الاتحاد الدولي للاتصالات

ITU-R

قطاع الاتصالات الراديوية في الاتحاد الدولي للاتصالات

التوصيـــة ITU-R BT.1852

(2009/09)

أنظمة النفاذ المشروط فيما يتعلق بالإذاعة الرقمية

السلسلة BT

الخدمة الإذاعية (التلفزيونية)

الاتحاد الدولي للاتصالات ITU

تمهيـــد

يضطلع قطاع الاتصالات الراديوية بدور يتمثل في تأمين الترشيد والإنصاف والفعالية والاقتصاد في استعمال طيف الترددات الراديوية في جميع خدمات الاتصالات الراديوية، بما فيها الخدمات الساتلية، وإجراء دراسات دون تحديد لمدى الترددات، تكون أساساً لإعداد التوصيات واعتمادها.

ويؤدي قطاع الاتصالات الراديوية وظائفه التنظيمية والسياساتية من خلال المؤتمرات العالمية والإقليمية للاتصالات الراديوية وجمعيات الاتصالات الراديوية بمساعدة لجان الدراسات.

سياسة قطاع الاتصالات الراديوية بشأن حقوق الملكية الفكرية (IPR)

يرد وصف للسياسة التي يتبعها قطاع الاتصالات الراديوية فيما يتعلق بحقوق الملكية الفكرية في سياسة البراءات المشتركة بين قطاع تقييس الاتصالات وقطاع الاتصالات الراديوية والمنظمة الدولية للتوحيد القياسي واللجنة الكهرتقنية الدولية (ITU-T/ITU-R/ISO/IEC) والمشار إليها في الملحق 1 بالقرار ITU-R 1. وترد الاستمارات التي ينبغي لحاملي البراءات استعمالها لتقديم بيان عن البراءات أو للتصريح عن منح رخص في الموقع الإلكتروني http://www.itu.int/ITU-R/go/patents/en حيث يمكن أيضاً الاطلاع على المبادئ التوجيهية الخاصة بتطبيق سياسة البراءات المشتركة وعلى قاعدة بيانات قطاع الاتصالات الراديوية التي تتضمن معلومات عن البراءات.

سلاسل توصيات قطاع الاتصالات الراديوية

(يمكن الاطلاع عليها أيضاً في الموقع الإلكتروني http://www.itu.int/publ/R-REC/en)

السلسلة	العنـــوان
BO	البث الساتلي
BR	التسجيل من أجل الإنتاج والأرشفة والعرض؛ الأفلام التلفزيونية
BS	الخدمة الإذاعية (الصوتية)
BT	**الخدمة الإذاعية (التلفزيونية)**
F	الخدمة الثابتة
M	الخدمة المتنقلة وخدمة التحديد الراديوي للموقع وخدمة الهواة والخدمات الساتلية ذات الصلة
P	انتشار الموجات الراديوية
RA	علم الفلك الراديوي
S	الخدمة الثابتة الساتلية
RS	أنظمة الاستشعار عن بعد
SA	التطبيقات الفضائية والأرصاد الجوية
SF	تقاسم الترددات والتنسيق بين أنظمة الخدمة الثابتة الساتلية والخدمة الثابتة
SM	إدارة الطيف
SNG	التجميع الساتلي للأخبار
TF	إرسالات الترددات المعيارية وإشارات التوقيت
V	المفردات والمواضيع ذات الصلة

ملاحظة: *تمت الموافقة على النسخة الإنكليزية لهذه التوصية الصادرة عن قطاع الاتصالات الراديوية بموجب الإجراء الموضح في القرار ITU-R 1.*

النشر الإلكتروني
جنيف، 2010

التوصيـــة ITU-R BT.1852

أنظمة النفاذ المشروط فيما يتعلق بالإذاعة الرقمية

(المسألة ITU-R 49/6)

(2009)

مجال التطبيق

تصف هذه التوصية المبادئ الرامية لتسهيل تطوير طرائق فعالة للنفاذ المشروط فيما يتعلق بالإذاعة الرقمية التي تستعمل تدفقات نقل MPEG-2. وهي توفر معلومات عن الحماية الموثوقة للخدمات الإذاعية من النفاذ غير المخوَّل.

إن جمعية الاتصالات الراديوية للاتحاد الدولي للاتصالات،

إذ تضع في اعتبارها

أ) أن هناك طلباً متزايداً في العديد من البلدان على حماية البرامج المذاعة من الاستقبال غير المخوَّل؛

ب) أن السبيل الفعال لضمان هذه الحماية لرزم تدفق نقل MPEG-2، المتعددة الإرسال وفقاً لتوصية قطاع تقييس الاتصالات H.222.0، يتمثل في تنفيذ أنظمة إذاعية ذات نفاذ مشروط؛

ج) أن أمثلة عن أنظمة النفاذ المشروط قد صُممت وشُغلت في التلفزيون الرقمي للأرض وتلفزيون الكبل الرقمي وتلفزيون بروتوكول الإنترنت (IP)، وكذلك في خدمات الصوت والوسائط المتعددة والبيانات؛

د) أن هناك حالات عديدة من تنفيذ أنظمة الإذاعة الرقمية القائمة على التوصيات ذات الصلة من سلسلتي BT وBO، مثل توصية قطاع الاتصالات الراديوية BO.1516 لأنظمة الإذاعة الرقمية الساتلية؛

