INSO
21236-4
1st.Edition
2016
Identical with ISO/IEC 23009-4: 2013

جمهوری اسلامی ایران
Islamic Republic of Iran
سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۲۱۲۳۶-۴
چاپ اول
۱۳۹۵

دارای محتوای رنگی

فناوری اطلاعات- جاری‌سازی تطبیقی پویا روی HTTP (DASH)- قسمت ۴: اصالت‌سنجی و رمزگذاری قطعه

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

ICS: 35.040

سازمان ملی استاندارد ایران

تهران، ضلع جنوب غربی میدان ونک، خیابان ولیعصر، پلاک ۲۵۹۲

صندوق‌پستی: ۶۱۳۹-۱۴۱۵۵ تهران- ایران

تلفن: ۵-۸۸۸۷۹۴۶۱

دورنگار: ۸۸۸۸۷۰۸۰ و ۸۸۸۸۷۱۰۳

کرج - شهر صنعتی، میدان استاندارد

صندوق پستی: ۱۶۳-۳۱۵۸۵ کرج - ایران

تلفن: ۸- ۳۲۸۰۶۰۳۱ (۰۲۶)

دورنگار: ۳۲۸۰۸۱۱۴ (۰۲۶)

رایانامه: standard@isiri.org.ir

وبگاه: http://www.isiri.org

Iranian National Standardization Organization (INSO)

No.1294 Valiasr Ave., South western corner of Vanak Sq., Tehran, Iran

P. O. Box: 14155-6139, Tehran, Iran

Tel: + 98 (21) 88879461-5

Fax: + 98 (21) 88887080, 88887103

Standard Square, Karaj, Iran

P.O. Box: 31585-163, Karaj, Iran

Tel: + 98 (26) 32806031-8

Fax: + 98 (26) 32808114

Email: standard@isiri.org.ir

Website: http://www.isiri.org

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

سازمان ملی استاندارد ایران به موجب بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفهٔ تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

تدوین استاندارد در حوزه‌های مختلف در کمیسیون‌های فنی مرکب از کارشناسان سازمان، صاحب‌نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می‌شود و کوششی همگام با مصالح ملی و با توجه به شرایط تولیدی، فناوری و تجاری است که از مشارکت آگاهانه و منصفانهٔ صاحبان حق و نفع، شامل تولیدکنندگان، مصرف‌کنندگان، صادرکنندگان و واردکنندگان، مراکز علمی و تخصصی، نهادها، سازمان‌های دولتی و غیردولتی حاصل می‌شود. پیش‌نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی‌نفع و اعضای کمیسیون‌های مربوط ارسال می‌شود و پس از دریافت نظرها و پیشنهادها در کمیتهٔ ملی مرتبط با آن رشته طرح و در صورت تصویب، به عنوان استاندارد ملی (رسمی) ایران چاپ و منتشر می‌شود.

پیش‌نویس استانداردهایی که مؤسسات و سازمان‌های علاقه‌مند و ذی‌صلاح نیز با رعایت ضوابط تعیین شده تهیه می‌کنند درکمیته ملی طرح، بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می‌شود. بدین ترتیب، استانداردهایی ملی تلقی می‌شود که بر اساس مقررات استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که در سازمان ملی استاندارد ایران تشکیل می‌شود به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین‌المللی استاندارد (ISO)[1]، کمیسیون بین‌المللی الکتروتکنیک (IEC)[2] و سازمان بین‌المللی اندازه‌شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می‌کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی‌های خاص کشور، از آخرین پیشرفت‌های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود.

سازمان ملی استاندارد ایران می‌تواند با رعایت موازین پیش‌بینی شده در قانون، برای حمایت از مصرف‌کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست‌محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری کند. سازمان می‌تواند به منظور حفظ بازارهای بین‌المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری کند. همچنین برای اطمینان بخشیدن به استفاده‌کنندگان از خدمات سازمان‌ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم‌های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه‌ها و مراکز واسنجی (کالیبراسیون) وسایل سنجش، سازمان ملی استاندارد این‌گونه سازمان‌ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می‌کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن‌ها اعطا و بر عملکرد آن‌ها نظارت می‌کند. ترویج دستگاه بین‌المللی یکاها، واسنجی وسایل سنجش، تعیین عیار فلزات گرانبها و انجام تحقیقات کاربردی برای ارتقای سطح استانداردهای ملی ایران از دیگر وظایف این سازمان است.

1- International Organization for Standardization
2- International Electrotechnical Commission
3- International Organization for Legal Metrology (Organisation Internationale de Metrologie Legals)
4- Contact point
5- Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

« فناوری اطلاعات- جاری‌سازی تطبیقی پویا روی HTTP (DASH)- قسمت ۴: اصالت‌سنجی و رمزگذاری قطعه»

رئیس:	**سمت و/یا محل اشتغال:**
مشرف، بهنوش (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس استاندارد – کارشناس ارشد سیستم‌های اطلاعاتی- شرکت برق منطقه‌ای هرمزگان
دبیر:	
ترابی، مهرنوش (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس استاندارد- کارشناس ارشد شبکه و سخت‌افزار- شرکت برق منطقه‌ای هرمزگان
اعضا: (اسامی به ترتیب حروف الفبا)	
زمانی، کرشنا (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس مرکز رایانه- دانشگاه مازندران
صداقت، وجیهه (کارشناسی مترجمی زبان انگلیسی)	کارشناس ارشد آموزش- شرکت برق منطقه‌ای هرمزگان
قسمتی، سیمین (کارشناسی ارشد مهندسی فناوری اطلاعات)	مشاور- مرکز آپای تربیت معلم
مومنی، حمیدرضا (کارشناسی ارشد مهندسی کامپیوتر- هوش مصنوعی)	عضو هیات علمی- دانشگاه تنکابن
میرزاده، سکینه (کارشناسی مهندسی کامپیوتر- نرم‌افزار)	کارشناس صادرات و واردات- اداره کل استاندارد استان هرمزگان
ویراستار:	
مشرف، بهنوش (کارشناسی ارشد مهندسی فناوری اطلاعات)	کارشناس استاندارد – کارشناس ارشد سیستم‌های اطلاعاتی- شرکت برق منطقه‌ای هرمزگان

فهرست مندرجات

عنوان **صفحه**

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات- جاری‌سازی تطبیقی پویا روی HTTP (DASH)- قسمت ۴: اصالت‌سنجی و رمزگذاری قطعه» که پیش‌نویس آن در کمیسیون‌های مربوط بر مبنای پذیرش استانداردهای بین‌المللی به عنوان استاندارد ملی ایران به روش اشاره شده در مورد الف، بند ۷، استاندارد ملی شمارهٔ ۵ تهیه و تدوین شده، در چهارصد و چهل و پنجمین اجلاسیه کمیتهٔ ملی استاندارد فناوری اطلاعات مورخ ۱۳۹۵/۹/۱۵ تصویب شد. اینک این استاندارد به استناد بند یک مادهٔ ۳ قانون اصلاح قوانین و مقررات مؤسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

استانداردهای ملی ایران بر اساس استاندارد ملی ایران شمارهٔ ۵ (استانداردهای ملی ایران- ساختار و شیوهٔ نگارش) تدوین می‌شوند. برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم وخدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح یا تکمیل این استانداردها ارائه شود، در هنگام تجدیدنظر در کمیسیون فنی مربوط، مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

این استاندارد ملی بر مبنای پذیرش استاندارد بین‌المللی زیر به روش «معادل یکسان» تهیه و تدوین شده و شامل ترجمه تخصصی کامل متن آن به زبان فارسی می‌باشد و معادل یکسان استاندارد بین‌المللی مزبور است:

ISO/IEC 23009-4:2013, Information technology — Dynamic adaptive streaming over HTTP (DASH) — Part 4: Segment encryption and authentication

فناوری اطلاعات- جاری‌سازی تطبیقی پویا روی HTTP (DASH)- قسمت ۴: اصالت‌سنجی و رمزگذاری قطعه

۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین موارد زیر است:

- سازوکارهای نشانک‌دهی و رمزگذاری قطعه قالب-مستقل برای استفاده با هر قالب قطعه رسانه که در جاری‌سازی تطبیقی پویا روی HTTP (DASH)[1] (استاندارد ISO/IEC 23009-1:2012) استفاده شده است.

- سازوکارهایی برای اطمینان از یکپارچگی و اصالتِ قطعه برای استفاده با هر قطعه که در DASH (استاندارد ISO/IEC 23009-1:2012) استفاده شده است.

۲ مراجع الزامی

در مراجع زیر ضوابطی وجود دارد که در متن این استاندارد به صورت الزامی به آن‌ها ارجاع داده شده است. بدین‌ترتیب، آن ضوابط جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مرجعی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن برای این استاندارد الزام‌آور نیست. در مورد مراجعی که بدون ذکر تاریخ انتشار به آن‌ها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی برای این استاندارد الزام‌آور است.

استفاده از مراجع زیر برای کاربرد این استاندارد الزامی است:

2-1 ISO/IEC 23009-1:2012, Information technology — Dynamic adaptive streaming over HTTP (DASH) — Part 1: Media presentation description and segment formats

2-2 Advanced Encryption Standard, Federal Information Processing Standards Publication 197, FIPS- 197, http://www.nist.gov/

2-3 Secure Hash Standard, Federal Information Processing Standards Publication 180, FIPS 180-3, http://www.nist.gov/

2-4 Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A, http://www.nist.gov/

2-5 Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, NIST, NIST Special Publication 800-38D, http://www.nist.gov/

2-6 IETF RFC 2104, HMAC: Keyed-Hashing for Message Authentication, H. Krawczyk, M. Bellare, R. Canetti, February 1997

1 - Dynamic adaptive streaming over HTTP

2-7 IETF RFC 2616, Hypertext Transfer Protocol – HTTP/1.1, June 1999

2-8 IETF RFC 3986, Uniform Resource Identifier (URI): Generic Syntax, January 2005

2-9 IETF RFC 5246, The Transport Layer Security (TLS) Protocol, T. Dierks et al, August 2008

2-10 IETF RFC 5652/STD 70, Cryptographic Message Syntax (CMS), R. Housley, September 2009

۳ اصطلاحات و تعاریف و کوته‌نوشت‌ها

۳-۱ اصطلاحات و تعاریف

در این استاندارد، اصطلاحات با تعاریف زیر به کار می‌رود:

۳-۱-۱

داده اصالت‌سنجی‌شده افزوده

additional authenticated data

داده ورودی برای تابع رمزگذاری اصالت‌سنجی‌شده که اصالت‌سنجی شده اما رمزگذاری نشده است.

۳-۱-۲

برچسب اصالت‌سنجی

authentication tag

مجموع مقابله‌ای رمزنگاشتی[1] بر روی داده که طراحی شده است تا خطاهای تصادفی و تغییرات عمدی داده را آشکار کند.

۳-۱-۳

رمزگذاری اصالت‌سنجی‌شده

authenticated encryption

حالت عملیاتی که در آن متن ساده به متن رمز[2] رمزگذاری می‌شود و برچسب اصالت‌سنجی بر روی AAD و متن رمزی تولید می‌شود.

۳-۱-۴

مدت‌رمز

cryptoperiod

تعداد قطعه‌های پیوسته‌ای که برای آن‌ها، از کلید رمزگذاری و بردار مقداردهی اولیه یکسان استفاده می‌شود.

