ETSI TR 101 053-2 V2.2.4 (2012-06)

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

Reference
RTR/SAGE-00027-2

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

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://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 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 annexes B, C, CA 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 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 http://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.

2.1 Normative references

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

Not applicable.

2.2 Informative references

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

[i.3] ETSI TR 101 053-1: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 1: TEA1".

[i.4] ETSI TR 101 053-3: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 3: TEA3".

3 Definitions and abbreviations

3.1 Definitions

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

end user: user organization that has been approved to use TEA2 by either the primary or secondary user

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 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

user: primary or secondary user

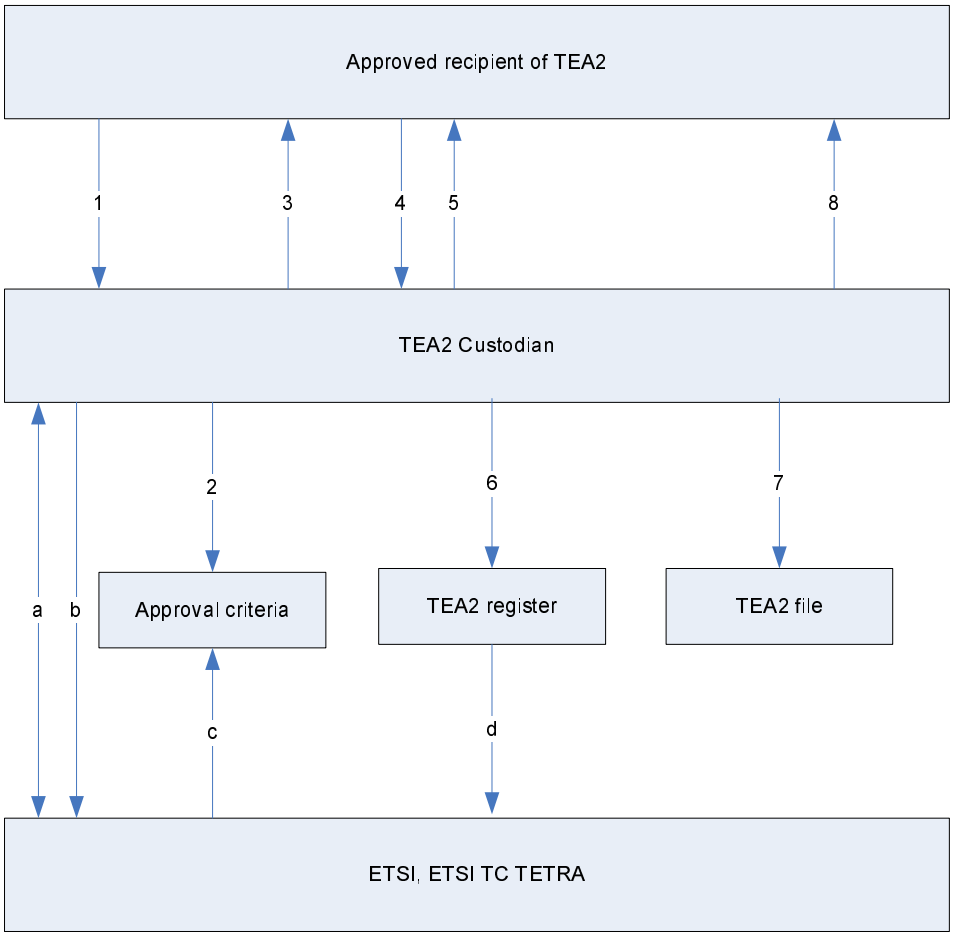
3.2 Abbreviations

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

CRUU	Confidentiality and Restricted Usage Undertaking
MS	Mobile Station
SFPG	Security and Fraud Prevention Group
TETRA	TErrestrial Trunked RAdio

4 TEA2 management structure

The management structure is depicted in figure 1.



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 principals 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.

The form of CRUU exchanged is summarised in figure 2.