هـ) أن من المرغوب فيه الحد من عدد الأنظمة المختلفة للنفاذ المشروط، مع الأخذ في الحسبان المتطلبات المختلفة لمختلف الخدمات الإذاعية وأنظمة الإرسال؛

و) أن وضع أكبر عدد ممكن من العناصر المشتركة للنفاذ المشروط في أجهزة الاستقبال في البداية من شأنه أن يعطي عامة الجمهور أوفر إمكانية للنفاذ إلى خدمات محمية بتكلفة مخفضة للمعدات؛

ز) أن أنظمة النفاذ المشروط توفر حماية؛ وأن أصحاب حقوق التأليف والنشر، وموردي البرامج وموردي الخدمات يرغبون بشبكات إذاعة/توزيع تتمتع بأمان عال للسماح بحماية برامجهم من خلال التحكم في النفاذ،

توصـــي

1 بأن أنظمة النفاذ المشروط لخدمات الإذاعة الرقمية التي تحمي رزم تدفق نقل MPEG-2 ينبغي لها أن:

- تقدم خدمات متاحة لأجهزة الاستقبال المخولة فقط؛
- وأن تضم في جهاز الاستقبال أكبر عدد من العناصر المشتركة؛
- وأن تُصمم وفقاً للمبادئ الأساسية في الملحق 1.

الملاحظة 1 – ترد في التذييل 1 أمثلة عن تطبيقات أنظمة النفاذ المشروط فيما يتعلق بالإذاعة الرقمية.

الملحق 1

المبادئ الأساسية لتصميم أنظمة النفاذ المشروط فيما يتعلق بالإذاعة الرقمية

1 مقدمة

ينبغي للمبادئ المبينة في هذا الملحق أن تسهل تطوير أنظمة فعالة للنفاذ المشروط فيما يتعلق بالإذاعة الرقمية القائمة على تدفق النقل وفقاً لتوصية قطاع تقييس الاتصالات H.222.0 (تدفق نقل MPEG-2) – أنظمة تناسب المشتركين ومورّدي الخدمة على السواء وتضمن الحماية الموثوقة للمعلومات من النفاذ غير المخوَّل.

وتسري المبادئ عموماً على تسليم خدمات التلفزيون الرقمي والخدمات الصوتية، فضلاً عن خدمات الإذاعة متعددة الوسائط وإذاعة البيانات. وتسري هذا المبادئ على تسليم رزمة تدفق النقل وفقاً لتوصية قطاع تقييس الاتصالات H.222.0 إلى مستهلكين عبر مختلف الوسائط، مثل الإذاعة الرقمية للأرض، وإذاعة الكبل الرقمي والساتل الرقمي، والإذاعة التي تستخدم بروتوكول الإنترنت (IP).

2 المراجع

1.2 المراجع المعيارية

توصية قطاع تقييس الاتصالات H.222.0: تكنولوجيا المعلومات – تشفير تنوعي للصور المتحركة والمعلومات السمعية المصاحبة: الأنظمة

2.2 المراجع الإعلامية

التوصية ITU-R BT.810: أنظمة الإذاعة ذات النفاذ المشروط

معيار رابطة الصناعات ومشاريع الأعمال الراديوية–B25 (ARIB STD-B25): مواصفات نظام النفاذ المشروط فيما يتعلق بالإذاعة الرقمية

معيار اللجنة الكهرتقنية الدولية 62455 (IEC 62455): النفاذ إلى الخدمة القائم على بروتوكول الإنترنت (IP) وتدفق النقل (TS).

3 المصطلحات والتعاريف والمختصرات

1.3 المصطلحات والتعاريف

التخليط في الإذاعة الرقمية

تجفير محتوى الإذاعة بما فيه المواد المرئية والصوتية والبيانات لمنع الاستقبال غير المخول للمعلومات في نسق غير مجفّر. وهذا التجفير هو عملية موصّفة تقع تحت مراقبة نظام النفاذ المشروط (الطرف المرسل).

إزالة التخليط في الإذاعة الرقمية

تجفير محتوى الإذاعة بما في ذلك المواد المرئية والصوتية والبيانات للسماح باستقبال المعلومات في نسق غير مجفّر. وفك التجفير هذا هو عملية موصّفة تقع تحت مراقبة نظام النفاذ المشروط (الطرف المستقبِل).

النفاذ المشروط

ينفُذ المستعمل إلى خدمة محمية بالتفاعل عبر وظائفية النفاذ المشروط في جهاز الاستقبال. فإذا استوفيت جميع شروط النفاذ في الجلسة، يتم التخويل، ويُحرَر مفتاح التجفير، ويُستعاد المحتوى.

ومن شأن استيقان المشترك أو تأكيد الحساب أو التحقق من تيسّر الخدمة أو غير ذلك من معلمات التحكم في البرنامج أن يفعّلوا مفتاح تجفير/إزالة تجفير الدورة للسماح لها باختتام عملية التخويل.

التحكم في النفاذ المشروط

إن وظيفة التحكم في النفاذ المشروط في الطرف المرسل هي إنتاج معلومات التحكم في التخليط و"مفاتيح" التجفير المصاحبة للخدمة.

