INSO

11947-9

1st. Edition

2015

جمهوری اسلامی ایران
Islamic Republic of Iran

سازمان ملی استاندارد ایران
Iranian National Standardization Organization

استاندارد ملی ایران
۱۱۹۴۷-۹
چاپ اول
۱۳۹۳

فناوری اطلاعات - فناوری‌های سامانه‌های گروه متخصصان تصویر متحرک (نماوادیس) (MPEG)- قسمت ۹: رمزگذاری مشترک جریان‌های انتقال MPEG-2

Information technology — MPEG systems technologies — Part 9: Common encryption of MPEG-2 transport streams

ICS: 35.040

به نام خدا

آشنایی با سازمان ملی استاندارد ایران

مؤسسهٔ استاندارد و تحقیقات صنعتی ایران به موجب بند یک مادهٔ۳ قانون اصلاح قوانین و مقررات مؤسسهٔ استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱ تنها مرجع رسمی کشور است که وظیفه تعیین، تدوین و نشر استانداردهای ملی (رسمی) ایران را به عهده دارد.

نام موسسه استاندارد و تحقیقات صنعتی ایران به موجب یکصد و پنجاه و دومین جلسه شورای عالی اداری مورخ ۹۰/۶/۲۹ به سازمان ملی استاندارد ایران تغییر و طی نامه شماره ۲۰۶/۳۵۸۳۸ مورخ ۹۰/۷/۲۴ جهت اجرا ابلاغ شده است .

تدوین استاندارد در حوزه های مختلف در کمیسیون های فنی مرکب از کارشناسان سازمان ، صاحب نظران مراکز و مؤسسات علمی، پژوهشی، تولیدی و اقتصادی آگاه و مرتبط انجام می شود وکوششی 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 وارد کنندگان، مراکز علمی و تخصصی، نهادها، سازمان های دولتی و غیر دولتی حاصل می شود .پیش نویس استانداردهای ملی ایران برای نظرخواهی به مراجع ذی نفع و اعضای کمیسیون های فنی 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 می شود.

پیش نویس استانداردهایی که مؤسسات و سازمان های علاقه مند و ذی صلاح نیز با رعایت ضوابط تعیین شده تهیه می کنند درکمیتهٔ ملی طرح و بررسی و درصورت تصویب، به عنوان استاندارد ملی ایران چاپ و منتشر می شود .بدین ترتیب، استانداردهایی ملی تلقی می شوند که بر اساس مفاد نوشته شده در استاندارد ملی ایران شمارهٔ ۵ تدوین و در کمیتهٔ ملی استاندارد مربوط که سازمان ملی استاندارد ایران تشکیل می‌دهد به تصویب رسیده باشد.

سازمان ملی استاندارد ایران از اعضای اصلی سازمان بین المللی استاندارد (ISO)[1] ،کمیسیون بین المللی الکتروتکنیک (IEC)[2] و سازمان بین المللی اندازه شناسی قانونی (OIML)[3] است و به عنوان تنها رابط[4] کمیسیون کدکس غذایی (CAC)[5] در کشور فعالیت می کند. در تدوین استانداردهای ملی ایران ضمن توجه به شرایط کلی و نیازمندی های خاص کشور ، از آخرین پیشرفت های علمی، فنی و صنعتی جهان و استانداردهای بین‌المللی بهره‌گیری می‌شود .

سازمان ملی استاندارد ایران می تواند با رعایت موازین پیش بینی شده در قانون، برای حمایت از مصرف کنندگان، حفظ سلامت و ایمنی فردی و عمومی، حصول اطمینان از کیفیت محصولات و ملاحظات زیست محیطی و اقتصادی، اجرای بعضی از استانداردهای ملی ایران را برای محصولات تولیدی داخل کشور و/یا اقلام وارداتی، با تصویب شورای عالی استاندارد، اجباری نماید. سازمان می تواند به منظور حفظ بازارهای بین المللی برای محصولات کشور، اجرای استاندارد کالاهای صادراتی و درجه‌بندی آن را اجباری نماید. همچنین برای اطمینان بخشیدن به استفاده کنندگان از خدمات سازمان ها و مؤسسات فعال در زمینهٔ مشاوره، آموزش، بازرسی، ممیزی و صدورگواهی سیستم های مدیریت کیفیت و مدیریت زیست‌محیطی، آزمایشگاه ها و مراکز کالیبراسیون (واسنجی) وسایل سنجش، سازمان ملی استاندارد ایران این گونه سازمان ها و مؤسسات را بر اساس ضوابط نظام تأیید صلاحیت ایران ارزیابی می کند و در صورت احراز شرایط لازم، گواهینامهٔ تأیید صلاحیت به آن ها اعطا و بر عملکرد آن ها نظارت می کند. ترویج دستگاه بین المللی یکاها، کالیبراسیون (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 of Legal Metrology (Organisation Internationale de Metrologie Legale)
4 - Contact point
5 - Codex Alimentarius Commission

