

# ETSI TS 100 392-7 V4.2.1 (2026-04)



## Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security

Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

---

**Reference**

---

RTS/TCCE-06227

---

---

**Keywords**

---

security, TETRA, V+D

---

**ETSI**

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex - FRANCE

---

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

Siret N° 348 623 562 00017 - APE 7112B  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° w061004871

---

**Important notice**

---

The present document can be downloaded from the  
[ETSI Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#) repository.

Users should be aware that the present document may be revised or have its status changed,  
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to  
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our  
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

---

**Notice of disclaimer & limitation of liability**

---

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

---

**Copyright Notification**

---

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2026.  
All rights reserved.

# Contents

|                                                                          |    |
|--------------------------------------------------------------------------|----|
| Intellectual Property Rights .....                                       | 12 |
| Foreword.....                                                            | 12 |
| Modal verbs terminology.....                                             | 13 |
| 1 Scope .....                                                            | 14 |
| 2 References .....                                                       | 14 |
| 2.1 Normative references .....                                           | 14 |
| 2.2 Informative references.....                                          | 15 |
| 3 Definition of terms, symbols and abbreviations.....                    | 16 |
| 3.1 Terms.....                                                           | 16 |
| 3.2 Symbols.....                                                         | 20 |
| 3.3 Abbreviations .....                                                  | 20 |
| 4 Air Interface authentication and key management mechanisms .....       | 23 |
| 4.a General .....                                                        | 23 |
| 4.0 Security classes .....                                               | 24 |
| 4.1 Air interface authentication mechanisms .....                        | 24 |
| 4.1.1 Overview .....                                                     | 24 |
| 4.1.1a Authentication and key management algorithms.....                 | 25 |
| 4.1.2 Authentication of an MS.....                                       | 25 |
| 4.1.3 Authentication of the infrastructure .....                         | 28 |
| 4.1.4 Mutual authentication of MS and infrastructure .....               | 30 |
| 4.1.5 The authentication key.....                                        | 35 |
| 4.1.6 Equipment authentication .....                                     | 35 |
| 4.1.6a Request for information related to an MS.....                     | 36 |
| 4.1.7 Authentication of an MS when migrated .....                        | 36 |
| 4.1.8 Authentication of the home SwMI when migrated.....                 | 39 |
| 4.1.9 Mutual Authentication of MS and infrastructure when migrated ..... | 41 |
| 4.2 Air Interface key management mechanisms.....                         | 41 |
| 4.2.0 General.....                                                       | 41 |
| 4.2.1 The Derived Cipher Key.....                                        | 42 |
| 4.2.1.1 DCK and DCKX overview .....                                      | 42 |
| 4.2.1.2 DCK derivation .....                                             | 42 |
| 4.2.1.3 DCKX derivation .....                                            | 42 |
| 4.2.1.4 Usage of DCK and DCKX.....                                       | 43 |
| 4.2.1.5 Validity of DCK and DCKX.....                                    | 43 |
| 4.2.2 The Group Cipher Key .....                                         | 43 |
| 4.2.2.0 General.....                                                     | 43 |
| 4.2.2.0a Validity of GCK and GCKX.....                                   | 44 |
| 4.2.2.0b Distribution of GCK.....                                        | 44 |
| 4.2.2.0c Distribution of GCKX.....                                       | 44 |
| 4.2.2.0d Decryption of sealed GCK and GCKX.....                          | 45 |
| 4.2.2.0e Summary of GCK distribution process .....                       | 45 |
| 4.2.2.1 Session key modifiers GCK0 and GCKX0 .....                       | 47 |
| 4.2.3 The Common Cipher Key.....                                         | 47 |
| 4.2.3.1 CCK and CCKX usage.....                                          | 47 |
| 4.2.3.2 CCK and CCKX identification .....                                | 48 |
| 4.2.3.3 CCK and CCKX distribution .....                                  | 48 |
| 4.2.3.4 CCK and CCKX validity .....                                      | 49 |
| 4.2.4 The Static Cipher Key.....                                         | 49 |
| 4.2.4.0 General.....                                                     | 49 |
| 4.2.4.0a SCK sets.....                                                   | 50 |
| 4.2.4.0b SCK and SCKX identification .....                               | 50 |
| 4.2.4.0c Distribution of SCK .....                                       | 50 |
| 4.2.4.0d Distribution of SCKX .....                                      | 51 |
| 4.2.4.0e Decryption of sealed SCK and SCKX .....                         | 51 |

