الاتحـــــــــاد الدولـــــــــي للاتصـــــــــالات

ITU-T

قطـــاع تقييس الاتصـــالات
في الاتحاد الدولي للاتصالات

X.1191

(2009/02)

السلسلة X: شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

تطبيقات وخدمات آمنه – أمن التلفزيون القائم على بروتوكول الإنترنت

المتطلبات الوظيفية لجوانب أمن التلفزيون القائم على بروتوكول الإنترنت (IPTV) ومعماريته

التوصيـــة ITU-T X.1191

الاتحاد الدولي للاتصالات ITU

توصيات السلسلة X الصادرة عن قطاع تقييس الاتصالات

شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن

الشبكات العمومية للبيانات	X.119-X.1
التوصيل البيني للأنظمة المفتوحة	X.299-X.200
التشغيل البيني للشبكات	X.399-X.300
أنظمة معالجة الرسائل	X.499-X.400
الدليـــل	X.599-X.500
التشغيل البيني لأنظمة التوصيل OSI ومظاهر النظام	X.699-X.600
إدارة التوصيل البيني للأنظمة المفتوحة (OSI)	X.799-X.700
الأمن	X.849-X.800
تطبيقات التوصيل البيني للأنظمة المفتوحة (OSI)	X.899-X.850
المعالجة الموزعة المفتوحة	X.999-X.900
أمن المعلومات والشبكات	
الجوانب العامة للأمن	X.1029-X.1000
أمن الشبكة	X.1049-X.1030
إدارة الأمن	X.1069-X.1050
الخصائص البيومترية	X.1099-X.1080
تطبيقات وخدمات آمنة	
أمن البث المتعدد	X.1109-X.1100
أمن الشبكة المحلية	X.1119-X.1110
أمن الخدمات المتنقلة	X.1139-X.1120
أمن الويب	X.1149-X.1140
بروتوكولات الأمن	X.1159-X.1150
الأمن بين جهتين نظيرتين	X.1169-X.1160
أمن معرفات الهوية عبر الشبكات	X.1179-X.1170
أمن التلفزيون القائم على بروتوكول الإنترنت	**X.1199-X.1180**
أمن الفضاء السيبراني	
الأمن السيبراني	X.1229-X.1200
مكافحة الرسائل الاقتحامية	X.1249-X.1230
إدارة الهوية	X.1279-X.1250
تطبيقات وخدمات آمنة	
اتصالات الطوارئ	X.1309-X.1300
أمن شبكات المحاسيس واسعة الانتشار	X.1339-X.1310

لمزيد من التفاصيل، يرجى الرجوع إلى قائمة التوصيات الصادرة عن قطاع تقييس الاتصالات.

التوصيـــة ITU-T X.1191

المتطلبات الوظيفية لجوانب أمن التلفزيون القائم على بروتوكول الإنترنت (IPTV) ومعماريته

ملخص

تتناول التوصية ITU-T X.1191 المتطلبات الوظيفية لجوانب أمن التلفزيون القائم على بروتوكول الإنترنت (IPTV)، وكذلك المعمارية والآليات من حيث محتوى تلفزيون IPTV والخدمات والشبكات والأجهزة المطرافية والمشتركين (المستعملين النهائيين).

المصدر

وافقت لجنة الدراسات 17 (2009-2012) لقطاع تقييس الاتصالات بتاريخ 20 فبراير 2009 على التوصية ITU-T X.1191 بموجب الإجراء الذي ينص عليه القرار 1 للجمعية العالمية لتقييس الاتصالات.

الكلمات الرئيسية

الاستيقان والتخويل والتجفير والتلفزيون القائم على بروتوكول الإنترنت وحماية الخصوصية والأمن ومعمارية الأمن والتخليط وحماية الخدمة والمحتوى.

تمهيـــد

الاتحاد الدولي للاتصالات وكالة متخصصة للأمم المتحدة في ميدان الاتصالات ومعلومات وتكنولوجيات الاتصالات (ICT). وقطاع تقييس الاتصالات (ITU-T) هو هيئة دائمة في الاتحاد الدولي للاتصالات. وهو مسؤول عن دراسة المسائل التقنية والمسائل المتعلقة بالتشغيل والتعريفة، وإصدار التوصيات بشأنها بغرض تقييس الاتصالات على الصعيد العالمي.

وتحدد الجمعية العالمية لتقييس الاتصالات (WTSA)، التي تجتمع مرة كل أربع سنوات، المواضيع التي يجب أن تدرسها لجان الدراسات التابعة لقطاع تقييس الاتصالات وأن تُصدر توصيات بشأنها.

وتتم الموافقة على هذه التوصيات وفقاً للإجراء الموضح في القرار رقم 1 الصادر عن الجمعية العالمية لتقييس الاتصالات.

وفي بعض مجالات تكنولوجيا المعلومات التي تقع ضمن اختصاص قطاع تقييس الاتصالات، تعد المعايير اللازمة على أساس التعاون مع المنظمة الدولية للتوحيد القياسي (ISO) واللجنة الكهرتقنية الدولية (IEC).

ملاحظـــة

تستخدم كلمة "الإدارة" في هذه التوصية لتدل بصورة موجزة سواء على إدارة اتصالات أو على وكالة تشغيل معترف بها.

والتقيد بهذه التوصية اختياري. غير أنها قد تضم بعض الأحكام الإلزامية (بهدف تأمين قابلية التشغيل البيني والتطبيق مثلاً). ويعتبر التقيّد بهذه التوصية حاصلاً عندما يتم التقيّد بجميع هذه الأحكام الإلزامية. ويستخدم فعل "يجب" وصيغ ملزمة أخرى مثل فعل "ينبغي" وصيغها النافية للتعبير عن متطلبات معينة، ولا يعني استعمال هذه الصيغ أن التقيّد بهذه التوصية إلزامي.

حقوق الملكية الفكرية

يسترعي الاتحاد الانتباه إلى أن تطبيق هذه التوصية أو تنفيذها قد يستلزم استعمال حق من حقوق الملكية الفكرية. ولا يتخذ الاتحاد أي موقف من القرائن المتعلقة بحقوق الملكية الفكرية أو صلاحيتها أو نطاق تطبيقها سواء طالب بها عضو من أعضاء الاتحاد أو طرف آخر لا تشمله عملية إعداد التوصيات.

وعند الموافقة على هذه التوصية، لم يكن الاتحاد قد تلقى إخطاراً بملكية فكرية تحميها براءات الاختراع يمكن المطالبة بها لتنفيذ هذه التوصية. ومع ذلك، ونظراً إلى أن هذه المعلومات قد لا تكون هي الأحدث، يوصى المسؤولون عن تنفيذ هذه التوصية بالاطلاع على قاعدة المعطيات الخاصة ببراءات الاختراع في مكتب تقييس الاتصالات (TSB) في الموقع http://www.itu.int/ITU-T/ipr/.

المحتـــويات

الصفحة

الصفحة

مقدمة

إن خدمات التلفزيون القائم على بروتوكول الإنترنت (IPTV)، والمحتوى المُسلَّم عبر تلك الخدمات، والأجهزة المطرافية المستخدمة في المعالجة وتزويد مثل هذه الخدمات، تحتاج إلى بحث الكثير من الجوانب الأمنية. وتصوغ هذه الوثيقة المتطلبات، والنماذج المعمارية، والكيانات الوظيفية، والأسطح البينية، والآليات، ومادة المعلومات الأساسية الإعلامية الإضافية التي تصف وتتناول هذه الجوانب الأمنية.

التوصيـــة ITU-T X.1191

المتطلبات الوظيفية لجوانب أمن التلفزيون القائم على بروتوكول الإنترنت (IPTV) ومعماريته

1 مجال التطبيق

تتناول هذه التوصية المتطلبات الوظيفية لجوانب أمن التلفزيون القائم على بروتوكول الإنترنت (IPTV) وكذلك المعمارية والآليات من حيث محتوى التلفزيون IPTV والخدمات والشبكات والأجهزة المطرافية، والمشتركين. ويتوقع إمكانية تطبيق المتطلبات والوظائف ذات الصلة المحددة في هذه التوصية بصورة سليمة طبقاً لنماذج خدمة وأعمال تلفزيون IPTV، وهو ما قد يتطلب مستوى مختلفاً من الإمكانيات الأمنية.

2 المراجع

تتضمن التوصيات التالية لقطاع تقييس الاتصالات وغيرها من المراجع أحكاماً تشكل من خلال الإشارة إليها في هذا النص جزءاً لا يتجزأ من هذه التوصية. وقد كانت جميع الطبعات المذكورة سارية الصلاحية في وقت النشر. ولما كانت جميع التوصيات والمراجع الأخرى تخضع إلى المراجعة، يرجى من جميع المستعملين لهذه التوصية السعي إلى تطبيق أحدث طبعة للتوصيات والمراجع الأخرى الواردة أدناه. وتُنشر بانتظام قائمة توصيات قطاع تقييس الاتصالات السارية الصلاحية. والإشارة إلى وثيقة ما في هذه التوصية لا يضفي على الوثيقة في حد ذاتها صفة التوصية.

[ITU-T X.509] التوصية ITU-T X.509 (2008) | المعيار ISO/IEC 9594-8:2008، *تكنولوجيا المعلومات – التوصيل البيني للأنظمة المفتوحة – الدليل: أطر شهادة المفاتيح العمومية والنعوت.*

[ITU-T Y.1910] التوصية ITU-T Y.1910 (2008)، *المعمارية الوظيفية للتلفزيون القائم على بروتوكول الإنترنت.*

3 مصطلحات وتعاريف

1.3 مصطلحات معرفة في وثائق أخرى

1.1.3 التحكم في النفاذ [b-ITU-T X.800]: الحيلولة دون الاستخدام غير المُخَوَّلْ لمورد من الموارد بما في ذلك منع استخدام مورد على نحو غير مُخَوّل.

2.1.3 التطبيق [b-ITU-T Y.101]: مجموعة مُبَنْيَنة من القدرات توفر عنصراً وظيفياً ذا قيمة مضافة تدعمه خدمة أو أكثر من خدمة.

3.1.3 الاستيقان [b-ITU-T X.800]: انظر استيقان منشأ البيانات واستيقان الكيانات النظيرة.

4.1.3 التخويل [b-ITU-T X.800]: منح حقوق النفاذ، التي تشمل منح النفاذ بناء على حقوق النفاذ.

5.1.3 التيسر [b-ITU-T X.800]: خاصية كون الشيء قابلاً للنفاذ والاستخدام بناء على طلب من كيان مُخَوّل.

6.1.3 السرية [b-ITU-T X.800]: خاصية عدم إتاحة المعلومات أو الكشف عنها لأشخاص غير مخولين أو لكيانات، أو عمليات غير مُخَوَّلَةْ.

7.1.3 استيقان منشأ البيانات [b-ITU-T X.800]: التدليل على أن مصدر البيانات المتلقاة هو كما يُدعَّى.

8.1.3 رفض تقديم الخدمة (DOS) [b-ITU-T X.800]: منع النفاذ المُخوّل إلى الموارد أو تأخير العمليات التي يمثل فيها الزمن عنصراً حرجاً.

9.1.3 التوقيع الرقمي [b-ITU-T X.800]: البيانات الملحقة بـــ، أو التحويل التجفيري (انظر التجفير) لوحدة بيانات يسمح لمستقبل وحدة البيانات هذه أن يُثبت مصدر وحدة البيانات وسلامتها، وأن يتوقى التحايل مثلاً من جانب المُسْتَقبِلْ.

10.1.3 قطار أساسي [b-ITU-T H.222.0]: وهو مصطلح تنوعي للفيديو المشفر، أو المادة المسموعة المشفرة أو أي قطار بتات مشفر في رزمة قطار أساسي بالرُزَم.

ملاحظة – PES تعني قطار أساسي بالرزم.

11.1.3 المعمارية الوظيفية [b-ITU-T Y.2012]: مجموعة من الكيانات الوظيفية، والنقاط **المرجعية** الموجودة فيما بينها، والمستخدمة في وصف بنية شبكة من شبكات الجيل التالي. وتكون هذه الكيانات الوظيفية منفصلة عن بعضها بواسطة نقاط مرجعية، ومن ثم، فهي تقوم بتعريف توزيع الوظائف.

12.1.3 الكيان الوظيفي [b-ITU-T Y.2012]: وهو كيان يشمل مجموعة غير قابلة للتجزيء من الوظائف المحددة. والكيانات الوظيفية هي مفاهيم منطقية، بينما تُستَخْدَم تجميعات الكيانات الوظيفية لوصف التطبيقات العملية المادية.

13.1.3 السلامة [b-ITU-T X.800]: وهي خاصية أن البيانات لم يطرأ عليها تغيير أو تدمير بصورة غير مخولة.

14.1.3 المفتاح [b-ITU-T X.800]: وهو تتابع رموز يتحكم في عمليات التشفير وفك التشفير.

15.1.3 إدارة المفاتيح [b-ITU-T X.800]: وهي توليد وتخزين وتوزيع، وإلغاء وحفظ واستعمال المفاتيح بما يتفق مع سياسات الأمن.

16.1.3 التنكر [ITU-T X.800]: وهو ادعاء أحد الكيانات بأنه كيان مختلف.

17.1.3 مورد الشبكات [b-ITU-T Q.1290]: وهو المنظمة التي تحافظ على مكونات الشبكات اللازمة لوظيفية التلفزيون القائم على بروتوكول الإنترنت وتقوم بتشغيلها.

الملاحظة 1 – يمكن لمورد الشبكة أن يقوم اختيارياً بدور مورد خدمات أيضاً.

الملاحظة 2 – على الرغم من كونهما كيانين منفصلين، فإن مورد الخدمات ومورد الشبكات يمكنهما اختيارياً أن يكونا كياناً تنظيمياً واحداً.

18.1.3 استيقان الكيانات النظيرة [b-ITU-T X.800]: وهو إثبات أن كيانا نظيراً داخل اتحاد ما، ما هو إلا الكيان المُدَّعَى.

19.1.3 الخصوصية [b-ITU-T X.800]: وهي حق الأفراد في التحكم في، أو التأثير على أي المعلومات ذات الصلة بهم هي التي يمكن جمعها وتخزينها بواسطة من، ولمن يمكن إفشاء هذه المعلومات.

20.1.3 الإنكار [b-ITU-T X.800]: نفي أحد الكيانات الضالعة في اتصال ما لأن يكون قد شارك في كل أو جزء من الاتصال.

21.1.3 الوسم الأمني [b-ITU-T X.800]: وهو العلامة المقصورة على مَوْرد (قد يكون وحدة بيانات) تبين اسم، أو تحدد النعوت الأمنية لذلك المَوْرد.

ملاحظة – قد تكون علامة الوسم/أو اللصق صريحة أو ضمنية.

22.1.3 السياسات الأمنية [b-ITU-T X.800]: مجموعة المعايير الخاصة بتقديم خدمات الأمن.

23.1.3 مورد الخدمة [b-ITU-T M.1400]: إشارة عامة إلى مُشّغِلْ يقدم خدمات الاتصالات إلى العملاء والمستعملين الآخرين إما على أساس تعريفة أو عقد. ويمكن لمورد الخدمة أن يقوم اختيارياً بتشغيل شبكة. ويمكن لمورد الخدمة أن يكون اختيارياً عميلاً لمورد خدمة آخر.

24.1.3 تهديد [b-ITU-T X.800]: خرق محتمل للأمن.

2.3 مصطلحات مُعَرَّفَة في هذه التوصية

تُعَرِف هذه التوصية المصطلحات التالية:

1.2.3 استحواذ: عملية حصول المستعمل النهائي على محتوى.

2.2.3 تصدير المحتوى: عملية الإرسال المأمون لمحتوى التلفزيون القائم على بروتوكول الإنترنت من مطراف تابع للتلفزيون القائم على بروتوكول الإنترنت إلى مطراف آخر مملوك للمستعمل صاحب الاستحقاق في الاستعمال.

3.2.3 حماية المحتوى: ضمان أن يكون بمقدور المستعمل النهائي أن يستعمل فقط المحتوى الذي حازه/حازته طبقاً للحقوق الممنوحة له/لها من جانب مالك الحقوق، وتنطوي حماية المحتوى على حماية المحتويات من الاستنساخ والتوزيع غير المشروعين، واعتراض طريق المحتويات أثناء انتقالها، والتلاعب فيها واستعمالها بصورة غير مُخَولة، إلى غير ذلك.

4.2.3 تتبع المحتوى: هي عملية تمكن من التعرف على المنشأ (التحكمي) للمحتوى و/أو الطرف المسؤول (مثل المستعمل النهائي) لتيسير التحقيق التالي في حالة الاستعمال غير المخول للمحتوَى، مثال ذلك، استنساخ أو إعادة توزيع المحتوى.

ملاحظة – يجوز إرفاق معلومات تتبع المحتوى بالمحتوى إما كبيانات شرحية أو كعلامة مائية قضائية.

5.2.3 الاستحقاقات: تشير إلى مستوى (مستويات) التخويل بما في ذلك معلومات النفاذ المشروط التي يمكن استخدامها من جانب مشترك للنفاذ إلى خدمات معينة من خدمات التلفزيون القائم على بروتوكول الإنترنت في جهازه/جهازها المطرافي للتلفزيون القائم على بروتوكول الإنترنت.

6.2.3 حماية الجهاز المطرافي للتلفزيون القائم على بروتوكول الإنترنت: التأكد من أن الجهاز المطرافي TD الذي يستخدمه مستعمل نهائي لاستقبال خدمة ما يمكنه أن يستخدم المحتوى بصورة أكيدة وآمنة بينما يقوم في نفس الوقت بإنفاذ حقوق الاستعمال الممنوحة لمثل هذا المحتوى أثناء الحماية المادية والإلكترونية لسلامة المطراف النهائي، وسرية المحتوى ومَعْلَمات الأمن الحَرِجة (مثال المفاتيح المحفوظة) غير المحمية.

7.2.3 التلفزيون الخطي: خدمة بث تلفزيوني شبيهة بالشكل الكلاسيكي لخدمات التلفزيون التي تقدم إما بواسطة التلفزيون الكبلي، أو عبر خدمات الأرض أو مشغل ساتلي مباشرة إلى المسكن، ويتم إرسال محتوى البرنامج في هذه الحالة طبقاً للجدول المحدد والموجه إلى استهلاك الوقت الفعلي من جانب المستعمل النهائي.

8.2.3 بيانات شرحية لتسهيل الوسم بالعلامات المائية: هي بيانات شرحية يتم وضعها للمساعدة في الوسم اللاحق بالعلامات المائية والتي تقوم أجهزة اتجاه المقصد بدمجها.

9.2.3 التحايل: وهو عملية الاستحواذ على معلومات حساسة أو شخصية مثل اسم المستعمل أو تاريخ الميلاد، أو تفاصيل بطاقة الائتمان وذلك عن طريق التخفي في صورة كيان جدير بالثقة.

10.2.3 الحقوق: وتشير إلى القدرة على القيام بمجموعة وظائف استعمال محددة سلفاً خاصة ببند محتوى؛ وتشمل وظائف الاستعمال هذه التصريحات (مثلاً بالمشاهدة/الاستماع، الاستنساخ، التعديل، التسجيل، الاقتباس، أخذ العينات، أو الاحتفاظ بالمحتوى لفترة معينة أو التوزيع)، والقيود (مثال ذلك العرض/المشاهدة/الاستماع لمرات عديدة، أو العرض/المشاهدة/الاستماع لعدد معين من الساعات)، والالتزامات (مثال، تسديد الرسوم، تتبع المحتوى) التي تنطبق على المحتوى وتوفر حرية الاستعمال التي تُمنح للمستعمل النهائي.

11.2.3 التعبير عن الحقوق: الصياغة التركيبية اللغوية للحقوق في شكل محدد ونظامي.

12.2.3 حماية الخدمة والمحتوى من طرف إلى طرف: أسلوب تشغيل حماية الخدمة والمحتوى حيث يتم النفاذ إلى المحتوى أو تبادله بواسطة أجهزة مطرافية وذلك طبقاً للحقوق الممنوحة باستعمال نظام واحد لحماية الخدمة والمحتوى

13.2.3 تجسير حماية الخدمة والمحتوى: هو أسلوب تشغيل حماية الخدمة والمحتوى يعمل فيه نظامان أو أكثر لحماية الخدمة والمحتوى على جهاز واحد يقوم مقام الجسر بين نظم حماية الخدمة والمحتوى هذه، ويمكن النفاذ إلى المحتوى الذي يتم الحصول

عليه عبر نظام واحد لحماية الخدمة والمحتوى عبر نظام آخر لحماية الخدمة والمحتوى موجود على الجسر وذلك طبقاً للحقوق الممنوحة

14.2.3 تبادل حماية الخدمة والمحتوى: وهو أسلوب تشغيل أكثر عمومية لحماية الخدمة والمحتوى ويضم جهازيْن أو أكثر، ويكون لكل جهاز منها نظامٌ أو أكثر من أنظمة تشغيل حماية الخدمة والمحتوى؛ أما المحتوى الذي يتم الحصول عليه بواسطة جهاز عبر نظام من أنظمته الخاصة بحماية الخدمة والمحتوى فيمكن نقله بأمان إلى جهاز آخر، وكذلك النفاذ إليه من جهاز آخر عبر نظام مختلف لحماية الخدمة والمحتوى بموجب الحقوق الممنوحة

15.2.3 التخليط: عملية مصممة لحماية محتوى متعدد الوسائط، وعادة ما يستخدم التخليط تكنولوجيا التجفير بغرض حماية المحتوى

16.2.3 خوارزمية التخليط: وهي الخوارزمية المستخدمة في عملية التخليط أو عملية إزالة التخليط

17.2.3 مخطط آمن للتحويل الشفري: وهو عبارة عن مخطط أمني يساعد عقدة الشبكة الوسيطة على القيام بالتحويل الشفري بدون إزالة التشفير مع الاحتفاظ في نفس الوقت بالأمن من طرف إلى طرف، ويمكن تنفيذ هذا المخطط عن طريق الجمع بين التشفير القابل للتوسع، والتجفير التدريجي، والترزيم. ويمكن للمخطط الآمن للتحويل الشفري أن يوفر كلا من السرية وسلامة الرسالة/الاستيقان.

18.2.3 حماية الخدمة: التأكد من أن أي مستعمل نهائي يمكنه فقط الحصول على الخدمة وعلى المحتوى الكائن فيها بمقدار ما هو/هي مُخوّل (مخولة) للحصول عليه منها، وتشمل حماية الخدمة حماية الخدمة من النفاذ غير المُخَوَّل ذلك أن محتويات التلفزيون القائم على بروتوكول الإنترنت تمتد عبر وصلات خدمة التلفزيون القائم على بروتوكول الإنترنت

19.2.3 حماية الخدمة والمحتوى: وهي تجميع لكل من حماية الخدمة وحماية المحتوى أو النظام الخاص بذلك أو تنفيذه

20.2.3 المخادعة (Spoofing): وهو نشاط ينجح فيه مَصْدَر مُزَوَرْ (احتيالي) (كشخص مثلاً أو برنامج حاسوب) بانتحال صفة مصدر قانوني وذلك عن طريق تزوير البيانات، وبغرض الحصول على معلومات و/أو التعتيم على المصدر الحقيقي بحيث يتمكن المصدر الزائف من إجراء أنشطة غير مُخَوَّلة كالقيام مثلاً بنشر مواد حاسوبية خبيثة (كالفيروسات مثلاً)، وما إلى ذلك.

21.2.3 مقاومة التلاعب: مقاومة التلاعب من جانب المستعملين الشخصيين/المهاجمين في منتج أو رزمة أو نظام بالنفاذ إليه مادياً/برمجياً.

