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.

5.6.2 Security requirements on service providers

5.6.2.1 Development

During development of Light Encryption, service providers should limit to a minimum the personnel having access to the secret cryptographic parameters distributed by TISA, and any customer and service specific cryptographic parameters. Development artefacts related to these parameters shall be stored in a protective fashion, to prevent unauthorized access.

5.6.2.2 Operation

During Light Encryption operations (including service key, Control Word and customerParameterInConfidence generation, and generation of encrypted content) access to server rooms and servers running Light Encryption operations or storing Light Encryption parameters should be protected. Physical storage of all cryptographic parameters should be governed by a conditional access mechanism including encryption. The chosen protection scheme should make it difficult to find, use, or replace confidential cryptographic parameters.

The Service Provider should limit to a minimum personnel having access to servers running Light Encryption or storing Light Encryption cryptographic parameters.

5.6.3 Security requirements on client manufacturers

5.6.3.1 Development

During development of Light Encryption, client device manufacturer should limit to a minimum the personnel having access to the secret cryptographic parameters distributed by TISA, and/or customer and service specific cryptographic parameters. Development artifacts related to these parameters shall be stored in a protective fashion, to prevent unauthorized access.

5.6.3.2 Firmware and firmware distribution

The secret cryptographic parameters distributed by TISA, and any further customer and service specific cryptographic parameters should be stored in encrypted/obfuscated form in a device's firmware, such as to prevent security leaks from inspecting firmware or firmware updates. The chosen protection scheme should make it difficult to find, use, or replace confidential cryptographic parameters. The chosen protection scheme for storage in a device's firmware may be proprietary.

6 Light encryption method of encryption and operation

6.1 Principles of operation for light encryption

The objective of Light Encryption for TPEG is to achieve a simple encryption method, while still allowing effective compression of service frame payload data. To do so, the selected operating principle is to encrypt the complete service frame payload data in one go (as opposed to encryption of individual service component frames). This principle affords a single access point for decryption in the TPEG client, which gets passed a complete TPEG service data frame to process. Efficient transmission can be achieved, since the service frame payload data can be compressed first, before applying encryption.

Consequently, when a service provider desires mixing unencrypted and encrypted TPEG data, this provider needs to set up different TPEG services with different TPEG Service IDs and mix these in the TPEG service multiplex. Access rights management and encryption shall be handled at the TPEG service multiplex level, where individual TPEG services are either encrypted or clear-to-air.

This scheme allows a TPEG service composition in which clear-to-air content in TPEG service multiplex is accessible for TPEG clients, without these clients needing to know of any encryption and/or conditional access system knowledge. Service providers can link content of such various services to each other, by

means of the TPEG concept of "originator" TPEG service ID ISO (TS21219-9). With the "originator" TPEG service ID, a service provider can inform a TPEG client that content from one clear-to-air TPEG service is from the same source as the content of an encrypted TPEG service.

Key requirements addressed in this conditional access mechanism are the following:

— The method shall support commonly used business models in TPEG over broadcast delivery;

— The method shall provide an appropriate level of security against unauthorized access and usage in Traffic and Traveller Information (TTI) context;

— The method shall be license-free to operate;

— The method shall be easy to implement at the TPEG client side and TPEG server side and shall have minimal overhead;

— The method shall be bearer-independent;

— The method shall allow granting and revoking of access to individual B2B customers.

6.2 Overview of the light encryption method

6.2.1 General

For Light Encryption, the used encryption algorithms are based on the Advanced Encryption Standard (AES; see Federal Information Processing Standards Publication 197). Light Encryption distinguishes two modes to support different business models. Technically, the two modes differ only in distribution of the "parameterInConfidence" with which the service keys are composed.

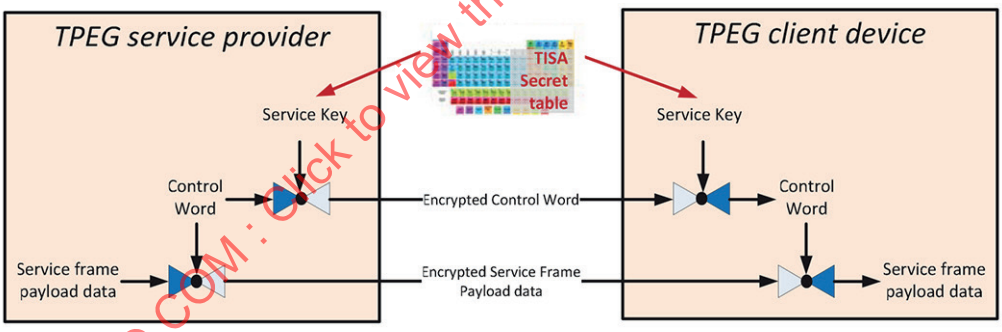

Figure 1 — Mode 1 encryption method principle

Figure 1 shows the encryption scheme for Light Encryption mode 1. In this mode 1, the service frame payload data is encrypted with a *Control Word*. This Control Word (common to all clients) may be changing over time for security reasons. New Control Words are encrypted with a *Service Key* before transmission to a client. The encrypted Control Words are distributed in the service with Entitlement Messages. In mode 1, a single Entitlement Message is provided for all clients.

The Service Keys are composed of a pre-shared, secret, key table maintained and distributed by TISA under strict confidentiality. The service key composition selects a substring of the TISA secret table, and then applies bit manipulation techniques (two XOR operations interspersed with a shift operation). For symmetry with mode 2, the TISA secret information contains the TISA key table and a generic "TISAparameterInConfidence". In mode 1, this parameter shall be used by all clients in the same way (whereas in mode 2, this "parameterInConfidence" shall be customer specific).

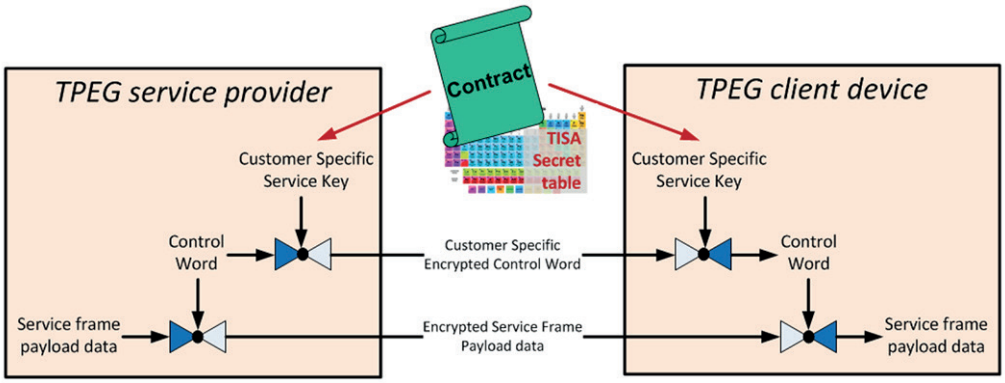

Figure 2 — Mode 2 encryption method principle

Figure 2 shows the encryption scheme for Light Encryption mode 2 which operates in the same fashion as mode 1. Only when composing the Service Key, instead of the *TISAparameterInConfidence*, a customer-specific *parameterInConfidence* is used to specify the Service Key for a specific customer. This customer specific "parameterInConfidence" (and allocated "customerID") shall be pre-shared between a specific TPEG Service Provider and a specific TPEG Client manufacturer as part of a contract agreement. Once the Service Key is used to encrypt (at service side) or decrypt (at client side) the transmitted encrypted Control Word, the rest of the process remains identical.

The encrypted Control Words are distributed in the service with Entitlement Messages. In mode 2, for every (B2B) customer a separate Entitlement Message is provided. The client shall check the "customerID" attribute contained in the Entitlement Message to obtain its customer-specific entitlement parameters.

