

ISO/IEC 23001-7:2016-02 (E)

Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms, definitions, and abbreviated terms	1
3.1	Terms and definitions	1
3.2	Abbreviated terms	2
4	Protection schemes	3
4.1	Scheme type signaling	3
4.2	Common encryption scheme types	3
5	Overview of encryption metadata	3
6	Encryption parameters shared by groups of samples	3
7	Common encryption sample auxiliary information	5
7.1	Definition	5
7.2	Sample Encryption Information box for storage of sample auxiliary information	6
7.2.1	Sample Encryption Box ('senc')	6
7.2.2	Syntax	6
7.2.3	Semantics	6
8	Box definitions	7
8.1	Protection system specific header box	7
8.1.1	Definition	7
8.1.2	Syntax	7
8.1.3	Semantics	8
8.2	Track Encryption box	8
8.2.1	Definition	8
8.2.2	Syntax	8
8.2.3	Semantics	9
9	Encryption of media data	9
9.1	Field semantics	9
9.2	Initialization Vectors	10
9.3	AES-CTR mode counter operation	11
9.4	Full sample encryption	12
9.4.1	General	12
9.4.2	Full sample encryption using AES-CTR mode	12
9.4.3	Full sample encryption using AES-CBC mode	12
9.5	Subsample encryption	13
9.5.1	Definition (normative)	13
9.5.2	Subsample encryption of NAL Structured Video tracks	14
9.6	Pattern encryption	18
9.6.1	Definition	18
9.6.2	Example of pattern encryption applied to a video NAL unit	19

9.7	Whole-block full sample encryption	19
10	Protection scheme definitions	19
10.1	`cenc' AES-CTR scheme	19
10.2	`cbc1' AES-CBC scheme	20
10.3	`cens' AES-CTR subsample pattern encryption scheme	20
10.4	`cbcs' AES-CBC subsample pattern encryption scheme	21
10.4.1	Definition	21
10.4.2	`cbcs' AES-CBC mode pattern encryption scheme application (informative)	22
11	XML representation of Common Encryption parameters	22
11.1	General	22
11.2	Definition of the XML cenc:default_KID attribute and cenc:pssh element	22
11.3	Use of the cenc:default_KID attribute and cenc:pssh element in DASH ContentProtection Descriptor elements	23
11.3.1	General	23
11.3.2	Addition of cenc:default_KID attributes in DASH ContentProtection Descriptors	23
11.3.3	Addition of the cenc:pssh element in Protection System Specific UUID ContentProtection Descriptors	24
11.3.4	Example of two Content Protection Descriptors in an MPD	24
	Bibliography	26