کمیسیون فنی تدوین استاندارد

«فناوری اطلاعات - فناوری‌های سامانه‌های گروه متخصصان تصویر متحرک (نماوادیس) (MPEG)- قسمت ۹: رمزگذاری مشترک جریان‌های انتقال MPEG-2»

رئیس:	**سمت و/یا نمایندگی**
یزدیان ورجانی، علی (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس و مسئول مرکز آپا تربیت مدرس
دبیر:	
قسمتی، سیمین (فوق لیسانس مهندسی فناوری اطلاعات)	مشاور مرکز آپا تربیت مدرس
اعضا: (اسامی به ترتیب حروف الفبا)	
اسدی‌پویا، سمیرا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیر عامل شرکت مهندسی پویا دانش و کیفیت آوا
شیخ‌الاسلامی، محمد کاظم (دکتری، برق)	عضو هیات علمی دانشگاه تربیت مدرس
شیرازی، مریم (لیسانس فناوری اطلاعات)	کارشناس پژوهشگاه استاندارد
صادقی، مریم (لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس سازمان نظام صنفی رایانه‌ای کشور
طی‌نیا، رضا (فوق لیسانس مهندسی فناوری اطلاعات)	مدیرعامل شرکت مهندسی کاربرد سیستم
فرهاد شیخ احمد، لیلا (فوق لیسانس مهندسی کامپیوتر، نرم‌افزار)	کارشناس حقیقی استاندارد سازمان ملی استاندارد ایران
محمدیان، مصطفی (دکتری، برق)	عضو هیات علمی و معاون پژوهشی دانشکده برق و کامپیوتر
معروف، سینا (لیسانس مهندسی کامپیوتر، سخت‌افزار)	کارشناس سازمان فناوری اطلاعات ایران

فهرست مندرجات

عنوان **صفحه**

پیش‌گفتار

استاندارد «فناوری اطلاعات - فناوری‌های سامانه‌های گروه متخصصان تصویر متحرک (نماوادیس) (MPEG)- قسمت ۹: رمزگذاری مشترک جریان‌های انتقال MPEG-2» که پیش‌نویس آن در کمیسیون‌های مربوط توسط مرکز آپا (آگاهی‌رسانی، امداد و پشتیبانی رخدادهای رایانه‌ای) دانشگاه تربیت مدرس تهیه و تدوین شده است و در سیصد و پنجاه و هفتمین اجلاس کمیته ملی استاندارد فناوری اطلاعات مورخ ۹۳/۱۰/۳۰ مورد تصویب قرار گرفته است، اینک به استناد بند یک ماده ۳ قانون اصلاح قوانین و مقررات موسسه استاندارد و تحقیقات صنعتی ایران، مصوب بهمن ماه ۱۳۷۱، به عنوان استاندارد ملی ایران منتشر می‌شود.

برای حفظ همگامی و هماهنگی با تحولات و پیشرفت‌های ملی و جهانی در زمینه صنایع، علوم و خدمات، استانداردهای ملی ایران در مواقع لزوم تجدید نظر خواهد شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود ، هنگام تجدید نظر در کمیسیون فنی مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدید نظر استانداردهای ملی استفاده کرد.

منبع و ماخذی که برای تهیه این استاندارد مورد استفاده قرار گرفته به شرح زیر است:

ISO/IEC 23001-9: 2014, Information technology — MPEG systems technologies — Part 9: Common encryption of MPEG-2 transport streams

فناوری اطلاعات - فناوری‌های سامانه‌های گروه متخصصان تصویر متحرک (نماوادیس) (MPEG)[1]- قسمت ۹: رمزگذاری مشترک جریان‌های انتقال MPEG-2

۱ هدف و دامنه کاربرد

هدف از تدوین این استاندارد، تعیین قالب رمزگذاری مشترک رسانه برای استفاده در جریان‌های انتقال MPEG-2 است. این قالب رمزگذاری برای استفاده به روشی تعامل‌پذیر با رسانه رمزگذاری‌شده با استفاده از قالب شرح داده شده در ISO/IEC 23001-7 در نظر گرفته می‌شود. این استاندارد تبدیل بین جریان‌های انتقال MPEG-2 رمزگذاری‌شده و فایل‌های قالب فایل رسانه مبتنی بر ISO[2] رمزگذاری‌شده را بدون رمزگذاری مجدد، مجاز می‌داند.

