



Technical Specification

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

Reference

RTS/TCCE-06186

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

The present document can be downloaded from:

<http://www.etsi.org>

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (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/chaicor/ETSI_support.asp

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2014.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Foreword.....	5
1 Scope	6
2 References	6
2.1 Normative references	6
2.2 Informative references.....	7
3 Definitions and abbreviations.....	7
3.1 Definitions.....	7
3.2 Abbreviations	7
4 TEA2 management structure.....	8
5 Use of TEA2.....	9
5.1 Primary and Secondary Users of TEA2	9
5.2 TEA2 States and Territories	10
6 Licence types.....	11
6.1 Manufacturer Licence.....	11
6.2 Installer/Repairer/Destruction Licence.....	11
6.3 Supplier Licence.....	12
6.4 Primary User Licence.....	12
6.5 Secondary User Licence	12
6.6 End User Licence	13
6.7 Destruction Licence.....	13
6.8 Exceptional.....	14
7 Distribution procedures	14
7.1 Distribution of parts 1, 2 and 3 of the TEA2 specification by the TEA2 Custodian	14
7.2 Distribution of part 3 of the TEA2 specification by the TEA2 Custodian	15
8 Approval criteria and restrictions	15
8.1 Approval Criteria.....	15
8.2 Revocation of TEA2 licences.....	16
8.3 Appeal against Licence Revocation	16
9 The TEA2 Custodian.....	17
9.1 Responsibilities	17
9.2 Appointment.....	17
Annex A (informative): Items delivered to approved recipient of TEA2 specifications	19
Annex B (normative): Confidentiality and Restricted Usage Undertaking for Manufacturers of TEA2	20
Annex C (normative): Confidentiality and Restricted Usage Undertaking for Installers, Repairers and Destruction of TEA2.....	23
Annex D (normative): Confidentiality and Restricted Usage Undertaking for Suppliers of Equipment or Services using TEA2	25
Annex E (normative): Confidentiality and Restricted Usage Undertaking for Primary and Secondary Users of TEA2	27
Annex F (normative): Confidentiality and Restricted Usage Undertaking for End Users of TEA2	30
Annex G (normative): Confidentiality and Restricted Usage Undertaking for Destruction of TEA2	33

Annex H (informative):	TEA2 State and Territories list	35
Annex I (informative):	Bibliography	36
History		37

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 Specification (TS) has been produced by ETSI Technical Committee TETRA and Critical Communications Evolution (TCCE).

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 licensing organizations to manufacture, possess, install, repair, hold, use and destroy equipment and components containing the TEA2 algorithm and to delivering parts 1, 2 and 3 of the TEA2 specifications.

Parts 1 and 2 of the specification are confidential.

Part 3 of the specification is not confidential and can be obtained directly from the TEA2 Custodian (see clause 7.2). There are no restrictions on the distribution of this part of the specification.

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 and Critical Communications Evolution, 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 H, which provides an exemplary list of the states and territories in which a User may become an approved recipient.

Clause 6 describes the types of licence that may be requested.

The procedures for delivering TEA2 specifications to approved recipients are defined in clause 7. This clause is supplemented by annex A, which specifies the items that are to be delivered.

Clause 8 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 to G which contain the Confidentiality and Restricted Usage Undertakings to be signed by the TEA2 Custodian and approved recipients of TEA2 specifications and/or equipment and components containing TEA2.

Clause 9 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".

3 Definitions and abbreviations

3.1 Definitions

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

computer software carrier: physical storage medium capable of containing and transporting computer software or data, such as a ROM chip, CD ROM or disk, or flash memory or computer hard drive

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

installer: organization that installs hardware or software components containing the TETRA Standard Algorithm TEA2 into TETRA subscriber equipment, fixed network equipment or TETRA system simulators

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

repairer: organization that repairs TETRA subscriber equipment, fixed network equipment, or system simulators that contain TEA2

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 network equipment 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

TEA2 custodian: the interface between ETSI and recipients of TEA2 licences and specifications

