INSO

21094

1st.Edition

2016

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

استاندارد ملی ایران

۲۱۰۹۴

چاپ اول

۱۳۹۵

دارای محتوای رنگی

# شبکه‌های داده، سامانه‌های باز ارتباطات و امنیت – برنامه‌های کاربردی و خدمات امن- امنیت تلویزیون مبتنی بر پروتکل اینترنت (IPTV) - الزامات کارکردی و معماری جنبه‌های امنیت IPTV

# DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY
## Secure applications and services – IPTV security
## Functional requirements and architecture for IPTV security aspects

ICS: 33.160.01

**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 کسب‌وکار 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 الزامات 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، پیاده‌سازی 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، پیاده‌سازی 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**

**« شبکه‌های داده، سامانه‌های باز ارتباطات و امنیت – برنامه‌های کاربردی و خدمات امن-امنیت تلویزیون مبتنی بر پروتکل اینترنت (IPTV) - الزامات کارکردی و معماری جنبه‌های امنیت IPTV»**

| **رئیس:** | **سمت و/ یا نمایندگی:** |
| --- | --- |
| گرامی، حسن<br>(دکتری مخابرات) | هیئت علمی دانشکده مخابرات |
| **دبیر:** | |
| غلام ابوالفضل، فرزانه<br>(کارشناسی مهندسی مخابرات) | مدیرکل فروش عمده شرکت مخابرات ایران |
| **اعضاء: (اسامی به ترتیب حروف الفبا)** | |
| ابراهیمی، شبنم<br>(کارشناسی ارشد مهندسی مخابرات) | پژوهشگر دانشگاه یزد |
| امین آقایی، اصغر<br>(کارشناسی مهندسی مخابرات) | مدیرکل تحقیق وتوسعه محصول شرکت مخابرات ایران |
| آقایی، حدیث<br>(کارشناسی ارشد مهندسی نرم افزار) | کارشناس مدیریت محصول شرکت مخابرات ایران |
| پاشایی زاد، حسن<br>(کارشناسی مهندسی مخابرات) | رئیس پژوهش و فناوری دانشکده مخابرات |
| پولادی، فرهاد<br>(کارشناسی ارشد مهندسی مخابرات) | هیئت علمی دانشکده مخابرات |
| تیموری، امیر<br>(کارشناسی ارشد مهندسی مخابرات) | رئیس اداره کنترل پروژه توسعه محصول شرکت مخابرات ایران |
| عروجی، سید مهدی<br>(کارشناسی ارشد مدیریت فناوری اطلاعات) | سرپرست گروه تدوین استاندارد سازمان تنظیم مقررات و ارتباطات رادیویی |
| غلام ابوالفضل، احمد رضا<br>(کارشناسی مترجمی زبان) | کارشناس مترجمی شبکه مترجمین ایرانیان مترجم |
| **ویراستار:** | |
| قسمتی، سیمین<br>(کارشناسی ارشد مهندسی فناوری اطلاعات) | مدیر پروژه مرکز آپا دانشگاه تربیت مدرس |

## فهرست مندرجات

**عنوان** **صفحه**

## پیش‌گفتار

استاندارد «شبکه‌های داده، سامانه‌های باز ارتباطات و امنیت – برنامه‌های کاربردی و خدمات امن-امنیت تلویزیون مبتنی بر پروتکل اینترنت (IPTV) - الزامات کارکردی و معماری جنبه‌های امنیت IPTV» که پیش‌نویس آن در کمیسیون‌های مربوط تهیه و تدوین شده است، دردویست ودهمین اجلاسیه کمیتهٔ ملی استاندارد مخابرات مورخ ۹۵/۱/۲۱ 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 زمینهٔ صنایع، علوم و خدمات، استانداردهای ملی ایران در صورت لزوم تجدیدنظر خواهند شد و هر پیشنهادی که برای اصلاح و تکمیل این استانداردها ارائه شود، هنگام تجدیدنظر در کمیسیون‌های مربوط مورد توجه قرار خواهد گرفت. بنابراین، باید همواره از آخرین تجدیدنظر استانداردهای ملی ایران استفاده کرد.

منبع و مأخذی که برای تهیه و تدوین این استاندارد مورد استفاده قرار گرفته به توصیف زیر است:

ITU-T X.1191: 2009, SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY Secure applications and services – IPTV security Functional requirements and architecture for IPTV security aspects

# شبکه‌های داده، سامانه‌های باز ارتباطات و امنیت – برنامه‌های کاربردی و خدمات امن- امنیت تلویزیون مبتنی بر پروتکل اینترنت (IPTV) - الزامات کارکردی و معماری جنبه‌های امنیت IPTV

## ۱ هدف و دامنهٔ کاربرد

هدف از تدوین این استاندارد، تعیین الزامات کارکردی، معماری و سازوکارهای مربوط به جنبه‌های امنیت و محافظت محتوا، خدمات، شبکه‌ها، افزاره‌های پایانه و مشترکین IPTV است. پیش‌بینی می‌شود که الزامات و کارکردهای شناسایی‌شده در این استاندارد را بتوان به‌طور متناسب مطابق با خدمت و مدل‌های کسب‌وکار IPTV به کار برد که می‌تواند نیازمند سطح مختلفی از قابلیت‌های امنیتی باشد.

## 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:

**۲-۱** استاندارد ملی ایران شماره ۱۷۱۱۵: سال ۱۳۹۴، فناوری اطلاعات - الزامات تشکیل و اعتبارسنجی مسیر گواهی دیجیتالی[۱]

**۲-۲** استاندارد ملی ایران شماره ۱۹۱۰: سال ۱۳۸۹،سری Y: زیرساخت اطلاعات جهانی و جنبه‌های پروتکل اینترنتی و شبکه‌های نسل بعدی- جنبه‌های پروتکل اینترنتی - تلویزیون پروتکل اینترنتی (IPTV) روی شبکه نسل بعدی (NGN) - معماری کارکردی تلویزیون پروتکل اینترنتی (IPTV)[۲]

## ۳ اصطلاحات و تعاریف

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

---

۱ - ITU-T X.509 (2008) | ISO/IEC 9594-8:2008

۲ - ITU-T Y.1910 (2008)

## ۳-۱ اصطلاحات تعریف شده در سایر منابع

در این استاندارد، اصطلاحات زیر که در سایر منابع تعریف شده است، به کار می‌رود.

### ۳-۱-۱

**واپایش دسترسی[۱] [b-ITU-T X.800]**

جلوگیری از استفاده غیرمجاز از یک منبع، از جمله جلوگیری از استفاده از یک منبع به یک شیوه غیرمجاز

### ۳-۱-۲

**برنامه کاربردی[۲] [b-ITU-T Y.101]**

مجموعه‌ای ساختار یافته از قابلیت‌ها که قابلیت کارکردی ارزش افزوده پشتیبانی‌شده که یک یا چند خدمت را فراهم می‌آورد.

### ۳-۱-۳

**اصالت‌سنجی[۳] [b-ITU-T X.800]**

به قسمت اصالت‌سنجی منشا داده‌ها و اصالت‌سنجی هستار ـ همتا مراجعه شود.

### ۳-۱-۴

**مجوزدهی[۴] [b-ITU-T X.800]**

اعطای حق که شامل اعطای دسترسی بر اساس حقوق دسترسی می‌شود.

### ۳-۱-۵

**دسترسی‌پذیری[۵] [b-ITU-T X.800]**

خصوصیت قابل دسترس بودن و قابل استفاده بودن بر مبنای تقاضای یک هستار مجاز است.

---

۱ -Access Control

۲- Application

۳- Authentication

۴- Authorization

۵ - Availability

**۶-۱-۳**

**قابلیت محرمانگی[۱] [b-ITU-T X.800]**

خصوصیت در دسترس نبودن یا فاش نشدن اطلاعات برای افراد، هستارها، یا فرآیندهای غیرمجاز است.

**۷-۱-۳**

**اصالت‌سنجی منشا داده‌ها[۲] [b-ITU-T X.800]**

تأیید این که منبع داده‌های دریافت‌شده همان منبعی است که ادعا شده است.

**۸-۱-۳**

**رد خدمت[۳] [b-ITU-T X.800] (DoS)**

جلوگیری از دسترسی مجاز به منابع و یا به تأخیر انداختن عملیات‌های حساس به زمان است.

**۹-۱-۳**

**امضای الکترونیکی[۴] [b-ITU-T X.800]**

اضافه کردن داده‌های پنهانی یا تبدیل به رمز کردن یک واحد داده که به گیرنده امکان می‌دهد تا از منبع و یکپارچگی واحد داده اطمینان حاصل کند و از جعل آن‌ها توسط گیرنده جلوگیری شود.

**۱۰-۱-۳**

**جریان پایه‌ای[۵] [b-ITU-T H.222.0]**

یک اصطلاح عمومی برای ویدئوی کدگذاری شده، صدای کدگذاری شده، یا سایر جریان بیتی کدگذاری‌شده دیگر در بسته PES است.

**یادآوری**- PES به معنی یک جریان پایه‌ای بسته‌بندی شده است.

---

۱- Confidentiality

۲ -Data Origin Authentication

۳ -Denial Of Service (Dos)

۴ -Digital Signature

۵ -Elementary Stream

**۱۱-۱-۳**

**معماری کارکردی[۱] [b-ITU-T Y.2012]**

مجموعه‌ای از هستارهای کارکردی و نقاط مرجع بین آن‌ها که برای تشریح ساختار یک NGN[۲] استفاده می‌شود. این هستار کارکردی به وسیله نقاط مرجع از هم جدا می‌شوند و بنابراین توزیع کارکردها را مشخص می‌کنند.

**۱۲-۱-۳**

**هستار کارکردی[۳][b-ITU-T Y.2012]**

هستاری که شامل مجموعه غیرقابل تقسیم از کارکردهای ویژه می‌شود. هستارهای کارکردی مفاهیم منطقی است در حالی که گروه‌بندی هستارهای کارکردی برای توصیف پیاده‌سازی‌های عملی فیزیکی مورد استفاده قرار می‌گیرد.

**۱۳-۱-۳**

**یکپارچگی[۴][b-ITU-T X.800]**

خصوصیتی مبنی بر این که داده‌ها به یک شیوه غیرمجاز دچار تغییر یا تخریب نشده‌اند.

**۱۴-۱-۳**

**کلید[۵][b-ITU-T X.800]**

رشته‌ای از علائم که عملیات کدگذاری و کدگشایی را واپایش می‌کند.

**۱۵-۱-۳**

**مدیریت کلید[۶][b-ITU-T X.800]**

ایجاد، ذخیره، توزیع، حذف، بایگانی، و به کارگیری کلیدها مطابق با سیاست امنیتی.

---

۱ -Functional Architecture

۲ -Next Generation Network

۳ -Functional Entity

۴ -Integrity

۵ -Key

۶ -Key Management

**۱۶-۱-۳**

**نقاب زدن[۱] [b-ITU-T X.800]**

یک هستار خود را جای یک هستار متفاوت دیگر وانمود می‌کند.

**۱۷-۱-۳**

**ارائه‌دهنده شبکه[۲] [b-ITU-T Q.1290]**

سازمانی که اجزای مورد نیاز شبکه برای قابلیت کارکرد IPTV را نگهداری و پیاده‌سازی می‌کند.

**یادآوری ۱-** یک ارائه‌دهنده شبکه می‌تواند به صورت اختیاری به عنوان ارائه‌دهنده خدمات نیز عمل کند.

**یادآوری ۲-** ارائه‌دهنده خدمت و ارائه‌دهنده شبکه اگر چه به عنوان دو هستار جداگانه در نظر گرفته می‌شوند اما می‌توانند به صورت اختیاری، یک هستار سازمانی باشند.

**۱۸-۱-۳**

**اصالت‌سنجی هستار ـ همتا[۳] [b-ITU-T X.800]**

تأیید این که یک هستار همتا در یک تجمع همان هستار ادعا شده است.

**۱۹-۱-۳**

**حریم‌خصوصی[۴] [b-ITU-T X.800]**

حق افراد برای واپایش یا اثرگذاری این که چه اطلاعاتی در باره آن‌ها را می‌توان جمع‌آوری و ذخیره کرد و توسط چه کسی این کار را انجام داد و این اطلاعات را برای چه کسی می‌توان فاش کرد.

**۲۰-۱-۳**

**رد[۵] [b-ITU-T X.800]**

رد مشارکت داشتن در همه یا بخشی از ارتباطات توسط یکی از هستارهای مشمول در ارتباطات است.

---

۱ -Masquerade

۲- Network Provider

۳ -Peer-Entity Authentication

۴ -Privacy

۵ -Repudiation

**۲۱-۱-۳**

**برچسب ایمنی[۱] [b-ITU-T X.800]**

یک علامت بر روی یک منبع (که می‌تواند یک واحد داده باشد) که ویژگی‌های امنیتی آن منبع را نام‌گذاری یا مشخص می‌کند.

**یادآوری**- این علامت‌گذاری و/یا برچسب می‌تواند به صورت واضح یا غیر واضح باشد.

**۲۲-۱-۳**

**سیاست امنیتی[۲] [b-ITU-T X.800]**

مجموعه‌ای از معیارها برای فراهم آوردن خدمات امنیتی.

**۲۳-۱-۳**

**ارائه‌دهنده خدمت[۳] [b-ITU-T M.1400]**

ارجاع کلی به یک اپراتور (کاروَر) [۴] که خدمات ارتباطات دور را برای مشتریان و دیگر کاربران بر اساس تعرفه و یا بر اساس قرارداد فراهم می‌آورد. ارائه‌دهنده خدمات می‌تواند به صورت اختیاری، یک شبکه داشته باشد. ارائه‌دهنده خدمات می‌تواند به صورت اختیاری، مشتری یک ارائه‌دهنده خدمات دیگر باشد.

**۲۴-۱-۳**

**تهدید[۵] [b-ITU-T X.800]**

یک مورد نقض بالقوه و احتمالی امنیت است.

## ۲-۳ اصطلاحات تعریف شده در این استاندارد

این استاندارد، اصطلاحات زیر را تعریف می‌کند:

---

۱ -Security Label

۲ -Security Policy

۳ -Service Provider

۴-Operator

۵ -Threat

**۱-۲-۳**

**اکتساب**[۱]

فرآیند به دست آوردن **محتوا** توسط کاربر نهایی است.

**۲-۲-۳**

**صدور محتوا**[۲]

فرآیند صادر کردن امن محتوای IPTV از پایانه IPTV به یک پایانه دیگر که تحت مالکیت کاربری قرار دارد که محق استفاده از آن است.

**۳-۲-۳**

**حفاظت محتوا**[۳]

تضمین این که کاربر نهایی می‌تواند تنها از محتوایی که قبلاً مطابق با حق اعطا شده به او توسط صاحب حق به او اعطا شده است استفاده کند؛ حفاظت محتوا شامل حفظ محتوا در برابر رونوشت‌برداری و توزیع غیرقانونی، ردگیری، مداخله، استفاده غیرمجاز، و غیره است.

**۴-۲-۳**

**ردگیری محتوا**[۴]

فرآیندی که شناسایی مبدأ (دلخواه) محتوا و/یا طرف مسئول (برای مثال کاربرد نهایی) را امکان‌پذیر می‌کند تا بررسی‌های بعدی در موردی که استفاده غیرمجاز از محتوا، نظیر رونوشت‌برداری و توزیع مجدد محتوا، روی داده باشد تسهیل شود.

**یادآوری**- اطلاعات ردگیری محتوا به صورت فراداده یا نشانه‌گذاری قانونی به محتوا الحاق شوند.

---

۱ -Threat

۲ -Content Export

۳ -Content Protection

۴ -Content Tracing

**۵-۲-۳**

**استحقاق**[۱]

استناد به سطوح مجوزدهی از جمله اطلاعات دسترسی مشروط که یک مشترک بتواند از آن‌ها برای دسترسی به خدمات معین IPTV در IPTV TD خود استفاده کند.

**۶-۲-۳**

**حفاظت افزاره پایانه مربوط به IPTV** [۲]

تضمین این که TD به کار گرفته شده توسط یک کاربر نهایی در وصول یک خدمت می‌تواند به‌طور قابل اطمینان و ایمن از محتوا استفاده کند، و در عین حال پیاده‌سازی کردن حقوق استفاده اعطا شده برای آن محتوا حفاظت فیزیکی و الکترونیکی از یکپارچگی TD و محرمانگی محتوا و پارامترهای حیاتی ایمنی (برای مثال کلیدهای ذخیره شده) که محافظت نشده‌اند.

**۷-۲-۳**

**تلویزیون خطی**[۳]

خدمت پخش تلویزیون مشابه شکل قدیمی خدمات تلویزیون ارائه شده توسط کابل؛ در اینجا محتوای برنامه مطابق با برنامه زمانی معین و در نظر گرفته شده برای مصرف آن در زمان واقعی توسط کاربر، ارسال می‌شود.

**۸-۲-۳**

**فراداده‌ها برای تسهیل نشانه‌گذاری‌گذاری**[۴]

فراداده‌های ایجاد شده بر کمک نشانه‌گذاری‌گذاری‌های بعدی توسط افزاره‌های جریان پایین دست است.

---

۱ -Entitlements

۲ -Iptv Terminal Device (Td) Protection

۳ -Linear TV

۴ -Metadata For Watermarking Facilitation

**۹-۲-۳**

**صیادی**[۱]

اکتساب اطلاعات حساس یا شخصی نظیر نام کاربری، تاریخ تولد، یا جزئیات کارت اعتباری شخص از طریق وانمود کردن خود به عنوان یک هستار موثق از طریق نقاب‌زنی است.

**۱۰-۲-۳**

**حقوق**[۲]

به توانایی انجام یک مجموعه‌ای از پیش تعریف شده از کارکردهای استفاده برای یک قلم محتوا اشاره دارد؛ این کارکردهای استفاده شامل مجوزها (برای مثال برای دیدن/شنیدن، رونوشت کردن، اصلاح کردن، ضبط، گلچین کردن، نمونه‌برداری، نگهداری برای یک مدت زمان یا توزیع معین) ، محدودیت‌ها (برای مثال: پخش/دیدن، شنیدن برای چندین مرتبه، پخش/دیدن شنیدن برای تعداد ساعات مشخص) و تعهدات (برای مثال: پرداخت، ردگیری محتوا) می‌شود که برای محتوا اعمال می‌شود و اختیار استفاده را برای کاربر نهایی فراهم می‌آورد.

**۱۱-۲-۳**

**بیان حقوق**[۳]

درج حقوق به یک شکل رسمی و منسجم است.

**۱۲-۲-۳**

**SCP انتها-به-انتها**[۴]

حالت بهره‌برداری از حفاظت خدمت و محتوا است که در آن محتوا مطابق با حقوق اعطا شده، با استفاده از یک سامانه خدمت منفرد و سامانه حفاظت محتوا توسط افزاره‌های نهایی مورد دسترسی یا تبادل قرار می‌گیرد.

---

۱- Phishing

۲ -Rights

۳ -Rights Expression

۴ -SCP End-To-End

**۱۳-۲-۳**

**ایجاد پل SCP** [۱]

حالت بهره‌برداری حفاظت خدمت و محتوا است که در آن دو یا چند سامانه حفاظت خدمت و محتوا بر روی یک افزاره منفرد کار می‌کنند که به عنوان یک پل بین این سامانه‌های حفاظت خدمت و محتوا عمل می‌کند. محتوای اکتساب‌شده از طریق یک سامانه حفاظت خدمت و محتوا توسط سامانه حفاظت خدمت و محتوای دیگر مطابق با حقوق اعطا شده، بر روی پل قابل دسترسی است.

**۱۴-۲-۳**

**تبادل SCP** [۲]

حالت بهره‌برداری عمومی‌تر حفاظت خدمت و محتوا که شامل دو یا چند افزاره است و هر افزاره دارای یک یا چند سامانه عملیاتی حفاظت خدمت و محتوا است. محتوای اکتساب شده توسط یک افزاره از طریق یکی از سامانه‌های حفاظت خدمت و محتوای آن را می‌توان به صورت ایمن به یک افزاره دیگر از طریق یک سامانه متفاوت حفاظت خدمت و محتوا مطابق با حقوق اعطا شده، انتقال داد و یا حق دسترسی آن را اعطا کرد.

**۱۵-۲-۳**

**مخلوط کردن**[۳]

فرآیند طراحی شده برای محافظت محتوای چند رسانه‌ای، در فرآیند مخلوط کردن به طور معمول از فناوری رمزنگاری برای حفظ محتوا استفاده می‌شود.

**۱۶-۲-۳**

**الگوریتم مخلوط کردن**[۴]

الگوریتم مورد استفاده در یک فرآیند مخلوط‌سازی یا یک فرآیند تفکیک است.

---

۱ -SCP Bridging

۲ -SCP Interchange

۳ -Scrambling

۴ -Scrambling Algorithm

**۱۷-۲-۳**

**طرح قابل انتقال ایمن کد**[۱]

**نوعی** طرح امنیتی که گره میانی شبکه را قادر می‌سازد تا تبدیل کد را بدون انجام فرآیند آشکارسازی انجام دهد و در عین حال امنیت انتها-به-انتها را حفظ کند. این طرح را می‌توان با ترکیب کدگذاری مقیاس‌پذیر، پنهان‌سازی تصاعدی، و بسته‌بندی داده‌ها پیاده‌سازی کرد. طرح قابلیت انتقال ایمن کد می‌تواند قابلیت محرمانگی و یکپارچگی/اعتبار پیام را فراهم آورد.

**۱۸-۲-۳**

**حفاظت خدمت**[۲]

تضمین این که یک کاربر نهایی می‌تواند تنها خدمت و محتوای را که حق دریافت آن را دارد، است اکتساب کند؛ حفاظت خدمت شامل حفاظت خدمت از دسترسی غیرمجاز در هنگامی که محتوای IPTV از طریق اتصالات خدمت IPTV منتقل می‌شود، است.

**۱۹-۲-۳**

**حفاظت خدمت و محتوا**[۳]

ترکیبی از حفاظت خدمت و حفاظت محتوا یا سامانه یا پیاده‌سازی وابسته به آن است.

**۲۰-۲-۳**

**جعل**[۴]

فعالیتی که در آن یک منبع جعلی (برای مثال: یک فرد یا یک برنامه کامپیوتری) با موفقیت به عنوان یک منبع مشروع نقاب می‌زند و داده‌ها را با هدف به دست آوردن اطلاعات/یا مبهم کردن منبع واقعی تحریف می‌کند به طوری که منبع جعلی بتواند فعالیت‌های غیرمجازی نظیر انتشار بدافزار کامپیوتری (برای مثال ویروس) و غیره را انجام دهد.

---

۱- Secure Transcodable Scheme

۲ -Service Protection

۳ -Service Protection

۴ -Spoofing

**۲۱-۲-۳**

**مقاوم در برابر مداخله**[۱]

**مقاومت** در برابر مداخله توسط کاربران شخصی/مهاجمان یک محصول، بسته نرم‌افزاری، یا سامانه که دسترسی فیزیکی/نرم‌افزاری به آن دارند.

**۲۲-۲-۳**

**تبدیل کد**[۲]

فرآیند تبدیل محتوای چند رسانه‌ای نظیر عکس، متن، صوت، و ویدئو از قالب اصلی به یک قالب یا کیفیت متفاوت است.

