

ETSI EN 300 392-7 V3.2.1 (2010-06)

European Standard (Telecommunications series)

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
<https://standards.iteh.ai/catalog/standards/sist/3bc1b660-557f-45e5-9b16-9d60843e2e58/etsi-en-300-392-7-v3.2.1-2010-06>



Reference

REN/TETRA-06179

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 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at

<http://portal.etsi.org/tb/status/status.asp>

If you find errors in the present document, please send your comment to one of the following services:

http://portal.etsi.org/chaicor/ETSI_support.asp

Copyright Notification

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

© European Telecommunications Standards Institute 2010.
All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™**, **TIPHON™**, the TIPHON logo and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.

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

LTE™ is a Trade Mark of ETSI currently being registered

for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

| | |
|--|----|
| Intellectual Property Rights | 10 |
| Foreword..... | 10 |
| 1 Scope | 12 |
| 2 References | 12 |
| 2.1 Normative references | 12 |
| 2.2 Informative references..... | 13 |
| 3 Definitions and abbreviations..... | 13 |
| 3.1 Definitions | 13 |
| 3.2 Abbreviations | 16 |
| 4 Air Interface authentication and key management mechanisms | 18 |
| 4.0 Security classes | 18 |
| 4.1 Air interface authentication mechanisms | 19 |
| 4.1.1 Overview | 19 |
| 4.1.2 Authentication of an MS..... | 19 |
| 4.1.3 Authentication of the infrastructure | 20 |
| 4.1.4 Mutual authentication of MS and infrastructure | 21 |
| 4.1.5 The authentication key..... | 23 |
| 4.1.6 Equipment authentication | 23 |
| 4.1.7 Authentication of an MS when migrated | 24 |
| 4.1.8 Authentication of the home SwMI when migrated..... | 24 |
| 4.1.9 Mutual Authentication of MS and infrastructure when migrated..... | 25 |
| 4.2 Air Interface key management mechanisms..... | 26 |
| 4.2.1 The DCK..... | 26 |
| 4.2.2 The GCK..... | 27 |
| 4.2.2.1 Session key modifier GCK0..... | 28 |
| 4.2.3 The CCK..... | 28 |
| 4.2.4 The SCK | 29 |
| 4.2.4.1 SCK association for DMO use..... | 31 |
| 4.2.4.1.1 DMO SCK subset grouping..... | 31 |
| 4.2.5 The GSKO | 34 |
| 4.2.5.1 SCK distribution to groups with OTAR..... | 35 |
| 4.2.5.2 GCK distribution to groups with OTAR..... | 35 |
| 4.2.5.3 Rules for MS response to group key distribution..... | 36 |
| 4.2.6 Encrypted Short Identity (ESI) mechanism | 36 |
| 4.2.7 Encryption Cipher Key | 37 |
| 4.2.8 Summary of AI key management mechanisms..... | 37 |
| 4.3 Service description and primitives | 39 |
| 4.3.1 Authentication primitives | 39 |
| 4.3.2 SCK transfer primitives | 39 |
| 4.3.3 GCK transfer primitives..... | 40 |
| 4.3.4 GSKO transfer primitives | 41 |
| 4.4 Authentication protocol..... | 42 |
| 4.4.1 Authentication state transitions..... | 42 |
| 4.4.2 Authentication protocol sequences and operations | 45 |
| 4.4.2.1 MSCs for authentication | 46 |
| 4.4.2.2 MSCs for authentication Type-3 element | 52 |
| 4.4.2.3 Control of authentication timer T354 at MS | 55 |
| 4.5 OTAR protocols | 56 |
| 4.5.1 CCK delivery - protocol functions..... | 56 |
| 4.5.1.1 SwMI-initiated CCK provision | 56 |
| 4.5.1.2 MS-initiated CCK provision with U-OTAR CCK demand..... | 58 |
| 4.5.1.3 MS-initiated CCK provision with announced cell reselection | 59 |
| 4.5.2 OTAR protocol functions - SCK | 59 |
| 4.5.2.1 MS requests provision of SCK(s)..... | 60 |
| 4.5.2.2 SwMI provides SCK(s) to individual MS | 61 |

