be false and RES2 shall not be included in this PDU.

If authentication of the RPDI was successful but authentication of the MS was not successful, BS-MM shall send D-AUTHENTICATION RESULT to indicate the result, R1.

If authentication of the RPDI was not successful, BS-MM shall not send D-AUTHENTICATION RESULT.

104 MS-MM shall retrieve R1.

4.3.2.5 Case 5: RPDI authenticates MS during registration

U-LOCATION UPDATE DEMAND,
D-AUTHENTICATION DEMAND shall contain RAND1+RS,
U-AUTHENTICATION RESPONSE shall contain RES1,
D-LOCATION UPDATE ACCEPT shall contain R1 + (TEI request),
(U-TEI PROVIDE shall contain TEI).

The normal message sequence in this case shall be according to figure 12.

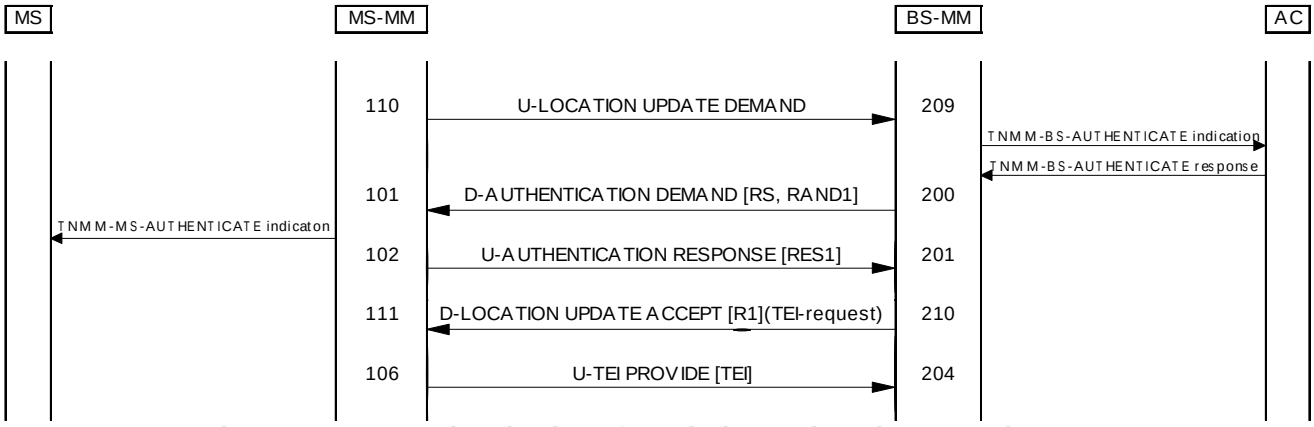


Figure 12: RPDI authentication of MS during registration procedure

110 MS-MM initiates registration. U-LOCATION UPDATE DEMAND may be sent by the MS as a result of one of the following registration scenarios:

- MS-initiated registration due to roaming (i.e. change of location area);
- user application initiated registration;
- MS-initiated registration due to migration after identity exchange with the RPDI;
- MS-initiated forward registration;
- after receiving D-LOCATION UPDATE COMMAND as part of RPDI-initiated registration.

NOTE: In the case of migration which requires identity exchange with the RPDI, the MS shall not include an authentication challenge in the first U-LOCATION UPDATE DEMAND of the procedure. The MS shall wait until it has received an SSI for use on the system (sent in D-LOCATION UPDATE PROCEEDING) and then include any authentication challenge in the second U-LOCATION UPDATE DEMAND which is sent using the visitor SSI allocated during identity exchange. Similarly, the RPDI shall not attempt to authenticate an MS when U-LOCATION UPDATE DEMAND is requesting an identity exchange, but only when the MS attempts registration with an ISSI or VASSI.

209 Since, in this case, the RPDI is configured to authenticate an MS at registration, the RPDI shall initiate authentication of the MS as described by case 1 in subclause 4.3.2.1.

200 Refer to case 1 in subclause 4.3.2.1.
101 Refer to case 1 in subclause 4.3.2.1.
102 Refer to case 1 in subclause 4.3.2.1.
201 Refer to case 1 in subclause 4.3.2.1.

210 BS-MM shall inform MS-MM whether or not authentication was successful.

If authentication was successful and registration is to be accepted by the RPDI, BS-MM shall send D-LOCATION UPDATE ACCEPT. BS-MM shall include the "Authentication downlink" type 3 element in D-LOCATION UPDATE ACCEPT to convey R1. BS-MM may request MS-MM to supply the MS TEI by setting the "TEI request flag" in the "Authentication downlink" element.

If authentication was not successful, BS-MM shall instead send D-LOCATION UPDATE REJECT. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed.

111 If MS-MM receives D-LOCATION UPDATE ACCEPT, MS-MM shall retrieve R1 which should indicate successful authentication. If authentication has failed, the MS should receive D-LOCATION UPDATE REJECT.

106 If authentication was successful and BS-MM requested the MS TEI in D-LOCATION UPDATE ACCEPT, MS-MM shall provide the MS TEI by sending U-TEI PROVIDE which shall contain the MS TEI and the address extension (MCC and MNC) for the MS so that the RPDI has the full ITSI of the MS.

If authentication was not successful or the RPDI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

204 BS-MM shall retrieve the MS TEI from U-TEI PROVIDE. The BS may record the association of ITSI and TEI.

4.3.2.6 Case 6: MS authenticates RPDI during registration

U-LOCATION UPDATE DEMAND shall contain RAND2;
D-AUTHENTICATION RESPONSE shall contain RES2+RS;
U-AUTHENTICATION RESULT shall contain R2;
D-LOCATION UPDATE ACCEPT (may contain TEI-request);
(U-TEI PROVIDE shall contain TEI).

The normal message sequence in this case shall be according to figure 13.

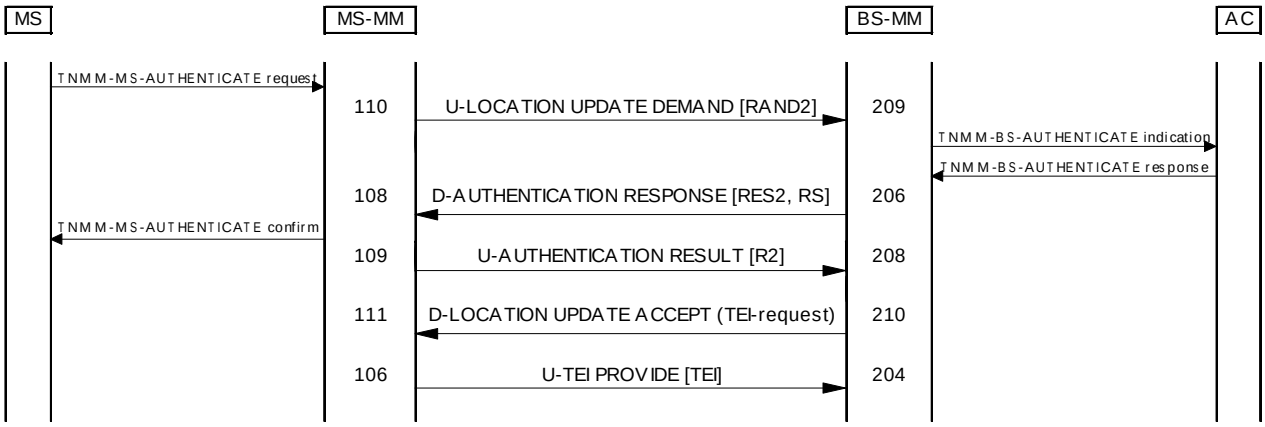


Figure 13: MS authentication of RPDI by the MS during registration

110 Refer to case 5 in subclause 4.3.2.5.

209 BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22P to generate RES2. BS-MM shall then respond to the authentication request from the MS as described by case 2 in subclause 4.3.2.2.

206 Refer to case 2 in subclause 4.3.2.2.
108 Refer to case 2 in subclause 4.3.2.2.
109 Refer to case 2 in subclause 4.3.2.2.
208 Refer to case 2 in subclause 4.3.2.2.

210 If authentication was successful and registration is to be accepted by the RPDI, BS-MM shall send D-LOCATION UPDATE ACCEPT. BS-MM may include the "Authentication downlink" type 3 element in D-LOCATION UPDATE ACCEPT to request MS-MM to supply the MS TEI by setting the "TEI request flag". Since, in this case, the authentication procedure has already been completed, R1 element shall be set to "successful".

If authentication was not successful, BS-MM should instead send D-LOCATION UPDATE REJECT. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed.

111 If MS-MM receives D-LOCATION UPDATE ACCEPT, after completing authentication of the RPDI, MS-MM shall ignore R1. If authentication has failed, the MS should receive D-LOCATION UPDATE REJECT.

106 If authentication was successful and BS-MM requested the MS TEI in D-LOCATION UPDATE ACCEPT, MS-MM shall provide the MS TEI by sending U-TEI PROVIDE which shall contain the MS TEI and the address extension (MCC and MNC) for the MS so that the RPDI has the full ITSI of the MS.

