INTERNATIONAL STANDARD

ISO 21219-10

First edition
2023-05

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 21219-10:2023(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword ..... **iv**
Introduction ..... **v**
1 Scope **1**
2 Normative references **1**
3 Terms and definitions **1**
4 Abbreviated terms **2**
5 Application specific constraints **2**
5.1 Application identification 2
5.2 Version number signalling 2
5.3 TPEG service component frame 2
6 Conditional access methodology **2**
7 CAI structure **3**
8 CAI message components **4**
8.1 CAIMessage 4
Annex A (normative) **TPEG CAI, TPEG-binary representation** **5**
Annex B (normative) **TPEG CAI, tpegML representation** **6**
Bibliography **7**

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 of the voluntary nature of standards, 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 www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 204, *Intelligent transport systems*.

This first edition cancels and replaces the first edition (ISO/TS 21219-10:2016), which has been technically revised.

The main changes are as follows:

— the document has been changed from a Technical Specification to an International Standard.

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

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

0.1 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 can 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, later 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, later 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, later 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 of parts of the ISO 18234 series to provide location referencing.

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

0.2 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 the 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 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).

TPEG2 is embodied in the ISO 21219 series and it comprises many parts that cover an 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 21219-2, ISO 21219-3 and ISO 21219-4 and the conversion to two current physical formats: binary (see Annex A) and XML (see Annex B); others can 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; this file forms the annex for each physical format.

TPEG2 has a three-container conceptual structure: message management (ISO 21219-6), application (several 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. Note that the list below is potentially incomplete, as there is the possibility that new TPEG2 parts will be introduced after the publication of this document.

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

— Special applications: TPEG2-SNI (ISO 21219-9), TPEG2-CAI (ISO 21219-10 - this document), TPEG2-LTE (ISO/TS 21219-24).

— Location referencing: TPEG2-OLR (ISO/TS 21219-22), TPEG2-GLR (ISO/TS 21219-21), TPEG2-TLR (ISO 17572-2), TPEG2-DLR (ISO 17572-3).

— Applications: TPEG2-PKI (ISO 21219-14), TPEG2-TEC (ISO 21219-15), TPEG2-FPI (ISO 21219-16), TPEG2-SPI (ISO 21219-17), TPEG2-TFP (ISO 21219-18), TPEG2-WEA (ISO 21219-19), TPEG2-RMR (ISO/TS 21219-23), TPEG2-EMI (ISO/TS 21219-25), TPEG2-VLI (ISO/TS 21219-26).

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 with 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:

SP20010_1.2_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 document defines the TPEG conditional access information (CAI) application. It allows the protection of the content of a TPEG service from unauthorized access. It further supports the management of subscriber information (e.g. control words and entitlement control message, ECM) on client devices in order to setup, prolong or revoke a subscription on a given client device.

The CAI application defines:

— the logical channel for the transmission of the additional CAI, and

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

This document is related to conditional access applied on the service component level. It can be integrated into 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 a service and network information (SNI) table that contains the link between scrambled content and related CAI.

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

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

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 21219-1 and ISO 21219-9 apply.

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

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

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

4 Abbreviated terms

For the purposes of this document, the abbreviated terms listed in ISO 21219-1, ISO 21219-9 and the following apply.

AID application identifier

CA conditional access

CRC cyclic redundancy check

ECM entitlement control message

EncID encryption identifier

SCID service component identifier

SNI service and network information

5 Application specific constraints

5.1 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 identity (AID). An AID number is defined in ISO 21219-1 whenever a new application is developed.

The AID number is used within the TPEG2-SNI application (ISO 21219-9) to indicate how to process TPEG content. It facilitates the routing of information to the appropriate application decoder.

5.2 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 can have an impact on client devices.

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

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	2

5.3 TPEG service component frame

CAI makes use of the “Service Component Frame with dataCRC” according to ISO 21219-4.

6 Conditional access methodology

Conditional access (CA) is specified within ISO 21219-5 and ISO 21219-9 as a function applied on the 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 document is related to conditional access applied on the service component level (EncID) according to ISO 21219-5.

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

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

Each of the aforementioned bundles can require CA management messages, which are transmitted separately 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 ISO 21219-9:2023, Table 6.

Table 2 illustrates the service components that can be contained in a TPEG service.

Table 2 — Examples for Service Component IDs (SCIDs) 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

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 examples listed as SCID 20 and 21. A third CAI component, in example number 30, contains CA-meta information that relates to all encrypted components, independent of which key is applied.

This document describes the generic containers for the CAI application. The container content will be proprietary and specified individually for each CA-System indicated by the EncID. The linking between encrypted service components and related CAI-Components is achieved via a reference table within the TPEG2-SNI (ISO 21219-9) application.

7 CAI structure

Unlike other TPEG applications, TPEG2-CAI does not use an MMC and does not use an LRC; it only uses CA system specific message data containers. The binary format and XML format of the TPEG2-CAI application for use in transmission shall be in accordance with Annexes A and B, respectively.

The following Figure 1 shows the logical structure of the CAI application.

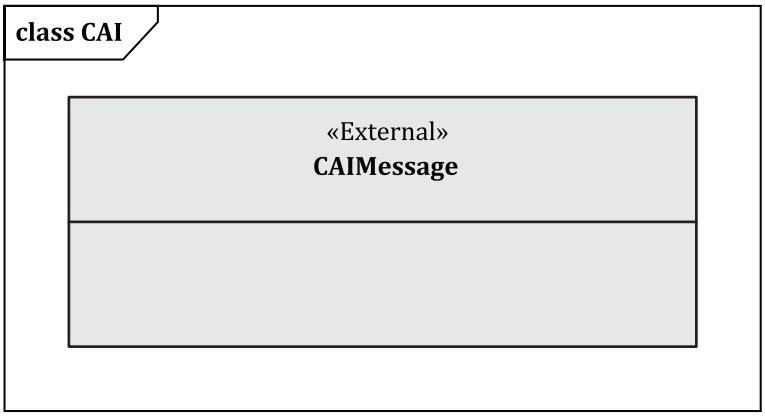

Figure 1 — CAI message structure

8 CAI message components

8.1 CAIMessage

A TPEG2-CAI message includes solely one single container for proprietary CA data. The CAIMessage 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 ISO 21219-3.

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 follow directly after the lengthAttr of the CAIMessage.

The CAIMessage is defined according to the TPEG2 component definition including IntUnLoMB lengthComp and lengthAttr indicators (see ISO 21219-3). 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.