| | | |
|----------|---|-----|
| 4.5.2.3 | SwMI provides SCK(s) to group of MSs | 64 |
| 4.5.2.4 | SwMI rejects provision of SCK | 66 |
| 4.5.3 | OTAR protocol functions - GCK | 66 |
| 4.5.3.1 | MS requests provision of GCK | 66 |
| 4.5.3.2 | SwMI provides GCK to an individual MS | 69 |
| 4.5.3.3 | SwMI provides GCK to a group of MSs | 71 |
| 4.5.3.4 | SwMI rejects provision of GCK | 73 |
| 4.5.4 | Cipher key association to group address | 73 |
| 4.5.4.1 | SCK association for DMO | 74 |
| 4.5.4.2 | GCK association | 78 |
| 4.5.5 | Notification of key change over the air | 80 |
| 4.5.5.1 | Change of DCK | 82 |
| 4.5.5.2 | Change of CCK | 82 |
| 4.5.5.3 | Change of GCK | 82 |
| 4.5.5.4 | Change of SCK for TMO | 82 |
| 4.5.5.5 | Change of SCK for DMO | 83 |
| 4.5.5.6 | Synchronization of Cipher Key Change | 83 |
| 4.5.6 | Security class change | 83 |
| 4.5.6.1 | Change of security class to security class 1 | 84 |
| 4.5.6.2 | Change of security class to security class 2 | 84 |
| 4.5.6.3 | Change of security class to security class 3 | 84 |
| 4.5.6.4 | Change of security class to security class 3 with GCK | 85 |
| 4.5.7 | Notification of key in use | 85 |
| 4.5.8 | Notification of GCK Activation/Deactivation | 85 |
| 4.5.9 | Deletion of SCK, GCK and GSKO | 85 |
| 4.5.10 | Air Interface Key Status Enquiry | 87 |
| 4.5.11 | Crypto management group | 90 |
| 4.5.12 | OTAR retry mechanism | 90 |
| 4.5.13 | OTAR protocol functions - GSKO | 91 |
| 4.5.13.1 | MS requests provision of GSKO | 91 |
| 4.5.13.2 | SwMI provides GSKO to an MS | 92 |
| 4.5.13.3 | SwMI rejects provision of GSKO | 93 |
| 4.5.14 | OTAR protocol functions - interaction and queuing | 93 |
| 4.5.15 | KSOv for OTAR operations in visited SwMI | 93 |
| 4.5.16 | Transfer of AI cipher keys across the ISI | 97 |
| 5 | Enable and disable mechanism | 97 |
| 5.1 | General relationships | 98 |
| 5.2 | Enable/disable state transitions | 98 |
| 5.3 | Mechanisms | 99 |
| 5.3.1 | Disable of MS equipment | 100 |
| 5.3.2 | Disable of an subscription | 100 |
| 5.3.3 | Disable of subscription and equipment | 100 |
| 5.3.4 | Enable an MS equipment | 100 |
| 5.3.5 | Enable an MS subscription | 100 |
| 5.3.6 | Enable an MS equipment and subscription | 100 |
| 5.4 | Enable/disable protocol | 101 |
| 5.4.1 | General case | 101 |
| 5.4.2 | Status of cipher key material | 102 |
| 5.4.2.1 | Permanently disabled state | 102 |
| 5.4.2.2 | Temporarily disabled state | 102 |
| 5.4.3 | Specific protocol exchanges | 103 |
| 5.4.3.1 | Disabling an MS with mutual authentication | 103 |
| 5.4.3.2 | Enabling an MS with mutual authentication | 105 |
| 5.4.3.3 | Enabling an MS with non-mutual authentication | 106 |
| 5.4.3.4 | Disabling an MS with non-mutual authentication | 107 |
| 5.4.4 | Enabling an MS without authentication | 108 |
| 5.4.5 | Disabling an MS without authentication | 109 |
| 5.4.6 | Rejection of enable or disable command | 109 |
| 5.4.6a | Expiry of Enable/Disable protocol timer | 110 |
| 5.4.7 | MM service primitives | 111 |
| 5.4.7.1 | TNMM-DISABLING primitive | 111 |