1 - Cryptographic checksum
2 - Ciphertext

۵-۱-۳

سامانه رمزگذاری

encryption system

سامانه‌ای که برای رمزگذاری «قطعه‌های رسانه» با استفاده از کلیدهای فراهم شده توسط «سامانه کلید» استفاده می‌شود.

۶-۱-۳

سامانه کلید

key system

سامانه‌ای که کلیدهای لازم را برای رمزگشایی «قطعه‌های رسانه» فراهم می‌کند.

۷-۱-۳

شماره قطعه

segment number

عدد صحیح مثبت یکتای مرتبط با «قطعه‌های رسانه» در درون یک «نمایش»[1] است.

یادآوری ۱- «قطعه‌های رسانه» ارائه شده (به ترتیب نمایش) پس از «قطعه‌های رسانه» با «شماره قطعه» N، «شماره قطعه» N+1 دارد.

۲-۳ کوته‌نوشت‌ها

AAD	Additional Authentication Data	داده اصالت‌سنجی افزوده
AES	Advanced Encryption Standard as specified in FIPS-197	استاندارد رمزگذاری پیشرفته، مشخص شده در استاندارد FIPS-197
AES-CBC	AES cipher in Cipher Block Chaining mode, as specified in NIST 800-38A	رمز AES در حالت زنجیره بستک (بلوک)[2] رمز، مشخص شده در استاندارد NIST 800-38A
ECB	Electronic Code Book, as specified in NIST 800-38A	کتاب کد الکترونیکی، مشخص شده در استاندارد NIST 800-38A
AES-GCM	AES cipher in Galois/Counter Mode, as specified in NIST 800-38D	رمز AES در حالت Galois/Counter، مشخص شده در استاندارد 800-38D

1 - Representation
2 - Block

HMAC	Hash-based Message Authentication Code, as specified in IETF RFC 2104	کد اصالت‌سنجی پیام مبتنی بر چکیده‌ساز، مشخص شده در استاندارد IETF RFC 2104
IV	Initialization Vector	بردار مقداردهی اولیه
MPD	Media Presentation Description, as specified in ISO/IEC 23009-1:2012	توصیف نمایش رسانه، مشخص شده در استاندارد ISO/IEC 23009-1:2012
SHA	Secure Hash Algorithm, as specified in FIPS 180-3	الگوریتم چکیده‌ساز امن، مشخص شده در استاندارد FIPS 180-3
SN	Segment Number	شماره قطعه
TLS	Transport Layer Security	امنیت لایه انتقال
URI	Uniform Resource Identifier	شناسانه منبع یکنواخت
URL	Uniform Resource Locator	نشانی وب
URN	Uniform Resource Name	نام منبع یکنواخت

۳-۳ نماد

«قطعه رسانه» با «شماره قطعه» i: S(i).

مدت‌رمز که با «شماره قطعه» i شروع می‌شود و دارای d «قطعه رسانه» است: CP(i,d)

بردار مقداردهی اولیه و کلید مورد استفاده در مدت زمان CP(i,d): $IV_{CP(i,d)}$, $K_{CP(i,d)}$

۴ مقدمه

۴-۱ رمزگذاری قطعه

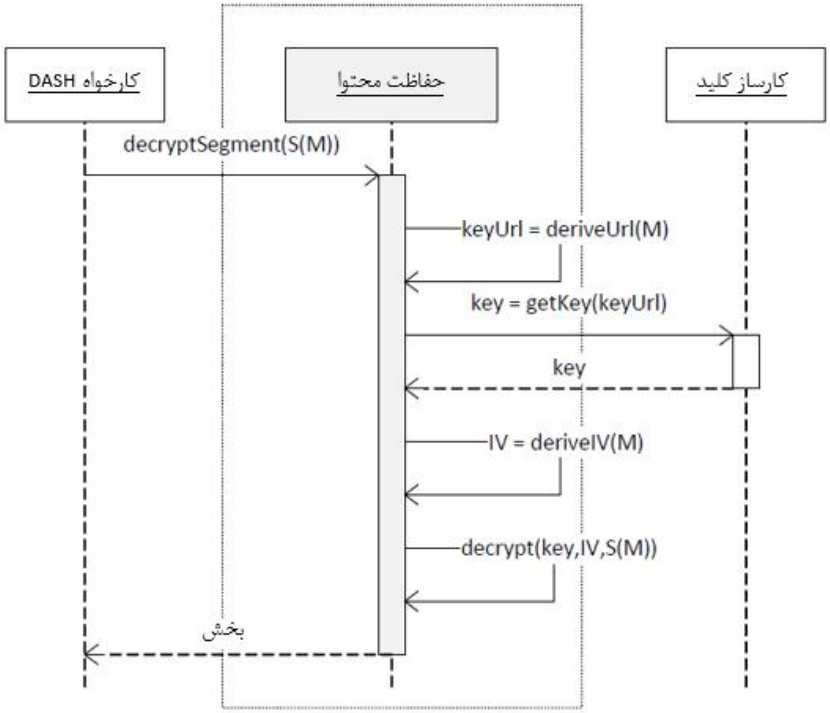
چارچوب حفاظت محتوا که در این استاندارد فراهم شده است، چارچوبی برای استخراج خارج-از-باند پارامترهایی است که برای رمزگشایی موفقیت‌آمیز قطعه‌های رسانه لازم است. ابزارهای فراهم شده واسط‌های MPD است که استخراج پارامترهای مقداردهی اولیه و کلید، رمزگذاری خط مبنا و روش‌های تفکیک کلید را اجازه می‌دهد و سرانجام نقاط توسعه‌پذیر را فراهم می‌کند تا الگوریتم‌های رمزگذاری و تفکیک کلید مختلف را با استفاده از واسط مشابه تطبیق دهد.

به‌طور مفهومی، چارچوب حفاظت محتوا که در این استاندارد فراهم شده است می‌تواند به عنوان دو هستار در نظر گرفته شود: سامانه کلید و سامانه رمزگذاری. سامانه کلید، کلیدهای مربوط به قطعه‌ای را استخراج می‌کند که اطلاعات فراهم شده در MPD را می‌دهد در حالیکه سامانه رمزگذاری، قطعه‌های رسانه‌ای را رمزگشایی می‌کند که اطلاعات و کلیدهای رمزگذاری به آن داده شده است؛ این اطلاعات در MPD فراهم شده است و این کلیدهای رمزگذاری توسط سامانه کلید فراهم شده است.

سامانه اجباری خط مبنا، رمزگذاری AES-CBC برای قطعه کامل به‌کار می‌برد و از HTTP(S) برای انتقال کلید استفاده می‌کند. در این سامانه خط مبنا، کارخواه DASH می‌تواند به‌طور انحصاری هر قطعه‌ای را تشخیص دهد که بردار مقداردهی اولیه و کلید برای رمزگذاری آنها استفاده شده است. سپس کارخواه درخواست GET برای کلید صادر می‌کند و درخواست GET را برای بردار مقداردهی اولیه صادر می‌کند یا آن را به‌طور محلی استخراج می‌کند. پس از دریافت بردار مقداردهی اولیه و کلید، کارخواه DASH می‌تواند با موفقیت قطعه رسانه را رمزگشایی کند و آن را به موتور رسانه انتقال دهد. در این توصیف، رمزگذاری قطعه-کامل AES-CBC ، سامانه رمزگذاری است و بازیابی کلید با استفاده از HTTP(s)، سامانه کلید است.

هنگامی‌که اغلب سامانه‌های DRM از سامانه‌های مبتنی بر مجوز برای استخراج کلیدها استفاده می‌کنند، سامانه‌های کلیدی مبتنی بر مجوز در این استاندارد پشتیبانی می‌شوند. در این مورد، مجوز بازیابی می‌شود و URIهای کلیدی، شناسانه‌های کلیدی مبهم هستند. سامانه کلیدی مبتنی بر مجوز، این شناسانه‌ها را به کلیدهایی با روش نامعلوم مقرر می‌کند[1] و کلیدها را به سامانه رمزگذاری انتقال می‌دهد. سپس کلیدهای فراهم شده توسط سامانه کلید و اطلاعات رمزگذاری (برای مثال، مشخصات الگوریتم و IV) فراهم شده توسط MPD، قطعه رسانه را رمزگشایی می‌کند.

1 - Resolve



شکل ۱- رمزگذاری قطعه خطِ مبنا

روش‌های دیگر رمزگذاری می‌تواند با استفاده از URIها و (احتمالاً) پارامترهای مربوط به رمزگذاری کلی که در این استاندارد فراهم شده است، نشانک‌دهی شود. این استاندارد مستقل از قالب است: این استاندارد به‌طور ویژه برای همه انواع قطعه رسانه به‌کار نمی‌رود و مفهوم آن از مدت‌رمزها، به‌طور کامل جدا از هر نوع قطعه ویژه است. سامانه رمزگذاری خط مبنا برای یک قطعه کامل به کاربرده می‌شود.

قسمت الزامی این چارچوب موارد زیر را فراهم می‌کند: الف) واسط MPD و ب) سامانه‌های رمزگذاری و کلید خط مبنا. این موارد در شکل ۱ نشان داده می‌شوند. یادآوری می‌شود که پیاده‌سازی نشان داده شده در این شکل برای اهداف تشریح است و بسیاری از عملیات‌ها را می‌توان برای مثال توسط موازی‌سازی و پیش‌واکشی[1] بهینه کرد.

طرح رمزگذاری قطعه، روش‌های نگاشت کلید و رمزگذاری استاندارد را مشخص می‌کند که می‌توان هنگامی استفاده کرد که حفاظت از این قطعه لازم است. این طرح توسط به‌کاربردن رمزگذاری برای قطعه‌ها، عمل می‌کند که به‌طور حفاظت شده‌ای فرستاده می‌شود. تعاریف فراهم می‌شوند تا قطعه‌ها را هنگامی‌که رمزگذاری می‌شوند، شناسایی کنند و کلید(ها) و IV(های) مناسب را از MPD شناسایی کنند.

1 - Pre-fetching

۴-۲ اصالت‌سنجی قطعه

چارچوب اصالت‌سنجی قطعه، چارچوبی است که استفاده از برچسب‌های اصیل را برای تمام انواع قطعه‌های DASH اجازه می‌دهد تا اصل و صحت محتوا را بازبینی کند. این چارچوب با محاسبه خلاصه اطلاعات یا یک MAC از قطعه رمزگذاری‌نشده و ذخیره کردن مقدار از خارج، کار می‌کند. واسط MPD، الگوهای URL را فراهم می‌کند تا اینها را با استفاده از HTTPS یا HTTP بازیابی کند. کارخواه، امضاء/ خلاصه اطلاعات را بازیابی[1] می‌کند، سپس آنها را به‌طور محلی در (زیر)قطعه رمزگشایی شده محاسبه می‌کند و در صورت عدم تطابق می‌تواند (زیر)قطعه را رد کند.

اگر باهم با رمزگذاری استفاده شوند، حالت عملیات این چارچوب، به جای حالت «رمزگذاری، سپس اصالت‌سنجی» که معمول‌تر است، «اصالت‌سنجی، سپس رمزگذاری» می‌باشد. حالت اول، ویژگی مهمی از تغییرناپذیری رمزگذاری را فراهم می‌کند: اگر رمزگذاری نباشد، یا پارامترها و / یا الگوریتم رمزگذاری مختلف برای رمزگذاری قطعه رسانه مشابه برای خدمت آن به کارخواهان مختلف استفاده شود، برچسب اصیل مادامی‌که خود محتوا تغییر نکرده است، مشابه باقی می‌ماند.

