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

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

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

Contents

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.

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".

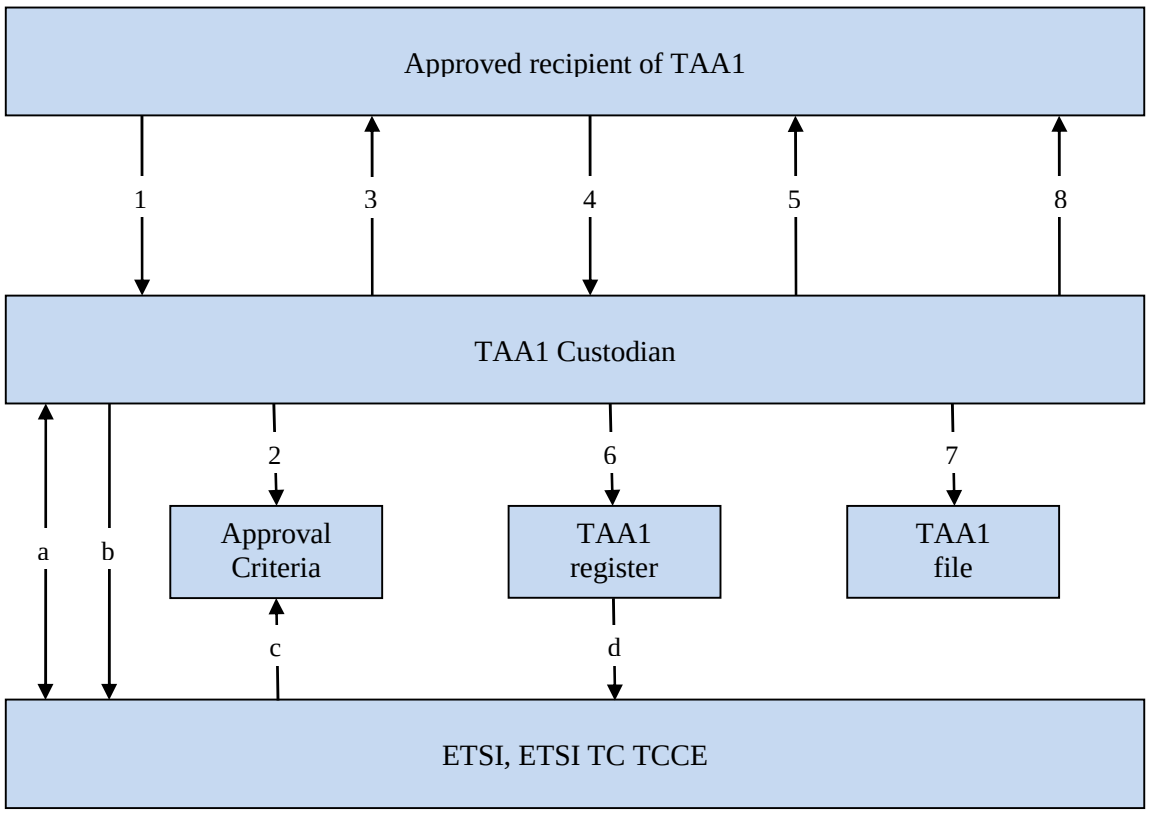
3 Abbreviations

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

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.

7 The TAA1 Custodian

7.1 Responsibilities

The TAA1 Custodian is expected to perform the following tasks:

T1 To approve requests for TAA1 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 TAA1 specifications as detailed in clause 5 (see note 1).

T4 To maintain the TAA1 Register as described in clause 5.

T5 To hold in custody the contents of the TAA1 File as specified in clause 5.

T6 To provide recipients of TAA1 with limited technical support, i.e. answer written queries arising from the specification or test data (see note 2).

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 TAA1 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 3).

T9 To provide ETSI/ETSI TC TCCE with information from the TAA1 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 TAA1 for the TETRA application.

NOTE 1: Registered postage will be used. If recipients require a different delivery service then they will be expected to pay the full costs.

NOTE 2: The TAA1 Custodian will only endeavour to answer questions relating to the TAA1 specifications. He is not expected to provide technical support for development programmes.

NOTE 3: Numbered copies of any changes to the TAA1 specifications will be automatically distributed to all recipients of the specification and a record of the distribution entered in the TAA1 Register.

7.2 Appointment

The TAA1 Custodian is:

- ETSI Secretariat

The contact person is:

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

The TAA1 Custodian will ask a fee from the recipient to cover the cost of distribution of Part 1 and 2 of the specifications.

The TAA1 Custodian may ask for an optional fee from the recipient to cover the cost of distribution of Part 3.

All requests for either the TAA1 specification Part 1 and 2 or the TAA1 specification Part 3 should be addressed to the indicated contact person or to ETSI.

Annex A (informative): Items delivered to approved recipient of TAA1

ITEM-1: Up to N numbered paper copies of the TAA1 specification (parts 1, 2 and 3) where N is the number of copies approved.

