

**Security Algorithms Group of Experts (SAGE);
Rules for the management of the TETRA standard authentication and key
management algorithm set TAA1**



European Telecommunications Standards Institute

Reference

DTR/SAGE-00011-1 (9qo00ics.PDF)

Keywords

SAGE, security, algorithm, TAA1

ETSI Secretariat

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - 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

X.400

c= fr; a=atlas; p=etsi; s=secretariat

Internet

secretariat@etsi.fr
<http://www.etsi.fr>

Copyright Notification

No part may be reproduced except as authorized by written permission.
The copyright and the foregoing restriction extend to reproduction in all media.

Contents

Intellectual Property Rights.....	4
Foreword	4
1 Scope.....	5
2 References.....	5
3 Abbreviations.....	5
4 TAA1 management structure	6
5 Distribution Procedures	7
5.1 Distribution by TAA1 Custodian.....	7
5.2 Transfers by a Licencee	8
5.3 Distribution of TAA1 specification Part 3 by the TAA1 Custodian	8
6 Approval criteria and restrictions	8
7 The TAA1 Custodian.....	9
7.1 Responsibilities.....	9
7.2 Appointment	9
Annex A: Items delivered to approved recipient of TAA1	11
Annex B: Confidentiality and Restricted Usage Undertaking for TAA1.....	12
History	15

Intellectual Property Rights

ETSI has not been informed of the existence of any Intellectual Property Right (IPR) which could be, or could become essential to the present document. However, pursuant to the ETSI Interim IPR Policy, no investigation, including IPR searches, has been carried out. No guarantee can be given as to the existence of any IPRs which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project Security Algorithms Group of Experts (SAGE).

1 Scope

The purpose of the present document is to specify the rules for the management of the TETRA standard encryption algorithm TAA1. This algorithm is intended for air interface encryption 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 this TR apply to Part 1 and Part 2 of the specifications. The 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 subclause 5.3). 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 the TAA1 (ETSI, ETSI PROJECT TETRA, TAA1 Custodian and approved recipients) together with the relationships and interactions between them.

The procedures for delivering the 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 5 is concerned with the criteria for approving an organization for receipt of the 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 6 is concerned with the appointment and responsibilities of the TAA1 Custodian. Furthermore in this clause the temporary role of the Interim Custodian is described.

2 References

There are no references required for the use of this document.

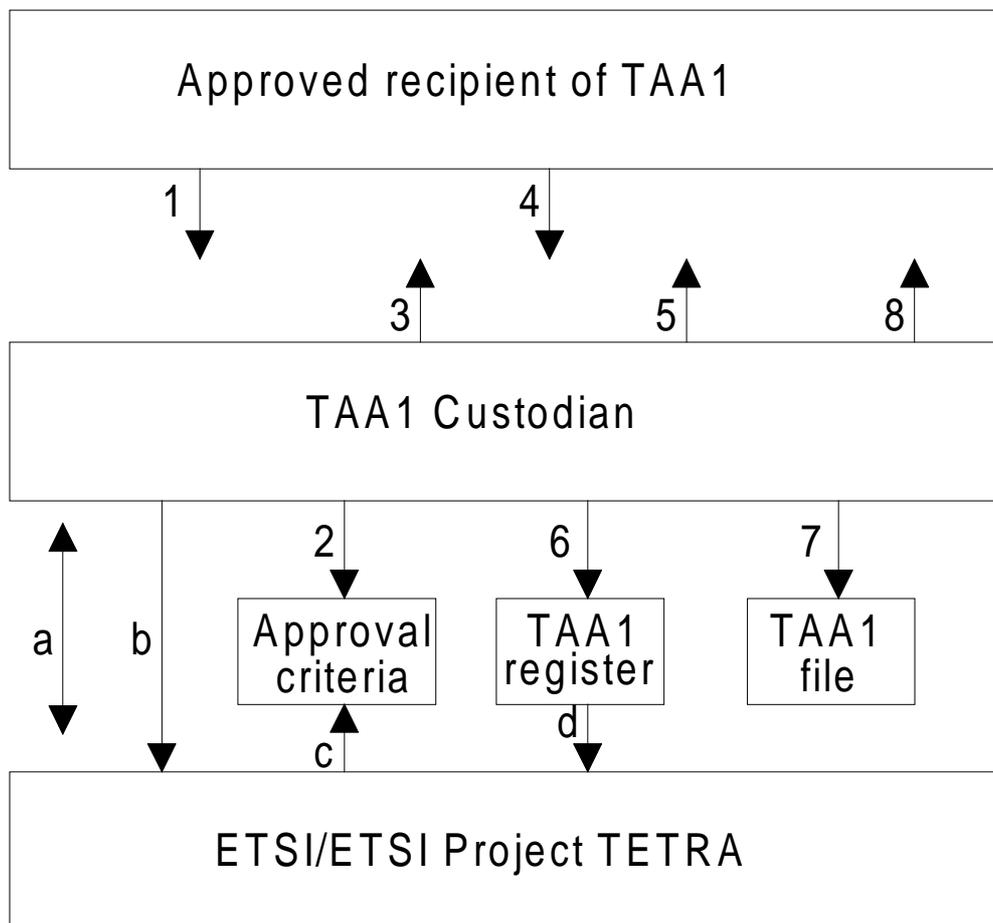
3 Abbreviations

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

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 = Restricted 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