۲ مراجع الزامی

مدارک الزامی زیر حاوی مقرراتی است که در متن این استاندارد ملی ایران به آنها ارجاع داده شده است. بدین ترتیب آن مقررات جزئی از این استاندارد محسوب می‌شوند.

در صورتی که به مدرکی با ذکر تاریخ انتشار ارجاع داده شده باشد، اصلاحیه‌ها و تجدیدنظرهای بعدی آن مورد نظر این استاندارد ملی ایران نیست. در مورد مدارکی که بدون ذکر تاریخ انتشار به آنها ارجاع داده شده است، همواره آخرین تجدیدنظر و اصلاحیه‌های بعدی آنها مورد نظر است.

استفاده از مراجع زیر برای این استاندارد الزامی است:

2-1 Rec. ITU-T H.222.0 | ISO/IEC 13818-1, *Information technology — Generic coding of moving pictures and associated audio information — Part 1: Systems*

2-2 ISO/IEC 13818-7, *Information technology — Generic coding of moving pictures and associated audio information — Part 7: Advanced Audio Coding (AAC).*

2-3 ISO/IEC 14496-10, *Information technology — Coding of audio-visual objects — Part 10: Advanced Video Coding* (technically aligned with Rec. ITU-T H.264)

2-4 ISO/IEC 14496-3, *Information technology — Coding of audio-visual objects — Part 3: Audio*

2-5 ISO/IEC 23001-7, *Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files*

2-6 ISO/IEC 23008-2, *Information technology — High efficiency coding and media delivery in heterogeneous environments — Part 2: High efficiency video coding*

2-7 IETF RFC 1321, *The MD5 Message-Digest Algorithm* , April 1992

1 - Moving Picture Experts Group, Motion Picture Experts Group
2 - ISO base media file format files

2-8 *Advanced Encryption Standard*, Federal Information Processing Standards Publication 197, FIPS-197

2-9 Recommendation of Block Cipher Modes of Operation, NIST, NIST Special Publication 800-38A

۳ اصطلاحات و تعاریف

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

۳-۱ واحد دسترسی (AU) رمزگذاری‌شده

قسمتی از جریان ابتدایی که شامل یک واحد دسترسی است.

یادآوری ۱ – در استانداردهای ISO/IEC 14496-10 و ISO/IEC 23008-2، این موارد، از یک یا چند واحد لایه دسترسی شبکه (NAL)[1] تشکیل شده است.

۴ کوته‌نوشت‌ها

AES	Advanced Encryption Standard (FIPS-197)	استاندارد رمزگذاری پیشرفته (FIPS-197)
AU	Access Unit	واحد دسترسی
CAT	Conditional Access Table (ISO/IEC 13818-1)	جدول دسترسی شرطی (ISO/IEC 13818-1)
CBC	Cipherblock Chaining (NIST 800-38A)	زنجیره‌های قالب‌رمز (NIST 800-38A)
CENC	Common Encryption (ISO/IEC 23001-7)	رمزگذاری مشترک (ISO/IEC 23001-7)
CETS	Common Encryption of MPEG-2 Transport Streams	رمزگذاری مشترک جریان‌های انتقال MPEG-2
CTR	Counter Mode (NIST SP 800-38A)	حالت مقابله (NIST SP 800-38A)
DTS	Decoding Time Stamp (ISO/IEC 13818-1)	رمزگشایی مهر زمانی (ISO/IEC 13818-1)
EAU	Encrypted Access Unit	واحد دسترسی رمزگذاری‌شده
ECM	Entitlement Control Message (ISO/IEC 13818-1)	پیام کنترل حق دسترسی (ISO/IEC 13818-1)
ISO-BMFF	ISO Base Media File Format (ISO/IEC 14496-12)	قالب فایل رسانه مبتنی بر ISO (ISO/IEC 14496-12)
IV	Initialization Vector (NIST SP 800-38A)	بردار مقداردهی اولیه (NIST SP 800-38A)