|           |                                                                                                                |     |
|-----------|----------------------------------------------------------------------------------------------------------------|-----|
| 4.2.4.0f  | Summary of SCK distribution process .....                                                                      | 51  |
| 4.2.4.1   | SCK association for DMO use .....                                                                              | 54  |
| 4.2.4.1.0 | General .....                                                                                                  | 54  |
| 4.2.4.1.1 | DMO SCK subset grouping.....                                                                                   | 54  |
| 4.2.5     | The Group Session Key for OTAR.....                                                                            | 57  |
| 4.2.5.0   | General .....                                                                                                  | 57  |
| 4.2.5.0a  | Validity of GSKO and GSKOX .....                                                                               | 57  |
| 4.2.5.0b  | Distribution of GSKO and GSKOX.....                                                                            | 58  |
| 4.2.5.1   | SCK and SCKX distribution to groups with OTAR .....                                                            | 59  |
| 4.2.5.2   | GCK and GCKX distribution to groups with OTAR .....                                                            | 60  |
| 4.2.5.3   | Rules for MS response to group key distribution .....                                                          | 60  |
| 4.2.5a    | OTAR of migrated MS .....                                                                                      | 60  |
| 4.2.5a.1  | Visited Session Keys for OTAR .....                                                                            | 60  |
| 4.2.5a.2  | Derivation of KSOv .....                                                                                       | 60  |
| 4.2.5a.3  | Derivation of KSOXv .....                                                                                      | 61  |
| 4.2.5a.4  | OTAR of CKX to migrated MS where home SwMI supports an air interface encryption algorithm from TEA set A ..... | 62  |
| 4.2.5a.5  | OTAR of CK to migrated MS where home SwMI supports an air interface encryption algorithm from TEA set B .....  | 63  |
| 4.2.6     | Encrypted Short Identity (ESI) mechanism .....                                                                 | 63  |
| 4.2.7     | Encryption Cipher Key .....                                                                                    | 65  |
| 4.2.8     | Summary of AI key management mechanisms.....                                                                   | 66  |
| 4.3       | Service description and primitives .....                                                                       | 68  |
| 4.3.1     | Authentication primitives .....                                                                                | 68  |
| 4.3.2     | Static Cipher Key transfer primitives.....                                                                     | 69  |
| 4.3.3     | Group Cipher Key transfer primitives .....                                                                     | 70  |
| 4.3.4     | Group Session Key for OTAR transfer primitives.....                                                            | 71  |
| 4.4       | Authentication protocol.....                                                                                   | 71  |
| 4.4.1     | Authentication state transitions.....                                                                          | 71  |
| 4.4.2     | Authentication protocol sequences and operations .....                                                         | 74  |
| 4.4.2.0   | General .....                                                                                                  | 74  |
| 4.4.2.1   | MSCs for authentication .....                                                                                  | 76  |
| 4.4.2.2   | MSCs for authentication and security type-3 elements.....                                                      | 82  |
| 4.4.2.3   | Control of authentication timer T354 at MS .....                                                               | 86  |
| 4.4a      | Information request protocol .....                                                                             | 87  |
| 4.5       | OTAR protocols .....                                                                                           | 90  |
| 4.5.1     | Common Cipher Key delivery - protocol functions.....                                                           | 90  |
| 4.5.1.0   | General .....                                                                                                  | 90  |
| 4.5.1.1   | SwMI-initiated CCK and CCKX provision .....                                                                    | 91  |
| 4.5.1.2   | MS-initiated CCK provision with U-OTAR CCK DEMAND.....                                                         | 93  |
| 4.5.1.3   | MS-initiated CCK or CCKX provision with announced cell reselection.....                                        | 93  |
| 4.5.2     | OTAR protocol functions - Static Cipher Key.....                                                               | 94  |
| 4.5.2.0   | General .....                                                                                                  | 94  |
| 4.5.2.1   | MS requests provision of SCK(s) or SCKX(s).....                                                                | 95  |
| 4.5.2.2   | SwMI provides SCK(s) or SCKX(s) to individual MS .....                                                         | 97  |
| 4.5.2.3   | SwMI provides SCK(s) or SCKX(s) to group of MSs .....                                                          | 98  |
| 4.5.2.4   | SwMI rejects provision of SCK or SCKX .....                                                                    | 99  |
| 4.5.3     | OTAR protocol functions - Group Cipher Key.....                                                                | 100 |
| 4.5.3.0   | General .....                                                                                                  | 100 |
| 4.5.3.1   | MS requests provision of GCK or GCKX.....                                                                      | 100 |
| 4.5.3.2   | SwMI provides GCK or GCKX to an individual MS .....                                                            | 102 |
| 4.5.3.3   | SwMI provides GCK or GCKX to a group of MSs .....                                                              | 103 |
| 4.5.3.4   | SwMI rejects provision of GCK or GCKX .....                                                                    | 105 |
| 4.5.4     | Cipher key association to group address.....                                                                   | 105 |
| 4.5.4.0   | General .....                                                                                                  | 105 |
| 4.5.4.1   | Static Cipher Key association for DMO.....                                                                     | 105 |
| 4.5.4.2   | Group Cipher Key association .....                                                                             | 108 |
| 4.5.5     | Notification of key change over the air.....                                                                   | 110 |
| 4.5.5.0   | General .....                                                                                                  | 110 |
| 4.5.5.1   | Change of Derived Cipher Key.....                                                                              | 111 |
| 4.5.5.2   | Change of Common Cipher Key .....                                                                              | 112 |
| 4.5.5.3   | Change of Group Cipher Key.....                                                                                | 112 |

