# ISO/IEC 23001-7:2023-08 (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 ..... 2
3.1 Terms and definitions ..... 2
3.2 Abbreviated terms ..... 3

4 Protection schemes ..... 3
4.1 Scheme type signalling ..... 3
4.2 Common encryption scheme types ..... 4

5 Overview of encryption metadata ..... 4

6 Encryption parameters shared by groups of samples ..... 4

7 Common encryption sample auxiliary information ..... 6
7.1 Definition ..... 6
7.2 Sample encryption information box for storage of sample auxiliary information ..... 7
7.2.1 Sample encryption box -- Definition ..... 7
7.2.2 Syntax ..... 8
7.2.3 Semantics ..... 8

8 Box definitions ..... 9
8.1 Protection system specific header box ..... 9
8.1.1 Definition ..... 9
8.1.2 Syntax ..... 10
8.1.3 Semantics ..... 10
8.2 Track Encryption box ..... 10
8.2.1 Definition ..... 10
8.2.2 Syntax ..... 11
8.2.3 Semantics ..... 11
8.3 Item encryption box ..... 11
8.3.1 Definition ..... 11
8.3.2 Syntax ..... 12
8.3.3 Semantics ..... 12
8.4 Item auxiliary information box ..... 13
8.4.1 Definition ..... 13
8.4.2 Syntax ..... 13
8.4.3 Semantics ..... 13

9 Encryption of media data ..... 14
9.1 Field semantics ..... 14
9.2 Initialization vectors ..... 15
9.3 AES-CTR mode counter operation ..... 16
9.4 Full sample encryption ..... 16
9.4.1 General ..... 16

9.4.2 Full sample encryption using AES-CTR mode ..... 16
9.4.3 Full sample encryption using AES-CBC mode ..... 17
9.5 Subsample encryption ..... 17
9.5.1 Definition ..... 17
9.5.2 Subsample encryption of NAL structured video tracks ..... 18
9.6 Pattern encryption ..... 23
9.6.1 Definition ..... 23
9.6.2 Example of pattern encryption applied to a video NAL unit ..... 24
9.7 Whole-block full sample encryption ..... 24
9.8 Content sensitive encryption ..... 24
9.8.1 Definition ..... 24
9.8.2 Content sensitive encryption applied to a video NAL unit ..... 25

10 Protection scheme definitions ..... 26
10.1 'cenc' AES-CTR scheme ..... 26
10.2 'cbc1' AES-CBC scheme ..... 26
10.3 'cens' AES-CTR subsample pattern encryption scheme ..... 27
10.4 'cbcs' AES-CBC subsample pattern encryption scheme ..... 27
10.4.1 Definition ..... 27
10.4.2 'cbcs' AES-CBC mode pattern encryption scheme application ..... 28
10.5 'sve1' AES-CTR sensitive encryption scheme ..... 29

11 XML representation of Common Encryption parameters ..... 29
11.1 General ..... 29
11.2 Definition of the XML cenc:default_KID attribute and cenc:pssh element ..... 29
11.3 Use of the cenc:default_KID attribute and cenc:pssh element in DASH ContentProtection Descriptor elements ..... 30
11.3.1 General ..... 30
11.3.2 Addition of cenc:default_KID attributes in DASH ContentProtection Descriptors ..... 30
11.3.3 Addition of the cenc:pssh element in Protection System Specific UUID ContentProtection Descriptors ..... 31
11.3.4 Example of two Content Protection Descriptors in an MPD ..... 31

Annex A (normative) Content sensitive encryption scheme ..... 33

Bibliography ..... 42