ISO/IEC 23009-4:2018 (E)

Information technology — Dynamic adaptive streaming over HTTP (DASH) — Part 4: Segment encryption and authentication

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms, definitions, abbreviated terms and notations

3.1 Terms and definitions
3.2 Abbreviated terms
3.3 Notations

4 Segment encryption and authentication

4.1 Segment encryption
4.2 Segment authentication
4.3 MPD security

5 Signalling encryption and authentication

5.1 Encryption declaration
5.1.1 ContentProtection element
5.1.1.1 Definition
5.1.1.2 Semantics
5.1.1.3 Service protection
5.1.2 SegmentEncryption element
5.1.3 Licence element
5.1.4 Common cryptoperiod properties
5.1.4.1 Definition
5.1.4.2 Semantics
5.1.5 CryptoPeriod element
5.1.5.1 Definition
5.1.5.2 Semantics
5.1.6 CryptoTimeline element
5.1.6.1 Definition
5.1.6.2 Semantics
5.2 Authentication declaration
5.2.1 General
5.2.2 ContentAuthenticity element
5.2.2.1 Definition
5.2.2.2 Semantics
5.2.3 URL derivation

6 Segment encryption

6.1 Segment format
6.2 Key systems
6.2.1 General
6.2.2 Licence-based key systems
6.3 Encryption systems
6.3.1 General
6.3.2 AES-128 CBC encryption system
6.3.3 AES-128 GCM encryption system
6.3.4 Common encryption system
6.4 Cryptoperiods

6.4.1 General
6.4.2 Assigning segments to cryptoperiods
6.4.3 Key derivation
6.4.3.1 General
6.4.3.2 Key format
6.4.4 IV derivation
6.4.4.1 General
6.4.4.2 IV derivation from segment number
6.4.4.3 IV format
6.4.5 AAD derivation
6.5 Adding new encryption and key systems

7 Segment authentication

7.1 General
7.2 Algorithms
7.2.1 SHA-256
7.2.2 HMAC-SHA1

Annex A (normative) XML schema

Annex B (informative) Implementation guidelines

B.1 Key delivery
B.2 Encryption
B.3 Content authenticity

Annex C (informative) MPD examples and usage

C.1 Video-on-demand
C.2 Live event with key rotation and authentication
C.3 Use of arbitrary ISO-BMFF content protection with content authentication
C.4 Use of licence-based key transport

Page count: 29