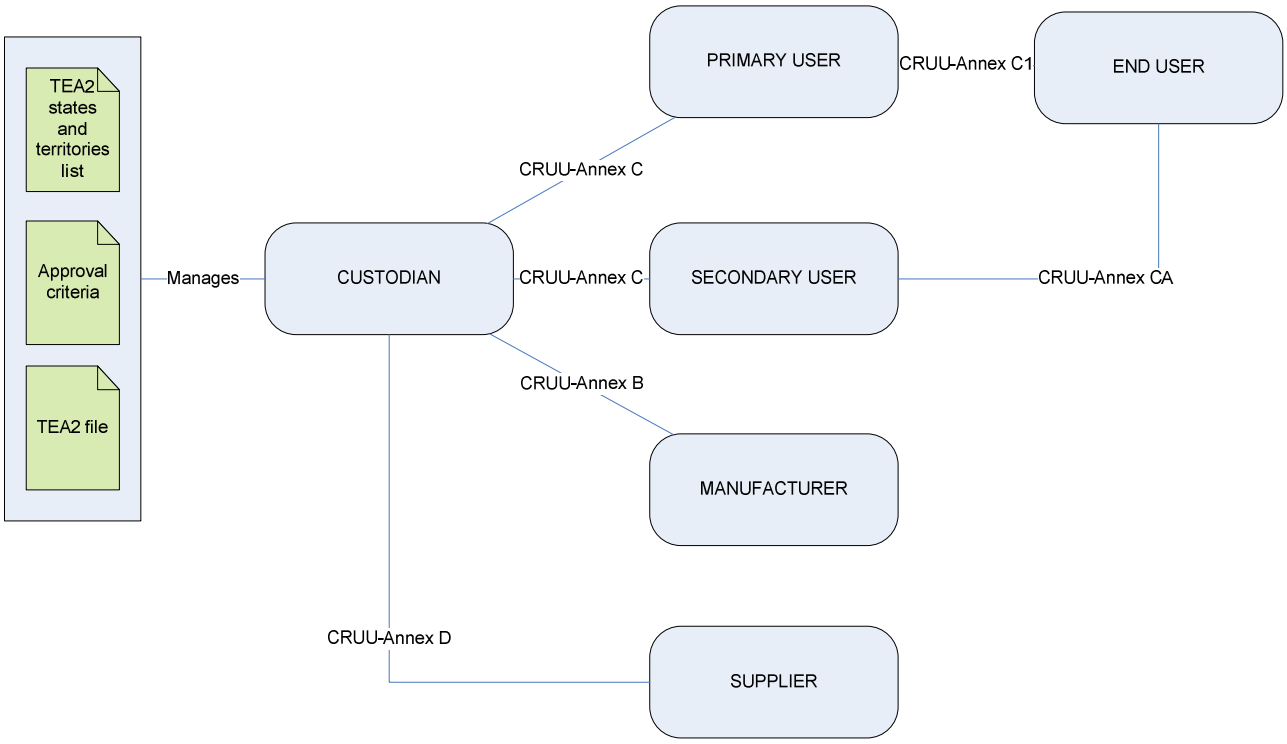


Figure 2: Summary of CRUU types maintained between TEA2 principals

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 1) 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. The Confidentiality and Restricted Usage Undertaking (CRUU) in annex C applies to primary users (see note 2). The TEA2 license is required for the use of TEA2 in any element of the TETRA network including TETRA Terminals (TETRA Mobile Station (MS)) where air interface encryption as defined in EN 300 392-7 [i.1] or ETS 300 396-6 [i.2] is applied.

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 or user organization. An organization that obtains a TEA2 End User License under these conditions is referred to as an end user of TEA2. The CRUU in annex CA applies to end users.

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 in its home state or territory. Such military organizations are referred to as secondary users. The CRUU in annex C applies to secondary users. Again 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. A military organization licensed as above may use its TEA2 network and terminal equipment in connection with its deployment in any location outside of the TEA2 approved states and territories subject to the permission of its primary user or governmental organization responsible for public safety, and the relevant export authority. When so deployed the use of the network and associated equipment is limited to members of that military organization and others associated with that deployment. The network and associated equipment must remain under the management of the owning military organization who will remain responsible and liable under the terms and conditions contained within the CRUU. Agreed standard operating procedures, including a strong and robust audit and accounting process, must be in place. All network and associated equipment must be recovered upon completion of that deployment.

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);

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

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

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

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

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 annex E. The custodian maintains the actual list of TEA2 states and territories.

