TECHNICAL SPECIFICATION

ISO/TS 21219-10

First edition
2016-05-01

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

Part 10: Conditional access information (TPEG2-CAI)

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

Partie 10: Information d'accès conditionnel (TPEG2-CAI)

Reference number
ISO/TS 21219-10:2016(E)

International Organization for Standardization

COPYRIGHT PROTECTED DOCUMENT

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 WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/TC 204 *Intelligent transport systems*, in cooperation with the Traveller Information Services Association (TISA), TPEG Applications Working Group through Category A Liaison status.

ISO/TS 21219 consists of the following parts, under the general title *Intelligent transport systems — Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2):*

— *Part 1: Introduction, numbering and versions*

— *Part 2: UML modelling rules*

— *Part 3: UML to binary conversion rules*

— *Part 4: UML to XML conversion rules*

— *Part 5: Service framework*

— *Part 6: Message management container*

— *Part 10: Conditional access information*

— *Part 18: Traffic flow and prediction application*

— *Part 19: Weather information*

The following parts are under preparation:

— *Part 9: Service and network information*

— *Part 14: Parking information application*

— *Part 15: Traffic event compact*

— *Part 16: Fuel price information application*

The following parts are planned:

— *Part 7: Location referencing container*

— *Part 11: Universal location reference*

— *Part 21: Geographic location referencing*

— *Part 22: OpenLR location referencing*

— *Part 23: Road and multimodal routes application*

— *Part 24: Light encryption*

— *Part 25: Electromobility information*

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/WG 4, in conjunction with ISO/TC 204/WG 10, 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). 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);

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

Location referencing: TPEG2-ULR (ISO/TS 21219-11), TPEG2-GLR (ISO/TS 21219-21), TPEG2-OLR (ISO/TS 21219-22);

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 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 Technical Specification is based on the TISA specification technical/editorial version reference:

SP13007/1.1/001.

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

Part 10:
Conditional access information (TPEG2-CAI)

1 Scope

This part of ISO/TS 21219 defines the TPEG Conditional Access Information (CAI) application. It allows to protect the content of a TPEG service from unauthorized access. It further supports the management of subscriber information (e.g. Control Words and ECM) on the client devices in order to setup, prolong or revoke a subscription on a given client device.

The application defines

— the logical channel, for the transmission of the additional CA information (CAI), and

— how the CAI is linked and synchronized to the scrambled content.

This part of ISO/TS 21219 is related to conditional access applied on service component level. It is open for an integration of different conditional access systems.

NOTE The basic concept behind the CAI application is to transport CAI in separate TPEG service components of a dedicated application type and to define an SNI table that contains the link between scrambled content and related CAI.

2 Terms and definitions

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

2.1
service
collection of different information streams (applications) logically bound together and delivered from a service provider to the end user

2.2
service component
information stream (application) that is part of a *service* (2.1)

Note 1 to entry: A TPEG stream is logically divided into parts known as service components. Each service component carries an application instance. A service component is effectively a “channel” within the multiplex of a TPEG stream. Each stream comprises a number of these “channels” which are identified by the component identifier in TPEG2-SFW [5] and linked to the COID and AID in the TPEG2-SNI application.

3 Abbreviated terms

For the purposes of this Technical Specification, the following abbreviated terms apply.

ACID	Application and Content Identifier
AID	Application Identification
CA	Conditional Access
CAI	Conditional Access Information
CEN	Comité Européen de Normalization
CRC	Cyclic redundancy check
EBU	European Broadcasting Union
ECM	Entitlement Control Message
EMM	Entitlement Management Message
MMC	Message Management Container
n.a.	not available
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

4 Application specific constraints

4.1 Application identification

The word “application” is used in the TPEG specifications to describe specific subsets of the TPEG structure. An application defines a limited vocabulary for a certain type of messages, for example, parking information or road traffic information. Each TPEG application is assigned a unique number, called the Application IDentification (AID). An AID is defined whenever a new application is developed and these are all listed in TPEG2-INV.

The application identification number is used within the TPEG2-SNI application to indicate how to process TPEG content and facilitates the routing of information to the appropriate application decoder.

4.2 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 TPEG2-INV.

Table 1 shows the current version numbers for signalling CAI within the SNI application.

Table 1 — Current version numbers for signalling of CAI

major version number	1
minor version number	1

4.3 TPEG Service Component Frame

CAI makes use of the “Service Component Frame with dataCRC” according to TPEG2-UXCR.

5 Conditional access methodology

Conditional access (CA) is specified within TPEG2-SFW and TPEG2-SNI as a function being applied on service frame or service component level. The method used is indicated via the Encryption Identifier (EncID) directly in the service frame or for components via the SNI Fast Tuning Table (Guide to the Services 1). This part of ISO/TS 21219 is related to conditional access applied on service component level (EncID) according to TPEG2-SFW.

Generally, a broadcast based CA-system requires encryption related data to be transmitted which is independent from the content, but necessary for decryption and subscriber management.

If a conditional access system is applied on the TPEG service component level, some service components may be encrypted using the same “encryption key”, while others remain unencrypted or use different “encryption keys”. Therefore, several service components can share the same conditional access information, if they are supposed to be offered as one bundle and hence are encrypted with the same keys.

Each of the aforementioned bundles may require CA-management-messages, which are to be transmitted separated from the (encrypted) content in the corresponding service components. The most appropriate way for the transport is the use of separate service components of a dedicated application type.

For each encrypted TPEG-Service component, a link or reference to the service component carrying the relevant CA information is required. This is handled by TPEG2-SNI GST-Table 6, Conditional Access Information Reference.