22.2.3 التحويل الشفري: وهو عملية تحويل محتوى الوسائط المتعددة كالصور، والنصوص، والمواد السمعية والمرئية من نسق أصلي إلى نسق مختلف أو نوعية مختلفة

23.2.3 حماية خصوصية المستَعْمِل: ضمان أن تظل المعلومات التي تعتبر خصوصية (سرية) من جانب مستعمل نهائي سرية، بينما تبقى في نفس الوقت قابلة للإفشاء الإجباري إذا استدعت الإجراءات القضائية ذلك

24.2.3 التوقيع الفيديوي: وهي البيانات الشرحية (أو السمة المرئية) للتعرف على المحتوى الفيديوي، والبصمة الفيديوية، فهي على خلاف العلامة المائية التي تُطْمَر عن طريق معالجة المحتويات الفيديوية الأصلية، تؤخذ من المحتوى الفيديوي ذاته دون مخاطرة تقليل جودة ذلك المحتوى

4 المختصرات والأسماء المختصرة

تستعمل هذه التوصية المختصرات والأسماء المختصرة التالية:

AAA الاستيقان، التخويل، والمحاسبة *(Authentication, Authorization, and Accounting)*

AD ميدان تحول *(Authorized Domain)*

CBC تسلسل فدرة الشفرة *(Cipher Block Chaining)*

CDN شبكة توصيل المحتوى *(Content Delivery Network)*

DNG بوابة شبكة التسليم *(Delivery Network Gateway)*

DNGF وظيفة بوابة شبكة التسليم *(Delivery Network Gateway Function)*

DoS رفض تقديم الخدمة *(Denial of Service)*

ECB كتاب الشفرة الكهربائية *(Electric Code Book)*

ECM رسالة مراقبة الاستحقاقات *(Entitlement Control Message)*

EMM رسالة إدارة الاستحقاقات *(Entitlement Management Message)*

EPG دليل البرنامج الإلكتروني *(Electronic Program Guide)*

HN شبكة محلية *(Home Network)*

HN-TD جهاز مطرافي في شبكة محلية *(Home Network Terminal Device)*

ID مُعرِّف هوية *(Identifier)*

IPTV التلفزيون القائم على بروتوكول الإنترنت *(Internet Protocol Television)*

MIKEY إبراق الإنترنت متعدد الوسائط *(Multimedia Internet KEYing)*

NAT ترجمة عنوان الشبكة *(Network Address Translation)*

OFB خرج التغذية المرتدة *(Output FeedBack)*

P2P بين طرف ونظيره *(peer to peer)*

PDA مساعد رقمي شخصي *(Personal Digital Assistant)*

PIN رقم تعرف هوية شخصي *(Personal Identification Number)*

PKI البنية التحتية للمفاتيح العمومية *(Public Key Infrastructure)*

PVR مسجل فيديوي شخصي *(Personal Video Recorder)*

QoE جودة الخبرة *(Quality of Experience)*

QoS جودة الخدمة *(Quality of Service)*

REL لغة التعبير عن الحقوق *(Rights Expression Language)*

SCP حماية الخدمة والمحتوى *(Service and Content Protection)*

SCP-B جسر حماية الخدمة والمحتوى *(SCP Bridge)*

SCP-EE حماية الخدمة والمحتوى من طرف إلى طرف *(SCP End-to-End)*

SCP-IX تبادل حماية الخدمة والمحتوى *(SCP Interchange)*

STS مخطط آمن قابل للتحويل الشفري *(Secure Transcodable Scheme)*

TD جهاز مطرافي مطابق للتلفزيون القائم على بروتوكول الإنترنت *(IPTV-compliant Terminal Device)*

USB ناقل متسلسل عالمي *(Universal Serial Bus)*

VoD فيديو حسب الطلب *(Video on Demand)*

5 الاصطلاحات

في هذه التوصية الكلمتان الرئيسيتان "يتعين على" **"is required to"** تشيران إلى مَطْلَبْ "يتعين" الالتزام الصارم به ولا يسمح بالحيْد عنه، وذلك للدفع بالتطابق مع هذه التوصية

الكلمتان الرئيسيتان "يوصَي بـــ" **"is recommended"** تشير إلى مطلب "موصى به" وإن كانت ليست ضرورية بصورة مطلقة. وهكذا لا يتطلب الأمر وجود هذا الشرط للدفع بالمطابقة.

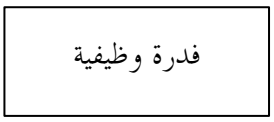
الكلمتان الرئيسيتان "يحظر على" **"is prohibited"** تشيران إلى اشتراط يجب الالتزام الصارم به وعدم السماح بالحيد عنه وذلك للدفع بالتطابق مع هذه التوصية.

الكلمتان الرئيسيتان "يمكن اختيارياً" **"can optionally"** تشيران إلى مطلب اختياري مسموح به دون أن ينطوي بأي معنى على أنه موصي به. وليس المقصود من هذا المصطلح أن يشير ضمناً إلى أن تنفيذ المورد يجب أن يوفر هذا الخيار، كما يمكن لهذه الخاصية أن تُفعَّل اختيارياً من جانب مُشغِل الشبكة/مورد الخدمات. بل يعني أن المورد قد يختار إتاحة هذه الخاصية ويظل مع ذلك يدفع بالتطابق مع هذه المواصفة.

وفي سياق معمارية أمن التلفزيون القائم على بروتوكول الإنترنت في هذه التوصية:

تُعرف "وظائف" بأنها مجموعة عناصر وظيفية ويُمثَل لها بالرمز التالي:

"**فدرة وظيفية**" وتُعرَّف بأنها زمرة عناصر وظيفية لم يتم الاستمرار في تقسيمها إلى أجزاء فرعية على مستوى التفاصيل الموصوفة في هذه التوصية ويمثل لها بالرمز التالي:



6 متطلبات الأمن

1.6 متطلبات الأمن العامة

- يُوصَى بأن تضع معمارية التلفزيون القائم على بروتوكول الإنترنت في اعتبارها ما للأداء، ونوعية الخدمة، والقابلية للاستعمال، والقابلية للتدرج والتعديل، وقيود الصرف من تأثير على نشر الأمن.
- يمكن لمعمارية التلفزيون القائم على بروتوكول الإنترنت اختيارياً أن تدعم حماية المحتوى الخاص بالمحتوى المتقاسم بين المستعملين النهائيين.

2.6 متطلبات أمن المحتوى

وتحدد هذه الفقرة المتطلبات التي تتعامل فرادى أو بصورة جماعية مع المحتوى وحماية المحتوى.

متطلبات المعمارية

- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم حماية المحتوى على النحو الوارد تعريفه في الفقرة 3.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم تصاحب المحتوى مع الحماية والبيانات الشرحية لإدارة المحتوى بما في ذلك البيانات الشرحية.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم التوصيل الآمن لحماية المحتوى والبيانات الشرحية لإدارة المحتوى بما في ذلك البيانات الشرحية لحقوق الاستعمال.
- يتعين على معمارية تلفزيون برتوكول الإنترنت أن تدعم البيانات الشرحية لحقوق استعمال المحتوى التي تميز بين حقوق الاستخدام التي تشمل الأداء (المشاهدة)، التخزين، (إعادة) التوزيع، وتوليفات من كل منهما.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم حماية المحتوى الذي يوزع في آنٍ واحد على عدد كبير جداً من المشتركين (قابلية التوسع).
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم حماية المحتوى المنقول على البث المتعدد و/أو البث الأحادي.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن يدعم تأمين المحتوى المخزون وفقاً لحق الاستعمال الممنوح.
- إذا تم نشر تتبع المحتوى، فيتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم التتبع الصارم للمحتوى خارج الخط (الوقت غير الفعلي) (محتوى الفيديو حسب الطلب).
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة دعم وسائل نقل معلومات تعقب المحتوى (مثال ذلك البيانات الشرحية لتيسير وضع العلامات المائية).
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت حجب الدعم عن تطبيق تكنولوجيا تتبع المحتوى في مخرجات الجهاز المطرافي (TD) وذلك بغرض قصر التعرف بصورة فريدة على دورة (مثال قناة، زمن/تاريخ)، جهاز مطرافي، و/أو مُشّغِلْ شبكة. ويجوز أن تشتمل نماذج تكنولوجيا تتبع المحتوى على معلومات مرئية وغير مرئية وذلك كخيار.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت منع استدعاء جميع معلومات تتبع المحتوى من المحتوى.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة دعم قابلية التشغيل البيني لحماية الخدمة والمحتوى حيث يقتصر استعمال محتوى تلفزيون برتوكول الإنترنت على المستعمل/المستعملين المرخص لهم بذلك أو الجهاز/الأجهزة المخولة حتى بعد نقله (نقلها) إلى نظام أمني آخر.
- ويحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة تقديم الدعم إلى قابلية التشغيل البيني لحماية الخدمة والمحتوى وذلك من أجل الاحتفاظ بمعلومات تعريف الهوية بحيث يمكن تعريف هوية محتوى التلفزيون القائم على بروتوكول الإنترنت بصورة مطابقة وذلك بغض النظر عن أي المخططات هي المستخدمة، وعن أي نظامٍ للأمن تم نقل المحتوى إليه.
- ويحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم إلى قابلية التشغيل البيني لحماية الخدمة والمحتوى وذلك لأجل تفادي تقليل مستوى الأمن عندما يتم نقل المحتوى إلى نظام أمني آخر.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم إلى قابلية التشغيل البيني لحماية الخدمة والمحتوى حيث يقتصر منح الحقوق على الأجهزة الموثوق بها.

- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم إلى قابلية التشغيل البيني لحماية الخدمة والمحتوى وذلك من أجل توفير بيئة آمنة لتبادل بيانات قابلية التشغيل البيني لحماية الخدمة والمحتوى (مثال معلومات الاستيقان، البيانات الشرحية، المعلومات عن المفاتيح، إلخ).
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم للتشغيل البيني لحماية المحتوى والخدمة بحيث لا تكون هذه القابلية للتشغيل مرتهنة ببرمجيات حاسوبية أو عتاد محدد.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت اشتراط تحديد آلية حماية الخدمة والمحتوى التابعة لأي جانب من جانبي مخططات قابلية التشغيل البيني لحماية الخدمة والمحتوى تحديداً صريحاً في محاولة منها لتحقيق قابلية التشغيل البيني.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم إلى قابلية التشغيل البيني لحماية الخدمة والمحتوى المرنة والقابلة للزيادة وذلك لدعم نماذج المتعددة للأعمال.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم إلى قابلية التشغيل البيني لحماية الخدمة والمحتوى فيما بين نظم الأمن المتعددة التي تستخدم آليات أمن مختلفة بغرض دعم خدمة الوقت المتغير السلسة (فيمكن للمشتركين أن يخزنوا المحتوى وأن يستدعوه في وقت لاحق) وخدمة المكان المتغير (أو يمكن للمشتركين مشاهدة المحتوى في أي مكان) حتى في ظل آليات أمن مختلفة.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم إلى قابلية التشغيل البيني لحماية الخدمة والمحتوى للاحتفاظ بالشفافية للمستعملين.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم إلى الآليات المتعددة لحماية المحتوى والخدمة بغض النظر عن المتطلبات الخاصة بالبرمجيات والعتاد.

توصيات المعمارية

- يستخدم محتوى التلفزيون القائم على بروتوكول الإنترنت تكنولوجيا تَتَبُّع المحتوى، ثم يوصي بأن تكون تكنولوجيا التتبُّع غير مُدرَكَة.
- يُوصي بأن تدعَم معمارية التلفزيون القائم على بروتوكول الإنترنت التتبُّع الصارم للمحتوى بالوقت الفعلي (مثال ذلك محتوى البث).
- يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت القدرة على استيقان وتخويل المستعملين النهائيين خدمات التشارك في المحتوى (مثال ذلك تصدير المحتوى وإعادة توزيع المحتوى)، إذا كان هناك دعم للتشارك في المحتوى.
- إذا استخدمت تنفيذ معمارية التلفزيون القائم على بروتوكول الإنترنت تكنولوجيا تتبع المحتوى التي تستند إلى البيانات الشرحية لتيسير وضع العلامات المائية والتي تطمر البيانات الشرحية ذات الصلة في القطار الأساسي للمحتوى؛ فإنه يوصي عندئذ باستخدام التدابير الخاصة "ببيانات المستعمل" التي ترد في مخطط التجفير المحدد.
- عندما يكون هناك جهاز مطرافي أو جهاز مطرافي لشبكة محلية داخل معمارية التلفزيون القائم على بروتوكول الإنترنت يدعم آليات متعددة لحماية المحتوى والخدمة، يوصى باستعمال وظيفة ترجمة قياسية مع التحسب لاحتمال توصيل أكثر من نظام من أنظمة حماية المحتوى والخدمة والترجمة فيما بينها بصورة متسقة مع ضمان قابلية التشغيل البيني لأي جهاز مطرافي أو أي جهاز مطرافي لشبكة محلية يشارك في آلية الترجمة هذه.

خيارات المعمارية

- يمكن لمعمارية التلفزيون القائم على بروتوكول الإنترنت أن تقوم اختيارياً بدعم إدراج معلومات تتبع المحتوى. ويمكن لمعلومات تتبع المحتوى تلك أن تشتمل اختيارياً على معرِّف هوية المُشَغِلْ، ومعرِّف هوية صاحب المحتوى، ومعرِّف هوية الجهاز المطرافي والمعلومات الأخرى.

متطلبات خوارزمية التخليط

- يتعين على خوارزميات تخليط قطار البث أن تدعم التحديث الدوري لمفاتيح التجفير الضرورية.
- يتعين تكوين خوارزميات التخليط للتلفزيون القائم على بروتوكول الإنترنت باستخدام خوارزميات التجفير المتاحة والموحدة.

توصيات بشأن خوارزمية التخليط

- يُوَصَّى بأن تشتمل خوارزميات التخليط للتلفزيون القائم على بروتوكول الإنترنت على اعتلاج (إنتروبي) للمفاتيح كبير بدرجة كافية لتحقيق الحماية الفعالة للمحتوى من التحليل التجفيري.
- لا يوجد ما يحول دون منع معمارية التلفزيون القائم على بروتوكول الإنترنت عن دعم خوارزميات التخليط شائعة الاستعمال.
- يُوصى بأن تمتنع معمارية التلفزيون القائم على بروتوكول الإنترنت عن إعاقة دعم أنظمة التخليط المتعدد.
- يُوصى بأن تكون خوارزميات التخليط للتلفزيون القائم على بروتوكول الإنترنت قابلة للتنفيذ بكفاءة بالنسبة لكل من عمليتي تنفيذ العتاد و/أو البرمجيات.
- يوصى بأن تكون خوارزميات التخليط للتلفزيون القائم على بروتوكول الإنترنت قابلة للتوسع وطيلة الأمد، أي المعلمات التجفيرية (مثال طول المفتاح، فترات التجفير، إلخ) أو الأسلوب التجفيري (مثال ذلك التحكم في حمالة النداء CBC، وأسلوب التغذية راجعة الخرج OFB، وكتاب الشفرة الإلكتروني ECB، إلخ).

خيارات خوارزمية التخليط

- يمكن لخوارزميات التخليط للتلفزيون القائم على بروتوكول الإنترنت أن تطبق اختيارياً خوارزميات تجفيرية متفاوتة القوة على أنماط محتوى مختلفة.

3.6 متطلبات أمن الخدمة

تحدد هذه الفقرة المتطلبات التي تُعْنى فردياً أو مجتمعة بالخدمات وحماية الخدمة.

متطلبات المعمارية

- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم حماية الخدمة الوارد تعريفها في الفقرة 3.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت الامتناع عن دعم تحديث نظام حماية الخدمة والمحتوى أو تجديده في الجهاز المطرافي من جانب المخدم.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم تخويل واستيقان المستعمل النهائي (المشترك).
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت دعم آلية التشوير للجهاز المطرافي لاستخدام خوارزمية تخليط محددة استناداً إلى إطار موحد.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تكون لها القدرة على استعمال نظم موحدة لإدارة المفاتيح (مثال، رسالة التحكم في تخويل النفاذ، EMC ورسالة الإدارة لتخويل النفاذ EMM، وإبراق الإنترنت متعدد الوسائط MIKEY)حسبما تقتضيه قابلية التشغيل البيني.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم القدرة على تحديث وتمحيص نظام حماية الخدمة والمحتوى فيما يتعلق بخوارزميات التخليط للتلفزيون القائم على بروتوكول الإنترنت، وأي خوارزميات تخليط أخرى يختارها المُشَغِّلْ على جانب المخدم عبر الأسطح البينية لحماية الخدمة والمحتوى.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم آليات حماية الخدمة والمحتوى المستقلة عن أنساق محتوى بعينها.

- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم وجود آلية لتوفير حماية السلامة والاستيقان من منشأ البيانات وذلك للبيانات الشرحية الحساسة.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم وجود آلية لضمان تسليم الحقوق بأمان ومعلومات التحكم في النفاذ إلى المحتوى إلى الأجهزة المطرافية.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم التحكم في استخدام المحتوى (مثل تكرار العرض).
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت دعم مختلف أساليب تكرار العرض، مثال ذلك وضع حد أقصى لعدد مرات العرض، وسقف زمني على مرات العرض، وتقييد تسريع التشغيل إلى الأمام وإلى الخلف.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم آلية للتمكين من المحافظة على سرية رسالة التشوير بين مخدم حماية الخدمة والمحتوى وحماية الخدمة والمحتوى للعميل.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم آلية للتمكين من المحافظة على صحة رسالات التشوير بين مخدم حماية الخدمة والمحتوى وحماية الخدمة والمحتوى للعميل.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم سلامة رسائل التشوير بين مخدم حماية الخدمة والمحتوى وحماية الخدمة والمحتوى للعميل.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم وجود آلية لاسترجاع مَعْلمات حماية الخدمة والمحتوى بصورة آمنة (مثلاً التشكيل، الحالة) من الجهاز المطرافي.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم وجود آلية لتحديث مَعْلمات حماية الخدمة والمحتوى بصورة آمنة (مثلاً التشكيل) للجهاز المطرافي.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت إعاقة الدعم لتكوين القدرة على تشغيل وإبطال وظيفة تتبع المحتوى بصورة قابلة للبرمجة (مثلاً على أساس الوقت، والحدث، المحتوى، أو القناة).
- يتعين على مثل هذا النظام إذا استعمل نظاماً لإدارة المفاتيح أن يكون مصمماً لتحقيق قابلية التوسع، والاعتمادية وقابلية التشغيل البيني.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تعوق الدعم لإنشاء وتشغيل حلول حماية الخدمة المتعددة بدون استبدال أجزاء عتاد وذلك باستثناء الأجهزة القابلة للسحب (مثل مقبس قصر الخدمة على المشترك USB وبطاقات تعريف هوية المشترك SIM).
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت حجب الدعم عن وجود آلية تعريف هوية بالنسبة لحلول حماية الخدمة المتاحة القادرة على تلبية المتطلبات المحددة لحماية المحتوى ذات الصلة.
- يحظر على معمارية تلفزيون برتوكول الإنترنت حجب الدعم عن آلية استكشاف نظام حماية الخدمة والمحتوى بحيث يمكنها من تعزيز طريقة للاستكشاف، وتكييف نفسها معه حيثما يحتاج ذلك محتوى محددٌ لنظام حماية خدمة محدد.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت حجب الدعم عن وجود آلية لانتقاء نظام لحماية الخدمة والمحتوى من بين نظم SCP المتوافرة وذلك بدون أي استبدال للعتاد باستثناء الأجهزة القابلة للسَحْب.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت حجب الدعم عن التحميل الآمن لنظام حماية الخدمة والمحتوى (SCP). ويمكن لنظام الـــSCP الذي تم تحميله أن يعتمد اختيارياً على متطلبات حماية خدمة محددة.
- إذا تم نشر حماية الخدمة والمحتوى القابلة للتحميل، فيتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تجري عملية حماية السلامة والاستيقان من منشأ البيانات لنظام حماية الخدمة والمحتوى الذي تم تحميله.
- إذا دُعِمَ التحميل الآمن لبرنامج تطبيقي على جهاز مطرافي، فيتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن يُجري عملية حماية لسلامة واستيقان من مصدر البيانات بالنسبة للتطبيقات التي تم تحميلها عن بعد.

توصيات المعمارية

- يُوصى بأن تمكِّن معمارية التلفزيون القائم على بروتوكول الإنترنت (IPTV) من المحافظة على سرية المحتوى.
- يُوصى بأن تدعم معمارية IPTV خوارزميات التخليط المتعدد.
- يُوصى بأن تدعم معمارية IPTV القدرة على الاستيقان وتخويل المستعملين النهائيين الحصول على خدمات تقاسم المحتوى (مثال تصدير المحتوى وإعادة توزيع المحتوى).
- إذا استخدمت معمارية IPTV نظاماً لإدارة المفاتيح، فيُوصي بالنظر في وضع مخطط إدارة مفاتيح متدرج وذلك لتعزيز القابلية للتوسع.
- إذ استخدمت معمارية IPTV نظاماً لإدارة المفاتيح يستخدم بروتوكولاً لإدارة زمرات مفاتيح، فإنه يوصي باستخدام إدارة مفاتيح متدرجة وبديل عن خوارزمية إدارة المفاتيح وذلك لأجل دعم قابلية التوسع (scalability).
- إذا استخدمت معمارية التلفزيون القائم على بروتوكول الإنترنت نظاماً لإدارة المفاتيح يستعمل مفاتيح قصيرة الأجل، فيوصى بالنظر في اتباع إدارة مفاتيح متدرجة بحيث لا يقيد هذا النظام تقاطع مترجمي عناوين الشبكة (NAT traversal) ولا يقيد عرض النطاق تبادل المفاتيح.
- يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت نفس درجة الحماية على الأقل (لأغراض التحكم في النفاذ غير المخوّل) لمعلومات تتبع–المحتوى المطبقة على المحتوى المُتَتَبع النظير.
- يُوصى بأن تدعم معمارية IPTV الإرسال المُشتَرك للمحتوى ولمعلومات تَتَبُّعْ المحتوى مع الاحتفاظ في نفس الوقت بتزامن المحتوى ومعلومات تتبع المحتوى وذلك أثناء النقل.
- إذا استخدمت معمارية IPTV بنية تحتية للمفاتيح العمومية (PKI) لأجل الاستيقان من جهاز مطرافي أو من خدمة أو مورد محتوى، فإنه يُوصَى ببحث التدرج متعدد السويات للبنية التحتية للمفاتيح وذلك لأجل دعم قابلية التوسع، والاعتمادية وقابلية التشغيل البيني.
- إذا استعملت معمارية IPTV بنية تحتية للمفاتيح العمومية لخدمة التلفزيون القائم على بروتوكول الإنترنت، فإن استخدام نسق شهادة موحد متوافر عمومي، أو قائمة فسخ الشهادات، أو بروتوكول على الخط لحالة الشهادات هو أمر يوصى به.
- يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت التحميل الآمن لبرامج التطبيق إلى جهاز مطرافي.
- ويُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت وجود آلية لتقييد حقوق مشاهدة برامج معينة بالنسبة لمجموعات معينة من المشتركين (كوقف المشاهدة مثلاً عن سكان منطقة بعينها، إذْ يمكن مثلاً أن يفيد ذلك في حالة الأحداث الرياضية).

خيارات المعمارية

- تقديم خدمة التلفزيون القائم على بروتوكول الإنترنت القابلة للتوسع إلى المطراف المملوك للمستعمل والذي تختلف استبانته عن استبانة مطراف المستعمل، ويمكن لمعمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم اختيارياً قدرة مخطط قابل للتحويل الشفري الآمن وذلك على النحو المُعَرّف في الفقرة 3.

4.6 متطلبات أمن الشبكات

تحدد هذه الفقرة المتطلبات التي تتعامل إفرادياً أو جماعياً مع الشبكات أو حمايتها.

متطلبات المعمارية

- يتعين على معمارية IPTV أن تدعم قدرة التخفيف من حدة هجوم رفض تقديم الخدمة.

- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت IPTV أن تدعم توفير التدابير الأمنية لوقف حركة غير مشروعة أو غير مرغوبة.
- يتعين على معمارية تلفزيون IPTV أن تكون لديها المرونة في مواجهة الهجمات على قدرات البث المتعدد.
- تُوصَى المعمارية متعددة البث أن تدعم القدرة على الاستيقان من بيئة متعددة البث عامة أو سطحية (مثيل إلى مثيل).
- يتعين حماية وصلة الاتصال بين الأجهزة المطرافية داخل نطاق الشبكة المحلية من أجل تحقيق أمن المحتوى وذلك عند حمل محتوى أولي غير محمي، مدفوع الثمن من قِبَلْ المستهلك.
- يتعين لمعمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم عملية استيقان بوابة شبكة التسليم (DNG) من جانب وظيفة إدارة التلفزيون القائم على بروتوكول الإنترنت.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم استيقان وظيفة إدارة التلفزيون القائم على بروتوكول الإنترنت بواسطة بوابة شبكة التسليم.

توصيات المعمارية

- ولحماية الشبكة المحلية من النفاذ الخبيث أو غير المخوّل، يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت قدرات وظيفة بوابة شبكة التسليم (DNGF) لإقامة جدار نيران يمكن تشكيلها عن بُعد وبمستويات أمن متعددة وبوابات تطبيق ذات مستويات ملائمة.
- يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت قدرة إدارة التلفزيون القائم على بروتوكول الإنترنت على القيام عن بعد بتشكيل مترجم عنوان الشبكة (NAT) وكذلك توفير وظيفة حماية لبوابة شبكة التسليم (DNG) من الغزو.
- يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت القدرة على القيام عن بُعد بتشكيل مترجم عنوان الشبكة ووظيفة الحماية من الغزو لبوابة شبكة التسليم عن طريق وظيفة إدارة التلفزيون القائم على بروتوكول الإنترنت عن بُعد.
- يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت إدارة جهاز مطرافي عن بُعد في حالة حدوث دعم للإدارة عن بُعد.
- يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت استعمال معلومات وسم المحتوى وذلك من أجل التحكم في تسليم المحتوى.

5.6 متطلبات أمن المطاريف

تحدد هذه الفقرة المتطلبات التي تُعنَى إفرادياً أو جماعياً بالأجهزة المطرافية أو حمايتها.

متطلبات المعمارية

- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم معمارية الأجهزة المطرافية على النحو المُعرف في الفقرة 3.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم استيقان الجهاز المطرافي.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم مقاومة التلاعب المادي في الجهاز المطرافي.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم وسائل الاستكشاف في حالات حدوث التلاعب المادي في الجهاز المطرافي.
- إذا تم نشر حماية خدمة ومحتوى قابلة للتحميل، فيتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم التحميل والتركيب الآمنين لشفرة تشغيل حماية الخدمة والمحتوى في الأجهزة المطرافية.

- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم سبل إجراء العمليات الحرجة أمنياً في الجهاز المطرافي مثل إدارة المفاتيح وسَلْسَلْة الوسائط لإفشال إعادة عرض المحتوى وذلك في حالة تعطل وظيفي ذي صلة بالأمن و/أو اكتشاف تلاعب، أو أي دليل آخر على إساءة الاستخدام.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن توفر حماية مادية لتمكين العمليات والمكونات الحساسة أمنياً والضالعة في معالجة إرسال وتخزين المحتوى القيِّم في الجهاز المطرافي وذلك في حالة غياب الحماية المنطقية (مثل التجفير أو العلامات المائية للتسلسل). وتشمل هذه العمليات إزالة التخليط وإجراء تسلسل الوسائط.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تُسلِم بالحاجة إلى الحماية المادية (من سَبر أو التلاعب بنظام وظائف حماية الخدمة والمحتوى الموجودة في الجهاز المطرافي) بالنسبة لعمليات التمكين من تحقيق الأمن في الأجهزة المطرافية بما في ذلك إزالة التخليط و تسلسل الوسائط (تتبع المحتوى) والبيانات الحرجة الداعمة لتلك العمليات، وكذلك بالنسبة لجميع المكونات الضالعة في معالجة، وإرسال وخزن أي محتوى قيّمْ يفتقر إلى عمليات الحماية المنطقية كالتجفير أو العلامات المائية الخاصة بتتبع المحتوى.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تعوق الدعم إلى تبادل المحتوى بين الجهاز المطرافي وغيره من الأجهزة (المادية أو المنطقية)، شريطة أن تشتمل الاستعمالات الممنوحة لهذا المحتوى على التبادل.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم آلية تسمح للجهاز المطرافي بالاستيقان من مخدمات حماية الخدمة والمحتوى.
- يحظر على معمارية التلفزيون القائم على بروتوكول الإنترنت الامتناع عن دعم تحديد نظام حماية الخدمة والبروتوكول في الجهاز المطرافي.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم الخرج الرقمي أو التماثلي الذي ينبغي حمايته كما يجب من جانب عميل نظام حماية الخدمة والمحتوى من التخزين خارج الجهاز في حالة توفر خرج فيديوي/سمعي رقمي أو تماثلي على الجهاز المطرافي.

توصيات المعمارية

- يُوصى بأن توفر معمارية التلفزيون القائم على بروتوكول الإنترنت تصدير المحتوى في الأجهزة المطرافية بما يُمَكِن محتوى IPTV من النقل الآمن من مطراف تابع للتلفزيون القائم على بروتوكول الإنترنت إلى مطراف آخر مملوك للمستعمل الذي من حقه استعماله.

6.6 متطلبات أمن المشتركين

تحدد هذه الفقرة المتطلبات التي تتعامل إفرادياً أو جماعياً مع المشتركين والمستعملين النهائيين أو حمايتهم.

متطلبات المعمارية

- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم حماية خصوصية المستعمل على النحو الوارد تعريفه في الفقرة 3.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تسمح للمشترك بإقامة آلية تَحَكُمْ في النفاذ (باستخدام كلمة مرور مثلاً) لتقييد النفاذ إلى المحتوى و/أو الخدمات.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تكون قادرة على الإشارة إلى سبب حرمان المستعمل من النفاذ إلى المحتوى.
- يتعين على معمارية التلفزيون القائم على بروتوكول الإنترنت أن تدعم آلية تساعد المشترك على طلب تمديدات لحقوق الاستعمال المرتبطة بحالات معينة للمحتوى (مثل المزيد من عدد مرات العرض، وزيادة أوقات العرض).

- يُوصى بأن تسمح معمارية التلفزيون القائم على بروتوكول الإنترنت للمستعمل النهائي (على نحو ما تسمح له الحقوق) بتغيير، أي، باستبدال، جهاز مطرافي دون أن ينطوي ذلك في حد ذاته على النيل من حقوق استهلاك المحتوى.
- يُوصى بأن تدعم معمارية التلفزيون القائم على بروتوكول الإنترنت آلية لتحديد قيمة للبرامج حسب المحتوى.

ملاحظة – يمكن استعمال معلومات التحديد حسب القيمة في التحكم في النفاذ، مثال، التحكم الأبوي.

7 معمارية الأمن

تُعرِّف هذه الفقرة معمارية أمن التلفزيون القائم على بروتوكول الإنترنت من زاوية معمارية الأمن العامة، وهي معمارية لحماية المحتوى، ومعمارية لحماية الخدمة وكيانات وظيفية للأمن وذلك للوفاء بالاحتياجات الموصوفة في الفقرات السابقة.

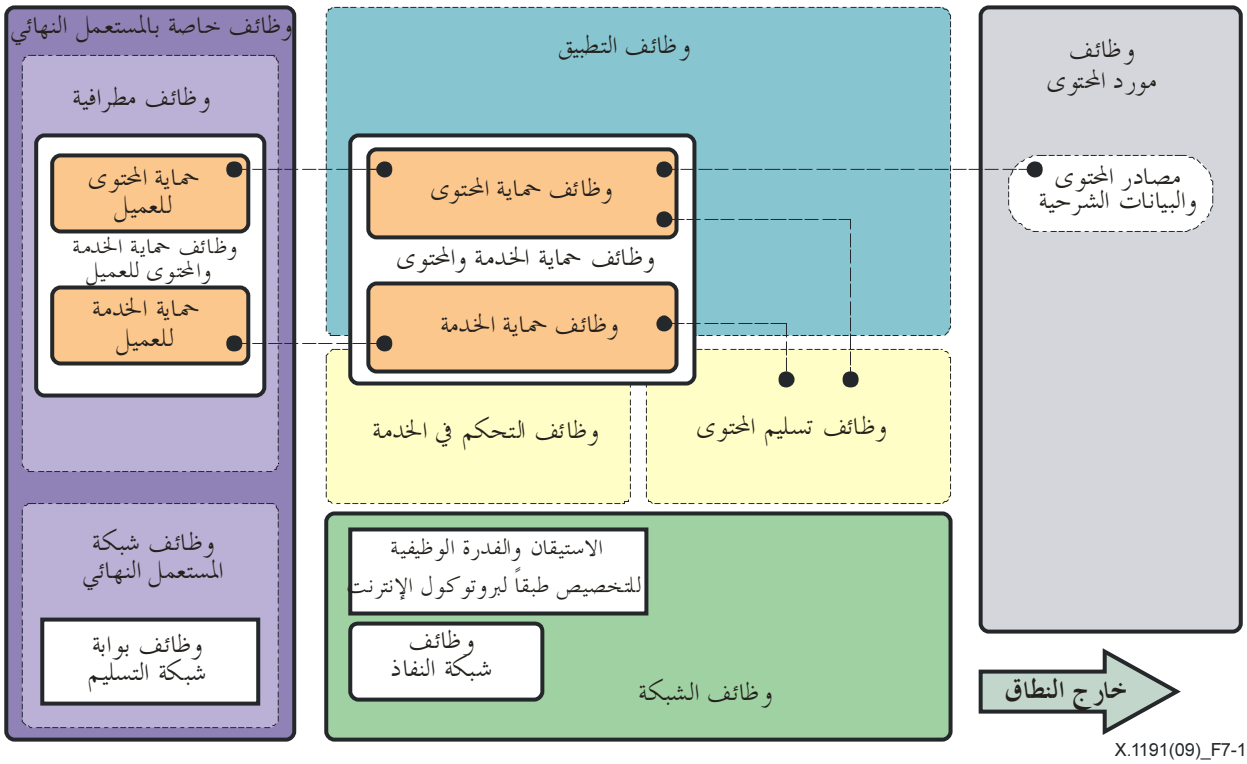
يفترض في معمارية أمن التلفزيون القائم على بروتوكول الإنترنت الموصوفة أدناه، بل ويقصد بها أن تُستْعمل في إطار الميادين الوظيفية للتلفزيون القائم على بروتوكول الإنترنت والإطار المعماري الوظيفي للتلفزيون القائم على بروتوكول الإنترنت على النحو المعرف في الفقرتين 6 و8 من التوصية [ITU-T Y.1910]، على التوالي.

1.7 معمارية الأمن العامة

يرد تصوير بياني لمعمارية عامة لأمن التلفزيون القائم على بروتوكول الإنترنت في الشكل 7-1 الوارد أدناه. وتقسم هذه المعمارية العامة إلى منطقتين أوليتين: إحداهما تُعتبر داخلة في نطاق المنظور القائم على أساس الغرض من هذه التوصية، والثانية تعتبر خارج هذا المنظور. وتشمل المنطقة الأولى المستعمل النهائي، ومورد الشبكة، وميادين موردي الخدمة، بينما تشمل المنطقة الثانية ميدان مورد المحتوى.

وفي المنطقة الثانية، تسيطر وتتقاطع جميع جوانب الأمن الموجودة في نطاق مورد الخدمة فيما بين موردي المحتوى وموردي الخدمة حيث تكون خاضعة لاتفاقات خاصة تبرم بين أصحاب المصلحة العاملين في تلك الميادين. ولذا، فهي تعتبر خارج نطاق هذه التوصية.

وعلى الرغم من أن ميدان مورد الخدمة، والتوصيل البيني بين ميداني مورد المحتوى ومورد الخدمة تعتبر خارج نطاق السياق الحالي، فإن ميدان مورد الخدمة يُدْرَج في الأشكال والأوصاف التالية لغرض الاكتمال. وبهذه الصورة فإن أي بيان يُدْلَى به في هذا السياق ويتعلق بهذه الميادين ينبغي أن يُعْتَبَر إعلامياً أو توضيحياً ليس إلا.



الملاحظة 1 – إن وظائف حماية المحتوى ووظائف حماية الخدمة في هذا الشكل هي أهم الأجزاء في معمارية أمن التلفزيون القائم على بروتوكول الإنترنت. ويمكن الإطلاع على المناقشات التفصيلية لهذه الوظائف في الشكل 7-2 (*معمارية حماية المحتوى*) والشكل 7-3 (*معمارية حماية الخدمة*).

الملاحظة 2 – حُذِفَ من الشكل بعض الوظائف والقدرات الوظيفية الخاصة بمعمارية التلفزيون القائم على بروتوكول الإنترنت، والتي ليس لها علاقة مباشرة بأمن التلفزيون القائم على بروتوكول الإنترنت وذلك بُغيَة تبسيطه.

الشكل 7-1 – المعمارية العامة لأمن التلفزيون القائم على بروتوكول الإنترنت

تنقسم المعمارية العامة للأمن بصورة تقريبية إلى أربع مجالات وظيفية بيانها كالتالي:

- وظائف مورد المحتوى (وهي خارج النطاق من الناحية التقنية)

ويفترض أن مورد (موردي) المحتوى يوفر النفاذ إلى المحتوى لموردي الخدمة الذين أنشأوا علاقة/علاقات مع مورد/موردي المحتوى. وفي بعض الحالات، يجوز أن يعمل مورد المحتوى نفسه كمورد خدمة؛ وفي هذه الحالة، تعتبر هذه العلاقة بينهما علاقة داخلية.

وبتزويد موردي الخدمة بالنفاذ إلى المحتوى، يمكن لمورد المحتوى أن يستعمل آليات معيارية أو خاصة للتحكم في، والتمكين من النفاذ إلى المحتوى؛ ولاحظ،مع ذلك، أن مثل هذه الآليات تعتبر خارج نطاق هذه الوثيقة ولا تخضع إلا لاتفاق خاص بين أصحاب المصلحة.

- وظائف حماية الخدمة والمحتوى (SCP) (تتداخل مع أجزاء معينة في وظائف التطبيق، ووظائف التحكم في الخدمة، ووظائف تسليم المحتوى)

تنهض وظائف حماية الخدمة والمحتوى بدور رئيسي في المعمارية العامة لأمن التلفزيون القائم على بروتوكول الإنترنت وبخاصة في ميدان مورد الخدمة. وبصورة محددة، تُمَكِن وظائف حماية الخدمة من حماية البنية التحتية للخدمة، وكذلك من التحكم في النفاذ إلى الخدمات والمحتوى الكائنة فيها. ومن ناحية أخرى، تُمَكِنْ وظائف حماية المحتوى من التحكم في استعمال الخدمات والمحتوى وفقاً للاستعمالات المرخص بها. وتنتشر الوظائف المحددة والقدرات الوظيفية لوظائف حماية الخدمة والمحتوى في ثلاث مجالات فرعية هي: وظائف التطبيق، وظائف التحكم في الخدمة ووظائف تسليم المحتوى.

ومورد الخدمات يكون مُلْزَماً بموجب الترخيص (التراخيص) الممنوح (الممنوحة) من موردي المحتوى بإتاحة المحتوى فقط عند توافر شروط معينة خاصة بالاستعمال، مثل، المشاهدة مرة واحدة ولكن بدون تسجيل، أو التسجيل مرة واحدة مع مرات مشاهدة متعددة، أو التسجيل مرة واحدة مع نقل حقوق التسجيل، إلخ. والهدف الأساسي لجوانب حماية المحتوى لوظائف حماية الخدمة والمحتوى (SCP) هو السماح لمورد خدمة بالوفاء بهذه الالتزامات على نحو يمكن التثبت منه موضوعياً.

والهدف الأولي لجوانب حماية الخدمة في وظائف حماية الخدمة والمحتوى هو الحيلولة دون النفاذ غير المخول إلى موارد الخدمة والمعلومات التي تعتبرها الكيانات في مختلف الميادين سرية: كالخدمة، والشبكة، والجهاز المطرافي والمستعمل النهائي (المشترك).

وثمة هدف ثانوي لجوانب حماية الخدمة في وظائف حماية الخدمة والمحتوى يتمثل في حماية البنية الأساسية للخدمات من التلف الناتج عن سوء الاستخدام العمدي و/أو العرضي للمورد.

ويرد تصوير للقدرات الوظيفية التفصيلية الخاصة بوظائف حماية المحتوى ووظائف حماية الخدمة في الشكل 7-2 *(معمارية حماية المحتوى)* والشكل 7-3 *(معمارية حماية الخدمة)* على التوالي.

- وظائف الشبكة

تنصب وظائف الأمن المعنية بميدان الشبكة على استيقان الكيانات، وتخويل النفاذ إلى الشبكة (الشبكات) التي يتم من خلالها تسليم خدمات التلفزيون القائم على بروتوكول الإنترنت. وثمة وظيفة ثانوية هي حماية سلامة الشبكة ذاتها -- مادياً وإلكترونياً، وتشغيلياً (مثال ذلك، عن طريق اكتشاف وإحباط هجمات رفض الخدمة على شبكة النفاذ أو شبكة الحمالة).

- وظائف المستعمل النهائي

تشمل جوانب الأمن التي تنطبق على المستعمل النهائي (المشترك) حماية سلامة الجهاز المطرافي الذي يعمل في منشآت المشتركين وكذلك حماية خصوصية المستعمل النهائي.

وفي ظروف معينة، يمكن اعتبار بوابة شبكة تسليم موجودة بين جهاز مطرافي وميدان شبكة أنها موجودة داخل نطاق ميدان المستعمل النهائي وتخضع لتدابير أمن المستعمل النهائي.

وفي النهاية، يوصى بتطبيق آليات السلامة integrity لضمان سلامة المحتوى الذي يتسلمه جهاز مطرافي ثم يعاد توزيعه بعد ذلك على أجهزة أخرى داخل أو خارج الشبكة المحلية. (وهذا ينتج عنه تداخل فيما بين جوانب أمن المستعمل النهائي وجوانب أمن المحتوى.)

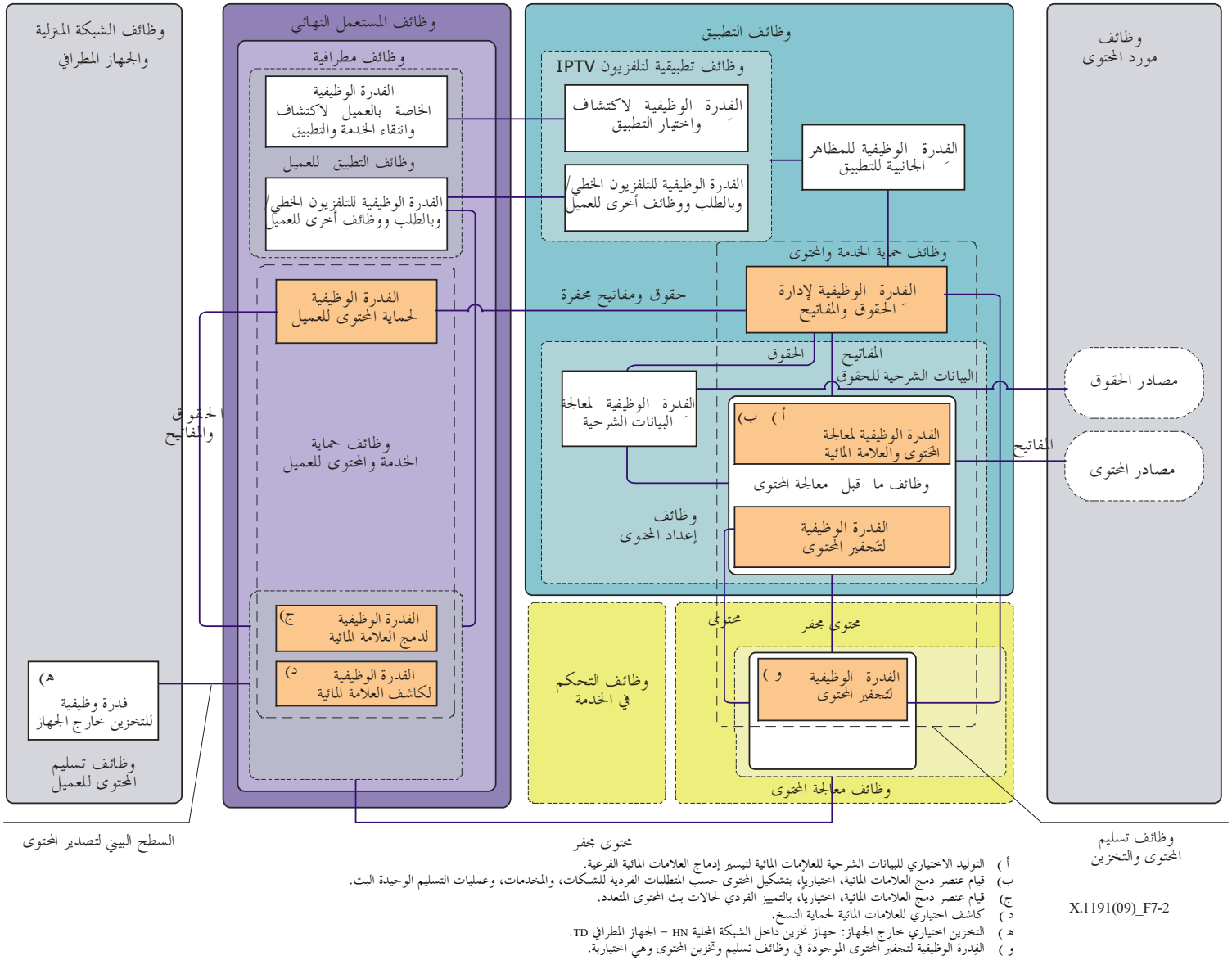
ويرد في الفقرة 1.4.7 أوصاف أكثر تفصيلاً للوظائف والقدرات الوظيفية المبينة في الشكل 7-1.

2.7 معمارية حماية المحتوى

يرد في هذا الشكل 7-2 الوارد أدناه تصوير لمعمارية حماية المحتوى للتلفزيون القائم على بروتوكول الإنترنت.

وتتمثل الوظيفة الرئيسية لمعمارية حماية المحتوى في رسم تدفق ومعالجة المعلومات الخاصة بحقوق استخدام المحتوى والمعلومات اللازمة لإدارة وتيسير مثل هذه الحقوق.

إن حقوق استخدام المحتوى تنشأ، في نهاية المطاف، عند مورد (موردي) المحتوى؛ ولاحظ، مع ذلك، أن مثل هذه الحقوق يمكن أن تُعَدَّل (بالتضييق أو التوسيع مثلاً) من جانب مورد (موردي) الخدمة وذلك وفقاً لاتفاقه (لاتفاقاتهم) مع موردي المحتوى وسياسات التشغيل والأعمال.



أ) التوليد الاختياري للبيانات الشرحية للعلامات المائية لتيسير إدماج العلامات المائية الفرعية.
ب) قيام عنصر دمج العلامات المائية، اختيارياً، بتشكيل المحتوى حسب المتطلبات الفردية للشبكات، والمخدمات، وعمليات التسليم الوحيدة البث.
ج) قيام عنصر دمج العلامات المائية، اختيارياً، بالتمييز الفردي لحالات بث المحتوى المتعدد.
د) كاشف اختياري للعلامات المائية لحماية النسخ.
ه) التخزين اختياري خارج الجهاز: جهاز تخزين داخل الشبكة المحلية HN – الجهاز المطرافي TD.
و) الفدرة الوظيفية لتجفير المحتوى الموجودة في وظائف تسليم وتخزين المحتوى وهي اختيارية.

ملاحظة – تتكون الفدرات الوظيفية لحماية المحتوى في هذا الشكل من وظائف حماية المحتوى ووظائف حماية المحتوى للعميل.