| | | |
|-----------------------------|--|------------|
| 5.4.7.2 | TNMM-ENABLING primitive | 111 |
| 6 | Air Interface (AI) encryption | 111 |
| 6.1 | General principles..... | 111 |
| 6.2 | Security class..... | 112 |
| 6.2.0 | Notification of security class | 113 |
| 6.2.0.1 | Security Class of Neighbouring Cells | 113 |
| 6.2.0.2 | Identification of MS security capabilities | 113 |
| 6.2.1 | Constraints on LA arising from cell class | 114 |
| 6.3 | Key Stream Generator (KSG) | 114 |
| 6.3.1 | KSG numbering and selection | 114 |
| 6.3.2 | Interface parameters..... | 115 |
| 6.3.2.1 | Initial Value (IV)..... | 115 |
| 6.3.2.2 | Cipher Key | 115 |
| 6.4 | Encryption mechanism | 116 |
| 6.4.1 | Allocation of KSS to logical channels | 116 |
| 6.4.2 | Allocation of KSS to logical channels with PDU association | 118 |
| 6.4.2.1 | General | 118 |
| 6.4.2.2 | KSS allocation on phase modulation channels..... | 118 |
| 6.4.2.3 | KSS allocation on QAM channels | 120 |
| 6.4.2.3.1 | Fixed mapping | 120 |
| 6.4.2.3.2 | Offset mapping | 121 |
| 6.4.3 | Synchronization of data calls where data is multi-slot interleaved | 122 |
| 6.4.4 | Recovery of stolen frames from interleaved data | 123 |
| 6.5 | Use of cipher keys | 123 |
| 6.5.1 | Identification of encryption state of downlink MAC PDUs | 124 |
| 6.5.1.1 | Class 1 cells..... | 124 |
| 6.5.1.2 | Class 2 cells..... | 125 |
| 6.5.1.3 | Class 3 cells..... | 125 |
| 6.5.2 | Identification of encryption state of uplink MAC PDUs | 125 |
| 6.6 | Mobility procedures | 126 |
| 6.6.1 | General requirements | 126 |
| 6.6.1.1 | Additional requirements for class 3 systems | 126 |
| 6.6.2 | Protocol description | 126 |
| 6.6.2.1 | Negotiation of ciphering parameters..... | 126 |
| 6.6.2.1.1 | Class 1 cells | 126 |
| 6.6.2.1.2 | Class 2 cells | 127 |
| 6.6.2.1.3 | Class 3 cells | 127 |
| 6.6.2.2 | Initial and undeclared cell re-selection..... | 127 |
| 6.6.2.3 | Unannounced cell re-selection | 128 |
| 6.6.2.4 | Announced cell re-selection type-3..... | 129 |
| 6.6.2.5 | Announced cell re-selection type-2..... | 129 |
| 6.6.2.6 | Announced cell re-selection type-1 | 129 |
| 6.6.2.7 | Key forwarding | 129 |
| 6.7 | Encryption control..... | 131 |
| 6.7.1 | Data to be encrypted | 131 |
| 6.7.1.1 | Downlink control channel requirements | 131 |
| 6.7.1.2 | Encryption of MAC header elements | 131 |
| 6.7.1.3 | Traffic channel encryption control..... | 131 |
| 6.7.1.4 | Handling of PDUs that do not conform to negotiated ciphering mode | 132 |
| 6.7.2 | Service description and primitives | 132 |
| 6.7.2.1 | Mobility Management (MM) | 133 |
| 6.7.2.2 | Mobile Link Entity (MLE)..... | 133 |
| 6.7.2.3 | Layer 2 | 135 |
| 6.7.3 | Protocol functions | 135 |
| 6.7.3.1 | MM | 135 |
| 6.7.3.2 | MLE | 135 |
| 6.7.3.3 | LLC | 135 |
| 6.7.3.4 | MAC | 136 |
| 6.7.4 | PDUs for cipher negotiation | 136 |
| Annex A (normative): | PDU and element definitions | 137 |

