

ISO/TS 21219-24:2017-02 (E)

Intelligent transport systems - Traffic and travel information (TTI) via transport protocol experts group, generation 2 (TPEG2) - Part 24: Light encryption (TPEG2-LTE)

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	3
5	Light Encryption specific constraints	4
5.1	Version number signalling	4
5.2	Extendibility	4
5.3	Endianness	4
5.4	Supported business models	4
5.5	Performance requirements	5
5.5.1	Repetition rate of light encryption parameters	5
5.5.2	Update rate of light encryption parameters	5
5.6	License agreement and security requirements	5
5.6.1	General	5
5.6.2	Security requirements on service providers	6
5.6.3	Security requirements on client manufacturers	6
6	Light encryption method of encryption and operation	6
6.1	Principles of operation for light encryption	6
6.2	Overview of the light encryption method	7
6.2.1	General	7
6.2.2	TISA secret KeyTable and TISAp parameterInConfidence	8
6.3	Encryption and decryption of service data frame payload data	9
6.3.1	General	9
6.3.2	Block cipher mode of operation	9
6.3.3	Initialisation Vector	11
6.4	Encryption and decryption of transmitted Control Words	11
6.5	Service Key composition	12
6.5.1	General	12
6.5.2	Light Encryption modes 1 and 2 common parameters for Service Key composition	13
6.5.3	Light Encryption Mode 1 specific parameters for Service Key composition	14
6.5.4	Light Encryption Mode 2 specific parameters for Service Key composition	14
6.5.5	Example Service Key Composition	14
7	Light Encryption structure and embedding in TPEG service data frames	16
7.1	General	16
7.2	Light encryption embedding in TPEG service data frames	16
7.3	Light Encryption components	16
7.4	LTE tables	18
7.5	Initialisation Vector composition	18
7.6	Service Key composition	18

8	LTE components	19
8.1	LteInformation	19
8.2	LteParameters	19
8.3	LteMode1Parameters	20
8.4	LteMode2Parameters	20
8.5	Mode1EMMessage	21
8.6	Mode2EMMessage	21
9	LTE Datatypes	22
9.1	ControlWord	22
9.2	Nonce	22
10	LTE Tables	23
10.1	lte001:LightEncryptionMode	23
Annex A (normative) TPEG application, TPEG-Binary Representation		24
Annex B (normative) TPEG application, TPEG-ML Representation		30
Annex C (informative) Light Encryption Guidelines		33