If authentication was not successful or the RPDI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

204 BS-MM shall retrieve the MS TEI from U-TEI PROVIDE. The BS may record the association of ITSI and TEI.

4.3.2.7 Case 7: Mutual authentication initiated by MS during registration

U-LOCATION UPDATE DEMAND shall contain RAND2;
D-AUTHENTICATION RESPONSE shall contain RES2+RS+RAND1;
U-AUTHENTICATION RESULT shall contain RES1+R2;
D-LOCATION UPDATE ACCEPT shall contain R1(+ TEI-request);
(U-TEI PROVIDE shall contain TEI).

The normal message sequence in this case shall be according to figure 14.

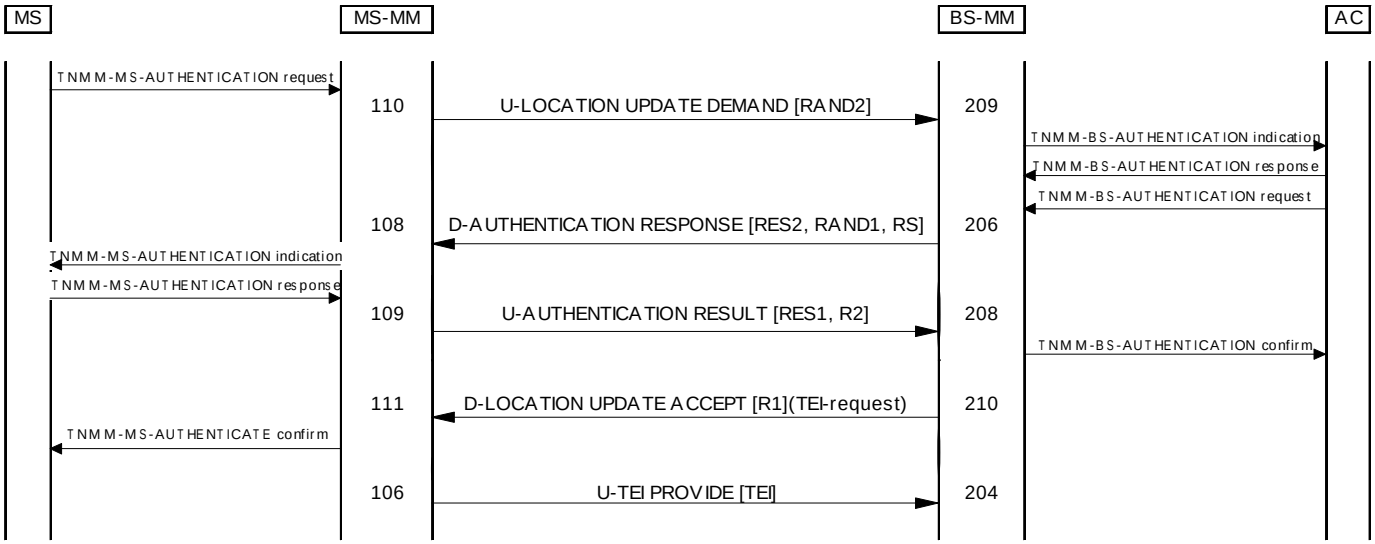


Figure 14: Mutual authentication started by the MS during registration

110 MS-MM initiates registration. U-LOCATION UPDATE DEMAND may be sent by the MS as a result of one of the following registration scenarios:

- MS-initiated registration due to roaming (i.e. change of location area);
- user application initiated registration;
- MS-initiated registration due to migration after identity exchange with the RPDI;
- MS-initiated forward registration;
- after receiving D-LOCATION UPDATE COMMAND as part of RPDI-initiated registration.

Note that, in the case of migration which requires identity exchange with the RPDI, the MS shall not include an authentication challenge in the first U-LOCATION UPDATE DEMAND of the procedure. The MS shall wait until it has received an SSI for use on the system (sent in D-LOCATION UPDATE PROCEEDING) and then include any authentication challenge in the second U-LOCATION UPDATE DEMAND which is sent using the visitor SSI allocated during identity exchange. Similarly, the RPDI shall not attempt to authenticate an MS when U-LOCATION UPDATE DEMAND is requesting an identity exchange, but only when the MS attempts registration with an ISSI or VASSI.

Since, in this case, MS-MM is configured to authenticate the RPDI at registration, MS-MM shall include the type 3 element "Authentication uplink" in U-LOCATION UPDATE DEMAND and MS-MM shall include the random challenge, RAND2, in this element.

209 BS-MM shall retrieve RAND2 and run algorithms TA21 and TA22P to generate RES2. Since, in this case, the RPDI is configured for mutual authentication, BS-MM respond to the authentication request from the MS as described by case 4 in subclause 4.3.2.4.

206 Refer to case 4 in subclause 4.3.2.4.
108 Refer to case 4 in subclause 4.3.2.4.
109 Refer to case 4 in subclause 4.3.2.4.
208 Refer to case 4 in subclause 4.3.2.4.

210 If authentication of the MS was successful as indicated by R2, BS-MM shall inform MS-MM whether or not authentication of the RPDI was successful.

If authentication of the RPDI was successful and registration is to be accepted by the RPDI, BS-MM shall send D-LOCATION UPDATE ACCEPT. BS-MM shall include the "Authentication downlink" type 3 element in D-LOCATION UPDATE ACCEPT to convey R1. BS-MM may request MS-MM to supply the MS TEI by setting the "TEI request flag" in the "Authentication downlink" element.

If authentication of the RPDI or authentication of the MS was not successful, BS-MM shall instead send D-LOCATION UPDATE REJECT. D-LOCATION UPDATE REJECT shall contain a reject reason which shall indicate that authentication has failed.

111 If MS-MM receives D-LOCATION UPDATE ACCEPT, MS-MM shall retrieve R1 which should indicate successful authentication. If authentication has failed, the MS should receive D-LOCATION UPDATE REJECT.

106 If authentication of the MS and RPDI were both successful and BS-MM requested the MS TEI in D-LOCATION UPDATE ACCEPT, MS-MM shall provide the MS TEI by sending U-TEI PROVIDE which shall contain the MS TEI and the address extension (MCC and MNC) for the MS so that the RPDI has the full ITSI of the MS.

If authentication was not successful or the RPDI did not request the MS TEI in D-LOCATION UPDATE ACCEPT, U-TEI PROVIDE shall not be sent.

204 BS-MM shall retrieve the MS TEI from U-TEI PROVIDE. The BS may record the association of ITSI and TEI.

4.3.2.8 Case 8: RPDI rejects authentication demand from MS

The normal message sequence in this case shall be according to figure 15.

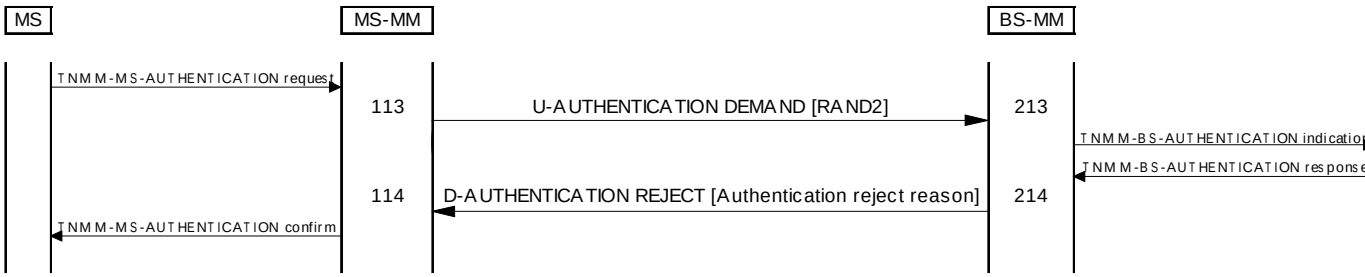


Figure 15: Authentication of MS as part of the registration procedure

113 The MS attempts to authenticate the RPDI by sending U-AUTHENTICATION DEMAND or by including the "Authentication uplink" type 3 element in U-LOCATION UPDATE DEMAND.

213 BS-MM receives an authentication challenge from the MS.

214 If the RPDI cannot support authentication, BS-MM shall respond to the authentication challenge with D-AUTHENTICATION REJECT. Note that if the RPDI responds to the authentication challenge with a mutual authentication, the MS shall not respond with U-AUTHENTICATION REJECT. If the MS initiates authentication of the RPDI, then the MS shall be able to support a mutual authentication request from the RPDI.

Note that, if the MS has sent an authentication challenge as part of a registration request (U-LOCATION UPDATE DEMAND) and the RPDI cannot support authentication because the MS has selected the wrong ciphering parameters in U-LOCATION UPDATE DEMAND, BS-MM shall reject the request by sending D-LOCATION UPDATE REJECT instead of D-AUTHENTICATION REJECT, which should also include a suggestion for what the ciphering parameters should be. This allows the MS to try again with the correct ciphering parameters.

114 MS-MM receives D-AUTHENTICATION REJECT and shall extract the reject reason which may be passed to the user application. If D-AUTHENTICATION REJECT is received in response to an authentication challenge embedded in U-LOCATION UPDATE DEMAND, MS-MM shall abandon the registration procedure. The MS may subsequently attempt to register with the RPDI without an authentication challenge.