اصالت‌سنجی قطعه، مستقل از هر طرح حفاظت محتوا است و ممکن است برای قطعه رمزگذاری‌نشده و همچنین برای قطعه‌های رمزگذاری‌شده استفاده شود که این قطعه‌های رمزگذاری‌شده با استفاده از هر سامانه DRM رمزدار شده است. یادآوری می‌شود که این بدین معناست که استفاده از چارچوب حفاظت محتوای این استاندارد به منظور استفاده از چارچوب اصالت‌سنجی محتوا، الزامی نیست.

قسمت الزامی این چارچوب موارد زیر را فراهم می‌کند: الف) واسط MPD و ب) الگوریتم اصالت‌سنجی خط مبنا.

۴-۳ امنیت MPD

چارچوب‌های فراهم شده در این استاندارد همانند MPD امن هستند. بنابراین حفاظت از MPD بسیار مهم است. برای مثال با فرستادن آن بر روی اتصال امن یا با بازبینی یکپارچگی و اصالت آن، می‌توان از آن حفاظت کرد.

روشهای حفاظت از MPD خارج از دامنه کاربرد این استاندارد است.

1 - Retrieve

۵ نشانک‌دهی (سیگنال‌دهی)[1] رمزگذاری و اصالت‌سنجی

۵-۱ اظهار رمزگذاری

۵-۱-۱ عنصر ContentProtection

۵-۱-۱-۱ تعریف

کاربرد قالب رمزگذاری تعریف شده در این استاندارد برای قطعه‌ها، باید با استفاده از URN urn:mpeg:dash:sea:enc:2013 به‌عنوان مقداری برای @schemeIdUri در یک توصیف‌گر **ContentProtection** کاربردپذیر برای قطعه‌های رمزگذاری‌شده، اظهار شود. توصیف‌گر **ContentProtection** ممکن است صفر یا چند عنصر **CryptoPeriod** و / یا **CryptoTimeline** داشته باشد.

یادآوری می‌شود که توصیف‌گر ContentProtection در فضای نام urn:mpeg:dash:schema:mpd:2011 تعریف شده در استاندارد ISO/IEC 23009-1، تعریف می‌شود. در حالی‌که **SegmentEncryption**، **CryptoPeriod** و **CryptoTimeline** در فضای نام urn:mpeg:dash:schema:sea:2013 تعریف شده در پیوست الف، تعریف می‌شود. برای اهداف تشریح، همه عناصر طرح بالا، در قواعد نحوی[2] زیر، با :sea پیشوند می‌شوند.

۵-۱-۱-۲ قواعد معنایی[3]

جدول ۱- استفاده از توصیف‌گر حفاظت محتوای DASH

نام عنصر یا خصیصه	استفاده	توصیف
ContentProtection		
@schemeIdUri	M	برای این استاندارد باید urn:mpeg:dash:sea:enc:2013 باشد.
sea:SegmentEncryption	1	سامانه رمزگذاری استفاده شده و خصوصیت‌های سراسریش را مشخص می‌کند. به زیربند ۵-۲-۱ مراجعه شود.
sea:License	0..N	سامانه کلید استفاده شده و راه‌های بدست آوردن مجوز را در صورت نیاز مشخص می‌کند.

1 - Signalling
2 - Syntax
3 - Semantics

نام عنصر یا خصیصه	استفاده	توصیف
sea:CryptoPeriod	0..N	اطلاعات مورد نیاز برای استخراج کلید و اطلاعات IV برای مدت‌رمز واحد را مشخص می‌کند. به زیربند ۵-۱-۴ مراجعه شود.
sea:CryptoTimeline	0..N	اطلاعات مورد نیاز برای استخراج کلید و اطلاعات IV برای چندین مدت‌رمز با طول ثابت را مشخص می‌کند. به زیربند ۵-۱-۶ مراجعه شود.
راهنما: برای خصیصه‌ها: M = اجباری، O = اختیاری، OD = اختیاری با مقدار پیش‌فرض، CM = به‌طور مشروط اجباری برای عناصر: <minOccurs>...<maxOccurs> (N = نامحدود) عناصر به‌صورت پررنگ هستند؛ خصیصه‌ها پررنگ نیستند و @ قبل از آن آمده است.		

۵-۱-۲ عنصر SegmentEncryption

عنصر **SegmentEncryption**، همانطور که در همه مدت‌رمزها استفاده شده است، خصوصیات سراسری رمزگذاری قطعه را توصیف می‌کند.

اگر مقدار **ContentProtection**@schemeIdUri برابر با urn:mpeg:dash:sea:enc:2013 باشد، عنصر **SegmentEncryption** واحد باید همیشه در توصیف‌گر **ContentProtection** وجود داشته باشد.

جدول ۲- قواعد معنایی عنصر SegmentEncryption

نام عنصر یا خصیصه	استفاده	توصیف
SegmentEncryption		خصوصیات سامانه رمزگذاری را مشخص می‌کند.
@schemeIdUri	M	سامانه رمزگذاری استفاده شده برای رمزگذاری قطعه را مشخص می‌کند. سامانه‌های رمزگذاری ممکن در زیربند ۶-۳-۲ مشخص شده‌اند.
@keyLength	OD	طول (به بیت) کلید استفاده شده در رمز تعریف شده در @schemeIdUri را مشخص می‌کند. مقدار پیش‌فرض ۱۲۸ است.
@ivLength	OD	طول (به بیت) بردار مقداردهی اولیه استفاده شده در رمز تعریف شده در @schemeIdUri را مشخص می‌کند. مقدار پیش‌فرض ۱۲۸ است.
@authTagLength	OD	اگر حالت عملیات بستک رمزگذاری اصالت‌سنجی‌شده (برای مثال، GCM) استفاده شود، طول (به بیت) برچسب اصالت‌سنجی استفاده شده را مشخص می‌کند. مقدار پیش‌فرض ۰ (یعنی، اصالت‌سنجی در دسترس نیست) است.
@earlyAvailability	OD	فاصله ثانیه‌ها بین زمانی‌که کلید و IV با استفاده از URIهای فراهم‌شده و زمان دردسترس اولین قطعه رمزگذاری شده با استفاده از این کلیدها، می‌توانند مقرر شوند. مقدار پیش‌فرض 1.0 ثانیه است.

نام عنصر یا خصیصه	استفاده	توصیف
@ivEncryptionFlag	OD	هنگامی که به «true» تنظیم می‌شود و شماره قطعه برای استخراج IV استفاده می‌شود (طبق تعریف در زیربند ۶-۴-۴)، رمزگذاری ECM IV استفاده خواهد شد. مقدار پیش‌فرض «false» است.
راهنما: برای خصیصه‌ها: M = اجباری، o = اختیاری، OD = اختیاری با مقدار پیش‌فرض، CM = به‌طور مشروط اجباری برای عناصر: <minOccurs>...<maxOccurs> (N = نامحدود) عناصر به‌صورت پررنگ هستند؛ خصیصه‌ها پررنگ نیستند و @ قبل از آن آمده است.		

۵-۱-۳ عنصر License

عنصر **License**، خصوصیات سراسری سامانه کلید استفاده شده در همه مدت‌رمزها را توصیف می‌کند.

اگر مقدار **ContentProtection**@schemeIdUri برابر با urn:mpeg:dash:sea:2013 و سامانه‌های کلید مبتنی بر مجوز استفاده شوند، یک یا چند عنصر License باید در درون توصیف‌گر **ContentProtection** وجود داشته باشد. اگر وجود نداشته باشند، URLهای فراهم شده در عناصر **CryptoPeriod** و **CryptoTimeline** باید برای برای بازیابی کلیدها کافی باشند.

جدول ۳- قواعد معنایی عنصر License

نام عنصر یا خصیصه	استفاده	توصیف
License		اطلاعات مورد نیاز برای بازیابی کلیدها را مشخص می‌کند.
@keySystemUri	M	URN سامانه کلید را مشخص می‌کند.
@keyLicenseUrlTemplate	O	الگوی HTTP(S) URL استفاده شده برای مجوز بازیابی که توسط سامانه کلید برای استخراج کلیدهای رمزگذاری استفاده می‌شود را با استفاده از قوانین نحوی مشابه و جانشینی متغیر تعریف شده در استاندارد ISO/IEC 23009-1:2012, 5.3.9.4.4، مشخص می‌کند.
راهنما: برای خصیصه‌ها: M = اجباری، o = اختیاری، OD = اختیاری با مقدار پیش‌فرض، CM = به‌طور مشروط اجباری برای عناصر: <minOccurs>...<maxOccurs> (N = نامحدود) عناصر به‌صورت پررنگ هستند؛ خصیصه‌ها پررنگ نیستند و @ قبل از آن آمده است.		

۵-۱-۴ خصوصیت‌های مدت‌رمز رایج

۵-۱-۴-۱ تعریف

مدت‌رمزها توسط پارامترهای رمزگذاری رایج و مدت زمان، تشخیص داده می‌شوند. بنابراین یک عنصر جدا، مدت‌رمز نمونه اولیه را نشان می‌دهد. هر دو عنصر **CryptoPeriod** و **CryptoTimeline** براساس این پایه ساخته می‌شوند که عنصر اول مدت‌رمز را نشان می‌دهد و عنصر بعدی چند مدت‌رمز متشابه را نشان می‌دهد.

۵-۱-۴-۲ قواعد معنایی

جدول ۴- خصوصیت‌های رایج مدت‌رمز

نام عنصر یا خصیصه	استفاده	توصیف
@numSegments	O	تعداد قطعه‌ها در مدت‌رمز را مشخص می‌کند. در مورد CryptoTimeline، این مورد، تعداد قطعه‌ها در هر مدت‌رمز از این **CryptoTimeline** است. @numSegments ممکن است فقط هنگامی موجود نباشد که این مورد، آخرین عنصر **CryptoPeriod** از دوره زمانی باشد. در این مورد، مدت‌رمز تا انتهای این دوره زمانی ادامه می‌یابد. یادآوری می‌شود که @numSegments برای همه عناصر **CryptoTimeline** باید وجود داشته باشد.
@keyUriTemplate	M	الگو برای تولید URI کلید با استفاده از قواعد نحوی و جانشینی متغیر تعریف شده در استاندارد ISO/IEC 23009-1:2012, 5.3.9.4.4، مشخص می‌کند. @keyUriTemplate در هر مدت‌رمز یک‌بار استفاده می‌شود، بنابراین برای مدت‌رمز CP(i,d)، URI مربوط به @keyUriTemplate با $Number$ = i ساخته می‌شود. همین کاربرد برای $Time$: (مقدار استفاده شده، مقدار $Time$ از قطعه S(i) است) استفاده خواهد شد. یادآوری می‌شود که استفاده از @keyUriTemplate به معنی استفاده از @ivUrlTemplate یا **SegmentTemplate** نیست. قواعد استخراج کلید در زیربند ۶-۴-۳ مشخص می‌شوند.

نام عنصر یا خصیصه	استفاده	توصیف
@ivUriTemplate	O	الگو برای تولید IV URI با استفاده از قواعد نحوی و جانشینی متغیر تعریف شده در استاندارد ISO/IEC 23009-1:2012, 5.3.9.4.4، مشخص می‌کند. @ivUriTemplate در هر مدت‌رمز یک‌بار استفاده می‌شود، بنابراین برای مدت‌رمز CP(i,d)، URI مربوط به @ivUrlTemplate با $Number$ = i ساخته می‌شود. همین کاربرد برای $Time$: (مقدار استفاده شده، مقدار $Time$ از قطعه S(i) است) استفاده خواهد شد. استفاده از @ivUrlTemplate به معنی استفاده از @keyUriTemplate یا **SegmentTemplate** نیست. برای تعریف قالب IV به زیربند ۶-۴-۴-۲ مراجعه شود.
راهنما: برای خصیصه‌ها: M = اجباری، o = اختیاری، OD = اختیاری با مقدار پیش‌فرض، CM = به‌طور مشروط اجباری برای عناصر: <minOccurs>...<maxOccurs> (N = نامحدود) عناصر به‌صورت پررنگ هستند؛ خصیصه‌ها پررنگ نیستند و @ قبل از آن آمده است.		