TPEG clients under valid contract with a Service Provider shall be able to decode both Light Encryption Mode 1 and Mode 2. This enables the Service Provider to switch temporarily to mode 1, when business reasons would warrant so.

Clients shall ascertain at all times whether they have the correct (decrypted) Control Word for a specific signalled Light Encryption Mode and Control Word Version Id. Only then they may proceed to decrypt the encrypted payload data. If not, they shall discard encrypted payload data.

NOTE In Annex C, guidelines (informative) for use of this document are given.

6.2.2 TISA secret KeyTable and TISAparameterInConfidence

This document uses two secret pieces of information which are distributed by TISA under strict confidentiality rules:

— TISA KeyTable: a several kilobyte, long byte, array containing random numbers;

— TISAparameterInConfidence: a 16 bytes, long byte, array containing random numbers for use in light encryption mode 1.

For secrecy reasons, this document does not contain these parameters. They can be obtained from TISA under FRAND conditions. An application shall be made using the request form on the TISA website (www.tisa.org). After signing and returning the corresponding confidentiality agreement to TISA, this TISA KeyTable and TISAparameterInConfidence shall be made available in digital form.

6.3 Encryption and decryption of service data frame payload data

6.3.1 General

The service data frame payload is encrypted using the AES standard (Federal Information Processing Standards Publication 197). The Control Word is used as the cryptographic key in AES for service payload data encryption. The 128-bit (16 bytes) long version of AES cipher is chosen (referred to as AES128 in NIST Special Publication 800-38A). Since the length of the service data frame payload is much longer than this standard 16 or (alternatively 32-byte AES) block cipher length, a block cipher mode of operation is needed. A mode of operation specifies how to repeatedly apply a block cipher's single-block operation to securely transform amounts of data larger than a block.

6.3.2 Block cipher mode of operation

For Light Encryption of service frame payload data, the *Counter Mode* (CTR) mode of operation is employed (NIST Special Publication 800-38A). Counter mode is the fastest mode of operation and processed concurrently by both the Service Provider and the client device.

The CTR mode is applied only for service frame payload encryption. For both Light Encryption modes 1 and 2, the service frame payload data is encrypted with CTR-AES128 (NIST Special Publication 800-38A).

NIST has made available CTR-AES128 test vectors in NIST Special Publication 800-38A, Appendices F5.1 and F5.2. These test vectors shall be used for validation of implementations of this document.

Payload encryption is performed on blocks of application data. In the CTR-AES128 mode of operation, a block consists of 16 bytes of service frame payload data as contained in a TPEG Service Data Frame. The CTR mode ensures that distinct ciphertexts blocks are produced even when the same plaintext block is encrypted multiple times independently with the same Control Word.

To do so, for each block a new Initialisation Vector (IV) is needed. Information for this IV (a Nonce [A NONCE is a Number used ONCE], the TPEG SID, and the LTE mode) is transmitted in front of the encrypted Service Data Frame payload data as part of the Light Encryption Information ("*LteInformation*") component (see Clause 7). These transmitted parameters are complemented by a running *counter* to construct the initialisation vector per block of data.

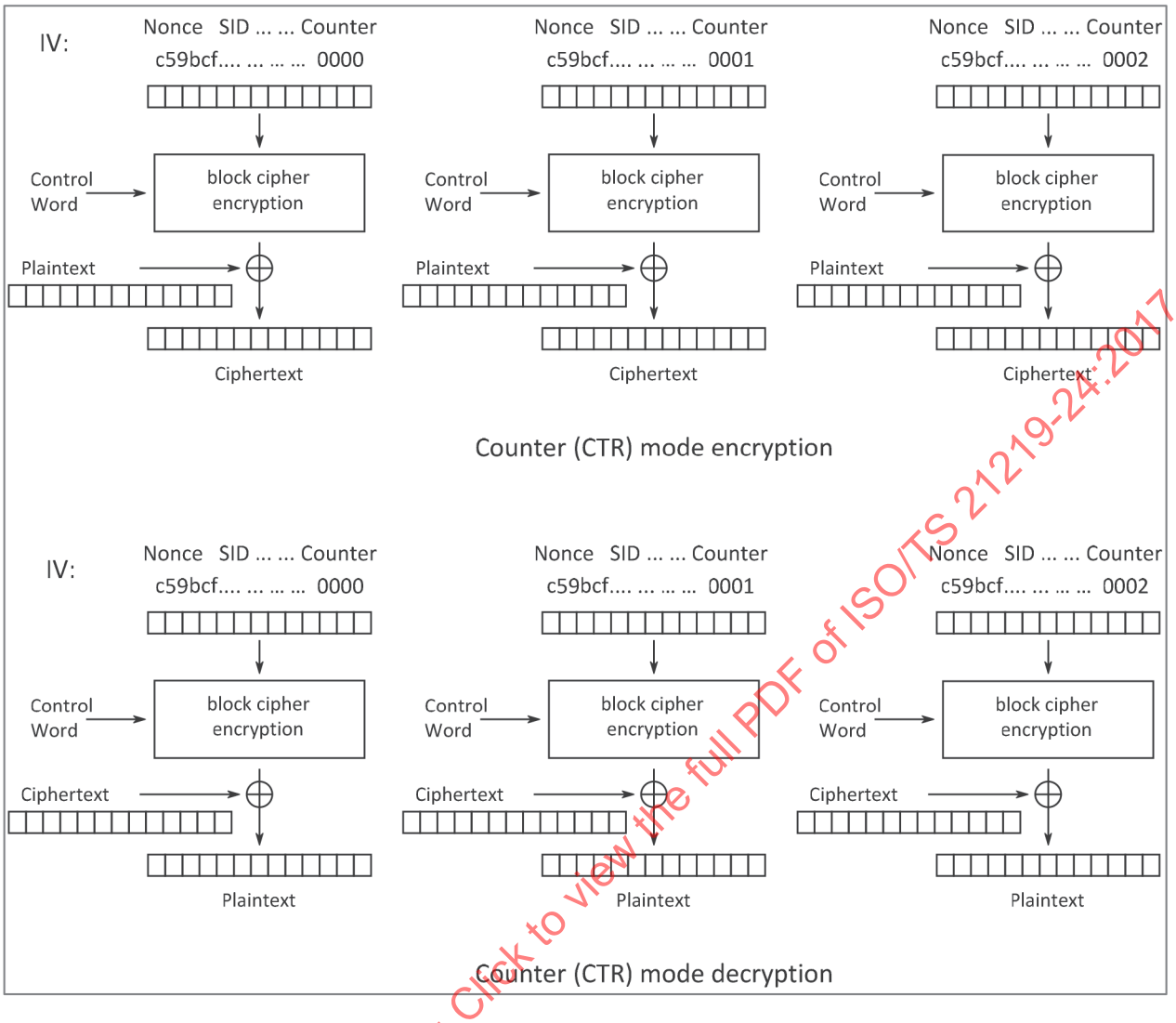

Figure 3 — CTR mode of operation for encryption and decryption of service data frame payload data

Figure 3 shows the principle of the CTR mode of operation. For each block of data, the constructed Initialisation Vector is encrypted using the Control Word. The encrypted Initialisation Vector is then subject to an XOR operation with the plaintext to produce the ciphertext for encryption (top), or alternatively, the encrypted Initialisation Vector then subject to an XOR operation with the ciphertext to produce the plaintext for decryption (bottom).

The counter is incremented by one (as an IntUnLi value) for every successive block of service frame payload data in the Initialisation Vector. The structure of this Initialisation Vector is detailed next.