4.3.2.9 Case 9: MS rejects authentication demand from RPDI

The normal message sequence in this case shall be according to figure 16.

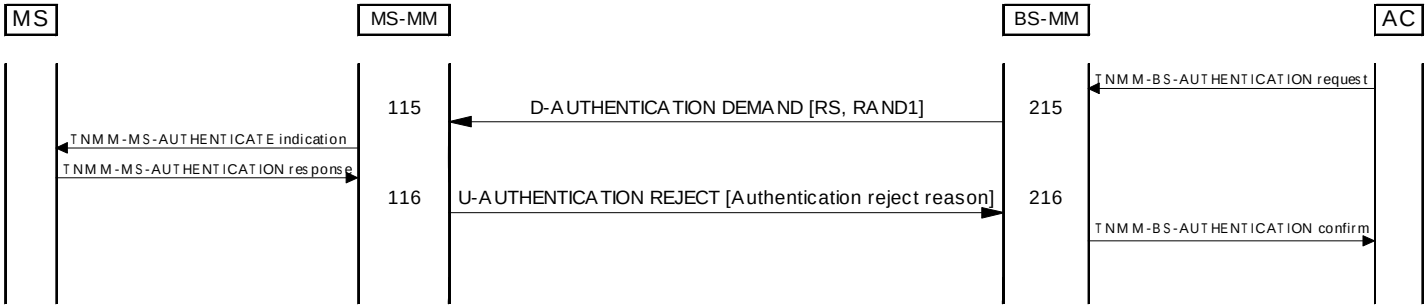


Figure 16: MS rejection of RPDI authentication demand

215 The RPDI attempts to authenticate the MS by sending D-AUTHENTICATION DEMAND. Note that this may be sent in response to a registration request from the MS or it may be initiated by the RPDI.

115 MS-MM receives an authentication challenge from the MS.

116 If the MS cannot support authentication, MS-MM shall respond to the authentication challenge with U-AUTHENTICATION REJECT. Note that if the MS responds to the authentication challenge with a mutual authentication, the RPDI shall not respond with D-AUTHENTICATION REJECT. If the RPDI initiates authentication of the MS, then the RPDI shall be able to support a mutual authentication request from the MS.

216 BS-MM receives U-AUTHENTICATION REJECT and shall extract the reject reason. If U-AUTHENTICATION REJECT is received in response to an authentication challenge which was sent as a result of an MS attempting to register (i.e. using U-LOCATION UPDATE DEMAND), BS-MM should respond with D-LOCATION UPDATE REJECT. This ensures that the RPDI does not allow an MS which cannot be authenticated to register on the network.

4.3.3 PDU descriptions

The PDUs detailed within this subclause shall be visible at the Um reference point (see ETS 300 393-1 [1], clause 5).

The general format of the PDU is defined according to table 4.

The elements shall be transmitted in the order specified by the table with the top element being transmitted first (before interleaving). The content of an information element is represented by a binary value and the most significant bit of that binary value shall be transmitted first (before interleaving). The coding of each element is specified in subclause 4.3.5.

Table 4: PDU layout

Information element	Length	Value	Remark
PDU Type	4		
Type 1 element (1)	varies		See definitions below.
Type 1 element (2)	varies		See definitions below.
…etc.	…etc.		…etc.
Type 1 element (n)	varies		See definitions below.
Optional bit (O-bit)	1	0	No optional type 2 or type 3 elements follow
		1	Optional type 2 or type 3 elements follow
Presence bit (P-bit) (1)	1	0	The type 2 element (1) is not present
		1	The type 2 element (1) is present.
Type 2 element (1)	varies		See definitions below.
Presence bit (P-bit) (2)	1	0	The type 2 element (2) is not present
		1	The type 2 element (2) is present.
Type 2 element (2)	varies		See definitions below.
…etc.	…etc.		…etc.
Presence bit (P-bit) (n)	1	0	The type 2 element (n) is not present
		1	The type 2 element (n) is present.
Type 2 element (n)	varies		See Type 2 element (1)
More bit (M-bit) (1)	1	0	No type 3 elements follow
		1	Type 3 elements follow
Type 3 Element Identifier (1)	4		See definitions below.
Length indicator (1)	11	0	Reserved for possible future use.
		$1\text{-}2047_{10}$	Length of the following type 3 Element in bits:
Type 3 Element (1)	varies		See definitions below.
More bit (M-bit) (2)	1	0	No more type 3 elements follow
		1	More type 3 elements follow
Type 3 Element Identifier (2)	4		See definitions below.
Length indicator (2)	11	0	Reserved for possible future use.
		$1\text{-}2047_{10}$	Length of the following type 3 Element in bits:
Type 3 Element (2)	varies		See definitions below.
…etc.	…etc.		…etc.
More bit (M-bit) (n)	1	0	No more type 3 elements follow
		1	More type 3 elements follow
Type 3 Element Identifier (n)	4		See definitions below.
Length indicator (n)	11	0	Reserved for possible future use.
		$1\text{-}2047_{10}$	Length of the following type 3 Element in bits:
Type 3 Element (n)	varies		See definitions below.
More bit (M-bit) (n+1) = 0	1	0	Last M-bit (Least Significant Bit in the PDU) = 0

The element type defines the encoding rule applied to an element.

Type 1 elements shall be placed within the PDU in a fixed order as specified in the PDU description tables. The elements shall have fixed lengths as specified in the length column or variable lengths as indicated by a preceding length element. Each Type 1 element shall either be a mandatory element or conditional to a mandatory element. Type 1 elements shall be placed before any Type 2 or Type 3 elements in the PDU. The last Type 1 element shall be followed by an O-bit. When the PDU contains any Type 2 or Type 3 elements the O-bit shall set to 1. When the PDU does not contain any Type 2 or Type 3 elements the O-bit shall be set to 0.

Type 2 elements are either optional or conditional to an optional element and shall be placed within the PDU in a fixed order as specified in the PDU description tables. There shall be one P-bit preceding each Type 2 optional element specified for the PDU to indicate presence of that element. The P-bit shall indicate either "Type 2 element present" or "Type 2 element not present". Type 2 elements shall have fixed lengths as specified in the length column of the PDU description tables. Type 2 elements shall be placed after all Type 1 elements and before any Type 3 elements in the PDU.

Type 3 elements are optional and shall be placed within the PDU in numerical order as specified within the 'Type 3 Element Identifier' element. Type 3 Elements shall be placed after any Type 1 and Type 2 elements. If there are any Type 3 elements specified for the PDU an M-bit shall follow the Type 1 and Type 2 elements. The M-bit shall indicate either "Type 3 element to follow" or "no Type 3 element to follow". If there are Type 3 elements to follow, they shall be preceded by a 'Type 3 Element Identifier' element and a 'Length Indicator' element in that order. A further M-bit shall follow the Type 3 element and after the last Type 3 element included the M-bit shall be set to 0 to indicate "no Type 3 element to follow". Type 3 element coding can contain sub-elements which can be either of Type 1, 2 or 3.

The following rules shall apply for decoding of the PDU:

```
DO for all possible Type 1 elements
IF element is not a conditional element
    THEN DECODE Type 1 element
    ELSE DECODE conditional Type 1 element if indicated
END DO
DECODE O-bit
IF O-bit set to 'No Optional Elements present'
    THEN END of PDU decoding
    ELSE
    DO for all possible Type 2 elements
        DECODE P-bit
        IF P-bit set to 'Present'
            THEN DECODE Type 2 element AND
            IF element points to conditional element(s)
                THEN DECODE indicated conditional element(s), END IF
        IF P-bit not set 'Present'
            THEN pass also elements conditional on that element
    END DO
    WHILE M-bit set to 'More Type 3 elements follows'
        DECODE Type 3 element
    END WHILE
END of PDU decoding.
```

NOTE: There is only one P-bit common for a type 2 optional element and any element(s) conditional on the first element. In that case the conditional element(s) follow immediately the first element (without a P-bit between them).

The information contained in the following PDU description tables corresponds to the following key:

Length: - length of the element in bits;
Type: - element type (1, 2, or 3) as defined above;
C/O/M: - conditional/optional/mandatory information in the PDU;
Remark: - comment.

NOTE: The preceding text has been taken and corrected (PDU length) from ETS 300 393-2 [2], table 45 and this reference is to be considered the normative source.

There shall be 11 PDUs defined at the air interface as shown in table 5:

Table 5: AIR INTERFACE PDUs

AIR INTERFACE PDU
D-AUTHENTICATION DEMAND
D-AUTHENTICATION RESPONSE
D-AUTHENTICATION RESULT
D-AUTHENTICATION REJECT
U-AUTHENTICATION DEMAND
U-AUTHENTICATION RESPONSE
U-AUTHENTICATION RESULT
U-AUTHENTICATION REJECT
U-TEI PROVIDE

In the tables that follow the contents of each PDU are presented in the order of transmission. Where elements can be repeated the order of these elements shall be maintained.

