TETRA + Critical Communications Association

Security and
Fraud
Prevention
Group

Information document

Overview of Standard TETRA Cryptographic Algorithms and their rules for management and distribution

Issue date: January 2014

Edition 4

TCCA SFPG Secretariat

Marjan Bolle, email: SFPG@TandCCA.com

1. Introduction

This document provides an overview of the TETRA standard cryptographic algorithms for air interface encryption. It describes their Rules for management and describes how the algorithms may be obtained. It also describes the applicability of export control regulations and distribution restrictions to standard air interface algorithms and equipment containing these algorithms, and the application of such regulations to other TETRA security features such as authentication and end-to-end encryption.

The information in this document may be helpful when describing TETRA encryption capability, TETRA algorithms and the aspects of export control regulation that apply to TETRA equipment and TETRA algorithms.

Export control regulations are a complex subject. Any user, manufacturer or distributor wishing to export TETRA equipment with security related functions is advised to consult his appropriate national authorities for the exact requirements relating to his circumstances.

2. References

[1] The Wassenaar Arrangement www.wassenaar.org

[2] ETSI EN302109 Synchronisation mechanism for end-to-end encryption

[3] SFPG Recommendation 02 – End-to-End Encryption
(available for Association members under a signed non-disclosure agreement; non-members need the support of an Association member)

3. TETRA standard air-interface encryption algorithms

Four standard encryption algorithms are currently available for use in TETRA systems. These have been developed by ETSI's Security Algorithm Group of Experts (SAGE) and are owned by ETSI. They are each held and distributed by a Custodian, see section 5 of this document.

All TETRA standard encryption algorithms and all TETRA equipment and components containing these algorithms are subject to export control. This applies to terminals and base stations alike. Many of the countries where TETRA equipment is designed and produced are signatories to the Wassenaar Arrangement (see ref [1]), and the countries where the custodians of the algorithms are located are amongst these.

The differences with respect to the application and distribution of the algorithms are explained below.

TEA2: Restricted Algorithm

This algorithm has been designed for use by Public Safety and Military Organisations. TEA2 has been assigned by ETSI for use exclusively in the European Union and related countries. Equipment containing TEA2 is not permitted to be supplied outside these countries.

TEA1, TEA3 and TEA4:

These algorithms have been designed for use by Public Safety and Military Organisations and are also appropriate for Civil use where security is a requirement. TEA1 is implemented in the majority of TETRA networks.

There may be differences in the exportability of each of the four algorithms. Consultation with national authorities is recommended to determine whether additional restrictions apply.

4. Algorithm Custodians

In the case of TEA1, TEA3 and TEA4, the custodian is ETSI (see http://portal.etsi.org/, section security algorithms and codes).

The TETRA and Critical Communications Association is the custodian for the TEA2 algorithm. Custodianship is entrusted to the chair of the TCCA Security and Fraud Prevention Group (SFPG). The TEA2 algorithm is distributed by the secretary of the SFPG (SFPG@TandCCA.com).

The standard TETRA Encryption Algorithms can be obtained under Confidentiality and restricted usage undertakings from the relevant Custodian. These undertakings require, among other things, that the algorithms are implemented in such a way that it is difficult to recover their design from the implementation. A full description of each undertaking can be found in the rules for management of the relevant algorithm.

5. TETRA standard set of Authentication and Key Management Algorithms

One standard set of Authentication and Key Management Algorithms is available. This standard TETRA Authentication and Key Management Algorithms set (TAA1) can be obtained under a Confidentiality and restricted usage undertaking from ETSI. This undertaking requires, among other things, that TAA1 is implemented in such a way that it is difficult to recover its design from the implementation.

Equipment containing authentication algorithms and performing authentication functions is not subject to export control regulations provided that the equipment contains no encryption functionality. However, equipment containing encryption key management functionality is subject to export control regulations.

6. Reference documents

The formal ETSI documents specifying the Rules for Management for the algorithm are listed below. In each case, the latest version of the listed document applies.

TR 101 052-1: Security Algorithms Group of Experts (SAGE); Rules for management of the TETRA standard authentication and key management algorithm set TAA1

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

TR 101 053-2: Security Algorithms Group of Experts (SAGE); Rules for management of the TETRA standard encryption algorithms; Part 2: TEA2

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

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

The Confidentiality and restricted usage undertakings for TEA1, TEA3, TEA4 and TAA1 can be obtained from the ETSI site: http://www.portal.etsi.org/, section security algorithms and codes. The contact person is Mrs. Gina Ebenezersson (Gina.Ebenezersson@etsi.org)

The Confidentiality and restricted usage undertaking for TEA2 can be obtained from the secretary of the Security and Fraud Prevention Group (SFPG), Mrs. Marjan Bolle (SFPG@TandCCA.com).

7. End to end encryption algorithms

There are no standard end-to-end encryption algorithms in TETRA. However the TETRA standard provides some specifications to assist the incorporation of end-to-end encryption in TETRA equipment. The standard specification is given in ref [2].

Additionally, more details on implementation of end-to-end encryption for speech are given in TCCA SFPG Recommendation 02, ref [3], including sample implementations for two algorithms, IDEA and AES.

Any equipment supporting end-to-end encryption functionality is subject to export control regulations. This includes equipment that contains an interface enabling end-to-end encryption to be implemented using an encryption module or smart card. In that case, the encryption module or smart card would also be subject to export control.