ISO/IEC 23001-7:2015-04 (E)

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

Contents

Page

Foreword iv

Introduction v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Abbreviated terms 2

5 Scheme Signaling 2

6 Overview of Encryption Metadata 2

7 Encryption Parameters shared by groups of samples 3

8 Common Encryption Sample Auxiliary Information 4
8.1 Sample Encryption Information Box for Storage of Sample Auxiliary Information 4
8.1.1 Sample Encryption Box (`senc') 4
8.1.2 Syntax 5

9 Box Definitions 5
9.1 Protection System Specific Header Box 5
9.1.1 Definition 5
9.1.2 Syntax 6
9.1.3 Semantics 6
9.2 Track Encryption Box 7
9.2.1 Definition 7
9.2.2 Syntax 7
9.2.3 Semantics 7

10 Encryption of Media Data 7
10.1 Encryption Schemes 7
10.2 Field semantics 8
10.3 Initialization Vectors 9
10.4 Counter Operation 9
10.5 Full Sample Encryption 9
10.6 Subsample Encryption 10
10.6.1 Definition 10
10.6.2 Encryption of NAL Structured Video Tracks 11

11 AES 128-bit Cipher Block Chaining (CBC-128) Encryption of Media Data 12
11.1 Introduction to AES 128-bit Cipher-Block Chaining (CBC-128) Mode 12
11.2 AES-CBC-128 Mode 13
11.2.1 Field Semantics for AES-CBC-128 Mode 13
11.2.2 Creation of Initialization Vectors (Informative) 13
11.2.3 AES-CBC-128 Mode Encryption of NAL Structured Video Tracks 13
11.2.4 Full Encryption in AES-CBC-128 Mode 13

12 XML Representation of Common Encryption Parameters 14
12.1 Definition of the XML cenc:default_KID attribute and cenc:pssh element 14
12.2 Use of the cenc:default_KID attribute and cenc:pssh element in DASH ContentProtection Descriptor Elements 15
12.2.1 Addition of cenc:default_KID attributes in DASH ContentProtection Descriptors15 12.2.2 Addition of the cenc:pssh element in protection system specific UUID Content Protection Descriptors 16
12.2.3 Example showing two Content Protection Descriptors included in an MPD 16

Bibliography 17