|          |                                                                                                  |     |
|----------|--------------------------------------------------------------------------------------------------|-----|
| 4.5.5.4  | Change of Static Cipher Key for TMO .....                                                        | 112 |
| 4.5.5.5  | Change of Static Cipher Key for DMO.....                                                         | 112 |
| 4.5.5.6  | Synchronization of Cipher Key Change .....                                                       | 113 |
| 4.5.5.7  | Change of identity encryption algorithm.....                                                     | 113 |
| 4.5.6    | Security class change .....                                                                      | 113 |
| 4.5.6.0  | General .....                                                                                    | 113 |
| 4.5.6.1  | Change of security class to security class 1 .....                                               | 114 |
| 4.5.6.2  | Change of security class to security class 2 .....                                               | 114 |
| 4.5.6.3  | Change of security class to security class 3 .....                                               | 115 |
| 4.5.6.4  | Change of security class to security class 3 with GCK or GCKX.....                               | 115 |
| 4.5.7    | Notification of key in use.....                                                                  | 115 |
| 4.5.8    | Notification of GCK or GCKX Activation/Deactivation.....                                         | 115 |
| 4.5.9    | Deletion of SCK/SCKX, GCK/GCKX and GSKO/GSKOX .....                                              | 115 |
| 4.5.10   | Air Interface Key Status Enquiry.....                                                            | 118 |
| 4.5.11   | Crypto management group.....                                                                     | 120 |
| 4.5.12   | OTAR retry mechanism.....                                                                        | 121 |
| 4.5.13   | OTAR protocol functions - Group Session Key for OTAR.....                                        | 122 |
| 4.5.13.0 | General .....                                                                                    | 122 |
| 4.5.13.1 | MS requests provision of GSKO or GSKOX.....                                                      | 122 |
| 4.5.13.2 | SwMI provides GSKO or GSKOX to an MS.....                                                        | 123 |
| 4.5.13.3 | SwMI rejects provision of GSKO or GSKOX .....                                                    | 123 |
| 4.5.14   | OTAR protocol functions - interaction and queuing.....                                           | 123 |
| 4.5.15   | Session Key for OTAR operations in visited SwMI.....                                             | 124 |
| 4.5.15.1 | General .....                                                                                    | 124 |
| 4.5.15.2 | Home and visited SwMI use air interface encryption algorithms from the same algorithm set.....   | 124 |
| 4.5.15.3 | Home and visited SwMI use air interface encryption algorithms from different algorithm sets..... | 127 |
| 4.5.16   | Transfer of AI cipher keys across the ISI .....                                                  | 129 |
| 5        | Enable and disable mechanism.....                                                                | 129 |
| 5.0      | General .....                                                                                    | 129 |
| 5.1      | General relationships .....                                                                      | 129 |
| 5.2      | Enable/disable state transitions.....                                                            | 130 |
| 5.3      | Mechanisms.....                                                                                  | 131 |
| 5.3.0    | General.....                                                                                     | 131 |
| 5.3.1    | Disable of MS equipment .....                                                                    | 132 |
| 5.3.2    | Disable of a subscription.....                                                                   | 132 |
| 5.3.3    | Disable of subscription and equipment.....                                                       | 132 |
| 5.3.4    | Enable an MS equipment .....                                                                     | 132 |
| 5.3.5    | Enable an MS subscription .....                                                                  | 132 |
| 5.3.6    | Enable an MS equipment and subscription.....                                                     | 132 |
| 5.4      | Enable/disable protocol .....                                                                    | 133 |
| 5.4.1    | General case.....                                                                                | 133 |
| 5.4.2    | Status of cipher key material.....                                                               | 134 |
| 5.4.2.1  | Permanently disabled state .....                                                                 | 134 |
| 5.4.2.2  | Temporarily disabled state .....                                                                 | 134 |
| 5.4.3    | Specific protocol exchanges .....                                                                | 135 |
| 5.4.3.0  | General .....                                                                                    | 135 |
| 5.4.3.1  | Disabling an MS with mutual authentication .....                                                 | 135 |
| 5.4.3.2  | Enabling an MS with mutual authentication .....                                                  | 136 |
| 5.4.3.3  | Enabling an MS with non-mutual authentication.....                                               | 137 |
| 5.4.3.4  | Disabling an MS with non-mutual authentication.....                                              | 139 |
| 5.4.4    | Enabling an MS without authentication.....                                                       | 140 |
| 5.4.5    | Disabling an MS without authentication.....                                                      | 140 |
| 5.4.6    | Rejection of enable or disable command .....                                                     | 140 |
| 5.4.6a   | Expiry of Enable/Disable protocol timer .....                                                    | 141 |
| 5.4.7    | MM service primitives.....                                                                       | 141 |
| 5.4.7.0  | General .....                                                                                    | 141 |
| 5.4.7.1  | TNMM-DISABLING primitive.....                                                                    | 142 |
| 5.4.7.2  | TNMM-ENABLING primitive.....                                                                     | 142 |
| 6        | Air Interface (AI) encryption .....                                                              | 142 |
| 6.1      | General principles.....                                                                          | 142 |

