INTERNATIONAL STANDARD

ISO/IEC 23009-4

First edition
2013-07-01

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 23009-4:2013(E)

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

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 software*[1]

— *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

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