أما وظيفة التحكم في النفاذ المشروط في الطرف المستقبِل فهي إنتاج معلومات التحكم في إزالة التخليط إلى جانب "المفاتيح" المصاحبة للخدمة.

التجفير وفك التجفير

يُستعمل هذان المصطلحان للدلالة على الطرائق المستعمَلة لحماية (وتأويل) بعض المعلومات ضمن "رسائل على صلة بالنفاذ" يتعين إرسالها من الطرف المرسل إلى الطرف المستقبِل في وظائف التحكم في النفاذ المشروط.

نقطة المنشأ

في نظام توزيع، هذه هي النقطة التي يصبح فيها برنامج أو محتوى آخر، لأول مرة، إشارة في نسقها الإذاعي/التوزيعي النهائي. وهي تمثل بدء الحماية من طرف إلى طرف. ويمكن لمحتوى الدخول أن يأخذ أي شكل، وليس بالضرورة شكلاً محسوساً بشرياً. ولا حاجة بمدخل المحتوى نفسه لأن يكون مفهوماً.

الملاحظة 1 – يشكل أصحاب حقوق التأليف والنشر، وموردو الخدمة والموزعون تراتبية ضخمة من العديد من نقاط المنشأ في انسياب المعلومات إلى مستهلك، ومن ثم في انسياب المحتوى المخلّط والمفاتيح المجفرة إلى مستهلك. ويجب أن تبدأ نقط المنشأ بصاحب التأليف والنشر أو بالمنتج. وفي الممارسة العملية، ستكون غالبية نقاط المنشأ مجرد نقاط دخول أينما صادف وجودها في النظام لدواعي تجارية وتشغيلية. وفيما قد تتعدد نقاط الدخول هذه فإن كل منها نقطة متفردة ومستقلة يمكن الحفاظ على اطراد المعلومات التي تمر عبرها أيما كان النسق الذي تُدخل فيه حتى تصل إلى المستهلك.

نقطة العرض

هي النقطة التي يظهر فيها برنامج أو محتوى آخر، للمرة الأخيرة، كإشارة في نظام توزيع قبل أن تتخذ شكلاً محسوساً بشرياً على شاشة ومجهار جهاز استقبال. وهي تمثل الخرج من الحماية.

المحتوى

هو أي شكل من البيانات الرقمية التي يمكن لجهاز حيازتها وعرضها.

الخدمة

هي واحد أو أكثر من انسيابات البيانات التي يراد عرضها معاً.

حماية الخدمة

هي حماية خدمة بحيث لا يمكن إلا للأجهزة المخولة استقبالها وفك تشفيرها.

2.3 المختصرات

Ks مفتاح التخليط (*Scrambling key*)

Kw مفتاح العمل (*Work key*)

Km المفتاح الرئيسي (*Master key*)

EMM رسالة إدارة الأحقية (*Entitlement management message*)

ECM رسالة مراقبة الأحقية (*Entitlement control message*)

CRC التحقق من الإطناب الدوري (*Cyclic redundancy check*)

DES معيار تجفير البيانات (*Data encryption standard*)

4 وصف عام لنظام النفاذ المشروط

تشمل أنظمة النفاذ المشروط وظيفتين أساسيتين فيما يتعلق بالإذاعة الرقمية: التخليط والتحكم في النفاذ. وهما مكونان متمايزان، وفي حالات كثيرة مستقلان، في نظام النفاذ المشروط. ويمثل كل منهما عملية معلومات متمايزة.

1.4 النموذج المرجعي

يتطلب النفاذ المشروط تخليط المعلومات قبل إذاعتها. وتتم هذه العملية بالتجفير لإذاعة تدفق بتات.