الشكل 7-2 – معمارية حماية محتوى التلفزيون القائم على بروتوكول الإنترنت

تتألف معمارية حماية المحتوى المبينة أعلاه من وظائف تقع بالدرجة الأولى داخل منطقتين وظيفيتين هما:

- وظائف حماية الخدمة والمحتوى (تتداخل مع وظائف التطبيق ووظائف تسليم المحتوى)

ويتم الحصول على المحتوى والحقوق المرتبطة به من موردي المحتوى وتكون مجمعة، ومعالجة لتسليمها إلى المستعمل النهائي، حيث تدار العملية الكلية بعدة وظائف مثل وظائف إعداد المحتوى باستخدام بيانات تصف حقوق المستعمل النهائي والشروط ذات الصلة.

ويتم تنظيم معلومات المحتوى، والحقوق، والمفاتيح (المستعملة لمنح النفاذ إلى المحتوى والتمكين من استعماله) في شكل يتناسب مع التطبيق المحدد مثال مشاهدة التلفزيون الخطي. ويتم تسليم معلومات الحقوق والمفاتيح إلى الفِدرة الوظيفية للعميل الخاصة بحماية المحتوى في الجهاز المطرافي كحق مكتسب (مثال رسالة الإدارة لتخويل النفاذ EMM) وذلك من جانب الفِدرة الوظيفية لإدارة الحقوق والمفاتيح؛ وتتم معالجة المحتوى لإدخال البيانات الشرحية لتتبع المحتوى (وضع العلامات المائية مثلاً) وذلك كخيار ثم يُجَفَّر بعد ذلك داخل وظائف إعداد المحتوى قبل التسليم. وفي بعض الحالات، (كحالة خدمات بروتوكول الإنترنت بالوقت الفعلي)، يمكن تجفير المحتوى بواسطة وظائف تسليم المحتوى وذلك كخيار.

وفي سياق معمارية محتوى التلفزيون القائم على بروتوكول الإنترنت (على عكس معمارية حماية خدمة التلفزيون القائم على بروتوكول الإنترنت التي يرد وصفها في موضع لاحق) يسلط الضوء على الإدارة، والمعالجة، وتسليم الحقوق والمفاتيح، وذلك على عكس تجفير هذه المعلومات أو المحتوى طبقاً لما تقتضيه هذه الحقوق.

- وظائف المستعمل النهائي

والوظائف المطرافية التي تعمل في ميدان المستعمل النهائي مسؤولة عن إنفاذ قواعد استعمال المحتوى المصاحب لمعلومات الحقوق (التي تعرف أيضاً بالبيانات الشرحية لحماية المحتوى). ويفسر هذا الكيان الوظيفي حقوق ومفاتيح المحتوى التي يتم الحصول عليها من الفِدرة الوظيفية لإدارة الحقوق والمفاتيح، ثم تأخذ بهذا التفسير للتحكم في الكيفية التي تتم بها معالجة المحتوى قبل إخراجه إلى المستعمل إما من خلال أجهزة عرض متكاملة (مثل نظام أداء للعرض أو للاستماع) أو من خلال توصيلات بينية مادية مع الأجهزة الخارجية.

أما في تلك الحالات التي يرسل فيها الجهاز المطرافي محتوى محمياً إلى جهاز خارجي (مثل خَرْجْ العرض)، فيجوز ترجمة حقوق المحتوى إلى أشكال أخرى، أما المحتوى الذي ينطبق عليه هذا الاستعمال فيجوز مواصلة معالجته لإدخال معلومات تتبع المحتوى في جانب العميل (مثل العلامات المائية) كخيار أو كمحتوى معاد تجفيره لتنفيذ التحكم في النفاذ في اتجاه المقصد.

وترد في الفقرة 4.7 أوصاف أكثر تفصيلاً للفدرات المعمارية. المبينة في الشكل 7-2.

وفي الشكل 7-2، يكون السطح البيني لتصدير المحتوى سطحاً بينياً منطقياً يربط بين الجهاز المطرافي للتلفزيون القائم على بروتوكول الإنترنت والجهاز المطرافي للشبكة المنزلية.ويجوز للجهاز المطرافي للشبكة المنزلية أن يستهلك المحتوى ذاته أو أن يصدر المحتوى إلى أجهزة مطرافية أخرى تابعة للشبكة المنزلية. ويجوز لوظائف تسليم المحتوى للعميل أن توائم الوسم الأمني المناظر لضمان قصر استهلاك وتصدير المحتوى على نظام الجهاز المطرافي للشبكة المنزلية المرخص له.

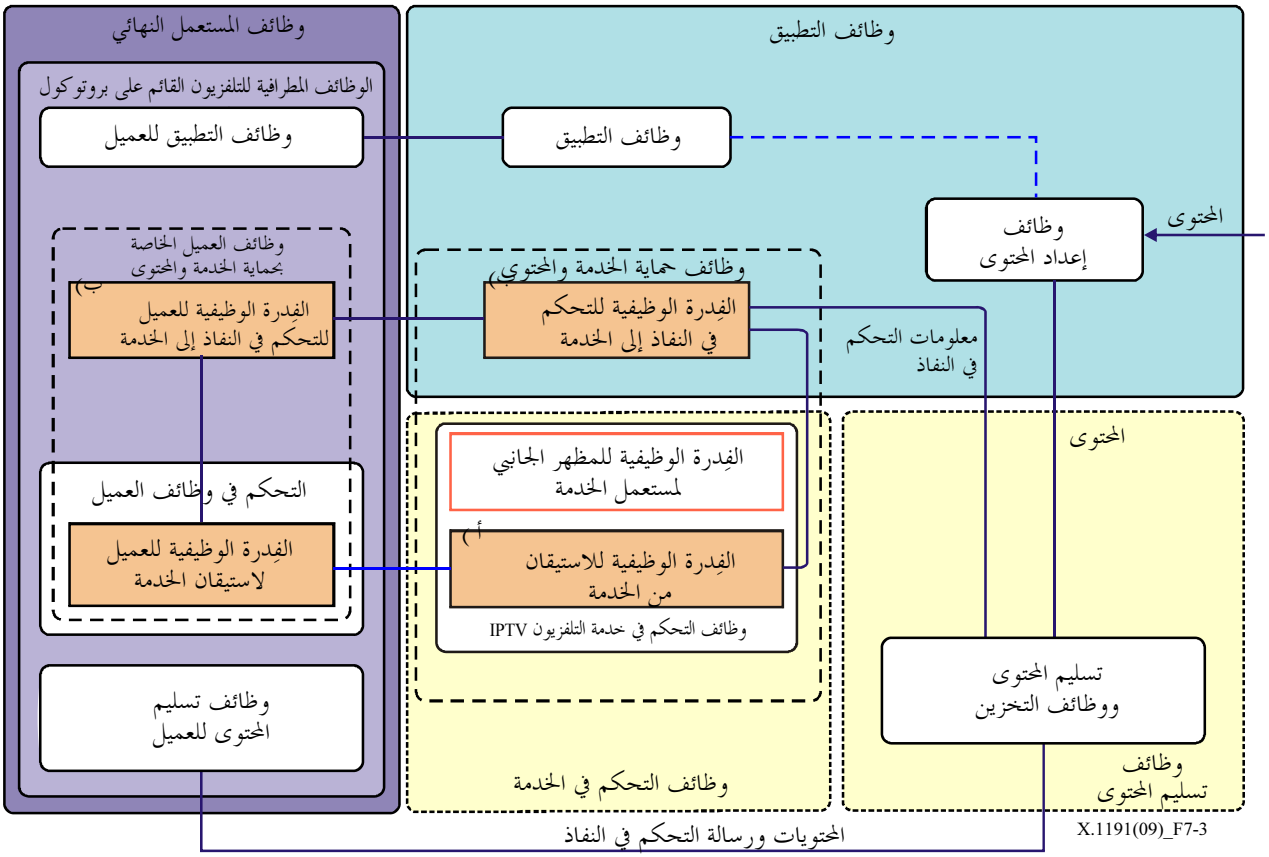
3.7 معمارية حماية الخدمة

بالنسبة للخدمات المدارة التي تحتوي على محتوى مَحْم، فإن الحالة النموذجية لذلك تحدث عندما يكون من الضروري الاستيقان من المستعمل النهائي (المشترك) والجهاز المطرافي وتخويلها عقب استيقان ناجح بالنفاذ إلى الخدمة (الخدمات) والمحتوى الكائن بها.

وتبعاً للظروف، يجوز إجراء وظيفتي الاستيقان والتخويل بصورة منفصلة على الجهاز المطرافي والمستعمل (المستعملين) النهائي(النهائيين). وفي حالات أخرى، قد تحتاج الأجهزة الإضافية الموجودة لدى منشآت المستعمل النهائي مثل بوابة شبكة التسليم وغيرها من أجهزة المستعمل النهائي، إلى الاستيقان قبل تخويل النفاذ إلى الخدمة.

ويمكن استخدام توليفة الاستيقان والتخويل للتحكم في النفاذ إلى كل من خدمة التلفزيون القائم على بروتوكول الإنترنت وإلى الجهاز المطرافي لأغراض الاستحواذ على الخدمة والمحتوى وذلك قبل الاستعمال.

ويرد وصف لمعمارية حماية الخدمة للتلفزيون القائم على بروتوكول الإنترنت IPTV في الشكل 7-3 أدناه.



أ) الاستيقان: وهو يحدد اسم المشترك ومعرّف هويته مع الامتياز المخصص.
ب) التحكم في النفاذ إلى الخدمة: لحماية الخدمة من التصرفات غير القانونية.

ملاحظة – تتألف الفدرات الوظيفية لحماية الخدمة في هذا الشكل من وظائف حماية الخدمة ووظائف حماية الخدمة بالنسبة العميل.

الشكل 7-3 – معمارية حماية خدمة التلفزيون القائم على بروتوكول الإنترنت

تشمل الوظائف الأساسية لمعمارية حماية خدمة التلفزيون القائم على بروتوكول الإنترنت ما يلي:

- استيقان المشترك والجهاز المطرافي

وهذه الوظيفة مسؤولة عن استيقان المشتركين والأجهزة المطرافية.

– الاستيقان من المشترك: وهو عملية التحقق من حقيقة المشترك.

– استيقان الجهاز المطرافي: وهو عملية التحقق من حقيقة الجهاز المطرافي.

وفي الحالات التي تستخدم فيها الشهادات الأساسية للتوصية X.509 كمسوغات للاستيقان، فيتعين وجود وظيفة إلغاء.

- استيقان المخدم

– توجد في أي جهاز مطرافي وظيفة استيقان المخدم وذلك من أجل الاستيقان المتبادل.

- التحكم في النفاذ إلى الخدمة

– وهي وظيفة تقييد استحواذ الخدمات أو النفاذ إليها من جانب مستعملين مُخَوَّلين باستعمال آليات أمن كالتخليط والتجفير.

وترد في الفقرة 4.7 أوصاف أكثر تفصيلاً للفدرات المعمارية المبينة في الشكل 7-3.

4.7 وصف للوظائف والقدرات الوظيفية في معماريات أمن التلفزيون القائم على بروتوكول الإنترنت

تقدم هذه الفقرة تفاصيل أكثر وصفية للوظائف والقدرات الوظيفية المرسومة في النماذج المعمارية الموجودة في الفقرة 1.7 (معمارية الأمن العامة)، والفقرة 2.7 (معمارية حماية المحتوى)، والفقرة 3.7 (معمارية حماية الخدمة) عاليه. ولا يرد تعريف هذه الوظائف والقدرات الوظيفية إلا بأوصاف عامة وتنقسم إلى ثلاثة أجزاء مناظرة لكل فقرة من هذه الفقرات الثلاث.

1.4.7 وظائف المعمارية العامة والقدرات الوظيفية

وظائف شبكة النفاذ: وهي تُعنَى بتحصيل وتجميع حركة التحكم والبيانات التي تنشأ في الشبكة (الشبكات)؛ وتمكين جودة الخدمة/جودة الخبرة بما في ذلك إدارة الدارئات، والاصطفاف الانتظاري، ووضع الجداول، وترشيح الرزم وتصنيف الحركة، والوسم، الضبط الأمني وتحديد شكل الحركة.

الملاحظة 1 – هذه الوظائف مستقلة عن وظيفتي حماية الخدمة والمحتوى وذلك من زاوية حماية خدمة ومحتوى التلفزيون القائم على بروتوكول الإنترنت.

وظائف التطبيق: وهي مقسمة بين جانب المخدم (مورد الخدمة) وجانب العميل (منشأة المستعمل النهائي)، وتتألف من مكونات وظيفية تُعِدْ، وتُولِد، وتَستقبل، وتُعالِج تطبيقات خدمة على مستوى التلفزيون القائم على بروتوكول الإنترنت مثال ذلك التلفزيون الخطي، والفَيديو حسب الطلب VOD، والمحتوى ذي الصلة، مثال معلومات النفاذ والتطبيقات التفاعلية إلخ.

الاستيقان والقِدرة الوظيفية للتخصيص حسب بروتوكول الإنترنت: وهي تزود بالعنصر الوظيفي لاستيقان القِدرة الوظيفية لبوابة شبكة التسليم المتصلة بوظائف الشبكة وكذلك توزيع عنوان بروتوكول الإنترنت IP على الوظائف المطرافية للتلفزيون القائم على بروتوكول الإنترنت.

وظائف حماية المحتوى: تزود بالآليات التي تساعد على إنفاذ سياسات استعمال المحتوى بما فيها التجميع، والتوزيع، وإدارة الحقوق والمفاتيح، والتوليد الاختياري ودمج معلومات تتبع المحتوى (مثال ذلك العلامات المائية)، وتجفير المحتوى (تحت إشراف وظائف حماية المحتوى).

الملاحظة 2 – وثَّمة مناقشة أوسع للقدرات الوظيفية المحددة التي تشكل وظائف حماية المحتوى في الفقرتين 2.7 و4.7.

وظائف حماية المحتوى للعميل: تتفاعل مع وظائف خدمة المحتوى في جانب المخدم لإنفاذ سياسات استعمال المحتوى.

وظائف مورد المحتوى: تقوم بتسليم المحتوى وحقوق المحتوى والبيانات الشرحية للمفاتيح إلى موردي الخدمة.

وظائف بوابة شبكة التسليم: وهي توفر التوصيلية بين الجهاز المطرافي وشبكة التسليم؛ وتقوم بإدارة التوصيلية المحلية لبروتوكول الإنترنت (منشآت المستعمل النهائي)، والحصول على عنوان (عناوين) بروتوكول الإنترنت، وتشكيل الجهاز المطرافي طبقاً لبروتوكول الإنترنت.

الملاحظة 3 – هذه الوظائف مستقلة عن وظائف حماية الخدمة والمحتوى من وجهة نظر حماية خدمة ومحتوى التلفزيون القائم على بروتوكول الإنترنت.

وظائف حماية الخدمة: وهي توفر آليات للقيام بالاستيقان والتخويل لخدمات ومحتوى التلفزيون القائم على بروتوكول الإنترنت الموجودة فيها والتحكم في النفاذ إليها، بما في ذلك التحكم في، والتنفيذ المباشر لإشارة التحكم وتجفير تبادل المحتوى إما بصورة مستقلة أو جنباً إلى جنب مع وظائف حماية المحتوى.

الملاحظة 4 – وهذه الوظائف مستقلة عن وظائف حماية الخدمة والمحتوى من وجهة نظر حماية الخدمة والمحتوى للتلفزيون القائم على بروتوكول الإنترنت.

الملاحظة 5 – ثمة مزيد من النقاش حول القدرات الوظيفية المحددة التي تشكل وظائف حماية الخدمة في الفقرة 3.7 والفقرة 3.4.7.

وظائف حماية الخدمة للعميل: وهي تتفاعل مع وظائف حماية الخدمة على جانب المخدم لأجل القيام بالتحكم في النفاذ إلى الخدمة ووظائف الحماية الأخرى.

الوظائف المطرافية: تزود حماية الخدمة وعملاء حماية المحتوى بما يلزم لفك تجفير سياسات استعمال الخدمة والمحتوى وإنفاذها طبقاً للبيانات الشرحية لحقوق الاستعمال؛ والقيام بتجفير طبقة الوصلة وترجمة حماية الخدمة والمحتوى (تبادل) حسبما يتطلبه المزيد من النقل في اتجاه المقصد لخرج المحتوى أو إعادة توزيعه، وتخزين المحتوى الداخلي (أو الخارجي) بما في ذلك دعم خطوط معالجة الوسائط بصورة آمنة (ومانعة للتلاعب) وتخزين السر (المفتاح مثلاً) المحلي، وقابلية تحديد برمجيات الأمن، واستيقان وتحقيق الأصول البرمجية المحملة وحماية بيانات المستعمل التي يتم تخزينها وتبادلها محلياً مع عدم الإخلال باعتبارات خصوصية المستعمل النهائي.

2.4.7 وظائف معمارية حماية المحتوى والقدرات الوظيفية

وظائف التطبيق للعميل: نقطة أساسية للتنسيق والتحكم في التفاعل بين المستعمل النهائي والخدمة (الخدمات) التي تقدمها وظائف تطبيق التلفزيون القائم على بروتوكول الإنترنت؛ للتطبيقات المعيارية مثل مشاهدة التلفزيون الخطي. وتوفير السطح البيني الأساسي للمستعمل وأسلوب تشغيل يحصل المستعمل النهائي من خلاله على خدمة.

- **الفِدرة الوظيفية للعميل الخاصة باكتشاف التطبيق واختياره:** تسمح للمستعمل النهائي و/أو الجهاز المطرافي أن يستكشف وجود، ويختار التطبيقات وخدمات التطبيق المتوافرة من مورد (موردي) الخدمة.

وظائف تطبيق التلفزيون القائم على بروتوكول الإنترنت: كيانات منطقية تجسد نقطة المنشأ لبعض خدمات تلفزيون IPTV مثل التلفزيون الخطي، والفيديو حسب الطلب، إلخ. وهي مسؤولة عن تنسيق جميع مرافق مورد الخدمة للتمكين من إيجاد خدمة (بعض الخدمات) تشغيلياً.

- **الفِدرة الوظيفية لاكتشاف التطبيق واختياره:** تتفاعل مع الفِدرة الوظيفية للعميل والخاصة باكتشاف التطبيق واختياره الموجودة أعلاه وذلك لمساعدة المستعمل النهائي و/أو الجهاز المطرافي على اكتشاف وجود التطبيقات وخدمات التطبيق واختيارها.

الفِدرة الوظيفية للمظهر الجانبي للتطبيق: وهي تقوم بخزن وإدارة معلومات التشكيل بشأن التطبيقات والخدمات ذات الطبيعة الكلية والمحددة للمستعمل النهائي (المشترك)؛ والتي تستخدم عادة للسماح لمخدم (مخدمات) التطبيق بتجهيز الخدمات والمحتوى للمستعمل النهائي حسب المواصفات المطلوبة، وهي تتفاعل غالباً مع مختلف الأنظمة المحاسبية أو تنفذها (داخلياً).

وظائف إعداد المحتوى: تقوم بالعديد من أنواع المعالجة المسبقة للمحتوى قبل التسليم كتحليل لتتبع المحتوى (مثال ذلك العلامات المائية) وتوليد البيانات الشرحية، وتعدد إرسال المحتوى والبيانات الشرحية للمحتوى، وتجفير المحتوى.

- **الفِدرة الوظيفية لمعالجة المحتوى والعلامة المائية:** خطوة/خطوات المعالجة الاختيارية التي تقوم بتحليل المحتوى لإنتاج البيانات الشرحية لتتبع المحتوى (مثال العلامة المائية) وذلك لاستعمالها في المعالجة الفرعية التالية، وبصفة خاصة في عملية التحديد الإفرادي (التي يتم التعرف عليها بواسطة معلومات من المصدر المصاحب) مثل البيانات الشرحية.
- **الفِدرة الوظيفية لمعالجة البيانات الشرحية:** وهي تدير وتعالج البيانات الشرحية ذات الصلة بالبرامج، وكذلك المعلومات عن حقوق الاستعمال التي يقدمها مورد المحتوى.
- **الفِدرة الوظيفية لتجفير المحتوى:** تقوم بتجفير (تخليط) المحتوى المحمي وذلك لتيسير التحكم في النفاذ وسرية مثل هذا المحتوى أثناء عملية تسليم المحتوى، ويمكن أن يُجَفَرْ المحتوى في الوقت الفعلي أو خارج الخط المُجَفّر سَلَفاً (ويمكن لتجفير المحتوى أن يقوم اختيارياً بدعم التحويل الشفري الآمن بدون فك التجفير).

الملاحظة 1 – يمكن أن يُنَفّذْ تجفير المحتوى في وظائف إعداد المحتوى داخل نطاق طبقة التطبيق. ويمكن تنفيذ تجفير المحتوى هذا في بعض الحالات في وظائف تسليم المحتوى وذلك كخيار.

الفِدرة الوظيفية لإدارة الحقوق والمفاتيح: تُوجِدْ ترابطاً بين الحقوق والمفاتيح وبين المحتوى وتدير توزيعهما على الفِدرة الوظيفية لحماية المحتوى للعميل في الجهاز المطرافي.

الفِدرة الوظيفية لحماية المحتوى للعميل: وهي تحصل على، أو تتلقى الحقوق والمفاتيح مستعملة هذه المعلومات للتحكم في تجفير المحتوى وإنفاذ قواعد الاستعمال، وتحتاج هذه الفِدرة الوظيفية أن تكون مقاوِمة للتلاعب.

وظائف تسليم المحتوى: تقوم بوظائف التخزين المؤقت والتخزين الدائم وتسليم المحتوى بناء على طلب من وظائف المستعمل النهائي؛ ويمكن لوظائف تسليم المحتوى القيام اختيارياً بمعالجة المحتوى (مثل التشفير، والتجفير).

وظائف تسليم المحتوى للعميل: وهي مسؤولة عن تَسَلُّمْ المحتوى في الوظائف المطرافية للتلفزيون القائم على بروتوكول الإنترنت، وهي تقوم بفك تجفير وسائط المحتوى، وإزالة تعدد الإرسال، وفك التشفير وما يتلو ذلك من معالجة للعرض والتخزين بشأن المحتوى (وهذه الوظائف تحتاج أيضاً لأن تكون لديها القدرة على مقاومة التلاعب).

- **الفِدرة الوظيفية للكشف عن العلامة المائية**: في حالة وجود هذه الفِدرة فإنها تقوم بالكشف عن استعمال علامة (علامات) مائية في المحتوى الوارد من مورد (موردي) الخدمة وذلك للتحقق من، أو لتنفيذ قواعد استعمال المحتوى المرغوب فيه داخل الجهاز المطرافي أو الأسطح البينية الفرعية للجهاز المطرافي.
- **الفِدرة الوظيفية لدمج العلامة المائية**: وفي حالة وجودها فإنها تقوم بالتمييز الفردي لطبيعة المحتوى وذلك للعرض ولما يتلو ذلك من تخزين أو إعادة توزيع.

مصادر الحقوق: إنشاء بيانات شرحية للمحتوى تُعْنَى بحقوق استعمال المحتوى.

مصادر المحتوى: إنشاء المحتوى لأجل تجميعه، ومعالجته، ثم تسليمه بعد ذلك إلى المستعملين النهائيين عن طريق تطبيقات الخدمة مثل التلفزيون الخطي، والفيديو حسب الطلب، إلخ.

الفِدرة الوظيفية للتخزين خارج الجهاز: آليات لتخزين المحتوى بعد تَسَلمه، وهي آليات توجد مادياً خارج الجهاز المطرافي ولا يخضع تخزينها وإدارتها للجهاز المطرافي.

الملاحظة 2 – في حالة وجود تخزين خارجي، ويكون استعماله خاضعاً لتحكم الجهاز المطرافي في جميع الأوقات، عندئذٍ يجوز اعتباره تخزيناً داخل الجهاز عبر سطح بيني مُخَول ومحمي تبعاً لقواعد التطابق والمتانة المطبقة للجهاز المطرافي.

