ETSI TS 101 053-1 V3.2.1 (2025-07)

TECHNICAL SPECIFICATION

Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1

Reference
RTS/TCCE-06215

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

The present document is part 1 of a multi-part deliverable covering the rules for the management of the TETRA standard encryption algorithms, as identified below:

Part 1: "TEA1";

Part 2: "TEA2";

Part 3: "TEA3";

Part 4: "TEA4";

Part 5: "TEA5";

Part 6: "TEA6";

Part 7: "TEA7".

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.

1 Scope

The present document has been designed to specify the rules for the management of the TETRA standard encryption algorithm TEA1. This algorithm is intended for air interface encryption in TETRA products.

The specification for TEA1 consists of the following three parts:

Part 1: Algorithm specification;

Part 2: Design conformance test data;

Part 3: Algorithm input/output test data.

The procedures described in the present document apply to parts 1 and 2 of the specification. Parts 1 and 2 are confidential. The algorithm primitives' section of part 1 of the specification has been published as ETSI TS 104 053-1 [i.1].

Part 3 of the specification is not confidential and can be obtained directly from the TEA1 Custodian (see clause 5.2). There are no restrictions on the distribution of this part of the specifications.

The management structure is defined in clause 4. This structure is defined in terms of the principals involved in the management of TEA1 (ETSI, ETSI Technical Committee TCCE, TEA1 Custodian and approved recipients (beneficiaries)) together with the relationships and interactions between them.

The procedures for delivering TEA1 to approved recipients are defined in clause 5. This clause is supplemented by annex A which specifies the items which are to be delivered.

Clause 6 is concerned with the criteria for approving an organization for receipt of TEA1 and with the responsibilities of an approved recipient.

Clause 7 is concerned with the appointment and responsibilities of the TEA1 Custodian.

Clause 8 describes an overview of the algorithm and its dimensions.

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.

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 are necessary for the application of the present document.

[1] Void.

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.

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 TS 104 053-1: "TETRA Air Interface Security, Algorithms Specifications; Part 1: TETRA Encryption Algorithms Set A".

[i.2] ETSI TS 100 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".

[i.3] ETSI TS 100 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

NOTE 2: References [i.2] and [i.3] may also be published as ETSI European Standards, specifically ETSI EN 300 392-7 and ETSI EN 300 396-6 respectively. In each case, the latest version of the specification, either TS or EN, applies.

[i.4] ETSI Algorithms & Codes webpage.

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

approved recipient: beneficiary of the algorithm specification as described in the Confidentiality and Restricted Usage Undertaking (CRUU)

3.2 Symbols

Void.