|           |                                                                          |     |
|-----------|--------------------------------------------------------------------------|-----|
| 6.2       | Security class .....                                                     | 143 |
| 6.2.a     | General .....                                                            | 143 |
| 6.2.0     | Notification of security class .....                                     | 144 |
| 6.2.0.0   | General .....                                                            | 144 |
| 6.2.0.1   | Security class of neighbouring Cells .....                               | 145 |
| 6.2.0.2   | Identification of MS security capabilities .....                         | 145 |
| 6.2.1     | Constraints on LA arising from cell class .....                          | 145 |
| 6.3       | Key Stream Generator (KSG) .....                                         | 146 |
| 6.3.0     | General .....                                                            | 146 |
| 6.3.1     | KSG numbering and selection .....                                        | 146 |
| 6.3.2     | Interface parameters .....                                               | 147 |
| 6.3.2.0   | General .....                                                            | 147 |
| 6.3.2.0a  | IV validity .....                                                        | 148 |
| 6.3.2.1   | Initial Value (IV) for algorithms in TEA set A .....                     | 148 |
| 6.3.2.2   | Cipher Key for algorithms in TEA set A .....                             | 149 |
| 6.3.2.3   | Initial Value (IV) for algorithms in TEA set B .....                     | 149 |
| 6.3.2.4   | Cipher Key for algorithms in TEA set B .....                             | 150 |
| 6.4       | Encryption mechanism .....                                               | 151 |
| 6.4.0     | General .....                                                            | 151 |
| 6.4.1     | Allocation of KSS to logical channels .....                              | 151 |
| 6.4.2     | Allocation of KSS to logical channels .....                              | 152 |
| 6.4.2.1   | General .....                                                            | 152 |
| 6.4.2.2   | KSS allocation on phase modulation channels .....                        | 153 |
| 6.4.2.3   | KSS allocation on QAM channels for algorithms in TEA set A .....         | 157 |
| 6.4.2.3.0 | General .....                                                            | 157 |
| 6.4.2.3.1 | Fixed mapping .....                                                      | 157 |
| 6.4.2.3.2 | Offset mapping .....                                                     | 158 |
| 6.4.2.4   | KSS allocation on QAM channels for algorithms in TEA set B .....         | 159 |
| 6.4.3     | Synchronization of data calls where data is multi-slot interleaved ..... | 161 |
| 6.4.4     | Recovery of stolen frames from interleaved data .....                    | 161 |
| 6.5       | Use of cipher keys .....                                                 | 162 |
| 6.5.0     | General .....                                                            | 162 |
| 6.5.1     | Identification of encryption state of downlink MAC PDUs .....            | 163 |
| 6.5.1.0   | General .....                                                            | 163 |
| 6.5.1.1   | Class 1 cells .....                                                      | 163 |
| 6.5.1.2   | Class 2 cells .....                                                      | 164 |
| 6.5.1.3   | Class 3 cells .....                                                      | 164 |
| 6.5.2     | Identification of encryption state of uplink MAC PDUs .....              | 164 |
| 6.6       | Mobility procedures .....                                                | 165 |
| 6.6.1     | General requirements .....                                               | 165 |
| 6.6.1.0   | Common requirements .....                                                | 165 |
| 6.6.1.1   | Additional requirements for class 3 systems .....                        | 165 |
| 6.6.2     | Protocol description .....                                               | 165 |
| 6.6.2.0   | General .....                                                            | 165 |
| 6.6.2.1   | Negotiation of ciphering parameters .....                                | 165 |
| 6.6.2.1.0 | General .....                                                            | 165 |
| 6.6.2.1.1 | Class 1 cells .....                                                      | 166 |
| 6.6.2.1.2 | Class 2 cells .....                                                      | 166 |
| 6.6.2.1.3 | Class 3 cells .....                                                      | 166 |
| 6.6.2.2   | Initial and undeclared cell re-selection .....                           | 166 |
| 6.6.2.3   | Unannounced cell re-selection .....                                      | 168 |
| 6.6.2.4   | Announced cell re-selection type-3 .....                                 | 169 |
| 6.6.2.5   | Announced cell re-selection type-2 .....                                 | 169 |
| 6.6.2.6   | Announced cell re-selection type-1 .....                                 | 169 |
| 6.6.2.7   | Key forwarding .....                                                     | 169 |
| 6.6.3     | Shared channels .....                                                    | 170 |
| 6.7       | Encryption control .....                                                 | 171 |
| 6.7.0     | General .....                                                            | 171 |
| 6.7.1     | Data to be encrypted .....                                               | 171 |
| 6.7.1.1   | Downlink control channel requirements .....                              | 171 |
| 6.7.1.2   | Encryption of MAC header elements .....                                  | 171 |
| 6.7.1.2a  | MAC Address Encryption mechanism for KSGs in TEA set B .....             | 172 |

|            |                                                                         |     |
|------------|-------------------------------------------------------------------------|-----|
| 6.7.1.2a.1 | Usage of MAC Address Encryption mechanism .....                         | 172 |
| 6.7.1.2a.2 | MAE operation .....                                                     | 172 |
| 6.7.1.2a.3 | Addresses to be encrypted .....                                         | 173 |
| 6.7.1.3    | Traffic channel encryption control .....                                | 174 |
| 6.7.1.4    | Handling of PDUs that do not conform to negotiated ciphering mode ..... | 174 |
| 6.7.2      | Service description and primitives .....                                | 174 |
| 6.7.2.0    | General .....                                                           | 174 |
| 6.7.2.1    | Mobility Management (MM) .....                                          | 175 |
| 6.7.2.2    | Mobile Link Entity (MLE) .....                                          | 176 |
| 6.7.2.3    | Layer 2 .....                                                           | 178 |
| 6.7.3      | Protocol functions .....                                                | 178 |
| 6.7.3.0    | General .....                                                           | 178 |
| 6.7.3.1    | MM .....                                                                | 178 |
| 6.7.3.2    | MLE .....                                                               | 178 |
| 6.7.3.3    | LLC .....                                                               | 179 |
| 6.7.3.4    | MAC .....                                                               | 179 |
| 6.7.4      | PDUs for cipher negotiation .....                                       | 179 |