user: primary or secondary user

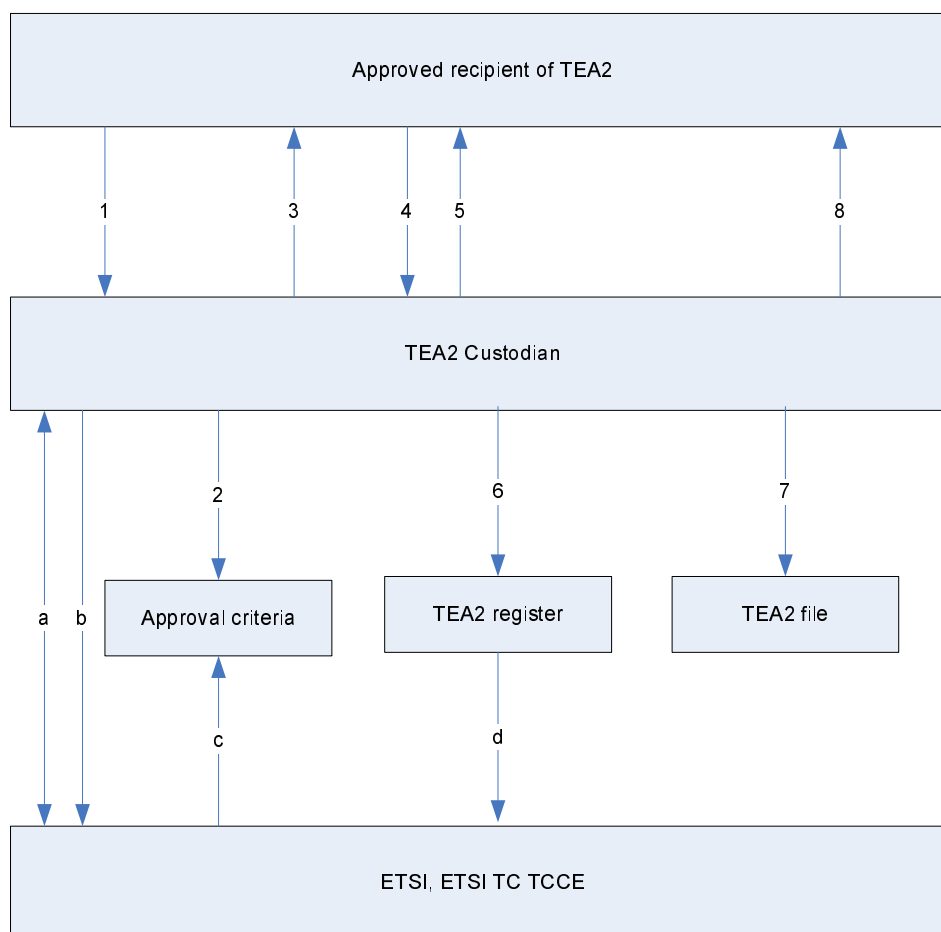
3.2 Abbreviations

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

CRUU	Confidentiality and Restricted Usage Undertaking
ETSI	European Telecommunications Standards Institute
MS	Mobile Station
SFPG	Security and Fraud Prevention Group
SwMI	Switching and Management Infrastructure
TEA2	TETRA standard Encryption Algorithm number 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 = Requested details of the TEA2 register
- 1 = Request for TEA2 specification and/or licence
- 2 = Check of request against approval criteria
- 3 and 4 = Exchange of Confidentiality and Restricted Usage Undertaking
- 5 = Dispatch of TEA2 specification (only if appropriate)
- 6 = Update the TEA2 register
- 7 = Document filing
- 8 = Technical advice (only if requested)

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 and Critical Communications Evolution sets the approval criteria for receipt of the algorithm (see clause 8).
- The TEA2 Custodian is the interface between ETSI and the recipients of TEA2 licences and specifications.

- The TEA2 Custodian is as identified in clause 9.2 of the present document. The TEA2 Custodian's duties are detailed in clause 9. They include distributing signed TEA2 Confidentiality and Restricted Usage Undertakings (CRUUs) and, if appropriate, specifications to approved recipients, as detailed in clauses 7 and 8, providing limited technical advice to approved recipients and providing algorithm status reports to ETSI Technical Committee TETRA and Critical Communications Evolution.

NOTE: A CRUU signed by both the TEA2 Custodian and applicant constitutes a licence to hold or use TETRA subscriber and fixed network equipment and components containing TEA2.

The form of CRUU exchanged is summarized in figure 2.