1 - Network Access Layer

KID	Key Identifier (ISO/IEC 23001-7)	شناسانه کلید (ISO/IEC 23001-7)
MD5	Message-Digest Algorithm (IETF RFC 1321)	الگوریتم چکیده پیام (IETF RFC 1321)
MPEG-2 TS	MPEG-2 Transport Stream (ISO/IEC 13818-1)	جریان انتقال MPEG-2 (ISO/IEC 13818-1)
NAL	Network Access Layer (ISO/IEC 14496-10, ISO/IEC 23008-2)	لایه دسترسی شبکه (ISO/IEC 14496-10، ISO/IEC 23008-2)
PAT	Program Association Table (ISO/IEC 13818-1)	جدول پیمان برنامه (ISO/IEC 13818-1)
PES	Packetized Elementary Stream (ISO/IEC 13818-1)	جریان ابتدایی بسته‌بندی‌شده (ISO/IEC 13818-1)
PID	Packet Identifier (ISO/IEC 13818-1)	شناسانه بسته (ISO/IEC 13818-1)
PMT	Program Map Table (ISO/IEC 13818-1)	جدول نگاشت برنامه (ISO/IEC 13818-1)
PTS	Presentation Time Stamp (ISO/IEC 13818-1)	مهر زمانی ارائه (ISO/IEC 13818-1)
RAP	Random Access Point	نقطه دسترسی تصادفی
VCL	Video Coding Layer (ISO/IEC 14496-10, ISO/IEC 23008-2)	لایه کدگذاری ویدئو (ISO/IEC 14496-10، ISO/IEC 23008-2)

۵ مقدمه

۵-۱ کلیات

طرح رمزگذاری مستقل از محفظه[1] تعامل‌پذیر، اجازه می‌دهد قالب محفظه تغییراتی در محتوای رمزگذاری‌شده‌ی شبکه دهد، بدون این که به گره‌ی پردازشگری که توانایی پشتیبانی و تعامل با مدیریت حقوق دیجیتال (DRM)[2] چندگانه را دارد، نیاز داشته باشد. با توجه به ضرورت پشتیبانی از کارخواه-هایی[3] که از قالب‌های مختلف محفظه استفاده می‌کنند، این قبیل قابلیت‌ها به کاربر نهایی مجاز، اجازه حفاظت محتوای انتها به انتها را از مرحله آماده‌سازی تا استفاده‌ی محتوا می‌دهد.

اگر جریان‌های ابتدایی قسمت‌های رمزگذاری‌شده، یکسان باشند و پارامترهایی که نیاز به پوشینه‌دارسازی مجدد[4] دارند، بدون رمز باشند، امکان پوشینه‌دارسازی مجدد، بدون رمزگذاری مجدد وجود دارد. رمزگذاری جریان بیتی جزئی مشخص‌شده در استاندارد ISO/IEC 23001-7، همتافتگری مجدد

1 - Container-independent
2 - Digital Rights Management
3 - Clients
4 - re-encapsulation

(مالتی‌پلکس مجدد)[1] برخی فایل‌های قالب فایل رسانه مبتنی بر ایزو (ISO-BMFF)[2] را امکان‌پذیر می‌سازد. استاندارد ISO/IEC 23001-7 برای ISO-BMFF تعیین شده است، در حالی که این استاندارد ملی، چارچوب MPEG-2 TS را که کارکرد مشابهی برای استانداردهای فنی (TS) MPEG-2 دارد، ارائه می‌کند. ترکیب ISO/IEC 23001-7 و ISO/IEC 23001-9 پوشینه‌دارسازی مجدد بین محتوای ISO-BMFF و MPEG-2 TS را بدون رمزگذاری مجدد مجاز می‌داند.

۵-۲ نظریه عملیات

در فرضیه اولیه رمزگذاری مشترک، هر واحد دسترسی به طور جداگانه به صورت کامل یا به صورت جزئی رمزگذاری می‌شود. از این جهت، هر واحد دسترسی به دو پارامتر کلید و بردار مقداردهی اولیه نیاز دارد. تفکیک[3] کلید، خارج از دامنه کاربرد این استاندارد است و بستگی به سامانه[4] کلید مورد نظر دارد. چکیده‌ی مورد استفاده در این استاندارد این است که پس از ارائه شناسانه و مجوز کلید، سامانه کلید یک کلید را باز خواهد گرداند. ECM برای انتقال بردارهای مقداردهی اولیه و شناسانه‌های کلید استفاده می‌شود. به منظور امکان رمزگشایی، نیاز است شناسایی شود کدام واحد دسترسی با کدام ترکیب کلید/ IV رمزگذاری شده است. جریان انتقال MPEG-2 (TS) کارکرد سطح انتقال و سطح PES را ارائه می‌کند، برای این کار از فیلد transport_scrambling_control استفاده می‌شود. بنابراین اگر مقدار فیلد transport_scrambling_control برابر ’00‘ باشد، پایه‌بار[5] بسته جریان انتقال، رمز نشده است. در غیر این صورت، پایه‌بار با ترکیب کلید/ IV که با مقدار فیلد transport_scrambling_control در نزدیکترین ECM شناسایی شده، رمزگذاری می‌شود.