## **Annex A (normative): PDU and element definitions .....180**

|         |                                                        |     |
|---------|--------------------------------------------------------|-----|
| A.0     | General .....                                          | 180 |
| A.1     | Authentication PDUs .....                              | 180 |
| A.1.1   | D-AUTHENTICATION DEMAND .....                          | 180 |
| A.1.2   | D-AUTHENTICATION REJECT .....                          | 180 |
| A.1.3   | D-AUTHENTICATION RESPONSE .....                        | 181 |
| A.1.4   | D-AUTHENTICATION RESULT .....                          | 181 |
| A.1.5   | U-AUTHENTICATION DEMAND .....                          | 181 |
| A.1.6   | U-AUTHENTICATION REJECT .....                          | 182 |
| A.1.7   | U-AUTHENTICATION RESPONSE .....                        | 182 |
| A.1.8   | U-AUTHENTICATION RESULT .....                          | 183 |
| A.2     | OTAR PDUs .....                                        | 183 |
| A.2.1   | D-OTAR CCK PROVIDE .....                               | 183 |
| A.2.1a  | D-OTAR CCKX PROVIDE .....                              | 183 |
| A.2.2   | U-OTAR CCK DEMAND .....                                | 184 |
| A.2.3   | U-OTAR CCK RESULT .....                                | 184 |
| A.2.4   | D-OTAR GCK PROVIDE .....                               | 185 |
| A.2.4a  | D-OTAR GCKX PROVIDE .....                              | 186 |
| A.2.5   | U-OTAR GCK DEMAND .....                                | 186 |
| A.2.6   | U-OTAR GCK RESULT .....                                | 187 |
| A.2.6a  | D-OTAR GCK REJECT .....                                | 187 |
| A.2.7   | D-OTAR SCK PROVIDE .....                               | 188 |
| A.2.7a  | D-OTAR SCKX PROVIDE .....                              | 189 |
| A.2.8   | U-OTAR SCK DEMAND .....                                | 189 |
| A.2.9   | U-OTAR SCK RESULT .....                                | 190 |
| A.2.9a  | D-OTAR SCK REJECT .....                                | 190 |
| A.2.10  | D-OTAR GSKO PROVIDE .....                              | 191 |
| A.2.10a | D-OTAR GSKOX PROVIDE .....                             | 191 |
| A.2.11  | U-OTAR GSKO DEMAND .....                               | 192 |
| A.2.12  | U-OTAR GSKO RESULT .....                               | 192 |
| A.2.12a | D-OTAR GSKO REJECT .....                               | 193 |
| A.3     | PDUs for key association to GTSI .....                 | 193 |
| A.3.1   | D-OTAR KEY ASSOCIATE DEMAND .....                      | 193 |
| A.3.2   | U-OTAR KEY ASSOCIATE STATUS .....                      | 194 |
| A.4     | PDUs to synchronize key or security class change ..... | 195 |
| A.4.1   | D-CK CHANGE DEMAND .....                               | 195 |
| A.4.2   | U-CK CHANGE RESULT .....                               | 196 |
| A.4.2a  | Void .....                                             | 196 |
| A.4.2b  | Void .....                                             | 196 |
| A.4.3   | D-DM-SCK ACTIVATE DEMAND .....                         | 196 |
| A.4.4   | U-DM-SCK ACTIVATE RESULT .....                         | 197 |

|          |                                                 |     |
|----------|-------------------------------------------------|-----|
| A.4a     | PDUs to delete air interface keys in MS .....   | 198 |
| A.4a.1   | D-OTAR KEY DELETE DEMAND .....                  | 198 |
| A.4a.2   | U-OTAR KEY DELETE RESULT .....                  | 198 |
| A.4b     | PDUs to obtain Air Interface Key Status .....   | 199 |
| A.4b.1   | D-OTAR KEY STATUS DEMAND .....                  | 199 |
| A.4b.2   | U-OTAR KEY STATUS RESPONSE .....                | 200 |
| A.5      | Other security domain PDUs .....                | 201 |
| A.5.1    | U-TEI PROVIDE .....                             | 201 |
| A.5.2    | U-OTAR PREPARE .....                            | 202 |
| A.5.3    | D-OTAR NEWCELL .....                            | 202 |
| A.5.3a   | D-OTAR NEWCELL-X .....                          | 202 |
| A.5.4    | D-OTAR CMG GTSI PROVIDE .....                   | 203 |
| A.5.5    | U-OTAR CMG GTSI RESULT .....                    | 204 |
| A.5.6    | U-INFORMATION PROVIDE .....                     | 204 |
| A.6      | PDUs for Enable and Disable .....               | 206 |
| A.6.1    | D-DISABLE .....                                 | 206 |
| A.6.2    | D-ENABLE .....                                  | 206 |
| A.6.3    | U-DISABLE STATUS .....                          | 207 |
| A.7      | MM PDU type 3 information elements coding ..... | 207 |
| A.7.0    | General .....                                   | 207 |
| A.7.1    | Authentication downlink .....                   | 207 |
| A.7.2    | Authentication uplink .....                     | 208 |
| A.7.3    | Security downlink .....                         | 208 |
| A.8      | PDU Information elements coding .....           | 210 |
| A.8.0    | General .....                                   | 210 |
| A.8.1    | Acknowledgement flag .....                      | 210 |
| A.8.1a   | Additional information present .....            | 210 |
| A.8.1b   | Additional security .....                       | 210 |
| A.8.2    | Address extension .....                         | 210 |
| A.8.2a   | AI algorithm information present .....          | 211 |
| A.8.2b   | AI algorithm information request flag .....     | 211 |
| A.8.3    | Authentication challenge .....                  | 211 |
| A.8.4    | Authentication reject reason .....              | 211 |
| A.8.5    | Authentication result .....                     | 211 |
| A.8.6    | Authentication sub-type .....                   | 212 |
| A.8.7    | CCK identifier .....                            | 212 |
| A.8.8    | CCK information .....                           | 212 |
| A.8.9    | CCK Location area information .....             | 213 |
| A.8.9a   | CCK provision flag .....                        | 213 |
| A.8.10   | CCK request flag .....                          | 213 |
| A.8.11   | Change of security class .....                  | 213 |
| A.8.12   | Ciphering parameters .....                      | 214 |
| A.8.13   | CK provision flag .....                         | 214 |
| A.8.14   | CK provision information .....                  | 214 |
| A.8.15   | CK request flag .....                           | 215 |
| A.8.16   | Class Change flag .....                         | 215 |
| A.8.17   | DCK forwarding result .....                     | 215 |
| A.8.18   | Disabling type .....                            | 215 |
| A.8.19   | Enable/Disable result .....                     | 216 |
| A.8.20   | Encryption mode .....                           | 216 |
| A.8.20.1 | Class 1 cells .....                             | 216 |
| A.8.20.2 | Class 2 cells .....                             | 216 |
| A.8.20.3 | Class 3 cells .....                             | 216 |
| A.8.21   | Equipment disable .....                         | 217 |
| A.8.22   | Equipment enable .....                          | 217 |
| A.8.23   | Equipment status .....                          | 217 |
| A.8.23a  | Explicit response .....                         | 217 |
| A.8.24   | Frame number .....                              | 217 |