6.3.3 Initialisation Vector

For Light Encryption mode 1 and mode 2, the binary representation of the 16 byte initialisation vector IV of the CTR mode is specified as follows:

<InitialisationVector<IV)>>:=	: 16 byte Initialisation Vector IV for CTR mode.
10 *<IntUnTi>(nonceValue),	: 10 byte value of the Nonce, signalled in the data structure mode1Nonce or mode2Nonce for mode 1 or mode 2 respectively (see 5.5). The value of this Nonce shall contain a unique numeric value for every service frame encrypted with the same Control Word.
<ServiceIdentifier>(SID),	: The TPEG Service Identifier (SID) as signalled in the header of the Service Frame.
<lte001:LightEncryptionMode> (lteMode),	: The Light Encryption Mode in use for this service, as signalled in the LteInformation component (see Figure 8).
<IntUnLi> (counter);	: 2 byte counter (initialized at 0 at the start of every encrypted service data frame)

The constructed Initialisation Vector shall be unique for every Service Provider and every mode. The attributes *nonceValue*, *lteMode* and *CWversionID* are transmitted in the *LteInformation* component (see Clause 7). The attribute *SID* is transmitted in the header of every Service Frame. The *counter* is not transmitted, but rather reset to 0 for every new encrypted service data frame, and then incremented by one for every successive block of 16 bytes to be encrypted or decrypted (see Figure 3).

Service providers shall transmit a unique Nonce (Number used once) value for every service data frame encrypted with the same Control Word. Only then, the IV satisfies the requirement of the CTR mode for a unique "counter block" (IV) for each plaintext block that is ever encrypted under a given key (Federal Information Processing Standards Publication 197). If, contrary to this requirement, the "counter block" (IV) would be used repeatedly, then the confidentiality of all of the plaintext blocks corresponding to that counter block could be compromised (Federal Information Processing Standards Publication 197).

Given the 10 byte value of the Nonce, a Service Provider would be able in principle to use the same Control Word for over 10^{24} Service Data Frames, and are able to satisfy the requirement for a unique "counter block". Practical security considerations however should suggest changing the Control World much more often.

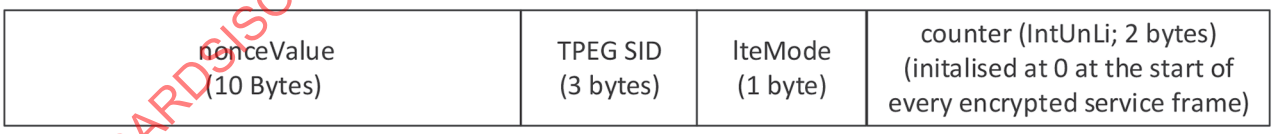

Figure 4 — Structure of Initialisation vector

In Figure 4, the structure of the 16 byte Initialisation vector is shown graphically. The parameters are detailed in 7.4.

A 2-byte counter is sufficient. A Service Frame is a maximum of 65 535 bytes, i.e. may contain maximally 4 096 cipher blocks. The counter shall be reset to 0 for every encrypted Service Frame.

6.4 Encryption and decryption of transmitted Control Words

New Control Words may be transmitted to protect the confidentiality of the payload data. To protect the transport of Control Words itself to TPEG clients, these Control Words are encrypted, with a Service Key.

For Light Encryption of Control Words, the Electronic Codebook (ECB) mode of operation is employed (NIST Special Publication 800-38A). In both Light Encryption modes 1 and 2, the transmitted Control Words are encrypted with ECB-AES128 (NIST Special Publication 800-38A).

NIST has made available ECB-AES128 test vectors in NIST Special Publication 800-38A, Appendices F1.1 and F1.2. These test vectors shall be used for validation of implementations of this document.

6.5 Service Key composition

6.5.1 General

The transmitted Control Words are encrypted with a Service Key. In Light Encryption, Service Keys are not transmitted, but rather composed of pre-shared information and a transmitted configuration parameter. That is, Service keys shall be composed based on a transmitted "mode<X>EncryptionConfiguration" parameter, the secret TISA information, and TPEG Service ID.

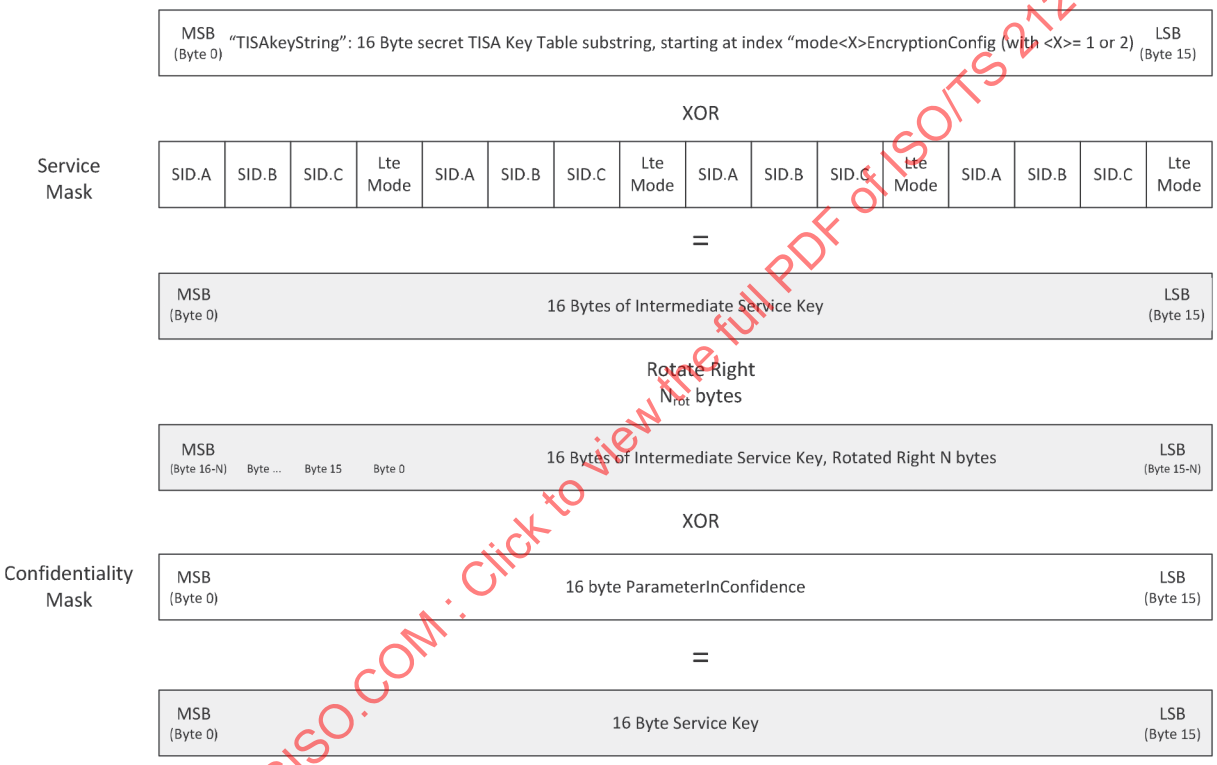

Figure 5 — Procedure for composing a Service Key, based on the secret TISA Key Table, transmitted service parameters and the ParameterInConfidence

Figure 5 shows the procedure for composing the Service Key, applicable both for Light Encryption mode 1 and mode 2.

The steps to compose a Service Key are as follows:

a) Selection of a 16 byte keystring TISAkeyString, based on the TISA KeyTable (see 6.2.1), and the transmitted parameter *lteMode<X>EncryptionConfig (where <X> equals 1 or 2)*; see 6.5.2.

b) Construction of a Service Mask; see 6.5.2.

c) Applying an exclusive OR operation between the TISAkeyString and the Service Mask, and storing the result as an Intermediate Service Key.

d) Determine the number of bytes N_{rot} to Rotate Right the Intermediate Service Key; see 6.5.2

e) Rotate Right the Intermediate Service Key N_{rot} bytes.

f) Construct the mode-specific Confidentiality Mask, see 6.5.3 for mode 1 and 6.5.4 for mode 2.

g) Applying an exclusive OR operation between the Right Rotated Intermediate Service Key and the Confidentiality Mask, and storing the result as the desired Service Key.

