ETSI TR 104 291 V1.1.1 (2026-04)

TECHNICAL REPORT

TETRA and Critical Communications Evolution (TCCE);
TETRA security;
Additional security measures introduced in TETRA standards

Reference
DTR/TCCE-06228

Keywords
security, TETRA

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

Contents

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 Report (TR) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

Modal verbs terminology

In the present document "**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.

Introduction

TETRA security is specified in ETSI EN 300 392-7 and ETSI TS 100 392-7 [i.1] (latest version of either specification applies) for Trunked Mode Operation (TMO) and in ETSI EN 300 396-6 and ETSI TS 100 392-6 [i.2] (latest version of either specification applies) for Direct Mode Operation (DMO). The security mechanisms specified in these documents have evolved over time in response to changing market needs and to perceived vulnerabilities.

Version 4.1.1 of [i.1] and version 2.1.1 of [i.2] incorporated new authentication algorithms ([i.1] only) and air interface encryption algorithms ([i.1] and [i.2]) to ensure that TETRA security remains protected against brute force attacks into the future as the cost of computing power falls over time. During development of these specifications, perceived vulnerabilities in the previous versions of these specifications were published, and so the revised specifications also include countermeasures against these perceived vulnerabilities. The perceived vulnerabilities were declared to ETSI under the ETSI CVD (Coordinated Vulnerability Disclosure) process, and all finders of perceived vulnerabilities are encouraged to use this process. ETSI TCCE have now also defined a TETRA-specific policy document which adds TCCE-specific roles and responsibilities to the ETSI process (ETSI TR 104 246 [i.3]).

The purpose of the present document is to list the updated security measures included in [i.1] from version 4.1.1 onwards and [i.2] from version 2.1.1 onwards, and the threats (or perceived vulnerabilities) against which the updates were made. This should allow users of TETRA to make their own evaluation of the threats, and to decide the necessity or urgency for implementing the countermeasures that were added to the standards in their own TETRA systems.

1 Scope

The present document describes the additional security measures put in place in the TETRA security standards, ETSI TS 100 392-7 [i.1] version 4.1.1 and later, and ETSI TS 100 396-6 [i.2] version 2.1.1 and later.

Clause 4 describes the security measures in turn, and the threats that led to the inclusion of each of measures. The threats may be due to a change in environment, or to specific perceived vulnerabilities in the TETRA standard. Clause 4 also lists countermeasures and, where applicable, the clauses in [i.1] in which they are specified.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

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

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 EN 300 392-7 or ETSI TS 100 392-7 (V4.1.1 and later): "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.2] ETSI EN 300 396-6 or ETSI TS 100 392-7 (V2.1.1 and later): "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

[i.3] ETSI TR 104 246: "TCCE Security; Application of ETSI CVD process within TCCE".

[i.4] RUB: "GPU Assisted Brute Force Cryptanalysis of GPRS,GSM, RFID, and TETRA".

[i.5] ETSI GR QSC 006: "Quantum-Safe Cryptography (QSC); Limits to Quantum Computing applied to symmetric key sizes".

[i.6] ETSI TS 101 053-1 (V3.2.1 or later): "Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1".

[i.7] ETSI TS 101 053-4 (V3.2.1 or later): "Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4".

[i.8] ETSI TS 101 053-7 (V1.2.1 or later): "Rules for the management of the TETRA standard encryption algorithms; Part 7: TEA7".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI EN 300 392-7 or ETSI TS 100 392-7 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

BL-ACK	Basic Link ACKnowledgement
BS	Base Station
CCK	Common Cipher Key
CVD	Coordinated Vulnerability Disclosure
DCK	Derived Cipher Key
DCKX	eXtended Derived Cipher Key
DMO	Direct Mode Operation
ESI	Encrypted Short Identity
GCK	Group Cipher Key
GPU	Graphics Processing Unit
IV	Initialization Value
K	authentication Key
MAC	Medium Access Control
MAE	MAC Address Encryption
MS	Mobile Station
OTAR	Over The Air Rekeying
RAND	Random number
RF	Radio Frequency
RS	Random Seed
SwMI	Switching and Management Infrastructure
TAA	TETRA Authentication Algorithm
TCCE	TETRA and Critical Communications Evolution
TDMA	Time Division Multiple Access
TEA	TETRA Encryption Algorithm
TETRA	TErrestrial Trunked RAdio
TMO	Trunked Mode Operation

4 Security enhancements

4.1 New authentication and air interface encryption algorithms

4.1.1 Threat

This threat applies to TMO and DMO.

The cost of computing falls year on year. The computing power needed to carry out a brute force attack on a key, which might have been out of the reach of a well-resourced attacker when an algorithm was designed, may become affordable decades later. Quantum computing, when feasible on a large scale, will provide an increased threat as it will speed up the attack time on keys used with a symmetric algorithm, compared with the attack times possible using classical computing.