یادآوری- با توجه به این که رمزگذاری مشترک به طور جداگانه در هر واحد دسترسی اعمال می‌شود، به احتمال زیاد مقدار فیلد transport_scrambling_control هر واحد دسترسی را تغییر می‌دهد، از این رو ECM به تناوب ظاهر خواهد شد. برای اولین بسته MPEG-2 TS رمزگذاری‌شده بسته PES، تنها ECM قبلی بی‌واسطه، تضمین می‌کند که شامل ترکیب کلید/ IV درست برای واحد دسترسی داده‌شده، است. چرا که scrambling_bits یک فیلد ۲ بیتی است و تنها ۳ وضعیت رمزگذاری دارد.

مجوز خاص فروشنده[6] برای هرگونه عملیات DRM عملی ضروری است. در ISO/IEC 23001-7، این موضوع برای هر DRM در یک یا چند جعبه `pssh` حمل می‌شود. در این استاندارد، اطلاعات مشابه در CETS PSSH PID خصوصی (یک PID در هر سامانه DRM) حمل می‌شود. این موضوع لزوما به این معنی نیست که داده `pssh` باید در کانال اصلی[7] حمل شود، این امر به تصمیم مجری واگذار شده است. پارامترهای مربوط به الگوریتم‌ها از طریق توصیف‌کننده CA_descriptor سیگنال‌دهی می‌شود.

---

1 - Re-multiplexing
2 - ISO base media file format
3 - Resolution
4 - System
5 - Payload

داده‌های کاربر که در مدار یا شبکه حمل می‌شود.

6 - A vendor-specific license
7 - Inband

در ISO/IEC 23001-7 هر شیار جعبه `tenc` خود و بردارهای مقداردهی اولیه (IV) نمونه خاص را دارد. در این استاندارد این موضوع به صورت PID ECM جداگانه پیاده‌سازی می‌شود. اگر ترکیب کلید/ IV مشابهی برای بیش از یک PID استفاده شده باشد (به طور مثال، ترکیب مشابه برای صدا و تصویر)، استفاده از ECM PID مشابه برای تمام شناسانه‌های بسته‌ای (PID) که ترکیب کلید/ IV مشابهی را به اشتراک می‌گذارند، امکان پذیر است. با این حال، این عمل ممکن است پیچیدگی و شکنندگی سامانه را افزایش دهد.

۶ سیگنال‌دهی پارامتر رمزگذاری

۶-۱ CETS ECM

۶-۱-۱ کلیات

در سطح بسیار ابتدایی، CETS ECM (الف) ID کلید و بردار مقداردهی اولیه برای هر حالت transport_scrambling_control و (ب) اعلان چرخش کلید آینده را ارائه می‌کند. در موردی که IV یا/و کلید در هر نمونه تغییر می‌کند، انتظار می‌رود CETS ECM به طور متناوب (ECM در هر AU) ظاهر شود.

از آن جا که ممکن است در وسط بسته PES تغییر کلید و/یا تغییرIV وجود داشته باشد (به طور مثال در موردی که PES چند واحد دسترسی را که برای صدا متداول است، حمل می‌کند)، CETS ECM آفست‌های بایت را در آغاز بایت‌های رمزگذاری‌شده نشان می‌دهد که با جفت کلید/IV مختلف رمزگذاری شده است.

CETS ECM همیشه در یک بسته تنها MPEG-2 TS وجود دارد، بنابراین اندازه cets_ecm نباید بیش از ۱۸۴ بایت باشد. مابقی فیلد سازگاری[1] باید برای اندازه‌های کوچکتر cets_ecm استفاده شود.

1 - Adaptation field

۶-۱-۲ نحو[1]

نحو	شماره بیت‌ها	قالب
cets_ecm(){		
num_states	2	uimbsf
next_key_id_flag	1	bslbf
reserved	3	bslbf
iv_size	8	uismbf
default_key_id	128	uismbf
for (i = 0; i < num_states; i++) {		
transport_scrambling_control	2	bslbf
num_au	6	uismbf
for (j = 0; j < num_au; j++) {		
key_id_flag	1	bslbf
reserved	3	uismbf
au_byte_offset_size	4	bslbf
if (key_id_flag == 1) {		
key_id	128	uismbf
}		
if (au_byte_offset_size > 0) {		
au_byte_offset	N1	uismbf
}		
initialization_vector	N2	uismbf
}		
}		
if (next_key_id_flag == 1) {		
countdown_sec	4	uismbf
reserved	4	bslbf
next_key_id	128	bslbf
}		
}		

۶-۱-۳ معناشناسی[2]