After step g), the Service Key is available for decrypting a transmitted, encrypted Control Word, following 6.4.

6.5.2 Light Encryption modes 1 and 2 common parameters for Service Key composition

6.5.2.1 TISAKeyString

For Light Encryption, the binary representation of the 16 byte TISAkeyString is determined as follows, using the secret TISAkeyTable (see 6.2.1) and the transmitted parameter *mode<X>EncryptionConfig*, where the <X> equals 1 or 2, for mode 1 or mode 2 respectively.

In mode 2, this *mode<X>EncryptionConfig* may be customer specific.

<KeyString<TISAkeyString**)>>**:=	: 16 byte TISA Key Table string which is the starting point for the Service Key composition.
<byte>(TISAkeyTable[*mode<X>EncryptionConfig*]),	: first byte of indexed TISA Key Table string.
<byte>(TISAkeyTable[*mode<X>EncryptionConfig + 1*]),	: second byte of indexed TISA Key Table string.
<byte>(TISAkeyTable[*mode<X>EncryptionConfig + 2*]),	: third byte of indexed TISA Key Table string
.....	: ....
<byte>(TISAkeyTable[*mode<X>EncryptionConfig + 14*]),	: fifteenth byte of indexed TISA Key Table string.
<byte>(TISAkeyTable[*mode<X>EncryptionConfig + 15*]),	: sixteenth byte of indexed TISA Key Table string

6.5.2.2 ServiceMask

For Light Encryption, the binary representation of the 16 byte Service Mask is specified as follows, using the transmitted parametersTPEG *SID* and *lteMode*:

<ServiceMask<serviceMask**)>>**:=	: Service Mask used for Service Key composition.
<ServiceIdentifier>(SID)**,**	: The TPEG Service Identifier (SID) as signalled in the header of the Service Frame.
<lte001:LightEncryptionMode> (lteMode),	: The Light Encryption Mode for this service data frame, as signalled in the Light Encryption Information component (see Figure 8).
<ServiceIdentifier>(SID),	: The TPEG Service Identifier (SID) (repeated).
<lte001:LightEncryptionMode> (lteMode),	: The Light Encryption Mode in use for this service data frame (repeated).
<ServiceIdentifier> (SID),	: The TPEG Service Identifier (SID) (repeated).

<lte001:LightEncryptionMode> (lteMode),	: The Light Encryption Mode in use for this service data frame (repeated).
<ServiceIdentifier> SID),	: The TPEG Service Identifier (SID) (repeated).
<lte001:LightEncryptionMode> (lteMode);	: The Light Encryption Mode in use for this service data frame (repeated).

6.5.2.3 N_{rot}

The parameter N_{rot}, (the number of bytes to rotate right in step 5) is determined as the lower nibble from the first byte of the TISAkeyString as follows:

N_{rot} := ((TISAkeyString[0]) & (0x0F)), (where "&" represents the bitwise AND operation).

This yields a "rotate right" value from 0 to 15 inclusive.

6.5.3 Light Encryption Mode 1 specific parameters for Service Key composition

For Light Encryption mode 1, the 16 byte Confidentiality Mask is specified as follows:

<ConfidentialityMask<mode1ConfidentialityMask**)>>**:=	: Confidentiality Mask used in mode 1 for Service Key composition.
16 *<byte>(TISAparameterInConfidence);	: The secret TISAparameterInConfidence provided by TISA together with the TISA Key Table under strict confidentiality rules (see 6.2.1).

6.5.4 Light Encryption Mode 2 specific parameters for Service Key composition

For Light Encryption mode 2, the binary representation of the 16 byte Confidentiality Mask is specified as follows:

<ConfidentialityMask<mode2ConfidentialityMask**)>>**:=	: Confidentiality Mask used in mode 2 for Service Key composition.
16 *<byte>(customerParameterInConfidence);	: The customer-specific parameterInConfidence provided by the Service Provider to the Client Manufacturer under strict confidentiality rules together with an allocated customerID.

For this mode 2, the "customerID" and the customer-specific "parameterInConfidence" shall be pre-shared between Service Provider and Client Manufacturer as part of a contract agreement. Table 3 shows example parameter values.

Table 3 — Assumed parameters for example service key composition (all values in hex)

lteMode	= 01
TPEG SID (100.100.255)	= 6464ff
TISAKeyString	= 0a1b2c3d4e5f60718293a4b5c6d7e8f9
TISAparameterInConfidence	= 00112233445566778899aabbccddeeff

6.5.5 Example Service Key Composition

Figure 6 shows an example of the construction of a service key for mode 1. Using the input parameters given in Table 3, in this figure a service key is constructed following the seven steps of 6.5.1.

In the first step, the TISAKeyString is selected as the substring of the TISA KeyTable from index *mode1EncryptionConfig* to, and including, index *mode1EncryptionConfig+15* (for example `0a1b2c3d4e5f60718293a4b5c6d7e8f9`).

NOTE This is an example value for the TISAKeyString without any relation with real TISA Key Table.

In the second step the Service Mask is constructed from the TPEG Service ID and lteMode (value `6464ff016464ff016464ff016464ff01`).

In the third step, the intermediate Service Key is formed with an XOR operation of the Service Mask and TISAKeyString (Intermediate Service Key value `6e7fd33c2a3b9f70e6f75bb4a2b317f8`).

In the fourth step, the number of bytes to be rotated right is determined to be 10, based on the lower "a" nibble in the first byte "0a" of the TISAKeyString.

In the fifth step, the Intermediate Service Key is then rotated right 10 bytes, yielding the value `9f70e6f75bb4a2b317f86e7fd33c2a3b`.

In the sixth step, the ConfidentialityMask is set for lte mode 1 to the value of the TISAparameterInConfidence (assumed value for this example `00112233445566778899aabbccddeeff`).

NOTE This is an example value only.

In the seventh step, the service key is determined with an XOR operation of the ConfidentialityMask and the right rotated Intermediate Service Key. This Service Key consequently has the value `9f61c4c41fe1c4c49f61c4c41fe1c4c4`.