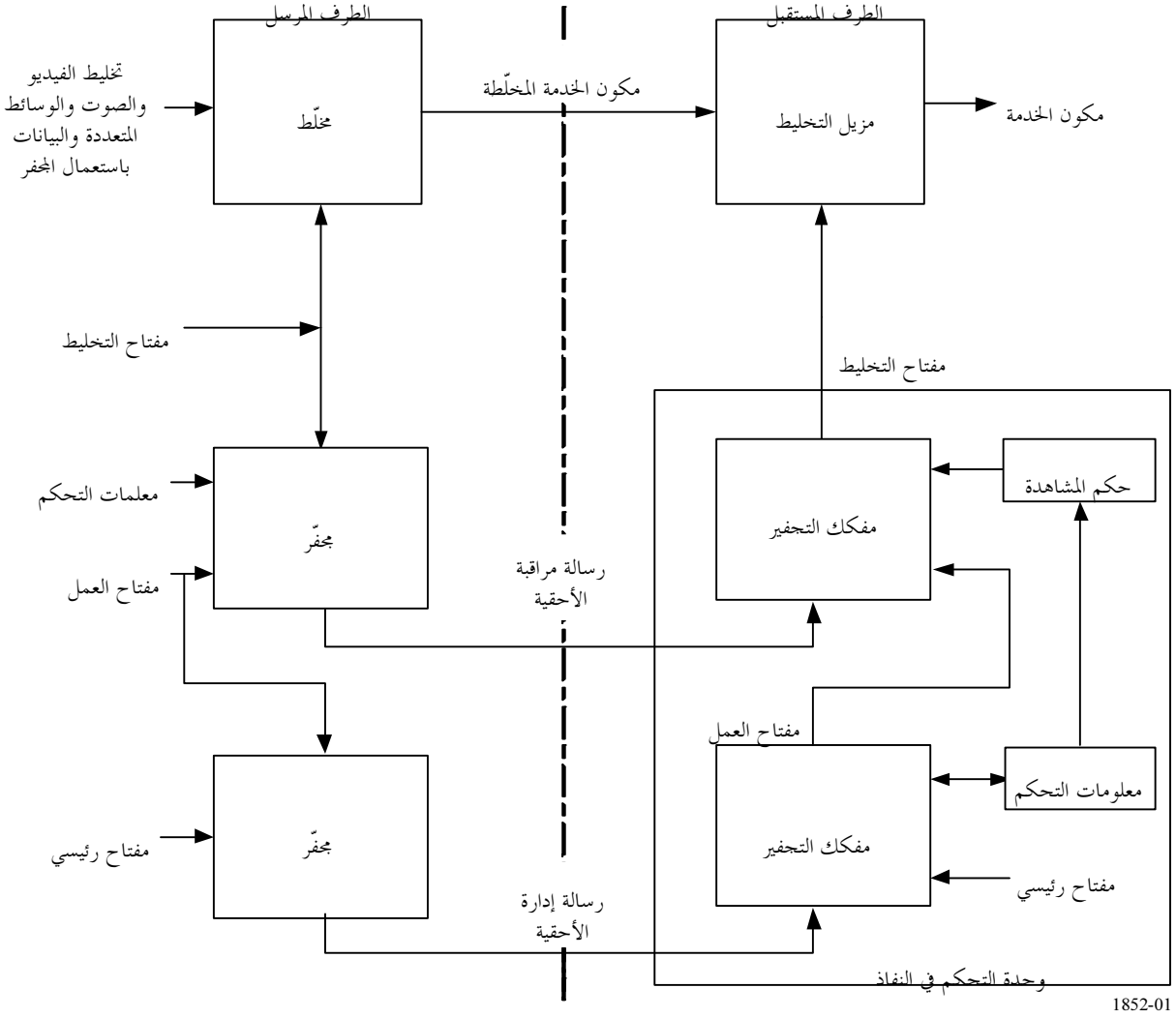
وتتطلب عملية إزالة التخليط عند الطرف المستقبل التجفير نفسه (إجراء إزالة التخليط في هذه الحالة) لاستعادة تدفق البتات الأصلي.

فلتوفير هذا التتابع ولضمان التزامن بين عمليتي الإرسال والاستقبال، يجري التحكم في شروط التجفير ببيانات يرسلها المجفر إلى مفكك التجفير وفقاً لبروتوكول خاص.

وترد البنية المفصلة لهذه العملية في الشكل 1.

الشـــكل 1

مثال مخطط وظيفي لنظام النفاذ المشروط فيما يتعلق بالإذاعة الرقمية



2.4 التخليط

هو عملية حماية بعض أو جميع مكونات خدمة للتعامل مع محاولات النفاذ غير المخول باستعمال التجفير تحت مراقبة نظام النفاذ المشروط لدى الطرف المرسل.

3.4 التحكم في النفاذ

هو تقديم المعلومات لتمكين المستعملين المخولين من إزالة تخليط الخدمة المحمية. ويتحكم نظام النفاذ المشروط بتوفر هذه المعلومات.

وبين المرسل والمستقبل (أو المستقبلات)، يُنظَّم هيكل هذه المعلومات في رسائل خاصة يمكن أن تكون مادةً لإرسال متعدد ضمن تدفق البتات المذاع نفسه، أو يمكن إيصالها بوسائل أخرى – عبر خط اتصالات مثلاً.

وفي الطرف المستقبل (أو الأطراف المستقبلة)، يتولى نظام التحكم في النفاذ تأويل هذه الرسائل للتحكم في إزالة التخليط عن الأجزاء المخولة من تدفق البتات المستقبَل في جهاز الاستقبال المخول (أو أجهزة الاستقبال المخولة).

5 متطلبات المستعمل

1.5 مناعة التجفير ضد الاختراق فيما يتعلق بالتخليط وإزالة التخليط

ينبغي أن تخضع فدرات المخلّط ومزيل التخليط لاختبار القدرة على مكافحة الاختراق. ويوصى بانتقاء تجفير من المعايير الدولية.

2.5 الأمن

يقاس أمن النظام بدرجة الصعوبة التي يواجهها مستعمل غير مخول لدى محاولته النفاذ إلى الخدمة المحمية.

- *إزالة تخليط الإشارة دون الرجوع إلى عملية التحكم في النفاذ*. وهذا مرهون بطبيعة الخدمات وطريقة التخليط. إذ يرجح أن تكون خدمات إذاعة التلفزيون والصوت والبيانات ذات طبيعة رقمية في أغلبها مما سيتيح عمليات تخليط على جانب كبير من الأمان.
- الحصول على مفتاح التحكم بالنفاذ على نحو غير مخول. وهذا مرهون بأمن خوارزميات تجفير المفتاح.

3.5 انتقاء خوارزمية تخليط مشتركة أو خاصة

يتاح النفاذ لأي مستعمل مخول يستوفي شروط النفاذ عبر خوارزمية تخليط مشتركة (شاملة) أو خاصة.