۵-۱-۵ عنصر CryptoPeriod

۵-۱-۵-۱ تعریف

عنصر **CryptoPeriod** مدت‌رمز را تعریف می‌کند – برای مثال، اطلاعاتی را فراهم می‌کند که استخراج بردار مقداردهی اولیه و کلید رمزگذاری و همچنین شناسایی قطعه‌هایی که با استفاده از دو عنصر سابق رمزگذاری شده‌اند را اجازه می‌دهد. عنصر **CryptoPeriod** به‌طور انحصاری مطابق قطعه شروع است. ممکن است به‌طور صریح مدت زمان معینی (برای مثال، تعداد قطعه‌ها) داشته باشد و یا ممکن است نامحدود (برای مثال، تا انتهای دوره فعلی ادامه دارد) باشد.

قطعه‌ها توسط «شماره قطعه» مطابق تعریف استاندارد ISO/IEC 23009-1:2012 5.3.9.4.4 شناسایی می‌شوند. مثال MPD که شامل عنصر **CryptoPeriod** است در زیربند ج-۱ نشان داده شده است.

۵-۱-۵-۲ قواعد معنایی

جدول ۵- قواعد معنایی عنصر CryptoPeriod

نام عنصر یا خصیصه	استفاده	توصیف
CryptoPeriod		اطلاعات و URIهای مورد نیاز برای استخراج اطلاعات کلید برای مدت‌رمز واحد، مشخص می‌کند.
@startOffset	OD	تعداد قطعه‌های رمزگذاری‌نشده بعد از انتهای مدت‌رمز گذشته و اولین قطعه رسانه که برای آن، اطلاعات کلید / IV به‌کار می‌رود را مشخص می‌کند. مقدار پیش‌فرض ۰ است. قواعد استخراج مشخص شده در زیربند ۶-۴-۲ به‌کار می‌رود.
@IV	O	بردار مقداردهی اولیه را مشخص می‌کند. اگر @ivUriTemplate موجود باشد، این خصیصه نباید وجود داشته باشد.
@aad	O	داده اصالت‌سنجی افزوده را مشخص می‌کند. قواعد استخراج AAD در زیربند ۶-۴-۴ مشخص شده است.
CryptoPeriodType	-	عناصر و خصیصه‌های رایج (عناصر و خصیصه‌ها از نوع پایه **CryptoPeriodType**) را مشخص می‌کند. برای جزئیات به زیربند ۵-۱-۴ مراجعه شود.
راهنما: برای خصیصه‌ها: M = اجباری، O = اختیاری، OD = اختیاری با مقدار پیش‌فرض، CM = به‌طور مشروط اجباری برای عناصر: <minOccurs>...<maxOccurs> (N = نامحدود) عناصر به‌صورت پررنگ هستند؛ خصیصه‌ها پررنگ نیستند و @ قبل از آن آمده است.		

۵-۱-۶ عنصر CryptoTimeline

۵-۱-۶-۱ تعریف

عنصر **CryptoTimeline** برای استخراج چند مدت‌رمز با طول ثابت استفاده می‌شود. در حالی‌که یک **CryptoPeriod** واحد مطابق با مدت‌رمز واحد است، عنصر **CryptoTimeline** واحد مطابق با چندین مدت‌رمز است.

استفاده از **CryptoTimeline** هنگامی تقویت می‌شود که الگوی بسیار منظمی از مدت‌رمزها مورد استفاده قرار می‌گیرد، برای مثال، هنگامی‌که یک زوج کلید / IV در هر ۴ مدت‌رمز تغییر می‌کند. هر مدت‌رمز تولید شده از **CryptoTimeline** شامل تعداد یکسانی از قطعه‌ها است (به مثال زیربند ج-۲ مراجعه شود).

۵-۱-۶-۲ قواعد معنایی

جدول ۶- قواعد معنایی عنصر CryptoTimeline

نام عنصر یا خصیصه	استفاده	توصیف
CryptoTimeline		توالی مدت‌رمزها که هریک شامل مقدار مشابه قطعه‌ها است را مشخص می‌کند.
@numCryptoPeriods	O	تعداد مدت‌رمزها با دوره زمانی ثابت مشخص می‌کند. اگر وجود نداشته باشد، آخرین مدت‌رمز با انتهای دوره زمانی که این توصیف‌گر **ContentProtection** به آن تعلق دارد، خاتمه می‌یابد. یادآوری می‌شود که این به این معنی است که مقدار قطعه‌ها در آخرین مدت‌رمز در این مورد، می‌تواند کوچکتر از مقدار خصیصه مشخص شده در @numSegments باشد.
@firstStartOffset	OD	تعداد قطعه‌های رمزگذاری شده بین انتهای آخرین مدت‌رمز و اولین قطعه اولین مدت‌رمز در این **CryptoTimeline** مشخص می‌کند. مقدار پیش‌فرض ۰ است. قواعد استخراج مشخص شده در زیربند ۶-۴-۲ به‌کار می‌رود.
@ivBase	OD	مقدار پایه IV برای این مدت‌رمز مشخص می‌کند. هنگامی‌که @ivBase موجود است، همانطور که در زیربند ۶-۴-۴-۲ مشخص شده است، IV برابر با جمع @ivBase و تعداد قطعه است. اگر وجود نداشته باشد، مقدار پیش‌فرض ۰ است. اگر @ivUriTemplate موجود باشد، این خصیصه نباید موجود باشد.
@aadBase	OD	مقدار پایه AAD را برای این مدت‌رمز مشخص می‌کند. AAD برابر با جمع @aadBase و شماره قطعه است. اگر وجود نداشته باشد، مقدار پیش‌فرض ۰ است.
CryptoPeriodType	-	عناصر و خصیصه‌های رایج(عناصر و خصیصه‌ها از نوع پایه **CryptoPeriodType**) را مشخص می‌کند. برای جزئیات به زیربند ۵-۱-۴ مراجعه شود.

راهنما:
برای خصیصه‌ها: M = اجباری، o = اختیاری، OD = اختیاری با مقدار پیش‌فرض، CM = به‌طور مشروط اجباری
برای عناصر: <minOccurs>...<maxOccurs> (N = نامحدود)
عناصر به‌صورت پررنگ هستند؛ خصیصه‌ها پررنگ نیستند و @ قبل از آن آمده است.

یادآوری- به‌طور نمونه در فرانامه[1] چرخش کلید @firstStartOffset و @numCryptoPeriods معلوم نمی‌شوند و زوج کلید / IV همه قطعه‌های @numSegments را تغییر می‌دهد.

۵-۲ اظهار اصالت‌سنجی

۵-۲-۱ کلیات

عنصر **ContentAuthenticity** که در قسمت پایین تعریف شده است باید در **EssentialProperty** یا **SupplementalProperty** تعریف شده در استاندارد ISO/IEC 23009-1:2012، بنا به الزامات برنامه کاربردی، استفاده شود.

1 - Scenario

اگر چارچوب اصالت‌سنجی استفاده شود، مقدار @schemeIdUri در **EssentialProperty** یا **SupplementalProperty** باید urn:mpeg:dash:sea:auth:2013 باشد.

چندین طرح تصدیق اصالت محتوا می‌تواند تعریف شود. دو طرح، خلاصه SHA-256 شناسایی شده توسط URN urn:mpeg:dash:sea:sha256:2013 و MAC HMAC-SHA1 شناسایی شده توسط urn:mpeg:dash:sea:hmac-sha1، در این استاندارد مشخص شده‌اند.

۵-۲-۲ عنصر ContentAuthenticity

۵-۲-۲-۱ تعریف

عنصر **ContentAuthenticity**،URLایی برای اکتساب کلید و الگویی برای ساخت URL فراهم می‌کند که بیشتر برای بارگیری[1] برچسب اصالت‌سنجی برای (زیر)قطعه معین استفاده می‌شود. قواعد ساخت URL در زیربند ۵-۲-۳ تعریف شده است.

1 - download

۵-۲-۲-۲ قواعد معنایی

جدول ۷- قواعد معنایی عنصر ContentAuthenticity

نام عنصر یا خصیصه	استفاده	توصیف
ContentAuthenticity		اطلاعات لازم برای محاسبه برچسب اصیل برای قطعه را مشخص می‌کند.
@authSchemeIdUri	M	الگوریتم استفاده شده برای محاسبه برچسب اصیل را مشخص می‌کند.
@authUrlTemplate	M	الگو برای ایجاد URL استفاده شده برای بازیابی مقدار برچسب اصیل مشخص می‌کند. قواعد ایجاد URL در زیربند ۵-۲-۳ مشخص شده‌اند.
@authTagLength	O	طول برچسب اصالت‌سنجی را به بیت مشخص می‌کند. اگر وجود نداشته باشد، طول برچسب، مشابه الگوریتم شناخته شده توسط @authSchemeIdUri است.
@keyUrlTemplate	O	الگو برای تولید URI کلید، با استفاده از قواعد نحوی و جانشینی متغیر طبق تعریف استاندارد ISO/IEC 23009-1:2012, 5.3.9.4.4، مشخص می‌کند.
راهنما: برای خصیصه‌ها: M = اجباری، o = اختیاری، OD = اختیاری با مقدار پیش‌فرض، CM = به‌طور مشروط اجباری برای عناصر: <minOccurs>...<maxOccurs> (N = نامحدود) عناصر به‌صورت پررنگ هستند؛ خصیصه‌ها پررنگ نیستند و @ قبل از آن آمده است.		

۵-۲-۳ استخراج URL

URLهای برچسب اصیل باید با سازوکار زیر ساخته شوند:

۱. یک URL کامل برای یک رسانه معین، مقداردهی اولیه، نمایه یا قطعه (زیرقطعه) سودهی[1] جریان بیت ساخته می‌شود.
۲. همان متغیرهای جایگزین در استاندارد ISO/IEC 23009-1:2012 پیوست E باید برای ساخت الگوهای URL امضاء یا خلاصه استفاده شوند. اگر درخواست شامل یک محدوده بیت نباشد، مقدار $first$ باید «۰» باشد و مقدار $last$ باید «Inf» باشد.

محدودیت[2]های زیر بر روی درخواست‌های محدوده بایت اعمال می‌شود:

۱. برچسب‌های اصیل نباید برای درخواست‌های محدوده بایت که مطابق با قطعه‌ها یا زیرقطعه‌ها نیست، درخواست شوند.

1 - Switching
2 - Restriction

۲. اگر زیرقطعه‌ها استفاده شوند، یک برچسب اصیل جدا به ازای هر زیرقطعه را می‌توان با استفاده از قواعد نحوی محدوده بایت بازیابی کرد.

۶ رمزگذاری قطعه

۶-۱ قالب قطعه

قطعه‌های رمزگذاری شده ممکن است مطابق با هیچ قالب «قطعه رسانه» تعریف شده در استاندارد ISO/IEC 23009-1:2012 نباشد. تمام تعاریف قالب «قطعه رسانه» و الزامات استاندارد ISO/IEC 23009-1:2012 برای «قطعه‌های رسانه» رمزگذاری نشده به‌کار می‌رود که مطابق با نوع MIME مشخص شده در پارامتر @mimeType مناسب مشخص شده در MPD است.