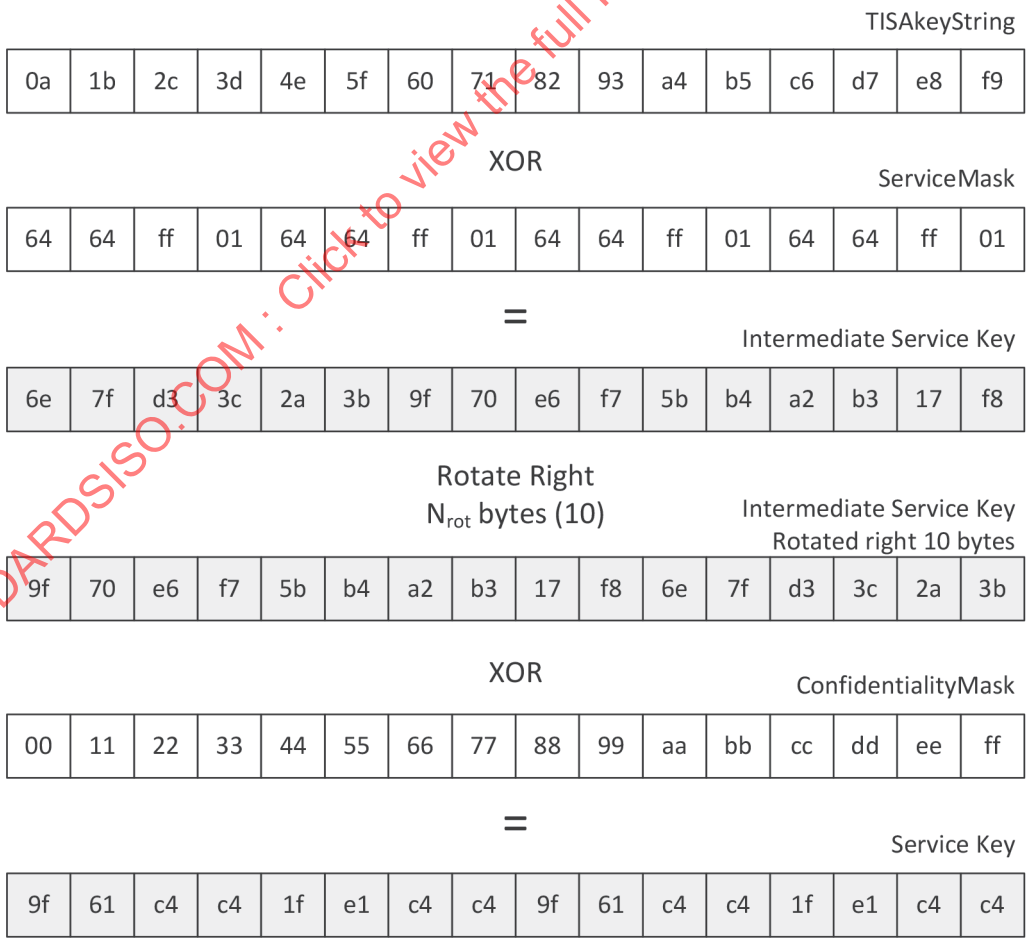

Figure 6 — Example Service Key Composition (all values in hexadecimal)

7 Light Encryption structure and embedding in TPEG service data frames

7.1 General

The chosen concept for realizing a light encryption method in a TPEG service transmission is an in-line access control/encryption method at the TPEG service data frame level. A service data frame is either completely encrypted (all content is encrypted) or clear-to-air (no encryption). This affords a single access point inside the TPEG client such that all conditional access/encryption functionality can be kept local in a client's system.

7.2 Light encryption embedding in TPEG service data frames

The Light Encryption service concept is based on in-line transmission of encryption parameters and encrypted payload as shown in Figure 7. In Figure 8, the service concept is shown with the service data frame containing an encryption indicator signalling the type of encryption used, followed by the encrypted service data frame payload. This payload contains a preamble containing the necessary encryption parameters and Control Words. This Light Encryption Information preamble is structured as an (unencrypted) TPEG2-style component (*LteInformation)*. The following CRC protects the data integrity of this component. The encrypted, and possibly compressed, service component multiplex is contained. The compression function, when used, is signalled in the Light Encryption Information preamble. After decryption, and when needed, decompression, the Service Component Frames can be accessed.

In Annex A, the TPEG binary representation of this Light Encryption service data frame structure is defined. In Annex B, the TPEG-ML representation for Light Encryption is specified.

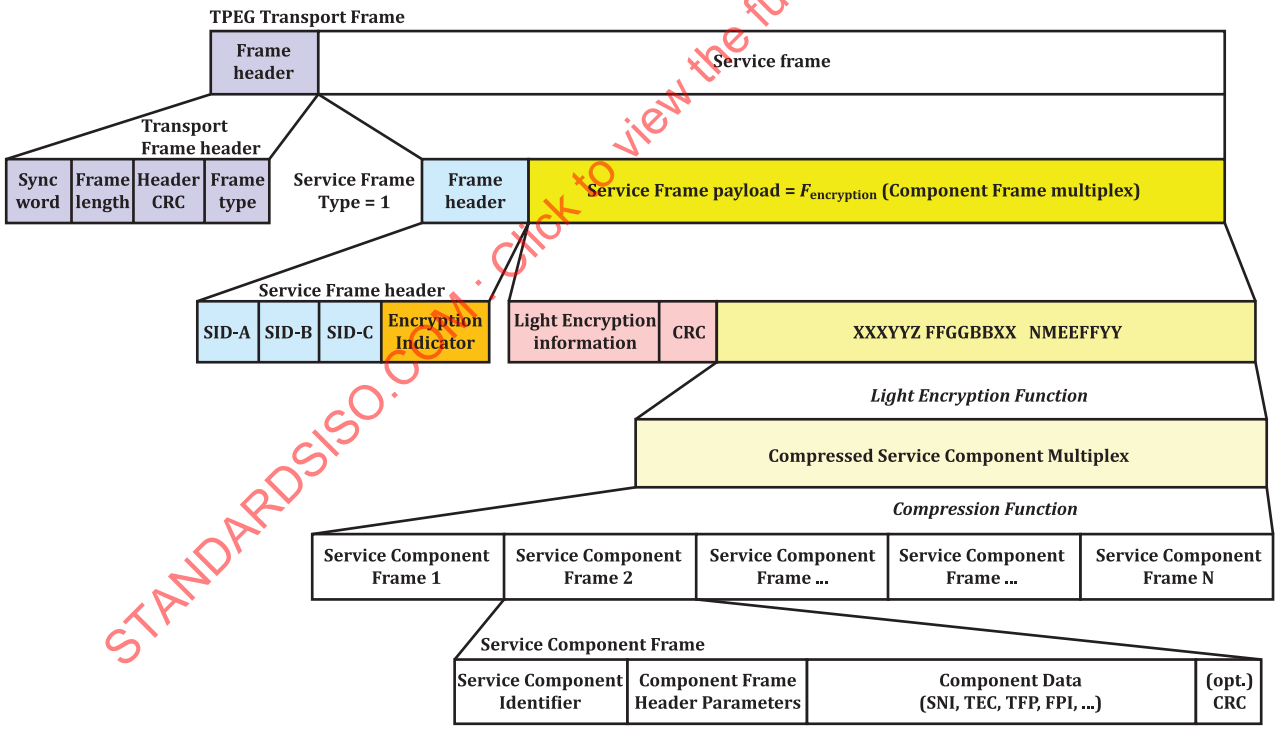

Figure 7 — Composition, compression, encryption, and framing for TPEG Light Encryption

7.3 Light Encryption components

The preamble containing all encryption information (the *LteInformation* component) is defined as a TPEG2 style component (see Figure 8). This top-level component contains the service general information, such as the version ID of the LTE specification, the encryption mode in use by the service and the payload (i.e. service component multiplex) compression method in use.