An analysis of the computing power needed using modern Graphics Processing Units (GPUs) to attack TEA3 is provided in [i.4]. This indicates that just over a million GPUs could brute force attack a TEA3 key in about a year. Although impractical today, it indicates with reducing cost of computing power, an attack will become practical in the future. An assessment of the impact of quantum computing is provided by ETSI in ETSI GR QSC 006 [i.5].

4.1.2 Countermeasure

New authentication algorithms in the TAA2 algorithm set uses an increased length of authentication key of 256 bits compared to 128 bits used with the original authentication algorithms. New air interface encryption algorithms TEA5, TEA6 and TEA7 have encryption keys 192 bits long, a considerable increase in length compared to the 80 bit long keys used with TEA1, TEA2, TEA3 and TEA4. New key encryption algorithms in the TAA2 algorithm set secure the Over The Air Rekeying (OTAR) of the increased length encryption keys.

NOTE: TEA1, TEA4 and TEA7 have key entropy reductions to enable export control of encrypted TETRA equipment where otherwise export control would not have been possible, see ETSI TS 101 053-1 [i.6], ETSI TS 101 053-4 [i.7] and ETSI TS 101 053-7 [i.8] respectively.

4.2 Requirement for different RAND values

4.2.1 Threat

This threat applies to TMO using the original TAA1 authentication algorithms only.

Authentication requires that the SwMI and MS both know the MS's secret authentication key K, which is used to generate session keys, and together with random numbers generated by SwMI and MS can allow each to prove that the other has knowledge of the correct K.

If an attacker can set up a fake base station and arrange the Radio Frequency (RF) environment such that it 'captures' the MS from the real system, and can initiate authentication of the MS using a chosen value of RS with the specific property that the chosen RS is palindromic, and can guess the random number that will be generated by the MS, the attacker's fake BS provides the MS with the random number expected to be generated by the MS, and can use properties of the session key generation and Derived Cipher Key DCK derivation algorithms to ensure a successful mutual authentication completes without knowledge of the K of the MS, and that the resulting DCK is set to a value of zero for as long as the MS remains captured by the fake base station. The attacker would need to have a detailed knowledge of the MS's design, and its initialization conditions to have any chance of guessing the random number even if the attacker can set up the fake base station environment.

4.2.2 Countermeasure

ETSI EN 300 392-7 or ETSI TS 100 392-7 [i.1], clause 4.1.4, note 2 will cause the authentication to be abandoned and restarted if the random numbers chosen by SwMI and MS are found to be equal.

The DCKX derivation algorithm used for authentication and encryption with the TEA set B algorithms is not vulnerable to this attack, and will not produce a DCK value of zero even if RAND1 and RAND2 are equal.

4.3 TDMA frame number validation - uplink

4.3.1 Threat

This threat applies to TMO only.

The encryption process is synchronized by the TDMA frame numbering system which is broadcast by the BS. The counter value for each slot, frame, multiframe and hyperframe is fed into the encryption algorithm as an Initialization Value (IV) on both uplink and downlink to ensure that the keystream used in the encryption process does not repeat within the lifetime of the counters (approximately 23 days).

If an attacker can set up a fake base station and arrange the Radio Frequency (RF) environment such that it 'captures' the MS from the real system, the attacker can alter the value of the frame numbering system broadcast by the fake base station. If the attacker can then persuade the MS to make an encrypted transmission in a specific timeslot, the attacker can analyse the transmission, and recover the encryption keystream used to encrypt the transmission one bit at a time by repeating the attack over and over again. Eventually, the attacker can compose a fake message and encrypt it using the captured keystream, and send it to the real BS in the chosen timeslot.

4.3.2 Countermeasure

ETSI EN 300 392-7 or ETSI TS 100 392-7 [i.1], clause 6.3.2.0a specifies that the MS should only treat the frame numbering received from the BS as valid following an authentication of the SwMI or following a mutual authentication.

4.4 TDMA frame number validation - downlink

4.4.1 Threat

This threat applies to TMO only.

The attacker sets a fake base station, manipulates the RF environment and captures the MS, and adjusts the values of the frame numbering system as described in clause 4.3.1 above.

The attacker then generates the shortest possible downlink message that will provoke a Basic Link Acknowledgement (BL-ACK) from the MS, and guesses a keystream sequence to encrypt the message. If the MS acknowledges, the attacker has guessed the correct keystream. The attack is repeated over and over again to learn downlink keystream one bit at a time.

The attacker then generates a fake message using the learnt keystream, and sends this to the MS. This message could be sent while the MS is receiving service from the fake base station, or the attacker allows the MS to return to the real system, and sends the message to the MS by overriding the downlink signal to the MS in the chosen timeslot.

4.4.2 Countermeasure

ETSI EN 300 392-7 or ETSI TS 100 392-7 [i.1], clause 6.3.2.0a specifies that the MS should only treat the frame numbering received from the BS as valid following an authentication of the SwMI or following a mutual authentication.