**۲۳-۲-۳**

**حفاظت حریم‌خصوصی کاربر**[۳]

تضمین این که اطلاعات در نظر گرفته شده به عنوان به عنوان اطلاعات خصوصی (محرمانه) توسط یک کاربر نهایی همچنان به صورت محرمانه باقی می‌ماند و در عین حال قابلیت افشای الزامی آن‌ها به خاطر فرآیندهای قانونی نیز حفظ می‌شود.

**۲۴-۲-۳**

**امضای ویدئویی**[۴]

فراداده‌ها برای شناسایی یک محتوای ویدئویی؛ برخلاف نشانه‌گذاری تعبیه‌شده از طریق دست‌کاری محتوای اصلی ویدئو، امضای ویدئویی از یک محتوای ویدئو بدون مخاطره افت کیفیت ویدئو استخراج می‌شود.

## ۴ کوته‌نوشت‌ها و سرنام‌ها

در این استاندارد ملی کوته‌نوشت‌ها و سرنام‌های زیر به کار می‌رود:

| | | |
|---|---|---|
| AAA | Authentication , Authorization,and accounting | اصالت‌سنجی، مجوزدهی و پاسخگویی |

۱ -Tamper-Resistant

۲ -Transcoding

۳ -User Privacy Protection

۴ -Ideo Signature

| | | |
|---|---|---|
| AD | Authorized Domain | دامنه مجاز |
| CBC | Cipher Block Chaining | زنجیره بسته رمزشده |
| CDN | Countent Delivery Network | شبکه تحویل محتوا |
| DNG | Delivery Network Gateway | دروازه شبکه تحلیل |
| DNGF | Delivery Network Gateway Function | کارکرد دروازه شبکه تحلیل |
| DoS | Denial of Service | رد خدمت |
| ECB | Electric Code Book | کتاب کد الکترونیکی |
| ECM | Entitlement Control Message | پیام واپایش استحقاق |
| EMM | Entitlement Management Message | پیام مدیریت استحقاق |
| EPG | Electric Program Guide | راهنمای برنامه الکترونیکی |
| HN | Home Network | شبکه خانگی |
| HN-TD | Home Network Terminal Device | افزاره پایانه شبکه خانگی |
| ID | Identifier | شناسانه |
| IPTV | Internet Protocol Television | تلویزیون مبتنی بر پروتکل اینترنت |
| MIKEY | Multimedia Internet KEYing | کلیدگذاری اینترنتی چند رسانه‌ای |
| NAT | Network Addess Translation | ترجمه نشانی شبکه |
| OFB | Output FeedBack | بازخورد خروجی |
| P2P | Peer to peer | همتا به همتا |
| PDA | Personal Digital Assistant | دستیار رقمی شخصی |
| PIN | Personal Identification Number | شماره شناسایی شخصی |
| PKI | Public Key Infrastructure | زیرساخت کلید عمومی |
| PVR | Personal Video Recorder | ضبط کننده‌ی ویدئویی شخصی |
| QoE | Quality of Experience | کیفیت تجربه |
| QoS | Quality of Service | کیفیت خدمت |
| REL | Rights Expression Language | زبان بیان حقوق |

| | | |
|---|---|---|
| SCP | Service and Content Protection | حفاظت خدمت و محتوا |
| SCP-B | SCP Bridge | پل SCP |
| SCP-EE | SCP End-to-End | انتها-به-انتها SCP |
| SCP-IX | SCP Interchange | تبادل SCP |
| STS | Secure Transcodable Scheme | طرح قابلیت تبدیل کد ایمن |
| TD | IPTV-compliant Terminal Device | افزاره پایانه سازگار با IPTV |
| USB | Universal Serial Bus | گذرگاه سری همگانی |
| VoD | Video on Demand | ویدئو درخواستی |

## ۵ قراردادها

در این استاندارد:

کلمه کلیدی «**لازم است که**[۱]» معرف یک الزام است که باید به صورت اکید از آن تبعیت شود و در صورتی که تبعیت از این مجموعه توصیه ادعا شده باشد، هیچ گونه انحرافی از الزام مذکور مجاز نیست.

کلمه کلیدی «**توصیه می‌شود**[۲]» معرف یک الزام است که توصیه می‌شود اما به‌طور مطلق مورد نیاز نیست. از این رو در صورت ادعا برای تبعیت از این مجموعه توصیه، لازم نیست که الزام مذکور حتماً ارائه شود.

اصطلاح کلیدی «**ممنوع است**[۳]» معرف یک الزام است که باید به صورت اکید تبعیت شود و در صورتی که تطابق با این مجموعه الزام ادعا شود، هیچ‌گونه تخلفی از الزام مذکور مجاز نیست.

اصطلاح کلیدی «**می‌تواند به صورت اختیاری**[۴]» معرف یک الزام اختیاری است که بدون اشاره به توصیه کردن آن مجاز است. این اصطلاح برای نشان دادن این که پیاده‌سازی مربوط به فروشنده باید این گزینه را فراهم آورد منظور نشده است و کاروَر شبکه/ ارائه‌دهنده خدمت می‌تواند به صورت اختیاری این گزینه را فعال کند. همچنین به این معنی است که فروشنده می‌تواند به صورت اختیاری این ویژگی را فراهم آورد و همچنان ادعای تبعیت از خصوصیات مطرح شده را داشته باشد. در زمینه معماری امنیت IPTV در این مجموعه توصیه:

«کارکردها» به عنوان مجموعه‌ای از قابلیت‌های کارکردی تعریف می‌شوند. این قابلیت‌ها توسط علائم زیر نشان داده می‌شوند:

---

۱ -Is Required To

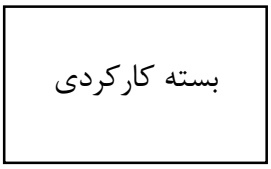
۲ -Is Recommended

۳- Is Prohibited From

۴- Can Optionally

کارکردها

یک «بخش کارکردی» به عنوان گروهی از قابلیت‌های کارکردی تعریف می‌شود که به سطوح جزئیات بیشتری که در این مجموعه توصیه توصیف شده‌اند تجزیه نمی‌شود و توسط علائم زیر نشان داده می‌شود:




## ۶ الزامات امنیتی

### ۶-۱ الزامات عمومی امنیت

- توصیه می‌شود که در معماری IPTV، تأثیر/ اثر عملکرد، کیفیت خدمت، قابلیت استفاده، مقیاس‌پذیری و قیدهای هزینه بر روی استقرار امنیت در نظر گرفته شود.
- معماری IPTV می‌تواند به صورت اختیاری از حفاظت محتوای مربوط به محتوای مشترک کاربر نهایی پشتیبانی کند.

### ۶-۲ الزامات امنیت محتوا

این بند الزامات را مشخص می‌کند که به صورت منفرد یا جمعی به محتوا و حفاظت محتوا مربوط می‌شوند.

*الزامات معماری*

- لازم است که معماری IPTV از حفاظت محتوا تعریف‌شده در بند ۳ پشتیبانی کند.
- لازم است که معماری IPTV با فراداده‌های حفاظت و فراداده‌های مدیریت محتوا از محتوای مرتبط پشتیبانی کند.
- لازم است که معماری IPTV از تحویل امن فراداده‌های حفاظت محتوا و مدیریت محتوا از جمله فراداده‌های حقوق پشتیبانی کند.
- لازم است که معماری IPTV از فراداده‌های حقوق استفاده‌ی محتوا که بین حقوق استفاده از جمله مشاهده، ذخیره‌سازی، توزیع یا توزیع مجدد و ترکیبی از آن‌ها تمایز ایجاد می‌کند پشتیبانی کند.
- لازم است که معماری IPTV از حفاظت محتوا که به صورت همزمان برای تعداد بسیار زیادی از مشترکین توزیع می‌شود پشتیبانی کند (مقیاس‌پذیری) .
- لازم است که معماری IPTV از حفاظت محتوای جریان چندپخشی[1] و /یا تک پخشی[2] پشتیبانی کند.

1 -Multicast
2- Unicast

- لازم است که معماری IPTV از ذخیره ایمن محتوا مطابق با حقوق استفاده اعطا شده پشتیبانی کند.
- اگر ردگیری محتوا مورد استفاده قرار می‌گیرد، لازم است که معماری IPTV از ردگیری استحکام محتوا به یک شیوه‌ی آفلاین (غیر زمان واقعی) پشتیبانی کند (برای مثال محتوای VoD)
- برداشتن و حذف کردن پشتیبانی روش‌های انتقال اطلاعات ردگیری ـ محتوا (برای مثال فراداده‌های تسهیل نشانه‌گذاری) از معماری IPTV ممنوع است.
- حذف پشتیبانی به‌کارگیری فناوری ردگیری محتوا در داخل خروجی TD با هدف شناسایی منحصر به فرد یک بخش کارکردی کارکردها (برای مثال کانال، زمان/تاریخ) ، TD، و/یا کاروَر شبکه، در معماری IPTV ممنوع است. نمونه‌هایی از این فناوری ردگیری محتوا می‌تواند شامل اطلاعات قابل مشاهده و غیرقابل مشاهده باشد.
- حذف بازیابی تمام اطلاعات ردگیری محتوا از محتوا در معماری IPTV ممنوع است.
- حذف پشتیبانی برای قابلیت همکاری حفاظت خدمت و محتوا در معماری IPTV ممنوع است که در آن تنها کاربر یا کاربران یا افزاره یا افزاره‌های مجاز، حتی بعد از انتقال آن به یک سامانه امنیتی دیگر مجاز به استفاده از محتوای IPTV است.
- حذف پشتیبانی برای قابلیت همکاری حفاظت خدمت و محتوا در معماری IPTV ممنوع است که اطلاعات شناسایی حذف شوند به طوری که محتوای IPTV را بتوان بدون توجه به این که کدام طرح‌های شناسایی مورد استفاده قرار می‌گیرد و محتوا به کدام سامانه امنیتی انتقال پیدا می‌کند، شناسایی کرد.
- حذف پشتیبانی برای قابلیت همکاری حفاظت خدمت و محتوا در معماری IPTV ممنوع است تا از افت سطح امنیت هنگامی که محتوا به یک سامانه امنیتی دیگر منتقل می‌شود جلوگیری شود.
- حذف پشتیبانی قابلیت همکاری حفاظت خدمت و محتوا در معماری IPTV که در آن حقوق تنها به افزاره‌های مورد اعتماد اعطا می‌شود ممنوع است.
- حذف پشتیبانی قابلیت همکاری حفاظت خدمت و محتوا در معماری IPTV ممنوع است تا یک محیط امن برای تبادل داده‌های قابلیت همکاری حفاظت خدمت و محتوا (برای مثال اطلاعات اصالت‌سنجی، فراداده‌ها، اطلاعات کلید و...) فراهم شود.
- حذف قابلیت همکاری حفاظت خدمت و محتوا در معماری IPTV ممنوع است به طوری که قابلیت همکاری وابسته به سخت‌افزار یا نرم‌افزار ویژه نباشد.
- در معماری IPTV ملزم کردن سازوکار حفاظت خدمت و محتوای هر یک از دو طرف طرح‌های SCP همکاری متقابل به باز بودن در تلاش برای دستیابی به قابلیت همکاری متقابل ممنوع است.
- حذف پشتیبانی قابلیت همکاری متقابل حفاظت خدمت و محتوا در معماری IPTV که برای پشتیبانی مدل‌های کسب‌وکار مختلف، انعطاف‌پذیر و قابل تعمیم است، ممنوع است.
- حذف پشتیبانی قابلیت همکاری متقابل حفاظت خدمت و محتوا در معماری IPTV در میان سامانه‌های امنیتی متعدد که از سازوکارهای امنیتی متفاوتی استفاده می‌کنند در معماری IPTV ممنوع است تا از خدمت یکپارچه تغییر ـ زمان (مشترکین می‌توانند محتوا را ذخیره کرده و بعداً آن را بازیابی کنند) و

خدمت تغییر ـ مکان (مشترکین می‌توانند در هر مکانی محتوا را ببینند) حتی با سازوکارهای امنیتی متفاوت حاصل شود.

- حذف پشتیبانی قابلیت همکاری متقابل حفاظت خدمت و محتوا در معماری IPTV ممنوع است تا شفافیت سامانه برای کاربران حفظ شود.
- حذف پشتیبانی سازوکارهای متعدد حفاظت خدمت و محتوا بدون توجه به الزامات خاص سخت‌افزار یا نرم‌افزار در معماری IPTV ممنوع است.

*توصیه‌هایی برای معماری*

- اگر در محتوای IPTV از یک فناوری ردگیری محتوا استفاده می‌شود، در این صورت توصیه می‌شود که در این فناوری ردگیری به صورت نامحسوس و غیرقابل مشاهده باشد.
- توصیه می‌شود که معماری IPTV از ردگیری استحکام محتوا در زمان واقعی (برای مثال پخش محتوا) پشتیبانی کند.
- توصیه می‌شود که معماری IPTV از قابلیت اصالت‌سنجی و مجوزدهی کاربران نهایی برای خدمات اشتراک محتوا (برای مثال صدور محتوا و توزیع مجدد محتوا) ، در صورتی که اشتراک محتوا مورد پشتیبانی قرار می‌گیرد، پشتیبانی کند.
- اگر در پیاده‌سازی معماری IPTV از فناوری ردگیری محتوا بر اساس فراداده‌های مربوط به تسهیل نشانه‌گذاری‌گذاری استفاده می‌شود، تعبیه فراداده‌های مرتبط در جریان ابتدایی محتوا با استفاده از تمهیداتی برای «داده‌های کاربر» همانند داده‌های فراهم آمده در طرح کدگذاری ویژه، توصیه می‌شود.
- در موردی که در آن یک TD یا HN-TD در داخل معماری IPTV از چندین سازوکار حفاظت محتوا و خدمت پشتیبانی می‌کند، توصیه می‌شود که از یک کارکرد انتقال استاندارد استفاده شود، که امکان پیوند بیش از یک سامانه SCP و انتقال بین آن‌ها به شیوه‌ای سازگار و تضمین قابلیت همکاری متقابل برای هر TD متصل‌شده یا HN-TD مشارکت کننده در این سازوکار انتقال را فراهم می‌آورد.

*گزینه‌های معماری*

- معماری IPTV می‌تواند به صورت اختیاری، لحاظ کردن اطلاعات ردگیری محتوا را پشتیبانی کند. این اطلاعات ردگیری محتوا می‌تواند به صورت اختیاری شامل ID کاروَر، ID مالک محتوا، ID مربوط به TD و سایر اطلاعات باشد.

*الزامات الگوریتم مخلوط‌سازی[1]*

- الگوریتم‌های مخلوط‌سازی برای پخش جریان لازم است که از به‌روزرسانی دوره‌ای کلیدهای لازم رمزنگاشتی پشتیبانی کنند.
- الگوریتم‌های مخلوط‌سازی برای IPTV لازم است که با استفاده از الگوریتم‌های رمزنگاری استاندارد شده‌ای که به‌طور عمومی در دسترس است ایجاد شود.

---

۱ - Scrambling

*توصیه‌های برای الگوریتم مخلوط‌سازی*

- توصیه می‌شود که الگوریتم‌های مخلوط‌سازی برای IPTV دارای آنتروپی کلید به اندازه کافی بزرگی باشند تا به‌طور مؤثر محتوا را از (خطر) تحلیل ـ رمز محافظت کند.
- حذف پشتیبانی برای الگوریتم‌های مخلوط‌سازی که به‌طور گسترده‌ای مورد استفاده قرار می‌گیرند در معماری IPTV ممنوع نیست.
- توصیه می‌شود که در معماری IPTV از حذف پشتیبانی برای چندین سامانه مخلوط‌سازی پرهیز شود.
- توصیه می‌شود که الگوریتم‌های مخلوط‌سازی برای IPTV به‌طور مؤثری برای پیاده‌سازی‌های سخت‌افزاری/یا نرم‌افزاری قابل پیاده‌سازی باشند.
- توصیه می‌شود که الگوریتم‌های مخلوط‌سازی برای IPTV مقیاس پذیر و مقاوم نسبت به رویدادهای آینده باشند، یعنی دارای پارامترهای رمزنگاری شده (برای مثال طول کلید، دوره‌های زمانی رمزی، و...) یا حالت رمزنگاری شده (برای مثال CBC، OFB، ECB، و غیره...)

*گزینه‌های الگوریتم مخلوط‌سازی*

- در الگوریتم‌های مخلوط‌سازی برای IPTV می‌توان به صورت اختیاری الگوریتم‌های رمزنگاری با قدرت مختلف به منظور انواع مختلف محتوا اعمال کرد.

### ۳-۶ الزامات امنیت خدمت

در این بند الزاماتی که به صورت منفرد یا به صورت جمعی به خدمات و حفاظت خدمت مربوط می‌شوند توصیف می‌شود.

*الزامات معماری*

- لازم است که معماری IPTV از حفاظت خدمت تعریف‌شده در بند ۳ پشتیبانی کند.
- حذف پشتیبانی برای به‌روزرسانیSCP یا نوسازی SCP در TD از طرف کارساز در معماری IPTV ممنوع است.
- لازم است که معماری IPTV از مجوزدهی و اصالت‌سنجی کاربر نهایی (مشترک) پشتیبانی کند.
- لازم است که معماری IPTV از سازوکاری برای TD نشانک[۱] به منظور به‌کارگیری الگوریتم مخلوط‌سازی ویژه بر اساس چارچوب استاندارد پشتیبانی کند.
- لازم است که معماری IPTV توانایی استفاده از سامانه‌های مدیریت کلید استاندارد (برای مثال MIKEY، EMM/ECM) که برای قابلیت همکاری متقابل لازم است را داشته باشد.
- لازم است که معماری IPTV از قابلیت به‌روزرسانی و جستجوی سامانه SCP در ارتباط با الگوریتم‌های مخلوط‌سازی برای IPTV و هرگونه الگوریتم مخلوط‌سازی منتخب توسط کاروَر در طرف کارساز از طریق واسط‌های SCP پشتیبانی کند.

---

۱-Signal

- لازم است که معماری IPTV از سازوکارهای SCP که مستقل از قالب ویژه محتوا است پشتیبانی کند.
- لازم است که معماری IPTV از سازوکاری برای فراهم آوردن حفاظت از یکپارچگی داده‌ها و اصالت‌سنجی منشا داده‌ها برای فرادادەهای حساس پشتیبانی کند.
- لازم است که معماری IPTV از سازوکاری برای تحویل امن اطلاعات حقوق و اطلاعات واپایش دسترسی محتوا به TDها پشتیبانی کند.
- لازم است که معماری IPTV از واپایش استفاده محتوا (برای مثال بازپخش) پشتیبانی کند.
- لازم است که معماری IPTV از حالت‌های مختلف بازپخش پشتیبانی کند، برای مثال محدودیت بر روی تعداد پخش‌ها، محدودیت زمان برای پخش‌ها ، محدودیت حرکت سریع به جلو یا به عقب.
- لازم است که معماری IPTV از سازوکاری برای امکان‌پذیر کردن حفظ محرمانگی پیام‌های بین کارساز SCP و کارخواه SCP پشتیبانی کند.
- لازم است که معماری IPTV از سازوکاری برای امکان‌پذیر کردن حفظ اعتبار پیام‌های بین کارساز IPTV و SCP پشتیبانی کند.
- لازم است که معماری IPTV از سازوکاری برای امکان‌پذیر کردن حفظ یکپارچگی پیام‌های بین کارساز SCP و کارخواه SCP پشتیبانی کند.
- لازم است که معماری IPTV از سازوکاری برای بازیافت امن پارامترهای SCP (برای مثال پیکربندی، وضعیت) از TD پشتیبانی کند.
- لازم است که معماری IPTV از سازوکاری برای به‌روزرسانی امن پارامترهای SCP (برای مثال پیکربندی) از TD پشتیبانی کند.
- حذف پشتیبانی برای قابلیت روشن کردن و خاموش کردن کارکرد ردگیری محتوا به شیوه‌ای قابل برنامه‌ریزی (برای مثال بر اساس زمان، رویداد، محتوا یا کانال) از معماری IPTV ممنوع است.
- اگر در معماری IPTV از سامانه مدیریت کلید استفاده شود، لازم است که این سامانه برای مقیاس‌پذیری، قابلیت اطمینان، و قابلیت همکاری متقابل طراحی شود.
- حذف پشتیبانی برای نصب و بهره‌برداری از راهکارهای متعدد حفاظت خدمت چندگانه بدون تعویض سخت‌افزار به جز افزاره‌های قابل حذف (نظیر قفل سخت افزاری USB و سیم‌کارت) از معماری IPTV ممنوع است.
- حذف پشتیبانی برای سازوکار شناسایی برای راهکاری در دسترس حفاظت خدمت که قادر به برآورده‌سازی الزامات مشخص شده برای حفاظت محتوای مرتبط است در معماری IPTV ممنوع است.
- حذف پشتیبانی سازوکار کشف سامانه SCP در معماری IPTV ممنوع است تا بتواند از یک روش کشف پشتیبانی کرده و خود را در هر زمانی که یک محتوای ویژه نیازمند سامانه حفاظت خدمت ویژه باشد، با آن سازگار سازد. حذف پشتیبانی برای سازوکاری برای انتخاب سامانه SCP از میان سامانه‌های موجود SCP بدون تعویض سخت‌افزار به جز افزاره‌های قابل برداشتن، از معماری IPTV ممنوع است.
- حذف پشتیبانی بارگیری امن برای سامانه SCP از معماری IPTV ممنوع است. سامانه SCP بارگیری شده می‌تواند به صورت اختیاری به الزامات ویژه حفاظت خدمت وابسته باشد.

- اگر SCP قابل بارگیری اعمال شود، لازم است که معماری IPTV، حفاظت یکپارچگی داده‌ها و اصالت‌سنجی منشا داده‌ها را برای سامانه SCP بارگیری شده پیاده‌سازی کند.
- اگر بارگیری امن یک برنامه کاربردی به TD پشتیبانی شود، لازم است که معماری IPTV حفاظت یکپارچگی داده‌ها و اصالت‌سنجی منشا داده‌ها را برای برنامه‌های کاربردی بارگیری شده پیاده‌سازی کند.