| | | |
|---------|--|-----|
| A.1 | Authentication PDUs..... | 137 |
| A.1.1 | D-AUTHENTICATION demand..... | 137 |
| A.1.2 | D-AUTHENTICATION reject..... | 137 |
| A.1.3 | D-AUTHENTICATION response..... | 138 |
| A.1.4 | D-AUTHENTICATION result..... | 138 |
| A.1.5 | U-AUTHENTICATION demand..... | 138 |
| A.1.6 | U-AUTHENTICATION reject..... | 139 |
| A.1.7 | U-AUTHENTICATION response..... | 139 |
| A.1.8 | U-AUTHENTICATION result..... | 140 |
| A.2 | OTAR PDUs | 140 |
| A.2.1 | D-OTAR CCK Provide | 140 |
| A.2.2 | U-OTAR CCK Demand | 140 |
| A.2.3 | U-OTAR CCK Result | 141 |
| A.2.4 | D-OTAR GCK Provide | 141 |
| A.2.5 | U-OTAR GCK Demand | 142 |
| A.2.6 | U-OTAR GCK Result | 143 |
| A.2.6a | D-OTAR GCK Reject | 143 |
| A.2.7 | D-OTAR SCK Provide..... | 144 |
| A.2.8 | U-OTAR SCK Demand..... | 145 |
| A.2.9 | U-OTAR SCK Result..... | 145 |
| A.2.9a | D-OTAR SCK Reject..... | 146 |
| A.2.10 | D-OTAR GSKO Provide..... | 146 |
| A.2.11 | U-OTAR GSKO Demand | 147 |
| A.2.12 | U-OTAR GSKO Result..... | 147 |
| A.2.12a | D-OTAR GSKO Reject..... | 147 |
| A.3 | PDUs for key association to GTSI | 148 |
| A.3.1 | D-OTAR KEY ASSOCIATE demand | 148 |
| A.3.2 | U-OTAR KEY ASSOCIATE status | 149 |
| A.4 | PDUs to synchronize key or security class change | 149 |
| A.4.1 | D-CK CHANGE demand..... | 149 |
| A.4.2 | U-CK CHANGE result..... | 150 |
| A.4.2a | U-OTAR KEY DELETE result..... | 151 |
| A.4.2b | U-OTAR KEY STATUS response..... | 152 |
| A.4.3 | D-DM-SCK ACTIVATE DEMAND..... | 153 |
| A.4.4 | U-DM-SCK ACTIVATE RESULT | 154 |
| A.4a | PDUs to delete air interface keys in MS | 155 |
| A.4a.1 | D-OTAR KEY DELETE demand..... | 155 |
| A.4a.2 | U-OTAR KEY DELETE result..... | 155 |
| A.4b | PDUs to obtain Air Interface Key Status | 156 |
| A.4b.1 | D-OTAR KEY STATUS demand..... | 156 |
| A.4b.2 | U-OTAR KEY STATUS response..... | 157 |
| A.5 | Other security domain PDUs..... | 158 |
| A.5.1 | U-TEI PROVIDE | 158 |
| A.5.2 | U-OTAR PREPARE | 159 |
| A.5.3 | D-OTAR NEWCELL..... | 159 |
| A.5.4 | D-OTAR CMG GTSI PROVIDE..... | 159 |
| A.5.5 | U-OTAR CMG GTSI RESULT | 160 |
| A.6 | PDUs for Enable and Disable..... | 160 |
| A.6.1 | D-DISABLE..... | 160 |
| A.6.2 | D-ENABLE..... | 161 |
| A.6.3 | U-DISABLE STATUS..... | 161 |
| A.7 | MM PDU type 3 information elements coding | 162 |
| A.7.1 | Authentication downlink | 162 |
| A.7.2 | Authentication uplink | 162 |
| A.8 | PDU Information elements coding..... | 163 |
| A.8.1 | Acknowledgement flag..... | 163 |

