TECHNICAL SPECIFICATION

ISO/TS 21219-24

First edition
2017-02

Intelligent transport systems — Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) —

Part 24: Light encryption (TPEG2-LTE)

Systèmes intelligents de transport — Informations sur le trafic et le tourisme via le groupe expert du protocole de transport, génération 2 (TPEG2) —

Partie 24: Cryptage léger (TPEG2-LTE)

Reference number
ISO/TS 21219-24:2017(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see the following URL: http://www.iso.org/iso/foreword.html

The committee responsible for this document is ISO/TC 204, *Intelligent transport systems*.

A list of all the parts in the ISO 21219 series can be found on the ISO website.

Introduction

History

TPEG technology was originally proposed by the European Broadcasting Union (EBU) Broadcast Management Committee, who established the B/TPEG project group in the autumn of 1997 with a brief to develop, as soon as possible, a new protocol for broadcasting traffic and travel-related information in the multimedia environment. TPEG technology, its applications and service features were designed to enable travel-related messages to be coded, decoded, filtered and understood by humans (visually and/or audibly in the user's language) and by agent systems. Originally, a byte-oriented data stream format, which may be carried on almost any digital bearer with an appropriate adaptation layer, was developed. Hierarchically structured TPEG messages from service providers to end-users were designed to transfer information from the service provider database to an end-user's equipment.

One year later, in December 1998, the B/TPEG group produced its first EBU specifications. Two documents were released. Part 2 (TPEG-SSF, which became ISO/TS 18234-2) described the Syntax, Semantics and Framing structure, which was used for all TPEG applications. Meanwhile, Part 4 (TPEG-RTM, which became ISO/TS 18234-4) described the first application for Road Traffic Messages.

Subsequently, in March 1999, CEN/TC 278, in conjunction with ISO/TC 204, established a group comprising members of the former EBU B/TPEG and this working group continued development work. Further parts were developed to make the initial set of four parts enabling the implementation of a consistent service. Part 3 (TPEG-SNI, ISO/TS 18234-3) described the Service and Network Information Application used by all service implementations to ensure appropriate referencing from one service source to another.

Part 1 (TPEG-INV, ISO/TS 18234-1) completed the series by describing the other parts and their relationship; it also contained the application IDs used within the other parts. Additionally, Part 5, the Public Transport Information Application (TPEG-PTI, ISO/TS 18234-5), was developed. The so-called TPEG-LOC location referencing method, which enabled both map-based TPEG-decoders and non-map-based ones to deliver either map-based location referencing or human readable text information, was issued as ISO/TS 18234-6 to be used in association with the other applications parts of the ISO/TS 18234 series to provide location referencing.

The ISO/TS 18234 series has become known as TPEG Generation 1.

TPEG Generation 2

When the Traveller Information Services Association (TISA), derived from former forums, was inaugurated in December 2007, TPEG development was taken over by TISA and continued in the TPEG applications working group.

It was about this time that the (then) new Unified Modelling Language (UML) was seen as having major advantages for the development of new TPEG Applications in communities who would not necessarily have binary physical format skills required to extend the original TPEG TS work. It was also realized that the XML format for TPEG described within the ISO/TS 24530 series (now superseded) had a greater significance than previously foreseen, especially in the content-generation segment and that keeping two physical formats in synchronism, in different standards series, would be rather difficult.

As a result, TISA set about the development of a new TPEG structure that would be UML based. This has subsequently become known as TPEG Generation 2.

TPEG2 is embodied in the ISO/TS 21219 series and it comprises many parts that cover introduction, rules, toolkit and application components. TPEG2 is built around UML modelling and has a core of rules that contain the modelling strategy covered in ISO/TS 21219-2, ISO/TS 21219-3, ISO/TS 21219-4 and the conversion to two current physical formats: binary and XML; others could be added in the future. TISA uses an automated tool to convert from the agreed UML model XMI file directly into an MS Word document file, to minimize drafting errors, that forms the Annex for each physical format.

TPEG2 has a three container conceptual structure: Message Management (ISO/TS 21219-6), Application (many Parts) and Location Referencing (ISO/TS 21219-7[1)]). This structure has flexible capability and can accommodate many differing use cases that have been proposed within the TTI sector and wider for hierarchical message content.

TPEG2 also has many Location Referencing options as required by the service provider community, any of which may be delivered by vectoring data included in the Location Referencing container.

The following classification provides a helpful grouping of the different TPEG2 parts according to their intended purpose.

— Toolkit parts: TPEG2-INV (ISO/TS 21219-1), TPEG2-UML (ISO/TS 21219-2), TPEG2-UBCR (ISO/TS 21219-3), TPEG2-UXCR (ISO/TS 21219-4), TPEG2-SFW (ISO/TS 21219-5), TPEG2-MMC (ISO/TS 21219-6), TPEG2-LRC (ISO/TS 21219-7), TPEG2-LTE (ISO/TS 21219-24);

— Special applications: TPEG2-SNI (ISO/TS 21219-9), TPEG2-CAI (ISO/TS 21219-10);

— Location referencing: TPEG2-ULR (ISO/TS 21219-11[2)]), TPEG2-GLR (ISO/TS 21219-21[3)]), TPEG2-OLR (ISO/TS 21219-22[4)]);

— Applications: TPEG2-PKI (ISO/TS 21219-14), TPEG2-TEC (ISO/TS 21219-15), TPEG2-FPI (ISO/TS 21219-16), TPEG2-TFP (ISO/TS 21219-18), TPEG2-WEA (ISO/TS 21219-19), TPEG2-RMR (ISO/TS 21219-23), TPEG2-EMI (ISO/TS 21219-25).