*توصیه‌های برای معماری*

- توصیه می‌شود که معماری IPTV قابلیت محرمانگی محتوا را امکان‌پذیر کند.
- توصیه می‌شود که معماری IPTV از الگوریتم‌های مخلوط سازی متعدد پشتیبانی کند.
- توصیه می‌شود که معماری IPTV از قابلیت اصالت‌سنجی و مجوزدهی به کاربران نهایی برای خدمات اشتراک‌گذاری محتوا (برای مثال صدور محتوا و توزیع مجدد محتوا) پشتیبانی کند.
- اگر معماری IPTV از سامانه مدیریت کلید استفاده می‌کند، توصیه می‌شود که یک طرح سلسله مراتبی مدیریت کلید جهت پشتیبانی مقیاس‌پذیری در نظر گرفته شود.
- اگر در معماری IPTV از یک سامانه مدیریت کلید استفاده می‌شود که در آن از پروتکل مدیریت کلید گروهی استفاده می‌شود، توصیه می‌شود که یک الگوریتم مدیریت سلسله مراتبی کلید و یک جایگزین الگوریتم مدیریت کلید جهت پشتیبانی مقیاس‌پذیری در نظر گرفته شود.
- اگر در معماری IPTV از یک سامانه مدیریت کلید استفاده می‌شود که در آن از کلید کوتاه مدت استفاده می‌شود، توصیه می‌شود که مسیر رسانه به گونه‌ای تدارک دیده شود که قیدهIPمایشNAT و قیدهای پهنای باند باعث محدود شدن تبادل کلید نشوند.
- توصیه می‌شود که معماری IPTV حداقل از همان میزان حفاظت (برای اهداف واپایش کردن دسترسی غیرمجاز) برای اطلاعات ردگیری محتوا که در محتوای ردگیری شده مرتبط اعمال شده است پشتیبانی کند.
- توصیه می‌شود که معماری IPTV از ارسال مشترک محتوا و اطلاعات ردگیری محتوا پشتیبانی کرده و در عین حال همگامی محتوا و اطلاعات ردگیری محتوا را در حین انتقال حفظ کند.
- اگر در معماری IPTV از PKI برای اصالت‌سنجی TD یا ارائه‌دهنده خدمت یا محتوا استفاده می‌شود، توصیه می‌شود که سلسله مراتب چند ـ سطحی PKI برای پشتیبانی مقیاس‌پذیری، قابلیت اطمینان و قابلیت همکاری متقابل در نظر گرفته شود.
- اگر در معماری IPTV از PKI برای خدمات IPTV استفاده می‌شود، توصیه می‌شود که از قالب گواهی استاندارد، فهرست گواهی‌های نقل شده، یا پروتکل وضعیت برخط گواهی‌ها که به‌طور عمومی در دسترس است استفاده شود.
- توصیه می‌شود که معماری IPTV از بارگیری امن برنامه‌های کاربردی به TD پشتیبانی کند.
- توصیه می‌شود که معماری IPTV از سازوکاری برای محدود کردن ـ حق مشاهده برنامه‌های معین برای گروه‌های معینی از مشترکان پشتیبانی کند (برای مثال مسدود کردن مشاهده ساکنین یک منطقه ویژه (برای مثال این ویژگی می‌تواند به صورت اختیاری برای رویدادهای ورزشی مفید باشد)

*گزینه‌های معماری*

- به منظور فراهم آوردن خدمت IPTV مقیاس‌پذیر برای پایانه تحت مالکیت کاربر که وضوح آن با وضوح پایانه کاربر متفاوت است. معماری IPTV می‌تواند به صورت اختیاری از توانایی داشتن یک طرح امن تبدیل کد تعریف‌شده در بند ۳ پشتیبانی کند.

### ۴-۶ الزامات امنیت شبکه

در این بند، الزاماتی توصیف می‌شوند که به صورت منفرد یا به صورت جمعی به شبکه‌ها یا حفاظت آن‌ها مربوط می‌شود.

*الزامات معماری*

- لازم است که معماری IPTV از قابلیت کاهش یک حمله DoS پشتیبانی کند.
- لازم است که معماری IPTV از تدارک معیارهای امنیتی برای مسدود کردن ترافیک غیرقانونی یا ناخواسته پشتیبانی کند.
- لازم است که معماری IPTV در برابر حمله به قابلیت‌های چندپخشی مقاوم باشد.
- توصیه می‌شود که معماری چندپخشی از قابلیتی برای اصالت‌سنجی یک همتا (همکار) در محیط چندپخشی کلی یا هم پوشان (همتا-به-همتا) پشتیبانی کند.
- لازم است که پیوند ارتباطی بین افزاره‌های پایانه در داخل شبکه اصلی (شبکه خانه) به منظور امنیت محتوا در هنگام حمل محتوای با ارزش، برای مثال محتوایی که مصرف کننده برای آن وجهی پرداخت کرده است، و مورد محافظت قرار نگرفته است، محافظت شود.
- لازم است که معماری IPTV از اصالت‌سنجی DNG توسط کارکرد مدیریت IPTV پشتیبانی کند.
- لازم است که معماری IPTV از اصالت‌سنجی کارکرد مدیریت IPTV توسط DNG پشتیبانی کند.

*توصیه‌های معماری*

- برای محافظت شبکه اصلی (شبکه خانه) از دسترسی بدخواهانه یا دسترسی غیرمجاز) توصیه می‌شود که معماری IPTV از توانایی کارکرد دروازه شبکه تحویل DNGF)) برای ایجاد یک دیوارآتش که از دور قابل پیکربندی است و دارای سطوح متعدد امنیتی و دروازه‌های متناسب با سطح برنامه کاربردی است، پشتیبانی کند.
- توصیه می‌شود که معماری IPTV از قابلیت مدیریت IPTV جهت پیکربندی از دور NAT و کارکرد حفاظت نفوذ DNG پشتیبانی کند.
- توصیه می‌شود که معماری IPTV از قابیلت پیکربندی از دور NAT و کارکرد محافظت نفوذ DNG توسط کارکرد مدیریت IPTV از دور پشتیبانی کند.
- توصیه می‌شود معماری IPTV امنیت مدیریت از دور، TD را در حالتی که مدیریت از دور پشتیبانی می‌شود، حفظ کند.
- توصیه می‌شود که معماری IPTV از استفاده از اطلاعات برچسب محتوا برای واپایش تحویل محتوا پشتیبانی کند.

### ۵-۶ الزامات پایانه

در این بند، الزاماتی توصیف می‌شوند که به صورت منفرد یا جمعی به TDها یا محافظت آن‌ها مربوط می‌شوند.

*الزامات معماری*

- لازم است که معماری IPTV از حفاظت TD تعریف شده در بند ۳ پشتیبانی کند.
- لازم است که معماری IPTV از اعتبار سنجی TD پشتیبانی کند.
- لازم است که معماری IPTV از مقاومت در برابر مداخله فیزیکی برای TD پشتیبانی کند.
- لازم است که معماری IPTV از روشی برای تشخیص در هنگامی که مداخله فیزیکی بر روی TD روی داده است پشتیبانی کند.
- در صورتی که SCP قابل بارگیری مورد استفاده قرار می‌گیرد، لازم است که معماری IPTV از بارگیری و نصب امن کد پیاده‌سازی SCP به TD پشتیبانی کند.
- لازم است که معماری IPTV از روشی امن برای انجام فرآیندهای حساس به امنیت در TD نظیر مدیریت کلید و سری‌سازی رسانه پشتیبانی کند تا پخش محتوا را در حالت نقص در امنیت، تشخیص مداخله یا دیگر نشانه‌های سوءاستفاده، قطع کند.
- لازم است که معماری IPTV حفاظت فیزیکی از فرآیندهای و مؤلفه‌های امکان‌پذیرکننده امنیت مشمول در پردازش ارسال و ذخیره‌سازی محتوای با ارزش در TD در غیاب حفاظت منطقه‌ای (نظیر پنهان کردن یا استفاده از نشانه‌گذاری‌های پیوسته) را فراهم آورد. این فرآیندها شامل تفکیک و سری‌سازی رسانه می‌شود.
- لازم است که معماری IPTV، نیاز به حفاظت فیزیکی (در برابر کاوش یا مداخله سامانه کارکردهای SCP بر روی TD) فرآیندهای حساس امکان‌پذیرکننده امنیت در TD، از جمله تفکیک محتوا و سری‌سازی رسانه (ردگیری محتوا) و داده‌های حیاتی پشتیبان این فرآیندها و همچنین برای همه مؤلفه‌های مشمول در پردازش، ارسال و ذخیره‌سازی هرگونه محتوای با ارزش فاقد محافظت فیزیکی، نظیر رمزنگاری یا نشانه‌گذاری‌های ردگیری محتوا، تشخیص دهد.
- حذف پشتیبانی برای تبادل محتوا بین TD و سایر افزاره‌ها (افزاره‌های فیزیکی یا منطقی) در معماری IPTV ممنوع است به شرط آن که استفاده‌های اعطاشده برای این محتوا شامل چنین تبادلی باشد.
- لازم است که معماری IPTV از سازوکاری پشتیبانی کند که به TD امکان می‌دهد تا کارسازهای SCP را اصالت‌سنجی کند.
- حذف پشتیبانی از نوسازی SCP در TD از معماری IPTV ممنوع است.
- لازم است که معماری IPTV از خروجی رقمی (رقمی) یا آنالوگ پشتیبانی کند که این خروجی در حالتی که خروجی ویدئو/صدای رقمی یا آنالوگ بر روی TD در دسترس باشد لازم است که مطابق با الزام ذخیره‌سازی کارخواه SCP در خارج از افزاره، محافظت شود.

*توصیه‌های معماری*

- توصیه می‌شود که معماری IPTV، صدور محتوا در TD را فراهم آورد کـه امکـان انتقـال امـن محتـوای IPTV از پایانه IPTV به پایانه دیگر تحت مالکیت کاربر مجاز به استفاده از آن را فراهم آورد.

### ۶-۶ الزامات امنیت مشترکان

در این بند الزاماتی توصیف می‌شود که به صورت منفرد یا جمعی به مشترکین و کاربران نهایی و یا حفاظت آن‌ها مربوط می‌شوند.

*الزامات معماری*

- لازم است که معماری IPTV از حفاظت حریم‌خصوصی کاربر تعریف‌شده در بند ۳ پشتیبانی کند.
- لازم است که معماری IPTV، به یک مشترک امکان دهد تا یک سازوکار واپایش دسترسی (بـرای مثـال استفاده از کلمه عبور) جهت محدود کردن دسترسی به محتوا/ خدمات تنظیم کند.
- لازم است که معماری IPTV قادر به نشان دادن این موضوع باشد که چرا دسترسی کاربر بـه محتـوا رد شده است.
- لازم است که معماری IPTV از سازوکاری پشتیبانی کند که به یک مشترک امکان دهـد تـا درخواسـت تعمیم حقوق استفاده (برای مثال پخش‌های بیشتر، زمان پخش بیشتر) مرتبط موارد خاص محتوا را ارائه دهد.

*توصیه‌های معماری*

- توصیه می‌شود که معماری IPTV به کاربر نهایی اجازه دهـد (آن گونـه کـه توسـط حقـوق اجـازه داده می‌شود) تا یک TD را تغییر دهد یا تعویض کند، بدون این که به‌طور ذاتی بر حقوق مربوط بـه مصـرف محتوا تأثیر بگذارد.
- توصیه می‌شود که معماری IPTV از سازوکاری برای رتبه‌بندی برنامه‌ها مطابق با محتوا پشتیبانی کند.

**یادآوری**- اطلاعات رتبه‌بندی را می‌توان برای واپایش دسترسی، برای مثال واپایش والدین، مورد استفاده قرار داد.

## ۷ معماری امنیت

در این بند معماری امنیت IPTV بر حسب معماری امنیت کلی، معماری حفاظت محتوا و معماری حفاظـت خدمت و همچنین هستارهای کارکردی امنیت جهت برآورده‌سازی الزام توصیف‌شده در بندهای قبلی تعریف می‌شود. معماری امنیت IPTV که در ادامه توصیف می‌شود برای اسـتفاده در زمینـه حـوزه‌هـای کـارکردی IPTV و چارچوب کارکردی معماری IPTV که بـه ترتیـب در بنـدهای ۶ و ۸ از [ITU-T Y.1910] تعریـف شده‌اند در نظر گرفته می‌شود.

## ۱-۷ معماری امنیت کلی عمومی

معماری امنیت کلی برای IPTV در شکل ۷-۱ نشان داده شده است. این معماری کلی بـه دو ناحیـه اصـلی تقسیم می‌شود: فرض می‌شود که یکی از این ناحیه‌ها در داخل قلمرو این مجموعه توصیه قرار داشته باشد و فرض می‌شود که ناحیه دیگر خارج از قلمرو موضوع این مجموعه توصیه باشد.

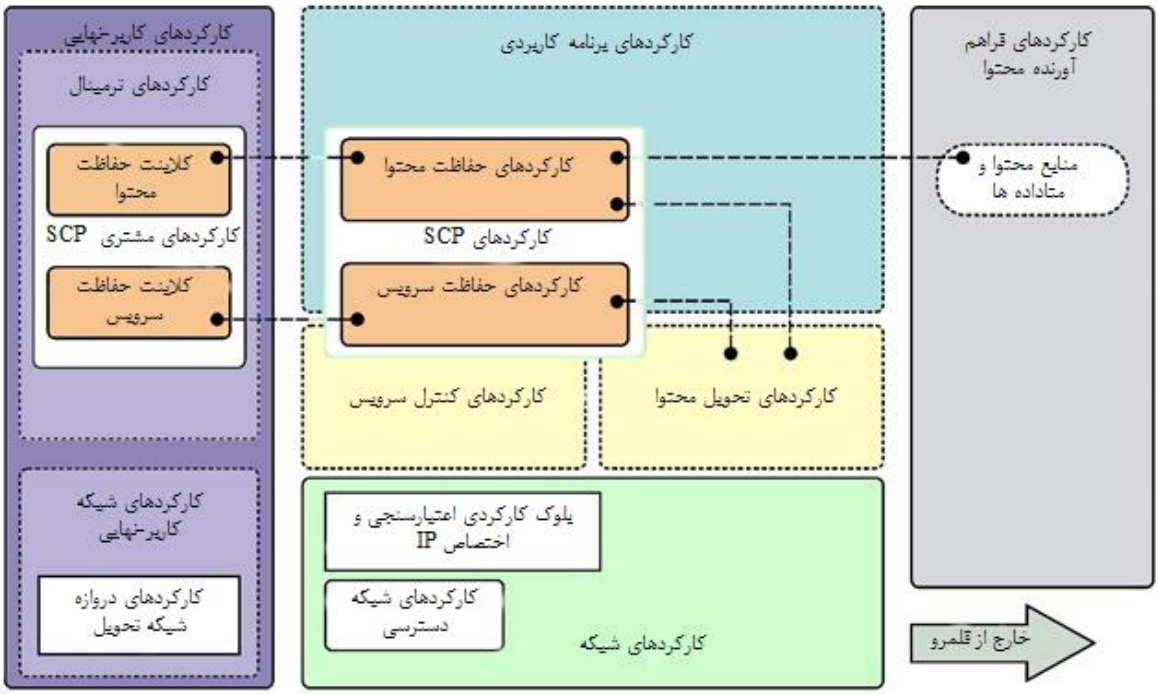
ناحیه اول شامل کاربر نهایی، ارائه‌دهنده شبکه، و ارائه‌دهنده خدمات می‌شود در حالی که ناحیـه دوم شـامل حوزه ارائه‌دهنده محتوا می‌شود.

در ناحیه دوم، تمام جنبه‌های امنیتی در داخل حوزه ارائه‌دهنده محتوا و اتصال متقابل بین ارائه‌دهنده محتوا و ارائه‌دهنده خدمات تحت توافق‌های خصوصی بین ذینفعان فعال در این حوزه‌ها قـرار دارد. بنـابراین فـرض می‌شود که این موارد خارج از قلمرو این مجموعه توصیه است.

اگر چه حوزه ارائه‌دهنده محتوا و اتصال متقابل بین حوزه‌ی ارائه‌دهنده محتوا و ارائـه‌دهنـده خـدمات فـرض می‌شود که خارج از قلمرو متن کنونی باشند، اما حوزه ارائه‌دهنده محتوا در شکل‌ها و توضیحات زیـر جهـت تکمیل بحث گنجانده شده است. از این رو، هرگونه توضیح و عبارت در مورد این حوزه‌ها لازم اسـت کـه بـه عنوان یک عبارت توضیحی یا آموزشی تلقی شود.

**یادآوری ۱-** کارکردهای حفاظت محتوا و کارکردهای حفاظت خدمات در این شکل، مهم‌ترین بسته‌های معماری امنیت IPTV است. بحث‌های دقیق در مورد این کارکردها را می‌توان در شکل ۷-۲ (معماری حفاظت محتوا) و شکل ۷-۳ (معماری حفاظت خدمت) یافت.

**یادآوری ۲-** برای معماری IPTV برخی کارکردها و بسته‌های کارکردی که بدون رابطه مستقیم با امنیت IPTV است در ایـن شکل جهت ساده‌سازی حذف شده‌اند.




**شکل ۷-۱ معماری امنیت کلی IPTV**

**یادآوری ۱**- کارکردهای حفاظت محتوا و کارکردهای حفاظت خدمات در این شکل، مهم‌ترین بسته‌های معماری امنیت IPTV است. بحث‌های دقیق در مورد این کارکردها را می‌توان در شکل ۷-۲ (معماری حفاظت محتوا) و شکل ۷-۳ (معماری حفاظت خدمت) یافت.

**یادآوری ۲**- برای معماری IPTV برخی کارکردها و بسته‌های کارکردی که بدون رابطه مستقیم با امنیت IPTV است در این شکل جهت ساده‌سازی حذف شده‌اند.

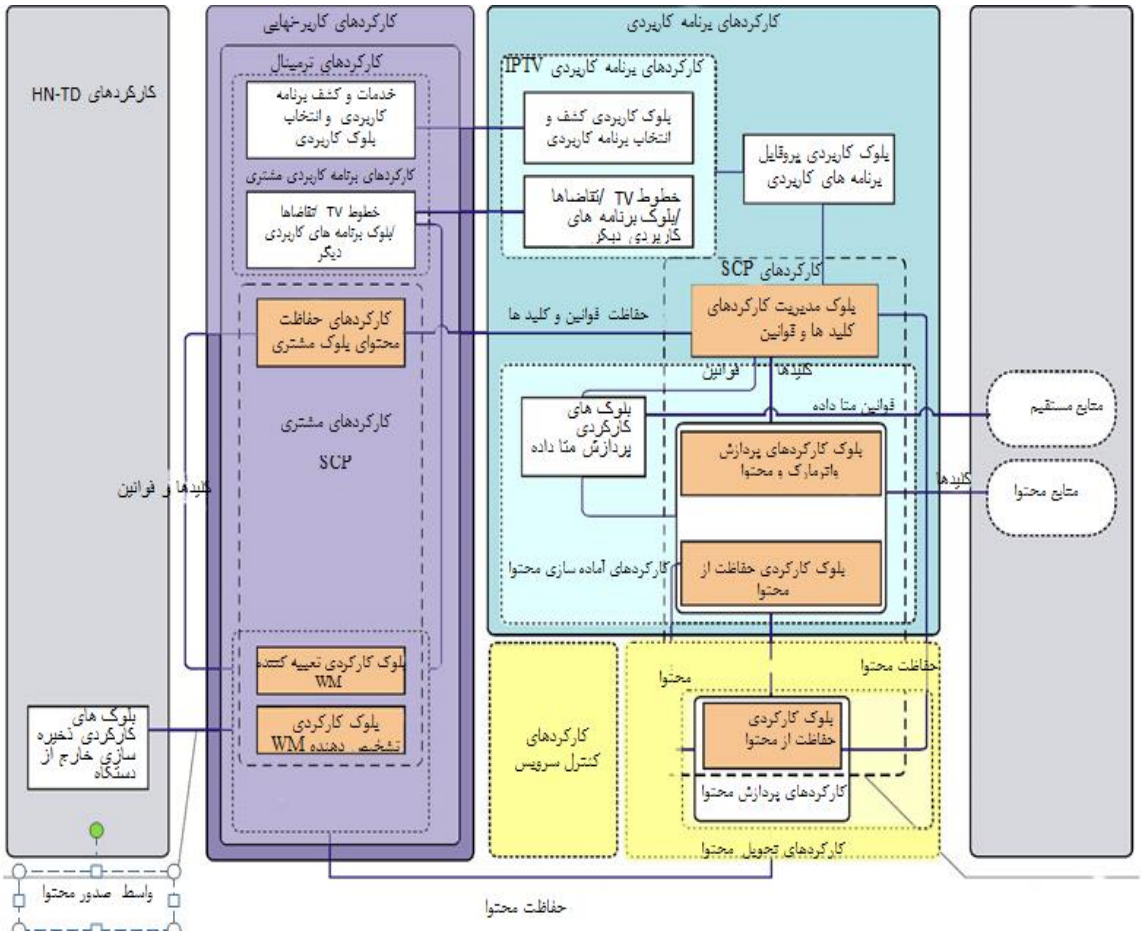
معماری امنیت عمومی IPTV به‌طور کلی به چهار حوزه کارکردی به صورت زیر تقسیم می‌شود:

- کارکردهای ارائه‌دهنده محتوا (که از لحاظ فنی خارج از قلمرو این مجموعه توصیه است): فرض می‌شود که ارائه‌دهنده محتوا، دسترسی به محتوا را برای فراهم‌آورندگان خدمات که روابطی را با ارائه‌دهنده محتوا ایجاد کرده‌اند، فراهم می‌آورد. در برخی موارد ارائه‌دهنده محتوا خود ممکن است ارائه‌دهنده خدمات نیز باشد. در چنین مواردی رابطه بیان‌شده به عنوان یک رابطه داخلی محسوب می‌شوند. در فراهم آوردن دسترسی به محتوا برای فراهم‌آورندگان خدمات، ارائه‌دهنده محتوا می‌تواند از سازوکارهای استاندارد یا خصوصی برای واپایش و امکان‌پذیر کردن دسترسی به محتوا استفاده کند؛ با این وجود توجه شود که چنین سازوکارهایی فراتر از قلمرو این مجموعه توصیه تلقی می‌شوند و تنها تحت توافق خصوصی بین ذینفعان قرار دارند.
- کارکردهای حفاظت خدمات و محتوا (SCP) (که با قسمت‌های معینی در کارکردهای برنامه کاربردی، کارکردهای واپایش خدمات و کارکردهای تحویل محتوا همپوشانی دارند): کارکردهای SCP نقش مهمی در معماری امنیت کلی IPTV به خصوص در حوزه ارائه‌دهنده خدمات ایفا می‌کنند. به‌طور خاص کارکردهای حفاظت خدمات، امکان حفاظت زیرساخت خدمات و همچنین واپایش دسترسی به خدمات و محتوای میزبانی شده در آن‌ها را فراهم می‌آورد. از سوی دیگر، کارکردهای حفاظت محتوا امکان واپایش استفاده از خدمات و محتوا را مطابق با استفاده‌های مجاز و مجوز دار فراهم می‌آورد. کارکردهای ویژه و بسته‌های کارکردی ویژه مربوط به کارکردهای SCP در ۳ زیر ناحیه پراکنده شده‌اند. کارکردهای برنامه کاربردی، کارکردهای واپایش خدمات و کارکردهای تحویل محتوا. ارائه‌دهنده خدمات توسط مجوز یا مجوزهای ارائه‌شده توسط ارائه‌دهنده محتوا متعهد می‌شود تا محتوا را تنها تحت شرایط معین استفاده، برای مثال یک بار دیدن بدون قابلیت ضبط کردن، یک بار ضبط کردن به همراه چند بار دیدن، یک بار ضبط کردن به همراه انتقال حقوق ضبط کردن و...، در دسترس قرار دهد. هدف اصلی جنبه‌های حفاظت محتوا در کارکردهای SCP این است که به ارائه‌دهنده خدمات اجازه داده شود تا چنین تعهداتی را در روشی قابل وارسی برآورده سازد. هدف اصلی جنبه‌های حفاظت خدمات در کارکردهای SCP عبارت است از جلوگیری از دسترسی غیرمجاز به منابع خدمات و اطلاعاتی که در حوزه‌های مختلف خدمات، شبکه، افزاره پایانه، و کاربر نهایی (مشترک) توسط هستارها به عنوان اطلاعات محرمانه تلقی می‌شوند. هدف ثانویه جنبه‌های حفاظت خدمات در کارکردهای SCP عبارت است از حفظ زیرساخت خدمات در برابر آسیب‌های ناشی از سوءاستفاده عمدی و/یا اتفاقی از منابع. جزئیات بسته‌های کارکردی مربوط به کارکردهای حفاظت محتوا و کارکردهای حفاظت خدمات به ترتیب در شکل‌های ۷-۲ (معماری حفاظت محتوا) و شکل ۷-۳ (معماری حفاظت خدمات) نشان داده شده‌اند.