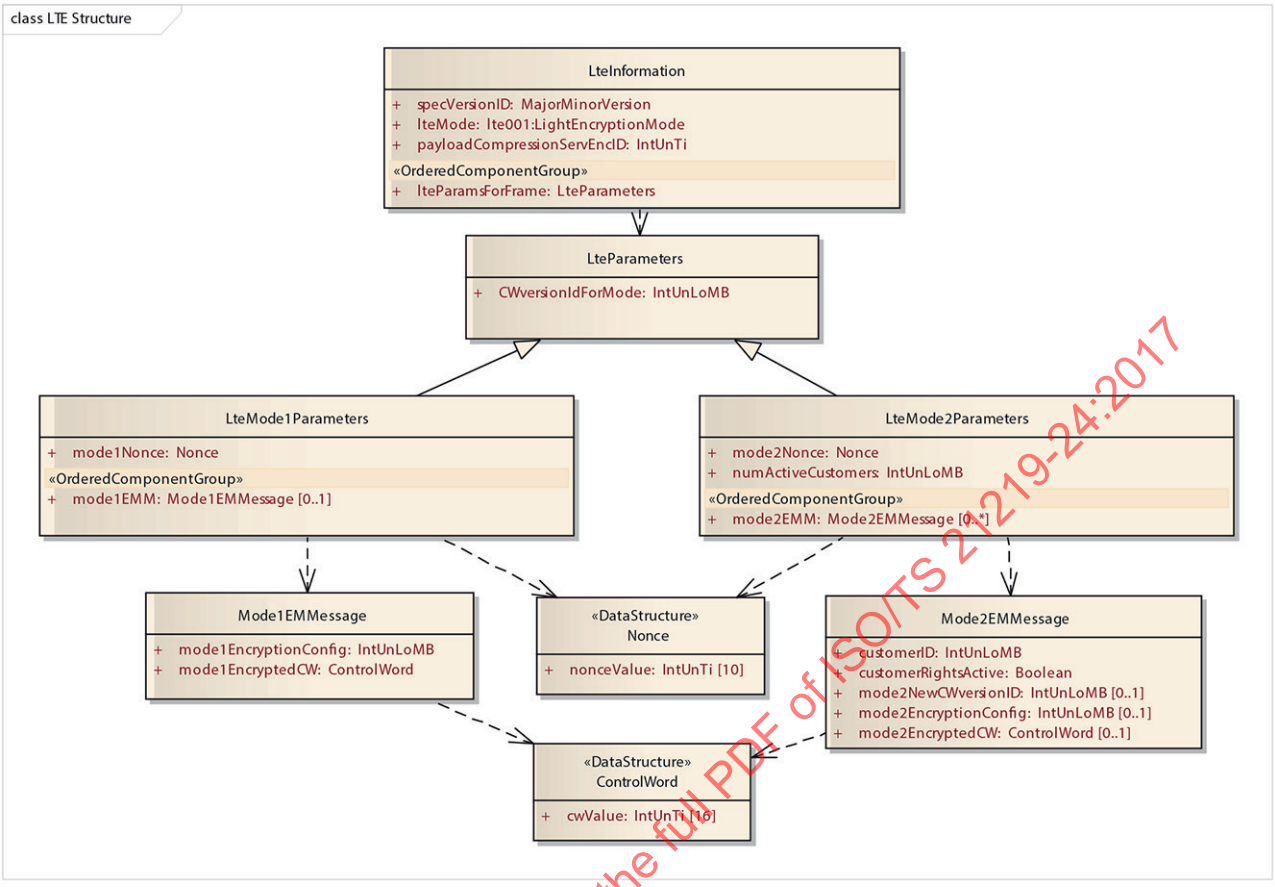

Figure 8 — LteInformation component structure

This top-level LteInformation component includes mode specific *LteParameters* components.

This document distinguishes two encryption modes, each having its own mode specific LteParameters component (see Figure 8). Common to all modes is the Control Word version ID (CWversionID).

Clients shall ascertain at all times whether they have the correct (decrypted) Control Word for a specific signalled Light Encryption Mode and Control Word Version Id (clients are expected to store the last received Control Word corresponding to the LTE Mode and Control Word ID for this purpose). Only then they may proceed to decrypt the encrypted Service Data Frame payload data. If not, they shall discard the encrypted Service Data Frame payload data.

For mode 1, a nonce ("number used once") is included as a parameter for the encryption seed (the Initialisation Vector) used in the decryption of the payload. Furthermore, a single *mode1EMMessage* for all users is included (but at the discretion of the TPEG service provider, optionally only once every few frames). This general entitlement management message contains the mode1 Encryption Configuration, specifying how the service key used for the encryption of the Control Word is computed, and the encrypted Control Word for mode 1 itself.

For mode 2, also a nonce is included as a parameter for the encryption seed used in the decryption of the payload. Also, the total number of active customers is signalled (numActiveCustomers) as a means to reliably detect whether after a change of access rights have been revoked (see C.4). Furthermore, for each customer a separate mode2EMMessage is included. This message contains the customerID, an indication whether the customer rights are active, and if so the (customer-specific) mode 2 Encryption Configuration and the (customer specific) encrypted Control Word.

In mode 2, new Control Words can be signalled in advance of their use, to enable a seamless change over in the client device. If so, in the Mode2EMMessage, the attribute "*mode2NewCWversionID*" indicates the new version of the Control Word and new configuration transmitted in the entitlement management

message. In all other cases, the mode2EMMmessage applies to the current Control Word Version ID, as signalled in the lteMode2Parameters.

7.4 LTE tables

This document contains only one table, which enumerates the applicable Encryption Modes (see Figure 9).

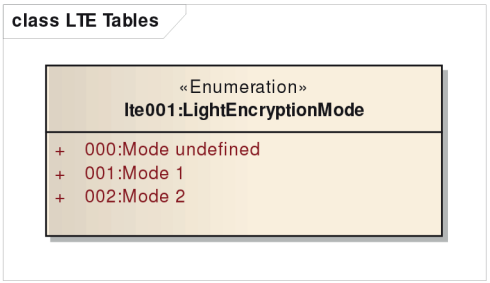

Figure 9 — LTE tables

7.5 Initialisation Vector composition

The Initalisation Vector composition is detailed in 6.3.3. Details are given here how the constituent parameters are transmitted for modes 1 and 2.

— The nonceValue shall be transmitted in the data structure "mode1Nonce" (for mode 1), or alternatively in data structure "mode2Nonce" (for mode 2). For both modes 1 and 2, the nonceValue inside this data structure contains exactly 10 bytes. This nonceValue shall be used in the composition of the initialisation vector.

— The TPEG "SID" is transmitted in the Service Frame Header (see Figure 7).

— The "lteMode" parameter is signaled in the LteInformation component (see Figure 8).

— The 2-byte IntUnLi counter is not transmitted, but rather reset to 0 at the start of every encrypted Service Data Frame. Then, following the CTR-AES128 function (NIST Special Publication 800-38A), this counter shall be incremented by 1 for decryption of every subsequent cipher text block as contained the Service Data Frame payload data.

NOTE In accordance with the TPEG UML to binary conversion rules in ISO/TS 21219-3 (TPEG2-UBCR), in the binary format of the Nonce data structure, the nonceValue array is signalled first with a IntUnLoMB array length indicator, and then the nonceValue IntUnTi array itself (see Annex A). The same applies for the ControlWord data structure.

7.6 Service Key composition

The Service Key composition is detailed in 6.5. Details are given on how the constituent parameters are transmitted for modes 1 and 2.

— The TPEG "SID" is transmitted in the Service Frame Header (see Figure 7).

— The "lteMode" parameter is signalled in the *LteInformation* component (see Figure 8).

— The "mode1EncryptionConfig" (for mode 1) or alternatively "mode2EncryptionConfig" parameter (for mode 2) is signaled in the *mode1EMMessage* or *mode2EMMmessage* respectively (see Figure 8).

— The secret TISA KeyTable and TISAparameterInConfidence (for mode 1) need to be obtained from TISA (see 6.2.1). For mode 2, the customer specific parameterInConfidence need to be obtained from the service providers.

8 LTE components

8.1 LteInformation

Table 4 shows the root, TPEG2-compliant component for Light Encryption Information to be included in the Service Data Frame in front of the encrypted Service Component Multiplex.

Table 4 — LteInformation

Name	Type	Multiplicity	Description
specVersionID	MajorMinorVersion	1	Major and Minor version of the Light Encryption specification as used to encrypt (and possibly compress) the service component multiplex.
lteMode	lte001:LightEncryptionMode	1	Active Encryption Mode in used by service provider for this service. The encryption mode in use may change over time for the service, but after every changeover of encryption mode, all frames shall use the same encryption mode until a next changeover of the encryption mode.
payloadCompressionServEncID	IntUnTi	1	Indicator for the compression method which is used for compressing the payload Service Component Multiplex, i.e. before encryption is applied. Valid values for this attribute are those TPEG Service Encryption Indicators indicating solely a compression method. The chosen compression method is applied to the complete Service Component Multiplex before encryption. Note: Range 0 to 127 refers to the TISA standard Service Encryption Indicators. Range 128 to 255 values may be freely chosen by Service Providers. Multiple service providers may use the same value in this range for different methods.
Ordered Components			
lteParamsForFrame	LteParameters	1	Mode specific Light Encryption parameters for this Service Data Frame.