۶-۲ سامانه‌های کلید

۶-۲-۱ کلیات

URIهای بردارهای مقداردهی اولیه و کلیدها با استفاده از سامانه‌های کلید توسط **License**@keySystemUri شناسایی می‌شوند. اگر عنصر **License** وجود نداشته باشد، تمام URL ها در عناصر **CryptoPeriod** و **CryptoTimeline** باید URLهای HTTP(S) باشند و درخواست موفقیت‌آمیز GET با این URLها باید بردارهای مقداردهی اولیه و کلیدها را در قالب دودویی برگرداند که در زیربند ۶-۴ مشخص شده است.

۶-۲-۲ سامانه‌های کلید مبتنی بر مجوز

سامانه‌های کلید اختصاصی ممکن است برای مقررکردن URNهای اختیاری استفاده شوند. بعضی از اینها ممکن است به اطلاعات مجوز بیشتری نیاز داشته باشند. سامانه‌های کلید که به اطلاعات مجوز نیاز دارند باید از **License**@keyLicenseUrlTemplate برای بازیابی مجوز استفاده کنند. قالب مجوز مخصوص سامانه است و در این استاندارد تعریف نمی‌شود.

مجوزهای مختلف مطابق با URIهای کلید مختلف می‌تواند وجود داشته باشد، بنابراین، **License**@keyLicenseUrlTemplate ممکن است برای مدت‌رمزهای مختلف، نتایج مختلفی را به دست آورند. متغیرهای جایگزین $Number$ و $Time$ استفاده شده در این الگو همانند متغیرها در مدت‌رمز متناظر هستند.

متغیر جایگزین افزوده، $KeyUri$، را می‌توان در این الگو استفاده کرد. این متغیر قالب URI دارد. مقدار آن به عنوان مقدار URI کلید برای مدت‌رمز معین تعریف می‌شود (برای مثال، @keyUriTemplate پس از توسعه متغیرهای جایگزین)

یادآوری- تعاریف بالا بدین معنا هستند که برای هر مدت‌رمز، keyUriTemplate@ ابتدا استخراج می‌شود و سپس استخراج keyLicenseUrlTemplate@ انجام می‌شود.

۶-۳ سامانه‌های رمزگذاری

۶-۳-۱ کلیات

قطعه‌های رسانه باید با استفاده از سامانه رمزگذاری، رمزگذاری شوند که توسط خصیصه **SegmentEncryption**@schemeIdUri مشخص می‌شوند.

مقداردهی اولیه، نمایه و قطعه‌های سودهی جریان بیت نباید رمزگذاری شوند.

هر الحاق[1] شامل قطعه‌های رمزگذاری شده باید پس از رمزگشایی، به کاربرده شود.

پیاده‌سازی سامانه رمزگذاری مناسب ضروری است، بنابراین کارخواهی که الگوریتم مشخص شده در **SegmentEncryption**@schemeIdUri را پیاده‌سازی نمی‌کند توصیه نمی‌شود که هیچ‌یک از قطعه‌های رسانه رمزگذاری‌شده را نمایش دهد.

کارخواه باید طرح رمزگذاری AES-128 CBC مشخص شده در زیربند ۶-۳-۲ را پیاده‌سازی کند.

۶-۳-۲ سامانه رمزگذاری AES-128 CBC

سامانه رمزگذاری قطعه - کامل AES-128 CBC توسط URN urn:mpeg:dash:sea:aes128-cbc:2013 شناسایی می‌شود. پشتیبانی این طرح برای کارخواهانی که این استاندارد را پیاده‌سازی می‌کنند، اجباری است.

در این الگوریتم، رمز AEC با کلیدهای ۱۲۸- بیتی در حالت CBC استفاده شده است. رمزگذاری باید برای کامل کردن قطعه‌ها استفاده شود. قطعه‌ها باید پشت سر هم طبق مشخصات PKCS7 قرار بگیرند تا ضریبی از ۱۶ بایت شوند، همان‌طور که در RFC 5652 توصیف شده‌است. قطعه‌ها از شروع یک بستک ۱۶- بیتی شروع می‌شوند. این بدین معناست که اگر قطعه‌های رسانه رمز شده از طریق محدوده‌های بایت در دسترس باشند، مرزهای قطعه باید برروی مرزهای ۱۶- بیتی باشد.

CBC فقط در یک قطعه اتفاق می‌افتد؛ در شروع هر قطعه، رمزگذاری با استفاده از بردار مقداردهی اولیه و کلید کاربردپذیر، بار دیگر شروع می‌شود.

1 - Concatenation

۶-۳-۳ سامانه رمزگذاری AES-128 GCM

سامانه رمزگذاری قطعه-کامل AES-128 GCM توسط URN urn:mpeg:dash:sea:aes128-gcm:2013 شناسایی می‌شود. پشتیبانی برای این طرح برای کارخواهانی که این استاندارد را پیاده‌سازی می‌کنند، اختیاری است.

در این الگوریتم، رمز AES در حالت GCM با بردارهای مقداردهی اولیه ۹۶- بیتی و برچسب‌های اصالت‌سنجی ۱۲۸- بیتی استفاده می‌شود. رمزگذاری باید در تکمیل قطعه‌ها استفاده شود.

ترکیب واحد کلید و بردار مقداردهی اولیه باید فقط یک‌بار در طی دوره کامل استفاده شود. در نتیجه، مدت‌رمز در این سامانه رمزگذاری باید فقط شامل یک قطعه واحد باشد و در دوره زمانی نباید ترکیبات یکسان کلید/IV وجود داشته باشد.

برچسب اصالت‌سنجی به بایت آخر قطعه الحاق می‌شود (یعنی، قطعه رمزگذاری‌شده، @authTagLength بایت بلندتر از قطعه رمزگذاری‌نشده است).

۶-۴ مدت‌رمزها

۶-۴-۱ کلیات

هر قطعه رسانه به صفر یا یک مدت‌رمز مرتبط می‌شود[1]؛ قطعه‌هایی که مدت‌رمزی ندارند که مرتبط با آنها باشد، نباید رمزگذاری شود. در یک مدت‌رمز، قطعه‌ها با یک زوج کلید/IV همانند رمزگذاری می‌شوند. خصوصیت‌های یک مدت‌رمز عبارتند از: یک کلید، یک بردار مقداردهی اولیه، اولین شماره قطعه و آخرین شماره قطعه.

یادآوری- مدت زمان مدت‌رمز با واحد قطعه سنجیده می‌شود و نه با واحد زمان. بنابراین هیچ الزامی برای قطعه‌ها که مدت زمان ثابتی داشته باشند، وجود ندارد.

۶-۴-۲ تخصیص قطعه‌ها به مدت‌رمزها

عنصر واحد CryptoPeriod مطابق با مدت‌رمز واحد، شامل قطعه‌های @numSegments است و با قطعه‌های @startOffset از پایان مدت‌رمز قبلی شروع می‌شود. اگر این مدت‌رمز، اولین مدت در طی این دوره باشد، @startOffset به شروع دوره زمانی مربوط می‌شود. یک عنصر CryptoPeriod با @numSegments = D و اولین شماره قطعه برابر با M متناظر با مدت‌رمز CP(M,D) است.

برای مدت‌رمز CP(M,D)، قطعه‌های S(M)، S(M+1) و... S(M+D-1) با ترکیب یکسان کلید/IV ، $K_{CP(M,D)}$ و $IV_{CP(M,D)}$ رمزگذاری می‌شوند.

1 - Associate

اگر به‌طور صریح نشانک‌دهی نشوند، قواعد استخراج کلید و IV در قسمت پایین استفاده می‌شود.

برای استخراج مدت‌رمزها CryptoTimeline@numCryptoPeriods از CryptoTimeline واحدی استفاده می‌شود؛ هر کدام شامل قطعه‌های CryptoTimeline@numSegments است. اولین مدت‌رمز در CryptoTimeline، قطعه‌های @firstStartOffset پس از پایان مدت‌رمز قبلی است. اگر این اولین مدت‌رمز، اولین در طی این مدت زمانی باشد، @firstStartOffset به شروع مدت زمانی، مربوط است.

برای عنصر CryptoTimeline با اولین شماره قطعه برابر با M، @numCryptoPeriods = N و @numSegments = D برای $0 \le k \le N$، k-اُمین مدت‌رمز تولیدشده با استفاده از این عنصر CryptoTimeline، برابر با CP(M + k×D, D) است.

اگر CryptoPeriod یا CryptoTimeline، آخرین عنصر این دوره زمانی باشد و مدت زمان مدت‌رمز به‌طور صریح توسط CryptoTimeline@numSegments یا CryptoPeriod@numSegments بیان نشود، فرض می‌شود که مدت‌رمز جاری تا انتهای دوره زمانی ادامه می‌یابد. یادآوری می‌شود در مورد CryptoTimeline، بدین معناست که فقط یک مدت‌رمز درون چنین CryptoTimelineایی وجود دارد.

اگر CryptoPeriod و CryptoTimeline نباشند، هیچ قطعه‌ای نباید رمزگذاری شود.

هیچ‌یک از قطعه‌هایی که با استفاده از قواعد این زیربند، با مدت‌رمز مرتبط نیستند، نباید رمزگذاری شوند.

۶-۴-۳ استخراج کلید

۶-۴-۳-۱ کلیات

URI کلید برای بازیابی منبع کلید استفاده می‌شود. باید یک URI مرتبط با مدت‌رمز داده شده، وجود داشته باشد.

URIایی که مکان کلید را شناسایی می‌کند، برای هر مدت‌رمز باید یک‌بار استخراج شود.

کلید و بردار مقداردهی اولیه باید هر دو قبل از شروع پنجره دسترس‌پذیری اولین قطعه مدت‌رمز، کمینه به مدت @earlyAvailability ثانیه و تا انتهای پنجره دسترس‌پذیری آخرین قطعه، در دسترس باشند. این بدین معنی است که در مورد همه‌پخشی زنده، ضمانت می‌شود که ترکیب کلید و بردار مقداردهی اولیه، کمینه @earlyAvailability ثانیه جلوتر از زمان در دسترس باشد.

URI کلید از خصیصه @keyUriTemplate ساخته می‌شود که این ساخته شدن با استفاده از قواعد نحوی و جانشینی متغیر طبق تعریف استاندارد ISO/IEC 23009-1:2012, 5.3.9.4.4 است. استفاده از متغیرهای جانشینی در الگو، الزامی نیست، بنابراین URIهای واحد می‌توانند در @keyUriTemplate مشخص شوند.

یادآوری- هنگامی‌که جانشینی متغیر الگو برای ساختن URI کلید برای مدت‌رمز CP(i,d) استفاده می‌شود، مقدار $Number$ برابر با i و مقدار $Time$ برابر با مقدار SegmentTimeline@numSegments متناظر با S(i) است.

توصیه می‌شود در URIهای کلید به جای HTTP از HTTPS استفاده شود. برای این منظور، به هیچ‌وجه استفاده از HTTP ترغیب نمی‌شود[1].

۶-۴-۳-۲ قالب کلید

کلید همیشه در قالب دودویی است، به این معنی که کلید توسط دنباله‌ای از بایت‌ها با طول داده شده توسط SegmentEncryption@keyLength، نمایش داده می‌شود.

