ETSI TR 101 053-2 V2.2.2 (2008-09)

Technical Report

Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 2: TEA2

Reference

RTR/SAGE-00025-2

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

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 (http://webapp.etsi.org/IPR/home.asp).

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 Report (TR) has been produced by Advisory Committee Security Algorithms Group of Experts (SAGE).

The present document is part 2 of a multi-part deliverable covering 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".

1 Scope

The purpose of the present document is to specify the rules for the management of the TETRA standard encryption algorithm TEA2. This algorithm is intended for air interface encryption in TETRA products.

The specification for TEA2 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. The parts 1 and 2 are confidential.

Part 3 of each of the specifications is not confidential and can be obtained directly from the TEA2 Custodian (see clause 6.5). 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 TEA2 (ETSI, ETSI Technical Committee TETRA, TEA2 Custodian and approved recipients) together with the relationships and interactions between them.

Clause 5 is concerned with the rules for the use of TEA2. This clause is supplemented by clause E in which the states and territories are listed in which a User can become an approved recipient.

The procedures for delivering TEA2 to approved recipients are defined in clause 6. This clause is supplemented by clause A that specifies the items that are to be delivered.

Clause 7 is concerned with the criteria for approving an organization for receipt of TEA2 deliverables and with the responsibilities of an approved recipient. This clause is supplemented by clauses B, C and D which contain a Confidentiality and Restricted Usage Undertaking to be signed by each approved recipient Manufacturer, User and Third Party Supplier.

Clause 8 is concerned with the appointment and responsibilities of the TEA2 Custodian.

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

For online referenced documents, information sufficient to identify and locate the source shall be provided. Preferably, the primary source of the referenced document should be cited, in order to ensure traceability. Furthermore, the reference should, as far as possible, remain valid for the expected life of the document. The reference shall include the method of access to the referenced document and the full network address, with the same punctuation and use of upper case and lower case letters.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area. For non-specific references, the latest version of the referenced document (including any amendments) applies.

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

[i.2] ETSI ETS 300 396-6: "Terrestrial Trunked Radio (TETRA); Direct Mode Operation (DMO); Part 6: Security".

3 Definitions and abbreviations

3.1 Definitions

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

manufacturer: bona fide designer or manufacturer of TETRA subscriber or fixed systems where TETRA Standard Algorithm TEA2 is included in the systems; or a bona fide designer or manufacturer of components for TETRA subscriber or fixed systems where at least one of the components includes TEA2; or a bona fide designer or manufacturer of TETRA system simulator for approval testing of TETRA subscriber or fixed systems where the simulator includes TEA2

primary user: governmental organization for a TETRA network that is primarily used by public safety organizations in their own state or territory

secondary user: military organization in a state or territory where there is no primary user with approval to operate a TETRA network given by the governmental organization that is responsible for public safety

supplier: supplier of TETRA subscriber or fixed systems in which TEA2 is included or of TETRA system simulators in which TEA2 is included, or a third party operator supplying TETRA services with TEA2 to a primary and/or secondary user

third-party operator: user who is not a primary or secondary user who is supplying TETRA services with TEA2 to primary and/or secondary users

user: primary or secondary user

3.2 Abbreviations

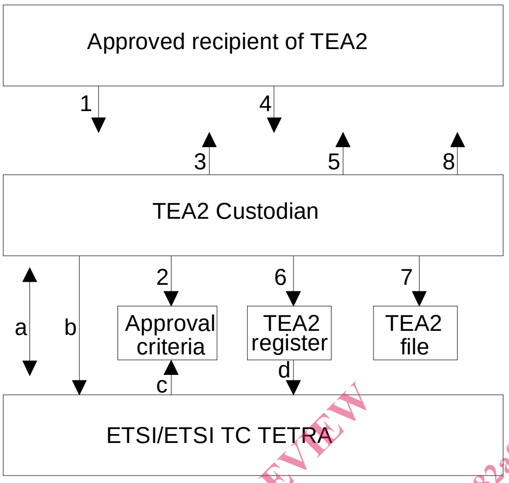
For the purposes of the present document, the following abbreviations apply:

CRUU	Confidentiality and Restricted Usage Undertaking
SFPG	Security and Fraud Prevention Group
SwMI	Switching and Management Infrastructure
TEA2	TETRA Standard Encryption Algorithm 2

TETRA TErrestrial Trunked RAdio

4 TEA2 management structure

The management structure is depicted in figure 1.



