INTERNATIONAL STANDARD

**ISO/IEC 23009-4**

Second edition
2018-10

Corrected version
2019-03

# 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*

Reference number
ISO/IEC 23009-4:2018(E)

© ISO/IEC 2018



**COPYRIGHT PROTECTED DOCUMENT**

© ISO/IEC 2018

All rights reserved. Unless otherwise specified, or required in the context of its implementation, 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
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Fax: +41 22 749 09 47
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

# Contents

Page

**Foreword** ... **iv**

**Introduction** ... **v**

**1 Scope** ... **1**

**2 Normative references** ... **1**

**3 Terms, definitions, abbreviated terms and notations** ... **1**
3.1 Terms and definitions ... 1
3.2 Abbreviated terms ... 2
3.3 Notations ... 3

**4 Segment encryption and authentication** ... **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 ... 8
5.1.5 CryptoPeriod element ... 9
5.1.6 CryptoTimeline element ... 10
5.2 Authentication declaration ... 11
5.2.1 General ... 11
5.2.2 ContentAuthenticity element ... 12
5.2.3 URL derivation ... 12

**6 Segment encryption** ... **13**
6.1 Segment format ... 13
6.2 Key systems ... 13
6.2.1 General ... 13
6.2.2 License-based key systems ... 13
6.3 Encryption systems ... 13
6.3.1 General ... 13
6.3.2 AES-128 CBC encryption system ... 14
6.3.3 AES-128 GCM encryption system ... 14
6.3.4 Common encryption system ... 14
6.4 Cryptoperiods ... 15
6.4.1 General ... 15
6.4.2 Assigning segments to cryptoperiods ... 15
6.4.3 Key derivation ... 16
6.4.4 IV derivation ... 16
6.4.5 AAD derivation ... 17
6.5 Adding new encryption and key systems ... 17

**7 Segment authentication** ... **18**
7.1 General ... 18
7.2 Algorithms ... 18
7.2.1 SHA-256 ... 18
7.2.2 HMAC-SHA1 ... 18

**Annex A** (normative) **XML schema** ... **19**

**Annex B** (informative) **Implementation guidelines** ... **21**

**Annex C** (informative) **MPD examples and usage** ... **22**

© ISO/IEC 2018 – All rights reserved

# 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

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. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see: www.iso.org/iso/foreword.html.

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

This second edition cancels and replaces the first edition (ISO/IEC 23009-4:2013), which has been technically revised.

The main changes compared to the previous edition are as follows:

— support for ISO/IEC 23001-7 has been added as an additional encryption system;

— support for service protection orthogonal to content protection has been added;

— interoperable reporting of authenticity tags has been enabled.

This corrected version of ISO/IEC 23009-4:2018 incorporates the following changes:

— 'licence' has been changed to 'license' throughout the document text;

— corrections have been made in code in Annex C.

A list of all parts in the ISO/IEC 23009 series can be found on the ISO website.

Any feedback or questions on this document should be directed to the user’s national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.


© ISO/IEC 2018 – All rights reserved

# 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, the ISO/IEC 23009 series focuses not on client or server procedures but on the data formats used to provide a DASH Media Presentation.

This document provides methods and interfaces for segment encryption and verification of segment integrity and authenticity.

© ISO/IEC 2018 – All rights reserved

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

# Part 4: Segment encryption and authentication

## 1 Scope

This document specifies:

— Format-independent segment encryption and signalling mechanisms for use with any media segment format used in DASH (ISO/IEC 23009-1).

— Mechanisms to ensure segment integrity and authenticity for use with any segment used in DASH (ISO/IEC 23009-1).

## 2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 23009-1:2014, *Information technology — Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats*

STANDARD A.E. Federal Information Processing Standards Publication 197, FIPS-197, http://www.nist.gov/

STANDARD S.H. 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/

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

RFC 7230, *Hypertext Transfer Protocol — HTTP/1.1, June 2014*

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

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

## 3 Terms, definitions, abbreviated terms and notations

### 3.1 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

© ISO/IEC 2018 – All rights reserved

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— IEC Electropedia: available at https://www.electropedia.org/

— ISO Online browsing platform: available at https://www.iso.org/obp

**3.1.1**
**additional authenticated data**
input data to the authenticated encryption function that is authenticated but not encrypted

**3.1.2**
**authentication tag**
cryptographic checksum on data that is designed to reveal both accidental errors and the intentional modification of the data

**3.1.3**
**authenticated encryption**
mode of operation in which the plaintext is encrypted into the ciphertext, and an authentication tag is generated on the AAD and the ciphertext

**3.1.4**
**cryptoperiod**
number of continuous segments for which the same encryption key and the same initialization vector are used

**3.1.5**
**encryption system**
system used for encryption of media segments using keys provided by the key system

**3.1.6**
**key system**
system that provides keys necessary for decryption of media segments

**3.1.7**
**segment number**
unique positive integer associated with a media segment within a representation

Note 1 to entry: The media segment presented (in presentation order) after media segment with segment number N has segment number N+1.

## 3.2 Abbreviated terms

| | |
|---|---|
| AAD | additional authentication data |
| AES | advanced encryption standard, as specified in FIPS-197 |
| AES-CBC | AES cipher in cipher block chaining mode, as specified in NIST 800-38A |
| AES-GCM | AES cipher in Galois/counter mode as specified in NIST 800-38D |
| CBC | cipher block chaining mode |
| DASH | dynamic adaptive streaming over HTTP, as specified in ISO/IEC 23009-1 |
| DRM | digital rights management |
| ECB | electronic code book, as specified in NIST 800-38A |
| GCM | Galois/counter mode, as specified in NIST 800-38D |
| HMAC | hash-based message authentication code, as specified in RFC 2104 |


© ISO/IEC 2018 – All rights reserved