

# ETSI TS 101 052 V2.1.1 (2016-02)



TECHNICAL SPECIFICATION

## Rules for the management of the TETRA standard authentication and key management algorithm set TAA1

**PREVIEW**  
iTech STANDARDS (standards.it-eu-api)  
Full standard catalog: <https://standards.it-eu-api/catalog/standards/405b08f-f29-410b-844a-423def134873/etsi-ts-101-052-v2.1.1-2016-02>

---

Reference

RTS/TCCE-06187

---

Keywords

algorithm, security, TAA1, 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 - NAF 742 C  
Association à but non lucratif enregistrée à la  
Sous-Préfecture de Grasse (06) N° 7803/88

---

**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 only prevailing document is the print of the Portable Document Format (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

<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/CommitteeSupportStaff.aspx>

---

**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.

© European Telecommunications Standards Institute 2016.

All rights reserved.

**DECT™**, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI 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 .....	4
Foreword.....	4
Modal verbs terminology.....	4
1 Scope .....	5
2 References .....	5
2.1 Normative references .....	5
2.2 Informative references.....	6
3 Abbreviations .....	6
4 TAA1 management structure .....	7
5 Distribution procedures .....	8
5.1 Distribution of parts 1, 2 and 3 of the TAA1 specification by the TAA1 Custodian .....	8
5.2 Distribution of TAA1 specification part 3 by the TAA1 Custodian.....	9
6 Approval criteria and restrictions .....	9
7 The TAA1 Custodian .....	10
7.1 Responsibilities .....	10
7.2 Appointment.....	10
<b>Annex A (informative): Items delivered to approved recipient of TAA1.....</b>	<b>12</b>
<b>Annex B (normative): Confidentiality and Restricted Usage Undertaking for TAA1 .....</b>	<b>13</b>
History .....	16

iTeh STANDARD PREVIEW  
 (standards.iteh.ai)  
 Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/4105b08f-f29-410b-844a-423def134873/etsi-ts-101-052-v2-1-1-2016-02>

---

## 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 (<https://ipr.etsi.org/>).

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

---

## 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.

iTeh STANDARD PREVIEW  
(standards.iteh.ai)  
Full standard:  
<https://standards.iteh.ai/catalog/standards/sist/445b88f-f29-410b-844a-423def134873/etsi-ts-101-052-v2.1.1-2016-02>

---

# 1 Scope

The purpose of the present document is to specify the rules for the management of the TETRA standard authentication and key management algorithm set TAA1. This algorithm set is intended for air interface security in TETRA products.

The specification for TAA1 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 TAA1 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 TAA1 (ETSI, ETSI Technical Committee TCCE, TAA1 Custodian and approved recipients) together with the relationships and interactions between them.

The procedures for delivering TAA1 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 TAA1 and with the responsibilities of an approved recipient. This clause is supplemented by annex B which contains a Confidentiality and Restricted Usage Undertaking to be signed by each approved recipient.

Clause 7 is concerned with the appointment and responsibilities of the TAA1 Custodian.

---

## 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 reference 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.

Not applicable.

## 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 reference 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.

- [i.1] ETSI EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security".
- [i.2] ETSI EN 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