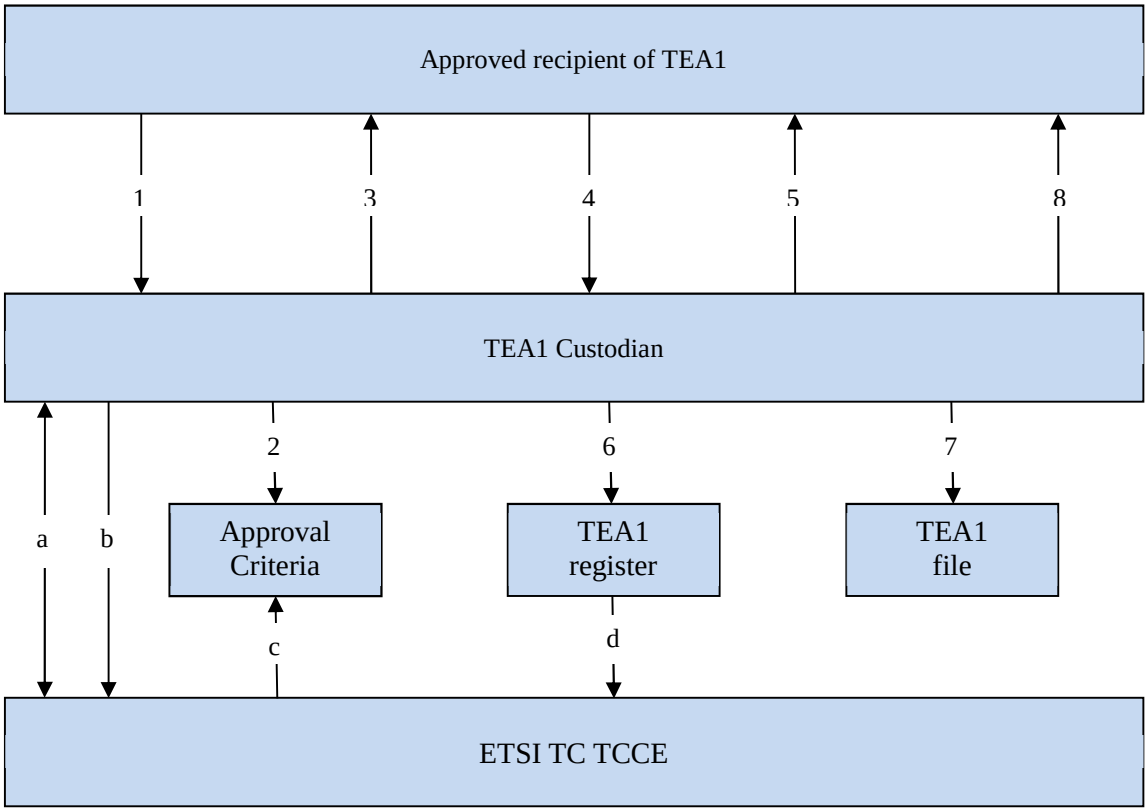
3.3 Abbreviations

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

CRUU	Confidentiality and Restricted Usage Undertaking
DMO	Direct Mode Operation
ISI	Inter-System Interface
TC	Technical Committee
TCCE	TETRA and Critical Communications Evolution
TEA1	TETRA Encryption Algorithm No. 1
TETRA	TErrestrial Trunked Radio

4 TEA1 management structure

The management structure is depicted in figure 1.



Key:

a	=	Agreement between TEA1 Custodian and ETSI TC TCCE
b	=	Status reports and recommendations
c	=	Setting of approval criteria
d	=	Requested details of the TEA1 register
1	=	Request for TEA1
2	=	Check of request against approval criteria
3 and 4	=	Exchange of Confidentiality and Restricted Usage Undertaking
5	=	Dispatch of TEA1 specification
6	=	Update the TEA1 register
7	=	Document filing
8	=	Technical advice

Figure 1: TEA1 management structure

Figure 1 shows the three principals involved in the management of TEA1 and the relationships and interactions between them.

ETSI is the Custodian of TEA1. ETSI together with ETSI TC TCCE sets the approval criteria for receipt of the algorithm (see clause 6).

The TEA1 Custodian is the interface between ETSI TC TCCE and the approved recipients of TEA1.

The Custodian shall be ETSI unless it is decided by ETSI and/or ETSI TC TCCE to delegate this task to a third party on the basis of an agreement between the latter and ETSI. The TEA1 Custodian's duties are detailed in clause 7. They include distributing TEA1 to approved recipients, as detailed in clause 5, providing limited technical advice to approved recipients.

5 Distribution procedures

5.1 Distribution of parts 1, 2 and 3 of the TEA1 specification by the TEA1 Custodian

The process for purchase and distribution of algorithm specifications is described at ETSI Algorithms & Codes [i.4].

5.2 Distribution of TEA1 specification part 3 by the TEA1 Custodian

The following procedure is defined for distributing only part 3 of the TEA1 specification:

1) The TEA1 Custodian receives a request for one single copy of part 3 of the TEA1 specification.
2) The TEA1 Custodian sends one copy of part 3 of the TEA1 specification to the applicant.
3) The TEA1 Custodian informs ETSI TC TCCE.

6 Approval criteria and restrictions

The approval criteria are set by ETSI together with ETSI TC TCCE. ETSI together with ETSI TC TCCE may recommend changes to these criteria.

ETSI TC TCCE shall decide whether an organization requesting the TEA1 specification may be considered to be an approved recipient. Where an organization consists of a group of companies or organizations, ETSI TC TCCE will decide whether one organization or company within the group may be an approved recipient on behalf of other organizations or companies within the group.

In order for an organization to be considered an approved recipient of the TEA1 specification it has to satisfy at least one of the criteria indicated in Article 3.2 of the Confidentiality and Restricted Usage Undertaking (CRUU) available at ETSI Algorithms & Codes [i.4].

In the event that an organization cannot comply with the rules as described in the present document, the TEA1 Custodian will inform ETSI TC TCCE who may provide a justification. If a special Confidentiality and Restricted Usage Undertaking is used, the TEA1 Custodian will first ask the ETSI Legal Department to approve this Confidentiality and Restricted Usage Undertaking (CRUU).

7 The TEA1 Custodian

7.1 Responsibilities

The TEA1 Custodian is expected to perform the following tasks:

T1 To approve requests for TEA1 by reference to the Approval Criteria given in Article 3.2 of the Confidentiality and Restricted Usage Undertaking (CRUU) after confirmation by ETSI TC TCCE.