ويعني استعمال خوارزمية تخليط مشتركة ضمناً أن إزالة التخليط ستكون مشتركة بين جميع أجهزة الاستقبال على أساس خوارزمية تخليط معيارية مستقلة عن وسائط الإيصال المستعملة ويمكن استخدمها في معدات منخفضة التكلفة ومرنة، ومع ذلك، تتيح المنافسة من خلال تطبيقات خاصة بمورّد الخدمة.

أما استعمال خوارزمية تخليط خاصة فهو يعني ضمناً أن عملية إزالة التخليط لن تنفّذ إلا على أجهزة الاستقبال المزودة بخوارزمية محددة.

4.5 أساليب النفاذ

يمكن لنظام التحكم في النفاذ أن يدعم طائفة من أساليب النفاذ، مثل:

- التوفر لأجل (الاشتراك في الخدمة) – يسري التخويل من موعد البدء إلى حين الانتهاء؛
- بند برنامج أو خدمة (شراء الحدث) – توفر بند خدمة معين، بصرف النظر عما إذا استُعمل بالكامل أم لا؛
- رسم الخدمة (القائم على الإذنة) – يتناسب الرسم أو الائتمان مع مدة الاستعمال و/أو قيمة الخدمة المعنية؛
- البث المجاني على الأثير – الخدمة محمية ولكن النفاذ إليها متاح مجاناً.

ويتعين أن تكون أساليب النفاذ متغيّرة فيما يتعلق بعدة معلمات، مثل:

- الوقت؛
- الشرائح المتنوعة للخدمة؛
- فئات المستعملين المستهدفين.

5.5 تقييس المعدات

توخياً للحد الأقصى من وفورات الحجم في تصنيع معدات الاستقبال، وتبسيطاً للإدارة والصيانة:

- ينبغي تقييس المعدات المشتركة بحيث تلبي أكبر عدد ممكن من خيارات الخدمة؛
- ويتعين على معمارية جهاز الاستقبال للمستهلك أن تدعم متطلبات وظائفية النفاذ المشروط لنظام النفاذ المشروط المختار. وتبعاً للنظام المختار، قد تستلزم الوظائفية دعم ميزات أمنية مدمجة أو قابلة للنزع (مثل البطاقة الذكية).

6.5 إدارة النفاذ

يقوم تعريف النفاذ المشروط على المفهوم الرسمي لأحقية النفاذ الذي يمكن تنفيذه بأشكال مختلفة. فالأحقية تعطي صاحبها تخويلاً بالنفاذ إلى خدمة ذات صلة. وينبغي اجتناب الاستعمال غير الاقتصادي للموارد جراء النفقات العامة للإدارة أو الإرسال.

7.5 تجنب الانقطاعات في الخدمة

ينبغي تجنب الانقطاعات الناجمة عن الاستحواذ الخاطئ أو غير الموثوق على بيانات التحكم في النفاذ.

6 رسائل مراقبة الأحقية (ECM)

توفر رسالة مراقبة الأحقية مفتاح التخليط لإزالة تخليط الخدمة المحمية.

ويُراقَب النفاذ إلى مفتاح التخليط في رسالة مراقبة الأحقية بواسطة الأحقيات أو الحقوق الواردة في رسالة إدارة الأحقية (EMM).

وترد رسالة مراقبة الأحقية نمطياً في التدفق الإذاعي إلى جانب الخدمة المحمية.

وتُغيَّر مفاتيح التخليط بكثرة عادةً للإقلال إلى أدنى حد من الضرر الناتج عن تسرب مفتاح التخليط.

ولكل نظام خصوصيته فيما يتعلق بمحتوى رسالة مراقبة الأحقية.

7 رسائل إدارة الأحقية (EMM)

تتحقق معالجة رسالة إدارة الأحقية من صحة الأحقية اللازمة لإزالة تخليط الخدمة المحمية أو تقدم هذه الأحقية. ويمكن لرسالة إدارة الأحقية أن تحوي مفتاح العمل الذي يوفر تجفير وفك تجفير مفتاح التخليط. وتجفَّر الرسائل و/أو مفاتيح العمل المعنونة إلى فرادى أجهزة الاستقبال. ويمكن للتجفير أن يستعمل المفتاح الرئيسي. ويمكن تخزين المفتاح الرئيسي في جهاز الاستقبال.

وفي أنظمة النفاذ المشروط الخاص بالإذاعة الرقمية، توزَّع رسائل إدارة الأحقية من خلال الإذاعة أو بوسائط أخرى.

- ويُعرف التوزيع من خلال الخدمات الإذاعية "بالعنونة على الهواء". ويمكن خفض وقت الدورة المصاحب لتوزيع المفاتيح على الهواء بتطبيق مبادئ تجفير المفتاح المتقاسَم. كما يمكن توزيع رسائل إدارة الأحقية بوسائط أخرى.
- ويتم التوزيع من خلال الوسائط الأخرى نمطياً عبر توصيلة النقطة إلى نقطة، مما يوفر إجراءً أمنياً إضافياً لضمان نفاذ الأجهزة المستهدفة حصراً إلى الرسائل.