4.3.3.1 D-AUTHENTICATION DEMAND

Shall be used by the infrastructure to initiate an authentication of the MS.

Direction: RPDI to MS
Service used: MM
Response to: U-LOCATION UPDATE DEMAND or none
Response expected: U-AUTHENTICATION RESPONSE

Table 6: D-AUTHENTICATION DEMAND PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0001_2
Random challenge [RAND1]	80	1	M	
Random seed [RS]	80	1	M	
Proprietary element		3	O	

4.3.3.2 D-AUTHENTICATION RESPONSE

Shall be used by the infrastructure to respond to an authentication demand from the MS.

Direction: RPDI to MS
Service used: MM
Response to: U-AUTHENTICATION DEMAND
Response expected: U-AUTHENTICATION RESULT

Table 7: D-AUTHENTICATION RESPONSE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1000_2
Random seed [RS]	80	1	M	
Response value [RES2]	32	1	M	
Mutual authentication flag	1	1	M	
Random challenge [RAND1]	80	1	C	note 1
Proprietary element		3	O	
NOTE: RAND1 is conditional on the Mutual authentication flag element. RAND1 shall be present if Mutual authentication flag = 1. Otherwise, RAND1 shall not be present in the PDU.				

4.3.3.3 D-AUTHENTICATION RESULT

Shall be used by the infrastructure to report the result of an MS authentication to the MS.

Direction: RPDI to MS
Service used: MM
Response to: U-AUTHENTICATION RESPONSE or U-AUTHENTICATION RESULT
Response expected: U-AUTHENTICATION RESULT or none

Table 8: D-AUTHENTICATION RESULT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1110_2
Authentication result [R1]	1	1	M	
Mutual authentication flag	1	1	M	
Response Value [RES2]	32	1	C	note 1
Proprietary element		3	O	
NOTE: RES2 is conditional on the Mutual authentication flag element. RES2 shall be present if Mutual authentication flag = 1. Otherwise, RES2 shall not be present in the PDU.				

4.3.3.4 D-AUTHENTICATION REJECT

Shall be used by the infrastructure to report to the MS any rejection of an authentication demand.

Direction: RPDI to MS
Service used: MM
Response to: U-AUTHENTICATION DEMAND
Response expected: none

Table 9: D-AUTHENTICATION REJECT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0010_2
Authentication reject reason	3	1	M	

4.3.3.5 U-AUTHENTICATION DEMAND

Shall be used by the MS to initiate an authentication of the BS/RPDI.

Direction: MS to RPDI
Service used: MM
Response to: none
Response expected: D-AUTHENTICATION RESPONSE

Table 10: U-AUTHENTICATION DEMAND PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0100_2
Random challenge [RAND2]	80	1	M	
Proprietary element		3	O	

4.3.3.6 U-AUTHENTICATION RESPONSE

Shall be used by MS-MM to respond to an authentication demand from the RPDI of the MS.

Direction: MS to RPDI
Service used: MM
Response to: D-AUTHENTICATION DEMAND
Response expected: D-AUTHENTICATION RESULT

Table 11: U-AUTHENTICATION RESPONSE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0000_2
Response Value [RES1]	32	1	M	
Mutual authentication flag	1	1	M	
Random challenge [RAND2]	80	1	C	note 1
Proprietary element		3	O	
NOTE: RAND2 is conditional on the Mutual authentication flag element. RAND2 shall be present if Mutual authentication flag = 1. Otherwise, RAND2 shall not be present in the PDU.				

4.3.3.7 U-AUTHENTICATION RESULT

Shall be used by MS-MM to report the result of an authentication of the BS/RPDI.

Direction: MS to RPDI
Service used: MM
Response to: D-AUTHENTICATION RESULT or D-AUTHENTICATION RESPONSE
Response expected: D-AUTHENTICATION RESULT or none

Table 12: U-AUTHENTICATION RESULT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0110_2
Authentication result [R2]	1	1	M	
Mutual authentication flag	1	1	M	
Response Value [RES1]	32	1	C	note 1
Proprietary element		3	O	
NOTE: RES1 is conditional on the Mutual authentication flag element. RES1 shall be present if Mutual authentication flag = 1. Otherwise, RES1 shall not be present in the PDU.				

4.3.3.8 U-AUTHENTICATION REJECT

Shall be used by the MS to report to the infrastructure any rejection of an authentication demand.

Direction: MS to RPDI
Service used: MM
Response to: D-AUTHENTICATION DEMAND
Response expected: none

Table 13: U-AUTHENTICATION REJECT PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1110_2
Authentication reject reason	3	1	M	

4.3.3.9 U-TEI PROVIDE

Shall be used by MS-MM to inform the RPDI of its terminal equipment identifier.

Direction: MS to RPDI
Service used: MM
Response to: D-LOCATION UPDATE ACCEPT
Response expected: none

Table 14: U-TEI PROVIDE PDU contents

Information Element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1001_2
TEI	60	1	M	
Address extension	24	1	M	
Proprietary element		3	O	

4.3.4 MM PDU type 3 information elements coding

The authentication mechanisms may be combined with the normal and RPDI-initiated registration procedures as shown in MSC scenarios earlier in clause 4. Therefore, type 3 elements are defined which carry the authentication information and which can be appended to the MM registration PDUs. These type 3 elements shall be as defined in this subclause.

4.3.4.1 Authentication uplink

This type 3 element shall be appended to U-LOCATION UPDATE DEMAND when the MS combines a registration request with a request to authenticate the RPDI or when the MS requests the CCK information for the current LA.

Direction: MS to RPDI
MM PDU: U-LOCATION UPDATE DEMAND
Response to: D-LOCATION UPDATE COMMAND or none
Response expected: D-AUTHENTICATION RESPONSE

Table 15: Authentication uplink element contents

Information Element	Length	Type	C/O/M	Remark
Random challenge [RAND2]	80	2	M	

4.3.4.2 Authentication downlink

This type 3 element shall be appended to D-LOCATION UPDATE ACCEPT to inform the MS about the result of an authentication procedure which has been combined with registration and/or to request that an MS supplies its TEI and/or to supply the MS with CCK information for the current cell.

Direction: RPDI to MS
MM PDU: D-LOCATION UPDATE ACCEPT
Response to: U-AUTHENTICATION RESPONSE
Response expected: none

Table 16: Authentication downlink element contents

Information Element	Length	Type	C/O/M	Remark
Authentication result [R1]	1	1	M	
TEI request flag	1	1	M	

4.3.5 PDU Information elements coding

The encoding of the elements for the PDUs described in subclause 4.3.3 is given in the following subclauses. The most significant bit of the values shown in the tables is transmitted first.

4.3.5.1 Address extension

The address extension element is used to indicate the full TSI address as defined below:

Table 17: Address extension element contents

Information Element	Length	Type	C/O/M	Remark
Mobile country code	10	1	M	
Mobile network code	14	1	M	

4.3.5.2 Authentication result

Authentication result indicates the success or failure of an authentication. If the authentication fails, this element gives the reason for failure.

Table 18: Authentication result element contents

Information element	Length	Value	Remark
Authentication Result [R1 or R2]	1	0	Authentication failed
		1	Authentication successful or no authentication currently in progress

4.3.5.3 Authentication reject reason

Authentication reject reason indicates why a demand for authentication is rejected.

Table 19: Authentication reject reason element contents

Information element	Length	Value	Remark
Authentication reject reason	3	000_2	Authentication not supported
		others	Reserved for future expansion

4.3.5.4 Mobile country code

The mobile country code of a TETRA network. For a full definition see ETS 300 393-1 [1], clause 6.

Table 20: Mobile country code element contents

Information element	Length	Value	Remark
Mobile country code	10	any	

4.3.5.5 Mobile network code

The mobile network code of a TETRA network. For a full definition see ETS 300 393-1 [1], clause 6.

Table 21: Mobile network code element contents

Information element	Length	Value	Remark
Mobile network code	14	any	

4.3.5.6 Mutual authentication flag

The Mutual Authentication Identifier is used to indicate whether or not the PDU is part of a mutual authentication exchange between the MS and RPDI.

Table 22: Mutual authentication flag element contents

Information element	Length	Value	Remark
Mutual Authentication flag	1	0	Mutual authentication = FALSE
		1	Mutual authentication = TRUE

4.3.5.7 PDU type

The PDU type indicates the MM PDU type for the authentication and OTAR PDUs. The PDU types in the following table are taken from the unused or security-reserved values of PDU type in the MM protocol. For more details, see ETS 300 393-2 [2], table 74.

Table 23: PDU type element contents

Information element	Length	Value	Downlink Assignment	Uplink Assignment
PDU Type	4	0000_2		U-AUTHENTICATION RESPONSE
		0001_2	D-AUTHENTICATION DEMAND	
		0010_2	D- AUTHENTICATION REJECT	
		0011_2	D-DISABLE	
		0100_2	D-ENABLE	U-AUTHENTICATION DEMAND
		0110_2		U-AUTHENTICATION RESULT
		1000_2	D- AUTHENTICATION RESPONSE	
		1001_2		U-TEI PROVIDE
		1011_2		U-DISABLE STATUS
		1110_2	D-AUTHENTICATION RESULT	U-AUTHENTICATION REJECT

NOTE: Values not shown on both uplink and downlink are assigned to other PDU types, which are given in ETS 300 393-2, [2], table 74.