3.4.7 وظائف معمارية حماية الخدمة والفدرات الوظيفية

الفِدرة الوظيفية للتحكم في النفاذ إلى الخدمة: وهي مسؤولة في المقام الأول عن التحكم في النفاذ إلى الخدمة، وتستخدم آليات للأمن كآلية التخليط والتجفير التي تستخدمها هذه الفِدرة الوظيفية لمنع المستعملين من النفاذ إلى الخدمات أو حيازتها بدون إذن.

الفِدرة الوظيفية للتحكم في نفاذ العميل إلى الخدمة: وهي تقوم بمهام متعلقة بحماية الخدمة بشأن العميل على نحو ما تُعرِفه الفِدرة الوظيفية للتحكم في النفاذ إلى الخدمة على جانب المخدم.

الفِدرة الوظيفية لاستيقان الخدمة: وهي تقوم بالاستيقان للتأكد من حقيقة المستعمل و/أو الجهاز المطرافي، وهي تلبي أيضاً طلبات الاستيقان التي ترد من الجهاز المطرافي للتحقق من حقيقة المخدم.

الفِدرة الوظيفية للعميل لاستيقان الخدمة: وبالإضافة إلى القيام بالمهام المرتبطة باستيقان العميل من الواجبات ذات الصلة في جانب العميل فهي تشمل كذلك وظيفة التحقق من حقيقة حماية الخدمة للاستيقان المتبادل في جانب المخدم.

8 آليات الأمن

لا تقدم هذه التوصية أي تعريف محدد لآلية أو حلا للأمن، ولكنها تقوم بدلاً من ذلك بوصف آليات أمن معينة وصفاً عاماً يمكن بحثه لأغراض تعريف أو تنفيذ الآليات التي تتناول متطلبات الأمن، والكيانات الوظيفية المعمارية للأمن، والتهديدات الأمنية.

أما مجموعة آليات الأمن الموصوفة أدناه فلا تتناول بصورة شاملة جميع المتطلبات الأمنية الموثقة أعلاه.

1.8 آليات الأمن المعنية بحماية المحتوى

تشمل آليات أمن المحتوى مجموعة وظائف تعمل فيما بين مصادر المحتوى والأجهزة المطرافية لتأمين إمكانية توزيع (أو إرسال) المحتوى بأمان من جانب شبكة ما وإمكان استحواذه، استهلاكه، تصديره، تخزينه، وإعادة توزيعه (أو إعادة إرساله) بأمان بواسطة مستعمل نهائي. ويمكن تطبيق آليات أمن المحتوى على توزيع المحتوى، واستحواذ المحتوى، استهلاك المحتوى، وتخزين المحتوى، تصدير المحتوى، وإعادة توزيع المحتوى. ويمكن استعمال الآليات التالية للوفاء بمتطلبات حماية محتوى وخدمة التلفزيون القائم على بروتوكول الإنترنت (وكلها اختيارية):

1.1.8 تجفير المحتوى

وفي كثير من الحالات، يجوز تجفير المحتويات للحيلولة دون استعمالها استعمالاً غير مشروع أثناء التسليم.

2.1.8 تتبع المحتوى وتعريف هويته

يستخدم تتبع المحتوى في التعرف على هوية، وتتبع منشأ (مصدر) المحتوى و/أو الطرف المسؤول (المستعمل النهائي مثلاً) وذلك لتيسير الاستقصاء التالي في حالة حدوث نفاذ واستعمال غير مخول للمحتوى.

ويمكن إرفاق معلومات تتبع المحتوى بالمحتوى سواء كبيانات شرحية أو كعلامة مائية قضائية. وتصمم العلامات المائية الخاصة بتتبع المحتوى عادة بحيث تكون متينة وغير مدركة وذلك لتوقي إزالتها عمداً أو عن غير وعي.

ويوصَى بتيسير التعرف على هوية المحتوى بواسطة تكنولوجيا التوقيع الفيديوي.

3.1.8 وضع العلامات المائية

يشير وضع العلامات المائية إلى عملية إضافة معلومات إلى المحتوى عن طريق تغيير ملامح معينة من ملامح المحتوى. ويسمى حقل الدراسة هذا بستر الرسائل داخل وسط ما (*steganography*).

ويفضل استخدام العلامات المائية في الكثير من التطبيقات وذلك بسبب صعوبة إزالة هذه المعلومات من المحتوى. ففي خدمة التلفزيون القائم على بروتوكول الإنترنت، قد يشير وضع العلامات المائية إلى إدراج معلومات مخبوءة مباشرة في فيديو أو في قطار سَمْعِي لمحتوى معدد إرساله. والوضع الأمثل أن، تكون العلامات المائية غير منظورة و/أو غير مسموعة لحواس الإنسان ولكنها تنجح في مقاومة التحول فيما بين أنساق الوسائط.

4.1.8 وسم المحتوى

ووسم المحتوى هو عملية إدخال أو جعل البيانات الشرحية مصاحبة للمحتوى، وهو يصف طبيعة المحتوى وكذلك جوانب المحتوى وخصائص هذا المحتوى. ويمكن للمحتوى الموسوم بهذه البيانات الشرحية أن يُفْرَز، أو يُرَشَحْ أو يوضع في فئات وذلك بصورة أكثر يسراً بواسطة أجهزة وسيطة في سلسلة توصيل المحتوى.

وقد تتطلب بعض المناطق، أو الإدارات أو عمليات الانتشار المحددة للتلفزيون القائم على بروتوكول الإنترنت وجود أنماط معينة من علامات وسم المحتوى مثل تحديد أهمية المعلومات للسماح بوجود درجة ما من تحكم المستعمل النهائي (المشترك) في النفاذ إلى المحتوى الذي يُعتبر غير مناسب أو ضار.

5.1.8 مخطط للتحويل الشفري الآمن

يشير مخطط التحويل الشفري الآمن (STS) إلى نوع من مخططات الأمن التي تُمَكِنْ عقدة الشبكة الوسيطة من إجراء التحويل الشفري بدون إزالة التجفير مع المحافظة في نفس الوقت على الأمن من طرف – إلى طرف. ويمكن تحقيق هذا المخطط عن طريق الجمع بين التشفير القابل للتوسع، والتجفير التدريجي والترزيم.

وبالنسبة لمخطط التحويل الشفري الآمن توجد هناك ثلاثة كيانات: المرسل، وعقدة الشبكة الوسيطة والمستعمل الذي يوجد لديه مطراف تابع للتلفزيون القائم على بروتوكول الإنترنت. ويؤدي المُرسِلْ وظيفة التحويل الشفري الآمن لإنتاج رزم مجفرة

قابلة للتوسع من الفيديو، ويضيف الرأسية غير المُجَفْرة لإرسال المعلومات. وتقوم عقدة الشبكة الوسيطة بقراءة الرأسية غير المجفرة، وتستعمل هذه المعلومات لتقويم أو لاستبعاد الرزم الكافية طبقاً لعملية التحويل الشفري المرغوبة، ويقوم مطراف التلفزيون القائم على بروتوكول الإنترنت بإزالة تشفير الرزم المجفرة، وإزالة تشفير الرزمة ذات النص الواضح وذلك لإنتاج الفيديو. ويرد الوصف التفصيلي لذلك في التذييل V لهذه التوصية.

ملاحظة – ليس القصد من هذه الفقرة تعريف أو وصف الآليات الإضافية لمخطط التحويل الشفري الآمن. ويحتاج هذا الموضوع للمزيد من المناقشة في توصيات أخرى.

2.8 آليات الأمن المعنية بحماية الخدمة

تشمل آليات أمن الخدمة الاستيقان والتخويل. ويجوز أيضاً إدراج عمليات تنفيذ آليات محددة للتحكم في النفاذ مثل نظم التجفير وإزالة التجفير.

1.2.8 استيقان الخدمة

وفي حالة الخدمات المدارة التي يكون للمستعمل النهائي (المشترك) فيها علاقة مباشرة مع مورد خدمة معين، سوف يحتاج مورد الخدمة عادة إلى الاستيقان من الجهاز المطرافي و/أو المستعمل النهائي (المشترك) بصورة آمنة وذلك قبل تقديم الخدمة له؛ وفي مثل هذه الحالة يشتمل الاستيقان على تقديم أو عرض– بصورة آمنة – تفويضات/معلومات يمكن مضاهاتها بقاعدة بيانات المشتركين الموجودة لدى المورد وذلك للتحقق من مصداقية الجهاز المطرافي و/أو المستعمل النهائي وذلك بغرض تقديم الخدمة.

2.2.8 تخويل الخدمة

وعقب استيقان المستعمل النهائي (المشترك) و/أو الجهاز المطرافي لغرض تقديم الخدمة، تستخدم آلية تخويل خدمة للتخويل وللسماح بالنفاذ إلى خدمات محددة، وإلى المحتوى الموجود بداخلها وذلك وفقاً لما يقتضيه توفير الخدمة والمرافق للمشترك.

3.2.8 التحكم في النفاذ إلى الخدمة

وفي معظم الحالات (إن لم يكن كلها) يشتمل نظام حماية الخدمة على آليات تستطيع أن تقوم، أو أنها تقوم بتجفير (تخليط) وإزالة تجفير (إزالة تخليط) لكل من حركة تشوير التحكم في الخدمة وحركة المحتوى. وعادة ما يتم تجفير تحكمي في الخدمة في اتجاهين – من المخدم إلى العميل، ومن العميل إلى المخدم. ومن ناحية أخرى، يتم تجفير قطارات المحتوى من المخدم فقط (مورد الخدمة) إلى العميل (الجهاز المطرافي). ومع ذلك، توجد تصورات (سيناريوهات) الاستعمال حيث يمكن ترحيل قطار المحتوى عكسياً من العميل إلى المخدم، وفي هذه الحالة يجوز تجفيره على جهاز مطرافي لأغراض التحميل العكسي (مثال ذلك التأكد من أن مورد الخدمة المستيقن والمخول وحده هو الذي يستطيع النفاذ إلى المحتوى المحمَّل عكسياً).

3.8 آليات الأمن المعنية بحماية الشبكات

لا تُعرِف هذه التوصية ولا تصف أية آلية تتعامل مع أمن الشبكات. وبصفة عامة، فإنه يتوقع لعمليات تنفيذ الشبكات الرئيسية، وشبكات النفاذ، والحمالات وشبكات التسليم أن تُمكِّن من تنفيذ كل ما يعتقد أنه مطلوب من الآليات تنفيذه، وهو أن تحمي السلامة التشغيلية للشبكة بما في ذلك الكشف عن رفض تقديم الخدمة ومنعه، مثلاً. وبصفة عامة تكون آليات الأمن التي يستخدمها مورد خدمة التلفزيون القائم على بروتوكول الإنترنت والأجهزة المطرافية شفافة بالنسبة لهذه الشبكات، شريطة أن تكون آليات الأمن هذه تعمل عند أو فوق مستوى عناصر بيانات الحمولة النافعة التي تقدمها طبقات الشبكة.

4.8 آليات الأمن المعنية بحماية الأجهزة المطرافية

تشمل آليات أمن الأجهزة المطرافية طائفةً واسعة من العناصر الوظيفية بما في ذلك التخزين الآمن المستعصي على التلاعب لبيانات الأسرار، واستيقان الخدمة، وتخويل الخدمة، وتشفير، وإزالة تشفير إشارات التحكم، وإزالة تجفير المحتوى، وفك تشفير البيانات الشرحية لحقوق المحتوى، وإنفاذ استعمال المحتوى، والكشف عن العلامات المائية ودمجها، والاستيقان والتحقق من

المحتوى البرنامجي، وتجسير وتبادل حماية الخدمة والمحتوى، وتجفير منفذ الخرج الرقمي (سطح بيني)، ومقاومة التلاعب بمسارات الوسائط، ومكونات ومعالجات أمن قابلة للعمل بالمقابس وقابلة للتجديد تعتمد على كل من العتاد والبرمجيات، إلخ.

5.8 آليات الأمن المعنية بالمشتركين أو المستعملين النهائيين

تتعلق آليات أمن المشتركين أو المستعملين النهائيين في المقام الأول بجمع وتخزين وإرسال المعلومات التي قد تخضع لاعتبارات الخصوصية أو سرية المستعمل النهائي. وهكذا، يمكن تقسيم هذه الآليات بين نقطة الجمع، والجهاز المطرافي، ومورد الخدمة إذْ يمكنها جمع والمحافظة على وإعادة استعمال هذه المعلومات. وبناء على ذلك، يُتَوَقَعْ لأوصاف وتعاريف هذه الآليات أن تُدْرج في فقرات تصف أمن الخدمة والجهاز المطرافي.

وفي هذا المقام، لا تسعى هذه التوصية إلى تعريف آليات أمن المشترك أو المستعمل النهائي. ومن المتوقع للأعمال المستقبلية بشأن هذه التوصية أن تواصل مناقشة هذه الموضوعات.

وترد في الملحق A معلومات إضافية بشأن أمن المشترك.

الملحق A

حماية أمن المُشترِك

(يشكل هذا الملحق جزءاً لا يتجزأ من هذه التوصية)

1.A حماية بيانات المستعمل

من الأمور الأساسية عند تنفيذ خدمات التلفزيون القائم على بروتوكول الإنترنت بين عامة المستعملين إيلاء اعتبار كاف لأمن حماية بيانات المشترك. وقد تشمل بيانات المشترك أيضاً معلومات بشأن البيانات المتتبعة مثال رقم القناة قبل وبعد تغيير القناة، ووقت التغيير ومعلومات المستعمل لخدمة دليل البرنامج الإلكتروني EPG، وتعريف هوية الرزمة، وزمن العرض، إلخ. والبيانات آنفة الذكر شخصية وسرية بطبيعتها وحماية كل بيانات المشترك هذه من سوء الاستخدام أمر يتطلب من مورد خدمة التلفزيون القائم على بروتوكول الإنترنت أن يولي الاعتبار لقضايا حماية خصوصية المستعمل.

- تستطيع خدمة التلفزيون القائم على بروتوكول الإنترنت أن تقوم اختيارياً بمناولة الحد الأدنى من البيانات الشخصية للمشترك والضرورية لتسليم خدمات التلفزيون القائم على بروتوكول الإنترنت.
- تستطيع خدمة التلفزيون القائم على بروتوكول الإنترنت أن تشرح – اختيارياً – الاستعمال المقصود للبيانات الشخصية للمشترك، وأن تحصل على موافقة المشترك وذلك قبل القيام بجمع معلومات المشترك، وأن تحصل على موافقته قبل جمع المعلومات اللازمة لتسليم خدمات التلفزيون القائم على بروتوكول الإنترنت.
- تستطيع خدمة التلفزيون القائم على بروتوكول الإنترنت – اختيارياً – تدمير البيانات الشخصية للمشترك التي تصبح غير ضرورية لاستمرار خدمات تلفزيون IPTV.
- عندما يقوم مورد الخدمة باستعمال البيانات الشخصية للمشترك، عندئذ تستطيع خدمة تلفزيون IPTV أن تقوم اختيارياً بتخزين البيانات المجمعة مع تطبيق قواعد أمن صارمة.

هناك كثير من الطرق المحتملة التي تتسرب البيانات الشخصية للمشترك عبرها: فيجوز أن تتسرب من شركة الخدمة، وأن تتسرب من الشبكة، وأن تتسرب من المنـــزل مثلاً عن طريق الأجهزة المطرافية. ونَعْرِضْ هنا لطرق حماية البيانات الشخصية للمشترك بالنسبة لكل مسار من هذه المسارات.

ولمنع تسرب البيانات ذات الصلة بالمشترك، يُوصَى مورد خدمة تلفزيون IPTV بالعناية الدقيقة بما يلي:

- تصنيف البيانات الشخصية للمشترك إلى بيانات تحتاج إلى التحكم فيها، وأخرى لا تحتاج إلى ذلك.
- إدارة بيانات المشترك الشخصية التي تحتاج إلى التحكم فيها وذلك بصورة آمنة.
- التأكد من أن البيانات الشخصية للمشترك التي تتطلب التحكم فيها لا تُسْتَعمَل في أغراض غير المقصودة.

ويوصى موردو خدمة التلفزيون القائم على بروتوكول الإنترنت IPTV بالعناية الدقيقة بالنقاط الواردة أدناه فيما يتعلق بالخدمات والعمليات التي تنطوي على مناولة بيانات المشترك الشخصية:

- تصنيف بيانات المشترك الشخصية إلى بيانات تحتاج إلى تحكم وأخرى لا تحتاج إلى تحكم
- استعمال قنوات الاتصال المجفرة لإرسال بيانات المشترك الشخصية التي تتطلب تحكماً

ويقوم موردو خدمة التلفزيون القائم على بروتوكول الإنترنت في بعض الأحيان بخَزْنِ بيانات المشترك الشخصية في أجهزة مطرافية لرفع كفاءة الخدمة. وفي مثل هذه الحالات، يُوصَى هؤلاء الموردون بإيلاء أهمية فائقة للنقاط الواردة أدناه. كما يوصى إيلاء الاعتبار للأمن عند تبادل الأجهزة المطرافية:

- ضمان عدم قيام طرف ثالث بسهولة بقراءة البيانات الشخصية للمشترك المخزونة داخل جهاز مطرافي.

- يمكن لمورد خدمة التلفزيون القائم على بروتوكول الإنترنت أن يتحكم اختيارياً في النفاذ إلى بيانات المشترك الشخصية المخزونة داخل الجهاز المطرافي.
- ضمان إمكانية الحذف الكامل لبيانات المشترك الشخصية المخزونة داخل الأجهزة المطرافية من جانب مشترك أو مورد خدمة.
- يتعين حماية الأجهزة المطرافية – بوصف ذلك أفضل التدابير – من الهجمات ببرمجيات حاسوبية خبيثة، مثل الفيروسات ووسائل التجسس، في المستقبل القريب.

2.A الرقابة الأبوية، وحماية القُصَّر قانوناً، والتحكم في النفاذ

في منصة التلفزيون القائم على بروتوكول الإنترنت، يمكن استعمال آلية لحماية القصر قانوناً لتقييد محتوى تلفزيون IPTV التي يمكن النفاذ إليها من جانب القصر قانوناً. ويقضي النسق الاعتيادي للاستعمال، أن يتم تقاسم جهاز مطرافي لتلفزيون IPTV بواسطة العديد من الأشخاص داخل مسكن، بمن فيهم القصر قانوناً. وبالنسبة للأجهزة المطرافية، يُوصَى مورد خدمة تلفزيون IPTV القيام بالآتي:

- التأكد من أنه يمكن ضبط قِيَم الرقابة الأبوية للمحتوى حسب الضرورة.
- التأكد من أن الأجهزة المطرافية يمكن تشغيلها طبقاً للقِيَمْ الأبوية.
- التأكد من أن الأجهزة المطرافية قادرة على تغيير معدلات القيم الأبوية.
- التأكد من أن الأجهزة المطرافية قادرة على الضوابط القائمة على كلمة المرور بحيث لا يتمكن سوى الأوصياء على القُصَّر القانونين من تغيير القيم الأبوية.
- التأكد من أن قيم المحتوى يمكن ضبطها لتتناسب مع الفئات العمرية المختلفة.
- التأكد من أن امتيازات المشترك يمكن توزيعها على الفئات العمرية المختلفة.
- التأكد من إمكان عمل التخويل في الأجهزة المطرافية للقصر قانوناً لمشاهدة قناة أو محتوى معين مثال ذلك وقف عرض المَشَاهد إلا باستعمال رقم التعريف الشخصي.
- التأكد من أن الأوصياء الذين ليسوا على مقربة من القصر قانوناً يمكنهم الرصد عن بعد واستقبال المحتوى للقصر قانوناً من مخزن النُسَخْ الخاص بالشبكة.

ومما يُذكر أن أخذ ظروف كل إدارة أو منطقة في الاعتبار بالنسبة لمنظمات الطرف الثالث لاستبعاد المحتوى الضار قد يكون ضرورياً، حيث أن ذلك يرتبط بالتحكم في تدفق المحتوى والنفاذ إليه. يمكن للمرء أن يفترض أن مؤلف المحتوى الأصلي يولي اعتباراً مناسباً لإعادة الإرسال التزامني للبث عند إنتاج المحتوى، ومن ثم ضرورة إيلاء اهتمام كافٍ لمُهَلات الإرسال وتوزيع الزيادات في التكاليف.

التذييل I

التهديدات الأمنية

(هذا التذييل لا يشكل جزءاً أساسياً من هذه التوصية)

يصف هذا التذييل مجموعة من تهديدات الأمن المُعَرَّفَة التي تتناولها بعض متطلبات أو آليات هذه التوصية.

وقد تم تناول نموذج تهديد الأمن والمواد الأساسية الأخرى طبقاً لتوصيات قطاع تقييس الاتصالات التالية:

- تُعرِف التوصية [b-ITU-T X.800] عناصر المعمارية العامة المعنية بالأمن والتي يمكن تطبيقها بصورة ملائمة في الظروف التي تحتاج إلى حماية الاتصال فيما بين النظم المفتوحة.
- وتُعرِف التوصية [b-ITU-T X.805] معمارية أمن الشبكة لتوفير أمن الشبكة من طرف – إلى – طرف.

وتُشَجَع الأطراف المهتمة باعتبارات الأمن المتصلة بالتلفزيون القائم على بروتوكول الإنترنت على قراءة توصيتي الأمن الأساسيتين هاتين، ويُفترض فيمن يقرأ هذه التوصية أن يكون واعياً للمعلومات الواردة في هاتين التوصيتين.

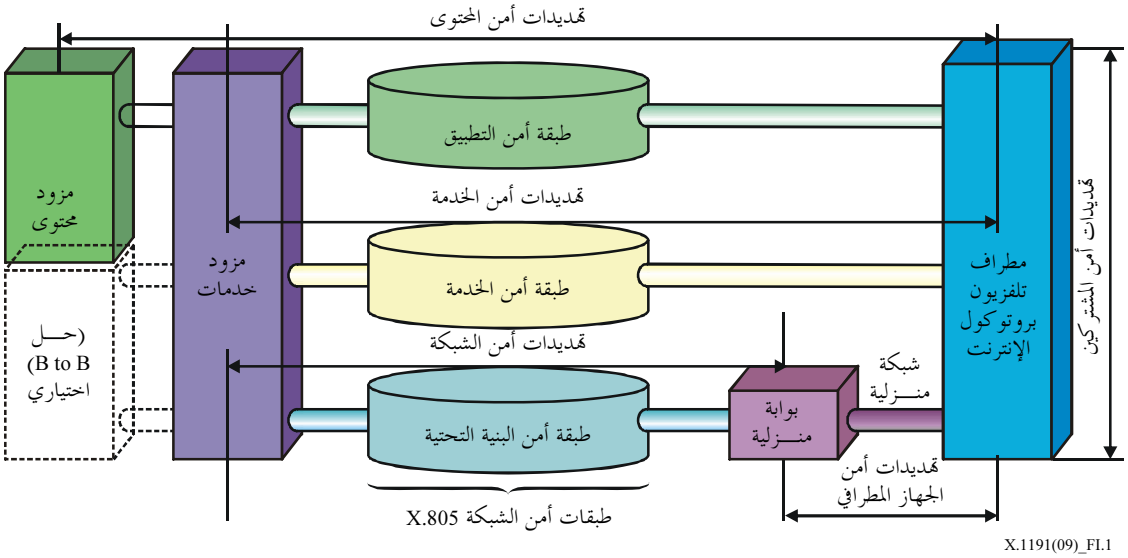
وتُعرِّف التوصيتان [b-ITU-T X.800] و[b-ITU-T X.805] تهديدات الأمن التالية للشبكات (والتي هي بمثابة تهديدات لأمن تطبيق الخدمة والمحتوى التي تسري على التلفزيون القائم على بروتوكول الإنترنت) بأنها:

- تدمير المعلومات و/أو الموارد الأخرى.
- إفساد المعلومات أو تعديلها.
- سرقة أو إلغاء أو فقدان المعلومات و/أو الموارد الأخرى.
- إفشاء المعلومات.
- انقطاع الخدمات.

