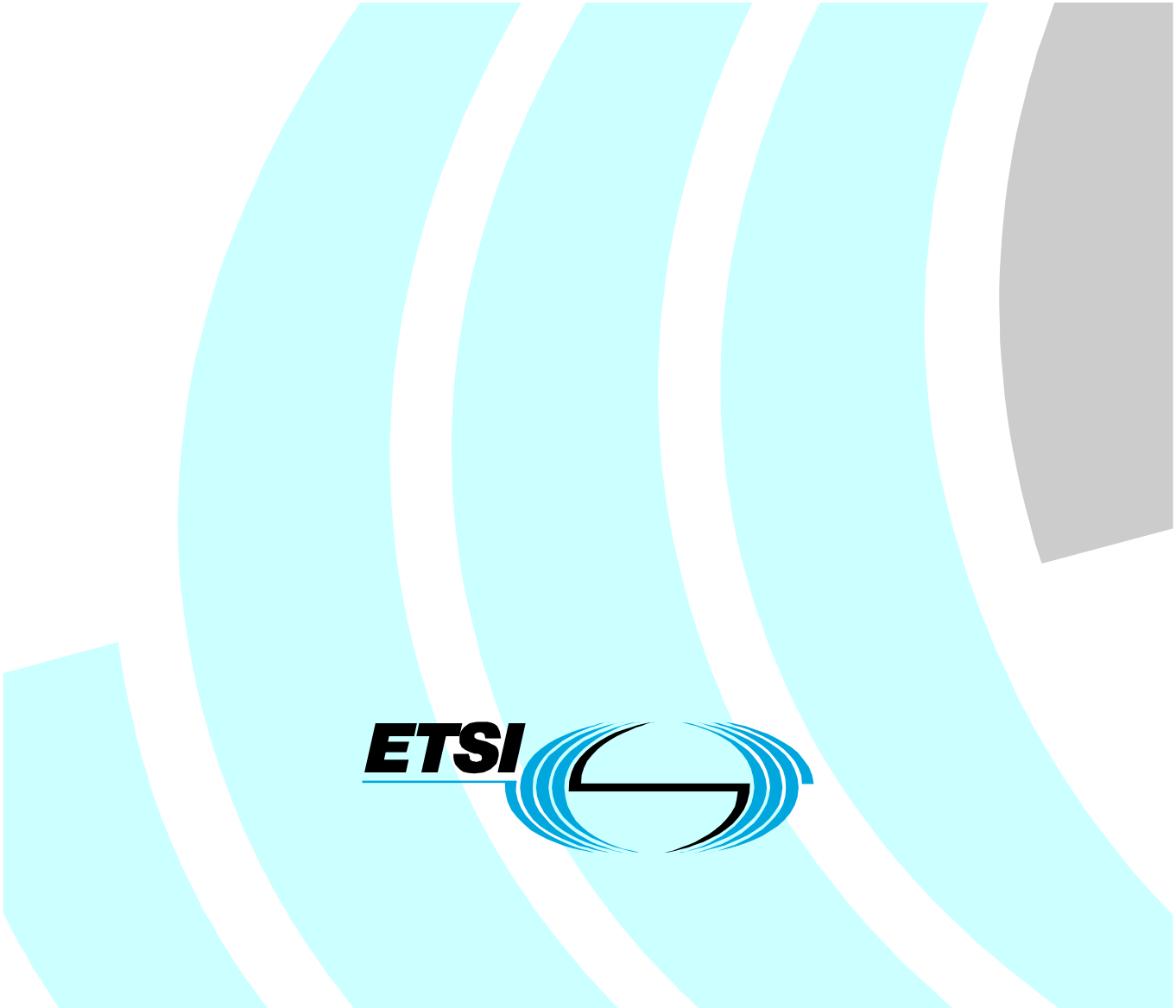
ETSI TR 101 053-2 V2.2.1 (2005-03)

Technical Report

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



Reference
RTR/SAGE-00022-2

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://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 the TEA2 (ETSI, ETSI PROJECT 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 annex E in which the states and territories are listed in which a User can become an approved recipient

The procedures for delivering the TEA2 to approved recipients are defined in clause 6. This clause is supplemented by annex 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 and D which contains 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

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

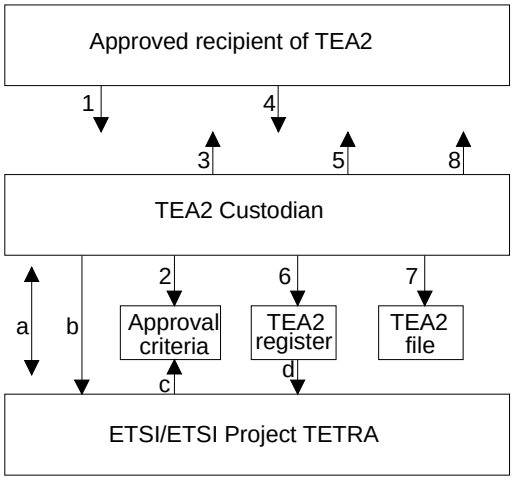
3 Abbreviations

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

TEA2	TETRA Standard Encryption Algorithm 2
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 principles involved in the management of the TEA2 and the relationships and interactions between them.

ETSI is the owner of the TEA2. ETSI Project 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 shall be the ETSI Secretariat unless it is decided ETSI Project TETRA to (temporarily) delegate this task to a third party on the basis of an agreement between the latter and the ETSI Secretariat. The TEA2 Custodian's duties are detailed in clause 8. They include distributing the TEA2 to approved recipients, as detailed in clause 7, providing limited technical advice to approved recipients and providing algorithm status reports to ETSI Project TETRA.