4.3.5.8 Proprietary

Proprietary is an optional, variable length element and shall be used to send and receive proprietary defined information appended to the PDUs.

The use, size and structure of the Proprietary element is outside the scope of this standard.

4.3.5.9 Random challenge

The random challenge is an 80 bit number used as the input to the authentication algorithm, from which a response is calculated.

Table 24: Random challenge element contents

Information element	Length	Value	Remark
Random challenge [RAND1 or RAND2]	80	Any	

4.3.5.10 Reject cause

The reject cause element is defined in table 75 of ETS 300 393-2 [2] for the MM PDU, D-LOCATION UPDATE REJECT. The following table gives additional reject causes which are defined by the security protocol which is incremental upon the MM protocol.

Table 25: Reject cause element contents

Information element	Length	Value	Remark
Reject cause	5	00000_2 to 10001_2	Used for MM protocol -see ETS 300 393-2 [2], table 75.
		10010_2	Ciphering required
		10011_2	Authentication failure
		10100_2 to 11111_2	Reserved

4.3.5.11 Random seed

The random seed is an 80 bit number used as the input to the session key generation algorithm, which is used in the authentication and OTAR processes. Only one random seed is used per D-OTAR PDU, irrespective of the number of keys contained in the PDU. It is only provided from RPDI to MS.

Table 26: Random seed element contents

Information element	Length	Value	Remark
Random seed [RS]	80	Any	

4.3.5.12 Response value

The response value is the value returned by the challenged party, calculated from the random challenge.

Table 27: Response value element contents

Information element	Length	Value	Remark
Response Value [RES1 or RES2]	32	Any	

4.3.5.13 TEI

This is the terminal equipment identifier of the MS. For a full definition see ETS 300 393-1 [1], clause 6.

Table 28: TEI contents

Information element	Length	Value	Remark
Terminal equipment identifier	60	Any	

4.3.5.14 TEI information

This is the terminal equipment identifier and address extension of the MS. For a full definition see ETS 300 393-1 [1], clause 6.

Table 29: TEI information contents

Information Element	Length	Type	C/O/M	Remark
Terminal equipment identifier	60	1	M	
Address extension	24	1	M	

4.3.5.15 TEI request flag

This bit indicates whether the MS should supply the TEI.

Table 30: TEI request flag contents

Information element	Length	Value	Remark
TEI request flag	1	0	Do not supply TEI
		1	Supply TEI

4.3.5.16 Type 3 element identifier

The type 3 element identifier indicates the MM type 3 element to be used in the MM PDUs for authentication and OTAR purposes. The type 3 element identifiers in the following table are taken from the reserved values of type 3 element identifier defined in the MM protocol. For more details, see ETS 300 393-2 [1], table 80.

Table 31: Type 3 element identifier element contents

Information element	Length	Value	Remarks
Type 3 element identifier	4	0100_2	Proprietary
		1001_2	Authentication uplink
		1010_2	Authentication downlink
		1011_2	Reserved for any future specified type 3 element
		1100_2	Reserved for any future specified type 3 element
		1101_2	Reserved for any future specified type 3 element
		1110_2	Reserved for any future specified type 3 element
		1111_2	Reserved for any future specified type 3 element

4.4 Boundary conditions for the cryptographic algorithms and procedures

In the following the symbol |XYZ| shall be used to denote the length of the parameter XYZ. If the length of a parameter can vary, |XYZ| denotes the range between the shortest and the longest possible values for XYZ.

TA11: Shall be used to compute KS from K and RS. The algorithm shall have the following properties:

Input 1: Bit string of length |K|;
Input 2: Bit string of length |RS|;

Output: Bit string of length |KS|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known).

TA21: Shall be used to compute the KS' from K and RS. The algorithm shall have the following properties:

Input 1: Bit string of length |K|;
Input 2: Bit string of length |RS|;

Output: Bit string of length |KS'|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known).

The pair of algorithms TA11 and TA21 should be designed such that it is difficult to infer any information about the output of one algorithm from the knowledge of input 2 and the output of the other algorithm (even if details of the algorithms are known).

TA12P: Shall be used to compute (X)RES1 from KS and RAND1. The algorithm shall have the following properties:

Input 1: Bit string of length |KS|;
Input 2: Bit string of length |RAND1|;

Output 1: Bit string of length |(X)RES1|;

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and Output 1 (even if the details of the algorithm are known).

NOTE: Algorithm TA12P is equivalent to algorithm TA12 defined in ETS 300 392-7 [5], clause 4 with output 2 ignored.

TA22P: Shall be used to compute (X)RES2 from KS' and RAND2. The algorithm shall have the following properties:

Input 1: Bit string of length |KS'|;
Input 2: Bit string of length |RAND2|;

Output 1: Bit string of length |(X)RES2|;

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and Output 1 (even if the details of the algorithm are known).

NOTE: Algorithm TA22P is equivalent to algorithm TA22 defined in ETS 300 392-7 [5], clause 4 with output 2 ignored.

TB1: Shall be used to compute K from AC. The algorithm shall have the following properties:

Input: Bit string of length |AC|;

Output: Bit string of length |K|.

The algorithm should be designed such that the Output is dependent on every bit of the Input.

TB2: Shall be used to compute K from UAK. The algorithm shall have the following properties:

Input: Bit string of length |UAK|;

Output: Bit string of length |K|.

The algorithm should be designed such that the Output is dependent on every bit of the Input.

TB3: Shall be used to compute K from UAK and PIN. The algorithm shall have the following properties:

Input 1: Bit string of length |PIN|;
Input 2: Bit string of length |UAK|;

Output: Bit string of length |K|.

The algorithm should be designed such that the Output is dependent on every bit of both Inputs.

4.5 Dimensioning of the cryptographic parameters

Table 32 shows in summary form the length of each parameter used in the algorithms described in subclause 4.4.

Table 32: Dimensioning of cryptographic parameters

Abbreviation	No. of Bits
AC	16 - 32
GTSI	48
K	128
KS	128
KS'	128
PIN	16 - 32
RAND1	80
RAND2	80
RES1	32
RES2	32
RS	80
SSI	24
UAK	128
XRES1	32
XRES2	32

4.6 Summary of the cryptographic processes

Figure 17 gives a summary of the authentication mechanisms explained in the previous subclauses.

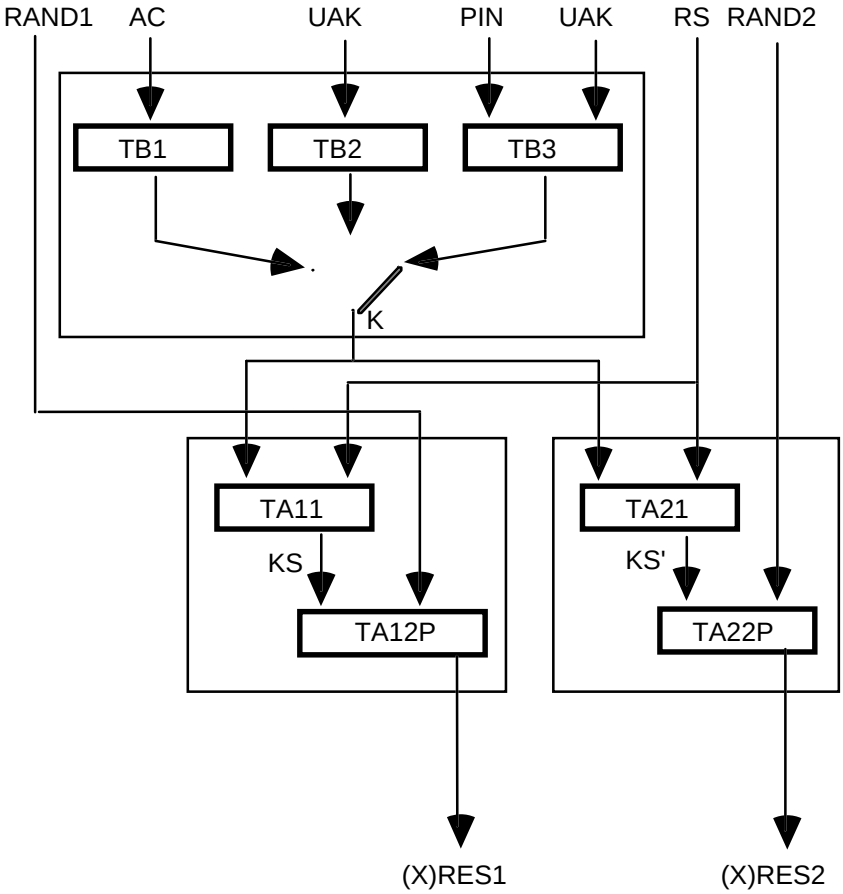


Figure 17: Overview of air interface authentication and key management

5 Secure Enable and Disable mechanism

5.1 General relationships

The relationship of user subscription, and the identifying identity, ITSI, and the hardware of the MS, identified by TEI, is shown in figure 18. The TEI is fixed and associated with the hardware of the MS. The user subscription, identified by ITSI, may be contained in a separable module. If ITSI is not contained in a separable module, it may still be changed by field programming equipment.

