ETSI TS 101 053-5 V1.1.1 (2022-12)

Rules for the management of the TETRA standard encryption algorithms; Part 5: TEA5

Reference
DTS/TCCE-06199

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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

The present document is part 5 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";

Part 5: "TEA5";

Part 6: "TEA6";

Part 7: "TEA7".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The purpose of the present document is to specify the rules for the management of the TETRA standard encryption algorithm TEA5. This algorithm is intended for air interface encryption in TETRA products.

The specification for TEA5 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 TEA5 algorithm and to delivering parts 1, 2 and 3 of the TEA5 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 TEA5 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 TEA5 (ETSI, ETSI Technical Committee TETRA and Critical Communications Evolution, TEA5 Custodian and approved recipients) together with the relationships and interactions between them.

Clause 5 is concerned with the rules for the use of TEA5. 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 TEA5 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 TEA5 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 TEA5 Custodian and approved recipients of TEA5 specifications and/or equipment and components containing TEA5.

Clause 9 is concerned with the appointment and responsibilities of the TEA5 Custodian.

2 References

2.1 Normative 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://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.

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

Not applicable.

2.2 Informative 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 referenced document (including any amendments) applies.

NOTE 1: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

NOTE 2: [i.1] and [i.2] may also be published as ETSI Technical Specifications, specifically TS 100 392-7 and TS 100 396-6 respectively. In each case, the latest version of the specification, either TS or EN, applies.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms 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 TEA5 by either the primary or secondary user or by the TEA5 custodian

installer: organization that installs hardware or software components containing the TETRA Standard Algorithm TEA5 into TETRA subscriber equipment, fixed network equipment or TETRA system simulators

manufacturer: bona fide designer or manufacturer of TETRA equipment or components which include TEA5

permitted state or territory: state or territory within which TEA5 is allowed to be used, where the list of states and territories is maintained by the TEA5 custodian

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 TEA5

secondary user: military organization in a state or territory with approval to operate a TETRA network given by the governmental organization that is responsible for public safety

supplier: supplier, distributor or reseller of TETRA subscriber or fixed network equipment in which TEA5 is included or TETRA system simulators in which TEA5 is included, or a third party operator or service provider supplying TETRA services with TEA5 to a primary and/or secondary user

TEA5 custodian: interface between ETSI and recipients of TEA5 licences and specifications

user: primary or secondary user

3.2 Symbols

Void.

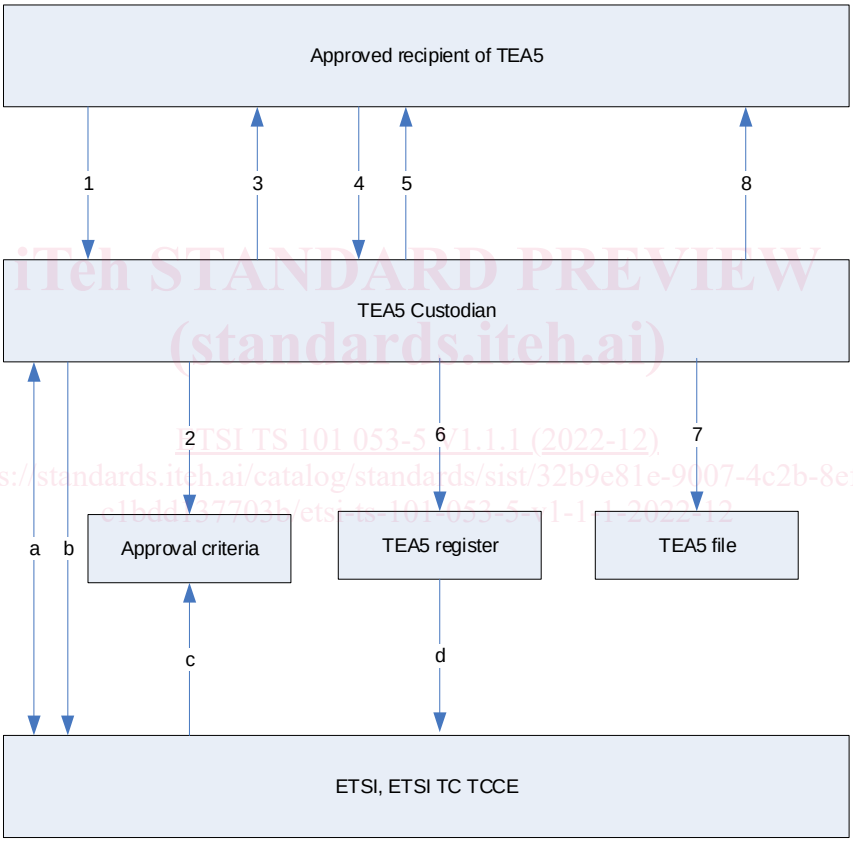
3.3 Abbreviations

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

CRUU	Confidentiality and Restricted Usage Undertaking
DMO	Direct Mode Operation
MS	Mobile Station
SFPG	Security and Fraud Prevention Group
SwMI	Switching and Management Infrastructure
TEA5	TETRA standard Encryption Algorithm number 5
TETRA	TErrestrial Trunked RAdio

4 TEA5 management structure

The management structure is depicted in figure 1.