NOTE: Key:

a	=	Agreement between TEA2 Custodian and ETSI
b	=	Status reports and recommendations
c	=	Setting of approval criteria
d	=	Restricted details of the TEA2 register
1	=	Request for TEA2
2	=	Check of request against approval criteria
3 and 4	=	Exchange of Confidentiality and Restricted Usage Undertaking
5	=	Dispatch of TEA2 specification
6	=	Update the TEA2 register
7	=	Document filing
8	=	Technical advice

Figure 1: TEA2 management structure

Figure 1 shows the three principles involved in the management of TEA2 and the relationships and interactions between them.

ETSI is the owner of the TEA2. ETSI Technical Committee TETRA sets the approval criteria for receipt of the algorithm (see clause 7).

The TEA2 Custodian is the interface between ETSI and the approved recipients of the TEA2.

The Custodian is as identified in clause 8.2 of the present document. The TEA2 Custodian's duties are detailed in clause 8. They include distributing TEA2 to approved recipients, as detailed in clause 7, providing limited technical advice to approved recipients and providing algorithm status reports to ETSI Technical Committee TETRA.

5 Use of TEA2

5.1 Users of TEA2

A TEA2 User License is given to a governmental organization for a TETRA network that is primarily used by public safety organizations (see note) in their own state or territory. A TETRA network may consist of fixed base stations and SwMI, all located in the home state or territory, and/or one or more base stations and SwMIs that may also be used outside the home state or territory if both base stations and SwMIs are controlled from the home state or territory. A governmental organization that obtains a TEA2 User License under these conditions is referred to as a primary user of TEA2.

NOTE 1: Public safety organizations are e.g. Police, Fire brigade, Customs and Excise, Ambulance and Emergency Medical Service, Coastguard.

NOTE 2: There may be more than one primary user in any allowed state and the number of primary users is a national option.

It is to be decided by the primary user of TEA2, who has received a TEA2 User License from TEA2 custodian, which user organizations can use the above-mentioned network. This may be done on the basis of a sublicensing procedure that may also be needed for the procurement of mobile terminals or movable equipment by a user organization.

A primary user can approve the use of TEA2 in a TETRA network owned by a military organization that is operational in the same state or territory as the primary user. In the case where there is no primary user in that state or territory the military organization has to demonstrate written approval to operate a TETRA network given by the governmental organization that is responsible for public safety. Such military organizations are referred to as secondary users. Also in these cases a TETRA network may consist of fixed base stations and SwMI, all located in the home state or territory, and/or one or more base stations and SwMIs that may also be used outside the home state or territory if both base stations and SwMIs are controlled from the home state or territory.

It is to be decided by the secondary user of TEA2, which has received a TEA2 User License from the TEA2 custodian, those user organizations that can use the above-mentioned network. This may be done on the basis of a sublicensing procedure that may also be needed for the procurement of mobile terminals or movable equipment by a user organization.

5.2 TEA2 States and Territories

Organizations can be a primary or secondary user of TEA2 when it is based and (normally) operates in a state or territory that is at least:

a) a Schengen state (see note 1); or

b) a European Union state (see note 2); or

c) a candidate European Union state (see note 3); or

d) a dependent area of one of the Schengen or (candidate) European Union states (but not overseas (see note 4)); or

e) a state (but not overseas) that has a bilateral agreement with the European Union;

f) a state that only has borders with TEA2 states or territories as in point a) through e).

NOTE 1: Including autonomous regions of that state that are also part of Schengen.

NOTE 2: Including autonomous regions of that state that are also part of the European Union.

NOTE 3: Including autonomous regions of that state that are also candidate part of the European Union.

NOTE 4: Overseas Countries and Territories as in Part Four of the Consolidated version of the Treaty establishing the European Community (2002) plus French overseas territories (French Guyana, Guadeloupe, Martinique, Réunion).

Based on this an initial list of TEA2 states and territories was drafted. This list is added as clause E. The custodian maintains the actual list of TEA2 states and territories.

6 Distribution procedures

6.1 Distribution by TEA2 custodian

The following procedures for distributing TEA2 to approved recipients are defined with reference to figure 1:

1) The TEA2 Custodian receives a written request for N copies of the TEA2 specification (see note 1) or a written request for entering in a Confidentiality and Restricted Usage Undertaking for a user or a third party supplier of TETRA equipment containing TEA2.