---

## 3 Abbreviations

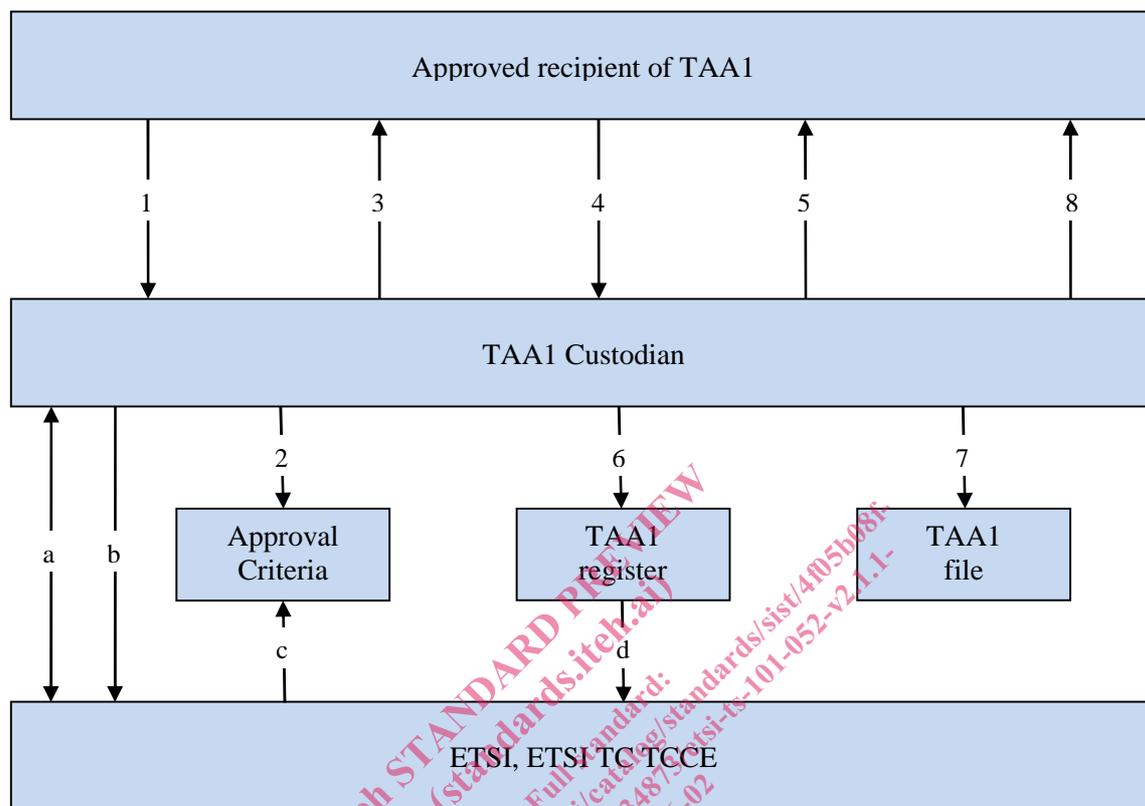
For the purposes of the present document, the following abbreviations apply:

CRUU	Confidentiality and Restricted Usage Undertaking
TAA1	TETRA Authentication Algorithm set No. 1
TC	Technical Committee
TCCE	TETRA and Critical Communications Evolution
TETRA	Terrestrial Trunked Radio

**PREVIEW**  
iTech STANDARD  
(standards.itih.ai)  
Full standard:  
<https://standards.itih.ai/catalog/standards/sist/405b08f-f29-410b-844a-423def134873/etsi-ts-101-052-v2.1.1-2016-02>

## 4 TAA1 management structure

The management structure is depicted in figure 1.



Key:

- a = Agreement between TAA1 Custodian and ETSI
- b = Status reports and recommendations
- c = Setting of approval criteria
- d = Requested details of the TAA1 register
- 1 = Request for TAA1
- 2 = Check of request against approval criteria
- 3 and 4 = Exchange of Confidentiality and Restricted Usage Undertaking
- 5 = Dispatch of TAA1 specification
- 6 = Update the TAA1 register
- 7 = Document filing
- 8 = Technical advice

**Figure 1: TAA1 management structure**

Figure 1 shows the three principals involved in the management of TAA1 and the relationships and interactions between them.

ETSI is the owner of TAA1. The ETSI Secretariat together with ETSI TC TCCE sets the approval criteria for receipt of the algorithm (see clause 6).

The TAA1 Custodian is the interface between ETSI and the approved recipients of TAA1.

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 TAA1 Custodian's duties are detailed in clause 7. They include distributing TAA1 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 TAA1 specification by the TAA1 Custodian

This clause describes the procedure for the distribution of parts 1, 2 and 3 of the TAA1 specification (see clause 1) when requested together. See clause 5.2 for the procedure for the distribution of part 3 as a separate item.

The TAA1 Custodian is responsible for determining whether an applicant meets the criteria to receive the TAA1 specification.