| | | |
|----------|--|-----|
| A.8.2 | Address extension..... | 163 |
| A.8.3 | Authentication challenge..... | 163 |
| A.8.4 | Authentication reject reason..... | 163 |
| A.8.5 | Authentication result..... | 164 |
| A.8.6 | Authentication sub-type..... | 164 |
| A.8.7 | CCK identifier..... | 164 |
| A.8.8 | CCK information..... | 164 |
| A.8.9 | CCK Location area information..... | 165 |
| A.8.10 | CCK request flag..... | 165 |
| A.8.11 | Change of security class..... | 165 |
| A.8.12 | Ciphering parameters..... | 166 |
| A.8.13 | CK provision flag..... | 166 |
| A.8.14 | CK provisioning information..... | 166 |
| A.8.15 | CK request flag..... | 167 |
| A.8.16 | Class Change flag..... | 167 |
| A.8.17 | DCK forwarding result..... | 167 |
| A.8.18 | Disabling type..... | 167 |
| A.8.19 | Enable/Disable result..... | 168 |
| A.8.20 | Encryption mode..... | 168 |
| A.8.20.1 | Class 1 cells..... | 168 |
| A.8.20.2 | Class 2 cells..... | 168 |
| A.8.20.3 | Class 3 cells..... | 169 |
| A.8.21 | Equipment disable..... | 169 |
| A.8.22 | Equipment enable..... | 169 |
| A.8.23 | Equipment status..... | 169 |
| A.8.23a | Explicit response..... | 170 |
| A.8.24 | Frame number..... | 170 |
| A.8.25 | Future key flag..... | 170 |
| A.8.26 | GCK data..... | 170 |
| A.8.27 | GCK key and identifier..... | 170 |
| A.8.28 | GCK Number (GCKN)..... | 171 |
| A.8.28a | GCK Provision result..... | 171 |
| A.8.28b | GCK rejected..... | 171 |
| A.8.29 | GCK select number..... | 171 |
| A.8.29a | GCK Supported..... | 172 |
| A.8.30 | GCK Version Number (GCK-VN)..... | 172 |
| A.8.31 | Group association..... | 172 |
| A.8.31a | Group Identity Security Related Information..... | 173 |
| A.8.32 | GSKO Version Number (GSKO-VN)..... | 173 |
| A.8.33 | GSSI..... | 173 |
| A.8.34 | Hyperframe number..... | 173 |
| A.8.35 | Intent/confirm..... | 173 |
| A.8.36 | Void..... | 174 |
| A.8.37 | Key association status..... | 174 |
| A.8.38 | Key association type..... | 174 |
| A.8.39 | Key change type..... | 174 |
| A.8.39a | Key delete type..... | 175 |
| A.8.39b | Key status type..... | 175 |
| A.8.39c | Key delete extension..... | 175 |
| A.8.40 | Key type flag..... | 176 |
| A.8.41 | KSG-number..... | 176 |
| A.8.42 | Location area..... | 176 |
| A.8.43 | Location area bit mask..... | 176 |
| A.8.44 | Location area selector..... | 176 |
| A.8.45 | Location area list..... | 177 |
| A.8.46 | Location area range..... | 177 |
| A.8.46a | Max response timer value..... | 177 |
| A.8.47 | Mobile country code..... | 177 |
| A.8.48 | Mobile network code..... | 177 |
| A.8.49 | Multiframe number..... | 177 |
| A.8.50 | Mutual authentication flag..... | 178 |
| A.8.51 | Network time..... | 178 |

| | | |
|---------|--|-----|
| A.8.52 | Number of GCKs changed | 178 |
| A.8.52a | Number of GCKs deleted | 178 |
| A.8.52b | Number of GCK status | 178 |
| A.8.52c | Number of GCKs provided | 179 |
| A.8.52d | Number of GCKs rejected | 179 |
| A.8.52e | Number of GCKs requested by GCKN | 179 |
| A.8.52f | Number of GCKs requested by GSSI | 180 |
| A.8.53 | Number of groups | 180 |
| A.8.53a | Number of GSKO status | 180 |
| A.8.54 | Number of location areas | 180 |
| A.8.55 | Number of SCKs changed | 181 |
| A.8.55a | Number of SCKs deleted | 181 |
| A.8.56 | Number of SCKs provided | 181 |
| A.8.56a | Number of SCKs rejected | 181 |
| A.8.57 | Number of SCKs requested | 182 |
| A.8.57a | Number of SCK status | 182 |
| A.8.57b | OTAR reject reason | 182 |
| A.8.57c | OTAR retry interval | 183 |
| A.8.58 | OTAR sub-type | 183 |
| A.8.59 | PDU type | 184 |
| A.8.60 | Proprietary | 185 |
| A.8.61 | Provision result | 185 |
| A.8.62 | Random challenge | 185 |
| A.8.63 | Random seed | 185 |
| A.8.64 | Random seed for OTAR | 185 |
| A.8.65 | Void | 186 |
| A.8.65a | Reject reason | 186 |
| A.8.66 | Response value | 186 |
| A.8.67 | SCK data | 186 |
| A.8.68 | SCK information | 186 |
| A.8.69 | SCK key and identifier | 187 |
| A.8.70 | SCK Number (SCKN) | 187 |
| A.8.71 | SCK number and result | 187 |
| A.8.72 | SCK provision flag | 187 |
| A.8.72a | Void | 188 |
| A.8.72b | SCK rejected | 188 |
| A.8.73 | SCK select number | 188 |
| A.8.73a | SCK subset grouping type | 188 |
| A.8.73b | SCK subset number | 189 |
| A.8.74 | SCK use | 189 |
| A.8.75 | SCK version number | 189 |
| A.8.76 | Sealed Key (Sealed CCK, Sealed SCK, Sealed GCK, Sealed GSKO) | 189 |
| A.8.77 | Security information element | 190 |
| A.8.77a | Security related information element | 191 |
| A.8.78 | Session key | 191 |
| A.8.79 | Slot Number | 191 |
| A.8.80 | SSI | 191 |
| A.8.81 | Subscription disable | 192 |
| A.8.82 | Subscription enable | 192 |
| A.8.83 | Subscription status | 192 |
| A.8.84 | TEI | 193 |
| A.8.85 | TEI request flag | 193 |
| A.8.85a | Timeshare cell and AI encryption information | 193 |
| A.8.86 | Time type | 194 |
| A.8.87 | Type 3 element identifier | 194 |