- کارکردهای شبکه: کارکردهای امنیتی که به تمرکز حوزه شبکه بر اصالت‌سنجی هستارها و مجوزدهی دسترسی به شبکه‌ای که خدمات IPTV از طریق آن تحویل می‌شوند و یا تحویل خواهند شد می‌پردازند. کارکرد ثانویه در اینجا عبارت است از حفاظت از یکپارچگی خود شبکه به صورت فیزیکی، الکترونیکی و عملیاتی (برای مثال از طریق تشخیص و ناکام‌گذاشتن حملات رد خدمت بر روی شبکه‌ی دسترسی یا شبکه حامل) .
- کارکردهای کاربر-نهایی: جنبه‌هایی از امنیت که برای کاربر نهایی (مشترک) اعمال می‌شوند و حفاظت یکپارچگی TD که بر اساس خصوصیات مطرح شده توسط مشترک کار می‌کند و همچنین حفاظت حریم‌خصوصی کاربر نهایی را شامل می‌شود. تحت شرایط معین یک DNT بین TD و حوزه شبکه در داخل حوزه کاربر نهایی می‌توان در نظر گرفت که تحت معیارهای و سنجه‌های امنیت کاربر نهایی قرار دارد.
- در نهایت، توصیه می‌شود که سازوکارهای یکپارچگی جهت تضمین یکپارچگی محتوای دریافت شده توسط یک TD که بعداً به سایر افزاره‌ها در داخل و یا خارج شبکه اصلی (شبکه خانه) توزیع مجدد می‌شود، اعمال شود (این کار منجر به همپوشانی جنبه‌های امنیت کاربر نهایی و جنبه‌های امنیت محتوا می‌شود) . توصیف دقیق‌تر این کارکردها و بسته‌های کارکردی نشان داده شده در شکل ۷-۱ در بند ۷-۴ ارائه شده است.

### ۷-۲ معماری حفاظت محتوا

معماری حفاظت محتوا در شکل ۷-۱ نشان داده شده است کارکرد اصلی این معماری حفاظت محتوا عبارت است از تعیین جریان و پردازش اطلاعات مرتبط با حقوق استفاده محتوا و اطلاعات لازم برای مدیریت و تسهیل این حقوق در نهایت، حقوق استفاده محتوا از ارائه‌دهنده محتوا ناشی می‌شوند؛ با این وجود توجه شود که چنین حقوقی می‌تواند توسط ارائه‌دهنده خدمات، مطابق با توافق ارائه‌دهنده خدمات با ارائه‌دهنده محتوا و سیاست‌های عملیاتی و کسب‌وکاری مورد اصلاح قرار گیرند (برای مثال محدودتر و یا حتی گسترده‌تر شوند).




الف) ایجاد فراداده‌های نشانه‌گذاری اختیاری برای تسهیل تعبیه نشانه‌گذاری جریان پایین دست.

ب) تعبیه کننده نشانه‌گذاری اختیاری جهت انفرادی‌سازی محتوا برای شبکه‌ها، کارسازها و تحویل‌های تک ـ پخشی.

ج) تعبیه کننده نشانه‌گذاری اختیاری جهت انفرادی سازی موارد محتوای چندپخشی.

د) تشخیص دهنده اختیاری برای نشانه‌گذاری‌های محافظت رونوشت برداری.

هـ) ذخیره اختیاری خارج از- افزاره: یک افزاره ذخیره‌سازی در داخل HN-TD

و) بخش کارکردی رمزنگاری محتوا، قرار گرفته در کارکردهای تحویل و ذخیره‌سازی محتوا، اختیاری است.

**یادآوری**- بسته‌های کارکردی حفاظت محتوا در این شکل متشکل است از کارکردهای حفاظت محتوا و کارکردهای کارخواه حفاظت محتوا.

**شکل ۷-۲ معماری حفاظت محتوا IPTV**

معماری حفاظت محتوای نشان داده شده در بالا متشکل است از کارکردهایی که به طور عمده در دو حوزه کارکردی قرار می‌گیرند:

- کارکردهای حفاظت خدمات و محتوا (که با کارکردهای برنامه کاربردی و کارکردهای تحویل محتوا همپوشانی دارند): محتوا و حقوق مربوط به آن از ارائه‌دهنده محتوا جمع‌آوری می‌شوند، در یک مجموعه تجمیع می‌شوند و برای تحویل به کاربر نهایی پردازش می‌شوند که در آن فرآیند کلی توسط چندین کارکرد نظیر کارکرد آماده‌سازی محتوا با استفاده از داده‌های توصیف کننده حقوق کاربر نهایی و شرایط مرتبط مدیریت می‌شود. اطلاعات محتوا، حقوق و کلیدها (که برای اعطای دسترسی به محتوا و

امکان‌پذیر کردن استفاده از آن) به کار می‌روند، در شکلی مناسب برای یک کاربرد ویژه، برای مثال تماشای تلویزیون خطی، سازماندهی می‌شود. اطلاعات حقوق و اطلاعات کلیدها به بخش کارکردی کارخواه حفاظت محتوا در افزاره پایانه به عنوان استحقاق (برای مثال EMM) اعطاشده توسط بخش کارکردی مدیریت حقوق و کلیدها، تحویل داده می‌شود؛ محتوا جهت اضافه کردن فراداده‌های ردگیری محتوا (برای مثال نشانه‌گذاری‌ها) به عنوان یک گزینه پردازش می‌شوند و سپس در کارکردهای آماده‌سازی محتوا قبل از تحویل، تحت پنهان‌سازی قرار می‌گیرند. در برخی موارد (برای مثال خدمات IP زمان واقعی) ، محتوا را همچنین می‌توان توسط تحویل کارکردهای محتوا به عنوان یک گزینه، مورد رمزنگاری قرار داد.

در زمینه معماری حفاظت محتوای IPTV (بر خلاف معماری حفاظت IPTV که در ادامه توصیف خواهد شد) ، بر خلاف رمزنگاری این اطلاعات یا محتوای قرار گرفته تحت این حقوق، به طور عمده بر مدیریت، پردازش و تحویل حقوق و کلیدها تمرکز می‌شود.

- کارکردهای کاربر- نهایی

کارکردهای پایانه پیاده‌سازی در حوزه‌ی کاربر نهایی مسئولیت پیاده‌سازی قواعد مرتبط با اطلاعات حقوق استفاده محتوا (که همچنین به نام فراداده‌های حفاظت محتوا نامیده می‌شوند) بر عهده دارند. این هستار کارکردی، حقوق و کلیدهای محتوا به دست آمده از بخش کارکردی مدیریت حقوق و کلیدها را تفسیر کرده و سپس بر اساس این تفسیر اقدام به واپایش چگونگی پردازش محتوا و چگونگی قرارگیری آن در معرض کاربر نهایی می‌کند که این کار را از طریق افزاره‌های یکپارچه ارائه (برای مثال سامانه نمایش یا پخش صدا) و یا از طریق اتصالات متقابل فیزیکی با افزاره‌های خارجی انجام می‌دهد. در مواردی که در آن‌ها TD محتوای محافظت شده را به یک افزاره خارجی (برای مثال خروجی نمایش) ارسال می‌کند، حقوق محتوا را می‌توان به شکل‌های دیگری ترجمه و تبدیل کرد؛ محتوایی که برای آن چنین استفاده‌ای به کار می‌رود را می‌توان مورد پردازش بیشتر قرار داد تا اطلاعات ردگیری محتوا در طرف- کارخواه (نشانه‌گذاری‌ها) را به عنوان یک گزینه یا محتوای رمزنگاری شده مجدد برای پیاده‌سازی واپایش دسترسی جریان پایین دست در آن وارد کرد.

توصیف‌های دقیق‌تر بسته‌های معماری نشان داده شده در شکل ۷-۲ در بند ۷-۴ ارائه خواهد شد.

در شکل ۷-۲، واسط صدور محتوا عبارت است از واسط منطقی که IPTV TD و HN-TD را به هم متصل می‌کند.

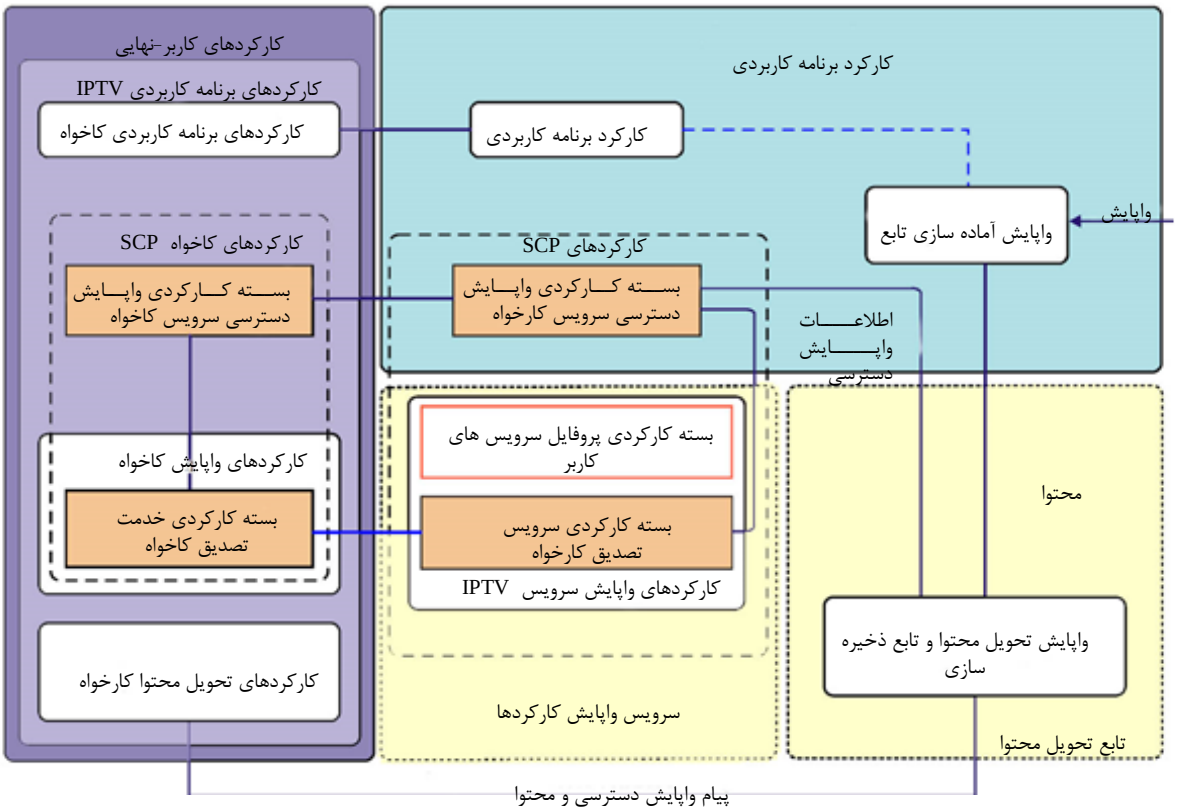
HN-TD می‌تواند محتوا را مصرف کند و یا محتوا را به یک HN-TD دیگر ارسال کند. کارکردهای کارخواه تحویل محتوا می‌توانند برچسب امنیتی متناظر را جهت تضمین این که تنها سامانه HN-TD مجاز می‌تواند محتوا را مصرف و صادر کند، تنظیم کند.

### ۷-۳ معماری حفاظت خدمت

برای خدمات مدیریت‌شده از جمله محتوای حفاظت شده، یک حالت معمول حالتی است که در آن کاربر نهایی (مشترک) و TD باید جهت دسترسی به خدمت و محتوای میزبانی شده در آن، مورد اصالت‌سنجی و

مجوزدهی قرار گیرند بسته به شرایط، کارکردهای اصالت‌سنجی و مجوزدهی را می‌توان به صورت جداگانه بر روی TD و کاربر نهایی پیاده‌سازی کرد. در موارد دیگر، افزاره‌های اضافی دیگری در قسمت کاربر- نهایی، نظیر دروازه شبکه تحویل و دیگر افزاره‌های کاربر نهایی ممکن است لازم باشد قبل از اعطای مجوز برای دسترسی به خدمت اصالت‌سنجی شود.

ترکیبی از اصالت‌سنجی و مجوزدهی را می‌توان برای واپایش دسترسی به خدمت IPTV و TD به منظور اهداف اکتساب خدمت و محتوا قبل از استفاده مورد استفاده قرار داد. معماری حفاظت خدمت برای IPTV در شکل ۷-۳ نشان داده شده است.




الف- اصالت‌سنجی: نام و ID مشترک را به همراه امتیاز مخصوص او شناسایی می‌کند.

ب- واپایش دسترسی خدمت: برای محافظت یک خدمت از دسترسی غیرمجاز غیرقانونی.

**یادآوری**- بسته‌های کارکردی حفاظت خدمت در این شکل متشکل از کارکردهای حفاظت خدمت و کارکردهای کارخواه حفاظت خدمت است.

**شکل ۷-۳معماری حفاظت خدمت برای IPTV**

کارکردهای اصلی معماری حفاظت خدمت شامل موارد زیر می‌شود:

- اصالت‌سنجی (دریافت کننده) و TD:

این کارکرد مسئول اصالت‌سنجی مشترکان و TDها است.

- اصالت‌سنجی مشترک (دریافت کننده): فرآیند اصالت‌سنجی کاربر
- اصالت‌سنجی TD: فرآیند اصالت‌سنجی TD

در حالتی که در آن گواهی‌های مبتنی بر X.509 به عنوان اعتبارنامه برای اصالت‌سنجی مورد استفاده قرار می‌گیرد، یک کارکرد رجوع[1] مورد نیاز است.

- اصالت‌سنجی کارساز:
  - در TD، یک کارکرد برای اصالت‌سنجی کارساز جهت اصالت‌سنجی متقابل.
- واپایش دسترسی خدمات:
  - کارکردی برای محدود کردن اکتساب و دسترسی به خدمات توسط کاربران مجاز با استفاده از سازوکارهای امنیتی نظیر مخلوط سازی و رمزنگاری.

توضیحات بیشتر در مورد بسته‌های معماری نشان داده شده در شکل ۷-۳ در بند ۷-۴ ارائه شده است.

### ۷-۴ توصیف کارکردها و بسته‌های کارکردی در معماری‌های امنیت IPTV

در این بند جزئیات توصیفی بیشتری در مورد کارکردها و بسته‌های کارکردی نشان داده شده در مدل‌های معماری مطرح شده در بند ۷-۱ (معماری امنیت عمومی) ، بند ۷-۲ (معماری حفاظت محتوا) ، و بند ۷-۳ (معماری حفاظت خدمت) ارائه می‌شود. این کارکردها و بسته‌های کارکردی تنها بر حسب عبارات و اصطلاحات توصیفی کلی تعریف می‌شوند و متناظر با هر یک از این سه بند، به سه قسمت تقسیم می‌شوند.

#### ۷-۴-۱ کارکردها و بسته‌های کارکردی معماری عمومی

**کارکردهای شبکه دسترسی**: برای جمع‌آوری و تجمیع واپایش و داده‌های نشات گرفته در شبکه ارائه می‌شوند؛ QoS/QoE از جمله مدیریت بافر[2]، صف‌بندی و زمان‌بندی، فیلتر سازی بسته، دسته‌بندی ترافیک، علامت‌گذاری، سیاست‌گذاری، و شکل دهی ترافیک را امکان پذیر می‌کند.

**یادآوری ۱**- این کارکردها از نقطه نظر حفاظت خدمت و محتوای IPTV مستقل از کارکردهای حفاظت خدمت و محتوا/ست.

**کارکردهای کاربردی**: بین طرف کارساز (ارائه‌دهنده خدمت) و طرف کارخواه (کاربر نهایی) تقسیم می‌شوند. متشکل است از مؤلفه‌های کارکردی است که برنامه‌های کاربردی IPTV را در سطح خدمات مورد آماده‌سازی، دریافت، و پردازش قرار می‌دهند، نظیر تلویزیون خطی، VoD و محتوای مرتبط نظیر اطلاعات دسترسی پذیری، برنامه‌های کاربردی تعاملی و غیره.

**بخش کارکردی اصالت‌سنجی و اختصاص IP:** قابلیت کارکرد برای بخش کارکردی دروازه شبکه‌ی تحویل که کارکردهای شبکه و همچنین اختصاص نشانی IP را به کارکردهای پایانه IPTV متصل می‌کند فراهم می‌آورد.

**کارکردهای حفاظت محتوا:** سازوکارهایی را فراهم می‌آورد که پیاده‌سازی سیاست‌های استفاده محتوا از جمله تجمیع، توزیع و مدیریت حقوق و کلیدها، ایجاد اختیاری و وارد کردن (جاسازی کردن) اطلاعات ردگیری

---

۱ - Revocation

۲ - Buffer

محتوا (برای مثال نشانه‌گذاری‌ها) و رمزنگاری محتوا (تحت واپایش کارکردهای حفاظت خدمت) را امکان پذیر می‌کند.

**یادآوری ۲-** بسته‌های کارکردی ویژه که کارکردهای حفاظت محتوا را شکل می‌دهند به‌طور مفصل‌تر در بنـدهای ۷-۲ و ۷-۴-۲ مورد بحث قرار خواهند گرفت.

**کارکردهای کارخواه حفاظت محتوا:** با کارکردهای حفاظت محتوا در طرف- کارساز فعل و انفعال متقابل دارند تا سیاست‌های استفاده محتوا پیاده‌سازی شود.

**کارکردهای ارائه‌دهنده محتوا:** محتوا و حقوق محتوا و فراداده‌های کلید را به فراهم‌آورندگان خدمت تحویل می‌دهند.

**کارکردهای دروازه‌ی شبکه‌ی تحویل:** برای اتصال بین افزاره پایانه و شبکه تحویل ارائه می‌شوند. اتصال محلی IP (امکانات کاربر- نهایی) را مدیریت می‌کنند، نشانی‌های پروتکل اینترنت (IP) و پیکربندی IP را برای TD به دست می‌آورند.

**یادآوری ۳-** این کارکردها از نقطه نظر حفاظت خدمت و محتوای IPTV، مستقل از کارکردهای حفاظت خدمت و محتوا است.

**کارکردهای حفاظت خدمت:** سازوکارهایی برای انجام اصالت‌سنجی و مجوزدهی برای دسترسی به خدمات و محتوای IPTV مرتبط و واپایش این دسترسی، از جمله واپایش و پیاده‌سازی مستقیم نشانک واپایشی و رمزنگاری تبادل محتوا به صورت مستقل و یا توأم با کارکردهای حفاظت محتوا، فراهم می‌آورند.

**یادآوری ۴-** این کارکردها از نقطه نظر حفاظت خدمت و محتوای IPTV، مستقل از کارکردهای حفاظت خدمت و محتوا است.

**یادآوری ۵-** بسته‌های کارکردی ویژه که کارکردهای حفاظت خدمت را تشکیل می‌دهند به‌طور مفصل‌تر در بنـدهای ۷-۳ و ۷-۴-۳ مورد بحث قرار می‌گیرند.

**کارکردهای کارخواه محافظت خدمت:** با کارکردهای حفاظت خدمت بر روی کارساز جهت انجام واپایش دسترسی خدمت و دیگر کارکردهای حفاظتی تعامل دارند.

**کارکردهای پایانه:** حفاظت خدمت و کارخواه‌های حفاظت محتوا برای رمزگشایی و پیاده‌سازی سیاست‌های استفاده از خدمت و محتوا را مطابق با فراداده‌های حقوق استفاده، فراهم می‌آورند؛ انجام رمزنگاری لایه پیوند و انتقال (تبادل) SCP که برای خروجی محتوای بیشتر جریان پایین دست یا توزیع مجدد آن و ذخیره‌سازی محتوای داخلی (یا خارجی) از جمله پشتیبانی برای خطوط پردازش امن (مقاوم در برابر مداخله) رسانه، ذخیره‌سازی محلی کلیدهای سری، قابلیت نوسازی نرم‌افزار امنیتی، اصالت‌سنجی و وارسی دارایی‌های نرم‌افزاری بارگیری شده و حفاظت داده‌های ذخیره‌شده محلی و تبادل شده کاربر تحت ملاحظات حریم‌خصوصی کاربر نهایی مورد نیاز است.

### ۷-۴-۲ کارکردها و بسته‌های کارکردی معماری حفاظت محتوا

**کارکردهای کارخواه برنامه کاربردی:** نقطه اصلی هماهنگی و واپایش تعاملات بین کاربر نهایی و خدمت یا خدمات فراهم آمده توسط کارکردهای برنامه کاربردی IPTV؛ برای کاربردهای استاندارد نظیر تماشای

تلویزیون خطی، جهت واسط اصلی کاربر و الگوی بهره برداری که از طریق آن کاربر نهایی یک خدمت را به دست می‌آورد، ارائه می‌شود.

- بخش کارکردی کارخواه کشف و انتخاب برنامه کاربردی: به کاربر نهایی و/ یا افزاره پایانه امکان می‌دهد تا وجود برنامه‌های کاربردی و خدمات کاربردی در دسترس از ناحیه ارائه‌دهنده خدمات را کشف و آن‌ها را انتخاب کند.

کارکردهای برنامه کاربردی IPTV: هستارهای منطقی که در برگیرنده‌ی نقطه‌ی شروع برخی خدمات IPTV نظیر تلویزیون خطی، VoD، و غیره است؛ مسئولیت هماهنگ کردن تمام تأسیسات ارائه‌دهنده خدمات برای امکان پذیر کردن وجود برخی خدمات عملیاتی را بر عهده دارند.

- بخش کارکردی کشف و انتخاب برنامه کاربردی: با بخش کارکردی کارخواه کشف و انتخاب برنامه کاربردی که در بالا توصیف شد تعامل دارد و به کاربر نهایی و/ یا افزاره پایانه امکان می‌دهد تا وجود برنامه‌های کاربردی و خدمات کاربردی را کشف و آن‌ها را انتخاب کند.

**بخش کارکردی پروفایل برنامه کاربردی**: اطلاعات پیکربندی برنامه‌های کاربردی و خدمات را هم برای یک هستار عمومی و کلی و هم برای هستار ویژه کاربر نهایی (مشترک) ذخیره‌سازی کرده و مدیریت می‌کند؛ به‌طور معمول برای اعطای اجازه به کارساز یا کارسازهای برنامه کاربردی جهت سفارشی سازی خدمات و محتوا برای کاربر نهایی مورد استفاده قرار می‌گیرد و به‌طور معمول با سامانه‌های مختلف حسابرسی (داخلی) تعامل دارد و یا آن‌ها را پیاده‌سازی می‌کند.

**کارکردهای آماده سازی محتوا**: انواع مختلف پیش پردازش محتوا قبل از تحویل را انجام می‌دهند نظیر تحلیل ردگیری محتوا (برای مثال نشانه‌گذاری) و ایجاد فراداده‌ها، همتافتگری محتوا و فراداده‌های محتوا و رمزنگاری محتوا.