اگر URI کلید، یک HTTP(S) URL باشد، محتوای بدنه پیام پاسخ HTTP باید فقط شامل SegmentEncryption@keyLength بایت باشد و MIME type application/octet-stream داشته باشد.

۶-۴-۴ استخراج IV

۶-۴-۴-۱ کلیات

مقدار IV مدت‌رمز که توسط عنصر CryptoPeriod تعریف می‌شود باید با استفاده از سازوکار زیر استخراج شود:

۱. اگر CryptoPeriod@IV موجود باشد، مقدارش برابر با IV و با قالب تعریف شده در زیربند ۶-۴-۴-۳ است.
۲. اگر CryptoPeriod@ivUriTemplate موجود باشد، این URI برای استخراج IV استفاده می‌شود.
۳. اگر هیچ‌یک از CryptoPeriod@IV و CryptoPeriod@ivUriTemplate موجود نباشند، پیاده‌سازی باید IV را از شماره قطعه طبق تعریف در زیربند ۶-۴-۴-۲، استخراج کند.

مقدار IV مدت‌رمز استخراج شده از CryptoTimeline باید به صورت زیر استخراج شود:

۱. اگر CryptoTimeline@ivUriTemplate استفاده شود، این URI برای استخراج IV استفاده می‌شود.
۲. در غیر این‌صورت پیاده‌سازی باید IV را از شماره قطعه طبق تعریف زیربند ۶-۴-۴-۲، استخراج کند.

۶-۴-۴-۲ استخراج IV از شماره قطعه

اگر مقدار **SegmentEncryption**@ivEncryptionFlag برابر با «false» باشد و عنصر CryptoPeriod استفاده شود، شماره قطعه باید به‌عنوان مقدار IV یعنی $IV_{CP(M,D)}$=SN استفاده شود.

1 - Discourage

اگر مقدار **SegmentEncryption**@ivEncryptionFlag برابر با «false» باشد و عنصر CryptoTimeline استفاده شود، حاصل‌جمع شماره قطعه و @ivBase باید به‌عنوان مقدار IV یعنی IVCP(M,D)=SN + ivBase استفاده شود. یادآوری می‌شود که مقدار پیش‌فرض @ivBase برابر با ۰ است، بنابراین اگر @ivBase موجود نباشد، $IV_{CP(M,D)}$=SN.

اگر مقدار **SegmentEncryption**@ivEncryptionFlag برابر با «true» باشد، IVهای رمزگذاری‌شده با ECB استفاده خواهد شد. این روش در پیوست C از استاندارد NIST 800-38A توصیف می‌شود و کاربرد آن در این استاندارد، در زیر تعریف می‌شود.

اگر مقدار **SegmentEncryption**@ivEncryptionFlag برابر با «true» باشد و عنصر CryptoPeriod استفاده شود، IV باید مقدار رمزگذاری‌شده با ECB از شماره قطعه باشد. برای مثال، هنگامی‌که رمزگذاری AES-128 استفاده می‌شود (در هر حالت)، ($IV_{CP(M,D)}$= AES(SN, $K_{CP(M,D)}$).

اگر مقدار **SegmentEncryption**@ivEncryptionFlag برابر با «true» باشد و عنصر CryptoTimeline استفاده شود، IV برابر است با حاصل‌جمع شماره قطعه و @ivBase که رمزگذاری‌شده با ECB است. برای مثال، هنگامی‌که رمزگذاری AES-128 استفاده می‌شود (در هر حالت)، ($IV_{CP(M,D)}$= AES(SN + ivBase, $K_{CP(M,D)}$).

اگر مقدار **SegmentEncryption**@ivEncryptionFlag برابر با «true» باشد و SegmentEncryption@ivLength کوچکتر از اندازه بستک خروجی از خروجی ECB باشد (برای مثال، هنگامی‌که IVهای ۹۶-بیتی استفاده می‌شوند)، باارزشترین بیت‌های اولین SegmentEncryption@ivLength از خروجی ECB باید به‌عنوان بردار مقداردهی اولیه استفاده شوند.

۶-۴-۴-۳ قالب IV

IV عددی در قالب شانزده شانزدهی است. نمایش دودویی با بیگ-اندین[1] این عدد باید در بافر SegmentEncryption@ivLength بایتی قرار گیرد و (در سمت چپ) با صفر خالی گذاشته شود (برای مثال، بایت‌ها با مقدار شانزده شانزدهی 0x00). اگر IV از شماره قطعه‌ای که به‌عنوان IV استفاده می‌شود، استخراج شود، باید در چنین میان‌گیری قرار گیرد و (در سمت چپ) با صفر خالی گذاشته شود.

هنگامی‌که @ivUriTemplate استفاده می‌شود، محتوای پاسخ HTTP به HTTP GET با IV URL باید فقط شامل تعداد SegmentEncryption@ivLength بایت باشد و MIME type application/octet-stream داشته باشد.

---

1 - Big-endian

باارزش‌ترین مقدار بامعنا در یک دنباله که در کوچک‌ترین آدرس موجود ذخیره می‌شود.

۶-۴-۵ استخراج ADD

برای عنصر CryptoPeriod، ADD توسط مقدار CryptoPeriod@aad داده می‌شود.

برای عنصر CryptoTimeline، شماره قطعه و aadBase@ برای استخراج ADD استفاده می‌شوند، یعنی، $AAD_{CP(M,D)}=SN + aadBase$

۶-۵ افزودن رمزگذاری جدید و سامانه‌های کلید

این استاندارد موارد زیر را تعریف می‌کند: الف) نشانک‌دهی خصوصیت‌های مدت‌رمز، ب) نشانک‌دهی خصوصیت‌های سامانه کلید و رمزگذاری و ج) سامانه‌های کلید و رمزگذاری اجباری. سامانه‌های کلید و رمزگذاری اجباری که به ترتیب در زیربندهای ۶-۲-۲ و ۶-۳-۲ تعریف شده‌اند یک خط مبنا را در اختیار قرار می‌دهند. تضمین می‌شود که این خط مبنا تعامل‌پذیر باشد.

سامانه‌های کاربر تعریف‌شده و بنابراین سامانه‌های رمزگذاری اختیاری و/ یا سامانه‌های کلید را می‌توان با استفاده از مقادیر مختلف URLها در encryptionSystemUrn@ و keySystemUrn@ اضافه کرد. مثال این سامانه در زیربند ج-۴ فراهم می‌شود. کارخواهی که این موارد را پیاده‌سازی نمی‌کند، می‌تواند قطعه‌های رمزگذاری‌شده و رمزگذاری‌نشده تشخیص دهد، اما نمی‌تواند قطعه‌های رسانه رمزگذاری‌شده را نشان دهد.

دو سازوکار توسعه اختیاری که با این قسمت از ویژگی فراهم شده است، مجوزها و توسعه‌پذیری[1] XML می‌باشند. keyLicenseUrlTemplate@ را می‌توان برای بازیابی اطلاعاتی استفاده کرد که برای معرفی سامانه کلیدی ضروری هستند، در حالی‌که استفاده از عناصر از فضاهای نام مختلف در عناصر SegmentEncryption، CryptoPeriod و CryptoTimeline، افزودن اطلاعات کاربر تعریف‌شده را اجازه می‌دهد.

۷ اصالت‌سنجی قطعه

۷-۱ کلیات

URLهای برچسب اصالت‌سنجی از طریق MPD و با استفاده از عنصر ContentAuthenticity فراهم می‌شوند. برچسب‌های اصالت‌سنجی ممکن است برای (زیر)قطعه‌های رسانه و همچنین برای قطعه‌های سودهی جریان بیت، شاخص و مقداردهی اولیه فراهم شوند.

اگر محافظت محتوا استفاده شود، برچسب‌های اصالت‌سنجی باید برروی قطعه رمزگذاری‌نشده محاسبه شوند. اصالت‌سنجی قطعه اگر با توصیف‌گر SupplementaryProperty استفاده شود، اختیاری است و اگر با توصیف‌گر EssentialProperty استفاده شود، الزامی است.

1 - Extensibility

اگر پاسخ HTTP به درخواست برچسب اصالت‌سنجی خطایی را بازگرداند، کارخواه ممکن است مادامی‌که (زیر)قطعه‌ها خودشان با موفقیت بازیابی شوند، همچنان نمایش را طبق معمول ادامه دهد.

۷-۲ الگوریتم‌ها

۷-۲-۱ SHA-256

الگوریتم چکیده‌ساز[1] SHA-256 در FIPS 180-3 تعریف می‌شود. کاربرد آن توسط مقدار ContentAuthenticity@authSchemeIdUri از urn:mpeg:dash:sea:sha256:2013 نشان داده می‌شود. قالب چکیده، عدد بیگ-اندین در قالب شانزده شانزدهی است.

یادآوری- استاندارد IETF RFC 6234، پیاده‌سازی مرجع SHA-256 را فراهم می‌کند.

۷-۲-۲ HMAC-SHA1

الگوریتم اصالت‌سنجی پیام HMAC-SHA1 در استاندارد IETF RFC 2104 تعریف می‌شود. کاربرد آن توسط مقدار @schemeIdUri از urn:mpeg:dash:sea:hmac-sha1:2013 شناسایی می‌شود. قالب امضاء، عدد بیگ-اندین در قالب شانزده شانزدهی است.

1 - Digest Algorithm

پیوست الف

(الزامی)

طرح XML

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:mpeg:dash:schema:sea:2013"
    attributeFormDefault="unqualified"
    elementFormDefault="qualified" xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns="urn:mpeg:dash:schema:sea:2013" xmlns:dash="urn:mpeg:dash:schema:mpd:2011">

    <!-- Global encryption properties -->

    <xs:complexType name="SegmentEncryption">
        <xs:sequence>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>

        <xs:attribute name="encryptionSystemUrn" type="xs:anyURI" use="required"/>
        <xs:attribute name="keyLength" type="xs:unsignedInt" default="128"/>
        <xs:attribute name="ivLength" type="xs:unsignedInt" default="128"/>
        <xs:attribute name="authTagLength" type="xs:unsignedInt" default="0"/>
        <xs:attribute name="earlyAvailability" type="xs:double" default="1.0"/>
        <xs:attribute name="ivEncryptionFlag" type="xs:boolean" default="false"/>
        <xs:anyAttribute namespace="##other" processContents="lax"/>

    </xs:complexType>

    <xs:complexType name="License">
        <xs:sequence>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="keySystemUrn" type="xs:anyURI" use="required"/>
        <xs:attribute name="keyLicenseUrlTemplate" type="xs:anyURI"/>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>

    <!-- Cryptoperiod signaling -->

    <xs:complexType name="CryptoPeriodType">
        <xs:sequence>
            <xs:any namespace="##other" processContents="lax"
                    minOccurs="0" maxOccurs="unbounded"/>
        </xs:sequence>
        <xs:attribute name="numSegments" type="xs:unsignedLong" default="1"/>
        <xs:attribute name="keyUriTemplate" type="xs:anyURI" use="required"/>
        <xs:attribute name="ivUriTemplate" type="xs:anyURI"/>
        <xs:anyAttribute namespace="##other" processContents="lax"/>
    </xs:complexType>

    <xs:complexType name="CryptoPeriod">
        <xs:complexContent>
            <xs:extension base="CryptoPeriodType">
                <xs:attribute name="startOffset" type="xs:unsignedLong" default="0"/>
                <xs:attribute name="IV" type="xs:hexBinary"/>
                <xs:attribute name="aad" type="xs:hexBinary"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>
```