8.2 LteParameters

Table 5 shows the abstract class for Light Encryption Parameters. Each mode specific Light Encryption Parameters class shall be derived from this abstract class.

Table 5 — LteParameters

Name	Type	Multiplicity	Description
CWversionIdForMode	IntUnLoMB	1	The current (mode specific) version of the Control World used for encryption of this frame. Control Words may be changed infrequently. Clients shall remember the last transmitted Control World per supported mode such that the (encrypted) Control Word does not need to be transmitted in every frame. The CWversionIdForMode is a monotonic increasing number per LTE mode.

8.3 LteMode1Parameters

Table 6 shows the Light Encryption Parameters for Encryption Mode 1.

Table 6 — LteMode1Parameters

Name	Type	Multiplicity	Description
CWversionIdForMode	IntUnLoMB	1	The current (mode specific) version of the Control World used for encryption of this frame. Control Words may be changed infrequently. Clients shall remember the last transmitted Control World per supported mode such that the (encrypted) Control Word does not need to be transmitted in every frame. The CWversionIdForMode is a monotonic increasing number per LTE mode.
mode1Nonce	Nonce	1	Nonce for use in the Initialisation Vector (IV) of mode 1.
Ordered Components			
mode1EMM	Mode1EMMessage	0..1	General mode 1 entitlement information for all clients.

8.4 LteMode2Parameters

Table 7 shows Light Encryption Parameters for Encryption Mode 2.

Table 7 — LteMode2Parameters

Name	Type	Multiplicity	Description
CWversionIdForMode	IntUnLoMB	1	The current (mode specific) version of the Control World used for encryption of this frame. Control Words may be changed infrequently. Clients shall remember the last transmitted Control World per supported mode such that the (encrypted) Control Word does not need to be transmitted in every frame. The CWversionIdForMode is a monotonic increasing number per LTE mode.
mode2Nonce	Nonce	1	Nonce for use in the Initialisation Vector (IV) of mode 2.
numActiveCustomers	IntUnLoMB	1	Total number of customers with active access rights to the LTE mode 2 service for the current Control Word version ID. TPEG clients are able to check with this parameter whether they have seen all customerIDs which still have access rights to the service, when inspecting successive frames encrypted with LTE mode 2. If in this list the expected customerID is not present, then the client knows that its service access right has been revoked.
Ordered Components			
mode2EMM	Mode2EMMessage	0..*	Customer Specific Entitlement Information for various customers.

8.5 Mode1EMMessage

Table 8 shows the Entitlement Management Message for Mode 1 Light Encryption.

Table 8 — Mode1EMMessage

Name	Type	Multiplicity	Description
mode1EncryptionConfig	IntUnLoMB	1	Index into the secret TISA Service Key Table to indicate the service encryption configuration used for Mode 1 in this Service. The service encryption configuration for mode 1 shall change only with a Control Word version ID change for mode 1, or after a switch from LTE mode 2 to LTE mode 1.
mode1EncryptedCW	ControlWord	1	Control Word for mode 1 encrypted according to attribute mode1EncryptionConfig.

8.6 Mode2EMMessage

Table 9 defines the Customer Specific Entitlement Management Message for Mode 2 Light Encryption for either the mode2NewCWversionID if explicitly signalled, or, if not signalled, the current CWversionIDForMode for this mode as signalled in the Light Encryption parameters for this frame.

Table 9 — Mode2EMMessage

Name	Type	Multiplicity	Description
customerID	IntUnLoMB	1	Customer ID as allocated by the Service Provider responsible for this encrypted service.
customerRightsActive	Boolean	1	Boolean indicating whether customer rights are active (True) or revoked (False) for this service.
mode2NewCWversionID	IntUnLoMB	0..1	The new version of the Control World for which this Customer Specific Control Word Information is given. This attribute is signalled in case information for a new Control Word is transmitted in advance of the actual change of the Control Word in the transmission. Advanced clients may store this advance information to speed up change over. If not provided, the current Control Word version ID (as signalled in the Mode2LightEncryptionParameters) applies to this Mode2EntitlementMessage.
mode2EncryptionConfig	IntUnLoMB	0..1	Customer specific index into the secret TISA Service Key Table to indicate the service encryption configuration used for mode 2 in this service, for this customer. This attribute shall be signalled only if customer rights are (still) active. When in the Mode2EMMessage the attribute mode-2NewCWversionId is included, this service encryption configuration is signalled in advance, and corresponds to the mode2NewCWversionID version (not the current version in use). This customer specific service encryption configuration for mode 2 shall change only with a Control Word Version ID change for mode 2, or after a switch from LTE mode 1 to LTE mode 2.
mode2EncryptedCW	ControlWord	0..1	Control Word for this customer, which is encrypted according to attribute mode2EncryptionConfig. This attribute shall be signalled only if customer rights are (still) active. When in the Mode2EMMessage the attribute mode2NewCWversionId is included, this Control Word is signalled in advance, and corresponds to the mode2NewCWversionID version (not the current version in use).

9 LTE Datatypes

9.1 ControlWord

Table 10 shows the data structure for a 16 byte Control Word.

Table 10 — ControlWord

Name	Type	Multiplicity	Description
cwValue	IntUnTi	16..16	16 byte value of the Control Word

9.2 Nonce

Table 11 shows the data structure for a 10 byte nonce. A NONCE is a Number used ONCE. For modes 1 and 2, a nonce is used in the Initialisation Vector (IV).

Table 11 — ControlWord

Name	Type	Multiplicity	Description
nonceValue	IntUnTi	10..10	10 byte value of the nonce.

10 LTE Tables

10.1 lte001:LightEncryptionMode

Table 12 enumerates the applicable modes for Light Encryption.

Table 12 — LightEncryptionMode

Code	Reference-English 'word'	Comment	Example
000	Mode undefined		
001	Mode 1	Light Encryption Mode 1. This mode is used for encrypted, but otherwise unrestricted, access service provisioning.	
002	Mode 2	Light Encryption Mode 2. This mode is used for encrypted and access controlled service provisioning.	

Annex A
(normative)

TPEG application, TPEG-Binary Representation

A.1 General

In this annex, the TPEG-Binary representation for Light Encryption is specified. The Service Data Frame contents when applying Light Encryption mode 1 or 2 are specified, and the specific (sub) components for the LteInformation component as contained in the Service Data Frame are given.

A.2 Service Frame of frame type = 1 (Service Data Frame) with Light Encryption mode 1 or 2 applied

A.2.1 Service Frame Specification

A TPEG Service Data Frame may contain a different range and number of Service Component Frames as required by the service provider. Furthermore, each Service Data Frame shall include service information that comprises the service identification elements and the service encryption indicator. The general concept and specification of the TPEG service data frame is contained in the TPEG2 Service Framework ISO/TS 21219-5.

The service encryption indicator signals the encryption method in use (in this document, the logical value *LteServEncID* is used to identify Light Encryption).

For Light Encryption, the Service Encryption Indicator in the Service Data Frame shall contain the appropriate value *LteServEncID*. Then for the two modes as specified in this document, the Service Data Frame definition is specialized as follows.