- بخش کارکردی پردازش محتوا و نشانه‌گذاری: گام یا گام‌های اختیاری پردازش که محتوا را مورد تحلیل قرار می‌دهند تا فراداده‌های ردگیری محتوا (برای مثال نشانه‌گذاری) برای استفاده در فرآیند بعدی جریان پایین دست، به خصوص فرآیند انفرادیسازی (که توسط اطلاعات ارائه‌شده توسط منبع مرتبط شناسایی می‌شوند) این فراداده‌ها را ایجاد کند.
- بخش کارکردی پردازش فراداده: فراداده‌های مرتبط با برنامه و اطلاعات حقوق استفاده تحویل شده توسط محتوا را مورد مدیریت و پردازش قرار می‌دهد.
- بخش کارکردی رمزنگاری محتوا: فرآیند رمزنگاری محتوای حفاظت شده را پیاده‌سازی می‌کند تا واپایش دسترسی و محرمانگی محتوای مرتبط را در حین فرآیند تحویل محتوا تسهیل کند؛ محتوا را می‌توان در زمان واقعی یا به صورت آفلاین (برون خط) رمزنگاری کرد (رمزنگاری می‌تواند به صورت اختیاری از تبدیل امن کد بدون رمز گشایی پشتیبانی کند) .

**یادآوری ۱**- رمزنگاری محتوا را می‌توان در کارکردهای آماده سازی محتوا در داخل لایه کاربردی پیاده‌سازی کرد. در این موارد همچنین می‌توان آن را در کارکردهای تحویل محتوا به عنوان یک گزینه پیاده‌سازی کرد.

**بخش کارکردی مدیریت حقوق و کلید**: حقوق و کلیدها را با محتوا مرتبط می‌سازد و توزیع آن‌ها را برای بخش کارکردی کارخواه حفاظت در افزاره پایانه مدیریت می‌کند.

**بخش کارکردی حفاظت محتوا**: حقوق و کلیدها را با استفاده از این اطلاعات جهت واپایش رمز گشایی محتوا و پیاده‌سازی قواعد استفاده به دست می‌آورد و یا دریافت می‌کند؛ نیاز است که این بخش کارکردی مقاوم در برابر مداخله باشد.

**کارکردهای تحویل محتوا**: قابلیت‌های کارکرد ذخیره‌سازی را انجام می‌دهد و محتوا را مطابق با درخواست کارکردهای کاربر- نهایی تحویل می‌دهد، کارکردهای تحویل محتوا می‌توانند به صورت اختیاری، محتوا را مورد پردازش (برای مثال کدگذاری، رمزنگاری) قرار دهند.

**کارکردهای کارخواه تحویل محتوا:** مسئولیت دریافت محتوا در کارکردهای پایانه IPTV را بر عهده دارند؛ رمزگشایی، واتافتگری، کدگشایی و ارائه بعدی و پردازش ذخیره‌سازی بر روی محتوا را انجام می‌دهد (این کارکردها نیز لازم است که دارای قابلیت مقاوم در برابر مداخله باشند) .

**بخش کارکردی آشکارساز نشانه‌گذاری:** اگر این بخش وجود داشته باشد، استفاده از نشانه‌گذاری در محتوای دریافت‌شده از ارائه‌دهنده خدمات را آشکار می‌سازد تا قواعد مطلوب استفاده محتوا در افزاره پایانه یا واسط‌های جریان پایین دست افزاره پایانه را وارسی کرده و یا پیاده‌سازی کند.

**بخش کارکردی تعبیه کننده‌ی نشانه‌گذاری:** اگر این بخش وجود داشته باشد، انفرادی سازی محتوا برای ارائه و ذخیره یا توزیع مجدد بعدی را انجام می‌دهد.

**منابع حقوق:** فرادادهای محتوا در ارتباط با حقوق استفاده محتوا را ایجاد می‌کنند.

**منابع محتوا:** محتوایی که باید تجمیع، پردازش، و سپس از طریق برنامه‌های کاربردی خدمات نظیر تلویزیون خطی، VoD، و غیره به کاربران نهایی تحویل شود را ایجاد می‌کند.

**بخش کارکردی ذخیره‌سازی خارج از افزاره**[1]: سازوکارهای ذخیره‌سازی محتوا بعد از دریافت که از لحاظ فیزیکی در خارج از TD قرار دارند و ذخیره‌سازی و استفاده‌ی محتوای آن‌ها توسط TD مدیریت نمی‌شود.

**یادآوری۲-** اگر ذخیره‌سازی خارجی وجود داشته باشد، و استفاده آن در همه زمان‌ها تحت واپایش TD باشد، در این صورت ممکن است آن را به عنوان یک ذخیره‌سازی «بر روی افزاره» از طریق یک واسط مجاز حفاظت شده بسته به قواعد تطابق و استحکام بودن افزاره پایانه، در نظر گرفت.

### ۳-۴-۷ کارکردها و بسته‌های کارکردی معماری حفاظت خدمت

**بسته کارکردی واپایش دسترسی خدمت**: اساساً مسئولیت واپایش دسترسی خدمت را بر عهده دارد؛ سازوکارهای امنیتی نظیر مخلوط سازی و رمزنگاری توسط این بسته کارکردی جهت جلوگیری از دسترسی یا اکتساب غیرمجاز خدمات از سوی کاربران مورد استفاده قرار می‌گیرند.

---

۱ - OFF-DEVICE

**بسته کارکردی کارخواه  واپایش دسترسی خدمت**: وظایف مرتبط با حفاظت خدمت را بر روی کارخواه  آن گونه که توسط بسته کارکردی کارخواه  واپایش دسترسی خدمت در طرف کارساز تعریف می‌شود، پیاده‌سازی می‌کند.

**بسته کارکردی اصالت‌سنجی خدمت**: اصالت‌سنجی را جهت وارسی اعتبار کاربر و/ یا TD انجام می‌دهد؛ همچنین از درخواست‌های اصالت‌سنجی که از سوی TD جهت وارسی کارساز ارائه می‌شوند پشتیبانی می‌کند.

**بسته کارکردی کارخواه  اصالت‌سنجی خدمت:** در کنار انجام وظایف اصالت‌سنجی مشترک (کاربر) در طرف کارخواه، شامل وارسی اعتبار طرف کارساز در حفاظت خدمات جهت اصالت‌سنجی متقابل می‌شود.

## ۸  سازوکارهای امنیتی

در این مجموعه توصیه‌ها هیچ گونه سازوکار یا راهکار امنیتی ویژه‌ای تعریف نمی‌شود بلکه سازوکارهای امنیتی معینی در حالت کلی توصیف می‌شوند که می‌توان آن‌ها را برای اهداف تعریف یا پیاده‌سازی سازوکارهایی که الزامات امنیتی را برآورده می‌سازند، که به الزامات امنیتی، هستارهای کارکردی امنیتی معماری، و تهدیدات امنیتی می‌پردازد. سازوکارهای امنیتی توصیف شده زیر به‌طور جامع به همه الزامات امنیتی فهرست شده در بالا نمی‌پردازد.

### ۸-۱  سازوکارهای امنیتی مربوط به حفاظت محتوا

سازوکارهای امنیت محتوا شامل مجموعه‌ای از کارکردهایی می‌شوند که بین محتوا و TDها پیاده‌سازی می‌شوند تا تضمین شود که محتوا را می‌توان به صورت امن توسط یک شبکه توزیع (یا ارسال) کرد و کاربر نهایی می‌تواند این محتوا را به صورت امن اکتساب، مصرف، صادر، ذخیره‌سازی، و توزیع مجدد (یا ارسال مجدد) کند.

سازوکار امنیت محتوا را می‌توان برای توزیع محتوا، اکتساب محتوا، مصرف محتوا، ذخیره‌سازی محتوا، صدور محتوا و توزیع مجدد محتوا به کار برد. سازوکارهای زیر را می‌توان برای برآورده‌سازی الزامات محتوای IPTV و حفاظت خدمت به کار برد (همه آن‌ها اختیاری است).

#### ۸-۱-۱  رمزنگاری محتوا

در بسیاری از موارد محتوا را می‌توان برای جلوگیری از استفاده غیرقانونی از آن‌ها در حین تحویل رمزنگاری کرد.

#### ۸-۱-۲  ردگیری و شناسایی محتوا

ردگیری محتوا برای شناسایی و ردگیری منشأ (منبع) محتوا و/یا طرف مسئول آن (برای مثال کاربر نهایی) به کار می‌رود تا بررسی‌های بعدی در صورت وجود دسترسی و استفاده غیرمجاز از محتوا تسهیل شود.

اطلاعات ردگیری محتوا را می‌توان به صورت فراداده‌ها یا نشانه‌گذاری قانونی به محتوا الحاق کرد. نشانه‌گذاری‌های ردگیری محتوا به‌طور معمول به گونه‌ای طراحی می‌شوند که استحکام و غیرقابل مشاهده باشند تا از حذف ناخواسته یا غیرعمدی آن‌ها جلوگیری شود.
توصیه می‌شود که شناسایی محتوا از طریق یک فناوری امضای ویدئو آسان شود.

### ۸-۱-۳ نشانه‌گذاری‌گذاری

نشانه‌گذاری‌گذاری به فرآیند اضافه کردن اطلاعاتی به محتوا از طریق تغییر ویژگی‌های معین محتوا اشاره دارد. این حوزه مطالعاتی به نام «استگانوگرافی[۱]» نامیده می‌شود. نشانه‌گذاری‌گذاری برای بسیاری از کاربردها ترجیح داده می‌شود زیرا حذف این اطلاعات از محتوا دشوار است. در یک خدمت IPTV، نشانه‌گذاری‌گذاری ممکن است به لحاظ کردن اطلاعات مخفی به‌طور مستقیم در یک فایل ویدئویی یا یک جریان صوتی از محتوا همتافتگر شده اشاره داشته باشد. به‌طور مطلوب، نشانه‌گذاری‌ها برای انسان غیر قابل مشاهده و/یا غیر قابل شنیده شدن است اما در تبدیل قالب‌های فایل‌های رسانه‌ای به یکدیگر این نشانه‌گذاری‌ها به خوبی باقی می‌مانند و تغییر نمی‌کنند.

### ۸-۱-۴ برچسب‌گذاری محتوا

برچسب‌گذاری محتوا عبارت است از فرآیند وارد کردن یا الحاق کردن فراداده‌ها به محتوا که توصیف شده هستار محتوا و همچنین جنبه‌ها و خصوصیات محتوا است.
محتوای برچسب‌گذاری شده با این فراداده‌ها را می‌توان به صورت آسان‌تری توسط افزاره‌های میانی در زنجیره تحویل محتوا مورد ذخیره‌سازی، فیلتر سازی، یا دسته‌بندی قرار داد.
برخی نواحی، پیاده‌سازی‌ها و یا پیاده‌سازی‌های ویژه IPTV ممکن است نیازمند وجود انواع معینی از برچسب‌های محتوا نظیر اطلاعات نرخ‌بندی[۲] باشند تا امکان درجه‌ای از واپایش کاربر نهایی (مشترک) بر روی محتوایی که نامناسب یا مضر تلقی می‌شود فراهم شود.

### ۸-۱-۵ طرح تبدیل کد ایمن

طرح تبدیل کد ایمن (STS) به نوعی طرح امنیتی که به یک گره میانی امکان می‌دهد تا تبدیل کد را بدون رمزگشایی انجام دهد و در عین حال امنیت انتها-به-انتها را نیز حفظ کند، اشاره دارد. این طرح را می‌توان با ترکیب کدگذاری مقیاس‌پذیر، رمزنگاری تصاعدی و تبدیل داده‌ها به بسته‌های داده به دست آورد. سه هستار در این ارتباط وجود دارد: یک گیرنده، یک گره میانی شبکه، و یک کاربر دارای یک پایانه IPTV. یک فرستنده یک کارکرد تبدیل کد ایمن را جهت ایجاد بسته‌های رمزنگاری شده مقیاس‌پذیر از فایل ویدئو پیاده‌سازی می‌کند و یک سرآیند رمزنگاری نشده را برای ارسال اطلاعات اضافه می‌کند؛ یک گره میانی شبکه، سرآیند رمزنگاری نشده را می‌خواند و از این اطلاعات برای کوتاه کردن یا کنار گذاشتن تعداد کافی

---

۱ - Steganography

۲ - Rating

بسته‌ها مطابق با عملیات مطلوب تبدیل کد استفاده می‌کند و پایانه IPTV، بسته‌های رمزنگاری شده را رمزگشایی می‌کند و بسته متن-ساده[1] را جهت ایجاد ویدئو کدگشایی می‌کند. توصیف مفصل آن در پیوست ۵ ارائه شده است.

**یادآوری**- این بند با هدف تعریف یا توصیف سازوکارهای اضافی برای STS در نظر گرفته نشده است. این موضوع لازم است که در مجموعه توصیه‌های دیگری مورد بحث قرار گیرد.

### ۸-۲ سازوکارهای امنیتی مربوط به حفاظت خدمت

سازوکارهای امنیت خدمت شامل اصالت‌سنجی و مجوزدهی می‌شوند. پیاده‌سازی سازوکارهای واپایش دسترسی ویژه نظیر سامانه‌های رمزنگاری و رمزگشایی را نیز می‌توان لحاظ کرد.

#### ۸-۲-۱ اصالت‌سنجی خدمت

در مورد خدمات مدیریت شده‌ای که برای آن‌ها کاربر نهایی (مشترک) دارای رابطه مستقیمی با ارائه‌دهنده خدمت معین است، ارائه‌دهنده خدمت به‌طور معمول ملزم می‌دارد که افزاره پایانه و/یا کاربر نهایی قبل از ارائه خدمت به یک روش امن (محفوظ) اصالت‌سنجی شود؛ در چنین مواردی، اصالت‌سنجی شامل ایجاد و ارائه اعتبارنامه/اطلاعات به یک شیوه ایمن (محفوظ) می‌شود که می‌توان آن را با پایگاه داده کاربر نهایی ارائه‌دهنده خدمات جهت وارسی اعتبار افزاره پایانه و/یا کاربر نهایی جهت تحویل خدمات مرتبط ساخت.

#### ۸-۲-۲ مجوزدهی خدمت

پس از اصالت‌سنجی کاربر نهایی (مشترک) و/یا افزاره پایانه برای هدف تحویل خدمات، سازوکار مجوزدهی برای اعطای حق دسترسی به خدمات ویژه و محتوای میزبانی شده در آن مطابق با تدارک خدمت و کاربر نهایی (مشترک) است.

#### ۸-۲-۳ واپایش دسترسی خدمت

در بیشتر موارد (و نه همه موارد) ، سامانه حفاظت خدمت حاوی سازوکارهایی است که می‌توانند رمزنگاری (مخلوط‌سازی) و رمزگشایی (تفکیک) ترافیک نشانک‌دهی و ترافیک محتوای واپایش خدمت را پیاده‌سازی کنند. به طور معمول ترافیک واپایش خدمت دوطرفه در هر دوی جهت‌ها، هم از کارساز به کارخواه و هم از کارخواه به کارساز رمزنگاری خواهد شد. از سوی دیگر، جریان محتوا به‌طور معمول تنها از کارساز (ارائه‌دهنده خدمات) به کارخواه (افزاره پایانه) رمزنگاری خواهد شد. با این وجود، فرانامه‌هایی وجود دارد که در آن‌ها جریان محتوا را می‌توان از یک کارخواه به یک کارساز بارگذاری کرد که در این حالت این محتوا را می‌توان بر روی یک افزاره پایانه برای اهداف بارگذاری رمزنگاری کرد (برای مثال برای تضمین این که تنها یک ارائه‌دهنده خدمت مجاز و معتبر می‌تواند به محتوای رمزنگاری شده دسترسی داشته باشد) .

---

۱ - Plain-text

### ۳-۸ سازوکارهای امنیتی مربوط به حفاظت شبکه

در این مجموعه توصیه هیچ‌گونه سازوکاری برای امنیت شبکه تعریف یا توصیف نمی‌شود. در حالت کلی، پیاده‌سازی شبکه‌های هسته مرکزی، دسترسی، حامل و تحویل برای امکان‌پذیر کردن پیاده‌سازی سازوکارهایی که برای حفظ یکپارچگی عملیاتی شبکه لازم تلقی می‌شوند، از جمله تشخیص و جلوگیری از رد خدمت (DoS) انتظار می‌رود. در حالت کلی سازوکارهای امنیتی به کار گرفته شده توسط ارائه‌دهنده خدمات IPTV و TDها به این شبکه‌ها منتقل خواهد شد به شرط آن‌که این سازوکارهای امنیتی در عناصر داده بار مفید ارائه‌شده توسط لایه‌های شبکه پیاده‌سازی شوند.

### ۴-۸ سازوکارهای امنیتی مربوط به حفاظت افزاره پایانه

سازوکارهای امنیت افزاره پایانه مشتمل می‌شود بر طیف وسیعی از قابلیت‌های کارکردی از جمله ذخیره‌سازی داده‌های سری به شیوه مقاوم در برابر مداخله، اصالت‌سنجی خدمت، مجوزدهی خدمت، رمزنگاری و رمزگشایی نشانک واپایش، رمزگشایی محتوا، کدگشایی فراداده‌های حقوق دسترسی، پیاده‌سازی استفاده محتوا، تشخیص و تعبیه نشانه‌گذاری، اصالت‌سنجی و وارسی محتوای برنامه‌ای، مرتبط‌سازی و تبادل حفاظت خدمت و محتوا، رمزنگاری درگاه (واسط) خروجی رقمی ، مقاومت مسیر رسانه در برابر مداخله، پردازشگرها و مؤلفه‌های امنیتی قابل اتصال و قابل تجدید مبتنی بر سخت‌افزار و نرم‌افزار و غیره.

### ۵-۸ سازوکارهای امنیتی مربوط به مشترکان یا کاربران نهایی

سازوکارهای مشترکان یا کاربران نهایی به طور عمده به جمع‌آوری، ذخیره، و ارسال اطلاعاتی مربوط می‌شوند که ممکن است تحت ملاحظات حریم‌خصوصی یا محرمانگی کاربر نهایی قرار داشته باشند. از این رو این سازوکارها ممکن است بین نقطه جمع‌آوری، افزاره پایانه و ارائه‌دهنده خدمات که به‌طور بالقوه این اطلاعات را مورد برداشت، نگهداری و استفاده مجدد قرار می‌دهند تقسیم شوند. در نتیجه انتظار می‌رود توصیف و تعریف این سازوکارها در بندهایی که امنیت خدمت و افزاره پایانه را توصیف می‌کنند گنجانده شود.

در حال حاضر در این مجموعه توصیه سازوکارهای امنیت مشترکان یا کاربران نهایی تعریف نمی‌شود. انتظار می‌رود در آینده کارهایی برای بحث بیشتر در مورد این موضوعات انجام شود. اطلاعات بیشتر در مورد امنیت مشترکان در پیوست الف ارائه شده است.

## پیوست الف

## حفاظت امنیت مشترکان

## (الزامی)

### الف-۱ حفاظت داده‌های کاربر

هنگام پیاده‌سازی خدمات IPTV در میان کاربران عمومی، توجه کافی به امنیت و حفاظت داده‌های مشترکان ضروری است.

داده‌های مشترکان ممکن است شامل اطلاعات داده‌های ردگیری شده نظیر شماره کانال بعد و قبل از تغییر کانال، زمان تغییر و اطلاعات کاربر خدمت EPG، شناسایی بسته‌بندی، زمان پخش، و غیره باشد. داده‌های بیان‌شده به طور ذاتی شخصی و محرمانه است. حفاظت همه این داده‌های مشترکان از سوءاستفاده نیازمند آن است که ارائه‌دهنده خدمت IPTV، مسائل حفاظت حریم‌خصوصی کاربر را در نظر بگیرد.

- خدمت IPTV می‌تواند به صورت اختیاری، مقدار کمینه داده‌های شخصی مشترکان که برای تحویل خدمات IPTV لازم است را ارسال کند.
- خدمت IPTV می‌تواند به صورت اختیاری قبل از جمع‌آوری اطلاعات لازم برای تحویل خدمات IPTV، استفاده مورد نظر از داده‌های شخصی مشترکان و به دست آوردن محتوای اطلاعاتی از مشترکان را توضیح دهد.
- خدمت IPTV می‌تواند به صورت اختیاری داده‌های شخصی مشترکان که برای ادامه خدمات IPTV غیرضروری است را منهدم کند.

هنگامی که ارائه‌دهنده خدمت بر داده‌های شخصی مشترکان احاطه دارد، خدمت IPTV می‌تواند به صورت اختیاری داده‌های جمع‌آوری شده را تحت امنیت شدید ذخیره‌سازی کند.

راه‌های ممکن متعددی برای نشت احتمالی داده‌های کاربر وجود دارد. ممکن است نشت اطلاعات در شرکت خدمات، شبکه، و خانه، برای مثال از طریق افزاره‌های پایانه روی دهد. در اینجا روش‌های حفظ داده‌های شخصی کاربران برای هر یک از مسیرهای نشت توصیف می‌شود.

برای جلوگیری از نشت داده‌های مشترکان، توصیه می‌شود ارائه‌دهنده خدمات IPTV توجه زیادی به موارد زیر داشته باشد:

- دسته‌بندی داده‌های شخصی مشترکان به داده‌هایی که نیازمند واپایش است و داده‌هایی که نیازمند واپایش نیستند.
- داده‌های شخصی مشترکان که نیازمند واپایش است به صورت امن مدیریت شود.
- اطمینان حاصل شود که داده‌هایی از مشترکان که نیازمند واپایش است برای اهداف دیگری غیر از اهداف مورد نظر مورد استفاده قرار نگیرد.

توصیه می‌شود که فراهم‌آورندگان خدمات IPTV توجه دقیقی به نکات زیر در ارتباط با خدمات و تراکنش‌های مشمول در جابه‌جایی و مدیریت داده‌های شخصی مشترکان داشته باشند:

- دسته‌بندی داده‌های مشترکان به داده‌هایی که نیازمند واپایش است و داده‌هایی که نیازمند واپایش نیستند.
- استفاده از کانال‌های ارتباطی رمزنگاری شده برای ارسال داده‌های شخصی مشترکان که نیازمند واپایش است. فراهم‌آورندگان خدمت IPTV گاهی اوقات داده‌های شخصی مشترکان را در افزاره‌های پایانه ذخیره می‌کنند تا کارایی خدمات را بهبود بخشند. در چنین مواردی توصیه می‌شود که توجه زیادی به نکات زیر داشته باشند. علاوه بر این، توصیه می‌شود در هنگام تبادل TDها به امنیت توجه شود.
- اطمینان از این که هیچ طرف سومی نمی‌تواند به راحتی داده‌های شخصی کاربران که در TD ذخیره شده‌اند را بخواند.
- ارائه‌دهنده خدمات IPTV می‌تواند به صورت اختیاری دسترسی به داده‌های شخصی مشترکان که در TD ذخیره شده‌اند را واپایش کند.
- اطمینان از این که داده‌های شخصی مشترکان که در TD ذخیره شده‌اند قابلیت حذف کامل توسط یک مشترک یا ارائه‌دهنده خدمات را دارند.
- لازم است که TDها به صورت مطلوب در برابر حمله از سوی بدافزارهای کامپیوتری نظیر ویروس و جاسوس افزار در آینده نزدیک حفاظت شوند.