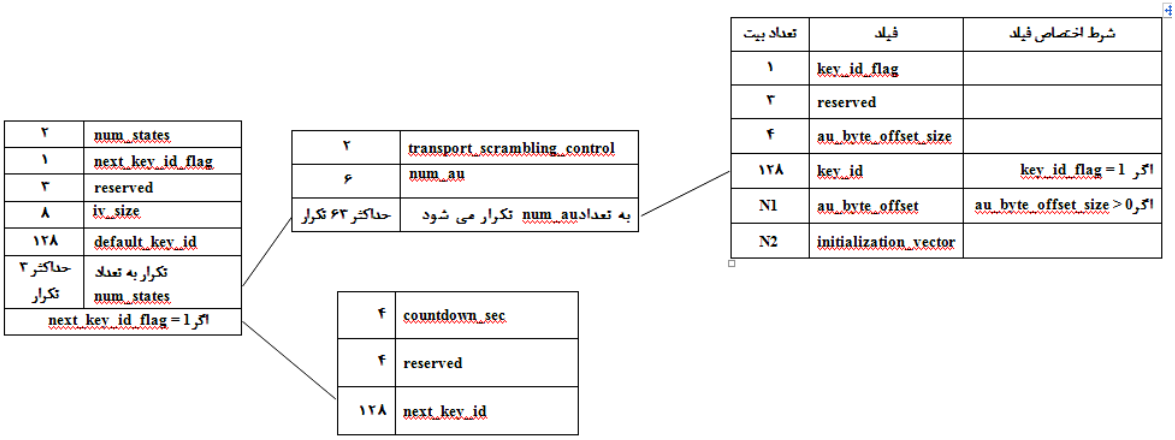
num_states: تعداد ترکیب‌های کلید/ IV توصیف‌شده در این ECM است.

next_key_id_flag: در صورتی که ۱ باشد، next_key_id در این ECM ارائه می‌شود.

iv_size: اندازه بردارهای مقداردهی اولیه، به بایت است. بردارهای مقداردهی اولیه ۸ بایت و ۱۶ بایت باید پشتیبانی شود.

1 - Syntax

۲- هر نحو، طبق جداول مربوط به رمزنگاری مورد تحلیل قرار گرفته است و در پاورقی معناشناسی نحو ترسیم شده است.



transport_scrambling_control: مقدار فیلد transport_scrambling_control که به این ترکیب کلید/IV مربوط است.

default_key_id: ID کلید پیش‌فرض که با واحدهای دسترسی فهرست‌شده در این ECM CETS استفاده می‌شود.

num_au: تعداد نمونه‌ها (واحدهای دسترسی) که وضعیت transport_scrambling_control و ID کلید مشابه را به اشتراک می‌گذارند.

key_id_flag: در صورتی که ۱ باشد، ID کلید آشکار (رمزنشده)[1] ارائه خواهد شد. در صورتی که صفر باشد، ID کلید پیش فرض استفاده می‌شود.

au_byte_offset_size: اندازه au_byte_offset، به بایت است.

key_id: شناسانه کلیدی که برای به‌دست آوردن کلید نمونه (واحد دسترسی) استفاده می‌شود.

au_byte_offset: در مورد واحدهای دسترسی چندگانه که در یک بسته PES بسته‌بندی شده است، آفست بایت از اولین بایت پایه‌بار PES تا اولین بایت رمزگذاری‌شده که از ترکیب کلید/IV فعلی استفاده می‌کند، است. طول فیلد توسط au_byte_offset_size ارائه می‌شود.

یادآوری- آفست‌ها به اولین بایت پایه‌بار بسته‌ی PES مربوط است، از این رو اولین واحد دسترسی هر بسته PES، یک آفست صفر خواهد داشت. آفست‌های غیر صفر به واحدهای دسترسی اضافی در بسته PES مشابه مربوط است. حلقه واحد دسترسی بیش از یک عدد صحیح از بسته‌های PES است و هر مقدار صفر au_byte_offset به آغاز بسته PES مربوط است.

initialization_vector: بردار مقداردهی اولیه استفاده‌شده در این ترکیب کلید/IV است. طول فیلد توسط iv_size ارائه می‌شود.

countdown_sec: ثانیه‌هایی که تا نزدیکترین چرخش کلید طی می‌شود.

next_key_id: ID کلیدی است که انتظار می‌رود برای اولین بار در ثانیه‌های countdown_sec در آینده استفاده شود.

یادآوری- ID کلید آینده اضافه می‌شود تا به کارخواه اجازه پیش واکشی[2] به موقع از آن‌ها را برای چرخش کلید بدهد؛ از این رو مقدار شمارش معکوس باید غیر صفر باشد، بدین معنی که اعلان چرخش کلید باید حداقل در ۱ ثانیه ارسال شود. شمارش معکوس، مبهم و غیر الزام‌آور است - و فقط هشدار زودهنگام را ارائه می‌کند. علاوه بر این، هیچ تضمینی وجود ندارد که یک کلید مشخص در زمان مشخص استفاده شود. اعلان اجباری استفاده کلید در فیلدهای default_key_id و key_id مربوط به ECM CETS استفاده می‌شود.