4.5 Entropy of TEA1

4.5.1 Threat

This threat applies to TMO and DMO.

The TEA1 algorithm has a key reduction step which reduces the effective keylength of the key to 32 bits. An overview is provided in ETSI TS 101 053-1 [i.6], clause 8. This was done to allow export of equipment containing TEA1 in some situations. This means that an attacker can mount a brute force attack - trying every possible reduced key in turn - with less effort (time and/or computing power) than for an unreduced 80 bit key.

4.5.2 Countermeasure

An alternative air interface encryption algorithm can be deployed instead of TEA1. TEA2, TEA3 or TEA4 from TEA set A may be deployed with either the TAA1 or TAA2 authentication and key management algorithm set, or TEA5, TEA6 or TEA7 from TEA set B may be deployed with the TAA2 authentication and key management algorithm set. Export control and usage limitations may prevent some algorithms from being used in some deployments, for example TEA2 and TEA5 are restricted to public safety and associated uses in Europe only. Note that TEA4 and TEA7 have reductions in effective keylength to 56 bits: see ETSI TS 101 053-4 [i.7], clause 8 and ETSI TS 101 053-7 [i.8], clause 8 respectively.

4.6 Identity Encryption

4.6.1 Threat

This threat applies to TMO only, and where an algorithm from TEA set A is in use.

If an attacker can capture several clear identities and the equivalent encrypted identities, it is possible to compute an intermediate encryption key that is used in the identity encryption process with less complexity than a full attack on the CCK.

4.6.2 Countermeasure

The attacker needs to capture a number of authentication transactions that take place in clear (without encryption) to determine a clear and encrypted identity pair for the MS. Encrypted registrations and encrypted authentication transactions (using the previous Derived Cipher Key that was established for the MS) can make the task of the attacker harder. A change of CCK also requires a new attack.

The TEA set B algorithms (TEA5, TEA6 and TEA7) can use a different identity encryption process: the MAC Address Encryption (MAE) encryption process, compared with the Encrypted Short Identity (ESI) process used with the TEA set A algorithms. This is not vulnerable to such an attack.

The encryption process in DMO also uses a different identity encryption mechanism that is not vulnerable to the attack with either TEA set A or TEA set B algorithms.

4.7 Message injection

4.7.1 Threat

This threat applies to TMO only.

If a key or a keystream can be recovered using the threat mechanisms outlined in clauses 4.3 and 4.4, or if the recipient accepts clear (encryption Class 1) messages as well as encrypted messages, a fake message can be composed and sent on the uplink to the real SwMI, or on the downlink to an MS provided that the signal from a genuine base station of the SwMI can be overpowered by a fake base station.

4.7.2 Countermeasure

An MS and SwMI can be configured to only accept encrypted messages sent outside a registration and authentication procedure.

An MS with the behaviour described in clause 4.3.2 (explicit IV validation, as specified in ETSI EN 300 392-7 or ETSI TS 100 392-7 [i.1], clause 6.3.2.0a) above will not be susceptible to the keystream recovery threats outlines in clauses 4.3.1 and 4.4.1.

Where TETRA data services act as bearers for user applications, those applications can add their own message integrity and authenticity checks.

4.8 Reuse of CCK between algorithms

4.8.1 Threat

This threat applies to TMO only where more than one encryption algorithm from TEA set A is in use on a SwMI, for example during transition from the use of one algorithm to use of another and where service is provided to all users of both algorithms on the same base stations.

If a SwMI supports multiple air interface encryption algorithms, the same CCK is used for all algorithms, as only a single CCK can be used for identity encryption. If the attacker is able to retrieve a CCK used by one algorithm, for example has mounted an attack on TEA1 as described in clause 4.5.1, the attacker can decrypt messages sent encrypted by the CCK using the other algorithm(s).

4.8.2 Countermeasure

Multiple air interface encryption algorithms should only be present for as short a time as possible on a SwMI, for example during transition from one algorithm to another. Users should be aware of the issue and manage the risks.

Individually addressed transmissions are encrypted using a Derived Cipher Key (DCK) that is unique to an MS and only used with a single algorithm, and are not vulnerable to the attack.

Group addressed transmissions encrypted with a Group Cipher Key (GCK) are not vulnerable to the attack.

If MSs using the different algorithms are provided with service on different base stations (e.g. TEA1 MSs are served by one set of cells, TEA3 MSs are served by a second set of cells), CCKs can be different between the two algorithms and so the attack is not possible. In some cases, it may be possible to 'split' a physical BS into two cells and support a different algorithm on each cell, with different CCKs on each.

Where an algorithm from TEA set A is in use at the same time as an algorithm from TEA set B, the communications using the algorithm from TEA set B are not vulnerable to the attack.

4.9 End-to-end encryption

The details of end-to-end encryption mechanisms are outside the scope of the TETRA security standards, which make provision for end-to-end encryption, but do not specify the mechanisms that can be employed.

History

Version	Date	Status
V1.1.1	April 2026	Publication