### الف-۲ واپایش والدین، حفاظت عوامل فرعی قانونی، واپایش دسترسی

در سکوی IPTV، سازوکاری برای حفظ عوامل فرعی[۱] قانونی را می‌توان برای محدود کردن محتوای IPTV که قابل دسترسی توسط عوامل فرعی قانونی است به کار برد. در یک الگوی معمول استفاده، یک افزاره پایانه برای خدمات IPTV در یک خانه توسط افراد متعدد از جمله عوامل فرعی قانونی به اشتراک گذاشته می‌شود. برای افزاره‌های پایانه، توصیه می‌شود که ارائه‌دهنده خدمات IPTV به موارد زیر توجه داشته باشد:

- تضمین این که رتبه‌بندی‌های والدین را می‌توان در صورت لزوم برای محتوا تنظیم کرد.
- تضمین این که افزاره‌های پایانه را می‌توان مطابق با رتبه‌بندی‌های والدین مورد بهره‌برداری قرار داد.
- تضمین این که افزاره‌های پایانه قابلیت تغییر تنظیمات رتبه‌بندی والدین را دارند.
- تضمین این که افزاره‌های پایانه قادر به واپایش مبتنی بر کلمه عبور است به طوری که تنها محافظان عوامل فرعی قانونی می‌توانند رتبه‌بندی‌های والدین را تغییر دهند.
- اطمینان از این که رتبه‌بندی‌های محتوا را می‌توان برای گروه‌های سنی مختلف تنظیم کرد.
- تضمین این که ترجیحات مشترکان را می‌توان برای گروه‌های سنی مختلف اختصاص داد.

---

۱ - Minors

- اطمینان از این که مجوزدهی را می‌توان در افزاره‌های پایانه برای عوامل فرعی قانونی که یک کانال یا محتوای خاص را مشاهده می‌کنند، برای مثال با استفاده از یک PIN، انجام داد.
- اطمینان از این که محافظانی که در مجاورت عوامل فرعی قانونی قرار ندارند می‌تواند به صورت از دور بر عوامل قانونی فرعی نظارت داشته و محتوای آن‌ها را از مخزن رونوشت شبکه دریافت کنند.

توجه شود که در نظر گرفتن شرایط هر حوزه پیاده‌سازی یا ناحیه در ارتباط با سازمان‌های طرف سوم برای حذف محتوای مضر نیز ممکن است لازم باشد زیرا این موضوع به واپایش جریان محتوا و دسترسی محتوا مربوط می‌شود. در یک حالت می‌توان فرض کرد که ایجادکننده اصلی محتوا توجه مناسبی به ارسال مجدد هم‌زمان در زمان ایجاد محتوا داشته باشد و از این رو نیاز به توجه کافی به تأخیر ارسال و هزینه توزیع افزایش می‌یابد.

## پیوست آ

## تهدیدات امنیتی

## (آگاهی دهنده)

این پیوست دسته‌ای از تهدیدات شناسایی‌شده که با ملاحظات یا سازوکارهای اشاره شده در این استاندارد مرتبط است را توضیح می‌دهد.مدل تهدیدات امنیتی و وسایر موارد پایه‌ای براساس توصیه نامه‌های ITU-T به توصیف زیر ارائه شده است:

- توصیه نامه [b-ITU-T X.800] که عنصرهای عمومی معماری مرتبط با امنیت را توصیف می‌کند که می‌تواند در این شرایط که محافظت ارتباطات بین سامانه‌های باز لازم است به خوبی پیاده شود
- توصیه نامه [b-ITU-T X.805]که معماری امنیتی شبکه برا برای ارائه شبکه امن انتها به انتها تعریف می‌کند.

به علاقمندان به ملاحظات امنیتی مربوط به تلویزیون مبتنی بر اینترنت توصیه می‌شود این توصیه نامه‌های پایه‌ای امنیت را بخوانند، فرض شده است که خوانندگان این توصیه نامه به اطلاعات ارائه شده در اینگونه توصیه نامه‌ها آگاه باشند.

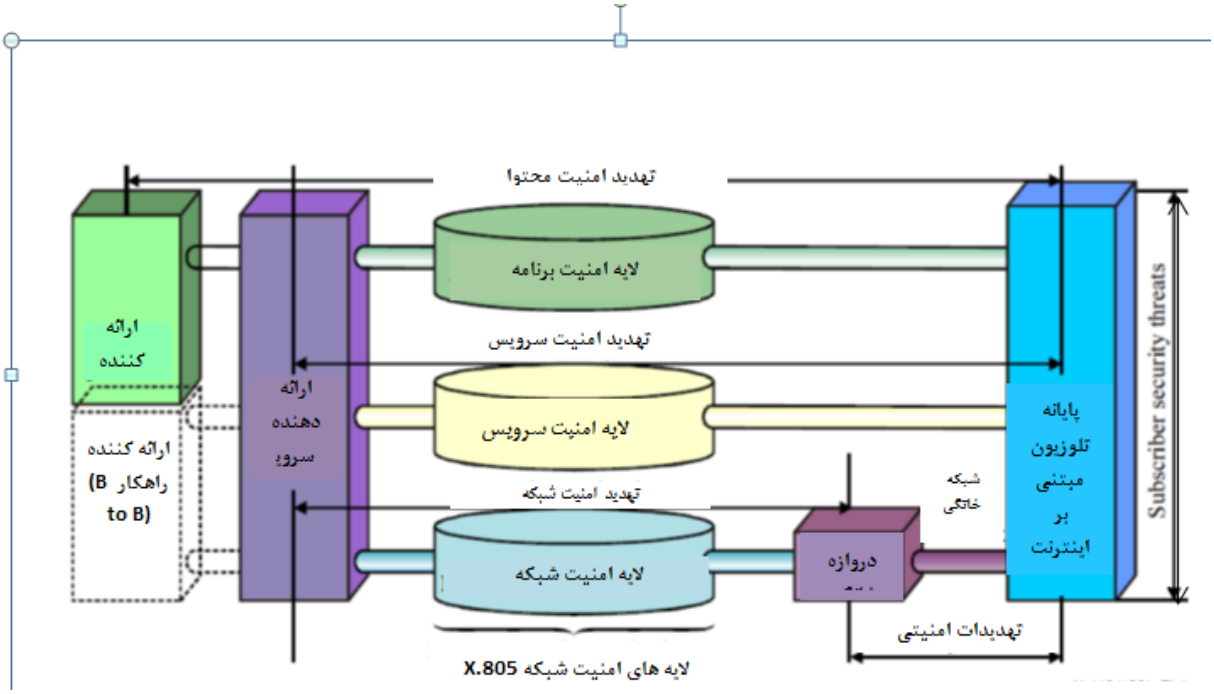
[b-ITU-T X.800] و [b-ITU-T X.805] تهدیدات امنیتی شبکه را به مطابق موارد زیر را توصیف کنند (همچنین تهدیدات امنیتی برای خدمت و محتوا که قابل اعمال به تلویزیون مبتنی بر اینترنت است):

- آسیب به اطلاعات و/یا سایر منابع
- تخریب یا تغییر اطلاعات
- دزدی، حذف یا از دست دادن اطلاعات یا سایر منابع
- وقفه در خدمت

### آ-۱ مدل تهدیدات امنیتی

تهدیدات امنیتی در خدمت تلویزیون مبتنی براینترنت را می‌توان به انواع مواردی که در ادامه می‌آید دسته‌بندی کرد: تهدیدات امنیت محتوا، تهدیدات امنیت خدمت، تهدیدات امنیت شبکه، تهدیدات امنیت افزاره، و تهدیدات امنیت کارخواه.

شکل آ-۱مدل تهدیدات امنیتی است که رابطه بین هر کدام از این تهدیدات امنیتی را نشان می‌هد.




**شکل آ-۱ مدل تهدیدات امنیتی**

### آ-۱-۱ تهدیدات امنیتی محتوا

**دارایی محتوایی**: دارایی که متعلق به ارائه‌دهنده محتوا و/یا ارائه‌دهنده خدمت بوده و می تواند از طریق افـزاره توسط کاربر نهایی مصرف شود. دارایی محتوایی که باید مجافظت شـود شـامل: محتـوای تلویزیـونی خطـی، محتوای ویدئوی مبتنـی بـر درخواسـت، محتـوای ویـدئوی مبتنـی بـر درخواسـت رانشـی، محتـوای PVR، کاربردهای بارگیری و غیره است. موارد زیر تهدیدات محتوا است:

- دستبرد[۱]: نقض محرمانگی محتوا از طریق نظارت خدمت شبکه به‌صورت غیر قانونی
- تماشای غیر مجاز
- تولید مجدد با توزیع مجدد غیر مجاز

### آ-۱-۲ تهدیدات امنیت خدمت

**دارایی خدمت**: دارایی متعلق به ارائه‌دهنده خدمت شامل خدمت‌دهنده، خدمات SCP و اطلاعات عملیاتی مانند سابقه خدمت واطلاعات صورتحساب موارد زیر تهدیدات خدمت است:

- نقض حق نشر[۲] برنامه‌های ارائه‌شده در سکوی خدمت تلویزیون مبتنی بر اینترنت به کارخواه
- پنهان‌سازی /جعل در ارائه‌دهنده خدمت تلویزیون و مبتنی بر اینترنت

---

۱- Interception

۲ -Copy right

- تهدیدات مزاحمت که کارساز خدمت تلویزیون مبتنی بر اینترنت را هدف گرفته‌اند (کارساز SCP، کارساز رسانه، سایر): که می‌تواند شامل هک کردن با هدفگیری نقص امنیتی نرم‌افزار کار بردی یا پروتکل ارتباطی و حمله رد خدمت وغیره باشد.
- دزدی (اغلب با استفاده از برنامه‌های مزاحم مثل اسب‌های تروا) از اطلاعات کاربران (مانند اطلاعات شناسایی، اطلاعات حساب، اطلاعات کاربری)

**آ-۱-۳ تهدیدات امنیتی شبکه**

**دارایی شبکه:** دارایی متعلق به ارائه‌دهنده شبکه که می‌تواند شامل تجهیزات فیزیکی ( مانند رهیاب‌ها، سوئیچ‌ها (سودهنده‌ها) و منابع شبکه (مانند پهنای باند، خدمات چندپخشی و غیره) باشد

موارد زیر تهدیدات شبکه است

- تهدیدات احتمالی تجهیزات و منابع (پهنای باند) را هدف می‌گیرند: حمله مزاحمت به شبکه نظیر رد خدمت
- تهدیدات امنیتی به فنون چندپخشی استفاده‌شده در شبکه حامل تلویزیون مبتنی بر اینترنت مانند پنهان‌سازی /جعل در منبع چندپخشی تلویزیون یا عضو غیر مجاز در گروه چندپخشی
- حمله مزاحمت (مانند DoS، هک) به نود توزیع محتوا در شبکه

**آ-۱-۴ تهدید امنیتی افزاره پایانه**

**دارایی‌های پایانه**: که دارایی است که متعلق به افزاره که می‌تواند توسط کاربر نهایی برای پردازش و ذخیره محتوا و سایر اطلاعات مرتبط برای خدمت تلویزیون مبتنی بر اینترنت استفاده شود

موارد زیر تهدیدات افزاره است.

- دسترسی غیر مجاز به محتوای شفاف با نفوذ به سخت‌افزار یا نرم‌افزار افزاره برای نمونه محتوا می‌تواند با نفوذ در انتقال داده یا نفوذ به نرم‌افزار SCP رونوشت شود.
- دسترسی غیر مجاز به کلیدها یا سایر اطلاعات محرمانه در افزاره با استفاده از نرم‌افزار یا سخت‌افزار نفوذ، حمله‌ها می‌تواند به حافظه افزاره نفوذ کند یا جریان داده را با به‌دست آوردن کلیدها و سایر دادهای محرمانه تحلیل کند (نشت کلید محتوا موجب نشت محتوا و نشت کلید افزاره موجب پنهان شدن افزاره می‌شود) .
- اختلال کارکرد افزاره با روش‌های سخت‌افزاری مانند واپایش ساعت سامانه افزاره برای از کار انداختن کارکرد سامانه SCP یا روش‌های نرم‌افزاری مانند نصب ویروس برای کاهش منابع افزاره
- برنامه‌های کاربردی غیر مجاز (مانند برنامه‌های نرم‌افزاری) در افزاره بارگذاری، اجرا وذخیره می‌شوند
- خطا در تجهیزات افزاره (سخت‌افزار یا نرم‌افزار) که توسط یک کد مزاحم /ویروس در شبکه ایجاد می‌شود
- اتصال افزاره غیرمجاز به شبکه خانه
- استفاده غیر مجاز کاربران

**آ-۱-۵ تهدیدات امنیتی کاربر**

**دارایی کاربر**: دارایی متعلق به کاربر که می‌تواند شامل اطلاعات اشتراک، اطلاعات خانه، اطلاعات کاربردهای خدمت تلویزیون مبتنی بر اینترنت و غیره باشد. امنیت کاربر نیازمند همکاری یک سازوکار امنیت محتوا و یک سازوکار امنیت خدمت با یکدیگر است زیرا خدمت تلویزیون مبتنی بر اینترنت شامل خدمتی است که در امنیت محتوا و امنیت خدمت ارائه می‌شود. نمونه‌های امنیت کاربر در جدول ۱-۱ ارائه شده است.

**جدول أ-۱ دسته‌بندی‌های امنیت کاربر**

| | امنیت کاربر | | |
|---|---|---|---|
| | نمونه خدمت | نمونه تهدید | نمونه سازوکار محافظت |
| امنیت محتوا | تلویزیون خطی، خدمت ویدئو درخواستی | نسخه برداری غیر قانونی | شناسایی افزاره (محافظت خدمت، محافظت محتوا) |
| امنیت خدمت | خدمت دو طرفه | حمله صیادی | شناسایی شخص (محافظت از داده شخصی، شناسه کاربری/PIN) |
| | خدمت والدین | حمله جعل | شناسایی شخص(شناسه کاربری/PIN، شناسایی) |
| امنیت شبکه | مشخص نشده | | شناسایی خط کارخواه، کدگذاری داده،واپایش اتصال چندپخشی |
| امنیت افزاره پایانه | خدمت شخص به شخص | نسخه برداری غیر قانونی | محافظت محتوا (شخص به شخص) |

## پیوست ب

## سازگار در SCP

## (الزامی)

### ب-۱ کلیات سازگار در SCP

چندین فرانامه برای سازگار در SCP وجود دارد: SCP-EE،SCP-BوSCP-IX. سازگار در SCP می‌توانـد در حوزه ارائه‌دهنده خدمت و در حوزه کاربر نهایی استفاده شود. این پیوست فقط بر بسته پایانه تمرکز دارد.

### ب-۲ فرانامه‌های سازگار در SCP

فرانامه‌های سازگار در SCP حداقل در سه نوع دسته‌بندی شده اند: SCP انتها بـه انتهـا (SCP-EE) ، SCP پل (SCP-B) و تبادل SCP (SCP-IX)

۱-SCP انتها به انتها (SCP-EE)

SCP-EE: یک نشانک SCP ودو یا بیشتر افزاره تبادل دسترسی محتوا براساس حقوق مشخص.این نوع ساده ترین نوع برای پیاده‌سازی است زیرا فقط یک نشانک SCP استفاده می‌شود

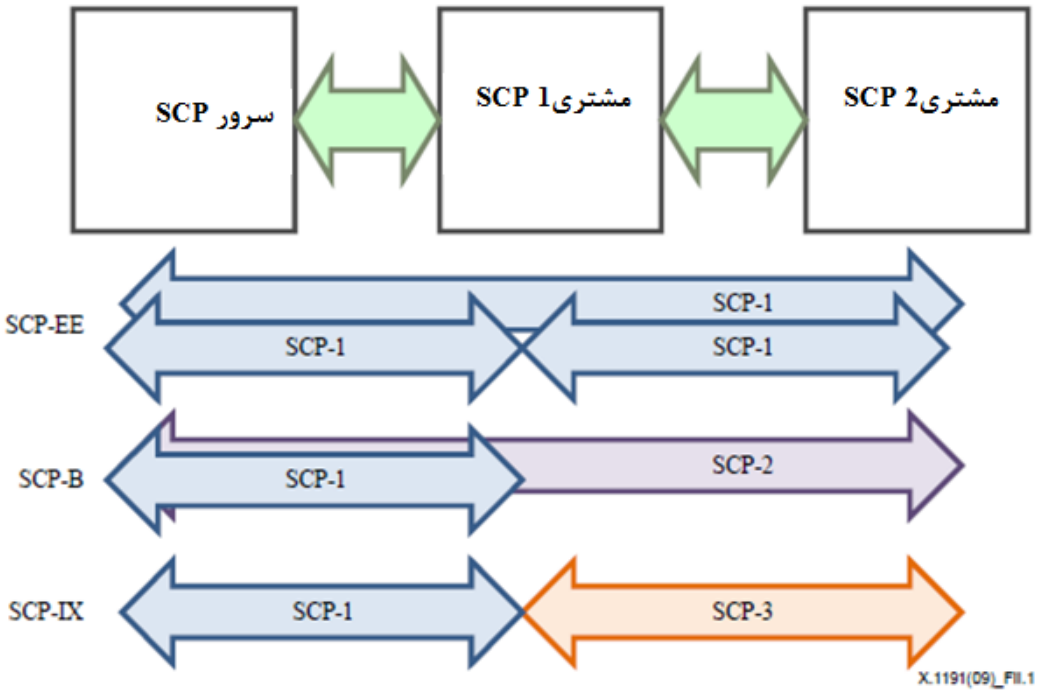
۲- SCP پل (SCP-B)

SCP-B: در یک افزاره، دو یا بیشتر SCP پیاده می‌شود. محتوایی که از طریـق یـک سـامانه SCP بـه‌دسـت می‌آید (مثلا از شبکه) می‌تواند از طریق SCP دیگر در دسترس قرار گرفته و مطابق حقوق مشخص در همان افزاره قرار گیرد.

۳- تبادل SCP (SCP-IX)

SCP-IX: این مورد دو یا بیشتر افزاره وجود دارد و در هر افزاره یک یا بیشتر SCP پیاده شده است. محتوایی که از طریق یک افزاره و یکی از SCPهای آن به‌دست آمده می‌تواند با امنیت منتقل و در دسترس یک افزاره دیگر از طریق یک SCP دیگر و براساس حقوق مشخص قرار گیرد.

شکل ب-۱ انواع توصیف شده در بالا را نشان می‌دهد.




**شکل ب-۱ مدل‌های سازگار SCP**

### ب-۳ حوزه‌های فنی سازگار SCP

در ادامه عنصرهای کلیدی لازم در انواع سازگار SCP-EE، SCP-B و SCP-IX مشخص شده است

۱- شناسایی افزاره، کاربر و SCP

قبل از آن که محتوا بتواند بین هستارها تبادل شود، شناسایی افزاره پایانه واحتمالا کاربرش باید با امنیت پیاده‌سازی شود. علاوه بر آن از آنجا که ممکن است فراهم‌کنندگان خدمت به مشخصات SCP اعتماد نکنند، شناسایی SCP (ها) یا پیاده‌سازی سطوح قبل از تبادل محتوا باید ممکن باشد. چنین شناسایی باید رویه رمزنگاری داشته و ممکن است فنون شناخته‌شده امضای الکترونیک را به‌کار گیرد. کلیدهای رمز نگاری عمومی یک سازوکار ساده برای امضا وپروتکل شناسایی ارائه می‌دهد.

۲- حقوق بیانگر تبادل

SCPهای مختلف از زبان بان حقوق و یا قالب‌های پروانه[۱] مختلف استفاده می‌کنند. برای کارکرد انواع SCP-B و SCP-IX یک رویه بیانگر حقوق یکسان لازم است. این می‌تواند به‌صورت یک زبان مشترک بیانگر حقوق (REL) یا یک ترجمه کر بیان حقوق باشد. روش دیگر تبادل بیان حقوقی مذاکره پروانه است.

۳- الگوریتم مشترک رمزنگاری برای تبادل محتوا

---

۱ - Licence

برای انتقال امن محتوا از حوزه واپایش یک SCP به یک SCPدیگر یا در حوزه واپایش همان SCP اما در افزاره‌های مختلف، رمزنگاری محتوا لازم است. این کار محتوای غیر لازم را به جز در مورد هستارهایی که کلیدهای مناسب یا لازم برای رمز گشایی دارند را کاهش می‌دهد. الگوریتم‌های متنوعی برای رمز نگاری وجود دارد (برای نمونه کدبسته ، کد جریان، کلید مبتنی بر کلید عمومی و غیره) اما به‌طور کلی آنهایی که از کلید متوازن استفاده می‌کنند به نظر می‌رسد برای تبادل محتوا با سرعت بالا متناسب باشد. برای اهداف سازگار تعداد کمی از الگوریتم‌هایی که بر آن توافق وجود دارد باید انتخاب شوند. به‌طور مطلوب یک الگوریتم پیش فرض نیز باید مشخص شود

۴- کلید مدیریت و/یا تبادل برای الگوریتم‌های رمزنگاری معمول

قبل از آنکه تبادل امن صورت گیرد، لازم است کلیدهایی که در موقعیت‌های مشخص استفده می‌شوند تبادل یا یا به‌صورت معمول توسط هستارهای مسئول شناسایی تولید شوند.کلید مدیریت معمولا سخت‌ترین بسته پیاده‌سازی امنیت در یک سامانه است. فنون نظیر کلید عمومی رمزنگاری، توزیع کلید افزاره را ساده می‌کند اما یک زیر ساخت کلید عمومی (PKI) برای انتشار وحفظ اعتبار این کلیدها نیاز دارد. چنین زیر ساختی ممکن است توسط یک ارائه‌دهنده پروانه که مسئول محافظت محتوا است (بر اعمال اساس امنیت عمومی شبکه) محدود شود

۵- بارگذاری امن ازاستفاده‌کننده SCP

به‌صورت مطلوب هر افزاره پایانه‌ای قادر به محتوایی به‌دست آمده (قانونی) از طریق سایر افزاره‌ها ویا استفاده از هر SCP بر اساس حقوق مشخص است(روش SCP-IX) . با این حال توجه کنید که بارگزاری اولیه درزمان تولید هر افزاره‌ای و هر سامانه SCP بر اساس ملاحظات بازار از دیدگاه پیاده‌سازی مشکل است و بنابراین نیاز به سازوکار امنیتی برای بارگزاری وپیاده‌سازی یک سامانه SCP انتخابی در یک افزاره لازم است. عنصرهای نظیر بارگزاری کننده اولیه امن وپروتکل بارگذاری امن نقش مهمی در این سازگار بازی می‌کنند.