```
    <xs:complexType name="CryptoTimeline">
        <xs:complexContent>
            <xs:extension base="CryptoPeriodType">
                <xs:attribute name="firstStartOffset" type="xs:unsignedLong" default="0"/>
                <xs:attribute name="numCryptoPeriods" type="xs:unsignedLong"
                              use="required"/>
                <xs:attribute name="ivBase" type="xs:hexBinary" default="00"/>
                <xs:attribute name="aadBase" type="xs:hexBinary" default="00"/>
            </xs:extension>
        </xs:complexContent>
    </xs:complexType>

    <!-- Authenticity signaling -->

    <xs:complexType name="ContentAuthenticity">
        <xs:attribute name="keyUriTemplate" type="xs:anyURI" use="required"/>
        <xs:attribute name="authSchemeIdUri" type="xs:anyURI" use="required"/>
        <xs:attribute name="authUrlTemplate" type="xs:anyURI" use="required"/>
        <xs:attribute name="authTagLength" type="xs:unsignedInt"/>
    </xs:complexType>
</xs:schema>
```

پیوست ب

(آگاهی‌دهنده)

راهنماهای پیاده‌سازی

ب-۱ تحویل کلید

هنگامی‌که سامانه کلید urn:mpeg:dash:sea:keysys:http:2013 استفاده می‌شود، توصیه می‌شود تحویل کلید بر روی کانال امن (برای مثال، HTTP بر روی TLS) انجام شود. در مورد جریان زنده، توصیه می‌شود کلیدها چند ثانیه قبل از قطعه‌ها در دسترس باشند.

برای طرح رمزگذاری urn:mpeg:dash:sea:aes128-cbc:2013، بردارهای مقداردهی اولیه را می‌توان بدون رمزگذاری تحویل داد.

اگر مدت‌رمزهای کوتاه استفاده شود، استفاده از اتصال‌های HTTP دائمی توصیه می‌شود تا از سربار برقراری ارتباط برای هر درخواست کلید جلوگیری کند. اگر IV از طریق URLهای HTTP بازیابی شود، موارد مشابه، برای درخواست‌های IV به‌کاربرده خواهد شد.

ب-۲ رمزگذاری

توصیه می‌شود مدت‌رمزها کوتاه بمانند. مدت‌رمزهای ۲ تا ۱۰ ثانیه، تنظیمات منطقی هستند.

استفاده از بردارهای مقداردهی اولیه غیرقابل پیش‌بینی بسیار توصیه می‌شود، به‌خصوص شروع بسیار قابل پیش‌بینی قطعه‌های رسانه معین برای MPEG-2 TS و ISO-BMFF. هنگامی‌که مقادیر رمزنگاشتی[1] مختلف به‌طور تصادفی تولید می‌شود، توصیه می‌شود تولیدکننده عدد تصادفی یا شبه‌تصادفی امن به‌طور رمزنگاشتی استفاده شود و بهترین شیوه صنعت را دنبال کند. تولیدکننده تشویق می‌شود تا برای توصیه‌ها در خصوص تولید عدد تصادفی امن، با نشریه مخصوص NIST به نام 800-90A مشورت کند.

توصیه می‌شود مقادیر IV یکتا در قطعه، با سامانه‌های رمزگذاری مبتنی بر رمز عمل‌شده در حالت جریان (برای مثال، GCM) استفاده شود. هنگامی‌که سامانه رمزگذاری AES128-GCM استفاده می‌شود، تشویق می‌شود تا برای توصیه‌ها در خصوص استفاده ایمن حالت GCM، با نشریه مخصوص NIST به نام 800-38D مشورت کند.

1 - Cryptographic

برای مدت‌رمزهای کوتاه، توصیه می‌شود که IVهای محلی تولید شود که نقطه مقابل استفاده از HTTP برای درخواست آنها است.

ب-۳ اصالت‌سنجی محتوا

هنگامی‌که برچسب‌های اصالت‌سنجی به‌طور مداوم درخواست می‌شوند، سربار برقراری ارتباط ممکن است با استفاده از ارتباط‌های HTTP دائمی اجتناب شود.

توصیه می‌شود که درخواست‌ها برای برچسب‌های اصالت‌سنجی برای محدوده‌های بایت که قطعه یا زیر قطعه را نشان نمی‌دهد، توسط کارساز HTTP نادیده گرفته شود و خطای 4XX برگردد.

برای درخواست برچسب اصالت‌سنجی به‌خصوص هنگامی‌که از چکیده (برای مثال، SHA) استفاده می‌شود، بهتر است که از HTTPS استفاده شود.

پیوست پ

(آگاهی‌دهنده)

مثال‌های MPD و کاربرد

پ-۱ ویدئو بنا به درخواست[1]

مثال زیر ساده‌ترین فرانامه را شرح می‌دهد. یک فلیم در قطعه‌های ۴ ثانیه‌ای کدبندی می‌شود. ۴ دقیقه اول فیلم رمزگذاری نشده‌است، درحالی‌که باقیمانده فیلم با همان زوج کلید/IV محافظت می‌شود. عنصر CryptoPeriod، URL لازم رابرای بازیابی کلید فراهم می‌کند و شامل IV درون‌خطی است که برای شروع رمزگشایی لازم است. تمام پارامترها به‌طور صریح تهیه می‌شوند، بنابراین نیازی به استخراج ندارد. خدمت اصالت‌سنجی در این مثال پیشنهاد نمی‌شود.

1 - Video on Demand

```
<?xml version="1.0" encoding="UTF-8"?>
<MPD xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:mpeg:dash:schema:mpd:2011 DASH-MPD.xsd"
    xmlns="urn:mpeg:dash:schema:mpd:2011"
    xmlns:sea="urn:mpeg:dash:schema:sea:2013 sea.xsd"
    type="static"
    mediaPresentationDuration="PT6158S"
    minBufferTime="PT1.4S"
    profiles="urn:mpeg:dash:profile:mp2t-simple:2011"
    maxSegmentDuration="PT4S">

    <BaseURL>http://cdn1.example.com/SomeMovie/</BaseURL>
    <BaseURL>http://cdn2.example.com/SomeMovie/</BaseURL>

    <Period id="42" duration="PT6158S">
        <AdaptationSet
            mimeType="video/mp2t"
            codecs="avc1.4D401F,mp4a"
            frameRate="24000/1001"
            segmentAlignment="true"
            subsegmentAlignment="true"
            bitstreamSwitching="true"
            startWithSAP="2"
            subsegmentStartsWithSAP="2">

            <ContentProtection  schemeIdUri="urn:mpeg:dash:sea:enc:2013" >

                <sea:SegmentEncryption
                    schemeIdUri="urn:mpeg:dash:sea:aes128-cbc:2013" />

                <!-- First 4 minutes of the movie are in the clear, -->
                <!-- the rest of the content is encrypted           -->

                <sea:CryptoPeriod
                    startSegment="60"
                    IV="0x1562abcd6798efgh1562abcd6798efgh"
                    keyUriTemplate="https://example.com/keys/xx.cgi?keyId=ef0d2b93"/>

            </ContentProtection>

            <ContentComponent contentType="video" id="481"/>
            <ContentComponent contentType="audio" id="482" lang="en"/>
            <ContentComponent contentType="audio" id="483" lang="es"/>

            <SegmentTemplate
                media="$RepresentationID$ $Number%05d$.ts"
                index="$RepresentationID$.sidx"
```

```
                initialization="$RepresentationID$-init.ts"
                bitstreamSwitching="$RepresentationID$-bssw.ts"
                duration="4"
                startNumber="1"/>
            <Representation id="720kbps"  bandwidth="792000"  width="640"  height="368"/>
            <Representation id="1130kbps" bandwidth="1243000" width="704"  height="400"/>
            <Representation id="1400kbps" bandwidth="1540000" width="960"  height="544"/>
            <Representation id="2100kbps" bandwidth="2310000" width="1120" height="640"/>
            <Representation id="2700kbps" bandwidth="2970000" width="1280" height="720"/>
            <Representation id="3400kbps" bandwidth="3740000" width="1280" height="720"/>
        </AdaptationSet>
    </Period>
</MPD>
```

پ-۲ رویداد[1] زنده با چرخش کلید و اصالت‌سنجی

مثال زیر فرانامه‌ای را شرح می‌دهد که در آن یک رویداد زنده در زمان حقیقی در قطعه‌های ۲- ثانیه‌ای کدبندی می‌شود. چرخش کلید در هر ۸ ثانیه یکبار در مرز قطعه انجام می‌شود. بردار مقداردهی اولیه از شماره قطعه استخراج می‌شود و تقریبا هر ۵۴۴ سال یکبار تکرار می‌شود.

یادآوری می‌شود که همان کلید در زمان مشابه، در تمام نمایش‌ها معتبر است. اگر کسی بخواهد کلیدهای مختلفی را برای نمایش‌های مختلف داشته باشد، توصیه می‌شود توصیف‌گرهای ContentProtection در سطح نمایش قرار گیرند.

کلید URL، برای قطعه رسانه با شماره قطعه برابر با ۴۲ از نمایش شناسانه «۷۲۰kbps»، https://example.com/key.cgi?sn=00000040 خواهد بود. IV عدد رمزگذاری‌شده ۴۰ است.

یادآوری- علی رغم اینکه شماره قطعه ۴۲ می‌شود، کلید و IV را برای قطعه ۴۰ درخواست می‌کنیم، از CryptoTimeline@numSegments می‌دانیم که مدت‌رمز به طول ۴ قطعه است و اولین دوره زمانی در ابتدا شروع می‌شود. بنابراین قطعه ۴۲، سومین قطعه از مدت‌رمز است که در قطعه ۴۰ شروع شده است.

کلید که ۷ ثانیه قبل از اولین قطعه زمان ۴۰ در دسترس است (یعنی HTTP GET با کلید URL برای موفقیت تضمین می‌شود)، می‌تواند با موفقیت بازیابی شود.

اصالت‌سنجی محتوا مبتنی بر HMAC نیز برای تمام قطعه‌ها فراهم می‌شود. ساخت URL امضاء در این مثال یک فرایند دومرحله‌ای است: اولین مرحله، یک URL قطعه است که مطابق قواعد ساخت الگو ساخته می‌شود که در زیربند ۵-۳-۹-۴-۴ از استاندارد ISO/IEC 23009-1:2012 تعریف شده است. URL نتیجه، مطابق قواعد پیوست E استاندارد ISO/IEC 23009-1:2012، به متغیرهای جایگزین URL امضاء تبدیل می‌شود.

برای قطعه رسانه با شماره قطعه ۴۲ از نمایش با شناسانه «۷۲۰kbps»، URL امضاء عبارت زیر خواهد شد:

http://verify.example.com?base=http://cdn2.example.com/SomeMovie/720kbps_00042.ts

در سبک مشابه، قطعه سودهی جریان بیت در نمایش مشابه «۷۲۰kbps»، URL امضاء عبارت زیر خواهد شد: http://verify.example.com?base=http://cdn2.example.come/someMovie/720kbps-bssw.ts

1 - Event

```
<?xml version="1.0" encoding="UTF-8"?>
<MPD xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:mpeg:dash:schema:mpd:2011 DASH-MPD.xsd"
    xmlns="urn:mpeg:dash:schema:mpd:2011"
    xmlns:sea="urn:mpeg:dash:schema:sea:2013 sea.xsd"
    id="a1fd4476-3523-4a1d-99e2-472ae55eb343"
    type="dynamic"
    availabilityStartTime="2012-07-07T07:07:07"
    minBufferTime="PT1.4S"
    profiles="urn:mpeg:dash:profile:mp2t-simple:2011"
    maxSegmentDuration="PT2S"
    minimumUpdatePeriod="PT3600S"
    timeShiftBufferDepth="PT240S">