وفيما يلي مثال عن التشغيل:

في حالة الدفع نظير كل وحدة زمنية أو كل برنامج/ يمكن لرسائل الإدارة أن تنقل شفرة تكلفة مجفرة ترسَل كجزء من الخدمة. ويمكن لمبلغ الائتمان أن يُحفظ في جهاز الاستقبال على شكل إذنات مالية مجفرة ترسّل كجزء من خدمة العنونة على الهواء. وبدلاً من ذلك، يمكن لمبلغ الائتمان أن يتخذ شكل إذنات مالية مخزنة ويجري توزيعها بوسائط أخرى. ويجري الدفع بتناقص الائتمان المخزن وفقاً لشفرة التكلفة المستقبَلة.

ولكل نظام خصوصيته فيما يتعلق بمحتوى رسالة إدارة الأحقية.

8 وظائفية النفاذ إلى جهاز الاستقبال

في الطرف المستقبِل، يمكن تطبيق النفاذ المشروط بشتى السبل، بما فيها ما يلي:

النمط 1: وظائفية الأمن (التي قد تشمل خوارزمية تجفير المفتاح، والمفاتيح الرئيسية) ووظائفية إزالة التخليط المنفذتان في جهاز الاستقبال.

النمط 2: وظائفية الأمن القابلة للنزع (مثل البطاقة الذكية) ووظائفية إزالة التخليط المنفذتان في جهاز الاستقبال.

النمط 3: وظائفية الأمن وإزالة التخليط القابلة للترع؛ وتنفَّذ جميع الوظائف التي تقوم باستعادة تدفق بيانات الدخل في وحدة قابلة للترع، وتتواصل مع جهاز الاستقبال عبر سطح بيني مقيّس (سطح بيني مشترك مثلاً)؛ وفي هذه الحالة يمكن استعمال أي جهاز استقبال مزود بمثل ذلك السطح البيني.

عند الطلب، تتحقق وظائفية الأمن من الشروط، وإذا ما استوفيت، تقدم مفتاح التخليط إلى الواصف. ويمكن لهذه الشروط أن تشمل ما يلي:

- شرط الفترة الزمنية، حيث يقع تاريخ معلمة التحكم بين تاريخي بدء الصلاحية وانتهائها في معلمة التخويل؛
- شرط الثمن، وبه لا يمكن تقديم تخويل إلا إذا تقاضت وحدة الأمن رسماً.

ويمكن لنظام نفاذ شرطي أن ينجز معاملة تنطوي على وظائفية أمنية على مراحل مختلفة، من قبيل:

- التعليمات الأولية، إن وُجدت (مثل كلمة المرور وقبول المستعمل وما إلى ذلك)؛
- تعليمات التشغيل باستعمال وحدة الأمن؛
- معالجة النتيجة (كإيصال كلمة التخليط).

التذييل 1
للملحق 1

الجـــدول 1

أمثلة عن تنفيذ نظام النفاذ المشروط فيما يتعلق بالإذاعة الرقمية

المرجع في الملحق 1	نظام "Roscrypt"	نظام "CAS-R"	"أنظمة الإذاعة الفيديوية الرقمية (DVB) بمعيار IEC 62455"
الفقرة 4 نمط التجفير للمخلّط ومزيل التخليط	استناداً إلى معيار دولة الاتحاد الروسي 89-28147	تجفير MULTI2 (ISO/IEC 9979)	خوارزمية التخليط المشتركة في نظام النفاذ المشروط إلى الإذاعة الفيديوية الرقمية (DVB-CSA) أو معيار التجفير المتقدم – 128 (AES-128) (إلزامي لجميع الأجهزة)؛ ومن الممكن كذلك معايير تجفير البيانات DES و3DES وMULTI2 (الاختيارية للأجهزة)
الفقرة 4 عملية التخليط	انتقال دوري متعدد الخطى قائم على مسجلات إزاحة تستعمل حدودية من الترتيب الرابع والستين على أساس خوارزميات غير خطية زهو تتابع عشوائي عملياً (ليس له شكل تحليلي)	أ) تتابعات 67 بتة مشفرة، يستعاض عن التشفير الأصلي بسلسلة شفرة اثنينية أخرى تستعمل متغيّرات طولها 64 بتة و256 بتة ب) في سلاسل الشفرة التي تقل عن 64 بتة، تُستعمل الطريقة الموصوفة في أ) أعلاه لتوليد سلسلة من التتابعات المشفرة شبه العشوائية التي تُدمج لإنتاج إشارة مخلّطة	DVB-CSA: وفقاً لمعيار ETSI ETR-289؛ AES-128: وفقاً لمعيار FIPS PUB 197: 2001 باستعمال أسلوب كتاب الشفرة الإلكتروني (ECB) أو تسلسل فدرات التجفير (CBC)؛ معيارا تجفير البيانات DES أو 3DES وفقاً لمعياري FIPS PUB 46-3:1999 وFIPS PUB 81:1980؛ تجفير MULTI2 وفقاً لمعيار ISO/IEC 9979
الفقرة 4 تزامن عملية التخليط	التزامن المتبادل للتتابع العشوائي ودارات قولبة تدفق الإذاعة الفيديوية الرقمية	تُستعمل المعلومات المصاحبة في رسائل مراقبة الأحقية (معلومات البرنامج والتحكم) ورسائل إدارة الأحقية (معلومات فردية) والرسائل المشتركة لإدارة الأحقية والرسائل الفردية لإدارة الأحقية من أجل مزامنة عملية التخليط	يُدرَج عَلَم المفرد–المزدوج والمتجه الأولي في رسالة تدفق المفتاح القائمة بإيصال مفتاح تجفير الحركة لتسهيل التزامن. وتبين القيم المقابلة للنقل والتخليط وبتات التحكم أي مفتاح يتعين استعماله في وقت معين