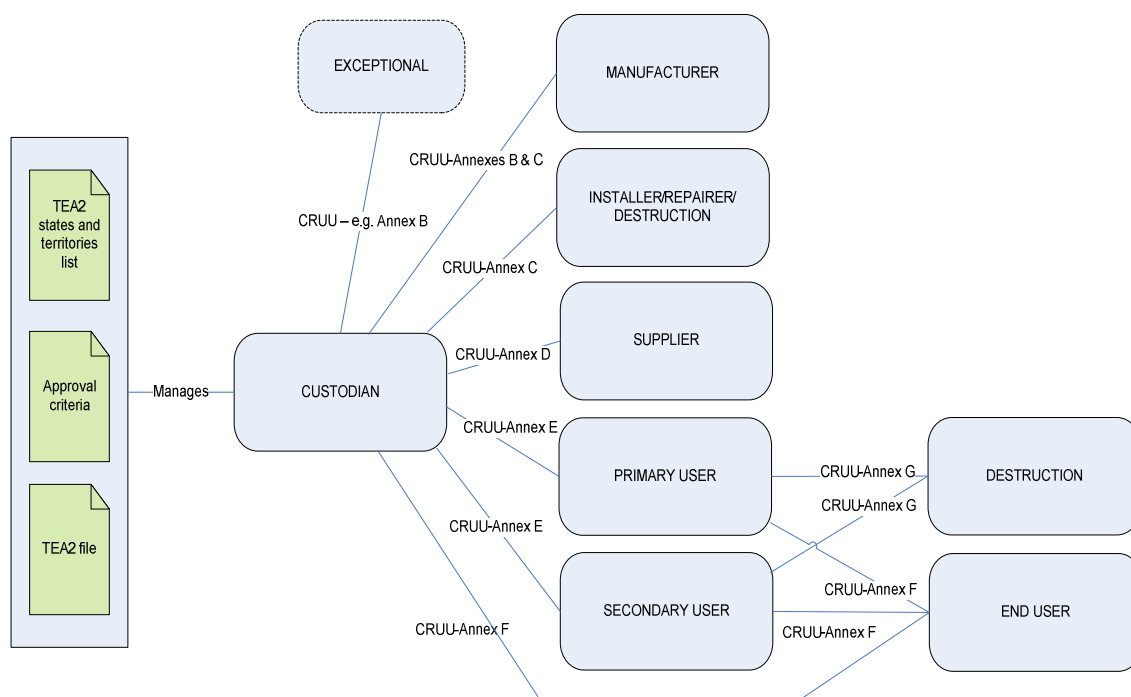


Figure 2: Summary of CRUU types maintained between TEA2 principals

5 Use of TEA2

5.1 Primary and Secondary Users of TEA2

A TEA2 Primary and Secondary User Licence 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 Licence under these conditions is referred to as a primary user of TEA2. The Confidentiality and Restricted Usage Undertaking (CRUU) in annex E applies to primary and secondary users (see note 2). The TEA2 licence is required for the use of TEA2 in any element of the TETRA network including TETRA Subscriber equipment (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 Licence 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 or user organization. An organization that obtains a TEA2 End User Licence under these conditions is referred to as an end user of TEA2. The CRUU in annex F 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 E 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.

NOTE 3: Primary and secondary users are expected to comply with the relevant national security policies concerning the management and sub-licensing of TEA2.

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).

An exemplary list of TEA2 states and territories is provided in annex H. The TEA2 Custodian maintains the definitive list of TEA2 states and territories.

6 Licence types

6.1 Manufacturer Licence

An organization wishing to manufacture TETRA equipment and/or components containing TEA2 obtains its licence and copies of the TEA2 specifications by the procedure defined in clause 7.1.

6.2 Installer/Repairer/Destruction Licence

An organization that installs hardware or software components containing TEA2 into equipment requires a manufacturer licence (see clause 6.1) or an installer/repairer/destruction licence.

An organization that repairs equipment or hardware or software components containing TEA2 requires a manufacturer licence or an installer/repairer/destruction licence.

An organization that destroys equipment or components containing TEA2 requires a manufacturer licence, an installer/repairer/destruction licence or a destruction licence (see clause 6.7).

An organization that destroys computer software carriers containing TEA2 requires a manufacturer licence or an installer/repairer/destruction licence.

A TETRA manufacturer that possesses a manufacturer licence may be permitted, subject to national legislation, to nominate a third party to install TEA2 into equipment, to repair equipment and components containing TEA2 and to destroy equipment, components and computer software carriers containing TEA2.

In this case, the TETRA manufacturer shall require the third party to sign two copies of the Confidentiality and Restricted Usage Undertaking for installers, repairers and destruction of TEA2 (see annex C). The TETRA manufacturer shall send these to the TEA2 Custodian together with a nomination letter signed by the manufacturer.

The TEA2 Custodian then enters the 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 installer, repairer or destruction organization.

NOTE 1: The TEA2 Custodian will not sign the Confidentiality and Restricted Usage Undertaking for an Installer/Repairer/Destruction Licence unless it is supported by a nomination letter signed by an organization possessing a manufacturer's licence.

NOTE 2: The TETRA manufacturer is responsible for checking that the nominated Installer/Repairer/Destruction organization complies with the relevant national security policies (e.g. with regard to the removal of key material).

NOTE 3: The TEA2 Custodian may check the suitability of the organization with respect to the relevant national legislation before granting an Installer/Repairer/Destruction licence.

NOTE 4: An organization may be granted multiple Installer/Repairer/Destruction licences, each nominated by a different manufacturer.

NOTE 5: If a manufacturer writes to the TEA2 Custodian withdrawing its nomination for an Installer/Repairer/Destruction licence, the TEA2 Custodian will revoke that licence.

NOTE 6: This licence is not required by an organization that only handles complete radio equipment, e.g. for the purpose of installation into a building or vehicle. (A supplier licence may be more suitable). This licence is required by an organization that opens radio equipment for repair of components containing TEA2 or installs executable code containing TEA2 into complete radio equipment.

NOTE 7: This licence is not required by an organization that only destroys equipment and components on behalf of a user. (A destruction licence may be more suitable). This licence is required by an organization that destroys computer software carriers.

6.3 Supplier Licence

A TETRA manufacturer that has obtained a TEA2 manufacturer licence may be allowed, subject to national legislation, to distribute TETRA equipment containing TEA2 via a supplier.

In this case, the TETRA manufacturer has to get the supplier 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 supplier.

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 or end users.

In this case, the third party operator shall demonstrate to the TEA2 Custodian that he meets the approval criteria (see clause 8.1) and shall send two signed copies of the Confidentiality and Restricted Usage Undertaking for Suppliers (see annex D) to the TEA2 Custodian.