T2 To process the Confidentiality and Restricted Usage Undertaking with approved recipients as described at ETSI Algorithms & Codes [i.4].

T2bis To obtain the administrative authorization and export licences required by the Customs Services of its country if any.

T3 To distribute, if approved, the TEA1 specifications as described at ETSI Algorithms & Codes [i.4].

T4 To maintain the TEA1 Register as described in clause 4.

T5 To hold in custody the contents of the TEA1 File as specified in clause 4.

T6 To provide recipients of TEA1 with limited technical support, i.e. answer written queries arising from the specification or test data (see note).

T7 To advise ETSI TC TCCE of any problems arising with the approval criteria.

T8 In the light of written queries from recipients of the TEA1 specifications, to make recommendations to ETSI TC TCCE for improvements/corrections to the specification and, subject to ETSI TC TCCE approval.

T9 To provide ETSI TC TCCE with information from the TEA1 Register when requested to do so.

NOTE : The TEA1 Custodian will only endeavour to answer questions relating to the TEA1 specifications. The TEA1 Custodian is not expected to provide technical support for development programmes.

7.2 Appointment

The TEA1 Custodian is:

- ETSI

The contact person is:

- ETSI Algorithms & Codes service
- Email: algorithms@etsi.org
- ETSI
  F-06921 Sophia Antipolis Cedex
  FRANCE

The TEA1 Custodian will ask a fee from the recipient to cover the cost of distribution of parts 1 and 2 of the specifications.

The TEA1 Custodian may ask for an optional fee from the recipient to cover the cost of distribution of part 3.

All requests for either the TEA1 specification parts 1 and 2 or the TEA1 specification part 3 should be addressed to the indicated contact person or to ETSI.

8 TEA1 Overview Description and Dimensions

The TEA1 algorithm is used as a stream cipher for providing confidentiality across the Air Interface and Inter-System Interface (ISI) of TETRA systems. It is used to protect control signalling, identities, speech and user data.

The algorithm specification is described in detail in clause 5 of ETSI TS 104 053-1 [i.1]. A full description of the TETRA air interface encryption, authentication and key management protocols are described in ETSI TS 100 392-7 [i.2] and ETSI TS 100 396-6 [i.3].

The algorithm generates a sequence of key bytes from a Cipher Key and an Initialization Vector. The key bytes are used to encrypt or to decrypt information transmitted via the TETRA system. The Cipher Key has an input length of 80 bits; the Initialization Vector has a length of 29 bits. The effective Cipher Key length of TEA1 is reduced within the algorithm to 32 bits to permit worldwide exportability without restrictions, at the time of definition.

Annex A (informative): Items delivered to approved recipient of TEA1

ITEM-1: The TEA1 specification (parts 1, 2 and 3).

ITEM-2: A countersigned Confidentiality and Restricted Usage Undertaking.

Annex B (normative): Void

Annex C (informative): Bibliography

- ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

NOTE: The two above references may also be published as ETSI Technical Specifications, specifically ETSI TS 100 392-7 and ETSI TS 100 396-6 respectively. In each case, the latest version of the specification, either TS or EN, applies.

- ETSI TS 101 053-2: "Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2".
- ETSI TS 101 053-3: "Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3".
- ETSI TS 101 053-4: "Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4".
- ETSI TS 101 053-5: "Rules for the management of the TETRA standard encryption algorithms; Part 5: TEA5".
- ETSI TS 101 053-6: "Rules for the management of the TETRA standard encryption algorithms; Part 6: TEA6".
- ETSI TS 101 053-7: "Rules for the management of the TETRA standard encryption algorithms; Part 7: TEA7".
- ETSI TS 104 053-2: "TETRA Air Interface Security, Algorithms specifications; Part 2: TETRA |Encryption Algorithms Set B".
- ETSI TS 104 053-3: "TETRA Air Interface Security, Algorithms Description; Part 3: TETRA and Authentication and Key Management Algorithms TAA1".
- ETSI TS 104 053-4: "TETRA Air Interface Security, Algorithms Description; Part 4: TETRA and Authentication and Key Management Algorithms TAA2".

History

Document history		
V1.1.1	June 1997	Publication as ETSI TR 101 053-1 (Historical)
V1.1.2	January 2006	Publication as ETSI TR 101 053-1 (Historical)
V2.1.1	February 2016	Publication
V3.1.1	February 2023	Publication
V3.2.1	July 2025	Publication