The TAA1 Custodian is responsible for signing TAA1 Confidentiality and Restricted Usage Undertakings with qualified applicants who require access to the TAA1 specification.

The TAA1 Custodian is responsible for sending copies of the TAA1 specification to qualified applicants.

The following procedure for distributing TAA1 specifications is defined with reference to figure 1.

- 1) The TAA1 Custodian receives a written request for N copies of the TAA1 specification parts 1, 2 and 3 (see notes 1 and 2).
- 2) The TAA1 Custodian determines whether the requesting organization meets the approval criteria (see clause 6).
- 3) If the request is not approved, the TAA1 Custodian informs the requesting organization that its request has not been approved.
- 4) If the request is approved, the TAA1 Custodian dispatches 2 copies of the corresponding Confidentiality and Restricted Usage Undertaking (as given in annex B) for signature by the approved recipient (see notes 2 and 6) together with a copy of the present document (Rules for the management of the TETRA standard authentication and key management algorithm set TAA1).
- 5) Both copies of the Confidentiality and Restricted Usage Undertaking (CRUU) have to be signed by the approved recipient (see notes 5 and 7) and returned to the TAA1 Custodian, together with the payment of any applicable charges.
- 6) The TAA1 Custodian sends up to N (see note 3) numbered copies of the TAA1 specification parts 1, 2 and 3 to the approved recipient, together with one countersigned copy of the returned Confidentiality and Restricted Usage Undertaking (CRUU) and a covering letter (see notes 4 and 6).
- 7) The TAA1 Custodian updates the TAA1 Register by recording the name and address of the recipient, the numbers of the copies of the TAA1 specification delivered and the date of delivery. If the original request is not approved, the TAA1 Custodian records the name and address of the requesting organization and the reason for rejecting the request in the TAA1 Register (see also note 8).
- 8) The TAA1 Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking (CRUU) in the TAA1 File together with a copy of the covering letter sent to the approved recipient.
- 9) The TAA1 Custodian may provide very limited technical advice with respect to answering questions concerning the TAA1 specification.
- 10) If there is a change in the contact details of the signatory or name or ownership of the organization, the organization shall inform the TAA1 Custodian.
- 11) All copies of the TAA1 specification shall be returned to the TAA1 Custodian when they are no longer required by the organization that received them (see note 8).

NOTE 1: Requests for the TAA1 specification may be made directly to the TAA1 Custodian or through ETSI.

NOTE 2: The Confidentiality and Restricted Usage Undertaking (CRUU) specifies the number of copies requested.

NOTE 3: The covering letter specifies the numbers of the copies delivered.

NOTE 4: If the request is approved, the TAA1 Custodian sends all items listed in annex A. Requests for part of the package of items are rejected.

NOTE 5: An organization may request the specification on behalf of a second organization to which it is subcontracting work which requires the specification. In this case, the first organization is responsible for returning a Confidentiality and Restricted Usage Undertaking (CRUU) signed by the second organization.

NOTE 6: Under normal circumstances the TAA1 Custodian is expected to respond within 25 working days, excluding the delay of the procedures with the Customs Services.

NOTE 7: The approved recipient is represented by its authorized officers.

NOTE 8: If a TAA1 specification is returned to the TAA1 Custodian (for example the recipient may decide not to make use of the information), then the TAA1 Custodian destroys the specification and enters a note to this effect in the TAA1 Register.

## 5.2 Distribution of TAA1 specification part 3 by the TAA1 Custodian

The following procedure is defined for distributing only part 3 of the TAA1 specification:

- 1) The TAA1 Custodian receives a written request for one single copy of part 3 of the TAA1 specification.
- 2) The TAA1 Custodian sends one copy of part 3 of the TAA1 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 TAA1 Custodian. The TAA1 Custodian may recommend changes to these criteria.

In order for an organization to be considered an approved recipient of the TAA1 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.

The TAA1 Custodian shall decide whether an organization requesting the TAA1 specification may be considered to be an approved recipient. Any doubtful cases shall be referred back to ETSI Secretariat or ETSI TC TCCE.