|         |                                                  |     |
|---------|--------------------------------------------------|-----|
| A.8.24a | Future information present .....                 | 218 |
| A.8.25  | Future key flag .....                            | 218 |
| A.8.26  | GCK data.....                                    | 218 |
| A.8.27  | GCK key and identifier .....                     | 218 |
| A.8.27a | GCKX key and identifier .....                    | 218 |
| A.8.28  | GCK Number (GCKN) .....                          | 219 |
| A.8.28a | GCK Provision result .....                       | 219 |
| A.8.28b | GCK rejected.....                                | 219 |
| A.8.29  | GCK select number .....                          | 219 |
| A.8.29a | GCK Supported.....                               | 220 |
| A.8.30  | GCK Version Number (GCK-VN).....                 | 220 |
| A.8.31  | Group association .....                          | 220 |
| A.8.31a | Group Identity Security Related Information..... | 221 |
| A.8.32  | GSKO Version Number (GSKO-VN).....               | 221 |
| A.8.33  | GSSI.....                                        | 221 |
| A.8.33a | HW SW version request flag.....                  | 221 |
| A.8.33b | HW version number present.....                   | 222 |
| A.8.34  | Hyperframe number .....                          | 222 |
| A.8.34a | Identity encryption .....                        | 222 |
| A.8.35  | Intent/confirm.....                              | 222 |
| A.8.36  | Void.....                                        | 222 |
| A.8.37  | Key association status .....                     | 223 |
| A.8.38  | Key association type.....                        | 223 |
| A.8.39  | Key change type .....                            | 223 |
| A.8.39a | Key delete type.....                             | 223 |
| A.8.39b | Key status type .....                            | 224 |
| A.8.39c | Key delete extension .....                       | 224 |
| A.8.40  | Key type flag .....                              | 224 |
| A.8.41  | KSG-number .....                                 | 225 |
| A.8.42  | Location area .....                              | 225 |
| A.8.43  | Location area bit mask .....                     | 225 |
| A.8.44  | Location area selector.....                      | 225 |
| A.8.45  | Location area list .....                         | 226 |
| A.8.46  | Location area range .....                        | 226 |
| A.8.46a | Max response timer value.....                    | 226 |
| A.8.47  | Mobile country code.....                         | 226 |
| A.8.48  | Mobile network code.....                         | 226 |
| A.8.48a | Model number information present .....           | 227 |
| A.8.48b | Model number request flag.....                   | 227 |
| A.8.49  | Multiframe number.....                           | 227 |
| A.8.50  | Mutual authentication flag.....                  | 227 |
| A.8.51  | Network time.....                                | 227 |
| A.8.52  | Number of GCKs changed .....                     | 227 |
| A.8.52a | Number of GCKs deleted .....                     | 228 |
| A.8.52b | Number of GCK status .....                       | 228 |
| A.8.52c | Number of GCKs provided .....                    | 228 |
| A.8.52d | Number of GCKs rejected.....                     | 229 |
| A.8.52e | Number of GCKs requested by GCKN .....           | 229 |
| A.8.52f | Number of GCKs requested by GSSI.....            | 229 |
| A.8.53  | Number of groups.....                            | 230 |
| A.8.53a | Number of GSKO status.....                       | 230 |
| A.8.53b | Number of KSGs present .....                     | 230 |
| A.8.54  | Number of location areas .....                   | 230 |
| A.8.55  | Number of SCKs changed.....                      | 231 |
| A.8.55a | Number of SCKs deleted.....                      | 231 |
| A.8.56  | Number of SCKs provided .....                    | 231 |
| A.8.56a | Number of SCKs rejected.....                     | 231 |
| A.8.57  | Number of SCKs requested .....                   | 232 |
| A.8.57a | Number of SCK status.....                        | 232 |
| A.8.57b | OTAR reject reason.....                          | 233 |
| A.8.57c | OTAR retry interval .....                        | 233 |
| A.8.58  | OTAR sub-type .....                              | 233 |