ITSI and TEI are described in ETS 300 393-1 [1], clause 6.

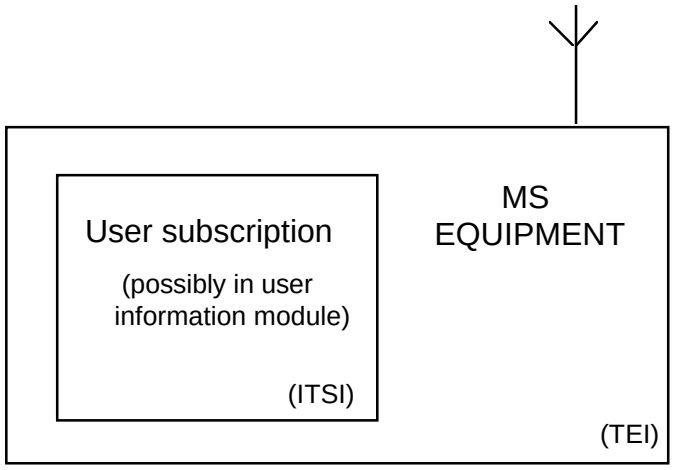


Figure 18: Relationship of TEI and ITSI in MS

5.2 Mechanisms

There are six possible transactions necessary for the enable/disable procedure which allow disable and enable of the MS equipment, the users' subscription, or both.

1. Disable of MS equipment.
2. Disable of MS subscription.
3. Disable an MS subscription and equipment.
4. Enable an MS equipment.
5. Enable an MS subscription.
6. Enable an MS equipment and subscription.

The state of the MS when either equipment or subscription are temporarily or permanently disabled shall follow the descriptions in ETS 300 393-2 [2], clause 15. Wherever the state of the MS is described as enabled or disabled in this subclause, the definition of operation in ETS 300 393-2 [2] shall apply. The mechanisms described in this sub clause shall replace those described in ETS 300 393-2 [2], clause 15.

The disable and enable mechanisms can be applied with or without authentication. Each MS should implement a disable and enable mechanism that requires the same level of security as that of its home RPDI. An MS should be disabled by a disable mechanism of equal or greater security to that in use in its home system, but should not be disabled by a lesser security mechanism. If the home RPDI of the MS employs authentication, the MS should not accept enable or disable requests without authentication.

There may be other mechanisms that withdraw service or disable the equipment that are outside the scope of this part of the ETS.

5.3 Service description and primitives

At the TNMM SAP a service shall be provided to indicate to the user application when the MS has been disabled or enabled. The primitives should be as follows:

TNMM-DISABLING Indication:

Used by MM to indicate to the user application that a temporary or permanent disabling of the MS is ordered.

TNMM-ENABLING indication:

Used by MM to indicate to the user application that the temporary disabling of the MS is cancelled.

The parameters of these primitives should be as shown in tables 33 and 34.

Table 33: Parameters for the primitive TNMM-DISABLING indication

Parameter	Indication
Enable/disable status	M

Table 34: Parameters for the primitive TNMM-ENABLING indication

Parameter	Indication
Enable/disable status	M

The parameter may take the following values:

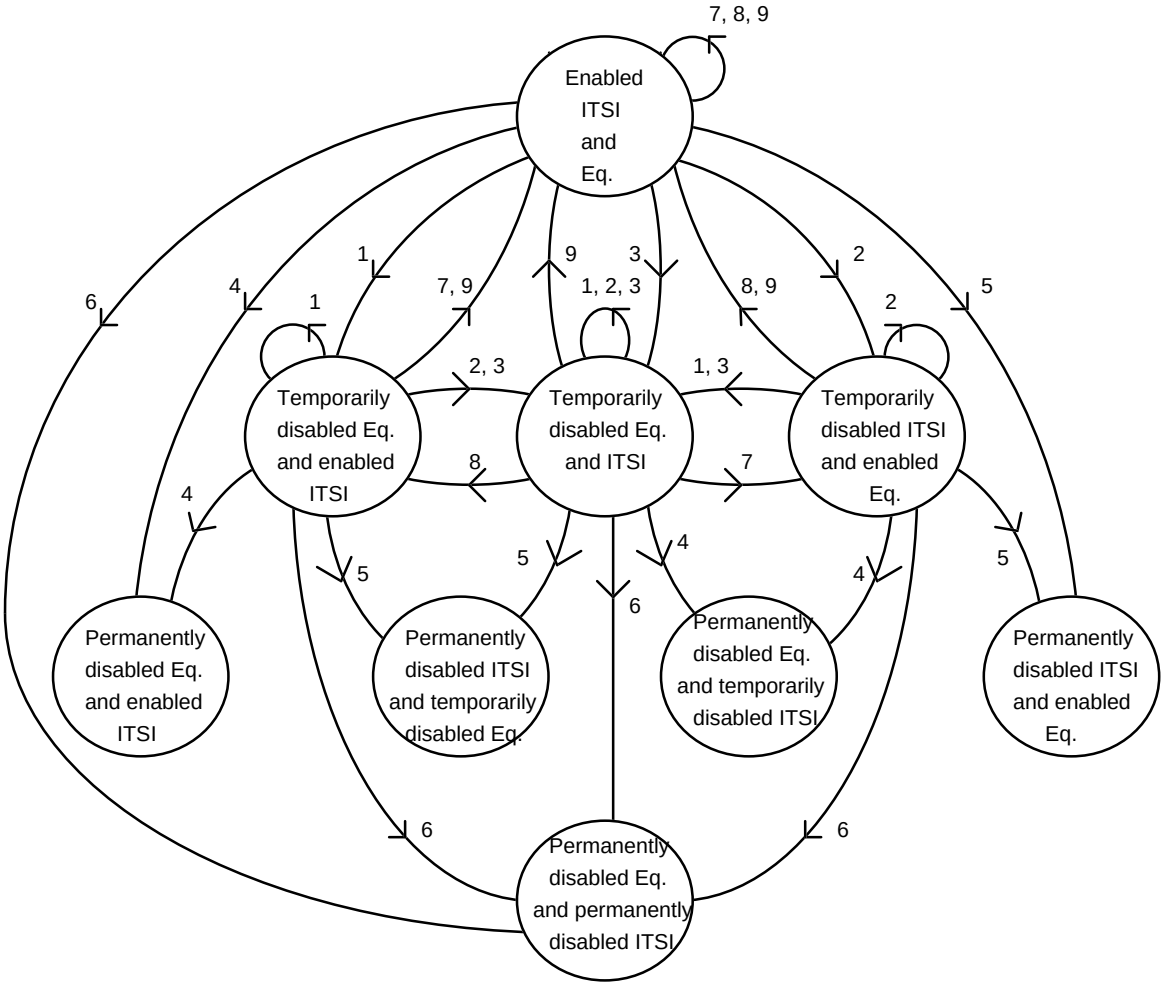
Enable/disable status =

Enabled;
Equipment temporary disabled;
Equipment permanently disabled;
Subscription temporary disabled;
Subscription permanently disabled;
Equipment and subscription temporary disabled;
Equipment and subscription permanently disabled.

5.4 Definition of enable-disable protocol

5.4.1 Enable/Disable state transitions

The state diagram in figure 19 shows all possible enabled and disabled states of one pair of MS equipment and ITSI. This diagram does not show state transitions due to separation of ITSI from, or fitting of ITSI into, an MS equipment.



1. temporary disabling of equipment
2. temporary disabling of ITSI
3. temporary disabling of equipment and ITSI
4. permanent disabling of equipment
5. permanent disabling of ITSI
6. permanent disabling of equipment and ITSI
7. enabling of equipment
8. enabling of ITSI
9. enabling of equipment and ITSI

Figure 19: State transitions of Enable/Disable mechanism

5.4.2 Overview of enable-disable protocol

The enable-disable protocol shall use the Mobility Management service of layer 3 in the TETRA PDO protocol stack.

The following pre-condition shall be satisfied for the protocol:

- RPDI shall know the ITSI/TEI binding

  NOTE 1: This may be obtained at registration.

The protocol shall be started with an "intent" message from RPDI to terminal. Where the RPDI supports authentication this shall include an authentication challenge. The MS should also authenticate the RPDI when possible to validate the instruction. The authentication protocol and PDUs are contained in clause 4. The protocol continues after completion of the authentication procedure with a "confirm" message from RPDI to terminal. The terminal shall then comply with the instruction (contained in the "intent" message).

The normal message exchanges shall be according to subclauses 5.4.2.1 and 5.4.2.2. In cases where authentication is not supported the U-DISABLE STATUS PDU shall be sent and encoded appropriately.

NOTE 2: In the MSCs the position of the primitives is given for information only.