Key:

a	=	Agreement between TEA5 Custodian and ETSI
b	=	Status reports and recommendations
c	=	Setting of approval criteria
d	=	Requested details of the TEA5 register
1	=	Request for TEA5 specification and/or licence
2	=	Check of request against approval criteria
3 and 4	=	Exchange of Confidentiality and Restricted Usage Undertaking
5	=	Dispatch of TEA5 specification (only if appropriate)
6	=	Update the TEA5 register
7	=	Document filing
8	=	Technical advice (only if requested)

Figure 1: TEA5 management structure

Figure 1 shows the three principals involved in the management of TEA5 and the relationships and interactions between them:

- ETSI is the owner of the TEA5. ETSI Technical Committee TETRA and Critical Communications Evolution sets the approval criteria for receipt of the algorithm (see clause 8).
- The TEA5 Custodian is the interface between ETSI and the recipients of TEA5 licences and specifications.
- The TEA5 Custodian is as identified in clause 9.2 of the present document. The TEA5 Custodian's duties are detailed in clause 9. They include distributing signed TEA5 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 TEA5 Custodian and applicant constitutes a licence to hold or use TETRA subscriber and fixed network equipment and components containing TEA5.

The form of CRUU exchanged is summarized in figure 2.

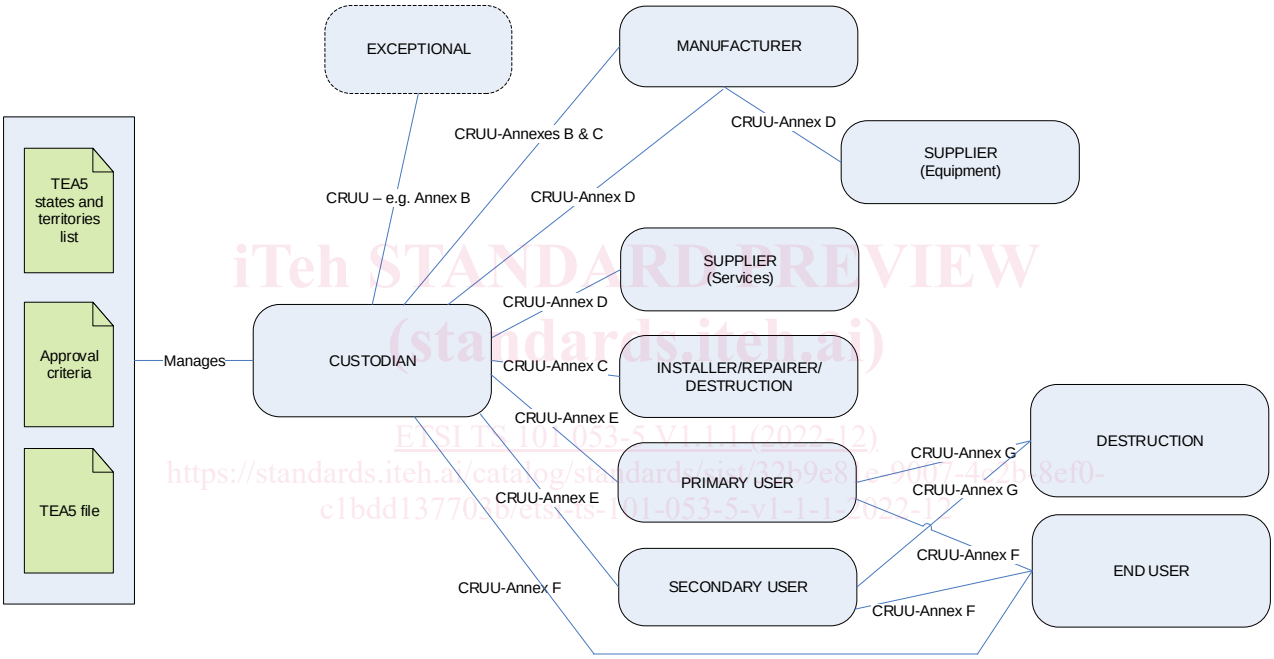


Figure 2: Summary of CRUU types maintained between TEA5 principals

5 Use of TEA5

5.1 Primary and Secondary Users of TEA5

A TEA5 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 TEA5 User Licence under these conditions is referred to as a primary user of TEA5. The Confidentiality and Restricted Usage Undertaking (CRUU) in annex E applies to primary and secondary users (see note 2). The TEA5 licence is required for the use of TEA5 in any element of the TETRA network including TETRA Subscriber equipment (TETRA Mobile Station (MS)) where air interface encryption as defined in ETSI EN 300 392-7 [i.1] or ETSI EN 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 TEA5, who has received a TEA5 User Licence from the TEA5 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 TEA5 End User Licence under these conditions is referred to as an end user of TEA5. A sub licence issued by the primary user of TEA5 is valid in the area of jurisdiction of that primary user, however it may also be extended to permit end users to operate in another permitted state or territory with the agreement of the primary user of that other state or territory. The CRUU in annex F applies to end users.