If the TEA2 Custodian is satisfied that the third party operator meets the approval criteria as listed in clause 8.1, the TEA2 Custodian 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.

NOTE: This licence is suitable for an organization that installs complete radio equipment into e.g. a building or vehicle. It is not suitable for an organization that opens radio equipment for repair of components containing TEA2 or installs executable code containing TEA2 into radio equipment.

6.4 Primary User Licence

The applicant for a primary user licence (see clause 5.1) of TETRA equipment containing TEA2 shall provide to the TEA2 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 applicant for a primary user licence shall sign two copies of the Confidentiality and Restricted Usage Undertaking for Primary and Secondary Users of TEA2 as in annex E. The applicant shall then send these to the TEA2 Custodian.

If the TEA2 Custodian is satisfied that the applicant meets the required criteria as listed in clause 8.1, the TEA2 Custodian enters the details in the TEA2 Register, countersigns the Confidentiality and Restricted Usage Undertakings, returns one of these together with a covering letter to the now approved primary user, and files the other and a copy of the letter in the TEA2 File.

6.5 Secondary User Licence

As described in clause 5.1 a military organization can become an approved recipient of a secondary user licence. 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 C9 as in clause 8.1). The primary user asks the intended secondary user to sign two copies of the Confidentiality and Restricted Usage Undertaking for Primary and Secondary Users of TEA2 as in annex E. 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 now approved secondary user.

In the second case the applicant for a secondary user licence shall provide to the TEA2 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 applicant for a secondary user licence shall sign two copies of the Confidentiality and Restricted Usage Undertaking for Users of TEA2 as in clause E. The secondary user shall then send these to the TEA2 Custodian. If the TEA2 Custodian is satisfied that the applicant meets the required criteria as listed in clause 8.1, 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 now approved secondary user, and files the other and a copy of the letter in the TEA2 File.

6.6 End User Licence

An organization which has already been approved as a primary user or as a secondary user and has obtained a TEA2 primary or secondary user licence may act as a licensor for end users 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) shall ensure that the end user (hereinafter referred to as the second organization) meets the approval criteria. The first organization shall require the second organization to sign two copies of the Confidentiality and Restricted Usage Undertaking for End users of TEA2 as in annex F. The first organization shall 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.

NOTE: The primary or secondary user is responsible for checking that its end users comply with the relevant national security policies.

If no primary or secondary user exists in a particular area of jurisdiction, an end user in that area of jurisdiction shall obtain its end user licence directly from the TEA2 Custodian. In that case, the TEA2 Custodian shall require the end user to demonstrate its suitability to receive an end user licence and shall require the end user to sign two copies of the Confidentiality and Restricted Usage Undertaking for End Users of TEA2 as in annex F. The TEA2 Custodian shall maintain a record of the end users with whom it has signed CRUUs. CRUUs signed in accordance with this process may be 'time limited' as determined by the TEA2 Custodian.

6.7 Destruction Licence

An organization that destroys equipment or components containing TEA2 requires a manufacturer licence (see clause 6.1), an installer/repairer/destruction licence (see clause 6.2) or a destruction licence.

An organization that possesses a primary user licence or secondary user licence may licence a third party to destroy equipment and components containing TEA2.

In this case, the primary or secondary user shall require the third party to sign two copies of the Confidentiality and Restricted Usage Undertaking for destruction (see annex G).

The primary or secondary user is responsible for passing (a copy of) the countersigned Confidentiality and Restricted Usage Undertaking to the third party destruction organization.

NOTE 1: The primary or secondary user is responsible for checking that its destruction facilities comply with the relevant national security policies.

NOTE 2: This licence is only suitable for an organization that destroys equipment and components. An organization that destroys computer software carriers requires an Installer/Repairer/Destruction Licence (see annex C).

6.8 Exceptional

In the event that an organization cannot comply with the rules as described in the present document, the TEA2 Custodian may still decide, on an exceptional basis, to distribute the TEA2 specifications to this organization. In this case the TEA2 Custodian will inform ETSI SAGE and TC TCCE about his decision and at the same time provide a motivation. If a special Confidentiality and Restricted Usage Undertaking is used, the TEA2 Custodian will first ask the ETSI Legal Department to approve this Confidentiality and Restricted Usage Undertaking (CRUU).

7 Distribution procedures

7.1 Distribution of parts 1, 2 and 3 of the TEA2 specification by the TEA2 Custodian

This clause describes the procedure for the distribution of parts 1, 2 and 3 of the TEA2 specification (see clause 1) when requested together. See clause 7.2 for the procedure for distribution of part 3 as a separate item.

The TEA2 Custodian is responsible for determining whether an applicant is qualified to receive the TEA2 specification.

The TEA2 Custodian is responsible for signing TEA2 Confidentiality and Restricted Usage Undertakings with qualified applicants who require access to the TEA2 specifications.

The TEA2 Custodian is responsible for sending copies of the TEA2 specification to qualified applicants.

The following procedure for distributing TEA2 specifications is defined with reference to figure 1.