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

ITEM-3: A cover letter from and signed by the TAA1 Custodian listing the delivered items (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered.

In all cases one copy of the present document will be delivered to each signatory of the CRUU.

Annex B (normative): Confidentiality and Restricted Usage Undertaking for TAA1

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the TAA1 algorithm for the protection of the information exchanged over the radio channels of the Terrestrial Trunked Radio (TETRA) System.

Between

(COMPANY NAME) .....

(COMPANY ADDRESS) .....

.....

.....

hereinafter called: the LICENCEE;

and

(COMPANY NAME) .....

(COMPANY ADDRESS) .....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas

The LICENCEE declares, supported by additional information provided, that he fulfils at least one of the following criteria:

- He is a bona fide designer or manufacturer of TETRA subscriber or fixed network equipment where TETRA Standard Authentication Algorithm set 1 (hereinafter referred to as TAA1) is included in the systems.
- He is a bona fide designer or manufacturer of components for TETRA subscriber or fixed network equipment where at least one of the components includes TAA1.
- He is a bona fide designer or manufacturer of TETRA system simulators for testing of TETRA subscriber or fixed network equipment where the simulator includes TAA1.

The CUSTODIAN undertakes to give to the LICENCEE:

- Registered copies of the detailed specification of the authentication and key management algorithm set TAA1 Part 1 and Part 2 for use in the security of a Terrestrial Trunked Radio system.

The LICENCEE undertakes to:

1) keep strictly confidential all information contained in the detailed specification of TAA1 and all related communications written or verbal which have been associated with that information after the signature of the present undertaking (the "INFORMATION").

2) take measures to ensure that his personnel do not disclose to third parties, without prior and explicit authorization in writing by the CUSTODIAN, all or part of the INFORMATION.

3) use the INFORMATION in the TAA1 specification exclusively for the provision of TETRA components, systems or services, thus refraining from making any other use of TAA1 or information in the TAA1 specification.

4) design his equipment in a manner that protects TAA1 from disclosure and ensures that it cannot be used for any purpose other than to provide the TETRA air interface security services for which it is intended.

   These services are specified in the following standards:

   - 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".

   TAA1 shall not be used to provide end-to-end security services.

The LICENSEE undertakes NOT to:

5) make copies of the TAA1 specifications (all copies of these specifications must be produced, numbered and registered by the TAA1 Custodian).

6) disclose the INFORMATION to any third party without prior and explicit authorization in writing by the CUSTODIAN.

7) register, or attempt to register, any IPR (patents or the like rights) relating to TAA1 and containing all or part of the INFORMATION.

8) subcontract any part of the design and build of his equipment, or the provision of his TETRA services, which requires a knowledge of TAA1, to any organization which has not signed the Confidentiality and Restricted Usage Undertaking.

9) publish a description or analysis of any aspects which may disclose the operation of TAA1 in any document that is circulated outside the premises of the LICENCEE.

10) export the TAA1 specification without the approval of the Export Control Authorities of its country if any.

The above restriction does not apply to information which:

- is or subsequently becomes (other than by breach by the LICENCEE of its obligations under this agreement) public knowledge; or
- is received by the LICENCEE without restriction on disclosure or use from a third party and without breach by a third party of any obligations of confidentiality to the CUSTODIAN.

If, after five years from the effective date hereof, the LICENCEE has not used the INFORMATION, or if he is no more active in the business mentioned above, he shall return the written INFORMATION which he has received. The LICENCEE is not authorized to keep copies or photocopies; it is forbidden for him to make any further use of the INFORMATION.

In the event that the LICENCEE breaches the obligations of confidentiality imposed on him pursuant to bullets 1 to 10 above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the LICENCEE agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach. The LICENCEE may not be held liable for any indirect or consequential or incidental losses (including loss of profits) suffered by any third party claiming against ETSI.

All disputes which derive from the present undertaking or its interpretation will be settled by the Court of Justice located in Grasse (Alpes Maritimes) and with the application of French Law regarding questions of interpretation.

The obligations of confidentiality herein will not apply vis-à-vis other LICENCEES. Evidence of being a LICENCEE will be given by providing a certified copy of this undertaking duly undersigned.

This undertaking supersedes all prior confidentiality and restricted scope undertakings between the parties and constitutes the entire agreement between the parties. All amendments to this undertaking will be agreed in writing and signed by a duly authorized representative of each of the parties.

Made in two originals, one of which is for the CUSTODIAN, the other for the LICENCEE.

For the CUSTODIAN	For the LICENCEE
.....	.....
(Name, Title (typed))	(Name, Title (typed))
.....	.....
(Name, Title (typed))	(Name, Title (typed))
.....	.....
(Date)	(Date)

History

Document history		
V1.1.1	June 1997	Publication as ETSI TR 101 052
V2.1.1	February 2016	Publication