|         |                                                      |     |
|---------|------------------------------------------------------|-----|
| A.8.58a | OTAR extension.....                                  | 234 |
| A.8.59  | PDU type.....                                        | 234 |
| A.8.60  | Proprietary.....                                     | 235 |
| A.8.61  | Provision result.....                                | 235 |
| A.8.62  | Random challenge.....                                | 235 |
| A.8.63  | Random seed.....                                     | 235 |
| A.8.64  | Random seed for OTAR.....                            | 236 |
| A.8.65  | Void.....                                            | 236 |
| A.8.65a | Reject reason.....                                   | 236 |
| A.8.66  | Response value.....                                  | 236 |
| A.8.67  | SCK data.....                                        | 236 |
| A.8.68  | SCK information.....                                 | 237 |
| A.8.69  | SCK key and identifier.....                          | 237 |
| A.8.69a | SCKX key and identifier.....                         | 237 |
| A.8.70  | SCK Number (SCKN).....                               | 237 |
| A.8.71  | SCK number and result.....                           | 238 |
| A.8.72  | SCK provision flag.....                              | 238 |
| A.8.72a | Void.....                                            | 238 |
| A.8.72b | SCK rejected.....                                    | 238 |
| A.8.73  | SCK select number.....                               | 239 |
| A.8.73a | SCK subset grouping type.....                        | 239 |
| A.8.73b | SCK subset number.....                               | 240 |
| A.8.74  | SCK use.....                                         | 240 |
| A.8.75  | SCK version number.....                              | 240 |
| A.8.76  | Sealed CCK, Sealed SCK, Sealed GCK, Sealed GSKO..... | 240 |
| A.8.76a | Sealed CCKX, Sealed SCKX, Sealed GCKX.....           | 241 |
| A.8.76b | Sealed GSKOX.....                                    | 241 |
| A.8.77  | Security information element.....                    | 241 |
| A.8.77a | Security parameters.....                             | 243 |
| A.8.77b | Security related information element.....            | 243 |
| A.8.78  | Session key.....                                     | 243 |
| A.8.79  | Slot Number.....                                     | 244 |
| A.8.80  | SSI.....                                             | 244 |
| A.8.81  | Subscription disable.....                            | 244 |
| A.8.82  | Subscription enable.....                             | 244 |
| A.8.83  | Subscription status.....                             | 244 |
| A.8.83a | SW version number present.....                       | 245 |
| A.8.84  | TEI.....                                             | 245 |
| A.8.85  | TEI request flag.....                                | 245 |
| A.8.86  | Time type.....                                       | 246 |
| A.8.87  | Type 3 element identifier.....                       | 246 |

**Annex B (normative):      Boundary conditions for the cryptographic algorithms and procedures .....247**

|     |                                                   |     |
|-----|---------------------------------------------------|-----|
| B.0 | General.....                                      | 247 |
| B.1 | Dimensioning of the cryptographic parameters..... | 256 |
| B.2 | Summary of the cryptographic processes.....       | 258 |

**Annex C (normative):      Timers .....271**

|     |                                                                              |     |
|-----|------------------------------------------------------------------------------|-----|
| C.1 | T354, authentication protocol timer.....                                     | 271 |
| C.2 | T371, delay timer for group addressed delivery of SCK/SCKX and GCK/GCKX..... | 271 |
| C.3 | T372, key forwarding timer.....                                              | 271 |
| C.4 | T355, disable control timer.....                                             | 271 |

**Annex D (informative):      Transition between air interface encryption algorithms in TEA set A and TEA set B .....272**

|     |               |     |
|-----|---------------|-----|
| D.1 | Overview..... | 272 |
|-----|---------------|-----|

|                               |                                                                                                  |            |
|-------------------------------|--------------------------------------------------------------------------------------------------|------------|
| D.2                           | Algorithm support .....                                                                          | 273        |
| D.2.1                         | General .....                                                                                    | 273        |
| D.2.2                         | SwMI dependencies .....                                                                          | 273        |
| D.2.3                         | MSs able to support more than one algorithm.....                                                 | 274        |
| D.2.4                         | MSs only able to support one algorithm.....                                                      | 274        |
| D.3                           | Group and broadcast communication during transition .....                                        | 275        |
| D.3.1                         | Group communication.....                                                                         | 275        |
| D.3.2                         | Broadcast communications.....                                                                    | 275        |
| D.4                           | Transition scenarios for TMO .....                                                               | 275        |
| D.4.1                         | Transition overview.....                                                                         | 275        |
| D.4.2                         | Phase 1: Encryption class while loading the new authentication algorithm and K2 keys to MSs..... | 276        |
| D.4.3                         | Phase 2: Encryption during transition to Set B.....                                              | 278        |
| D.4.4                         | Phase 3: Identity Encryption using MAE .....                                                     | 279        |
| D.5                           | Transition scenarios for DMO.....                                                                | 279        |
| D.5.1                         | General .....                                                                                    | 279        |
| D.5.2                         | MS to MS DMO operation .....                                                                     | 279        |
| D.5.3                         | DMO repeater operation.....                                                                      | 280        |
| D.5.4                         | DMO gateway operation .....                                                                      | 280        |
| <b>Annex E (informative):</b> | <b>Bibliography.....</b>                                                                         | <b>281</b> |
| <b>Annex F (informative):</b> | <b>Change request history.....</b>                                                               | <b>282</b> |
| History .....                 |                                                                                                  | 283        |

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

# Intellectual Property Rights

## Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the [ETSI IPR online database](#).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

## Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™**, **LTE™** and **5G™** logo are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

# Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

The present document is part 7 of a multi-part deliverable covering the Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D), Release 2, as identified below:

- Part 1: "General network design";
- Part 2: "Air Interface (AI)";
- Part 3: "Interworking at the Inter-System Interface (ISI)";
- Part 4: "Gateways basic operation";
- Part 5: "Peripheral Equipment Interface (PEI)";
- Part 7: "Security";**
- Part 9: "General requirements for supplementary services";
- Part 10: "Supplementary services stage 1";
- Part 11: "Supplementary services stage 2";
- Part 12: "Supplementary services stage 3";
- Part 13: "SDL model of the Air Interface (AI)";
- Part 14: "Protocol Implementation Conformance Statement (PICS) proforma specification";
- Part 15: "TETRA frequency bands, duplex spacings and channel numbering";
- Part 16: "Network Performance Metrics";

Part 17: "TETRA V+D and DMO specifications";

Part 18: "Air interface optimized applications";

Part 19: "Interworking between TETRA and Broadband systems".

