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

*Technologies de l'information — Diffusion en flux adaptatif dynamique
sur HTTP (DASH) —*

Partie 4: Cryptage et authentification des segments

Withhold & NDA

Withdrawn



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2013

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

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

This is a preview - [click here to buy the full publication](#)

- B.1 Key Delivery19
- B.2 Encryption19
- B.3 Content Authenticity.....19
- Annex C (informative) MPD Examples and Usage20
- 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 Authentication22
- C.4 Use of License-based Key Transport24

Withdrawn

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 23009-4 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 29, *Coding of audio, picture, multimedia and hypermedia information*.

ISO/IEC 23009 consists of the following parts, under the general title *Information technology — Dynamic adaptive streaming over HTTP (DASH)*:

- *Part 1: Media presentation description and segment formats*
- *Part 2: Conformance and reference software¹*
- *Part 3: [Technical Report]²*
- *Part 4: Segment encryption and authentication*

¹ To be published.

² To be published.

Introduction

Dynamic Adaptive Streaming over HTTP (DASH) enables media-streaming model for delivery of media content in which control lies exclusively with the client. Clients may request data using the HTTP protocol from standard web servers that have no DASH-specific capabilities. Consequently, ISO/IEC 23009 focuses not on client or server procedures but on the data formats used to provide a DASH Media Presentation.

This part of ISO/IEC 23009 provides methods and interfaces for segment encryption and verification of segment integrity and authenticity

Withdrawn

Information technology — Dynamic adaptive streaming over HTTP (DASH) —

Part 4: Segment encryption and authentication

1 Scope

This part of ISO/IEC 23009 specifies:

- format-independent segment encryption and signalling mechanisms for use with any media segment format used in DASH (ISO/IEC 23009-1:2012);
- mechanisms to ensure segment integrity and authenticity for use with any segment used in DASH (ISO/IEC 23009-1:2012).

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 23009-1:2012, *Information technology — Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats*

Advanced Encryption Standard, Federal Information Processing Standards Publication 197, FIPS-197, <http://www.nist.gov/>

Secure Hash Standard, Federal Information Processing Standards Publication 180, FIPS 180-3, <http://www.nist.gov/>

Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A, <http://www.nist.gov/>

Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST, NIST Special Publication 800-38D, <http://www.nist.gov/>

IETF RFC 2104, *HMAC: Keyed-Hashing for Message Authentication*, H. Krawczyk, M. Bellare, R. Canetti, February 1997

IETF RFC 2616, *Hypertext Transfer Protocol – HTTP/1.1*, June 1999

IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*, January 2005

IETF RFC 5246, *The Transport Layer Security (TLS) Protocol*, T. Dierks et al, August 2008

IETF RFC 5652/STD 70, *Cryptographic Message Syntax (CMS)*, R. Housley, September 2009