TETRA ASSOCIATION

TETRA Association
Association House
South Park Road
Macclesfield
Cheshire
SK11 6SH
United Kingdom
+44 1625 267886
+44 1625 267879

TETRA Association
Security and
Fraud
Prevention
Group

Information document

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

Issue Date: 20 February 2008

Edition 2

The Tetra Association Limted
Registered Office,
Richmond House, Broad Street
Ely, Cambridgeshire, CB7 4AH, UK
Registration No.4155039 in UK
VAT Registration Number GB 755 4236 24

TETRA SFPG Secretariat
Marjan Bolle
SFPG@tetra-association.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 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 equipments containing these algorithms, are subject to export control. 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. Therefore the design of the algorithms, and their intended application has been considered with this in mind.

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

TEA2 and TEA3: Restricted Export Algorithms

These algorithms are controlled items under the 1998 Wassenaar Arrangement rules. The algorithms have been primarily designed for use by Public Safety Organisations. TEA2 has been assigned by ETSI for use by Public Safety and Military Organisations in the European Union and related countries, and is not permitted to be sold outside these countries. TEA3 is an alternative for organisations that cannot obtain TEA2.

TEA1 and TEA4: Readily Exportable Algorithms

TEA1 and TEA4 are generally licensable for export.

4. Equipment containing TETRA air interface encryption algorithms

Equipment containing the TETRA standard encryption algorithms and performing air interface encryption is generally subject to export control law. This applies to terminals and base stations alike. The only exception is made where equipment fulfils all of the following criteria:

- it is sold to members of the public through normal retail means;
- the equipment does not permit the user to easily change the cryptographic function;
- the supplier is not expected to provide substantial support in installation;
- the equipment is not capable of end-to-end encryption.

This exception may therefore apply to mobile stations designed for use on public TETRA networks that are sold through normal retail channels and are not capable of end-to-end encryption. Ref [1] should be consulted for more information.

5. Algorithms Custodians

In the case of TEA1, TEA3 and TEA4, the custodian is ETSI (see http://portal.etsi.org/, section security algorithms and codes). The custodian for the TEA2 algorithm is the chair of the TETRA Security and Fraud Prevention Group (SFPG). The TEA2 algorithm is distributed by the secretary of the TETRA SFPG in the Netherlands.

The standard TETRA Encryption Algorithms TEA1, TEA3 and TEA4 can be obtained under a 'Non disclosure and restricted usage licence' from ETSI. This undertaking requires, among other things, that the algorithms are implemented in such a way that it is difficult to recover their design from the implementation. A user of TETRA who is entitled to use a particular TEAx (according to the rules for management of that algorithm) may also be able to obtain the algorithms from the relevant custodian and make his own assessment of whether it is appropriate for his use.

6. 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 'Non disclosure and restricted usage licence' 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.

7. 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 'Non disclosure and restricted usage licences' 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 'Non disclosure and restricted usage licence' for TEA2 can be obtained from the TEA2 custodian, the chair of the TETRA Security and Fraud Prevention Group (SFPG). The contact person is Mrs. Marjan Bolle (SFPG@tetra-association.com).

8. 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 TETRA SFPG Recommendation 02, ref [3], including sample implementations for two algorithms, IDEA and AES.

Any equipment containing end-to-end encryption functionality is subject to export control regulations. Any equipment which would enable a third party to add an end-to-end encryption function, for example an equipment that has an interface for an end-to-end encryption module (for example a Smart card encryption device), is also subject to export control regulation.