<ServiceData<ServiceFrame(1)>>:=	: Service data frame
<ServiceIdentifier>(SID),	: Service identification (SID-A, SID-B, SID-C)
<IntUnTi>(ServEncID),	: Service encryption indicator, 0 = no encryption, the logical value LteServEncID indicates use of Light Encryption
*LightEncryptionFunctionMode1and2***(<ServCompMultiplex>);**	: With ServEncID==LteServEncID, encryption function *LightEncryptionFunctionMode1and2* is utilized for encryption of the Service Component Multiplex

This document distinguishes two modes of operation. For encryption of the Service Component Multiplex, however, this function *LightEncryptionFunctionMode1and2* yields the same structure and internal functions as follows:

*LightEncryptionFunctionMode1and2***<ServCompMultiplex)>>**:=	:
<LightEncryptionInformation>(lightEncryptionInformation),	: LightEncryptionInformation component
<CRC>(lteInfoCRC),	: CRC of lightEnryptionInformation component,
CTR-AES128 **(***compressionFunction***<ServCompMultiplex>));**	: CTR-AES128 encryption of the (possibly compressed) Service Component Multiplex. The compression function as used is signalled in the LightEncryptionInformation component.

A.2.2 Attributes

ServiceFrame attributes are specified in the TPEG2 Service Framework specification ISO/TS 21219-5 (TPEG2-SFW). Here, only those attributes/functions are specified which are specific to this Light Encryption mechanism.

lteInfoCRC

The lteInfoCRC attribute enables an error detection of the LightEncryptionInformation component.

This CRC shall be two bytes long, and shall be based on the ITU-T polynomial $x^{16} + x^{12} + x^5 + 1$.

Calculation of the CRC is specified in the TPEG2 Service Framework ISO/TS 21219-5, Annex D. The calculation of this CRC shall be done on the complete LteInformation component, including component ID, component length and attribute length fields.

When a CRC mismatch is detected, the integrity of the LightEncryptionInformation cannot be guaranteed, therefore the entire service frame shall be discarded by a receiver.

CTR-AES128

The CTR-AES128 function is specified by NIST in NIST Special Publication 800-38A.

compressionFunction

The compressionFunction is used as signal in the LightEncryptionInformation component, attribute payloadCompressionServEncID. An attribute value of 0 indicates absence of compression.

A.3 Message components

A.3.1 List of Generic Component IDs

Table A.1 defines the Generic Component IDs for use in the TPEG binary representation

Table A.1 — Generic Component IDs

Name	Id
LteInformation	0
LteMode1Parameters	1
LteMode2Parameters	2
Mode1EMMessage	101
Mode2EMMessage	102

A.3.2 LteInformation

<LteInformation(0)>:=	
<IntUnTi>(0),	: id of this component
<IntUnLoMB>(lengthComp),	: number of bytes in component
<IntUnLoMB>(lengthAttr),	: number of bytes in attributes
<MajorMinorVersion>(specVersionID),	: Major and Minor version of the Light Encryption specification as used to encrypt (and possibly compress) the service component multiplex.
<lte001:LightEncryptionMode>(lteMode),	: Active Encryption Mode is used by service provider for this service. The encryption mode in use may change over time for the service, but after every changeover of encryption mode, all frames shall use the same encryption mode until a next changeover of the encryption mode.
<IntUnTi>(payloadCompressionServEncID),	: Indicator for the compression method which is used for compressing the payload Service Component Multiplex, i.e. before encryption is applied. Valid values for this attribute are those TPEG Service Encryption Indicators indicating solely a compression method. The chosen compression method is applied to the complete Service Component Multiplex before encryption. Note: Range 0 to 127 refers to the TISA standard Service Encryption Indicators. Range 128 to 255 values may be freely chosen by Service Providers. Multiple service providers may use the same value in this range for different methods.
ordered {	
<LteParameters>(lteParamsForFrame)	: Mode specific light encryption parameters for this Service Data Frame.
};	

A.3.3 LteParameters

<LteParameters(x)>:=	
<IntUnTi>(x),	: id of this component
<IntUnLoMB>(lengthComp),	: number of bytes in component
<IntUnLoMB>(lengthAttr),	: number of bytes in attributes
<IntUnLoMB>(CWversionIdForMode);	: The current (mode specific) version of the Control Word used for encryption of this frame. Control Words may be changed infrequently. Clients shall remember the last transmitted Control Word per supported mode such that the (encrypted) Control Word does not need to be transmitted in every frame. The CWversionIdForMode is a monotonic increasing number per LTE mode.

A.3.4 LteMode1Parameters

<LteMode1Parameters(1)<LteParameters(1)>>:=	
<IntUnTi>(1),	: id of this component
<IntUnLoMB>(lengthComp),	: number of bytes in component
<IntUnLoMB>(lengthAttr),	: number of bytes in attributes
<IntUnLoMB>(CWversionIdForMode);	: The current (mode specific) version of the Control Word used for encryption of this frame. Control Words may be changed infrequently. Clients shall remember the last transmitted Control Word per supported mode such that the (encrypted) Control Word does not need to be transmitted in every frame. The CWversionIdForMode is a monotonic increasing number per LTE mode.
<Nonce>(mode1Nonce),	: Nonce for use in the Initialisation Vector (IV) of mode 1.
ordered {	
n *<Mode1EMMessage>(mode1EMM)[0..1]	: General mode 1 entitlement information for all clients.
};	

A.3.5 LteMode2Parameters

<LteMode2Parameters(2)<LteParameters(2)>>:=	
<IntUnTi>(2),	: id of this component
<IntUnLoMB>(lengthComp),	: number of bytes in component
<IntUnLoMB>(lengthAttr),	: number of bytes in attributes
<IntUnLoMB>(CWversionIdForMode);	: The current (mode specific) version of the Control Word used for encryption of this Frame. Control Words may be changed infrequently. Clients shall remember the last transmitted Control Word per supported mode such that the (encrypted) Control Word does not need to be transmitted in every frame. The CWversionIdForMode is a monotonic increasing number per LTE mode.
<Nonce>(mode2Nonce),	: Nonce for use in the Initialisation Vector (IV) of mode 2.
<IntUnLoMB>numActiveCustomers),	: Total number of customers with active access rights to the LTE mode 2 service for the current Control Word version ID. TPEG clients are able to check with this parameter whether they have seen all customerIDs which still have access rights to the service, when inspecting successive frames encrypted with LTE mode 2. If in this list the expected customerID is not present, then the client knows that its service access right has been revoked.

ordered {	
n *<Mode2EMMessage>(mode2EMM)	: Customer Specific Entitlement Information for various customers.
};	

A.3.6 Mode1EMMessage

<Mode1EMMessage(101)>:=	
<IntUnTi>(101),	: id of this component
<IntUnLoMB>(lengthComp),	: number of bytes in component
<IntUnLoMB>(lengthAttr),	: number of bytes in attributes
<IntUnLoMB>(mode1EncryptionConfig),	: Index into the secret TISA Service Key Table to indicate the service encryption configuration used for mode 1 in this Service. The service encryption configuration for mode 1 may change only with a Control Word version ID change for mode 1, or after a switch from LTE mode 2 to LTE mode 1.
<ControlWord>(mode1EncryptedCW);	: Control Word for mode 1 encrypted according to attribute mode1EncryptionConfig.

A.3.7 Mode2EMMessage

<Mode2EMMessage(102)>:=	
<IntUnTi>(102),	: id of this component
<IntUnLoMB>(lengthComp),	: number of bytes in component
<IntUnLoMB> lengthAttr),	: number of bytes in attributes
<IntUnLoMB>(customerID),	: Customer ID as allocated by the Service Provider responsible for this encrypted service.
BitArray(selector),	
if (bit 0 of selector is set)	
<Boolean>(customerRightsActive),	: Boolean indicating whether customer rights are active (True) or revoked (False) for this service.
if (bit 1 of selector is set)	
<IntUnLoMB>(mode2NewCWversionID),	: The new version of the Control Word for which this Customer Specific Control Word Information is given. This attribute is signalled in case information for a new Control Word is transmitted in advance of the actual change of the Control Word in transmission. Advanced clients may store this advance information to speed up changeover. If not provided, the current Control Word version ID (as signalled in the Mode2LightEncyptionParameters) applies to this Mode2EntittlementMessage.
if (bit 2 of selector is set)	