TPEG2 has been developed to be broadly (but not totally) backward compatible with TPEG1 to assist in transitions from earlier implementations, while not hindering the TPEG2 innovative approach and being able to support many new features, such as dealing with applications having both long-term, unchanging content and highly dynamic content, such as Parking Information.

This document is based on the TISA specification technical/editorial version reference:

SP14002/1.0/001

1) Under development.

2) To be published.

3) Under development.

4) Under development.

Intelligent transport systems — Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) —

Part 24: Light encryption (TPEG2-LTE)

1 Scope

This document defines the LTE encryption mechanism for TPEG Service Data Frames. It has been specifically designed for use with Business to Business (B2B) business models.

The objective of this document is to provide a simple to use, yet effective Conditional Access mechanism for TPEG including encryption for use with both broadcast and/or point-to-point delivery.

For both service providers and device manufacturers, a standardized conditional access mechanism is beneficial to avoid a proliferation of proprietary methods with multiplied implementation effort and lead times.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/TS 21219-1, *Intelligent transport systems (ITS) — Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) — Part 1: Introduction, numbering and version (TPEG2-INV)*

ISO/TS 21219-2, *Intelligent transport systems (ITS) — Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) — Part 2: UML modeling rules (TPEG2-UMR)*

ISO/TS 21219-3, *Intelligent transport systems (ITS) — Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) — Part 3: UML to binary conversion rules (TPEG2-UBCR)*

ISO/TS 21219-4, *Intelligent transport systems (ITS) — Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) — Part 4: UML to XML conversion rules (TPEG2-UXCR)*

ISO/TS 21219-5, *Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) — Part 5: TPEG service framework (TPEG2-SFW)*

ISO/TS 21219-9, *Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) — Part 9: Service and network information (TPEG2-SNI)*

Federal Information Processing Standards Publication 197 — Specification for the ADVANCED ENCRYPTION STANDARD (AES), November 26, 2001

NIST Special Publication 800-38A:2001 Recommendation for Block Cipher Modes of Operation: Methods and Techniques

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at http://www.electropedia.org/

— ISO Online browsing platform: available at http://www.iso.org/obp

3.1
access controlled
conditions for use apply for which permission in writing is required

3.2
block cipher
family of functions and their inverse functions that is parameterized by cryptographic keys

Note 1 to entry: The functions map bit strings of a fixed length to bit strings of the same length.

3.3
block cipher mode of operation
algorithm that uses a block cipher to provide an information service such as confidentiality or authenticity

3.4
Control Word
cryptographic key used to protect the data stream, i.e. the payload data in a TPEG service data frame, by means of encryption

3.5
cryptographic key
parameter used in the block cipher algorithm that determines the forward cipher operation and the inverse cipher operation

3.6
encryption
process of encoding messages (or information) in such a way that only authorized parties can read it

3.7
service key
cryptographic key used to encrypt the transmission of the Control Word

Note 1 to entry: Service keys may be customer specific.

3.8
TPEG application
application layer protocol fulfilling the general TPEG requirements at the highest layer of the ISO OSI model and standardized by TISA/ISO

Note 1 to entry: A TPEG Application consists of a set of classes and rules for encoding information required to a traffic information service.

3.9
TPEG service
multiplex of TPEG Service Components with a dedicated Service Identifier

3.10
TPEG service component
virtual channel for messages of a dedicated TPEG Application

3.11
TPEG service multiplex
multiplex of TPEG Services within one data stream or file

3.12
service frame
data structure implementing the TPEG Service in the TPEG binary representation

3.13
service component frame
data structure implementing the TPEG Service Component stream in the TPEG binary representation

3.14
service data frame
service frame of type 1 containing TPEG service data as a multiplexed set of Service Component Frames

3.15
unrestricted access
no conditions for use apply, may be freely used without any permission or authorization

4 Abbreviated terms

AES	Advanced Encryption Standard
B2B	Business to Business
CRC	Cyclic Redundancy Check
CTR	Counter (a block cipher mode of operation)
CW	Control Word
EBU	European Broadcasting Union
ECB	Electronic Code Book (a block cipher mode of operation)
EMM	Entitlement Management Message
FRAND	Fair, Reasonable and Non-Discriminatory
LTE	LighT Encryption
ServEncID	Service encryption indicator (signalled in a TPEG Service Data Frame)
SID	TPEG Service ID
SFW	TPEG Service Framework: Modelling and Conversion Rules
TISA	Traveller Information Services Association
TPEG	Transport Protocol Expert Group
TTI	Traffic and Traveller Information
UML	Unified Modelling Language
XOR	eXclusive OR operation (a bit manipulation technique)

5 Light Encryption specific constraints

5.1 Version number signalling

Version numbering is used to track the separate versions of an application through its development and deployment. The differences between these versions may have an impact on client devices.