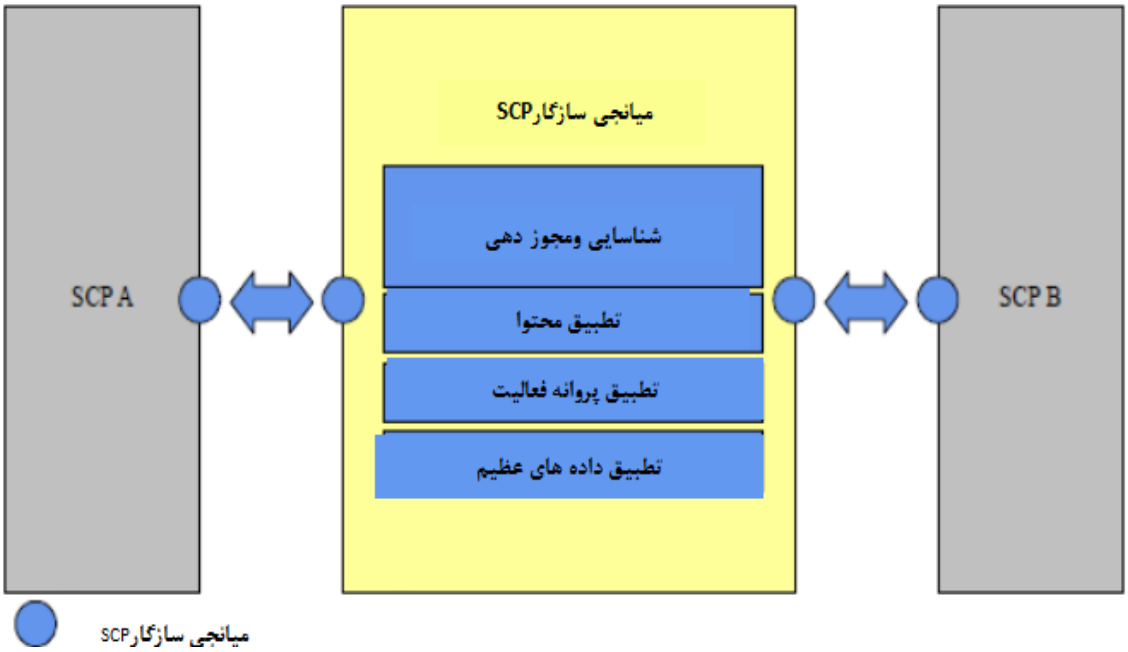
**یادآوری**- زمانی که سازگار SCP در افزاره وسامانه انتهایی پیاده‌سازی می‌شود، افزاره تلویزیون مبتنی بر اینترنت باید حاوی معماری اعتماد برای پشتیبانی از سازگار امنیت خدمت باشد.

۶- انتقال امن حقوق

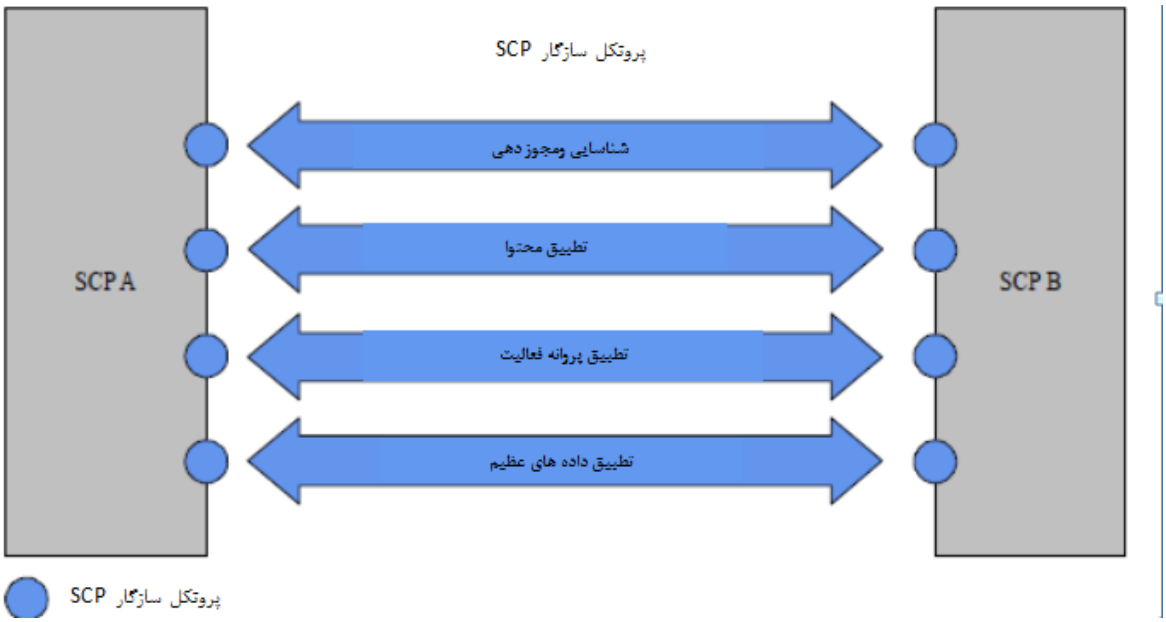
برای انتقال امن حقوق، کاربر SCP باید بررسی شود که اجازه انتقال حقوق به سامانه SCP مقصد وجود دارد. حقوق رقمی ممکن است شامل حقوقی برای توانمندسازی سامانه SCP برای ارسال حقوق باشد. در چنین شرایطی کاربرSCP باید این حقوق را بررسی کند وبه سامانه SCP هدف اجازه انتقال حقوق رقمی را بدهد.

### ب-۴ معماری سازگار SCP

دو معماری برای سازگار SCP می‌توان در نظر گرفت، یکی معماری سازگار مبتنی بر واسط که یک سامانه میانی قرار گرفته بین دو سامانه SCP را برای تبادلات سازگار استفاده می‌کند و دیگری معماری مبتنی بر پروتکل استاندارد که واسطها وپروتکل‌های استاندارد را برای ارسال امن محتوای رقمی واطلاعات مرتبط بین دو سامانه SCP متفاوت استفاده می‌کند. هر دو معماری در شکل ب-۲ وب-۳ نمایش داده شده اند.




شکل ب-۲ معماری سازگار بین SCPها مبتنی بر میانجی




شکل ب-۳ معماری سازگار بین SCPها مبتنی بر پروتکل استاندارد

## توصیف بسته‌های عملکردی

- **همخوان سازی محتوا**: همخوان سازی محتوا مسئول تبدیل الگوریتم رمز نگاری است. پیش تعریف چندین الگوریتم رمزنگاری استاندارد این فرایند را آسان می‌کند.
- **همخوان سازی پروانه**: همخوان سازی پروانه، مسئول تبدیل پروانه است. هر پروانه استاندارد یا موقت شناخته شده برای دو طرف باید یک رفتار مجوز دهی (برای دارایی مدیا و مجوز مصرف) را همانگونه که در پروانه اولیه آمده داشته باشند. ممکن است در همخوان سازی پروانه یک مجموعه نگاشت حقوق (نگاشت نحوه بیان حقوق ونگاشت معنایی) وجود داشته باشد. علاوه بر این همخوان سازی پروانه ممکن است مسئول بسته‌بندی مجدد اطلاعات حقوق وارسال امن آنها به کاربر SCP اصلی باشد.
- **همخوان سازی داده‌های عظیم**: همخوان‌سازی داده‌های عظیم، مسئول تبدیل اطلاعات داده‌های عظیم است. داده‌های عظیم استاندارد یا موقتی آشنا برای دو طرف باید همان اطلاعاتی را که داده‌های عظیم اولیه داشته ارائه دهند. ممکن است در همخوان سازی داده‌های عظیم یک مجموعه نگاشت داده‌های عظیم (نگاشت خطاها و معنایی) وجود داشته باشد.علاوه بر ان همخوانی داده‌ای عظیم می‌تواند مسئول مسئول بسته‌بندی مجدد اطلاعات داده‌های عظیم وارسال امن آنها به SCP دیگر باشد.
- **شناسایی ومجوز دهی**: هر SCP باید در مورد این که SCPدیگر برای سازگار مناسب است یا خیر قضاوت کند.این رویه معمولا در قدم اول با یک فرایند شناسایی دو طرفه بین دوSCP همراه است.
- **موارد استثناء**: اگر SCP الف وSCPب در یک افزاره قرار گرفته باشند و یا در صورتی که یک کانال امن اختصاصی بین دو SCP وجود داشته باشد، درهمخوان سازی محتوای نیازی به فرایند سازگار نیست

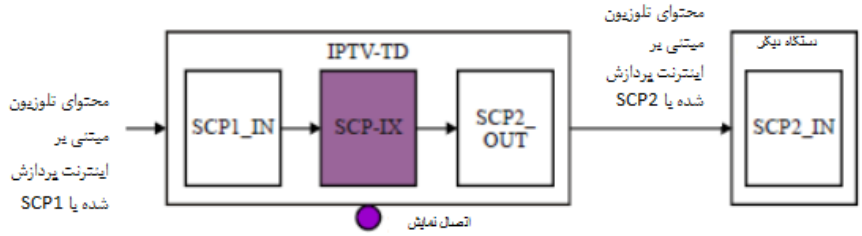
### ب-۵ فرانامه SCP-B و SCP-IX پیاده شده در افزاره

در اینجا سه فرانامه ممکن برای تبادل خدمت امن ومحتوای امن بین SCPها توصیف می‌شود.

#### ب-۵-۱ تعریف عبارت‌های به‌کارگرفته شده در شکل

- SCP-IN: درگاه اکتسابی که محتوای تلویزیون مبتنی بر اینترنت محافظت شده توسط SCP از آن وارد می‌شود
- SCP-OUT :درگاه خروجی که محتوای تلویزیون مبتنی بر اینترنت محافظت شده توسط SCP از آن خارج می‌شود

#### ب-۵-۲ فرانامه ۱: SCP با SCP-IX

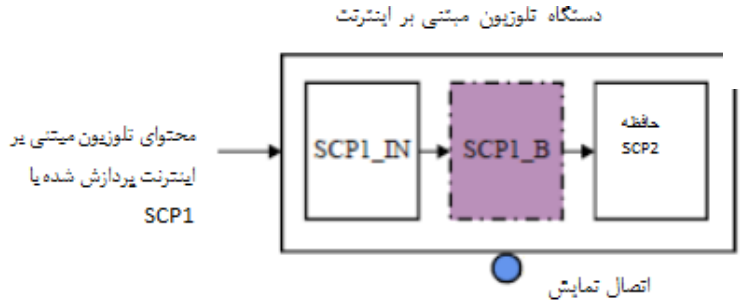



**شکل ب-۴ SC با SCP-IX**

افزاره پایانه تلویزیون مبتنی بر اینترنت در این حالت SCP با SCP-IX دارد تا از سازگار بین افزارهها بدون حافظه که فقط امنیت خدمت مشخصی را دارند و افزارهای خارجی با حافظه که فقط محافظت محتوای مشخصی دارند پشتیبانی کند.

برای پشتیبانی از اتصال انعطاف پذیر به هر نوع افزاره خارجی که انواع سازوکارهای محافظت را داشته باشد، افزاره تلویزیون مبتنی بر اینترنت باید به جای اتصالات امن موردی بین دو افزاره SCP-IX داشته باشد.

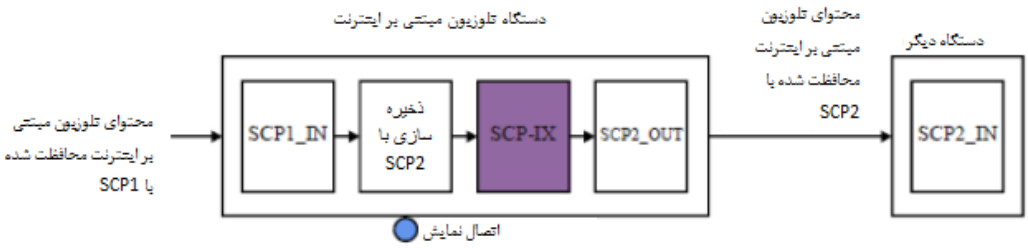
### ب-۵-۳ فرانامه ۲: SCP با SCP-B و حافظه اختیاری




**شکل ب-۵ SCP با SCP-B و حافظه اختیاری**

افزاره پایانه تلویزیون مبتنی بر اینترنت در این حالت SCP با SCP-B برای پشتیبانی از سازگار بین محافظت خدمت ومحافظت محتوا در یک افزاره دارد. در تولید افزاره تلوزوین مبتنی بر اینترنت ممکن است سازوکار اختصاصی محافظت محتوا برای حافظه داخلی در نظر گرفته شود.در چنین حالتی SCP-B نیاز نیست وSCP1 ممکن است توسط حافظه استفاده شود.ب رای پشتیبانی از اتصال انعطاف پذیر با هر نوع حافظه داخلی که انواع سازوکارهای محافظت محتوا را دارا میباشند، توصیه میشود افزاره تلویزیون مبتنی بر اینترنت به جای پیادهسازی مورد به مورد امنیت اتصال بین محافظت خدمت و محافظت محتوا از SCP-B استفاده کند.

### ب-۵-۳ فرانامه ۳: SCP با حافظه و SCP-IX




**شکل ب-۶ فرانامه۳:SCP با حافظه وSCP-IX**

در این حالت افزاره تلویزیون مبتنی بر اینترنت SCP دارای با حافظه و SCP-IX برای پشتیبانی از سازگار بین سازوکار داخلی محافظت محتوا و سازوکارهای خارجی است.

برای پشتیبانی از اتصال انعطاف‌پذیر با هر نوع حافظه خارجی که دارای انواع سازوکارهای محافظت محتوا باشد توصیه می‌شود افزاره تلوزوین مبتنی بر اینترت به جای پیاده سازی امنیت اتصال بین سازوکارهای داخلی وخارجی محافظت محتوا به‌صورت مورد به مورد دارای SCP-IX باشند.

## پیوست ج

## نمونه‌ای از فرایند محافظت محتوا در تلویزیون مبتنی بر اینترنت

## (آگاهی دهنده)

در ادمه نمونه‌ای از فرآیند ویدئوی درخواستی برای محافظت محتوا توصیف می‌شود.

- مرحله شناسایی کاربر
- کاربر برنامه کاربردی ویدئو درخواستی را از طریق "کشف خدمت وبرنامه وانتخاب بسته کارکردی کارخواه" انتخاب می‌کند.
- با دریافت "پرونده برنامه بسته کارکردی"، "کارکرد برنامه تلوزوین مبتنی بر اینترنت" یک در خواست تایید کارخواه ارسال می‌کند. اگر موفق بود، اطلاعات شناسایی مربوط به مشترک برای بررسی در "پرونده برنامه بسته کارکردی" به طور موقت ذخیره می‌شود.
- مرحله انتخاب محتوا
- کاربر می‌تواند با استفاده از اطلاعات به‌دست آمده از EGC یک محتوای مشخص را انتخاب کند و"بسته کارکردی ویدئو درخواستی" اطلاعات محل محتوای انتخاب شده (URL) را به افزاره ارسال می‌کند.
- " بسته کارکردی ویدئو درخواستی" در افزاره، محل محتوا را برای ارسال به "کارکرد تحویل محتوای کارخواه دریافت می‌کند.
- مرحله تحویل محتوای رمزنگاری شده
- "کارکرد تحویل محتوای کارخواه" با استفاده از اطلاعات محل محتوا برای محتوا(ی رمزنگاری شده) درخواست می‌دهد، همچنین برای حقوق وکلیدهای مرتبط با این محتوا به "بسته کارکرد محافظت محتوای کارخواه" درخواست می‌دهد.
- مرحله توزیع حقوق وکلیدها
- اگر کلیدها وحقوق را نداشته باشد "بخش کارکرد محافظت محتوای کارخواه" این اطلاعات را از "بخش کارکرد مدیریت کلیدها وحقوق" در ارائه‌دهنده خدمت تلویزیون مبتنی بر اینترنت مطالبه می‌کند.
- "بخش کارکرد مدیریت کلیدها و حقوق" برای اطلاعات مربوط به مجوزدهی برای این کارخواه را از "بخش کارکرد پرونده برنامه" در خواست می‌کند که آیا کارخواه حق استفاده از محتوا را دارد یاخیر
- اگر پاسخ مثبت بود،کلیدهای حقوق این محتوا برای "بخش کارکرد محافظت محتوای کارخواه" ارسال می‌شود
- با دریافت آن،"بخش کارکرد محافظت محتوای کارخواه" کلیدها وحقوق را به "کارکرد تحویل محتوای کارخواه" ارسال می‌کند تا مجتتوا را رمز گشایی کرده و استفاده از آن را واپایش کند.

## پیوست د

## محافظت از محتوای DVB ومدیریت نسخه‌برداری

## (آگاهی دهنده)

این پیوست به توصیف کلیات محافظت از محتوای DVB ومدیریت نسخه برداری می‌پردازد.
مشخصات (DVB-CPCM) توسط ETSI توسعه یافته است.
DVB-CPCM یک نمونه از سامانه کاملا استاندارد برای محافظت از تلویزیون و سایر محتواها در شبکه خانگی وبیش از ان است. DVB-CPCM می‌تواند محتوا را از سازوکار محافظت) خدمت تلویزیون مبتنی بر اینترنت (یا سایرموارد تعریف شده توسط ITU دریافت و محافظت محتوا را از طریق چرخه عمر از شروع تا استفاده شامل ذخیره، فرآیند و ارسال محتوای محافظت شده به سایر سازوکارهای محافظت خدمت تلویزیون مبتنی بر اینترنت درحالی که مجوز کاربرد صحیح را نگه داشته، حفظ کند.

### د-۱ معرفی

سامانه DVB CPCM یک سامانه محافظت محتوا و مدیریت نسخه برداری برای مصارف تجاری و محتوای رقمی بخش آزاد که برای مصرف کنندگان محصولات و شبکه خانگی تحویل شده است.CPCM مصرف محتوا را از ابتدا ی قرار گرفتن در سامانه CPCM تا مصرف نهایی ویا ارسال از سامانه CPCM بر اساس قوانین مصرف هر محتوا مدیریت می‌کند. CPCM برای استفاده در فضایی که هر محتوایی مانند صوت و ویدئو وبرنامه‌ها و داده‌های مرتبط آنها محافظت شده اند در نظر گرفته شده است.CPCM قابلیت‌های برای تسهیل سازگار چنین محتواهایی بعد از قرار گرفتن آنها در CPCM توسط شبکه‌ای از افزاره کاربران برای شبکه خانگی و دسترسی از دور ارائه می‌دهد.این قابلیت‌ها از بخشهایی که برخی نشانک دهی واقدامات لازم برای الزامات فنی را ارائه می‌دهند وبرخی دیگرمنطق پشت این قابلیت‌ها شامل راهنمای پیاده سازی را توصیف می‌کند تشکیل شده است. مدل مرجع، کارپایه سامانه CPCM را ارئه داده و به عنوان زیر ساختی است که عنصرهای این مشخصات بر آن ساخته می‌شود.

### د-۲ تعاریف

در این پیوست اصطلاحات زیر علاوه بر اصطلاحات متن اصلی تعریف می‌شود:

**د-۲-۱**

**اکتسابی**[۱]

مرتبط با دریافت و اکتساب محتوا از بیرون سامانه CPCM به درون سامانه CPCM است.

**د-۲-۲**

**نقطه اکتساب**[۲]

یک مفهوم انتزاعی کارکردی در CPCM که عملیات اکتساب در آن صورت می‌گیرد.

**د-۲-۳**

**اکتساب** [۳]

دریافت محتوا از بیرون سامانه CPCM به درون سامانه CPCM است.

**د-۲-۴**

**حوزه مجاز**[۴]

مجموعه‌ای مجزا از افزاره‌های منطبق با BDV CPCM که دراختیار، اجازه یا واپایش یک خانه باشد، در اینجا یک خانه به عنوان یک واحد اجتماع شامل اشخاصی که با هم زندگی می‌کنند مانند ساکنان یک اقامتگاه در نظرگرفته شده اند (در خصوص محل فیزیکی افزاره‌هایی که دراختیار، اجازه یا واپایش یک خانه اند هیچ ملاحظاتی وجود ندارد)

**د-۲-۵**

**به‌کارگیری مجاز**[۵]

به‌کارگیری مجاز محتوای CPCM، شامل مجموعه‌ای از قوانین به‌کارگیری قابل اعمال بر محتوای مد نظر است.

---

1-Acquire

۲- Acquisition Point

۳ -Acquisition

۴ -Authorized Domain

۵ -Authorized Usage

**د-۲-۶**

**مصرف کردن** [۱]

موجب کاهش قابل ملاحظه محتوا یا خروجی قابل ملاحظه محتوا که بـدون جلـوگیری از هـر بـه‌کـارگیری دیگری باشد.

**د-۲-۷**

**نقطه مصرف (AP)** [۲]

مفهوم انتزاعی کارکردی در CPCM که در آن مصرف صورت می‌گیرد.

**د-۲-۸**

**مصرف**[۳]

کاهش قابل ملاحظه محتوا یا خروجی افزاره شامل یک انتقال یا یک نشانک برای منع استفاده به جز تبادل بلافاصله محتوا به صوت یا تصویر است.

**د-۲-۹**

**مورد محتوا**[۴]

یک نمونه گسسته از محتوای با مدت محدود مانند برنامه/واقعه یا یک بخش غیر کامل آن است.

**د-۲-۱۰**

**مجوز محتوا**[۵]

یک ساختار داده شامل اطلاعات ضروری برای مدیریت امنیت مورد محتوا در CPCM که به‌صورت امن حفظ و تبادل شود.

---

۱ -Consume

۲ -Consumption Point

۳ -Consumption

۴- Content Item

۵ -Content License

**د-۲-۱۱**

**محتوا**[۱]

داده‌های قابل محافظت در سامانه CPCM، این تعریف به‌طور کلی به محتوایی شامل پیوست‌های اختیـاری داده مانند زیرنویس، تصویر/شکل، پویانمایی، صفحات وب، متن، بازی، نرم‌افزار (کد منبع وکد شـیء) ، مـتن سند و هر اطلاعات دیگری که به کاربر ارسال و توسط او مصرف می‌شود اشاره دارد.

**د-۲-۱۲**

**نسخه برداری**[۲]

یک فرآیند مدیریت در CPCM که در آن قلم محتوایی جدید از محتوای اکتسابی یا قلم محتـوایی ذخیـره شده تهیه می‌شود.

**د-۲-۱۳**

**افزاره CPCM**[۳]

افزاره‌ای که میزبان یک یا چند نمونهCPCM باشد.

**د-۲-۱۴**

**سامانه CPCM**[۴]

یک مجموعه از همه افزاره‌های سازگار با CPCM است.

**د-۲-۱۵**

**افزاره کاربرد** [۵]

هر کارکردی در افزاره CPCM که غیر CPCM باشد.

---

۱ -Content

۲ -Copy

۳ -Cpcm Device

۴ -Cpcm System

۵ -Device Application

**د-۲-۱۶**

**نقطه صادرات (EP)** [۱]

یک مفهوم انتزاعی کارکردی در CPCMکه در آن محتوا سامانه CPCM را ترک می‌کند.

**د-۲-۱۷**

**صادر کردن**[۲]

آزاد کردن محتوای CPCM از محافظت صریح و مدیریت سامانه CPCM به یک واپـایش کننـده CSP،CSP مورد اعتماد یا یک فضای خارج از محدوده اعتماد است.

**د-۲-۱۸**

**حرکت** [۳]

فرآیند نسخه برداری که در ان نسخه اصلی حذف، پاک یا کم می‌شود دیگر در دسترس نیست.

**د-۲-۱۹**

**خروجی**[۴]

افزاره واسط یا CPS که برای ارسال محتوای CPCM،مصرف محتوا یا صادر کردن محتوا استفاده می‌شود.

**د-۲-۲۰**

**هستار پردازشی (PE)** [۵]

یک هستار انتزاعی کارکردی در CPCM که در ان محتوای CPCM پردازش می‌شود.