Annex B (normative): Boundary conditions for the cryptographic algorithms and procedures195

| | | |
|-----|--|-----|
| B.1 | Dimensioning of the cryptographic parameters | 200 |
| B.2 | Summary of the cryptographic processes | 201 |

| | | |
|-------------------------------|--|------------|
| Annex C (normative): | Timers | 206 |
| C.1 | T354, authorization protocol timer | 206 |
| C.2 | T371, Delay timer for group addressed delivery of SCK and GCK..... | 206 |
| C.3 | T372, Key forwarding timer..... | 206 |
| C.4 | T355, disable control timer | 206 |
| Annex D (informative): | Bibliography..... | 207 |
| Annex E (informative): | Change request history..... | 208 |
| History | | 209 |

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/3bc1b660-557f-45e5-9b16-9d60843e2e58/etsi-en-300-392-7-v3.2.1-2010-06>

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: "*Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards*", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (<http://webapp.etsi.org/IPR/home.asp>).

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

Foreword

This European Standard (Telecommunications series) has been produced by ETSI Technical Committee Terrestrial Trunked Radio (TETRA).

The present document is part 7 of a multi-part deliverable covering the Voice plus Data (V+D), as identified below:

- EN 300 392-1: "General network design";
- EN 300 392-2: "Air Interface (AI)";
- EN 300 392-3: "Interworking at the Inter-System Interface (ISI)";
- ETS 300 392-4: "Gateways basic operation";
- EN 300 392-5: "Peripheral Equipment Interface (PEI)";
- EN 300 392-7: "Security";**
- EN 300 392-9: "General requirements for supplementary services";
- EN 300 392-10: "Supplementary services stage 1";
- EN 300 392-11: "Supplementary services stage 2";
- EN 300 392-12: "Supplementary services stage 3";
- ETS 300 392-13: "SDL model of the Air Interface (AI)";
- ETS 300 392-14: "Protocol Implementation Conformance Statement (PICS) proforma specification";
- TS 100 392-15: "TETRA frequency bands, duplex spacings and channel numbering";
- TS 100 392-16: "Network Performance Metrics";
- TR 100 392-17: "TETRA V+D and DMO specifications";
- TS 100 392-18: "Air interface optimized applications".

NOTE: 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.

National transposition dates

| | |
|--|-------------------|
| Date of adoption of this EN: | 17 June 2010 |
| Date of latest announcement of this EN (doa): | 30 September 2010 |
| Date of latest publication of new National Standard or endorsement of this EN (dop/e): | 31 March 2011 |
| Date of withdrawal of any conflicting National Standard (dow): | 31 March 2011 |

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/3bc1b660-557f-45e5-9b16-9d60843e2e58/etsi-en-300-392-7-v3.2.1-2010-06>

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 two authentication services have been specified for the air-interface in ETR 086-3 [1.3], based on a threat analysis:

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

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.

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

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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <http://docbox.etsi.org/Reference>.

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

2.1 Normative references

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: "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 ETS 300 396-1: "Terrestrial Trunked Radio (TETRA); Technical requirements for Direct Mode Operation (DMO); Part 1: General network design".

2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

- [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".
- [i.4] ETSI EN 300 392-7 (V2.3.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [i.5] ETSI EN 300 392-7 (V2.1.1): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [i.6] ETSI TS 100 392-18-1: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D) and Direct Mode Operation (DMO); Part 18: Air interface optimized applications; Sub-part 1: Location Information Protocol (LIP)".
- [i.7] ETSI EN 300 392-10-21: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 10: Supplementary services stage 1; Sub-part 21: Ambience Listening (AL)".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

All SwMI MNI: network address used to signal to an MS that the current transaction shall be applied to parameters stored by the MS for use in all SwMIs

NOTE: The All SwMI MNI is encoded as all binary ones (11...11₂).

Authentication Code (AC): (short) sequence to be entered by the user into the MS that may be used in addition to the UAK to generate K with algorithm TB3