1 - Explicit key
2 - Pre-fetch

CETS PSSH ۲-۶

۱-۲-۶ کلیات

بسته CETS PSSH پایه‌بار کامل جعبه `pssh`، را همان طور کـه در ISO/IEC 23001-7 تعریـف شـده است، حمل می‌کند. هر بسته از نحو خصوصی (اختصاصی) استفاده می‌کند و جعبه `pssh` همراه بـا کـد درهم‌آمیخته MD5 برای یکپارچگی حمل می‌شود.

اولین بسته جریان انتقال CETS PSSH باید payload_units_start_indicator را به ۱ تنظیم کند.

۲-۲-۶ نحو

نحو	شماره بیت‌ها	قالب
cets_pssh_packet(){		
md5_flag	1	bslbf
reserved	31	bslbf
pssh_box()		FullBox
if (md5_flag == 1)		
md5sum	128	bslbf
}		
}		

۳-۲-۶ معناشناسی[۱]

md5_flag: اگر درست باشد، کد درهم‌آمیخته MD5 پس از جعبه `pssh` ظاهر خواهد شد.

pssh_box: جعبه `pssh`، همان طور که در ISO/IEC 23001-7 تعریف شده، کامل می‌شود.

یادآوری- طول پیام از فیلدهایی که توسط `pssh` کلاس جعبه (Box) به ارث برده می‌شود، مشتق می‌شود. برای جزئیات در ساختار جعبه به ISO/IEC 14496-12 مراجعه شود.

md5_sum: کد درهم‌آمیخته MD5 بسته CETS PSSH، از md5_flag شروع می‌شود و تا آخرین بایت جعبه `pssh` ادامه می‌یابد.

CA_descriptor ۳-۶

۱-۳-۶ کلیات

CA_descriptor برای نشان دادن خصوصیات طرح حفاظت محتوا استفاده می‌شود.

یادآوری- توصیه می‌شود که اندازه CA_descriptor طوری تنظیم شود که بخش‌های PMT و CAT بتواند متناسـب یـک بسته جریان انتقال شود.

۱- تحلیل نحو

شرط اختصاص فیلد	فیلد	تعداد بیت
	md5_flag	۱
	reserved	۳۱
	pssh_box()	
md5_flag = 1	**md5sum**	۱۲۸

۶-۳-۲ نحو

نحو	شماره بیت‌ها	قالب
CA_descriptor(){		
descriptor_tag	8	bslbf
descriptor_length	8	bslbf
CA_SystemID //'ce'	16	bslbf
reserved	3	bslbf
CA_PID	13	uismbf
scheme_type	32	baslbf
scheme_version	32	uismbf
num_systems	8	bslbf
encryption_algorithm	24	uismbf
for (i = 0; i < num_system_id; i++) {		
system_id	128	bslbf
pssh_pid	13	uismbf
reserved	3	bslbf
}		
for (i=0; i<N;i++) {		
private_data_byte	8	uismbf
}		
}		

۶-۳-۳ معناشناسی[۱]

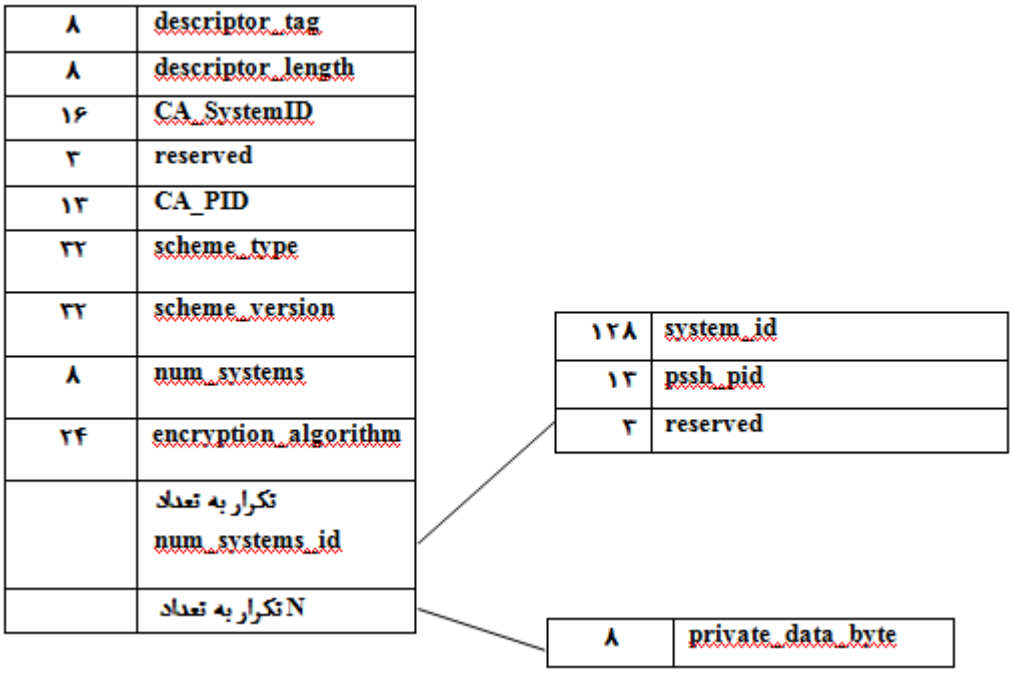
CA_SystemID: شناسانه سامانه این سامانه، طبق تعریف ISO/IEC 13818-1 در این استاندارد باید 'ce' باشد.