الجـــدول 1 (*تابع*)

المرجع في الملحق 1	نظام "Roscrypt"	نظام "CAS-R"	"أنظمة الإذاعة الفيديوية الرقمية (DVB) بمعيار IEC 62455"
الفقرة 6 رسائل مراقبة الأحقية (ECM)	محتوى رسالة مراقبة الأحقية: – معرف هوية مفتاح العمل – مفتاح التخليط (مفرد/مزدوج) – يُستعمل إطناب بنيوي لتدفق الإذاعة الفيديوية الرقمية بواسطة عداد مجفر ومجموع تدقيقي مجفر، أو احتياطات مخصصة على نحو إضافي	قسم ECM ومعماريته الأساسية لحمولة ECM النافعة: – يخضع قسم ECM كله لقسم التحقق من الإطناب الدوري (CRC) – تتألف حمولة ECM النافعة من جزء ثابت يُرسل دوماً وجزء متغير يتغير محتواه حسب هدف الإرسال – لا تُدرَج إلا معلومات وظيفة ECM الضرورية في الجزء المتغير من ECM	تحمل رسالة مراقبة الأحقية رسالة تدفق مفتاح تضم مجالات لحمل المعلومات التالية: – مؤشر مفتاح المحتوى – علم المفرد–المزدوج – أسلوب التجفير – المتجه الأولي التالي – مادة مفتاح الحركة المجفرة – عمر مفتاح الحركة – دلالة الوقت – واصفات معايير النفاذ – فئة الأذونات – مفتاح تجفير البرنامج المجفر – تمديد معرف قناة (CID) البرنامج – شفرة استيقان رسالة (MAC) البرنامج – تمديد معرف قناة (CID) الخدمة – شفرة استيقان رسالة (MAC) الخدمة ويعتمد إدراج أي من هذه المجالات في رسالة تدفق مفتاح معينة على بضعة عوامل، من قبيل ما إذا كان مورّد الخدمة يريد إتاحة النفاذ على أساس كل برنامج على حدة
مفتاح رئيسي	256 بتة	256 بتة	لا يوجد "مفتاح رئيسي" بحد ذاته. وتقوم حماية مفاتيح تجفير الخدمة (SEK) أو مفاتيح تجفير البرنامج (PEK) على مفاتيح خوارزمية RSA التي تبلغ بتاتها 1 024 أو 2 048 أو 4 096 بتة تبعاً لسلطة الوثوق. وفي أسلوب الإذاعة، يقوم مفتاح التجفير المستنتج (IEK) ذو الـــ128 بتة بدور مماثل. فهو يُشتق من مجموعة المفاتيح المسلمة إلى جهاز الاستقبال أثناء التسجيل. وتستند حماية مجموعة المفاتيح إلى مفاتيح خوارزمية RSA التي تبلغ بتاتها 1 024 أو 2 048 أو 4 096 بتة

الجـــدول 1 (تتمة)

المرجع في الملحق 1	نظام "Roscrypt"	نظام "CAS-R"	"أنظمة الإذاعة الفيديوية الرقمية (DVB) بمعيار IEC 62455"
الفقرة 6 تغيير مفتاح التخليط والعَلَم	يغيَّر مفتاح التخليط حسب الضرورة. وتُستعمل الحالات الأربع جميعها لعلم التخليط	تغيَّر مفاتيح التخليط (المفرد/المزدوج) كل ثانيتين عادةً	يتغيّر مفتاح تجفير الحركة كثيراً بوتيرة مرة كل دقيقة أو مرة كل ثانية
الفقرة 7 رسالة إدارة الأحقية (EMM)	محتوى EMM: – رقم البروتوكول – معرف المجموعة المذيعة – مفتاح العمل – معرف البرنامج – معرف وحدة الأمن – حقوق النفاذ – العداد المجفر والمجموع التدقيقي المجفر – يُستعمل إطناب بنيوي لتدفق الإذاعة الفيديوية الرقمية أو احتياطات مخصصة على نحو إضافي	يمكن لقسم EMM أن يحمل حمولات نافعة متعددة. ويخضع قسم EMM كله لكشف الخطأ بطريقة التحقق من الإطناب الدوري (CRC). تتألف حمولة EMM النافعة من جزء ثابت يُرسل دوماً وجزء متغير يتغير محتواه حسب هدف الإرسال لا تُدرَج إلا معلومات وظيفة EMM الضرورية في الجزء المتغير من EMM تُرسل هوية البطاقة والمعلومات المصاحبة بطول بايتة واحدة إلى بداية الجزء الثابت من EMM (الجزء غير المجفر). ويرشح جهاز الاستقبال هذه المنطقة لتحديد حمولات EMM النافعة المعنونة لذاتها	في الأسلوب التفاعلي، تُستعمل أغراض حقوق OMA DRM 2.0 بدلاً من رسائل إدارة الأحقية لإيصال الحقوق ومفاتيح تجفير الخدمة (SEK) أو مفاتيح تجفير البرنامج (PEK) إلى أجهزة الاستقبال. ويجري إيصالها عبر قناة التفاعل. وفي أسلوب الإذاعة، تُستعمل نسخة اثنانية (تدعى BCRO) عن أغراض الحقوق هذه.
الفقرة 8 وظائفية التحكم في النفاذ	يقع داخل وحدة النفاذ المشروط (CAM) أو يُدمج ضمن الوحدة الطرفية للمشترك (STB)	النمط 2: وحدة الأمن قابلة للترع ووحدة إزالة التخليط مدمجة داخل جهاز الاستقبال	يُتوقع النمط 1، ولكن لا تُستبعد التطبيقات الأخرى أيضاً
العداد المجفر والمجموع التدقيقي المجفر	ECM, EMM	تُدرَج شفرة استيقان الرسالة (MAC) في رزمتي ECM وEMM كلتيهما	تُدرَج شفرة استيقان الرسالة (MAC) في رسائل تدفق المفتاح وأغراض حقوق أسلوب الإذاعة. وتحمى أغراض حقوق الأسلوب التفاعلي بتوقيع
الفقرة 8 وظائفية الأمن	يقع داخل وحدة النفاذ المشروط (CAM) أو يُدمج ضمن الوحدة الطرفية للمشترك (STB)	يتم استيقانه بصورة متبادلة بين البطاقة الذكية وجهاز الاستقبال	المعيار لا يملي التنفيذ. وتضع سلطة الوثوق قواعد التطابق والمتانة