A primary user can approve the use of TEA5 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 TEA5 network and terminal equipment in connection with its deployment in any location outside of the TEA5 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 shall 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, shall be in place. All network and associated equipment shall 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 TEA5.

5.2 TEA5 States and Territories

Organizations can be a primary or secondary user of TEA5 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 TEA5 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 TEA5 states and territories is provided in annex H. The TEA5 Custodian maintains the definitive list of TEA5 states and territories.

5.3 Manufacture, supply, installation, repair and destruction of TEA5 equipment and services

A manufacturer licence may be issued to an organization that designs and/or manufactures completed equipment containing TEA5, or components of equipment (such as sub-assemblies, software modules or semiconductors) containing TEA5 or test equipment containing TEA5.

NOTE: An entity which manufactures TETRA equipment that does not contain TEA5 is not classified as a 'manufacturer' for the purposes of the present document, and provided that the entity does not subsequently install or integrate TEA5 from another source, such an entity may not need a manufacturer licence.

The licensee may provide such equipment, components or test equipment directly to an end user, or may provide these to another manufacturer, or to a supplier, installer or repairer of equipment containing TEA5, and may provide equipment or components for destruction. The recipient of a manufacturer licence may also supply, install, repair and destroy equipment containing TEA5 without the need for an additional licence. In order to provide equipment, components or test equipment containing TEA5 to another party, the manufacturer shall be provided with a copy of the TEA5 CRUU issued to that other party where that CRUU has been countersigned by the Custodian or primary or secondary user.

A supplier licence may be issued to an organization that provides equipment, components or test equipment containing TEA5 to an end user, but where the supplying organization does not manufacture or assemble such equipment, components or test equipment itself. Examples of suppliers of equipment can be distributors or resellers of equipment who act as intermediaries between the manufacturer and the end user. There can be multiple suppliers who have contractual responsibility in a chain of equipment supply between manufacturer and end user, and the supplier licence is applicable to all suppliers in such a chain of supply. A candidate for a supplier licence needs to be nominated by the manufacturer of the equipment, components or test equipment that contains TEA5. In a supplier relationship with the manufacturer and end user, at least one of the supplier and the manufacturer shall be supplied with a copy of the TEA5 CRUU issued to the end user where that CRUU has been countersigned by the Custodian or primary or secondary user, and the party that has been supplied with this copy of the end user's licence shall confirm to the other party or parties in the chain of supply that the copy of the end user licence has been provided. This usage of the supplier licence is illustrated as 'supplier (equipment)' in figure 2.

A supplier licence may be issued to an organization that operates a TETRA network containing TEA5 in order to provide TETRA services to end users. A supplier licence may also be issued to a service provider that provides network services to the end users on behalf of the network operator. In a service provider relationship with the end user, at least one of the service provider and network operator shall be supplied with a copy of the TEA5 CRUU issued to the end user to whom service is provided where that CRUU has been countersigned by the Custodian or primary or secondary user, and the party that has been supplied with this copy of the end user's licence shall confirm to the other party or parties in the chain of service provision that the copy of the end user licence has been provided. This usage of the supplier licence is illustrated as 'supplier (services)' in figure 2.

An installer/repairer/destruction licence may be issued to an organization that installs completed equipment containing TEA5, and which may possess test equipment containing TEA5. The installer/repairer/destruction licence may be given to an organization that repairs equipment containing TEA5 and which may handle components and/or software carriers containing TEA5, and which may possess test equipment containing TEA5. The installer/repairer/destruction licence may be given to an organization that destroys equipment containing TEA5 on behalf of a manufacturer, supplier or end user. The holder of the installer/repairer/destruction licence may only install equipment for or supply repaired equipment to an end user whose end user licence has been verified either by the party carrying out the installation or repair, or by a manufacturer on whose behalf the installation or repair has been carried out and where the manufacturer confirms to the installer or repairer that the copy of the end user's licence has been provided.

A destruction licence may be issued to an organization that destroys equipment or components or software carriers or test equipment containing TEA5, and who does not need to be able to install or repair equipment containing TEA5.

6 Licence types

6.1 Manufacturer Licence

An organization wishing to manufacture TETRA equipment and/or components containing TEA5 obtains its licence and copies of the TEA5 specifications by the procedure defined in clause 7.1.

6.2 Installer/Repairer/Destruction Licence

An organization that installs hardware or software components containing TEA5 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 TEA5 requires a manufacturer licence or an installer/repairer/destruction licence.

An organization that destroys equipment or components containing TEA5 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 TEA5 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 TEA5 into equipment, to repair equipment and components containing TEA5 and to destroy equipment, components and computer software carriers containing TEA5.

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 TEA5 (see annex C). The TETRA manufacturer shall send these to the TEA5 Custodian together with a nomination letter signed by the manufacturer.

The TEA5 Custodian then enters the details in the TEA5 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 TEA5 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 TEA5 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 TEA5 Custodian may check the suitability of the organization with respect to the relevant national legislation before granting an Installer/Repairer/Destruction licence.