CA_PID: همان طور که در استاندارد ISO/IEC 13818-1 تعریف شده است.

scheme_type: مشابه فیلد `schm`.scheme_type

scheme_version: مشابه فیلد `schm`.scheme_version

۱- تحلیل نحو



num_systems: تعداد ID سامانه‌های ۱۲۸ بیتی که در زیر ارائه شده است.

encryption_algorithm: الگوریتم رمزگذاری را مشابه فیلد `tenc`.IsEncrypted مشخص می‌کند.

system_id: مشابه فیلد `pssh`.SystemID

pssh_pid: PID ای که در آن جعبه (های) `pssh` می‌تواند برای این سامانه حفاظت محتوا یافت شود.

۷ عملیات

۷-۱ محدودیت رمزگذاری

۷-۱-۱ کلیات

برای رمزگشایی پایه‌بار بسته TS، فقط یک کلید و یک بردار مقداردهی اولیه لازم است.

سرآیندهای PES نباید رمزگذاری شود.

یادآوری- در نتیجه، اولین بسته جریان انتقال پایه‌بار حامل بسته PES، رمزگشایی خواهد شد.

۷-۱-۲ ISO/IEC 14496-10 و ISO/IEC 23008-2

کدهای شروع و سرآیندهای NAL نباید رمزگذاری شود. علاوه بر این VPS، SPS، PPS و AUD نیز نباید رمزگذاری شود.

توصیه می‌شود واحدهای غیر VCL رمزگذاری نشود، با این حال گاهی اوقات لازم است پیام‌های SEI رمزگذاری شود. همچنین توصیه می‌شود سرآیندهای برش[1] رمزگذاری نشود.

یادآوری- این بدان معنی است که تضمین می‌شود، مجری توانایی تجزیه این موضوع را دارد: به طور مثال صرف نظر از مقدار بیت‌های درهم‌ساز، می‌تواند PTS، DTS، AUD و SPS / PPS را به صورت قابل اعتماد تجزیه کند. با بیان این که مجری نباید فرض کند منع شبیه‌سازی کد شروع در بسته‌های با مقدار غیر صفر transport_ scrambling_control اعمال می‌شود.

۷-۱-۳ ISO/IEC 13818-7 و ISO/IEC 14496-3

ممکن است قاب‌های ADTS، raw_data_bytes رمزگذاری شود، اما فیلدهای adts_fixed_header، adts_variable_header، adts_error_check، adts_header_error_check و adts_raw_data_block_error_check نباید رمزگذاری شود.

هنگامی که LATM / LOAS در پیکربندی داخل باند در ساختار AudioSpecificConfig() حمل می‌شود، نباید رمزگذاری شود.

۷-۲ جریان‌های ابتدایی حفاظت‌شده چندگانه

اطلاعات کلید/ IV برای هر PID رمزگذاری‌شده باید در PID ECM جداگانه حمل شود.

1 - Slice headers

استفاده از PID ECM مشابه برای چند جریان ابتدایی امکان‌پذیر است. در این مورد، au_byte_offset_size باید صفر باشد و در نتیجه بسته PES تنها باید یک واحد دسترسی منفرد را حمل کند.

یادآوری- باید توجه داشت تا اطمینان حاصل شود که برای هر واحد دسترسی، آخرین بسته ECM همیشه ترکیب کلید/ IV صحیح برای مقدار transport_scrambling_control در بسته‌های جریان انتقال حامل این واحد دسترسی را شامل می‌شود.