

ISO/IEC 23009-4:2013-07 (E)

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

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Definitions	2
3.1	Terms and definitions	2
3.2	Abbreviated terms	2
3.3	Notation	3
4	Introduction	3
4.1	Segment Encryption	3
4.2	Segment Authentication	4
4.3	MPD security	5
5	Signalling encryption and authentication	5
5.1	Encryption declaration	5
5.1.1	ContentProtection element	5
5.1.2	SegmentEncryption element	6
5.1.3	License element	7
5.1.4	Common cryptoperiod properties	7
5.1.5	CryptoPeriod element	8
5.1.6	CryptoTimeline element	9
5.2	Authentication declaration	10
5.2.1	General	10
5.2.2	ContentAuthenticity element	11
5.2.3	URL derivation	11
6	Segment encryption	12
6.1	Segment Format	12
6.2	Key systems	12
6.2.1	General	12
6.2.2	License-based Key Systems	12
6.3	Encryption systems	12
6.3.1	General	12
6.3.2	AES-128 CBC Encryption System	13
6.3.3	AES-128 GCM Encryption System	13
6.4	Cryptoperiods	13
6.4.1	General	13
6.4.2	Assigning segments to cryptoperiods	13
6.4.3	Key derivation	14
6.4.4	IV derivation	15
6.4.5	AAD derivation	16
6.5	Adding new encryption and key systems	16
7	Segment authentication	16
7.1	General	16
7.2	Algorithms	16

7.2.1	SHA-256	16
7.2.2	HMAC-SHA1	16
Annex A (normative) XML Schema		17
Annex B (informative) Implementation Guidelines		19
B.1	Key Delivery	19
B.2	Encryption	19
B.3	Content Authenticity	19
Annex C (informative) MPD Examples and Usage		20
C.1	Video on Demand	20
C.2	Live Event with Key Rotation and Authentication	21
C.3	Use of Arbitrary ISO-BMFF Content Protection with Content Authentication	22
C.4	Use of License-based Key Transport	24