6 Distribution procedures

6.1 Distribution by TEA2 custodian

NOTE: This clause covers the "supplier", "manufacturer", "primary user" and "secondary user" licence types.

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 into a Confidentiality and Restricted Usage Undertaking for 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 annexes 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 have 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).

10) In case the contact details of the signatory change the custodian should be informed.

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 authorised 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 Authorisation to use TEA2 from a primary or secondary user to an end user

NOTE: This clause covers the "end user" licence type (CRUU defined in annex CA).

An organization which has already been approved and has obtained TEA2 specifications as a primary user or as a secondary user may act as a licensor for end user organizations in the area of jurisdiction of the primary or secondary user.

In this case, the primary user or secondary user hereinafter referred to as the first organization has to ensure that the end user hereinafter referred to as 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 End users of TEA2 as in annex CA. The first organization is expected to maintain a record of the end users with whom it has signed a CRUU. CRUUs signed in accordance with this process may be 'time limited' as determined by the primary or secondary user to meet their operational needs.

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 annex 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 annex 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.

6.5 Use of TEA2 by a secondary user

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

As described in clause 5.1 a military organization can become an approved recipient. Such a military organization is referred to as a secondary user.

There are two cases:

1) There is a primary user in the home state or territory that is responsible for the public safety network containing TEA2.

2) There is no such primary user in the home state or territory.

In the first case, the primary user has to ensure that the intended secondary user meets the approval criteria (i.e. fulfils Approval Criterion C5 as in clause 7). The primary user has to get the intended secondary user to sign two copies of the Confidentiality and Restricted Usage Undertaking for Users of TEA2 as in annex C. The primary user 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 to the primary user together with a covering letter and files the other and a copy of the letter in the TEA2 File. The primary user transfers the Confidentiality and Restricted Usage Undertaking to the secondary user.

In the second case the secondary user has to demonstrate to the custodian written approval to operate a TETRA network given by the governmental organization that is responsible for public safety in the home state or territory. The secondary user signs two copies of the Confidentiality and Restricted Usage Undertaking for Users of TEA2 as in clause C. The secondary user 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 secondary user, and files the other and a copy of the letter in the TEA2 File.

6.6 Distribution of TEA2 specification part 3 by the TEA2 custodian

The following procedures for distributing the TEA2 specification part 3 are defined:

1) The TEA2 Custodian receives a written request for one single copy of the TEA2 specification part 3.

2) The TEA2 Custodian sends one copy of the requested part 3 of the TEA2 specification part 3 to the applicant.

7 Approval criteria and restrictions

The approval criteria are set by the ETSI TC TETRA and maintained by the TEA2 Custodian. The TEA2 Custodian may recommend changes to these criteria.

In order for an organization to be considered an approved recipient of TEA2 deliverables 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 systems, 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 systems, 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 approval testing of TETRA subscriber or fixed systems, where the simulator includes the algorithm requested.

C4 The organization is a governmental organization for a network that is primarily used by public safety organizations in the own state or territory as listed in clause E. This is referred to as a primary user.

C5 The organization is a military organization operating a TETRA network in a state or territory where also a TETRA network of a primary user is in operation (see note).

NOTE: In this case the primary user has to arrange the singing of Confidentiality and Restricted Usage Undertakings as specified in clause 6.4.

C6 The organization is a military organization operating a TETRA network in a state or territory as listed in clause E where there is no public safety TETRA network but where written approval to operate a TETRA network by the governmental organization that is responsible for public safety has been demonstrated.

C7 The organization has been appointed by a TETRA manufacturer as a third party supplier for TETRA equipment containing the TEA2 algorithm.

The TEA2 Custodian will decide whether an organization requesting the TEA2 specification may be considered to be an approved recipient.

7.1 Revocation of TEA2 licences

The Custodian reserves the right to revoke any TEA2 licence and require return of all related documentation in case:

- any of the approval criteria cease to apply;
- expiry of a time limited licence;
- any breach of the Licensee undertakings as contained in the relevant CRUU.

7.2 Appeal against Licence Revocation

Appeals against revocation are initially to be addressed to, and considered by the TEA2 Custodian and thereafter may be referred to ETSI TC TETRA for a final decision.