1.I نموذج التهديدات الأمنية

يمكن تصنيف تهديدات أمن التلفزيون القائم على بروتوكول الإنترنت في الأنماط التالية: تهديدات أمن المحتوى، تهديدات أمن الخدمة، تهديدات أمن الشبكة، تهديدات أمن المطراف النهائي وتهديدات أمن المشترك.

الشكل I-1 يوضح نموذج التهديدات الأمنية الذي يبين العلاقات فيما بين كل واحد من هذه التهديدات وغيره.



الشكل 1.I - نموذج للتهديدات الأمنية

1.1.I تهديدات أمن المحتوى

أصول المحتوى: يمكن للأصول التي تنتمي لمورد المحتوى و/أو مورد الخدمة أن تُستَهلك بواسطة المستعمل النهائي عبر الجهاز المطرافي.

وتشتمل أصول المحتوى التي تحتاج إلى حماية على: محتوى التلفزيون الخطي، محتوى الفيديو حسب الطلب، محتوى الفيديو حسب الطلب بالضغط، محتوى مسجل فيديو شخصي والتطبيقات المُحمَلة، إلخ.

وفيما يلي بيان بتهديدات المحتوى:

- اعتراض طريق المحتوى: وهو خرق لسرية المحتوى الرقمي من خلال الرصد غير المشروع لشبكات الخدمة.
- المشاهدة غير المُخَولَة.
- الاستنساخ غير المخول أو إعادة التوزيع.

2.1.I تهديدات أمن الخدمة

أصول الخدمة: وهي الأصول التي تتبع مورد خدمة؛ وهي تشمل مخدمات الوسائط، ومخدمات حماية الخدمة، والمحتوى والمعلومات التشغيلية مثل ملفات تسجيل الخدمة ومعلومات الفوترة على أقل القليل.

وفيما يلي بيان بتهديدات الخدمة:

- السطو على حقوق تأليف البرامج التي تقدمها منصة خدمة تلفزيون IPTV إلى المشتركين.
- التنكر/الاحتيال على مورد خدمات التلفزيون القائم على بروتوكول الإنترنت IPTV.
- التهديدات الخبيثة التي تستهدف مخدمات تلفزيون IPTV (مخدمات حماية الخدمة والمحتوى، مخدمات الوسائط، إلخ): ويمكن أن تشمل الاحتيال الذي يستهدف التسريبات الأمنية في تطبيق البرمجيات أو بروتوكول الاتصال، أو هجوم رفض تقديم الخدمة، إلخ.
- السرقة (وغالباً ما تستخدم برامج خبيثة كحصان طروادة) لمعلومات المشترك (مثال ذلك معلومات تعريف الهوية، معلومات الفوترة، معلومات الاشتراكات).

3.1.I تهديد أمن الشبكات

أصول الشبكة: وهي الأصول التابعة لمورد الشبكة، ويمكن أن تشتمل على العتاد المادي (مثل المسيّرات، والمبدلات) وموارد الشبكة (مثال عرض النطاق وخدمات البث المتعدد، إلخ).

وفيما يلي بيان بتهديدات الشبكة:

- التهديدات المتعمدة تستهدف عتاد أو موارد الشبكة (عرض النطاق): الهجمات الخبيثة على شبكة الحمالة كرفض تقديم الخدمة.
- التهديدات لأمن تقنية البث المتعدد المستخدمة في شبكة الحمالة للتلفزيون القائم على بروتوكول الإنترنت مثل التنكر/التحايل على مصادر التلفزيون متعدد البث أو أعضاء زمرة البث المتعدد غير القانونية.
- الهجمات الخبيثة (مثل حجب الخدمة، واقتحام hacking) على العقدات داخل شبكة توزيع الإنترنت.

4.1.I تهديد أمن الأجهزة المطرافية

الأصول المطرافية: هي الأصول التابعة للجهاز المطرافي والتي يمكن استعمالها من جانب المستعمل النهائي لمعالجة المحتوى وتخزينه إلى جانب المعلومات ذات الصلة بخدمة التلفزيون القائم على بروتوكول الإنترنت.

وفيما يلي بيان بالتهديدات المطرافية:

- النفاذ غير المشروع إلى محتوى واضح عن طريق التلاعب بعتاد الأجهزة أو البرمجيات، فمثلاً يمكن استنساخ المحتويات الواضحة عبر اعتراض طريق بيانات الناقل أو كسر شفرة البرمجيات SCP.
- النفاذ غير المشروع إلى المفاتيح أو المعلومات السرية الأخرى باستخدام كسر شفرة البرمجيات أو التلاعب بالعتاد؛ ويمكن للمهاجمين التلاعب بذاكرة الجهاز أو تحليل تدفق البيانات لأجل الحصول على مفاتيح وعلى أسرار أخرى (يؤدي افتضاح مفاتيح الجهاز إلى انتحال شخصية الجهاز).
- التسبب في تعطيل الجهاز بطريقة عتادية مثل التحكم في نظام ميقاتية الجهاز لتعطيل وظائف حماية الخدمة والمحتوى أو بطريقة برمجيات مثل إنشاء فيروسات لاستنفاد موارد الجهاز.
- التطبيقات غير المخولة (مثل تحميل برامج البرمجيات) وعرضها وتخزينها داخل الأجهزة المطرافية.
- إيقاف عمل الجهاز المطرافي (العتاد والبرمجيات) بواسطة شفرات/فيروسات خبيثة من الشبكة.
- توصل أجهزة مطرافية غير مخولة، بالشبكة المنزلية.
- الاستعمال غير المخول من جانب المشتركين.

5.1.I تهديد أمن المشترك

أصول المشتركين: وهي الأصول التابعة لمشترك، ويمكن أن تتألف من معلومات بشأن المشترك، وأسرة المشترك، ومعاملاتهم الخاصة بالتلفزيون القائم على بروتوكول الإنترنت، إلخ.

ويتطلب أمن المشترك تعاون آلية تحقيق أمن المحتوى، وآلية تحقيق أمن الخدمة معاً، لأن خدمة تلفزيون IPTV تضم خدمة يعمل فيها أمن المحتوى وأمن الخدمة في علاقة تعاونية.

أدرجت أمثلة لتهديدات المشترك في الجدول 1.I.

الجدول 1.I – فئات أمن المشترك

	أمن المشترك		
	مثال الخدمة	**عينات للتهديدات**	**مثال لآلية حماية**
أمن المحتوى	التلفزيون الخطي، خدمة فيديو حسب الطلب	نسخة غير قانونية	تعريف هوية الجهاز المطرافي (حماية الخدمة، حماية المحتوى)
أمن الخدمة	خدمة ثنائية الاتجاه	الاحتيال	تعريف الهوية الشخصية (حماية البيانات الشخصية، تعريف الهوية الشخصية/كلمة المرور)
	أبوي	المخادعة	تعريف الهوية الشخصية (استيقان/تعريف الهوية الشخصية/كلمة المرور)
أمن الشبكة	غير محدد	التنصت	تعريف هوية خط المشترك بيانات تجفير، تحكم مشترك في البث المتعدد
أمن الجهاز المطرافي	خدمة P2P	نسخة غير قانونية	حماية المحتوى نقطة-إلى-نقطة (P2P)

التذييل II

قابلية التشغيل البيني لحماية الخدمة والمحتوى

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.II نظرة شاملة على التشغيل البيني لحماية الخدمة والمحتوى

هناك العديد من السيناريوهات لحماية الخدمة والمحتوى القابلة للتشغيل البيني: حماية الخدمة والتشغيل البيني من طرف إلى طرف، SCP-EE، تجسير حماية الخدمة والمحتوى SCP-B، وتبادل حماية الخدمة والمحتوى SCP-IX. ويمكن تطبيق هذه الحماية القابلة للتشغيل البيني الخاصة بالخدمة والمحتوى سواء في ميدان مورد الخدمة أو ميدان المستعمل النهائي. ويسلط هذا التذييل الضوء فقط على الجانب المطرافي.

2.II سيناريوهات حماية الخدمة والمحتوى القابلة للتشغيل البيني

تصنف سيناريوهات حماية الخدمة والمحتوى القابلة للتشغيل البيني إلى ما لا يقل عن ثلاثة أساليب هي: حماية الخدمة والمحتوى من طرف إلى طرف (SCP-EE)، وتجسير حماية الخدمة والمحتوى (SCP-B)، وتبادل حماية الخدمة والمحتوى (SCP-IX).

(1) حماية الخدمة والمحتوى من طرف إلى طرف (SCP-EE)

SCP-EE: باستعمال حماية خدمة ومحتوى وحيدة، وتبادل جهازين أو أكثر، والنفاذ إلى المحتوى طبقاً للحقوق الممنوحة. ويحتاج هذا الأسلوب لكي يكون أبسط الأساليب من حيث التنفيذ، حيث لا تستعمل إلا حماية واحدة فقط للخدمة والمحتوى.

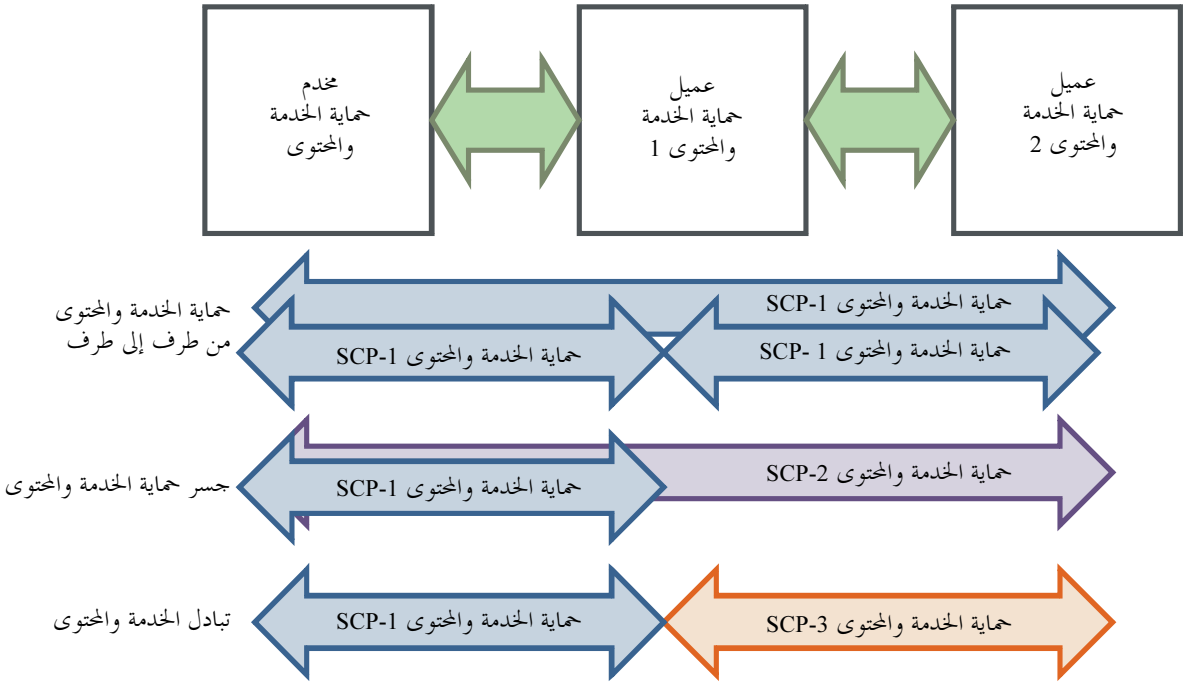
(2) تجسير حماية الخدمة والمحتوى (SCP-B)

SCP-B: توضع على جهاز مطرافي وحيد، وتنشر نقطتان أو أكثر لحماية الخدمة والمحتوى. أما المحتوى الذي يتم استحواذه عبر نظام واحد لحماية الخدمة والمحتوى (مثلاً من شبكة) فيمكن النفاذ إليه عبر نقطة حماية ومحتوى موجودة على نفس الجهاز طبقاً للحقوق الممنوحة.

(3) تبادل حماية الخدمة والمحتوى (SCP-IX)

SCP-IX: تتميز هذه الحالة بوجود جهازين أو أكثر، بحيث يتم النشر على كل واحد من الأجهزة نقطة أو أكثر من نقاط حماية الخدمة والمحتوى. أما المحتوى الذي يتم الحصول عليه عبر واحد من نقاط حماية الخدمة والمحتوى التابعة له فيمكن نقله أو النفاذ إليه بصورة آمنة على جهاز آخر وذلك طبقاً للحقوق الممنوحة.

يبين الشكل II-1: نموذجاً للحالة الوارد وصفها آنفاً



الشكل 1.II - أسلوب التشغيل البيني لحماية الخدمة والمحتوى

3.II المجالات الفنية القابلة للتشغيل البيني لحماية الخدمة والمحتوى

تمثل المجالات التالية العناصر الرئيسية للتشغيل البيني اللازمة لأساليب حماية الخدمة والمحتوى من طرف إلى طرف SCP-EE، وتجسير حماية الخدمة والمحتوى SCP-B وتبادل حماية الخدمة والمحتوى SCP-IX:

(1) استيقان الأجهزة والمستعملين ونقاط حماية الخدمة والمحتوى

قبل إمكان تبادل المحتوى بين كيانات، ينبغي الإنشاء الآمن لمُعَرِف هوية الجهاز المطرافي وربما المستعمل (المستعملين). وبالإضافة إلى ذلك، فنظراً إلى أن موردي المحتوى قد لا يثقون بنقاط حماية خدمة ومحتوى محدودة، فينبغي أن تتوافر إمكانية استيقان نقطة (نقاط) حماية الخدمة والمحتوى المتلقية أو سويات التنفيذ وذلك قبل تبادل المحتوى. وينبغي لمثل هذا الاستيقان أن ينبني على أساس تجفيري سليم، وقد يستعمل تقنيات مختلفة للبصمة الرقمية المعروفة.ويوفر تجفير المفاتيح العمومية بصفة خاصة آلية صحيحة للتوقيعات الرقمية في بروتوكولات الاستيقان.

(2) تبادل التعبير عن الحقوق

تستخدم نقاط حماية الخدمة والمحتوى المختلفة لغات مختلفة للتعبير عن الحقوق أو أنساقاً مختلفة للتراخيص. ولكي يؤدي أسلوبا SCP-B و SCP-IX وظائفهما، فإن الأمر يتطلب وجود وسيلة للتعبير عن الحقوق بصورة مشتركة. ويمكن لذلك أن يتخذ شكل لغة مشتركة للتعبير عن الحقوق (REL) أو مترجم تعبير عن الحقوق. والتفاوض بشأن التراخيص هو آلية محتملة أخرى لتبادل التعبير عن الحقوق.

(3) خوارزميات التجفير المشتركة لتبادل المحتوى

يتعين تجفير المحتوى حتى يمكنه أن يمر بأمان من تحكم نقطة حماية خدمة ومحتوى إلى أخرى أو داخل نفس نقطة حماية الخدمة والمحتوى ولكن على أجهزة مادية مختلفة. وهذا من شأنه أن يجعل المحتوى غير قابل للاستعمال إلا بالنسبة للكيانات التي يوجد في حوزتها المفتاح المناسب أو المفاتيح الضرورية حتى تحدث إزالة التجفير. وهناك الكثير من الأنماط المختلفة لخوارزميات التجفير (مثال شفرات الفدرات وشفرات القطارات، وهي قائمة على المفاتيح العمومية، إلخ)، غير أن الأنماط التي تستخدم

المفاتيح المتماثلة عامة تكون هي المناسبة إلى أبعد حد لتبادل المحتوى عالي السرعة ولأغراض قابلية التشغيل البيني يتعين اختيار عدد صغير من الخوارزميات المتفق عليها بصورة مشتركة. والأفضل، أنه ينبغي تحديد خوارزمية بالتغيب.

(4) إدارة المفاتيح و/أو تبادل خوارزميات التجفير المشتركة

قبل أن يصبح في الإمكان تبادل آمن للمحتوى، يجب تبادل المفاتيح التي تستخدم في حالات محددة، أو توليدها عامة بواسطة كيانات مستيقَنة. وإدارة المفاتيح تكون عادة أصعب جزء يتم تنفيذه في نظام الأمن. لقد أسهم وجود أساليب تقنية مثل تجفير المفاتيح العمومية في تبسيط توزيع مفاتيح الأجهزة، ولكنه يحتاج إلى بنية تحتية للمفاتيح العمومية (PKI) لأجل إنشاء هذه المفاتيح والمحافظة على صلاحيتها. ويمكن السماح بمثل هذه البنية التحتية والمحافظة عليها من جانب هيئة معنية بالتراخيص ومسؤولة عن حماية المحتوى (وذلك مقابل الأمن العام للشبكة).

(5) التحميل الآمن لعميل حماية الخدمة والمحتوى

والوضع المثالي هو أن يتمكن أي جهاز مطرافي من تبادل المحتوى الذي يتم الحصول عليه (بصورة مشروعة) عن طريق أجهزة أخرى و/أو استخدام أي حماية خدمة ومحتوى طبقاً للحقوق الممنوحة (أي أسلوب تبادل حماية الخدمة والمحتوى SCP-IX). وتجدر ملاحظة أنه ليس من العملي كثيراً التحميل المسبق – وقت التصنيع لكل جهاز مطرافي بكل نظام لحماية الخدمة والمحتوى تطلبه قوى السوق، ومن ثم تبرز الحاجة إلى وجود آلية آمنة لتحميل وتنفيذ نظام منتقى لحماية الخدمة والمحتوى على الجهاز المطرافي. وتلعب وسائل تحميل برامج التشغيل الأساسية (boot loaders) وبروتوكولات التحميل الآمن دوراً في مجال قابلية التشغيل البيني هذا.

ملاحظة – عندما يتم نشر خاصية قابلية التشغيل البيني لحماية الخدمة والمحتوى في الأجهزة والأنظمة المطرافية، ينبغي لأجهزة التلفزيون القائم على بروتوكول الإنترنت أن تكون لديها معمارية موثوق بها لدعم قابلية التشغيل البيني لأمن المحتوى.

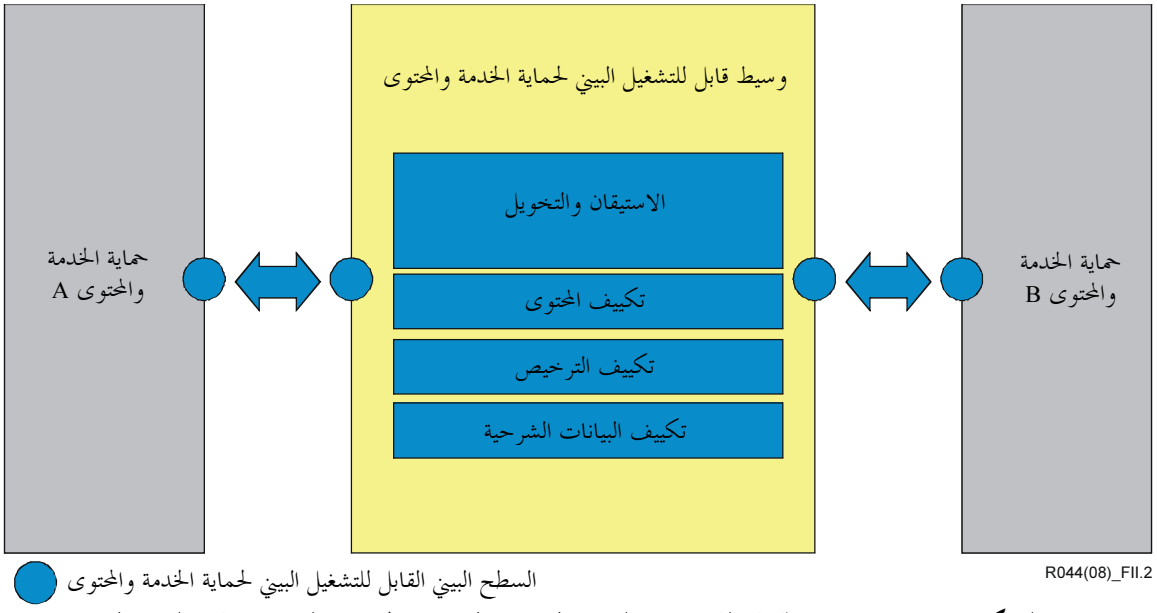
(6) تصدير الحقوق الآمن

لتصدير الحقوق الرقمية بصورة آمنة، ينبغي لعميل حماية خدمة ومحتوى تلفزيون برتوكول الإنترنت التأكد مما إذا كانت حقوق الاستعمال مسموح بتصديرها بحيث تستهدف نظام حماية الخدمة والمحتوى. وقد يكون للحقوق الرقمية تعبيرات حقوقية تُمَكِنْ نظام حماية الخدمة والمحتوى المستهدف من تصدير الحقوق. وفي هذه الحالة ينبغي لعميل حماية خدمة ومحتوى تلفزيون IPTV أن يتأكد من تعبيرات هذه الحقوق وأن يُخَوِلْ لنظم حماية الخدمة والمحتوى السليمة المستهدفة تصدير الحقوق الرقمية.

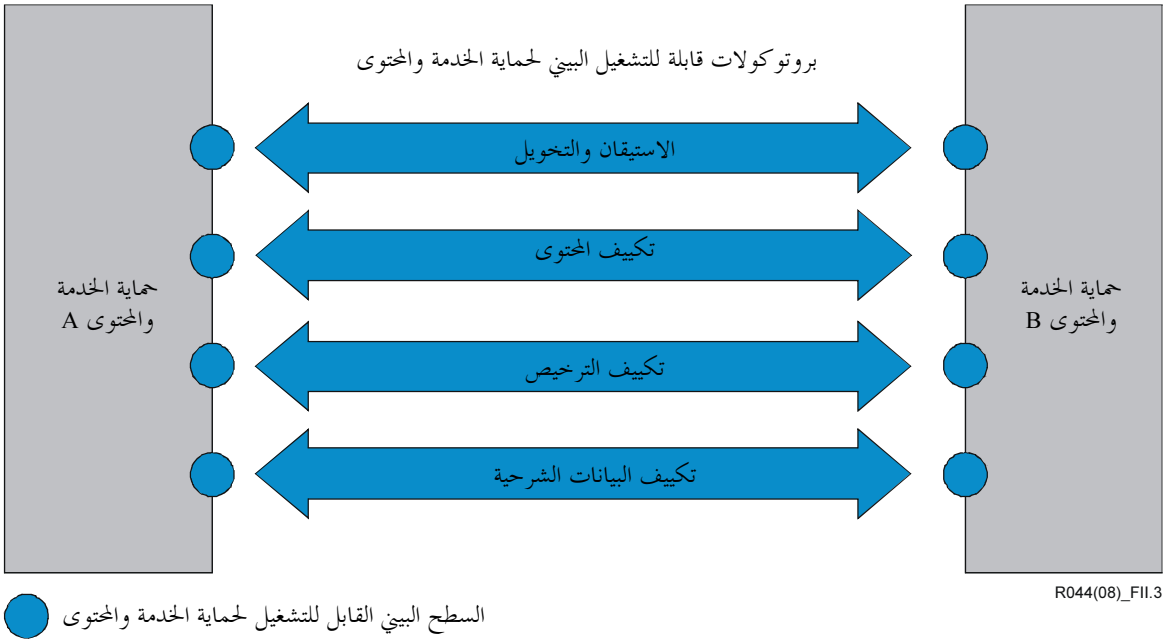
4.II المعماريات القابلة للتشغيل البيني لحماية الخدمة والمحتوى

يمكن النظر في نوعين من المعماريات القابلة للتشغيل البيني لحماية الخدمة والمحتوى، أحدهما يعتمد على معمارية قابلية التشغيل البيني القائمة على الوسيط، والتي تستعمل نظام وسيط يقع بين نظامين لحماية الخدمة والمحتوى وذلك لمعالجة الإرسال القابل للتشغيل البيني. والنوع الآخر هو معمارية معيارية تقوم على أساس البروتوكول وتستعمل أسطحاً بينية معيارية وبروتوكولاتٍ لتحويل المحتوى الرقمي المحمي والمعلومات المصاحبة بين نظامين مختلفين لحماية الخدمة والمحتوى.