EXAMPLE Table 2 illustrates that a TPEG Service may contain the following service components.

Table 2 — Example for Service Component IDs within a TPEG Service

SCID	Application
0	SNI
2	TEC
5	TEC (encrypted)
7	TEC (encrypted)
8	PTI
10	PKI (encrypted)
20	CAI
21	CAI
30	CAI

The service components 5 and 7 are encrypted with key 1, while service component 10 is encrypted using key 2. Hence, two components with CA-meta information for the corresponding component are required, in the example listed as SCID 20 and 21. A third CAI component, in the example number 30, contains CA-meta information that relates to all encrypted components independent which key is applied.

This part of ISO/TS 21219 describes the generic containers for the CAI application. The container content will be proprietary and specified individually for each CA-System indicated by the encryption indicator (EncID). The linking between encrypted service components and related CAI-Components is achieved via a reference table within the TPEG2-SNI application.

6 CAI structure

Unlike other TPEG applications, TPEG2-CAI does not use a Message Management Container and does not use a Location Referencing Container; it only uses CA system specific message data containers.

The following Figure 1 shows the logical structure of the Conditional Access Information (CAI) application.

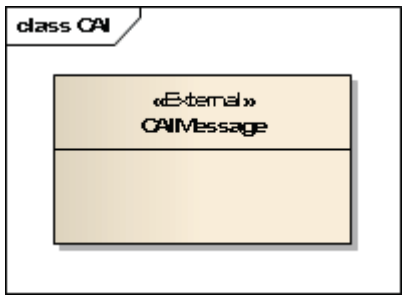

Figure 1 — CAI message structure

7 CAI message components

7.1 CAIMessage

A TPEG2-CAI Message includes solely one single container for proprietary CA data. The CAI Message Container is available to carry data, which is defined within the CA system specific specifications and determined by the encryption indicated for the components in the SNI.

This is the proposed TPEG2 definition. However, the definition of the CAIMessage container and its format may be overridden by CA system specifications, depending on the encryption indicator signalled in the SNI.

Annex A
(normative)

TPEG CAI, TPEG-binary representation

A.1 General

This Annex provides the TPEG binary representation derived via application of the UML to binary conversion rules specified in TPEG2-UBCR.

A.2 Message components

A.2.1 List of generic component Ids

Table A.1 shows the identifier (Id) used for the CAIMessage.

Table A.1 — CAIMessage Identifier

Name	Id
CAIMessage	1

A.2.2 CAIMessage

Table A.2 shows the structure of the CAIMessage.

Table A.2 — CAIMessage structure

<CAIMessage(1)>:=	
External <UndefinedPackage(1)>;	: External package is not defined here, but instead in the CA system specification signalled by the encryption indicator.

The message contents are directly following after the lengthAttr of the CAIMessage.

The CAIMessage is defined according to the TPEG2 component definition including IntUnLoMB Length indidcator and lengthAttr. However, the definition of the CAIMessage container and its format may be overridden by CA system specifications, depending on the encryption indicator signalled in the SNI.

Annex B
(normative)

TPEG CAI, tpegML Representation

B.1 General

This Annex provides the XML representation derived via application of the UML to XML conversion rules specified in TPEG2-UXCR.

NOTE In the course of ISO processing, XML-compliant quotation marks are replaced with non-compliant quotation marks. When taking over material from these sections, be advised to substitute any double quote to the XML-compliant equivalent quotation mark (Unicode U +0022).

B.2 Message components

The CAIMessage is defined in the CA system specification and needs to be imported into the following template schema definition.

B.3 Full CAI schema definition

```
<?xml version="1.0" encoding = "UTF-8"?>
<!- This XML schema is generated with tpegUMLconverter V2.1 ->
<xs:schema xmlns="http://www.tisa.org/TPEG/CAI_1_1"
  targetNamespace="http://www.tisa.org/TPEG/CAI_1_1"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:tsf="http://www.tisa.org/TPEG/SFW_1_1"
  xmlns:tdt="http://www.tisa.org/TPEG/TPEGDataTypes_2_0"
  elementFormDefault="qualified"
  attributeFormDefault="qualified" >
  <xs:import namespace="http://www.tisa.org/TPEG/SFW_1_1" schemaLocation = "file://./sfw.
xsd"/>
  <xs:import namespace="http://www.tisa.org/TPEG/
TPEGDataTypes_2_0" schemaLocation = "file://./tdt.xsd"/>
</xs:schema>
```

This schema needs to import the CA system specific external CAIMessage xsd.

Bibliography

[1] ISO/TS 18324-10, *Intelligent transport systems (ITS) — Traffic and Travel Information (TTI) via Transport Protocol Experts Group, Generation 1 (TPEG1) binary data format —Part 10: Conditional Access Information (TPEG1-CAI)*

[3] ISO/TS 21219-1, *Intelligent transport systems — Traffic and travel information via transport protocol experts group, generation 2 (TPEG2) — Part 1: Introduction, numbering and versions*

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

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

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

[7] ISO/TS 21219-5, *Intelligent transport systems — Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) — Part 5: Service framework (TPEG2-SFW)*

[8] ISO/TS 21219-6, *Intelligent transport systems — Traffic and travel information via transport protocol experts group, generation 2(TPEG2) — Part 6: Message management container (TPEG2-MMC)*

[9] ISO/TS 21219-9,[1)]*Intelligent transport systems — Traffic and travel information via transport protocol experts group, generation 2 (TPEG2) — Part 9: Service and network information*

[10] SCHEMA DEFINITION X.M.L. http://www.w3.org/XML/Schema

1) To be published.

ICS 03.220.01; 35.240.60

Price based on 7 pages