5 Use of the TEA2

5.1 Users of the 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 the TEA2.

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

It is to be decided by the primary user of the TEA2, who has received a TEA2 User License from the 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 the 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 the 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 the 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 annex 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 the 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 the 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 annex 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 shall 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 EPT TETRA about his decision and at the same time provide a motivation. If a special Confidentiality and Restricted Usage Undertaking (i.e. different from annex B, C or D) is used, the TEA2 custodian will first ask the ETSI Legal Department to approve this Confidentiality and Restricted Usage Undertaking.

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 the TEA2 are delivered the covering letter specifies the numbers of the copies delivered.

NOTE 4: The TEA2 Custodian sends all items listed in annex 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 annex 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 the TEA2 through a third party

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 the 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

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

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, at the same time indicating if the secondary user requires a copy of the TEA2 specification.

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, if required, a copy of the TEA2 specification and files the other and a copy of the letter in the TEA2 File. The primary user transfers the Confidentiality and Restricted Usage Undertaking and, if applicable, the copy of the TEA2 specification 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 annex C. The secondary user then sends these to the TEA2 Custodian, at the same time indicating if he requires a copy of the TEA2 specification.

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 and, if required a copy of the TEA2 specification, 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 Project 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 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 a 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 a 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 is a governmental organization for a network that is primarily used by public safety organizations in the own state or territory as listed in annex 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 annex 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.

8 The TEA2 custodian

8.1 Responsibilities

The TEA2 Custodian is expected to perform the following tasks:

T1 To approve requests for the 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 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 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 the 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 Project 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 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 TEA2 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 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:

ISC, the Netherlands

The contact person is:

ISC

attn. Mr. Hanno Steenbergen Fax: +31 343 534799

PO BOX 238

NL-3970 AE Driebergen

The Netherlands

The TEA2 Custodian will ask a fee from the recipient to cover the cost of distribution of parts 1 and 2 of the specifications. This fee is set to Euro 1 000 per application, this including the entering into a Confidentiality and Restricted Usage Undertaking. The fee for entering a user into a Confidentiality and Restricted Usage Undertaking without distribution of part 1 and 2 of the specifications is set to Euro 500. The fee for entering a third party operator into a Confidentiality and Restricted Usage Undertaking is set to Euro 500.

The TEA2 Custodian may ask an optional fee from the recipient to cover the cost of distribution of Confidentiality and Restricted Usage Undertakings or 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.

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 1).

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 (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered (see note 2).

NOTE 1: Only in the case where copies of the TEA2 are requested.

NOTE 2: In the case of a transfer (see clause 6.2), 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 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 designer of or competent to manufacture TETRA portable or TETRA fixed systems where TETRA Standard Encryption Algorithm 2 (hereinafter referred to as TEA2) 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 includes the TEA2.
- 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 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 Trans European Trunked Radio system.

The LICENCEE undertakes:

1) To keep strictly confidential all information contained in the detailed specification of the 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 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 TEA2 specification exclusively for the provision of TETRA components, systems or services, thus refraining from making any other use of the TEA2 or information in the TEA2 specification.

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

7) To design his equipment in a manner that protects the 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".

   The 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 the 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 the 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 end 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 the TEA2 (as in annex 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 end responsible user or supplier has request 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 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)

Annex C:
Confidentiality and Restricted Usage Undertaking for 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 territorylist 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 Trans European Trunked Radio system.

The LICENCEE undertakes:

1) To keep strictly confidential all information related to the 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 authorization in writing by the CUSTODIAN.

3) 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.

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

5) To use equipment containing the 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".

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

6) To use equipment containing the 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 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)

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 portable or fixed systems in which the TETRA Standard Encryption Algorithm 2 (hereinafter referred to as TEA2) is included or TETRA system simulators in which the 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 the 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 authorization in writing by the CUSTODIAN.

3) 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.

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

5) To only provide equipment containing the 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 the 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 the 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 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)

Annex E:
TEA2 State and Territories list

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

Category: / State/territory:	Schengen state	European Union state	Dependent area of Schengen state or European Union (Candidate) state	Bilateral agreement with European Union	European Union Candidate state	Only borders with other TEA2 states
Austria	X	X				
Belgium	X	X				
Denmark (see note 1)	X	X				
Finland (see note 2)	X	X				
France	X	X				
Germany	X	X				
Greece	X	X				
Iceland	X					
Italy (see note 3)	X	X				
Luxembourg	X	X				
Netherlands	X	X				
Norway	X					
Portugal (see note 4)	X	X				
Spain (see note 5)	X	X				
Sweden	X	X				
Ireland		X				
United Kingdom		X				
Channel Islands			X			
Faroe Islands			X			
Gibraltar			X			
Isle of Man			X			
Svalbard			X			
Switzerland				X		
Cyprus		X				
Czech Republic		X				
Estonia		X				
Lithuania		X				
Latvia		X				
Hungary		X				
Malta		X				
Poland		X				
Slovakia		X				
Slovenia		X				
Bulgaria					X	
Romania					X	
Turkey					X	
Andorra						X
Liechtenstein						X
Monaco						X
San Marino						X
Vatican						X

NOTE 1: Including Helgoland.
NOTE 2: Including Aland.
NOTE 3: Including Livigno.
NOTE 4: Including Azores and Madeira Islands.
NOTE 5: Including Balearic Islands, Canary Islands, Ceuta and Mellila.

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