وَتَظْهر المعماريتان المحتملتان في الشكلين 2.II و3.II.



الشكل 2.II - معمارية قابلة للتشغيل البيني لحماية الخدمة والمحتوى القائمة على الوسيط



الشكل 3.II - المعمارية المعيارية القائمة على البروتوكول والقابلة للتشغيل البيني لحماية الخدمة والمحتوى

وصف الفدرات الوظيفية

- **تكييف المحتوى**: تكييف المحتوى مسؤول عن تحويل الخوارزمية التجفيرية. أما خوارزميات التجفير المعيارية العديدة سابقة التعريف المذكورة فمن شأنها أن تيسر هذه العمليات.
- **تكييف الترخيص**: وتكييف الترخيص مسؤول عن تحويل ترخيص. وينبغي لأي ترخيص زمني أو معياري معروف لكلا الطرفين أن يحتفظ بنفس سلوكيات التصريح تقريباً (بثنائية أصول الوسائط والتصريح بالاستهلاك) على النحو الذي يحدده الترخيص الأصلي. ويمكن إدراج مجموعة من العناصر المتقابلة (تقابل التعبير عن الحقوق وتقابل الدلالات اللغوية) في تكييف الترخيص. وبالإضافة إلى ذلك، يُحْتمل أن يكون تكييف الترخيص مسؤولاً عن إعادة ترزيم المعلومات الصحيحة وتسليمها بصورة آمنة لعملاء حماية الخدمة والمحتوى الأصليين.

- **تكييف البيانات الشرحية**: تكييف البيانات الشرحية مسؤول عن تحويل معلومات البيانات الشرحية. وينبغي للبيانات الشرحية الزمنية أو المعيارية المعلومة لكلا الطرفين أن تحتفظ بنفس المعلومات التي كانت لدى البيانات الشرحية الأصلية. ويجوز إدراج مجموعة متقابلة من البيانات الشرحية (تقابل التركيب اللغوي والدلالات اللغوية) في تكييف البيانات الشرحية. وبالإضافة إلى ذلك، قد يكون تكييف البيانات الشرحية مسؤولاً عن إعادة ترزيم معلومات البيانات الشرحية وتسليمها بأمان إلى طرف الآخر لحماية الخدمة والمحتوى.
- **الاستيقان والتخويل**: ينبغي لكل طرف مَعْنِي بحماية الخدمة والمحتوى أن يحكم بما إذا كان الطرف الآخر هدفاً سليماً لتحقيق التشغيل البيني لحماية الخدمة والمحتوى، وعادة ما يصاحب ذلك عملية استيقان متبادلة كخطوة أولية بين طرفي حماية الخدمة والمحتوى.

حالة استثنائية: إذا كانت حماية الخدمة والمحتوى A وحماية الخدمة والمحتوى B موجودتين داخل نفس الجهاز، أو في حالة وجود قناة اتصال مخصصة آمنة بين طرفي حماية خدمة ومحتوى، فإن عملية تكييف المحتوى قد لا تحتاج إلى معالجة تشغيل بيني.

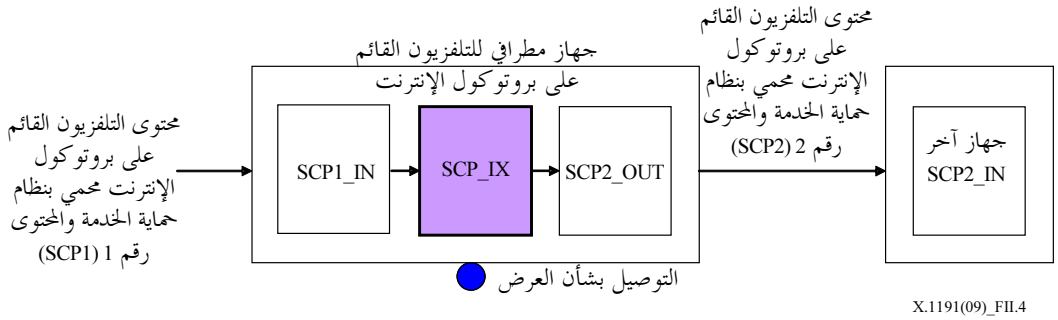
5.II سيناريوهات تجسير حماية الخدمة والمحتوى SCP-B وتبادل حماية الخدمة والمحتوى SCP-IX المنشورة في الجهاز المطرافي

تصف هذه الفقرة ثلاثة سيناريوهات محتملة تحتاج إلى تبادل حماية الخدمة والمحتوى بين أمن الخدمة وأمن المحتوى.

1.5.II تعاريف المصطلحات المستخدمة في هذا الرسم التوضيحي

- SCP_IN: منفذ دخل يدخل منه محتوى التلفزيون القائم على بروتوكول الإنترنت المحمي بواسطة حماية الخدمة والمحتوى
- SCP_OUT: منفذ خَرْج يخرج من خلاله محتوى التلفزيون القائم على بروتوكول الإنترنت المحمي بواسطة حماية الخدمة والمحتوى

2.5.II السيناريو 1: حماية الخدمة والمحتوى بتبادل حماية الخدمة والمحتوى (SCP_IX)

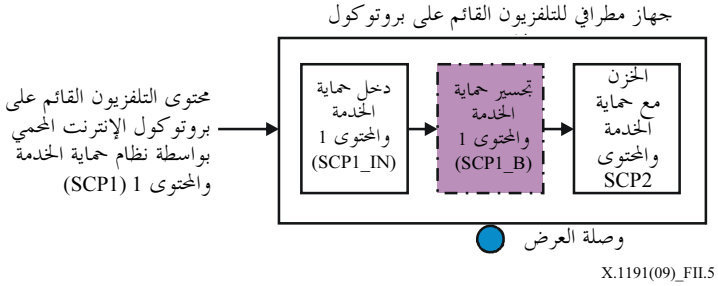


الشكل 4.II - حماية خدمة ومحتوى بتبادل حماية الخدمة والمحتوى (SCP-IX)

ويكون لدى (الجهاز المطرافي) للتلفزيون القائم على بروتوكول الإنترنت في هذه الحالة حماية خدمة ومحتوى بتبادل حماية الخدمة والمحتوى وذلك لتعزيز قابلية التشغيل البيني بين جهاز مطرافي للتلفزيون القائم على بروتوكول الإنترنت بدون تخزين يأخذ فقط بأمن خدمة محدد وجهاز خارجي مزود بتخزين ليس له إلا حماية محتوى محدد.

ولتعزيز توصيلية آمنة ومرنة مع أي نوع من الأجهزة الخارجية التي تأخذ بآليات حماية محتوى متنوعة، ينبغي للجهاز المطرافي التابع للتلفزيون القائم على بروتوكول الإنترنت أن يزود بآلية تبادل حماية خدمة ومحتوى (SCP-IX) بدلاً من التنفيذ حالة بحالة لتوصيل الأمن بين جهازين.

3.5.II السيناريو 2: حماية خدمة ومحتوى مزودة بتجسير حماية الخدمة والمحتوى (SCP-B) وبتخزين اختياريين



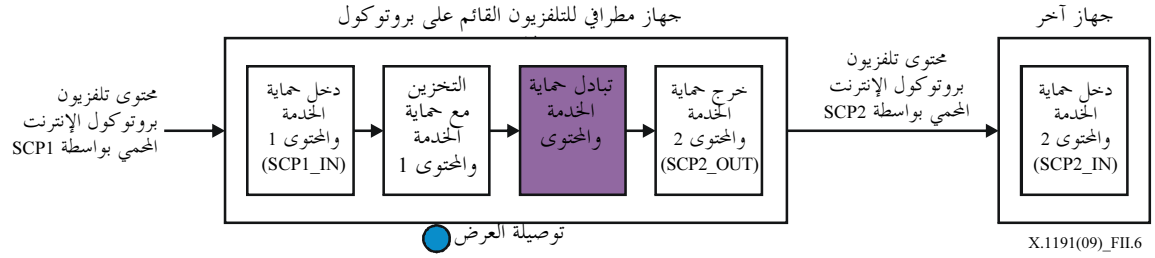
الشكل 5.II - حماية خدمة ومحتوى مزود بتجسير حماية الخدمة والمحتوى (SCP-B) وتخزين اختياريين

يوجد في هذه الحالة لدى الجهاز المطرافي للتلفزيون القائم على بروتوكول الإنترنت حماية خدمة ومحتوى مزودة بتجسير حماية الخدمة والمحتوى (SCP-B) وذلك لتعزيز قابلية التشغيل البيني بين حماية الخدمة وحماية المحتوى في جهاز واحد.

وقد تعتمد جهة تصنيع الجهاز المطرافي للتلفزيون القائم على بروتوكول الإنترنت آلية لحماية المحتوى محكومة بواسطة المالك لأغراض التخزين الداخلي. وفي مثل هذه الحالة لا يكون تجسير حماية الخدمة والمحتوى (SCP_B) ضرورياً، ويجوز استعمال حماية الخدمة والمحتوى 1 (SCP1) بواسطة التخزين.

ولدعم توصيلية مرنة بأي نوع من التخزين الداخلي الذي يعتمد مختلف آليات حماية المحتوى، يوصى بأن يكون لدى الجهاز المطرافي للتلفزيون القائم على بروتوكول الإنترنت آلية لتجسير حماية الخدمة والمحتوى (SCP_B) بدلاً من التنفيذ حالة بحالة لتوصيل الأمن بين حماية الخدمة وحماية المحتوى.

4.5.II السيناريو 3: حماية خدمة ومحتوى مزودة بالتخزين بتبادل حماية للخدمة والمحتوى (SCP-IX)



الشكل 6.II - حماية خدمة ومحتوى مزودة بالتخزين وبتبادل حماية الخدمة والمحتوى (SCP_IX)

ويكون للجهاز المطرافي للتلفزيون القائم على بروتوكول الإنترنت في هذه الحالة، حماية SCP مزودة بتخزين وبتبادل الحماية (SCP_IX) وذلك لدعم قابلية التشغيل البيني بين آلية حماية المحتوى الداخلية وآلية الحماية الخارجية.

ولتعزيز توصيلية مرنة بأي نوع من التخزين الخارجي الذي يعتمد آليات حماية محتوى متعددة، يُوصَى بتزويد الجهاز المطرافي للتلفزيون القائم على بروتوكول الإنترنت بآلية لتبادل الحماية للخدمة والمحتوى (SCP-IX) بدلاً من التنفيذ – حالة إلى حالة – لتوصيلة الأمن بين آلية حماية المحتوى الداخلية والآلية الخارجية.

التذييل III

مثال لعملية حماية محتوى التلفزيون القائم على بروتوكول الإنترنت

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يصف ما يلي عينة لعملية تطبيق فيديو حسب الطلب لحماية المحتوى:

- *مرحلة استيقان المشترك*
  - يختار مشترك تطبيق فيديو حسب الطلب عن طريق "الفِدرة الوظيفية للعميل لاكتشاف واختيار الخدمة والتطبيق."
  - ترسل "وظائف التطبيق الخاصة بالتلفزيون القائم على بروتوكول الإنترنت" الطلب فور تسلمه إلى "الفِدرة الوظيفية للمظهر الجانبي للتطبيق" للتحقق من هذا المشترك. فإذا نجحت هذه العملية، تحفظ نسخة من معلومات التخويل الخاصة بالمشترك داخل " الفِدرة الوظيفية للمظهر الجانبي للتطبيق" للاستفسار.
- *مرحلة اختيار المحتوى*
  - يمكن للمشترك أن يختار محتوى الوسائط المعين باستخدام معلومات من زمرة المكونات الإلكترونية (ECG)، ثم تقوم "الفِدرة الوظيفية لتطبيق الفيديو حسب الطلب" بتسليم معلومات موقع المحتوى المنتقى (URL) إلى الجهاز المطرافي.
  - تتلقى "الفِدرة الوظيفية لعميل الفيديو حسب الطلب" في الجهاز المطرافي موقع المحتوى لإرساله إلى "وظائف تسليم المحتوى للعميل."
- *مرحلة تسليم المحتوى المجفر*
  - تنطبق "وظائف تسليم المحتوى للعميل" على محتوى الوسائط (المجفر) وذلك باستعمال معلومات موقع المحتوى؛ وهي تنطبق أيضاً على الحقوق والمفاتيح المصاحبة لهذا المحتوى من "الفِدرة الوظيفية لحماية المحتوى للعميل."
- *مرحلة توزيع الحقوق والمفاتيح*
  - إذا لم يكن لدى "الفِدرة الوظيفية لحماية المحتوى للعميل" الحقوق والمفاتيح، فإنها تطلب هذه المعلومات من "الفِدرة الوظيفية لإدارة الحقوق والمفاتيح" لدى مزود خدمة التلفزيون القائم على بروتوكول الإنترنت IPTV.
  - تقدم "الفِدرة الوظيفية لإدارة الحقوق والمفاتيح" طلباً للحصول على معلومات التخويل المصاحبة لهذا المشترك والموجودة لدى "الفِدرة الوظيفية للمظهر الجانبي للتطبيق" للتأكد مما إذا كان للمشترك حق في استهلاك هذه المعلومات الخاصة باستخدام المحتوى.
  - إذا نجحت في ذلك فإن الحق والمفتاح للمحتويات المختارة سوف يسلمان إلى " الفِدرة الوظيفية لحماية المحتوى للعميل."
  - وفور التسلم، تقوم "الفِدرة الوظيفية لحماية المحتوى للعميل بنقل المفتاح والحق إلى "وظائف تسليم المحتوى للعميل" لفك تجفير المحتويات وللتحكم في استعمالها.

التذييل IV

حماية محتوى البث الفيديوي الرقمي DVB وإدارة النسخ

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

يقدم هذا التذييل موجزاً لمجموعة مواصفات البث الفيديوي الرقمي – حماية المحتوى وإدارة النسخ DVB-CPCM، التي وضعها المعهد الأوروبي لمعايير الاتصالات (ETSI).

والبث الفيديوي الرقمي – حماية المحتوى وإدارة النسخ DVB-CPCM عبارة عن مثال لنظام كامل التقييس لحماية التلفزيون وغيره من محتوى داخل شبكة محلية وخارجها. ويمكن لـــ DVB-CPCM أن تحصل على محتوى من آلية حماية خدمة التلفزيون القائم على بروتوكول الإنترنت معرفة طبقاً لتعاريف الإتحاد الدولي للاتصالات ITU (أو غيره) وتحافظ على حماية محتوى التلفزيون القائم على بروتوكول الإنترنت طوال دورة حياة المحتوى بدءاً من الاستحواذ وحتى الاستهلاك بما في ذلك تخزين، ومعالجة وتصدير المحتوى المحمي إلى آليات أمن التلفزيون القائم على بروتوكول الإنترنت، مع المحافظة في نفس الوقت على الاستعمال الصحيح المخول.

1.IV المقدمة

إن البث الفيديوي الرقمي – حماية المحتوى وإدارة النسخ DVB-CPCM هو نظام لحماية المحتوى وإدارة النسخ للمحتوى التجاري والبث الحر (غير المحفر)، للمحتوى الرقمي الذي يُسلم إلى منتجات المستهلك وإلى الشبكات المنـــزلية. ويقوم نظام حماية المحتوى وإدارة النسخ (CPCM) بإدارة استعمال المحتوى منذ الاستحواذ داخل نظام CPCM وحتى الاستهلاك النهائي أو التصدير من نظام CPCM وذلك طبقاً لقواعد الاستعمال المعينة لمثل هذا المحتوى. والمقصود بالعملية CPCM هو استعمالها لحماية جميع أنماط المحتوى، مثال ذلك التطبيقات السمعية، والفيديوية والتطبيقات المصاحبة والبيانات. ويوفر CPCM المواصفات لتسهيل قابلية التشغيل البيني لمثل هذا المحتوى عقب استحواذه داخل النظام CPCM بواسطة أجهزة المستهلك المترابطة شبكياً لكل من الربط الشبكي المنـــزلي والنفاذ عن بُعْد. وتتألف هذه المواصفة من أجزاء يحدد بعضها التشوير والتدابير اللازمة للمطابقة التقنية، بينما تقوم أجزاء أخرى بشرح السند المنطقي وراء المواصفة، بما في ذلك المبادئ التوجيهية للتنفيذ. ويوفر النموذج المرجعي الإطار لنظام CPCM كما يقوم مقام الأساس الذي تنبني عليه عناصر المواصفة الأخرى.

2.IV التعاريف

يعرف هذا التذييل المصطلحات التالية إضافة إلى المصطلحات المعرفة في المتن الرئيسي:

1.2.IV **يستحوذ**: وتشمل تلَقّى والتِقَام المحتوى من خارج نظام حماية المحتوى وإدارة النسخ CPCM إلى داخل نظام CPCM.

2.2.IV **نقطة استحواذ (AP)**: كيان وظيفي مجرد لحماية المحتوى وإدارة النسخ يتم داخله استحواذ المحتوى.

3.2.IV **الاستحواذ**: تلقى والتقام المحتوى من خارج نظام حماية المحتوى وإدارة النسخ CPCM إلى داخل نظام حماية المحتوى وإدارة النسخ.

4.2.IV **الميدان المُخَول (AD)**: مجموعة قابلة للتمييز من الأجهزة المطابقة للبث الفيديوي الرقمي – حماية المحتوى وإدارة النسخ DVB-CPCM مملوكة لأفراد أسرة واحدة أو مؤجرة أو متحكم فيها من جانبهم، وتعتبر الأسرة هي الوحدة الاجتماعية التي تتألف من جميع الأفراد الذين يعيشون معاً كقاطنين لنفس المسكن (أسرة وليست ثمة خلافات تتعلق بالأماكن المادية للأجهزة المملوكة، أو المؤجرة أو المتحكم فيها من قِبَلْ أفراد هذه الأسرة).

5.2.IV **الاستعمال المخول**: الاستعمال المسموح به لمحتوى CPCM؛ ويتألف من مجموعة من تأكيدات لقاعدة الاستعمال التي تنطبق على مثل هذا المحتوى.

6.2.IV يستهلك: وتشمل بصورة ملموسة استخلاص محتوى أو خَرْج محتوى بحيث لا ينطوي على حظر أي استعمال آخر.

7.2.IV نقطة استهلاك (CP): كيان وظيفي مجرد لحماية المحتوى وإدارة النسخ CPCM يتم داخله الاستهلاك.

8.2.IV الاستهلاك: استخلاص ملموس لمحتوى أو خَرْج جهاز يحتوى على تحويل أو إشارة المقصود منها حَظْر أي استعمال غير التحويل الفوري للمحتوى إلى صوت وصورة.

9.2.IV بند محتوى: حالة منفصلة من محتوى ذي مدة منتهية، مثال ذلك برنامج/حدث أو جزء غير كامل منه.

10.2.IV ترخيص محتوى: بِنْيَة بيانات مُصَانة ومُبَلَّغَة بصورة آمنة، تشمل معلومات ضرورية لإدارة أمن بند محتوى تابع لحماية المحتوى وإدارة النسخ CPCM.

11.2.IV محتوى: البيانات المراد حمايتها بواسطة نظام حماية المحتوى وإدارة النسخ CPCM، وهذا يشير عامة إلى محتوى سمعي مرئي يشتمل على بيانات اختيارية مُصاحبة مثل العناوين الفرعية، والصور/الرسوم البيانية، الصور المتحركة، صفحات الويب، نص، الألعاب، البرمجيات (كلٍ من شفرة المصدر وشفرة الشيء)، النصوص المُعَدَّة للتنفيذ، أو أي معلومات أخرى يراد تسليمها إلى مستعمل واستهلاكها بواسطته.

12.2.IV النسخ Copy: عملية مدارة بواسطة حماية المحتوى وإدارة النسخ ينشأ أثناءها بند محتوى جديد مُخَزَّن من محتوى تم استحواذه أو من بند محتوى موجود ومُخَزَّن.

13.2.IV جهاز حماية المحتوى وإدارة النسخ CPCM device: وهو جهاز يأوي حالة أو أكثر من حالات حماية المحتوى وإدارة النسخ.

14.2.IV نظام حماية المحتوى وإدارة النَسْخ CPCM system: وهو مجموعة تتكون من جميع أجهزة CPCM المطابقة.

15.2.IV تطبيق الجهاز Device application: أي عُنْصر وظيفي غير مطابق لحماية المحتوى وإدارة النسخ NON-CPCM موجود داخل جهاز نظام حماية المحتوى وإدارة النَسْخْ CPCM.

16.2.IV نقطة تصدير (EP): كيان وظيفي مجرد لحماية المحتوى وإدارة النسخ CPCM وفيه يغادر محتوى CPCM نظام CPCM.

17.2.IV تصدير Export: الإفراج عن محتوى CPCM من الحماية والإدارة الصريحتين لنظام CPCM إلى نظام حماية محتوى متحكم فيه، أو نظام حماية محتوى موثوق فيه أو إلى فضاء غير موثوق فيه.

18.2.IV تحريك Move: عملية عمل نسخة يتم فيها استبعاد الأصل، وشطبه أو وقف إمكانية النفاذ إليه.

19.2.IV خَرْج Output: سطح بيني لجهاز أو نظام حماية محتوى يستعمل لإرسال محتوى CPCM أو محتوى مُسْتَهلَك أو محتوىَ مُصَدِّر.

20.2.IV كيان معالجة (PE): كيان وظيفي مجرد لحماية المحتوى وإدارة النسخ CPCM حيث تجري فيه معالجة محتوى CPCM.

21.2.IV معالجة Processing: عملية مطابقة لنظام CPCM على محتوى مُجَفر أو غير مُجَفر لأغراض خلاف الاستهلاك أو التصدير، مثال ذلك أن يمر محتوى CPCM بعملية تحويل مسموح بها من شكله الأصلي وذلك لخلق محتوى CPCM جديد مُحوّل، أو معلومات كاستخلاص سويات جهارة الصوت المسموع أو الصور الساكنة من المحتوى.

22.2.IV معلومات عن حالة الاستعمال (USI): بيانات شرحية لمحتوى CPCM ترسل إشارات الاستعمال مخول بالنسبة لكل بند من بنود محتوى CPCM.

23.2.IV يشاهد: يستهلك.

ملاحظة: ويشمل هذا أيضاً الاستماع إلى محتوى سمعي فقط.

24.2.IV مشاهدة: استهلاك.

ملاحظة: ويشمل هذا أيضاً الاستماع إلى محتوى سمعي فقط.