8 The TEA2 custodian

8.1 Responsibilities

The TEA2 Custodian is expected to perform the following tasks:

T1 To approve requests for TEA2 or an exchange for a Confidentiality and Restricted Usage Undertaking by reference to the Approval Criteria given in clause 7.

T2bis To obtain the Administrative authorisation 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 6.

T3 To distribute, if required, the TEA2 specifications as detailed in clause 6 (see note 1).

T4 To maintain the TEA2 Register as described in clause 6.

T5 To hold in custody the contents of the TEA2 File as specified in clause 6.

T6 To provide recipients of TEA2 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 TETRA of any problems arising with the approval criteria.

T8 In the light of written queries from recipients of the TEA2 specifications, to make recommendations to ETSI/ETSI TC TETRA for improvements/corrections to the specification and, subject to ETSI/ETSI TC TETRA approval, make and distribute the changes (see note 3).

T9 To provide ETSI/ETSI TC TETRA with information from the TEA2 Register when requested to do so.

T10 To monitor published advances in crypto-analysis and advise the ETSI TC TETRA of any advances which have a significant impact upon the continued suitability of TEA2 for the TETRA application.

NOTE 1: For the distribution of TEA2 specifications 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 TEA2 Custodian will only endeavour to answer questions relating to the TEA2 specifications. He is not expected to provide technical support for development programmes.

NOTE 3: Numbered copies of any changes to the TEA2 specifications will be automatically distributed to all recipients of the specification and a record of the distribution entered in the TEA2 Register.

8.2 Appointment

The TEA2 Custodian is agreed by the ETSI Secretariat (as owner of TEA2) and ETSI Technical Committee TETRA as:

The TETRA Association

Custodianship is entrusted to the chair of the Security and Fraud Prevention Group (SFPG) who should be a non-commercial member of the TETRA Association. Where this is not the case it will revert to the Chief Executive Officer of the TETRA Association.

The contact person is:

Mrs. Marjan Bolle Fax: +31 70 320 02 56

Wildenborch 63, 2261 XK Leidschendam

The Netherlands

e-mail: SFPG@tetra-association.com

The TEA2 Custodian will ask a fee from the recipient to cover the cost of distribution of parts 1 and 2 of the specifications. The fees are set out in table 8.1 for each licencee type and item as specified in annex A. The fees are subject to review. The TEA2 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 TEA2 specification parts 1 and 2 or the TEA2 specification part 3 should be addressed to the indicated contact person.

Table 8.1: Fees for distribution of TEA2 (as of July 1st 2008)

Licencee	ITEM-1 (Parts 1 and 2 of the specification)	ITEM-2 (CRUU) (note 1)	ITEM-3 (Covering letter)	Part 3 of specification
User (note 2)	500 €/numbered copy	500 €	No charge	Discretionary
Manufacturer	500 €/numbered copy	500 €	No charge	Discretionary
Supplier	Not provided	500 €	No charge	Not provided
End user	Not provided	Discretionary (note 3)	No charge	Not provided
NOTE 1: Each registration of a CRUU invokes a fee due of 500 € from the registering party. NOTE 2: Parts 1 and 2 should only be supplied to users with due authority. NOTE 3: A fee is applied at the discretion of the primary or secondary user, or may be paid directly to the custodian.				

Annex A:
Items delivered to approved recipient of TEA2

ITEM-1: Up to N numbered paper copies to the TEA2 specification where N is the number of copies requested (see note).

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

ITEM-3: A cover letter from and signed by the TEA2 Custodian listing the delivered items (ITEMS-1 and-2) and the numbers of the specifications delivered.

NOTE: Only in the case where copies of TEA2 are requested and approved.

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

Annex B:
Confidentiality and Restricted Usage Undertaking for Manufacturers of TEA2

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the TEA2 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 fulfils at least one of the following criteria:

- He is a bona fide designer or manufacturer of TETRA subscriber or fixed systems where TETRA Standard Encryption Algorithm 2 (hereinafter referred to as TEA2) is included in the systems.
- He is a bona fide designer or manufacturer of components for TETRA subscriber or fixed systems where at least one of the components includes TEA2.
- He is a bona fide designer or manufacturer of TETRA system simulator for approval testing of TETRA subscriber or fixed systems where the simulator includes TEA2.