The figure shows the three principals involved in the management of the TAA1 and the relationships and interactions between them.

ETSI is the owner of the TAA1. The ETSI Secretariat together with ETSI Project TETRA sets the approval criteria for receipt of the algorithm (see clause 5).

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

The Custodian shall be the ETSI Secretariat unless it is decided by ETSI Secretariat and/or ETSI Project TETRA to (temporary) 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 5. They include distributing the TAA1 to approved recipients, as detailed in clause 5, providing limited technical advice to approved recipients and providing algorithm status reports to ETSI Project TETRA.

5 Distribution Procedures

5.1 Distribution by TAA1 Custodian

The following procedures for distributing the TAA1 to approved recipients are defined with reference to figure 1.

- 1) The TAA1 Custodian receives a written request for N copies of the TAA1 specification (see note 1).
- 2) The TAA1 Custodian indicates whether the requesting organization meets the approval criteria (see clause 6). In case of non-compliance of the organization with the approval criteria, the Custodian shall justify its decision.
- 3) 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 this document (Rules for the Management of the TETRA Standard Encryption Algorithm TAA1).
- 4) Both copies of the Confidentiality and Restricted Usage Undertaking shall be signed by the approved recipient (see notes 5 and 7) and returned to the TAA1 Custodian, together with the payment of charges if any.
- 5) The TAA1 Custodian sends up to N numbered copies (see note 3) of the TAA1 specification to the approved recipient, together with one countersigned copy of the returned Confidentiality and Restricted Usage Undertaking and a covering letter (see notes 4 and 6).
- 6) 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).
- 7) The TAA1 Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking in the TAA1 File together with a copy of the covering letter sent to the approved recipient.
- 8) The TAA1 Custodian may provide very limited technical advice with respect to answering questions concerning the TAA1 specification.

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

NOTE 2: The confidentiality and Restricted Usage Undertaking specifies the number of copies requested.

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

NOTE 4: The TAA1 Custodian sends all items listed in Appendix 1. 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 signed by the second organization. Refer to the Transfer details given in subclause 5.2.

NOTE 6: Under normal circumstances the 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 Transfers by a Licencee

An organization which has already been approved and has obtained TAA1 specifications may transfer one or more of these specifications, subject to national legislation, to a second organization which requires the specification.

In this case, the first organization has to ensure that the second organization meets the approval criteria. The first organization has to get the second organization to sign two copies of the Confidentiality and Restricted Usage Undertaking. The first organization then sends these to the TAA1 Custodian, together with the numbers of the specifications which are to be transferred.

The TAA1 Custodian then enters the transfer details in the TAA1 Register, countersigns the Confidentiality and Restricted Usage Undertakings, returns one of these together with a covering letter to the first organization, and files the other and a copy of the letter in the TAA1 File.

The first organization is responsible for passing (a copy of) the countersigned Confidentiality and Restricted Usage Undertaking to the second organization.

5.3 Distribution of TAA1 specification Part 3 by the TAA1 Custodian

The following procedures for distributing the TAA1 specification Part 3 are defined:

- 1) The TAA1 Custodian receives a written request for one single copy of the TAA1 specification Part 3.
- 2) The TAA1 Custodian sends one copy of the requested Part 3 of the TAA1 specification Part 3 to the applicant.

6 Approval criteria and restrictions

The approval criteria are set by the ETSI Secretariat together with ETSI Project TETRA 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 one of the TAA1 it has to satisfy at least one of the following criteria:

- C1 The organization is designer of or competent to manufacture TETRA portable or TETRA fixed systems, where the algorithm requested is included in the systems.
- C2 The organization is designer of or competent to manufacture components for TETRA portable or TETRA fixed systems, where at least one of the components includes the algorithm requested.
- C3 The organization is designer of or competent to manufacture a TETRA system simulator for approval testing of TETRA portable or fixed systems, where the simulator includes the algorithm requested.
- C4 The organization intends to use the algorithm requested in order to become an operator of a TETRA system.