3.IV الاختصارات والأسماء المختصرة

يستعمل هذا التذييل الاختصارات التالية إضافة إلى تلك الواردة في المتن الرئيسي:

AD ميدان مُخَول *(Authorized Domain)*

AP نقطة استحواذ *(Acquisition Point)*

APECS استحواذ، معالجة، تصدير، استهلاك، تخزين *(Acquisition, Processing, Export, Consumption, Storage)*

CL ترخيص محتوى *(Content License)*

CP نقطة استهلاك *(Consumption Point)*

CPCM حماية المحتوى وإدارة النسخ *(Content Protection and Copy Management)*

CPE تجهيزات منشآت العمل *(Customer Premise Equipment)*

CPS نظام حماية محتوى *(Content Protection System)*

DVB البث الفيديوي الرقمي *(Digital Video Broadcasting)*

EP نقطة تصدير *(Export Point)*

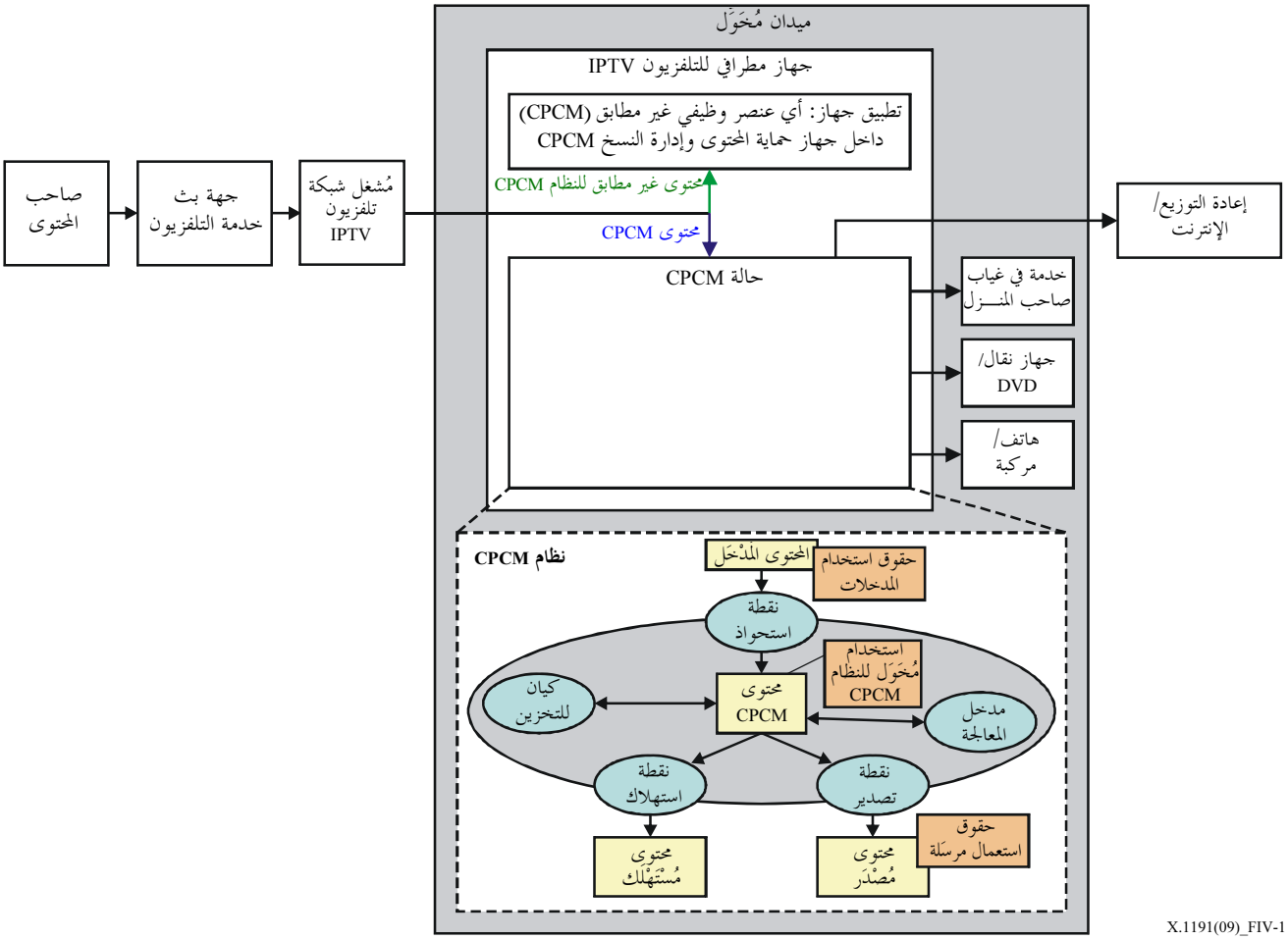
PE كيان معالجة *(Processing Entity)*

SE كيان للتخزين *(Storage Entity)*

USI معلومات حالة الاستعمال *(Usage State Information)*

4.IV معمارية حماية المحتوى وإدارة النسخ CPCM architecture

يقع "الميدان المخول" في قلب حماية المحتوى وإدارة النسخ، وهو مجموعة من الأجهزة التي تتبع أسرة حتى عندما يكون أفرادها بعيدين عن البيت. ويُسَلِم مفهوم "الميدان المخول" بأن ربط المحتوى بجهاز واحد لفك التشفير (جهاز مطرافي)، وعرض تلفزيوني مُلحق ليس بكاف في عصر الترفيه المترابط شبكياً. وتأخذ حماية المحتوى وإدارة النسخ للمحتوى المحتوى من مصدر موثوق به لنظام حماية الخدمة والمحتوى للتلفزيون القائم على بروتوكول الإنترنت وذلك كتجسيد للجهاز المطرافي أو كجزء منه، وتقوم بحماية قطار أو ملف المحتوى المُستَلَم، وتدير كيفية إمكانية مشاهدته، ونقله ونسخه. أما محتوى الدخل "INPUT CONTENT"، بصفته نموذج إدارة محتوى حماية المحتوى وإدارة النسخ "CPCM" فهو يدخل نظام CPCM ليصبح محتوى CPCM. ويدار محتوى CPCM ويُحمى داخل نظام CPCM، وهو يغادر نظام CPCM هذا باستهلاك المستعمل له أو بتصديره إلى نظام آخر.



الشكل 1.IV - تدفق المحتوى في بيئة نظام حماية المحتوى وإدارة النسخ CPCM

يدعم نظام حماية المحتوى وإدارة النسخ مجموعة متنوعة من استعمالات المحتوى الموجودة على شبكة منـــزلية؛ ويمكنه كذلك أن يدير النفاذ إلى محتوى وارد من مواقع نائية مثل الحاسوب المحمول (Laptop) على وصلة إنترنت واسعة المجال. إن مزودي الخدمات يمكنهم باستعمال النظام CPCM أن يبعثوا بإشاراتهم إلى مُصَنِعِي الأجهزة بالمسارات المتصورة (السيناريوهات) المسموح بها لكل نمط من أنماط المحتوى. وهذا يوسع نطاق الكثير من طرق الحماية المعروفة اليوم كتلك المتجسدة في تكنولوجيا حماية الخدمة والمحتوى للتلفزيون القائم على بروتوكول الإنترنت حيث المحتوى يكون مقصوراً عادة على كابل توصيل بيني من نقطة إلى نقطة فيما بين جهاز مصدر المحتوى (مثل وحدة فك التشفير) وجهاز العرض الرقمي.

ويتجاوز نظام حماية المحتوى وإدارة النسخ CPCM حدود الحماية المُحددة الموقع، فيعطي لجهات البث، ومشغلي الشبكة، وملاك المحتوى خيار السماح لأفراد الأسرة بالنفاذ من مكان ناءٍ كالفندق أثناء رحلة عمل أو إجازة.

ويمكن لنظام حماية المحتوى وإدارة النسخ أيضاً أن يسمح للمستعملين باستنساخ محتوى إلى أجهزة نقالة، وإلى تخزين قابل للنقل مثل الأقراص DVD مثلاً. ومادام جهاز إعادة العرض يتبع نفس الميدان المُخَول، فإن الجهاز سيكون قادراً على إعادة عرض المحتوى حتى وإن كان مفصولاً عن المترل وعن مُوَرِد الخدمة الأصلي. ولا يحتاج محتوى CPCM إلى أي تخويل على الخط من مورد الخدمة لإضافة أو إزالة أجهزة إلى/من الميدان المخول.

ونظام حماية المحتوى CPCM ليس كياناً منفصلاً وقائماً بذاته بل هو مدمج/داخل في نظام التوزيع الكلي طرف – إلى طرف لحماية الخدمة والمحتوى للتلفزيون القائم على بروتوكول الإنترنت. وهو على حالته هذه؛ يتعايش مع، بدلاً من أن يحل محل، نظام لحماية الخدمة والمحتوى للتلفزيون القائم على بروتوكول الإنترنت. ففي أي جهاز مطرافي تكون المطابقة مع النظام CPCM اختيارية؛ ومع ذلك فإنها إذا لم تكن موجودة، فلن تُمنح النفاذ إلى أي محتوى محمي بنظام CPCM. ومع هذا، فإن

الجهاز المطرافي ليس بحاجة لأن يُنفِذ جميع عناصر النظام CPCM. وأن العناصر المفيدة للجهاز المطرافي هي وحدها المطلوب منها أداء العنصر الوظيفي الذي تحتاج إليه. فمثلاً، يمكن لجهاز بسيط أن ينفذ فقط العناصر الوظيفية للاستحواذ والاستهلاك الخاصة بحماية المحتوى وإدارة النسخ CPCM إذا لم تكن تتوافر له متطلبات خزن النظام CPCM أو تصديره.

5.IV النموذج المرجعي والكيانات الوظيفية للنظام CPCM

يُعرَّف النموذج المرجعي لحماية المحتوى وإدارة النسخ CPCM مجموعة من خمسة وظائف مجردة لإدارة المحتوى تغطي جميع سيناريوهات استعمال المحتوى ذات الصلة داخل بيئة المستهلك ألا وهي: الاستحواذ، والتخزين، والمعالجة والاستهلاك والتصدير. وهذه الوظائف تقابل الكيانات الوظيفية الخمسة للنظام CPCM ألا وهي نقطة الاستحواذ، كيان التخزين، كيان المعالجة، نقطة الاستهلاك ونقطة التصدير. ويلقي الشكل VI-1 نظرة على نظام CPCM من منظور مجموعة الكيانات الوظيفية المجردة.

وهكذا، فإن المحتوى المدخل الداخل إلى نظام حماية المحتوى وإدارة النسخ CPCM يفعل ذلك من خلال استحواذه لدى نقطة الاستحواذ هذه بواسطة جهازCPCM ينفذ نقطة الاستحواذ هذه لكي تصبح محتوىCPCM ويمكن لمحتوى CPCM أن يُخزَن أو يعالج بواسطة الكيانين الوظيفيين المقابلين (كيان التخزين، كيان المعالجة) المنفَّذَيْن على جهاز CPCM. ويغادر محتوى CPCM نظام حماية المحتوى وإدارة النسخ CPCM عندما يُستَهلَك في نقطة استهلاك أو يصدر من عند نقطة تصدير. ومرة أخرى، يمكن لهذه الكيانات الوظيفية أن تُنَفَذْ داخل أي جهاز تابع لحماية المحتوى وإدارة النسخ CPCM.

6.IV الميدان المخول التابع لحماية المحتوى وإدارة النسخ CPCM

يمكن تجميع أجهزة حماية المحتوى وإدارة النسخ منطقياً داخل ميادين مخولة.. فإذا كانت كل تلك الأجهزة تنتمي إلى أسرة واحدة، فإنها تُشَكِلُ عندئذ الميدان المخول لتلك الأسرة. وهكذا، يوفر الميدان المخول مقصداً للمحتوى الذي يقابل حدود أسرة واحدة. ويمكن، بصفة عامة، النظر إلى الميدان المخول على اعتبار أنه التجميع المنطقي لجميع أجهزة حماية المحتوى وإدارة النسخ CPCM التابعة لأسرة واحدة، أي الأجهزة الموجودة مكانياً في نفس المسكن الرئيسي والأجهزة الموجودة مكانياً في مسكن آخر (مثال المسكن أثناء إجازة) والأجهزة النقالة المحمولة يدوياً التي تتصل فقط بصورة متقطعة بالأجهزة الثابتة آنفة الذكر، أو الأجهزة المثبَّتة في مَرْكَبَة (مركبات) وتابعة لنفس الأسرة. وقد صُمِمَ الميدان المخول (AD) لكي يكون مجموعة منطقية من الأجهزة المستقلة ذاتياً، وهو لا يحتاج إلى أي إدارة خارجية. ولاحظ، مع ذلك، أنه قد توجد حالات يكون الميدان المخول (AD) فيها موصولاً بمُزَوِد خدمة معين قد يعرض القيام بإدارة الميدان المخول (AD) كجزء من الخدمات التي يزود المستهلك بها.

7.IV قواعد استعمال محتوى CPCM

إن الاستعمال المخول لأي بند من بنود محتوى CPCM هو مجموعة التأكيدات الخاصة بالاستعمال المعبر عنها في قواعد استعمال النظام CPCM المُلحقة بالمحتوى. وقد تقع مسؤولية وضع قواعد استعمال النظام CPCM على كاهل مورد المحتوى أو الخدمة أو تم تقابلها من شكل التسليم (مثل البث الحر غير المقيد). وقد يخضع نطاق عمليات التخزين والاستهلاك والتصدير لحدود الاستعمال المخول للمحتوى. ويحدد النظام CPCM مجموعة مشتركة من قواعد الاستعمال يمكن لأي مزود محتوى أن يختار من بينها، وأن يشتق الاستعمال المُخَوَّل المرغوب فيه بالنسبة للمحتوى في إطار نظام CPCM تبعاً لذلك. وقد صممت مجموعة قواعد استعمال النظام CPCM بحيث تكون مرنة بالقدر الذي يكفي ليغطي جميع نماذج حماية المحتوى والإدارة المطابقة، وبحيث تكون دقيقة بالقدر الذي يكفي للإبقاء على نماذج استعمال محتوى واضحة وبسيطة نسبياً للمستهلك.

8.IV البيانات الشرحية لمعلومات حالة الاستعمال

يُشَفَّر الاستعمال المخول لبند محتوى ما على هيئة بيانات شرحية للمحتوى CPCM تسمى معلومات حالة الاستعمال (USI). وتتم إدارة وحماية المحتوى طبقاً لمعلومات حالة الاستعمال USI التي تطبق على كل بند محتوى.. وباستثناء عمليات انتقال معلومات حالة الاستعمال المطابقة التي تجرى ضمنياً بواسطة نظام CPCM، يمكن للكيانات التي لديها تخويل قانوني بالنسبة للمحتوى داخل إطار نظام حماية المحتوى وإدارة النسخ CPCM أن تُنَفِّذ تغييرات أخرى على المعلومات حالة USI الخاصة ببند من بنود المحتوى وذلك بعد استحواذه داخل نظام CPCM.

9.IV محتوى CPCM

يشير لفظ "محتوى" عادة إلى محتوى سمعي مرئي بالإضافة إلى بيانات اختيارية مصاحبة كالعناوين الفرعية، الصور/الرسوم البيانية، الصور المتحركة، صفحات الويب، النص، الألعاب، البرمجيات (كل من شفرة المصدر وشفرة الشيء)، النصوص المكتوبة المُعَدَّة للتنفيذ، أو أي معلومات أخرى يراد تسليمها إلى مُستَعمِلْ أو تستهلكَ بواسطته. ومحتوى CPCM هو محتوى محمٍ ومدارٌ بواسطة نظام حماية المحتوى وإدارة النسخ CPCM وطبقاً لقواعده. وبند المحتوى هو جزء منفصل من المحتوى ذو فترةٍ محددة. وكل بند محتوي CPCM يكون مصحوباً بترخيص محتوى يحمل معلومات حالة الاستعمال المصاحبة إلى جانب المزيد من البيانات الشرحية لحماية المحتوى وإدارة النسخ. ويستطيع نظام CPCM أن يتناول ترخيص المحتوى وبند المحتوى ذاته بطرق مختلفة تبعاً للعنصر الوظيفي المقصود و/أو إنفاذ قواعد الاستعمال بالصورة التي تتطلبها معلومات حالة الاستعمال.

10.IV جهاز حماية المحتوى وإدارة النسخ CPCM

جهاز حماية المحتوى وإدارة النسخ هو جهاز يُنَفِذْ أي عنصر وظيفي للنظام CPCM بصورة مطابقة. ويشار إلى تنفيذ العنصر الوظيفي للنظام CPCM على أنه نظام لحماية المحتوى وإدارة النسخ. وجهاز CPCM هو جهاز يأوي واحداً أو أكثر من الآليات التنفيذية لحماية المحتوى وإدارة النسخ. وهو يمكن أيضاً أن يشتمل على وظائف أخرى غير مطابقة للنظام CPCM وذلك بالإضافة إلى عنصره الوظيفي الخاص بحماية المحتوى وإدارة النسخ. وتتم مناولة CPCM فقط بواسطة الآلية التنفيذية للنظام CPCM داخل الجهاز. أما الجزء من الجهاز غير المنتمي للنظام CPCM فليس له منفذ إلى محتوى CPCM. ويمكن للجهاز التابع للنظام CPCM أن يأوي العنصر الوظيفي الآمن غير التابع لحماية المحتوى وإدارة النسخ CPCM من أجل استحواذ المحتوى من نظم حماية أخرى أو من أجل التصدير الآمن (أو ربما الاستهلاك) لمحتوى CPCM.

11.IV قواعد الاستعمال ومعلومات حالة الاستعمال

إن قاعدة الاستعمال في جهاز حماية المحتوى وإدارة النسخ هي عملية أو سلوك معينين للمحتوى المراد التحكم فيه داخل نطاق نظام حماية المحتوى وإدارة النسخ. ويشار إلى المجموعة الكاملة لتأكيدات قواعد الاستعمال لبند معين من بنود محتوى CPCM على أنها الاستعمال المخوّل لمثل هذا البند التابع للنظام CPCM. ويتم التعبير عن الاستعمال المخول لأحد بنود المحتوى باستعمال شفرته في معلومات حالة الاستعمال (USI)، وبالبيانات الشرحية لمحتوى CPCM التي تؤشر للاستعمال المخول لذلك المحتوى بصفة خاصة.

التذييل V

مخطط التحويل الشفري الآمن

(لا يشكل هذا التذييل جزءاً أساسياً من هذه التوصية)

1.V نظرة عامة على مخطط التحويل الشفري الآمن

اجتذب التحويل الشفري للمحتوى قدراً كبيراً من الانتباه نظراً لتزايد شعبية أنماط متعددة من الأجهزة مثل المساعد الشخصي الرقمي PDA، والأجهزة من غير أجهزة الحاسوب الشخصي، والهواتف الخليوية، والمطراف المتنقل الذكي. ويشير التحويل الشفري إلى عملية تحويل محتوى متعدد الوسائط كالصور، والنص، والمواد السمعية والمرئية من نسق أصلي إلى نسق مختلف أو إلى جودة مختلفة.

ويرمي التحويل الشفري إلى تقليل تأخير تحميل المحتوى المتعدد الوسائط على وصلات نفاذ ذات عرض نطاق منخفض، مثل وصلات المودم، ووصلات النفاذ اللاسلكية، وإلى القضاء على التنافر بين نسق التشفير المعزز بجهاز عميل وبين النسق الذي يستخدمه مزود محتوى متعدد الوسائط. وهو يسمح أيضاً لمطراف التقييد الحسابي بإظهار المحتوى مشفراً على أساس قدرات التحويل الشفري.

توجد هناك كيانات ثلاثة لمخطط التحويل الشفري الآمن هي: مُرسِل، وعقدة شبكة وسيطة، ومستعمل لديه مطراف التلفزيون القائم على بروتوكول الإنترنت IPTV . وتوجد وظيفة التحويل الشفري داخل عقدة وسيطة بالشبكة تقع بين مورد المحتوى وجهاز العميل. وهناك نوعان من معماريات التحويل الشفري هما: معمارية التحويل الشفري التقليدية ومعمارية التحويل الشفري المؤمنة.

ففي معمارية التحويل الشفري التقليدية يستعمل وكيل تحويل شفري كعقدة شبكة وسيطة بين مخدم المحتوى وجهاز عميل. ويقوم المرسل بتجفير المحتوى بانضغاط كافٍ ثم إرسال المحتوى المُجَفَّر إلى عقدة الشبكة الوسيطة التي تسمى وكيل التحويل الشفري، ويقوم وكيل التحويل الشفري بإزالة تجفير المحتوى، مع إزالة الانضغاط. ثم يحول حجم المحتوى أو نَسَقَه بانضغاط جديد، ثم يقوم في النهاية بإعادة تجفير بيانات التحويل الشفري وذلك للإرسال إلى جهاز العميل. ويقوم جهاز العميل بإزالة تجفير المحتوى المجفر، ويزيل انضغاط المحتوى، وذلك باستعمال خوارزمية انضغاط جديدة. لاحظ، مع ذلك، أن هناك مشكلة تتعلق بالأمن تحدث في المحول الشفري بالوكالة، أي أنه بمجرد أن يُزال تجفير المحتوى داخل وكيل التحويل الشفري وقبل أن يتم تجفيره يبقى المحتوى داخل وكيل التحويل الشفري. وبمعنى آخر، أن أي مراقب يستطيع أن ينفذ إلى المحتوى غير المجفر عن طريق التصنت. ومثل هذا المحتوى غير المجفر يضعف الضمان الأمني للخصوصية من طرف – لطرف، حيث أن المرسل والعميل القانوني هما وحدهما اللذان يفترض نفاذهما إلى المحتوى أثناء وجوده في حالة عدم تجفير.

ولحل هذه المشكلة الأمنية، تم اقتراح معمارية التحويل الشفري المؤمنة. ومخطط التحويل الشفري الآمن هو نوع من المخطط الأمني يساعد عقدة الشبكة الوسيطة على إجراء التحويل الشفري بدون إزالة التجفير مع المحافظة في نفس الوقت على الأمن من طرف – إلى – طرف. ويمكن تنفيذ هذا المخطط عن طريق الجمع بين التشفير القابل للتوسع، والتجفير التدريجي، والترزيم. ويؤدي المرسل وظيفة تحويل شفري آمن لإنتاج رزم مشفرة قابلة للزيادة من الفيديو، ويضيف إليها الرأسية غير المجفرة لأجل إرسال المعلومات، وتُقْرأ عقدة الشبكة الوسيطة تلك الرأسية غير المجفرة، وتستعمل المعلومات لتقويم أو استبعاد الرزم الكافية وذلك طبقاً لعملية التحويل الشفري المرجوة، مع قيام مطراف التلفزيون القائم على بروتوكول الإنترنت بإزالة تجفير الرزم المجفرة وفك تشفير رزمة النص الخالص لإنتاج الفيديو.

بيبليوغرافيا

[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*.

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

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

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

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

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

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

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

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

[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>

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

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

سلاسل التوصيات الصادرة عن قطاع تقييس الاتصالات

السلسلة A	تنظيم العمل في قطاع تقييس الاتصالات
السلسلة D	المبادئ العامة للتعريفة
السلسلة E	التشغيل العام للشبكة والخدمة الهاتفية وتشغيل الخدمات والعوامل البشرية
السلسلة F	خدمات الاتصالات غير الهاتفية
السلسلة G	أنظمة الإرسال ووسائطه والأنظمة والشبكات الرقمية
السلسلة H	الأنظمة السمعية المرئية والأنظمة متعددة الوسائط
السلسلة I	الشبكة الرقمية متكاملة الخدمات
السلسلة J	الشبكات الكبلية وإرسال إشارات تلفزيونية وبرامج صوتية وإشارات أخرى متعددة الوسائط
السلسلة K	الحماية من التداخلات
السلسلة L	إنشاء الكبلات وغيرها من عناصر المنشآت الخارجية وتركيبها وحمايتها
السلسلة M	إدارة الاتصالات بما في ذلك شبكة إدارة الاتصالات (TMN) وصيانة الشبكات
السلسلة N	الصيانة: الدارات الدولية لإرسال البرامج الإذاعية الصوتية والتلفزيونية
السلسلة O	مواصفات تجهيزات القياس
السلسلة P	نوعية الإرسال الهاتفي والمنشآت الهاتفية وشبكات الخطوط المحلية
السلسلة Q	التبديل والتشوير
السلسلة R	الإرسال البرقي
السلسلة S	التجهيزات المطرافية للخدمات البرقية
السلسلة T	المطاريف الخاصة بالخدمات التلماتية
السلسلة U	التبديل البرقي
السلسلة V	اتصالات البيانات على الشبكة الهاتفية
السلسلة X	**شبكات البيانات والاتصالات بين الأنظمة المفتوحة ومسائل الأمن**
السلسلة Y	البنية التحتية العالمية للمعلومات وملامح بروتوكول الإنترنت وشبكات الجيل التالي
السلسلة Z	اللغات والجوانب العامة للبرمجيات في أنظمة الاتصالات

طُبعت في سويسرا
جنيف، 2009