---

۱- Export Point

۲ -Export

۳ -Move

۴ -Output

۵ -Processing Entity

**د-۲-۲۱**

**پردازش**[۱]

عملیات سازگار با CPCM بر رمزنگاری/رمزگشایی محتوا به جز مصرف و صادرات مانند محتوای CPCM که برای تبدیل از حالت اصلی به یک محتوای جدید CPCM یا اطلاعاتی مانند سطح بلندی صوت یا تصاویر ثابت گزیده شده از محتوا مجوز دارد.

**د-۲-۲۲**

**اطلاعات وضعیت مصرف (USI)** [۲]

داده‌های عظیم محتوای CPCM که مجوز استفاده برای مورد محتوایی CPCM دارد.

**د-۲-۲۳**

**دید**[۳]

مصرف

**یادآوری**- این موضوع شامل شنیدن برای محتوای فقط صوتی هم می‌شود.

**د-۲-۲۴**

**دیدن**[۴]

مصرف

**یادآوری**- این موضوع شامل شنیدن برای محتوای فقط صوتی هم می‌شود

## د-۴ کوته‌نوشت‌ها و سرنام‌ها

در این پیوست کوته‌نوشت‌های زیر علاوه بر موارد مطرح شده در متن اصلی به کار می‌رود:

| | | |
|---|---|---|
| AP | Acquisition Point | نقطه اکتساب |
| APECS | Acquisition,Processing, Export, Consumption, Storage | اکتساب، پردازش، صادرات، مصرف، ذخیره‌سازی |

۱ -Processing

۲ -Usage State Information

۳- View

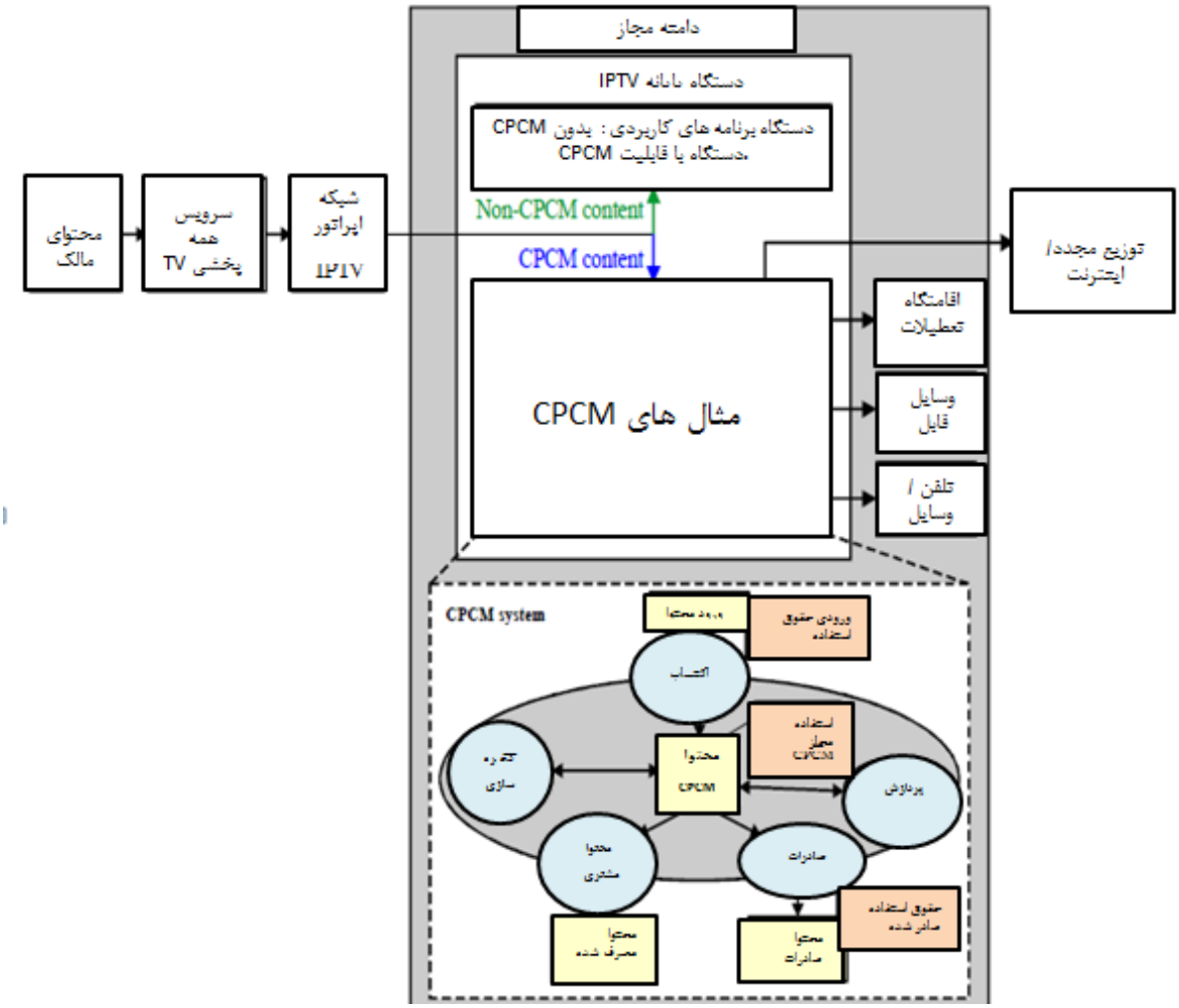
۴ -Viewing

| | | |
|---|---|---|
| CL | Content License | پروانه محتوا |
| CP | Consumption Point | نقطه مصرف |
| CPCM | Content Protection and Copy Management | حفاظت از محتوا و مدیریت نسخه‌برداری |
| CPE | Customer Premises Equipment | تجهیزات سمت مشتری |
| CPS | Content Protection System | سامانه حفاظت از محتوا |
| DVB | Digital Video Broadcasting | پخش ویدئویی رقمی |
| EP | Export Point | نقطه صادرات |
| PE | Processing Entity | هستار پردازشی |
| SE | Storage Entity | هستار ذخیره‌سازی |
| USI | Usage State Information | اطلاعات وضعیت مصرف |

### د-۴ معماری CPCM

در قلب CPCM «حوزه مجاز» قراردارد، یک مجموعه افزاره‌ها که به یک خانه تعلق دارند حتی وقتی که از خانه دور باشند. مفهوم AD نشان می‌دهد که مرتبط کردن محتوا به یک افزاره و یک بخش تلویزیون در عصر سرگرمی‌های شبکه‌ای کافی نیست.

CPCM محتوا را از منابع مورد اعتماد مانند سامانه SCP خدمت تلویزیون مبتنی بر اینترنت به عنوان یک تضمین یا یک بخش از افزاره می‌گیرد و جریان محتوا یا فایل را محافظت کرده و چگونگی مشاهده، جابجایی یا نسخه برداری آنرا مدیریت می‌کند. بر اساس مدل پایه مدیریت محتوای CPCM، محتوای اکتسابی به سامانه CPCM وارد می‌شود تا به محتوای CPCM تبدیل شود. محتوای CPCM در سامانه CPC محافظت و مدیریت می‌شود و زمانی که توسط کارخواه مصرف می‌شود یا به سامانه دیگر صادر می‌شود سامانه CPCM را ترک می‌کند.




**شکل ه-۱ جریان محتوا در محیط CPCM**

CPCM انواع مختلفی از کاربرد محتوا در شبکه خانگی پشتیبانی می‌کند، همچنین می‌تواند دسترسی از دور مانند دسترسی از طریق رایانه‌های قابل حمل و اتصال اینترنت را مدیریت کند. با استفاده از CPCM ارائه‌دهندگان خدمت می‌توانند فرانامه‌های مجاز برای هر نوع محتوا را به تولیدکنندگان ارائه دهند. با این حال بسیاری از روش‌های محافظت امروزی مانند مواردی که در فناوری SCP تلویزیون مبتنی بر اینترنت به‌کار می‌رود و محتوا به‌طور معمول به کابل اتصال متقابل نقطه به نقطه یگانه بین افزاره منبع محتوا (مانند افزاره دریافت تلویزیون مبتنی بر اینترنت) و افزاره نمایش رقمی محدود است توسعه می‌یابد.

CPCM به خدمت‌دهنده‌های همه‌پخشی، کاروَرهای شبکه یا صاحبان شرکت امکان ارائه دسترسی از دور مانند دسترسی در هتل در طول یک سفر کاری یا تفریحی به عضو خانواده می‌دهد و لذا از روش‌های محلی محافظت فراتر می‌رود.

همچنین CPCM می‌تواند به کاربران اجازه نسخه برداری از محتوا بر یک افزاره قابل حمل یا حافظه قابل جانبی مانند DVD را می‌دهد. تا زمانیکه افزاره پخش مجدد به همان حوزه مجاز تعلق دارد افزاره می‌تواند محتوا را حتی اگر از شبکه خانه و ارائه‌دهنده اصلی خدمت قطع اتصال شده باشد می‌تواند محتوا را مجددا پخش کند.

محتوای CPCM برای حذف و اضافه کردن افزاره از/به حوزه مجاز نیاز به مجوز دهی بر خط از خدمت دهنده ندارد.

سامانه محافظت محتوای CPCM یک هستار مستقل نیست و ترکیب/قرارگرفته بر سامانه انتها به انتهای توزیع SCP تلویزیون مبتنی بر اینترنت است، بنابر این در کنار سامانه انتها به انتهای توزیع SCP تلویزیون مبتنی بر اینترنت قرار می‌گیرد نه بجای آن.در هر افزاره‌ای مورد CPCM اختیاری است و اگر نباشد دسترسی به هر محتوای محافظت شده با CPCM را نمی توان تضمین کرد. با این حال افزاره‌ها نیاز به پیاده‌سازی همه عنصرهای CPCM ندارند. تنها مواردی که برای افزاره کاربرد دارد برای کارکرد آن لازم است. برای مثال یک افزاره ساده شاید فقط دارای کارکردهای اکتساب CPCM و مصرف CPCM باشد و حافظه CPCM و یا ملزومات صادرات محتوا را نداشته باشد

## د-۵ مدل مرجع وهستارهای کارکردی CPCM

مدل مرجع CPCM مجموعه‌ای از پنج کارکرد مدیریت محتوا CPCM شامل همه فرانامه‌های مربوط به کاربرد محتوا در محیط کارخواه : اکتساب، ذخیره، پردازش، مصرف و صادرات را توصیف می‌کند. این کارکردها به پنج هستار کارکردی CPCM شامل: نقطه اکتساب، هستار ذخیره، هستار پردازش، نقطه مصرف و نقطه صادرات نگاشت می‌شود. شکل ه-۵ سامانه CPCM را از منظر مفهوم هستارهای کارکردی نمایش می‌دهد.

بنابراین محتوای اکتسابی که به سامانه CPCM وارد می‌شود از طریق نقطه اکتسابی افزاره‌ای که نقطه اکتساب را ایجاد کرده وارد شده و به محتوای تبدیل CPCM می‌شود.

محتوای CPCM می‌تواند توسط هستارهای کارکردی تبادل (هستار ذخیره‌سازی،هستار پردازش) که در افزاره CPCM قرارگرفته ذخیره یا پردازش می‌شود. محتوای CPCM سامانه CPCM را زمانی که در نقطه مصرف، مصرف شد یا در نقطه صادرات،صادر شد ترک می‌کند. مجددا این هستارهای کارکردی می‌توانند در هر دستگاه CPCMD قرارگیرد.

## د-۶ حوزه مجاز

افزاره‌های CPCM می‌توانند به‌صورت منطقی در حوزه‌های مجاز گروه‌بندی شوند. اگر همه آن افزاره‌ها به یک خانه تعلق داشته باشند آنگاه تشکیل یک حوزه مجاز خانگی (AD) می‌دهند. بنابراین حوزه مجاز یک مقصد برای محتوایی است که به گروه یک خانه نگاشت می‌شود.

به‌طور کلی AD را می‌توان به عنوان یک گروه‌بندی منطقی از همه افزاره‌های CPCM که به یک خانه تعلق دارند نگاه کرد،افزاره‌های قرارگرفته در اقامتگاه اصلی یا افزاره‌های قرار گرفته در سایر اقامتگاه‌ها (مانند اقامتگاه تعطیلات) ، افزاره‌های قابل حمل که به تناوب به افزاره‌های ایستگاه یاد شده در بالا متصل می‌شوند و یا افزاره‌هایی که درون وسایل نقلیه خانه قرار می‌گیرند. با این حال توجه شود که ممکن است مواردی باشد که AD به یک اراده دهنده خدمت خاص که مدیریت AD هم بخشی از مدیریت خدمتی که به کاربر ارائه می‌دهد متصل باشد.

### د-۷ قوانین استفاده محتوای CPCM

استفاده مجاز از هر موردی از محتوای CPCM شامل یک مجموعه از بیانیه‌های به‌کارگیری است که قوانین به‌کارگیری CPCM مربوط به محتوا را بیان می‌کند. قوانین به‌کارگیری CPCM می‌تواند توسط ارائه‌دهنده محتوا یا ارائه‌دهنده خدمت تنظیم شود یا از نحوه تحویل (مثلا همه‌پخشی آزاد) نگاشت شود.
حدی که ذخیره، مصرف و عملیات صادرات می‌تواند پیاده‌سازی شود ممکن است موضوع به‌کارگیری مجاز محتوا باشد. CPCM یک مجموعه قوانین معمول کاربرد تعریف می‌کند که هر ارائه‌دهنده محتوا می‌تواند از بین انها انتخاب کند و کاربرد مجاز مدنظر در سامانه CPCM را ارائه دهد.
مجموعه قوانین کاربرد CPCM به‌گونه‌ای طراحی شده که انعطاف کافی برای پوشش همه مدل‌های کاربردهای مجافظت و مدیریت محتوا داشته باشد و همچنین به اندازه کافی مختصر باشد تا مدلی کاربرد محتوایی شفاف و ساده برای مصرف کننده ارائه دهد.

### د-۸ داده‌های عظیم اطلاعات وضعیت کاربرد

کاربرد مجاز یک مورد محتوایی به‌صورت داده‌های عظیم محتوای CPCM کد شده که به آن اطلاعات وضعیت کاربرد (USI) می‌گویند. محتوای CPCM بر اساس USI مربوط به هر مورد محتوایی مدیریت و محافظت می‌شود.

به جز تغییر وضعیت USI که به‌طور ضمنی توسط سامانه CPCM پیاده‌سازی می‌شود هستارهایی که مجوز قانونی بر محتوای سامانه CPCM دارند می‌توانند سایر تغییرات وضعیت USI بعد از اکتساب به سامانه CPCM را اعمال کنند

### د-۹ محتوای CPCM

به‌طور کلی "محتوا" به محتوای صوتی تصویری به اضافه داده‌های پیوست نظیر زیرنویس، تصویر /شکل، پویا نوایی، صفحات وب؛ متن، نرم‌افزار (کد منبع وکد شیء) ، متن برنامه،یا هر اطلاعاتی که به کاربر تحویل وتوسط او مصرف شود اطلاق می‌شود. محتوای CPCM محتوایی است که توسط وبا مطابقت با سامانه CPCM محافظت و مدیریت می‌شود. یک مورد محتوایی یک نمونه مجزا از محتوا در یک دوره محدود است. هر مورد محتوایی CPCM دارای یک پروانه محتوا که USI و داده‌های عظیم CPCM را حمل می‌کند است. سامانه CPCM می‌تواند پروانه محتوا و خود مورد محتوایی را در روش‌های مختلف بسته به هدف کارکرد و یا قوانین کاربرد اعمال شده به عنوان ملزومات USI به‌کار گیرد.

### د-۱۰ افزاره CPCM

یک افزاره CPCM یک افزاره است که هر کارکرد CPCM را در یک روش سازگار پیاده می‌کند. پیاده‌سازی کارکرد CPCM به عنوان نمونه CPCM مطرح می‌شود. یک افزاره CPCM یک افزاره میزبان یک یا چند نمونه CPCM است. همچنین ممکن است علاوه بر کارکردهای CPCM شامل کارکردهای سازگار با غیر CPCM باشد. اداره محتوای CPCM تنها با نمونه CPCM درون افزاره انجام می‌شود. بخش غیر CPCM افزاره به بخش محتوای CPCM دسترسی ندارد. افزاره CPCM می‌تواند میزبان کارکردهای امن غیر CPCM برای امنیت اکتساب محتوا از دیگر سامانه‌های محافظت یا صادرات امن (یا در صورت امکان مصرف) محتوای CPCM هم باشد.

### د-۱۱ قوانین کاربرد و اطلاعات وضعیت کاربرد

قانون کاربرد CPCM عملیات پیاده‌سازی یا رفتار محتواست که باید در محدوده سامانه CPCM واپایش شود. مجموعه کامل بیانیه‌های قوانین کاربرد برای مورد محتوایی CPCM مشخص، کاربرد مجاز مورد محتوایی CPCM است. کاربرد مجاز مورد محتوایی توسط کدگذاری اطلاعات وضعیت کاربرد(USI) ، داده‌ای عظیم محتوای CPCM که کاربرد مجاز محتوای مشخص را نشان می‌دهد، بیان می‌شود.

## پیوست ه

## طرح کد قابل تبدیل امن

## (الزامی)

### ه-۱ کلیات طرح کدقابل تبدیل امن

تبدیل کد محتوا به دلیل افزایش عمومیت انواع مختلف افزاره‌ها مانند PDA، افزارهای غیر PC، تلفن همراه و پایانه‌های هوشمند موبایل توجه زیادی را جلب کرده اند.تبدیل کد به پردازش تغییر حالت محتوای چند رسانه‌ای مانند تصویر، متن، صوت و ویدئو از قالب اصلی به قالب و کیفیت متفاوت اشاره دارد.

تبدیل کد در جستجوی کاهش تاخیر بارگذاری محتوای چند رسانه‌ای بر ارتباط دسترسی باند باریک مانند پیوندهای مودم و ارتباطات دسترسی بیسیم و حل عدم تطابق بین قالب‌های کدگذاری پشتیبانی شده توسط افزاره کاربر و محتوای چند رسانه‌ای ارائه‌دهنده خدمت است.

همچنین اجازه می‌دهد محدودیت‌های پردازشی پایانه محتوای کدگذاری شده را بر اساس قابلیت‌های تبدیل کد نمایش دهند. سه هستار برای طرح تبدیل کد امن وجود دارد: یک فرستنده، یک گره واسط شبکه، و یک کاربر با پایانه تلویزیون مبتنی بر اینترنت.

کارکرد تبدیل کد در گره واسط شبکه که بین ارائه‌دهنده محتوا و افزاره کارخواه است قرار گرفته است. دو نوع معماری تبدیل کد وجود دارد: معماری تبدیل کد سنتی و معماری تبدیل کد امن. در معماری تبدیل کد سنتی یک واسط تبدیل کد به عنوان یک گره واسط شبکه بین خدمت دهنده محتوا و افزاره کارخواه به کارگرفته می‌شود. ارسال کننده محتوا را با فشرده سازی کافی کدگذاری کرده و محتوای کدگذاری شده را به گره واسط شبکه که به آن واسط تبدیل کد می‌گویند ارسال می‌کند. واسط تبدیل کد، محتوا را کد گشایی کرده واز حالت فشرده خارج می‌کند. سپس انداره و یا قالب محتوا را در یک فشرده‌سازی جدید تغییر می‌دهد و نهایتا داده‌ها را برای ارسال به افزاره کارخواه دوباره کدگذاری می‌کند.افزاره کارخواه محتوای کد شده را کدگشایی کرده و از با استفاده از الگوریتم فشرده سازی حالت فشرده خارج می‌کند. با این حال توجه شود که مشکلات امنیتی در واسط تبدیل کد اتفاق می‌افتد برای نمونه زمانی که محتوا در واسط تبدیل کد کدگشایی می‌شود و قبل از آنکه کدگذاری شود، محتوای کدگشایی شده در واسط تبدیل کد قرار می‌گیرد. به عبارت دیگر مشاهده‌گر می‌تواند با استراق سمع به محتوای کدگشایی شده دسترسی پیدا کند. چنین محتوای کد گشایی شده‌ای با این که تنها ارسال کننده و کارخواه مجاز برای دسترسی به محتوای در مرحله کدگشایی پشتیبانی می‌شوند، تضمین امنیت انتها به انتهای حریم‌خصوصی را تضعیف می‌کند.

برای رسیدگی به مشکل امنیت، معماری تبدیل کد امن پیشنهاد می‌شود. طرح کد قابل تبدیل امن یک نوع طرح امنیتی است که گره واسط شبکه را قادر به پیاده‌سازی تبدیل کد بدون کدگشایی با حفظ امنیت انتها به انتها کند. این طرح می‌تواند با ترکیب کدگذاری مقیاس‌پذیر، کدگذاری پیشران، و بسته‌سازی پیاده‌سازی شود. ارسال کننده یک کارکرد تبدیل کد امن را برای تولید بسته‌های کدگذاری شده مقیاس‌پذیر از ویدئو و اضافه کردن سربار کد نشده برای ارسال اطلاعات پیاده‌سازی می‌کند، گره واسط شبکه سربار کد نشده را

می‌خواند و اطلاعات را برای کوتاه کردن یا حذف بسته‌های کافی مطابق عملیات تبدیل کد استفاده می‌کند و پایانه تلویزیون مبتنی بر اینترنت بسته‌های کد شده را کد گشایی کرده و بسته‌های کد متن ساده را برای تولید ویدئو استفاده می‌کند.

## کتاب‌نامه


**[1]** [b-ITU-T H.222.0] Recommendation ITU-T H.222.0 (2006) | ISO/IEC 13818-1:2007, Information technology – Generic coding of moving pictures and associated audio information: Systems.

**[2]** [b-ITU-T H.622.1] Recommendation ITU-T H.622.1 (2008) , Architecture and functional requirements for home networks supporting IPTV services.

**[3]** [b-ITU-T M.1400] Recommendation ITU-T M.1400 (2006) , Designations for interconnections among operator's networks.

**[4]** [b-ITU-T Q.1290] Recommendation ITU-T Q.1290 (1998) , Glossary of terms used in the definition of intelligent networks.

**[5]** [b-ITU-T X.800] Recommendation ITU-T X.800 (1991) , Security architecture for open systems interconnection for CCITT applications.

**[6]** [b-ITU-T X.805] Recommendation ITU-T X.805 (2003) , Security architecture for systems providing end-to-end communications.

**[7]** [b-ITU-T Y.101] Recommendation ITU-T Y.101 (2000) , Global Information Infrastructure terminology: Terms and definitions.

**[8]** [b-ITU-T Y.1901] Recommendation ITU-T Y.1901 (2009) , Requirements for the support of IPTV services.

**[9]** [b-ITU-T Y.2012] Recommendation ITU-T Y.2012 (2006) , Functional requirements and architecture of the NGN release 1.

**[10]** [b-ETSI TS 102 825] ETSI TS 102 825 (all parts) , Digital Video Broadcasting (DVB) ; Content Protection and Copy Management (DVB-CPCM) . <http://pda.etsi.org/pda/AQuery.asp>

**[11]** [b-ATIS 0800001] ATIS 08000001, IPTV DRM Interoperability Requirements, ATIS-IIF, April 2007. <htpps://www.atis.org/docstore/product.aspx?id=21212>

**[12]** [b-ATIS 0800006] ATIS 0800006, IIF Default Scrambling Algorithm (IDSA) IPTV Interoperability Specification, February, 2007. <htpps://www.atis.org/docstore/product.aspx?id=22663>