NOTE 1: Part 3, sub-parts 6 and 7 (Speech format implementation), part 4, sub-part 3 (Data networks gateway), part 10, sub-part 15 (Transfer of control), part 13 (SDL) and part 14 (PICS) of this multi-part deliverable are in status "historical" and are not maintained.

NOTE 2: Some parts are also published as Technical Specifications such as ETSI TS 100 392-2 and those may be the latest version of the document.

---

## Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

# Sample Document

get full document from [standards.iteh.ai](https://standards.iteh.ai)

---

# 1 Scope

The present document defines the Terrestrial Trunked Radio system (TETRA) supporting Voice plus Data (V+D). It specifies the air interface, the inter-working between TETRA systems and to other systems via gateways, the terminal equipment interface on the mobile station, the connection of line stations to the infrastructure, the security aspects in TETRA networks, the management services offered to the operator, the performance objectives, and the supplementary services that come in addition to the basic and teleservices.

The present part describes the security mechanisms in TETRA V+D. It provides mechanisms for confidentiality of control signalling and user speech and data at the air interface, authentication and key management mechanisms for the air interface and for the Inter-System Interface (ISI).

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

- authentication of an MS by the TETRA infrastructure;
- authentication of the TETRA infrastructure by an MS;
- mutual authentication of MS and TETRA infrastructure.

The key management mechanisms specified in clause 4 enable the provision of key material for the air interface encryption mechanisms specified in clause 6.

Clause 5 describes the mechanisms and protocol for enable and disable of both the mobile station equipment and the mobile station user's subscription.

Air interface encryption may be provided as an option in TETRA. Where employed, clause 6 describes the confidentiality mechanisms using encryption on the air interface, for circuit mode speech, circuit mode data, packet data and control information. Clause 6 describes both encryption mechanisms and mobility procedures. It also details the protocol concerning control of encryption at the air interface. Encryption mechanisms and control protocol are specified for two different air interface encryption algorithm sets.

Annex A specifies the Protocol Data Units and Information Elements required to fulfil the protocols specified in clauses 4, 5 and 6. Annex B specifies boundary conditions, dimensioning and summaries of the cryptographic algorithms, parameters and processes specified in the present document. Annex C specifies timer values used within the protocols. Annex D provides considerations for a transition process between the usage of encryption algorithms from different air interface encryption algorithm sets.

The present document does not address the detail handling of protocol errors or any protocol mechanisms when TETRA is operating in a degraded mode. These issues are implementation specific and therefore fall outside the scope of the TETRA standardization effort.

The detail description of the Authentication Centre is outside the scope of the present document.

---

## 2 References

### 2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found in the [ETSI docbox](https://standards.iteh.ai/catalog/standards/etsi/33481f4f-a391-4eec-9759-836fbb031ac1/etsi-ts-100-392-7-v4-2-1-2026-04).

NOTE 1: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

NOTE 2: Note that for the TETRA standards, the reference is always to a European Standard (ETSI EN 300 xxx) if such has been published, but the latest version of that standard can be either an EN or a Technical Specification (ETSI TS 100 xxx), even if this is not visible in the reference list.

The following referenced documents are necessary for the application of the present document.

- [1] [ETSI EN 300 392-1](#): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 1: General network design".
- [2] [ETSI EN 300 392-2](#): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".
- [3] [ISO 7498-2](#): "Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture".
- [4] [ETSI EN 300 812-3](#): "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (SIM-ME) interface; Part 3: Integrated Circuit (IC); Physical, logical and TSIM application characteristics".
- [5] [ETSI EN 300 396-6](#): "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".
- [6] [ETSI EN 302 109](#): "Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption".
- [7] [ETSI EN 300 392-12-22](#): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 12: Supplementary services stage 3; Sub-part 22: Dynamic Group Number Assignment (DGNA)".
- [8] [ETSI EN 300 392-3-5](#): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-System Interface (ISI); Sub-part 5: Additional Network Feature for Mobility Management (ANF-ISIMM)".
- [9] [ETSI EN 300 396-1](#): "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".
- [10] [ETSI ES 200 812-2](#): "Terrestrial Trunked Radio (TETRA); Subscriber Identity Module to Mobile Equipment (TSIM-ME) interface; Part 2: Universal Integrated Circuit Card (UICC); Characteristics of the TSIM application".

## 2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE 1: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

NOTE 2: Note that for the TETRA standards, the reference is always to a European Standard (ETSI EN 300 xxx) if such has been published, but the latest version of that standard can be either an EN or a Technical Specification (ETSI TS 100 xxx), even if this is not visible in the reference list.

The following referenced documents may be useful in implementing an ETSI deliverable or add to the reader's understanding, but are not required for conformance to the present document.

- [i.1] ETSI ETS 300 392-2 (1996): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 2: Air Interface (AI)".
- [i.2] ETSI ETS 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [i.3] ETSI ETR 086-3: "Trans European Trunked Radio (TETRA) systems; Technical requirements specification; Part 3: Security aspects".