5.4.2.1 Disabling an MS using authentication

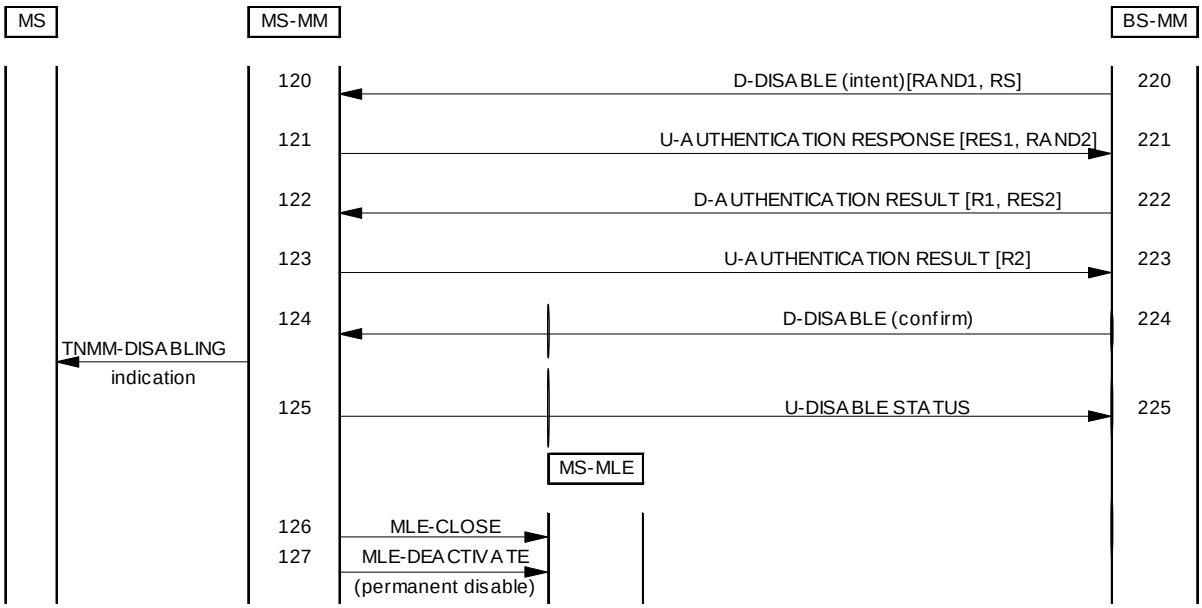


Figure 20: Disabling an MS with authentication

220 The RPDI shall send a D-DISABLE intent to the MS addressed by its ITSI. The "Equipment disable" and "Subscription disable" elements shall indicate whether the equipment or subscription or both are to be disabled. If the subscription is to be disabled, the "Address extension" element shall be present; and if the equipment is to be disabled, the "TEI" element shall be present. The D-DISABLE intent shall indicate whether the disabling is temporary or permanent by setting the "Disabling type" element appropriately. Since, in this case, the RPDI is configured to authenticate the MS before disabling, D-DISABLE intent shall also contain the "Authentication challenge" element to authenticate the MS.

120 If the TEI and/or address extension is included in D-DISABLE intent and they match those of the MS and, if authentication is supported by the MS, it shall then send a U-AUTHENTICATION RESPONSE to the RPDI containing the response to the RPDI's challenge. The MS should mutually authenticate the RPDI by including a random challenge in U-AUTHENTICATION RESPONSE.

If the TEI and/or address extension is included in D-DISABLE intent and either of these does not match those of the MS, the MS shall respond to D-DISABLE intent with U-DISABLE STATUS which shall indicate that the disabling attempt has failed due to mismatch of the TEI and/or address extension.

If authentication is not supported by the MS, it shall instead send U-AUTHENTICATION REJECT to the RPDI in response to D-DISABLE intent. The RPDI may then send D-DISABLE intent again, this time without the "Authentication challenge element" to attempt to disable the MS without authentication.

221/222 On receiving U-AUTHENTICATION RESPONSE, the RPDI shall send a D-AUTHENTICATION RESULT with the result of the RPDI's authentication of the MS. If the MS has requested mutual authentication, the RPDI shall also include its response to the MS challenge in D-AUTHENTICATION RESULT.

122/123 If mutual authentication is in progress, the MS shall send a U-AUTHENTICATION RESULT containing the result of the MS's authentication of the RPDI.

If the MS has not previously requested mutual authentication, and D-AUTHENTICATION RESULT indicates that the RPDI has successfully authenticated the MS, the MS shall send U-DISABLE STATUS to inform the RPDI of the result of the disable procedure, which should be successful if authentication was successful. If successful disabling is indicated in U-DISABLE STATUS, the TEI and address extension shall be included in this PDU.

223/224 If mutual authentication is in progress and U-AUTHENTICATION RESULT indicates that the MS authentication of the RPDI was successful, the RPDI shall send a D-DISABLE confirm PDU using the new encryption parameters to confirm the disabling command. D-DISABLE confirm shall include the same parameters as the previously sent D-DISABLE intent, except that D-DISABLE confirm shall not include an "Authentication challenge" element.

124/125 The MS shall reply with a U-DISABLE STATUS PDU (indicating that disabling was successful), in which it shall send its TEI together with the address extension to the RPDI. The "Equipment status" and "Subscription status" elements shall indicate the new state of the MS; note that it is possible that an MS already disabled by one means may subsequently be disabled by the other, hence these elements may not correspond to the desired status of the "Disable subscription" and "Disable equipment" elements in the D-DISABLE PDUs.

126 The MS shall then comply with the request, and disable itself, sending an MLE-CLOSE req. primitive from MM to MLE to prevent the MS from taking part in calls, and may send a TNMM-DISABLING ind primitive to the user application.

NOTE: Once temporarily disabled, the MS may still respond to further disable requests, for example to be disabled by TEI when already disabled by ITSI, or responding to a duplicate request. If permanently disabled, the MS shall not respond to further signalling.

127 If the MS is to be permanently disabled MS-MM shall send an MLE-DEACTIVATE primitive.

5.4.2.2 Enabling an MS using authentication

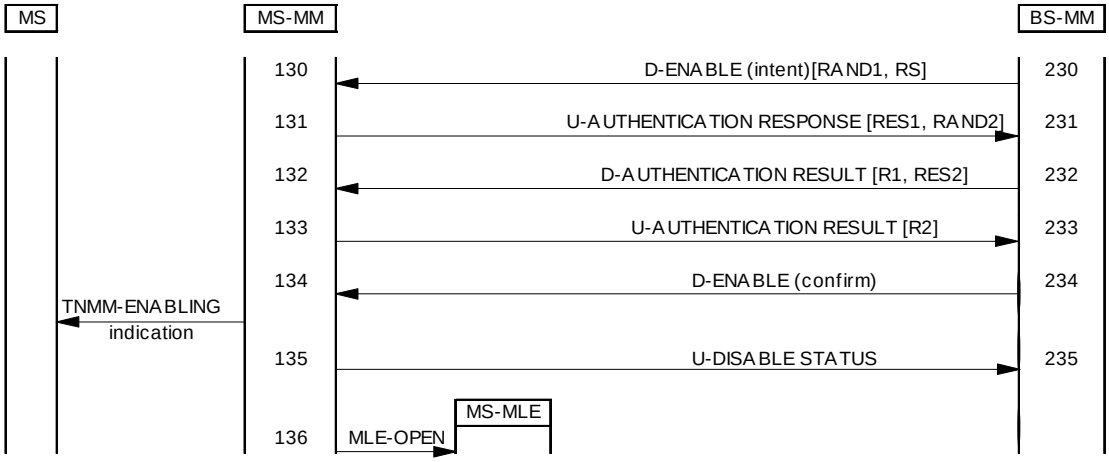


Figure 21: Enabling an MS with authentication

230 The RPDI shall send a D-ENABLE intent to the MS addressed by its ITSI. The "Equipment enable" and "Subscription enable" elements shall indicate whether the equipment or subscription is to be re-enabled, or both. If the subscription is to be enabled, the "Address extension" element shall be present; and if the equipment is to be enabled, the "TEI" element shall be present. An enable from permanent disable shall not be permitted as the MS may only be enabled after a temporary disabling. Since, in this case, the RPDI is configured to authenticate the MS before enabling, D-ENABLE intent shall also contain the "Authentication challenge" element to authenticate the MS.

130/131 If the TEI and/or address extension included in D-ENABLE intent match those of the MS and, if authentication is supported by the MS, it shall then send a U-AUTHENTICATION RESPONSE to the RPDI containing the response to the RPDI's challenge. The MS should also mutually authenticate the RPDI by including a random challenge in U-AUTHENTICATION RESPONSE.

If either the TEI and/or address extension included in D-ENABLE intent does not match those of the MS, the MS shall respond to D-ENABLE intent with U-DISABLE STATUS which shall indicate that the enabling attempt has failed due to mismatch of the TEI and/or address extension.

If authentication is not supported by the MS, it shall send U-AUTHENTICATION REJECT to the RPDI in response to D-ENABLE intent. The RPDI may then send D-ENABLE intent again, this time without the "Authentication challenge element" to attempt to enable the MS without authentication.