The CUSTODIAN undertakes to give to the LICENCEE:

- Registered copies of the detailed specification of the confidentiality algorithm TEA2 parts 1 and 2 for protection of the information exchanged over the radio channels of a TETRA system.

The LICENCEE undertakes:

1) To keep strictly confidential all information contained in the detailed specification of TEA2 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 TEA2 specifications (all copies of these specifications must be produced, numbered and registered by the TEA2 Custodian).

3) Not to disclose the INFORMATION to any third party without prior and explicit authorisation in writing by the CUSTODIAN.

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

5) To use the INFORMATION in the TEA2 specification exclusively for the provision of TETRA components, systems or services, thus refraining from making any other use of TEA2 or information in the TEA2 specification.

6) Not to register, or attempt to register, any IPR (patents or the like rights) relating to TEA2 and containing all or part of the INFORMATION.

7) To design his equipment in a manner that protects TEA2 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:

   EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security"; and

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

   TEA2 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 knowledge of TEA2, 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 TEA2 in any document that is circulated outside the premises of the LICENCEE.

10) To only provide equipment containing TEA2 for TETRA applications to a user who is responsible for this intended TETRA application or to a supplier of TETRA equipment for these TETRA applications who have signed a Confidentiality and Restricted Usage Undertaking for users of TEA2 (as in clause C) or a Confidentiality and Restricted Usage Undertaking for Suppliers of Equipment containing TEA2 with the TEA2 Custodian. Before supplying equipment incorporating TEA2, the Licencee has to verify that this responsible user or supplier has requested this user or supplier to supply him with a copy of the respective Confidentiality and Restricted Usage Undertaking for TEA2 which is countersigned by the Custodian.

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 authorised 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 authorised 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)

Annex C:
Confidentiality and Restricted Usage Undertaking for Primary and Secondary Users of TEA2

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the TEA2 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 fulfils at least one of the following criteria:

- The organization is a governmental organization for a network that is primarily used by public safety organizations in their own state or territory as listed in the TEA2 state and territory list that is maintained by the custodian. This is referred to as a primary user.
- The organization is a military organization operating a TETRA network in a state or territory where a TETRA network of a primary user is also in operation.
- The organization is a military organization operating a TETRA network in a state or territory as listed in the TEA2 state and territory list that is maintained by the custodian where there is no public safety TETRA network but where written approval by the governmental organization that is responsible for public safety has been demonstrated.

Description of intended application and user group(s)
……..
……..
……..
……..
……..

If requested by the LICENCEE the CUSTODIAN undertakes to give to the LICENCEE:

- One registered copy of the detailed specification of the confidentiality algorithm TEA2 parts 1 and 2 for protection of the information exchanged over the radio channels of a TETRA system.

The LICENCEE undertakes:

1) To keep strictly confidential all information related to TEA2 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 disclose the INFORMATION to any third party without prior and explicit authorisation in writing by the CUSTODIAN.

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

4) Not to register, or attempt to register, any IPR (patents or the like rights) relating to TEA2 and including all or part of the INFORMATION.

5) To use equipment containing TEA2 only to provide the TETRA air interface security services for which it is intended.

   These services are specified in the following standards:

   EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security"; and

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

   TEA2 may not be used to provide the end-to-end security services described in these standards.

6) To use equipment containing TEA2 only for providing TETRA services to user groups as limited by this undertaking.

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.

In the event that the LICENCEE breaches the obligations of confidentiality imposed on him pursuant to bullets 1 to 6 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 authorised 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)

Annex CA:
Confidentiality and Restricted Usage Undertaking for End Users of TEA2

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the TEA2 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 USER.

NOTE: Only primary and secondary users may adopt the role of user for the purposes of this CRUU.

Whereas

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

- The organization has been identified by the primary user as a legitimate end user of a network that is primarily used by public safety organizations in their own state or territory as listed in the TEA2 state and territory list that is maintained by the custodian.
- The organization has been identified by the secondary user as a legitimate end user of a network that is primarily used by public safety organizations in their own state or territory as listed in the TEA2 state and territory list that is maintained by the custodian.

Description of intended application and user group(s)
……..
……..
……..
……..
……..

FOR CLARIFICATION: The LICENCEE is not expected to request a copy of the detailed specification of the confidentiality algorithm TEA2 parts 1 and 2.