- 1) The TEA2 Custodian receives a written request for N copies of the TEA2 specification parts 1, 2 and 3 (see notes 1 and 2) or a written request for entering into a Confidentiality and Restricted Usage Undertaking concerning TETRA equipment and/or components containing TEA2.
- 2) The TEA2 Custodian determines whether the requesting organization meets the approval criteria (see clause 8).
- 3) If the request is not approved, the TEA2 Custodian informs the requesting organization that its request has not been approved.
- 4) If the request is approved, the TEA2 Custodian dispatches 2 copies of the corresponding Confidentiality and Restricted Usage Undertaking (as given in annex B) for signature by the approved recipient (see note 6) together with a copy of the present document (Rules for the Management of the TETRA Standard Encryption Algorithm TEA2).
- 5) 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).
- 6) The TEA2 Custodian sends up to N (see note 3) numbered copies of the TEA2 specification parts 1, 2 and 3 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).
- 7) 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).
- 8) 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.
- 9) The TEA2 Custodian may provide very limited technical advice with respect to answering questions concerning the TEA2 specification.
- 10) If there is a change in the contact details of the signatory or name or ownership of the organization, the organization shall inform the TEA2 Custodian.

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

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

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

NOTE 4: If the request is approved, 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 clause 6.8.

NOTE 6: Under normal circumstances the TEA2 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.

NOTE 9: The TEA2 Custodian may check the suitability of the applicant with respect to relevant national security policies before granting a licence.

7.2 Distribution of part 3 of the TEA2 specification by the TEA2 Custodian

The following procedure is defined for distributing only part 3 of the TEA2 specification:

- 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.

8 Approval criteria and restrictions

8.1 Approval Criteria

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

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

In order for an organization to be considered an approved recipient of TEA2 specifications it shall be located in one of the states or territories listed in the TEA2 Custodian's list of States and Territories (Annex H is an example). In addition, it shall satisfy at least one of the following criteria:

- C1 The organization is a bona fide designer or manufacturer of TETRA subscriber or fixed network equipment, where the algorithm requested is included in the systems.
- C2 The organization is a bona fide designer or manufacturer of components for TETRA subscriber or fixed network equipment, where at least one of the components includes the algorithm requested.
- C3 The organization is a bona fide designer or manufacturer of a TETRA system simulator for approval testing of TETRA subscriber or fixed network equipment, where the simulator includes the algorithm requested.
- C4 The organization has provided the TEA2 Custodian with exceptional reasons that have been approved by the TEA2 Custodian.

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

In order for an organization to be considered an approved recipient of a TEA2 licence it shall be located in one of the states or territories listed in the TEA2 Custodian's list of States and Territories (annex H is an example). In addition, it shall satisfy at least one of the criteria C1 to C4 (above) or one of the following criteria:

- C5 The organization has been appointed by a TETRA manufacturer as an installer and/or repairer and/or destroyer of TETRA equipment or components containing the TEA2 algorithm.
- C6 The organization has been appointed by a TETRA manufacturer as a supplier of equipment containing the TEA2 algorithm.
- C7 The organization operates a TETRA fixed network using TEA2 that provides communication services to primary and/or secondary users or to end users.
- C8 The organization is a governmental organization for a network that is primarily used by public safety organizations in its own state or territory as listed in the TEA2 Custodian's list of States and Territories (annex H is an example). This is referred to as a primary user.
- C9 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). This is referred to as a secondary user.

NOTE: In this case the primary user has to arrange the signing of Confidentiality and Restricted Usage Undertakings as specified in clause 6.5.

- C10 The organization is a military organization operating a TETRA network in a state or territory as listed in the TEA2 Custodian's list of States and Territories (annex H is an example) 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. This is referred to as a secondary user.
- C11 The organization has been appointed by a primary or secondary user as an end user of TEA2.
- C12 No primary or secondary user exists in a particular area of jurisdiction and the organization has demonstrated to the TEA2 Custodian that it is a public safety organization operating in that area of jurisdiction.
- C13 The organization has been appointed by a primary or secondary user as a destroyer of TETRA equipment or components containing the TEA2 algorithm.

8.2 Revocation of TEA2 licences

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

- any of the approval criteria ceasing to apply;
- expiry of a time limited licence;
- any breach of the Licensee undertakings as contained in the relevant CRUU;
- written withdrawal of the manufacturer's nomination for an Installer/Repairer/Destruction licence;
- a change in relevant national security policies.

8.3 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 TCCE for a final decision.

9 The TEA2 Custodian

9.1 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 8.
- T2 To obtain the Administrative authorization and export licences required by the Customs Services of its country if any.
- T3 To exchange the Confidentiality and Restricted Usage Undertaking with approved recipients as described in clauses 6 and 7.
- T4 To distribute, if required and approved, the TEA2 specifications as detailed in clause 7 (see note 1).
- T5 To maintain the TEA2 Register as described in clauses 6 and 7.1.
- T6 To hold in custody the contents of the TEA2 File as specified in clauses 6 and 7.1.
- T7 To provide recipients of TEA2 with limited technical support, i.e. answer written queries arising from the specification or test data (see note 2).
- T8 To advise ETSI/ETSI TC TCCE of any problems arising with the approval criteria.
- T9 In the light of written queries from recipients of the TEA2 specifications, to make recommendations to ETSI/ETSI TC TCCE for improvements/corrections to the specification and, subject to ETSI/ETSI TC TCCE approval, make and distribute the changes (see note 3).
- T10 To provide ETSI/ETSI TC TCCE with information from the TEA2 Register when requested to do so.
- T11 To monitor published advances in cryptanalysis and advise the ETSI TC TCCE of any advances which have a significant impact upon the continued suitability of 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.