231/232 On receiving U-AUTHENTICATION RESPONSE, the RPDI shall send a D-AUTHENTICATION RESULT with the result of the RPDI's authentication of the MS. If the MS has requested mutual authentication, the RPDI shall also include its response to the MS challenge in D-AUTHENTICATION RESULT.

132/133 If mutual authentication is in progress, the MS shall then send a U-AUTHENTICATION RESULT containing the result of the MS's authentication of the RPDI.

If the MS has not previously requested mutual authentication, and D-AUTHENTICATION RESULT indicates that the RPDI has successfully authenticated the MS, the MS shall send U-DISABLE STATUS to inform the RPDI of the result of the enable procedure, which should be successful if authentication was successful. If successful enabling is indicated in U-DISABLE STATUS, the TEI and address extension shall be included in this PDU

233/234 If mutual authentication is in progress and U-AUTHENTICATION RESULT indicates that the MS authentication of the RPDI was successful, the RPDI shall then send a D-ENABLE confirm PDU using the new encryption parameters to confirm the enabling command. D-ENABLE confirm shall include the same parameters as the previously sent D-ENABLE intent, except that D-ENABLE confirm shall not include an "Authentication challenge" element.

134/135 The MS shall reply with U-DISABLE STATUS (indicating that enabling was successful), in which it shall include its TEI together with the address extension to the RPDI. The "Equipment status" and "Subscription status" elements shall indicate the new state of the MS which may or may not correspond to the requested status, depending whether the enabling corresponded to previous disabling or not.

136 If the both "status" elements had been set to indicate "enabled", the MS shall enable itself, sending an MLE-OPEN req. primitive from MM to MLE to enable the MS and sending a TNMM-ENABLING ind primitive to the user application to allow the application to be enabled also. If the enabling request did not correspond fully to a previous disabling, the "status" elements shall indicate that some disabling is not cleared, and the MLE shall not be opened.

5.4.3 MM PDUs structures and contents

The PDUs described here replace PDUs described in ETS 300 393-2 [2], table 74, as follows:

D-DISABLE and D-ENABLE retain the same type values, however the PDU structures shall change as described below.

U-DISABLE STATUS uses a previously reserved value (1011_2).

5.4.3.1 D-DISABLE

Message: D-DISABLE
Response to: -
Response expected: U-DISABLE STATUS or U-AUTHENTICATION RESPONSE
Short description: The message is sent by the Infrastructure to indicate that the mobile station shall be disabled (permanently or temporarily)

Table 35: D-DISABLE contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0011_2
Intent/Confirm	1	1	M	Intent or confirm
Disabling type	1	1	M	Temporary or permanent
Equipment disable	1	1	M	Disable equipment
TETRA Equipment Identity	60	1	C	Present if equipment disable = 1
Subscription disable	1	1	M	Disable subscription
Address Extension	24	1	C	Present if Subscription disable = 1
Authentication challenge	16 0	2	O	
Proprietary		3	O	

NOTE: The definition in table 35 replaces the definition of ETS 300 393-2 [2], table 47.

5.4.3.2 D-ENABLE

Message: D-ENABLE
Response to: -
Response expected: U-DISABLE STATUS or U-AUTHENTICATION RESPONSE
Short description: The message is sent by the Infrastructure to indicate that the mobile station shall be enabled after a disable.

Table 36: D-ENABLE contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	0100_2
Intent/Confirm	1	1	M	Intent or confirm
Equipment enable	1	1	M	Enable of equipment
TETRA Equipment Identity	60	1	C	Present if equipment enable = 1
Subscription enable	1	1	M	Enable of subscription
Address Extension	24	1	C	Present if Subscription disable =1
Authentication challenge	16 0	2	O	
Proprietary		3	O	

NOTE: The definition in table 36 replaces the definition of ETS 300 393-2 [2], table 48.

5.4.3.3 U-DISABLE STATUS

Message: U-DISABLE STATUS
Response to: D-DISABLE or D-ENABLE
Response expected: None
Short description: The message is sent by the mobile station to inform the infrastructure of its response to an enable or disable request and its resulting status.

Table 37: U-DISABLE STATUS contents

Information element	Length	Type	C/O/M	Remark
PDU Type	4	1	M	1011_2
Equipment status	2	1	M	Indicates disabled state of equipment
Subscription status	2	1	M	Indicates disabled state of subscription
Enable/Disable result	2	1	M	
Address Extension	24	1	C	Present only if enable/disable result = 000_2
TETRA Equipment Identity	60	1	C	Present only if enable/disable result = 000_2
Proprietary		3	O	

5.4.4 MM Information elements coding

5.4.4.1 Address extension

The Address Extension Element shall be used to indicate the extended part of TSI address.

Table 38: Address Extension element contents

Information sub element	Length	Type	Remark
Mobile Country Code (MCC)	10	1	
Mobile Network Code (MNC)	14	1	

5.4.4.2 Authentication challenge

The Authentication Challenge element shall contain the random seed and random challenge from the RPDI.

Table 39: Authentication challenge element contents

Information sub element	Length	Type	Remark
Random challenge RAND1	80	1	
Random seed RS	80	1	

5.4.4.3 Disabling type

The purpose of the Disabling Type element shall be to indicate which of the disabling types (i.e. temporary or permanent) is requested.

Table 40: Disabling Type element contents

Information element	Length	Value	Remark
Disabling Type	1	0	Temporary
		1	Permanent

5.4.4.4 Enable/disable result

The purpose of the enable/disable result element shall be to indicate whether or not enabling or disabling was successful.

Table 41: Enable/disable result element contents

Information element	Length	Value	Remark
Enable/disable result	3	000_2	enable/disable successful
		001_2	enable/disable failure, address extension mismatch
		010_2	enable/disable failure, TEI mismatch
		011_2	enable/disable failure, TEI and address extension mismatch
		100_2	enable/disable failure, authentication is required
		others	reserved

5.4.4.5 Equipment disable

The purpose of the equipment disable element shall be to indicate whether the equipment is to be disabled.

Table 42: Equipment disable element contents

Information element	Length	Value	Remark
Equipment disable	1	0	Equipment not to be disabled
		1	Equipment to be disabled

5.4.4.6 Equipment enable

The purpose of the Equipment enable element shall be to indicate whether the equipment is to be enabled.

Table 43: Equipment enable element contents

Information element	Length	Value	Remark
Equipment enable	1	0	Equipment not to be enabled
		1	Equipment to be enabled

5.4.4.7 Equipment status

The purpose of the Equipment status element shall be to indicate the enabled or disabled state of the equipment.

Table 44: Equipment status element contents

Information element	Length	Value	Remark
Equipment status	2	00_2	Equipment enabled
		01_2	Equipment temporarily disabled
		10_2	Equipment permanently disabled
		11_2	Reserved

5.4.4.8 Intent/confirm

The purpose of the Intent/confirm element shall be to indicate whether the enable or disable command is the first intent, always used with or without authentication, or the confirmation once successful authentication has been carried out.

Table 45: Intent/confirm element contents

Information element	Length	Value	Remark
Intent/confirm	1	0	Intent
		1	Confirm

5.4.4.9 PDU Type

The PDU type. (The table modifies the definitions given in ETS 300 393-2 [2], table 74).

Table 46: PDU Type element contents

Information element	Length	Value	Downlink Assignment	Uplink Assignment
PDU Type	4	0011_2	D-DISABLE	
		0100_2	D-ENABLE	
		1011_2		U-DISABLE STATUS

NOTE: Values not shown on both uplink and downlink are assigned to other PDU types, which are given in ETS 300 393-2, [2], table 74.

5.4.4.10 Proprietary

Proprietary is an optional, variable length element and shall be used to send and receive proprietary defined information appended to the PDUs.

The use, the size and the structure of the Proprietary element is outside the scope of this ETS.

5.4.4.11 Subscription disable

The purpose of the Subscription disable element shall be to indicate whether the subscription is to be disabled.

Table 47: Subscription disable element contents

Information element	Length	Value	Remark
Subscription disable	1	0	Subscription not to be disabled
		1	Subscription to be disabled

5.4.4.12 Subscription enable

The purpose of the Subscription enable element shall be to indicate whether the subscription is to be enabled.

Table 48: Subscription enable element contents

Information element	Length	Value	Remark
Subscription enable	1	0	Subscription not to be enabled
		1	Subscription to be enabled

5.4.4.13 Subscription status

The purpose of the Subscription status element shall be to indicate the enabled or disabled state of the subscription.

Table 49: Subscription status element contents

Information element	Length	Value	Remark
Subscription status	2	00_2	Subscription enabled
		01_2	Subscription temporarily disabled
		10_2	Subscription permanently disabled
		11_2	Reserved

5.4.4.14 TETRA equipment identity

The TETRA Equipment Identity element shall be used to indicate the TETRA Equipment Identity (TEI).

Table 50: TETRA Equipment Identity element contents

Information element	Length	Value	Remark
TETRA Equipment Identity	60		See ETS 300 393-1 [1] subclause 6

History

Document history			
July 1996	Public Enquiry	PE110:	1996-07-22 to 1996-11-15
February 1997	Vote	V 9717:	1997-02-25 to 1997-04-25