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

7 The TAA1 Custodian

7.1 Responsibilities

The TAA1 Custodian is expected to perform the following tasks:

- T1 To approve requests for the TAA1 by reference to the Approval Criteria given in clause 6.
- T2bis To obtain the Administrative authorization and export licences required by the Customs Services of its country if any.
- T2 To exchange the Confidentiality and Restricted Usage Undertaking with approved recipients as described in clause 5.
- T3 To distribute 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 the 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 Project TETRA 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 Project TETRA for improvements/corrections to the specification and, subject to ETSI/ETSI Project TETRA approval, make and distribute the changes (see note 3).
- T9 To provide ETSI/ETSI Project TETRA with information from the TAA1 Register when requested to do so.
- T10 To monitor published advances in crypto-analysis and advise the ETSI Project TETRA of any advances which have a significant impact upon the continued suitability of the TAA1 for the TETRA application.

NOTE 1: Registered postage will be used. If recipients require a different delivery service then they can be excepted 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:

Mr Pierre De Courcel Fax +33 4 93 65 47 16

ETSI

F-06921 Sophia Antipolis Cedex

France

Until the Custodian has arranged all administrative procedures required, an Interim Custodian will be appointed. This Interim Custodian is:

KPN Research, the Netherlands

The contact person is:

Mr Gert Roelofsen

Fax +31 70 3326477

KPN Research

PO Box 421

NL-2260 AK Leidschendam

the Netherlands

Both the TAA1 Custodian as well as the Interim Custodian will ask a fee from the recipient to cover the cost of distribution of Part 1 and Part 2 of the specifications. This fee is set to ECU 1000 per application per algorithm requested (i.e. TAA1).

Both the TAA1 Custodian as the Interim Custodian may ask an optional fee from the recipient to cover the cost of distribution of Part 3 of the specifications.

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

Annex A:

Items delivered to approved recipient of TAA1

ITEM-1: Up to N numbered paper copies to the TAA1 specification where N is the number of copies requested.

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 (see note 1).

NOTE 1: In the case of a transfer (see subclause 5.2), only ITEM-2 and the cover letter are delivered. Moreover, the cover letter details the numbers of the transferred specifications.

Annex B: 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 has alleged, supported by additional information provided, that he fulfills at least one of the following criteria:

- He is designer of or competent to manufacture TETRA portable or TETRA fixed systems where TETRA Standard Encryption Algorithm 1(hereinafter referred to as TAA1) is included in the systems.
- He is designer of or competent to manufacture components for TETRA portable or TETRA fixed systems where at least one of the components include the TAA1.
- He is designer of or competent to manufacture TETRA system simulator for approval testing of TETRA portable or fixed systems where the simulator includes the TAA1.

He will provide the services as an Operator of a TETRA system using the TAA1.

The CUSTODIAN undertakes to give to the LICENCEE:

- registered copies of the detailed specification of the confidentiality algorithm TAA1 Part 1 and Part 2 for protection of the information exchanged over the radio channels of a Trans European Trunked Radio system.

The LICENCEE undertakes:

- 1) To keep strictly confidential all information contained in the detailed specification of the 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) Not to make copies of the TAA1 specifications (all copies of these specifications must be produced, numbered and registered by the TAA1 Custodian).

- 3) Not to disclose the INFORMATION to any third party without prior and explicit authorization in writing by the CUSTODIAN.
- 4) To take measures to avoid that his personnel disclose to third parties, without prior and explicit authorization in writing by the CUSTODIAN, all or part of the INFORMATION.
- 5) To 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 the TAA1 or information in the TAA1 specification.
- 6) Not to register, or attempt to register, any IPR (patents or the like rights) relating to the TAA1 and containing all or part of the INFORMATION.
- 7) To design his equipment in a manner that protects the 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:

ETS 300 392-7: "Trans-European Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security";

ETS 300 393-7: "Trans-European Trunked Radio (TETRA); Packet Data Optimized (PDO); Part 7: Security"; and

ETS 300 396-6: "Trans-European Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

The TAA1 may not be used to provide the end-to-end security services described in these standards.

- 8) Not to subcontract any part of the design and build of his equipment, or the provision of his TETRA services, which requires a knowledge of the TAA1, to any organization which has not signed the Confidentiality and Restricted Usage Undertaking.
- 9) Not to publish a description or analysis of any aspects which may disclose the operation of the TAA1 in any document that is circulated outside the premises of the LICENCEE.

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 9 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

.....

(Name, Title (typed))

.....

(Name, Title (typed))

.....

(Date)

For the LICENCEE

.....

(Name, Title (typed))

.....

(Name, Title (typed))

.....

(Date)

History

Document history		
June 1997	1.1.1	Publication