9.2 Appointment

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

The TETRA + Critical Communications 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 + Critical Communications Association. Where this is not the case it will revert to the Chief Executive Officer of the TETRA + Critical Communications Association.

The contact person is:

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

Wildenborch 63, 2261 XK Leidschendam

The Netherlands

e-mail: SFPG@TandCCA.com

The TEA2 Custodian will ask a fee from the recipient to cover the cost of distribution of the CRUU's and parts 1 and 2 of the specifications. The fees are set out in table 1 for each licensee 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 1: Fees for distribution of TEA2 (as of tbd)

Licensee	ITEM-1 (Parts 1 and 2 of the specification)	ITEM-2 (CRUU) (see note 1)	ITEM-3 (Covering letter)	Part 3 of specification
Manufacturer	500 €/numbered copy	500 €	No charge	Discretionary
Supplier	Not provided	500 €	No charge	Not provided
Installer/Repairer/Destruction	Not provided	500 €	No charge	Not provided
Primary and Secondary User	Not provided	500 €	No charge	Discretionary
End user managed by a primary or secondary user	Not provided	Discretionary (see note 2)	No charge	Not provided
End user applying directly to the TEA2 Custodian	Not provided	500 €	No charge	Not provided
Destruction	Not provided	500 €	No charge	Not provided
Exceptional	500 €/numbered copy	500 €	No charge	Discretionary

NOTE 1: Each registration of a CRUU invokes a fee due of 500 € from the registering party.

NOTE 2: A fee may be applied at the discretion of the primary or secondary user.

Annex A (informative): Items delivered to approved recipient of TEA2 specifications

- ITEM-1: Up to N numbered paper copies to the TEA2 specification (parts 1, 2 and 3), where N is the number of copies approved (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 parts 1, 2 and 3 are requested and approved.

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

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

.....

.....

VAT registration no.

hereinafter called: the LICENSEE;

and

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas

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

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

The CUSTODIAN undertakes to give to the LICENSEE:

- 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 LICENSEE undertakes to:

- 1) keep strictly confidential all information contained in the detailed specification of TEA2 (if provided) and all related communications written or verbal which have been associated with that information after the signature of the present undertaking (the "INFORMATION").
- 2) take measures to ensure that his personnel do not disclose to third parties, without prior and explicit authorization in writing by the CUSTODIAN, all or part of the INFORMATION.
- 3) use the INFORMATION in the 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.
- 4) 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 shall not be used to provide the end-to-end security services described in these standards.

- 5) provide equipment and components containing TEA2 for TETRA applications only to an organization which has signed the appropriate TEA2 Confidentiality and Restricted Usage Undertaking (as in annexes B to G) with the TEA2 Custodian or primary or secondary user. Before supplying equipment incorporating TEA2, the LICENSEE undertakes to verify that this organization has supplied him with a copy of the respective TEA2 Confidentiality and Restricted Usage Undertaking which is countersigned by the Custodian or primary or secondary user. Where the equipment is being provided to an end user, the manufacturer undertakes to verify that he has validated this end user with the primary or secondary user or the TEA2 Custodian within the previous twelve months.
- 6) check that any organization that he nominates for receipt of an Installer/Repairer/Destruction licence complies with the relevant national security policies.
- 7) provide computer software carriers containing TEA2 for TETRA applications only to an installer, repairer or destroyer of equipment or components containing TEA2 who has signed a Confidentiality and Restricted Usage Undertaking for installers, repairers and destroyers of equipment containing TEA2 with the Custodian (as in annex C). Before providing computer software carriers containing TEA2, the LICENSEE undertakes to verify that this installer, repairer or destroyer has supplied him with a copy of the Confidentiality and Restricted Usage Undertaking for installers, repairers and destroyers of equipment containing TEA2 which is countersigned by the Custodian.

The LICENSEE undertakes NOT to:

- 8) make copies of the TEA2 specifications (all copies of these specifications must be produced, numbered and registered by the CUSTODIAN).
- 9) disclose the INFORMATION to any third party without prior and explicit authorization in writing by the CUSTODIAN.
- 10) register, or attempt to register, any IPR (patents or the like rights) relating to TEA2 and containing all or part of the INFORMATION.
- 11) 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.
- 12) 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 LICENSEE.

- 13) export the TEA2 specification to any territory outside the list of TEA2 approved states maintained by the TEA2 Custodian.
- 14) export TEA2 components or equipment containing TEA2 to any territory outside the list of TEA2 approved states maintained by the TEA2 Custodian without the prior agreement of the TEA2 Custodian.