2) The TEA2 Custodian indicates whether the requesting organization meets the approval criteria (see clause 7).

3) If the request is approved, the TEA2 Custodian dispatches 2 copies of the corresponding Confidentiality and Restricted Usage Undertaking (as given in clause B, C or D) 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 Encryption Algorithm TEA2).

4) Both copies of the Confidentiality and Restricted Usage Undertaking are to be signed by the approved recipient (see notes 5 and 7) and returned to the TEA2 Custodian, together with the payment of charges (if any).

5) The TEA2 Custodian sends up to N (see note 3) numbered copies of the TEA2 specification to the approved recipient and one countersigned copy of the returned Confidentiality and Restricted Usage Undertaking and a covering letter (see notes 4 and 6).

6) The TEA2 Custodian updates the TEA2 Register by recording the name and address of the recipient, the numbers of the copies of the TEA2 specification delivered, if any, and the date of delivery. If the original request is not approved, the TEA2 Custodian records the name and address of the requesting organization and the reason for rejecting the request in the TEA2 Register (see also note 8).

7) The TEA2 Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking in the TEA2 File together with a copy of the covering letter sent to the approved recipient.

8) The TEA2 Custodian may provide very limited technical advice with respect to answering questions concerning the TEA2 specification.

9) In case an organization cannot comply with the rules as described in the present document the TEA2 custodian can still decide, on an exceptional basis, to distribute the TEA2 algorithm to this organization. In this case the TEA2 custodian will inform ETSI SAGE and TC TETRA about his decision and at the same time provide a motivation. If a special Confidentiality and Restricted Usage Undertaking (i.e. different from clause B, C or D) is used, the TEA2 custodian will first ask the ETSI Legal Department to approve this Confidentiality and Restricted Usage Undertaking (CRUU).

NOTE 1: Requests for the TEA2 specification may be made directly to the TEA2 Custodian or through ETSI, where appropriate.

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

NOTE 3: N may be 0. In case specifications of TEA2 are delivered the covering letter specifies the numbers of the copies delivered.

NOTE 4: The TEA2 Custodian sends all items listed in clause A. Requests for part of the package of items will be rejected.

NOTE 5: An organization may request the specification on behalf of a second organization. In this case, the first organization is responsible for returning a Confidentiality and Restricted Usage Undertaking signed by the second organization. Refer to the details given in clauses 6.2, 6.3 and 6.4.

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 TEA2 specification is returned to the TEA2 Custodian (for example the recipient may decide not to make use of the information), then the TEA2 Custodian destroys the specification and enters a note to this effect in the TEA2 Register.

6.2 Transfers by a licencee

An organization which has already been approved and has obtained TEA2 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 for Manufacturers of TEA2 as in clause B. The first organization then sends these to the TEA2 Custodian, together with the numbers of the specifications that are to be transferred.

The TEA2 Custodian then enters the transfer details in the TEA2 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 TEA2 File.

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

6.3 Distribution of TETRA equipment containing TEA2 through a third party

NOTE: This clause covers the "supplier" licence type.

A TETRA manufacturer that has already been approved and has obtained TEA2 specifications may be allowed, subject to national legislation, to distribute TETRA equipment containing TEA2 via a third party.

In this case, the TETRA manufacturer has to get the third party to sign two copies of the Confidentiality and Restricted Usage Undertaking for Suppliers (see clause D). The TETRA manufacturer then sends these to the TEA2 Custodian.

The TEA2 Custodian then enters the transfer details in the TEA2 Register, countersigns the Confidentiality and Restricted Usage Undertakings, returns one of these together with a covering letter to the TETRA manufacturer, and files the other and a copy of the letter in the TEA2 File.

The TETRA manufacturer is responsible for passing (a copy of) the countersigned Confidentiality and Restricted Usage Undertaking to the third party.

6.4 Third party operator supplying TETRA services with TEA2

NOTE: This clause covers the "supplier" licence type.

There may be a third party operator who is not a primary or secondary user, but who is supplying TETRA services with TEA2 to primary and/or secondary users.

In this case, the third party operator has to sign two copies of the Confidentiality and Restricted Usage Undertaking for Suppliers (see clause D) and sends these to the TEA2 Custodian.

The TEA2 Custodian then enters the transfer details in the TEA2 Register, countersigns the Confidentiality and Restricted Usage Undertakings, returns one of these together with a covering letter to the third party operator, and files the other and a copy of the letter in the TEA2 File.