The version numbering principle is defined in ISO/TS 21219-1.

Table 1 shows the current version numbers for signalling LTE:

Table 1 — Current version numbers for signalling of LTE

major version number	1
minor version number	0

5.2 Extendibility

Light Encryption is based on a TPEG2 style specification of encryption parameters. Light Encryption information and parameters specifications are specified with a TPEG2 component, in accordance with the TPEG2 modelling rules in ISO/TS 21219-2 (TPEG2-UMR), ISO/TS 21219-3 (TPEG2-UBCR) and ISO/TS 21219-4 (TPEG2-UXCR). Future LTE extensions then may insert new components or may replace existing components by new ones without losing backward compatibility. That means an LTE decoder shall be able to detect and skip unknown components.

5.3 Endianness

TPEG assumes big endian representation of all multi byte constructs in the TPEG binary representation defined in ISO/TS 21219-3 (TPEG2-UBCR)), as does the AES standard (Federal Information Processing Standards Publication 197) and the NIST recommendation for Block Cipher Mode of Operations (NIST Special Publication 800-38A).

This document also assumes a big endian representation throughout, i.e. the Most Significant Byte/Bit is transmitted/stored first, and the Least Significant Byte/Bit is transmitted/stored last.

5.4 Supported business models

This document supports a number of common business models with the following two modes of encryption:

— Light Encryption Mode 1: free to air, yet encrypted transmission of TPEG data;

— Light Encryption Mode 2: controlled access, encrypted transmission of TPEG data, on basis of a business-2-business contract agreement.

Mode 1 is a generic mode, which does not differentiate between various client devices nor manufacturers. Mode 2 targets business-to-business (B2B) relations. This mode is able to differentiate various (B2B) customers.

In mode 2, a service provider is able to activate or revoke access to its service by changing its transmission scheme. Moreover, in mode 2, access can be separately activated for individual (B2B) customers.

Conversely, in mode 2, access can also be revoked separately for individual (B2B) customers, through updates of the transmitted Light Encryption parameters. In this last use case, new encrypted Control Words will be provided to all customers except the revoked B2B customer. This revoked customer is no longer able to decrypt TPEG data, due to the lack of the new version of the Control Word.

Table 2 — Supported business models

Business model	B2B relation established before sale of device	B2B relation established after sale of device		No relation, unrestricted access
Service type	**Mode 2, Access Controlled Service** **B2B Keys exchanged before sale of device**		**Mode 1, free Trial Service**	**Mode 1, Free-to-Air Service**
Activation model	B2B Service Keys given to **established customers** On-air Activation before sale of device	B2B Service Keys given to **potential customers** On-air Activation only after establishment B2B relation	**Temporary free service; activation by SP only** (no access rights management required for client manufacturer, free service kept alive until Software Update o client devices)	**Permanent free to air service** (no access rights management required for client manufacturer)

Table 2 shows a number of supported business models. Light Encryption Mode 1 can be used either as a temporary, free trial service or as a permanent free-to-air service with encrypted content.

Mode 2 supports business-to-business relationships. When a B2B relationship is established before the sale of the client device, all necessary precautions should be taken such as exchange of needed "parameters-in-confidence". Light Encryption provides the means for a service provider to activate access for the particular customer after the commencement of a contract agreement. In advance, by pre-allocating and pre-sharing "parameters-in-confidence" with a potential customer, device manufacturers are able to prepare their devices ahead of service transmissions. In this way, potential B2B user devices can be prepared in parallel to a contract agreement, reducing or eliminating lead-time for device implementations.

5.5 Performance requirements

5.5.1 Repetition rate of light encryption parameters

All necessary entitlement parameters for any access-permitted TPEG client (i.e. a client with active access permissions to the current state of the service) to start using the service and decrypting its content shall be available with a repetition rate of one minute or less. This is to reduce start-up latency.

Advance information of upcoming changes in entitlement parameters may be distributed at a slower rate. Clients are recommended to store relevant encryption parameters and Control Words over power-down cycles for fastest start-up. The Control Word Version ID (attribute *CWversionID*) signals the version in use, and clients shall match stored versions with the signalled version before proceeding with decryption on basis of stored parameters.

5.5.2 Update rate of light encryption parameters

Encryption parameters and consequent Control Word versions should be updated infrequently, but shall not be updated more than once every 10 min. TPEG clients may receive reliably all necessary parameters, even under less than perfect reception conditions.

5.6 License agreement and security requirements

5.6.1 General

This document uses two secret pieces of information (cryptographic parameters – see 6.2.1). These are distributed by TISA under FRAND conditions, but subject to a license agreement. The license agreement with TISA shall ensure strict confidentiality in handling, storage, and proper use (for intended purposes only) of these secret cryptographic parameters.