    <BaseURL>http://cdn1.example.com/SomeMovie/</BaseURL>
    <BaseURL>http://cdn2.example.com/SomeMovie/</BaseURL>
    <Period id="42" >

        <AdaptationSet
            mimeType="video/mp2t"
            codecs="avc1.4D401F,mp4a"
            frameRate="24000/1001"
            segmentAlignment="true"
            bitstreamSwitching="true"
            startWithSAP="2" >

            <!-- Key/IV combination changes every 8 sec. during the broadcast -->
            <!-- Key files are available 7 sec. ahead of time -->
            <!-- IV is an Segment Number -->
            <ContentProtection schemeIdUri="urn:mpeg:dash:sea:2013" >
                <sea:SegmentEncryption
                    schemeIdUri="urn:mpeg:dash:sea:aes128-cbc:2013"
                    earlyAvailability="7.0" />

                <sea:CryptoTimeline
                    numSegments="4"
                    keyUriTemplate="https://example.com/key.cgi?sn=$Number%08d$" />

            </ContentProtection>

            <!-- HMAC authentication -->
            <SupplementalProperty schemeIdUri="urn:mpeg:dash:sea:auth:2013">
                <sea:ContentAuthenticity
                    authSchemeIdUri="urn:mpeg:dash:sea:hmac-sha1"
                    keyUrlTemplate="https://verify.example.com/key.cgi?keyId=ef0d2b93"
                    authUrlTemplate= "http://verify.example.com?base=$base$" />
            </SupplementalProperty>

            <ContentComponent contentType="video" id="481"/>
            <ContentComponent contentType="audio" id="482" lang="en"/>
            <ContentComponent contentType="audio" id="483" lang="es"/>

            <SegmentTemplate
                media="$RepresentationID$ $Number%08d$.ts"
                bitstreamSwitching="$RepresentationID$-bssw.ts"
                duration="4" startNumber="1"/>
            <Representation id="720kbps"  bandwidth="792000"  width="640"  height="368"/>
            <Representation id="1130kbps" bandwidth="1243000" width="704"  height="400"/>
            <Representation id="1400kbps" bandwidth="1540000" width="960"  height="544"/>
            <Representation id="2100kbps" bandwidth="2310000" width="1120" height="640"/>
            <Representation id="2700kbps" bandwidth="2970000" width="1280" height="720"/>
            <Representation id="3400kbps" bandwidth="3740000" width="1280" height="720"/>
        </AdaptationSet>
    </Period>
</MPD>
```

پ-۳ استفاده از حفاظت محتوای ISO-BMFF اختیاری با اصالت‌سنجی محتوا

مثال زیر فرانامه ویدئوی مورد تقاضایی را شرح می‌دهد که صدا و تصویر با طرح‌های حفاظت محتوای مشخص نشده مختلف، محافظت می‌شود. این مثال یک قطعه واحد در هر نمایش دارد. بنابراین با استفاده از زیرقطعه‌ها در دسترس است (از این‌رو از محدوده‌های بایت استفاده می‌کند).

توصیف‌گر اصالت‌سنجی محتوا، الگوی URL برای بازیابی چکیده‌های SHA-256 از هر زیرقطعه فراهم می‌کند و از قواعد ساخت URL محدوده بیت که در پیوست E استاندارد ISO/IEC 23009-1 مشخص شده است، استفاده می‌کند.

فرض کنید زیرقطعه رسانه که در دسترس است، اولین زیرقطعه از یک قطعه با URL مقابل است: http://cdn.example.com/movie23453235/video1024.mp4 و محدوده بایت متناظر، ۰-۲۳۴۵۶ است و URL چکیده عبارت زیر خواهد بود:

https://verify.example.com?base=http://cdn.example.com/movie23453235/video1024.mp4&range=0-23456

یادآوری می‌شود که SHA-256 به‌طور جداگانه برای هر زیرقطعه رمزگذاری‌نشده محاسبه می‌شود.

```
<?xml version="1.0" encoding="UTF-8"?>
<MPD
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns="urn:mpeg:dash:schema:mpd:2011"
    xmlns:drm="http://example.net/052011/drm"
    xmlns:sea="urn:mpeg:dash:schema:sea:2013 sea.xsd"
    xsi:schemaLocation="urn:mpeg:dash:schema:mpd:2011 DASH-MPD.xsd"
    type="static"
    mediaPresentationDuration="PT3256S"
    minBufferTime="PT10.00S"
    profiles="urn:mpeg:dash:profile:isoff-on-demand:2011">

    <BaseURL>http://cdn.example.com/movie23453235/</BaseURL>
    <Period>
        <!-- Audio protected with a specified license -->
        <AdaptationSet  mimeType="audio/mp4" codecs="mp4a.0x40" lang="en"
            subsegmentStartsWithSAP="1"
            subsegmentAlignment="true">
            <ContentProtection schemeIdUri="http://example.net/052011/drm">

<drm:License>http://MoviesSP.example.com/protect?license=kljklsdfiowek</drm:License>

<drm:Content>http://MoviesSP.example.com/protect?content=oyfYvpo8yFyvy</drm:Content>
            </ContentProtection>

            <Representation id="1" bandwidth="64000">
                <BaseURL>audio/en/64.mp4</BaseURL>
            </Representation>
        </AdaptationSet>

        <!-- Video protected with a specified license -->
        <AdaptationSet  mimeType="video/mp4" codecs="avc1"
            subsegmentAlignment="true" subsegmentStartsWithSAP="2">
            <ContentProtection schemeIdUri="http://example.net/052011/drm">
                <drm:License>
                    http://MoviesSP.example.com/protect?license=jfjhwlsdkfiowkl
                </drm:License>
                <drm:Content>
                    http://MoviesSP.example.com/protect?content=mslkfjsfiowelkfl
                </drm:Content>
            </ContentProtection>
            <BaseURL>video/</BaseURL>
            <Representation id="6" bandwidth="256000" width="320" height="240">
                <BaseURL>video256.mp4</BaseURL>
            </Representation>
            <Representation id="7" bandwidth="512000" width="320" height="240">
                <BaseURL>video512.mp4</BaseURL>
            </Representation>
            <Representation id="8" bandwidth="1024000" width="640" height="480">
                <BaseURL>video1024.mp4</BaseURL>
            </Representation>
```

```
        </AdaptationSet>

        <!-- SHA-256 digests is available for all (sub)segments -->
        <SupplementalProperty schemeIdUri="urn:mpeg:dash:sea:auth:2013">
            <sea:ContentAuthenticity
                authSchemeIdUri="urn:mpeg:dash:sea:sha256"
                authUrlTemplate=
"https://verify.example.com?base=$base$&amp;range=$first$-$last$" />
        </SupplementalProperty>
    </Period>
</MPD>
```

ج-۴ استفاده از انتقال کلید مبتنی بر مجوز[1]

مثال زیر همانند مثال در زیربند ج-۱ است، اما از یک سامانه کلید اختصاصی استفاده می‌شود.

قطعه‌های رسانه در زیربند ج-۱ و در این مثال به‌طور دقیق همانند هستند؛ بنابراین سامانه کلید SomeDRM که در این مثال استفاده شده است با استفاده از روش اختصاصی، URIهای کلید را به مقادیر کلید ۱۶-بایتی ترجمه می‌کند. SomeDRM با استفاده از اطلاعات مجوز، مقداردهی اولیه می‌شود که با استفاده از @keyLicenseUrlTemplate بازیابی شده است.

استفاده بیش از یک سامانه کلید به‌طور همزمان امکان‌پذیر است، به شرطی‌که روش‌های رمزگذاری واقعی، کلیدها و پارامترهای دیگر با هم جور باشند[2]. در پایین، با OtherDRM با استفاده از روش اختصاصی مختلف مقررکردن URL کلید، شرح داده می‌شود در حالی‌که از پارامترهای رمزگذاری مشابه استفاده می‌شود.

```
<?xml version="1.0" encoding="UTF-8"?>
<MPD xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="urn:mpeg:dash:schema:mpd:2011 DASH-MPD.xsd"
    xmlns="urn:mpeg:dash:schema:mpd:2011"
    xmlns:sea="urn:mpeg:dash:schema:sea:2013 sea3.xsd"
    xmlns:somedrm="urn:com:vendor:somedrm:2013 somedrm.xsd"
    type="static"
    mediaPresentationDuration="PT6158S"
    minBufferTime="PT1.4S"
    profiles="urn:mpeg:dash:profile:mp2t-simple:2011"
    maxSegmentDuration="PT4S">

    <BaseURL>http://cdn1.example.com/SomeMovie/</BaseURL>
    <BaseURL>http://cdn2.example.com/SomeMovie/</BaseURL>

    <Period id="42" duration="PT6158S">
        <AdaptationSet
            mimeType="video/mp2t"
            codecs="avc1.4D401F,mp4a"
            frameRate="24000/1001"
            segmentAlignment="true"
            subsegmentAlignment="true"
            bitstreamSwitching="true"
            startWithSAP="2"
            subsegmentStartsWithSAP="2">

            <ContentProtection  schemeIdUri="urn:mpeg:dash:sea:2013" >

                <!--  Segment encryption used with proprietary key system  -->
                <!--  The key system adds its own proprietary information  -->
                <sea:SegmentEncryption
                    schemeIdUri="urn:mpeg:dash:sea:aes128-cbc:2013" />
```

1 - License-based
2 - Match

```
            <sea:License
                keySystemUri="com:vendor:somedrm:2013"
                keyLicenseUrlTemplate="https://example.com/keys/sdrm-license.cgi" >
                <somedrm:Session
                    sessionId="https://example.com/session.cgi?cid=f23f28c0" />
            </sea:License>

            <sea:License
                keySystemUri="com:vendor:otherdrm:2013"
                keyLicenseUrlTemplate="https://example.com/keys/odrm-license.cgi" >
            </sea:License>

            <!-- First 4 minutes of the movie are in the clear, -->
            <!-- the rest of the content is encrypted           -->

            <sea:CryptoPeriod
                startSegment="60"
                IV="0x1562abcd6798efgh1562abcd6798efgh"
                keyUriTemplate="urn:uuid:e5817e50-cf5e-48e4-ae71-055ece558411"/>
        </ContentProtection>

        <ContentComponent contentType="video" id="481"/>
        <ContentComponent contentType="audio" id="482" lang="en"/>
        <ContentComponent contentType="audio" id="483" lang="es"/>

        <SegmentTemplate
            media="$RepresentationID$_$Number%05d$.ts"
            index="$RepresentationID$.sidx"
            initialization="$RepresentationID$-init.ts"
            bitstreamSwitching="$RepresentationID$-bssw.ts"
            duration="4"
            startNumber="1"/>
        <Representation id="720kbps"  bandwidth="792000"  width="640"  height="368"/>
        <Representation id="1130kbps" bandwidth="1243000" width="704"  height="400"/>
        <Representation id="1400kbps" bandwidth="1540000" width="960"  height="544"/>
        <Representation id="2100kbps" bandwidth="2310000" width="1120" height="640"/>
        <Representation id="2700kbps" bandwidth="2970000" width="1280" height="720"/>
        <Representation id="3400kbps" bandwidth="3740000" width="1280" height="720"/>
    </AdaptationSet>
  </Period>
</MPD>
```