The above restrictions do not apply to information which:

- is or subsequently becomes (other than by breach by the LICENSEE of its obligations under this agreement) public knowledge; or
- is received by the LICENSEE 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 LICENSEE 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 LICENSEE 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 LICENSEE breaches the obligations of confidentiality imposed on him pursuant to the undertakings above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the LICENSEE agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach. The LICENSEE 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 LICENSEES. Evidence of being a LICENSEE 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 LICENSEE.

For the CUSTODIAN

For the LICENSEE

.....

.....

(Name, Title)

(Name, Title)

.....

.....

(Signature)

(Signature)

.....

.....

(Date)

(Date)

Annex C (normative): Confidentiality and Restricted Usage Undertaking for Installers, Repairers and Destruction of TEA2

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the installation, repair and destruction of equipment and components containing 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).....

.....

.....

VAT registration no.

hereinafter called: the LICENSEE;

and

(COMPANY)

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas

The LICENSEE has demonstrated that he fulfils at least one of the following criteria:

- He is an installer of hardware or software components containing TEA2 into subscriber equipment, fixed network equipment or system simulators.
- He is a repairer of subscriber equipment, fixed network equipment, or system simulators in which TEA2 is included.
- He destroys equipment, components or computer software carriers containing TEA2.

The LICENSEE undertakes to:

- 1) provide equipment and components containing TEA2 only to an organization which has signed the appropriate TEA2 Confidentiality and Restricted Usage Undertaking (as in annexes B to G) with the CUSTODIAN or a primary or secondary user. Before supplying equipment or components containing TEA2 or returning repaired equipment or components containing TEA2, the LICENSEE undertakes to verify that the organization has provided him with a copy of the appropriate TEA2 Confidentiality and Restricted Usage Undertaking which has been countersigned by the CUSTODIAN or a primary or secondary user. Where the equipment or components are being provided to an end user, the LICENSEE undertakes to verify that he has validated the end user with the primary or secondary user or the TEA2 Custodian within the previous twelve months.
- 2) irrevocably destroy all equipment, components and computer software carriers containing TEA2 that have been supplied to him for destruction.
- 3) provide computer software carriers containing TEA2 only to an organization which has signed a TEA2 Confidentiality and Restricted Usage Undertaking for a manufacturer (as in annex B) or a TEA2 Confidentiality and Restricted Usage Undertaking for an installer/repairer/destruction (as in annex C). Before supplying computer software carriers containing TEA2 the LICENSEE undertakes to verify that the organization has provided him with a copy of the appropriate TEA2 Confidentiality and Restricted Usage Undertaking which has been countersigned by the CUSTODIAN.
- 4) comply with the relevant national security policies.

The LICENSEE undertakes NOT to:

- 5) export components or equipment containing TEA2 to any territory outside the list of TEA2 approved states maintained by the TEA2 Custodian.

The above restrictions do not apply to information which:

- is or subsequently becomes (other than by breach by the LICENSEE of its obligations under this agreement) public knowledge; or
- is received by the LICENSEE 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 LICENSEE breaches the obligations imposed on him pursuant to the undertakings above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the LICENSEE agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach. The LICENSEE 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 herein will not apply vis-à-vis other LICENSEES. Evidence of being a LICENSEE 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 LICENSEE.

For the CUSTODIAN

For the LICENSEE

.....

.....

(Name, Title)

(Name, Title)

.....

.....

(Signature)

(Signature)

.....

.....

(Date)

(Date)

Annex D (normative): Confidentiality and Restricted Usage Undertaking for Suppliers of Equipment or Services using 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).....

.....

.....

VAT registration no.

hereinafter called: the LICENSEE;

and

(COMPANY)

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the CUSTODIAN.

Whereas

The LICENSEE has demonstrated that he fulfils at least one of the following criteria:

- He is a supplier of TETRA subscriber or fixed network equipment 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 user and/or secondary user and/or end user.

The LICENSEE undertakes to:

provide equipment containing TEA2 for TETRA applications only to an organization which has signed the appropriate TEA2 Confidentiality and Restricted Usage Undertaking (as in annexes B to G) with the Custodian or a primary or secondary user. Before supplying equipment incorporating TEA2 to an organization, the LICENSEE undertakes to verify that this organization has supplied him with a copy of the appropriate TEA2 Confidentiality and Restricted Usage Undertaking which is countersigned by the Custodian or a primary or secondary user. Where the equipment is being supplied to an end user, the supplier undertakes to verify that he validated this end user with the primary or secondary user or the TEA2 Custodian within the previous twelve months.

The LICENSEE undertakes NOT to:

export components or equipment containing TEA2 to any territory outside the list of TEA2 approved states maintained by the TEA2 Custodian.

In the event that the LICENSEE breaches the obligations imposed on him pursuant to the undertakings above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the LICENSEE agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach. The LICENSEE 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 LICENSEES. Evidence of being a LICENSEE 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 LICENSEE.

For the CUSTODIAN

.....

(Name, Title)

.....

(Signature)

.....

(Date)

For the LICENSEE

.....

(Name, Title)

.....

(Signature)

.....

(Date)

Annex E (normative): 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).....

