ETSI TS 101 053-1 V3.1.1 (2023-02)

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 101 053-1 V3.1.1 (2023-02)
https://standards.iteh.ai/catalog/standards/sist/4eb7e2b0-fcbf-4819-a962-22608d70c0b1/etsi-ts-101-053-1-v3-1-1-2023-02

Reference
RTS/TCCE-06204

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

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 at www.etsi.org/deliver.

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
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

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 2023.
All rights reserved.

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 101 053-1 V3.1.1 (2023-02)
https://standards.iteh.ai/catalog/standards/sist/[illegible]/etsi-ts-101-053-1-v3-1-1-2023-02

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 Web server (https://ipr.etsi.org/).

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™** and **LTE™** 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

Foreword

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

https://standards.iteh.ai/catalog/standards/sist/4eb7e2b0-fcbf-4819-a962-22608d70c0b1/etsi-ts-101-053-1-v3.1.1-2023-02

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 purpose of the present document is 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 specifications. Parts 1 and 2 are confidential for each of the algorithms.

Part 3 of each of the specifications 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) 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2 References

ETSI TS 101 053-1 V3.1.1 (2023-02)
https://standards.iteh.ai/catalog/standards/sist/4eb7e2b0-fcbf-4819-a962-22608d70c0b1/etsi-ts-101-053-1-v3-1-1-2023-02

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 at https://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.

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

[1] ETSI Algorithms.

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

Not applicable.

3 Definition of terms, symbols and abbreviations

3.1 Terms

Void.

3.2 Symbols

Void.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.3 Abbreviations

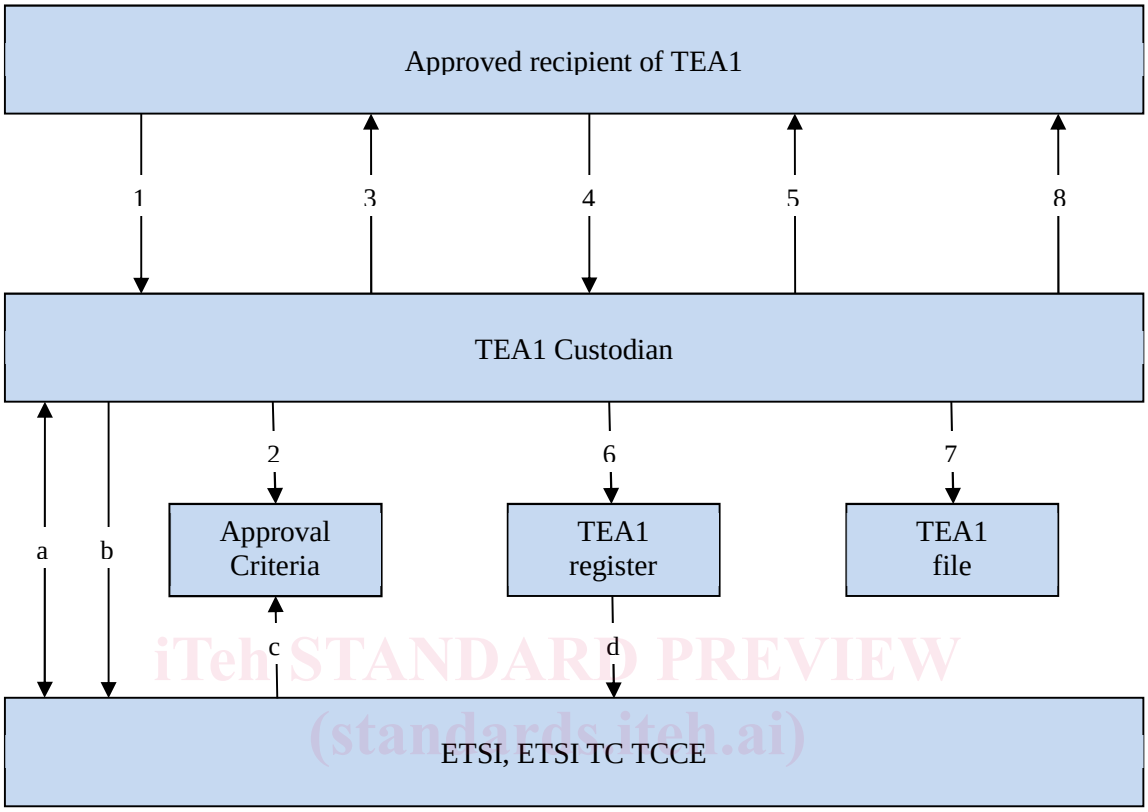
For the purposes of the present document, the following abbreviations apply:

ETSI TS 101 053-1 V3.1.1 (2023-02)
https://standards.iteh.ai/catalog/standards/sist/4eb7e2b0-fcbf-4819-a962-[illegible]0b1/etsi-ts-101-053-1-v3-1-1-2023-02

CRUU	Confidentiality and Restricted Usage Undertaking
DMO	Direct Mode Operation
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.



iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 101 053-1 V3.1.1 (2023-02)
https://standards.iteh.ai/catalog/standards/sist/4eb7e2b0-fcbf-4819-a962-[illegible]/etsi-ts-101-053-1-v3-1-1-2023-02

Key:

a	=	Agreement between TEA1 Custodian and ETSI
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 owner of TEA1. The ETSI Secretariat 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 and the approved recipients of TEA1.

The Custodian shall be the ETSI Secretariat unless it is decided by ETSI Secretariat and/or ETSI TC TCCE to (temporarily) delegate this task to a third party on the basis of an agreement between the latter and the ETSI Secretariat. 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 and providing algorithm status reports to ETSI TC TCCE.

5 Distribution procedures

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

The process for distribution of algorithm specifications is described at https://www.etsi.org/security-algorithms-and-codes/security-algorithms [1].

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.

6 Approval criteria and restrictions

The approval criteria are set by the ETSI Secretariat together with ETSI TC TCCE and maintained by the TEA1 Custodian. The TEA1 Custodian may recommend changes to these criteria.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

The TEA1 Custodian 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, the TEA1 Custodian 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. Any doubtful cases shall be referred back to ETSI Secretariat or ETSI TC TCCE.

ETSI TS 101 053-1 V3.1.1 (2023-02)
https://standards.iteh.ai/catalog/standards/sist/4eb7e2b0-fabf-4819-a962-22608d70c0b1/etsi-ts-101-053-1-v3-1-1-2023-02

In order for an organization to be considered an approved recipient of the TEA1 specification it has to satisfy at least one of the following criteria:

C1 The organization is a bona fide designer or manufacturer of TETRA subscriber or fixed network equipment, where the algorithm requested is included in the systems.

C2 The organization is a bona fide designer or manufacturer of components for TETRA subscriber or fixed network equipment, where at least one of the components includes the algorithm requested.

C3 The organization is a bona fide designer or manufacturer of a TETRA system simulator for testing of TETRA subscriber or fixed network equipment, where the simulator includes the algorithm requested.

C4 The organization has provided the TEA1 Custodian with exceptional reasons that have been approved by the TEA1 Custodian.

In the event that an organization cannot comply with the rules as described in the present document, the TEA1 Custodian may still decide, on an exceptional basis, to distribute the TEA1 specifications to this organization. In this case the TEA1 Custodian will inform ETSI TC TCCE about the decision and at the same time provide a motivation. 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 clause 6.

T2 To exchange the Confidentiality and Restricted Usage Undertaking with approved recipients as described in clause 5.

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 detailed in clause 5.

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 1).

T7 To advise ETSI/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/ETSI TC TCCE for improvements/corrections to the specification and, subject to ETSI/ETSI TC TCCE approval, make and distribute the changes (see note 2).

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

T10 To monitor published advances in cryptanalysis and advise the ETSI TC TCCE of any advances which have a significant impact upon the continued suitability of TEA1 for the TETRA application.

NOTE 1: 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.

NOTE 2: Numbered copies of any changes to the TEA1 specifications will be automatically distributed to all recipients of the specification and a record of the distribution entered in the TEA1 Register.

7.2 Appointment

The TEA1 Custodian is:

- ETSI Secretariat

The contact person is:

- ETSI Algorithms & Codes
- 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
https://standards.iteh.ai/catalog/standards/sist/4eb7e2b0-fcbf-4819-a962-

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI TS 101 053-1 V3.1.1 (2023-02)
https://standards.iteh.ai/catalog/standards/sist/4eb7e2b0-fcbf-4819-a962-22608d70c0b1/etsi-ts-101-053-1-v3-1-1-2023-02