

# 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)

---

<b>Contents</b>		<b>Page</b>
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

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