VAT registration no.

hereinafter called: the LICENSEE;

and

(COMPANY NAME).....

(COMPANY ADDRESS).....

hereinafter called: the CUSTODIAN.

Whereas

The LICENSEE declares, 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.

- Additional information:

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

The LICENSEE undertakes to:

- 1) 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 shall not be used to provide the end-to-end security services described in these standards.

- 2) use equipment containing TEA2 only for providing TETRA services to user groups as limited by this undertaking.
- 3) check that any destruction facility appointed by the LICENSEE complies with the relevant national security policies.

The LICENSEE undertakes NOT to:

- 4) pass on equipment or components containing TEA2 to a third party without validating the permission of the third party to hold equipment containing TEA2.
- 5) export components or equipment containing TEA2 to any territory outside the list of TEA2 approved states maintained by the TEA2 Custodian unless the LICENSEE is a military organization maintaining full control of the exported components or equipment as specified by the Rules for the Management of the TETRA Standard Encryption Algorithm TEA2.

The above restrictions do not apply to information which:

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

In the event that the LICENSEE breaches the obligations imposed on him pursuant to the undertakings above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the LICENSEE agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach. The LICENSEE 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 LICENSEES. Evidence of being a LICENSEE 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 LICENSEE.

For the CUSTODIAN

For the LICENSEE

.....

.....

(Name, Title)

(Name, Title)

.....

.....

(Signature)

(Signature)

.....

.....

(Date)

(Date)

Annex F (normative): 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).....

.....

.....

VAT registration no.

hereinafter called: the LICENSEE;

and

(COMPANY NAME).....

(COMPANY ADDRESS).....

.....

.....

hereinafter called: the USER or CUSTODIAN.

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

Whereas

The LICENSEE declares, 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.

- The organization has been acknowledged by the CUSTODIAN as a legitimate end user of a network that is primarily used by public safety organizations in a state or territory listed in the TEA2 state and territory list that is maintained by the CUSTODIAN, and no primary or secondary user has been appointed in that state or territory.
- Additional information:

Description of intended application and user group(s)

.....

.....

.....

.....

.....

.....

The LICENSEE undertakes to:

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

The LICENSEE undertakes NOT to:

- 3) pass on equipment containing TEA2 to a third party without validating the permission of the third party to hold equipment containing TEA2. Where the equipment is being provided to an end user the LICENSEE undertakes to verify that he has validated the end user with the primary or secondary user or the TEA2 Custodian within the previous twelve months.
- 4) export components or equipment containing TEA2 to any territory outside the list of TEA2 approved states maintained by the TEA2 Custodian.

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 LICENSEES. Evidence of being a LICENSEE 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 USER or CUSTODIAN, the other for the LICENSEE.

For the USER or CUSTODIAN

For the LICENSEE

.....

.....

(Name, Title)

(Name, Title)

.....

.....

(Signature)

(Signature)

.....

.....

(Date)

(Date)

Annex G (normative): Confidentiality and Restricted Usage Undertaking for Destruction of TEA2

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the destruction of equipment and components containing 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).....

.....

.....

VAT registration no.

hereinafter called: the LICENSEE;

and

(COMPANY)

(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 LICENSEE has demonstrated that he destroys equipment or components containing TEA2.

The LICENSEE undertakes to irrevocably destroy all equipment and components containing TEA2 that have been supplied to him for destruction, in accordance with the relevant national security policies.

The LICENSEE undertakes NOT to export components or equipment containing TEA2 to any territory outside the list of TEA2 approved states maintained by the TEA2 Custodian.

In the event that the LICENSEE breaches the obligations imposed on him pursuant to the undertaking above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the LICENSEE agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach. The LICENSEE 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 LICENSEES. Evidence of being a LICENSEE 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 USER, the other for the LICENSEE.

For the USER

.....

(Name, Title)

.....

(Signature)

.....

(Date)

For the LICENSEE

.....

(Name, Title)

.....

(Signature)

.....

(Date)

Annex H (informative): TEA2 State and Territories list

The list below is an exemplary list showing in which countries TEA2 may be used. The TEA2 Custodian maintains the definitive 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		
Bosnia & Herzegovina	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	
Montenegro	Yes			X
Netherlands	Yes	X		
Norway	Yes	X		
Poland	Yes	X		
Portugal	Yes	X		
Romania	Yes	X		
San Marino	Yes		X	
Serbia	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			

Annex I (informative): Bibliography

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

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

ETSI TR 101 053-4: "Security Algorithms Group of Experts (SAGE); Rules for the management of the TETRA standard encryption algorithms; Part 4: TEA4".

History

Document history		
V1.1.1	June 1997	Publication as TR 101 053-2
V1.1.2	October 1998	Publication as TR 101 053-2
V2.1.1	September 2003	Publication as TR 101 053-2
V2.2.1	March 2005	Publication as TR 101 053-2
V2.2.2	September 2008	Publication as TR 101 053-2
V2.2.3	June 2010	Publication as TR 101 053-2
V2.2.4	June 2012	Publication as TR 101 053-2
V2.3.1	April 2014	Publication