The LICENCEE undertakes:

1) To use equipment containing TEA2 only to provide the TETRA air interface security services for which it is intended.

   These services are specified in the following standards:

   EN 300 392-7: "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 7: Security"; and

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

   TEA2 may not be used to provide the end-to-end security services described in these standards.

2) To use equipment containing TEA2 only for providing TETRA services to user groups as limited by this undertaking.

3) To undertake not to pass on equipment containing TEA2 to a third party without validating the permission of the third party to hold equipment containing TEA2.

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 authorised representative of each of the parties.

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

For the USER	For the LICENCEE
….....	.....
(Name, Title (typed))	(Name, Title (typed))

.....	.....
(Name, Title (typed))	(Name, Title (typed))
.....	.....
(Date)	(Date)

Annex D:
Confidentiality and Restricted Usage Undertaking for Suppliers

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the TEA2 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 ….....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas

The LICENCEE has alleged, that he fulfils at least one of the following criteria:

- He is a supplier of TETRA subscriber or fixed systems in which the TETRA Standard Encryption Algorithm 2 (hereinafter referred to as TEA2) is included or TETRA system simulators in which TEA2 is included.
- He is a third party operator supplying TETRA services with TEA2 to a primary and/or secondary user.

The LICENCEE undertakes:

1) To keep strictly confidential all information related to TEA2 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 disclose the INFORMATION to any third party without prior and explicit authorisation in writing by the CUSTODIAN.

3) To take measures to avoid that his personnel disclose to third parties, without prior and explicit authorisation in writing by the CUSTODIAN, all or part of the INFORMATION.

4) Not to register, or attempt to register, any IPR (patents or the like rights) relating to TEA2 and containing all or part of the INFORMATION.

5) To only provide equipment containing TEA2 for TETRA applications where the user who is end responsible for this intended TETRA application has signed a Confidentiality and Restricted Usage Undertaking for users of TEA2 with the TEA2 Custodian. Before supplying equipment incorporating TEA2, the Licencee has to verify that this end responsible user has to request this user to supply him with a copy of the Confidentiality and Restricted Usage Undertaking for users of TEA2 which is countersigned by the Custodian.

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.

In the event that the LICENCEE breaches the obligations of confidentiality imposed on him pursuant to bullets 1 to 5 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 authorised 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)

Annex E:
TEA2 State and Territories list

The list below is an initial list showing in which countries TEA2 can be used. The custodian maintains the actual list of States and Territories.

Category: / State/territory:	Can use TEA2	Schengen state or European state	Dependent area or only borders with other TEA2 states	European Union Candidate state
Andorra	Yes		X	
Austria	Yes	X		
Belgium	Yes	X		
Bulgaria	Yes	X		
Channel Islands	Yes		X	
Croatia	Yes			X
Cyprus	Yes	X		
Czech republic	Yes	X		
Denmark	Yes	X		
Estonia	Yes	X		
Faroe Islands	Yes		X	
Finland	Yes	X		
France	Yes	X		
Germany	Yes	X		
Gibraltar	Yes		X	
Greece	Yes	X		
Hungary	Yes	X		
Iceland	Yes	X		
Ireland	Yes	X		
Isle of Man	Yes		X	
Italy	Yes	X		
Latvia	Yes	X		
Liechtenstein	Yes		X	
Lithuania	Yes	X		
Luxembourg	Yes	X		
Macedonia	Yes			X
Malta	Yes	X		
Monaco	Yes		X	
Netherlands	Yes	X		
Norway	Yes	X		
Poland	Yes	X		
Portugal	Yes	X		
Romania	Yes	X		
San Marino	Yes		X	
Slovakia	Yes	X		
Slovenia	Yes	X		
Spain	Yes	X		
Svalbard	Yes		X	
Sweden	Yes	X		
Switzerland	Yes		X	
Turkey	Yes			X
United Kingdom	Yes	X		
Vatican	Yes		X	
Other states/territories	No			

History

Document history		
V1.1.1	June 1997	Publication
V1.1.2	October 1998	Publication
V2.1.1	September 2003	Publication
V2.2.1	March 2005	Publication
V2.2.2	September 2008	Publication
V2.2.3	June 2010	Publication
V2.2.4	June 2012	Publication