1 وصف نظام "Roscrypt"

يجري تنفيذ نظام النفاذ المشروط (CAS) "Roscrypt" في روسيا حالياً في سياق متصل بالتحول إلى الإذاعة التلفزيونية الرقمية. وقد صُمم نظام "Roscrypt" لحماية تدفقات بيانات الإذاعة الفيديوية الرقمية من الاستقبال غير المخول. وهو نظام تتعدد أوجه استخداماته على نطاق واسع مع مختلف سلاسل الإذاعة الفيديوية الرقمية الساتلية وللأرض، ويتسم بالمرونة من حيث إدارة مشتركيها.

ويتألف نظام "Roscrypt" مما يلي:

- *المخلّط* الذي يقوم بتجفير مكونات تدفق نقل الإذاعة الفيديوية الرقمية المنتقى مسبقاً؛ ويمكنه العمل على نحو مستقل أو تحت تحكم حاسوب شخصي؛
- *وحدة النفاذ المشروط* التي يتم إدخالها في شق السطح البيني المشترك (CI) لجهاز الاستقبال بغية إزالة تخليط المكونات المختارة؛
- *وحدة الأمن* المزودة بوحدة طرفية للمشترك.

وتركَّب المعدات اللازمة لعمل نظام التحكم المشترك والمراقبة في الطرف المرسل.

ويحل نظام "Roscrypt" المشاكل التالية:

- حصر الإذاعة ضمن مساحة البلد لحماية حقوق أصحاب البرنامج في الإذاعة المحدودة؛
- حماية إذاعة الشركات والإدارات من النفاذ غير المخول؛
- تنظيم الإذاعة التجارية.

ويأخذ نظام "Roscrypt" في الحسبان السمات المميزة للسلاسل المحمية من النفاذ غير المخول.

1.1 السمات الوظيفية والتقنية لنظام "Roscrypt"

- يقابل نموذج العمل الشائع لنظام النفاذ المشروط (CAS) "Roscrypt" الشكل 1 في الملحق 1.
- *خوارزمية التخليط*: هناك خوارزميتا تخليط خاصتان محققتان في تخليط وإزالة تخليط "Roscrypt". ويمكن للمشغل أن يغير خوارزمية التخليط الراهنة في أي وقت.
- *مفاتيح الأمن*: تُستعمل المفاتيح التالية في نظام النفاذ المشروط (CAS) "Roscrypt":
  - يوفر مفتاح التخليط ومفتاح العمل تخليط/إزالة تخليط المحتوى.
  - وتوفر قاعدة المفاتيح الرئيسية المتفردة فك تجفير رسالة مراقبة الأحقية (ECM) (مفتاح عمل) وتحكم في النفاذ في –إطار المشترك.
  - وتتيح مفاتيح البرنامج عزل المشتركين لدى مختلف المشغلين عن بعضهم البعض وتقسيم جميع المشتركين وفق أي معيار.
  - ويمكن للمشغلين أن يقوموا بتغيير سريع للمفاتيح دون توزيع مادي وإلكتروني.
- *أسلوب النفاذ*: هناك أسلوبان للنفاذ من أجل الإدارة الفعالة للمشتركين: توفر الفترة، وبند البرنامج والخدمة.
  - معلمات أسلوب النفاذ: يبلغ وقت إدارة المشترك 000 1 مشترك في الثانية، ولا حدود لعدد المشتركين، ويبلغ عدد مكونات التخليط 150؛ ومجموعات المستعملين المستهدفين 000 64.

- *رسالة إدارة الأحقية (EMM) ورسالة مراقبة الأحقية (ECM)*: يكون هيكل إشارات رسالة إدارة الأحقية (EMM) ورسالة مراقبة الأحقية (ECM) وفقاً لما ورد في الفقرتين 6 و7 من الملحق 1.
- هناك عداد مجفر ومجموع تدقيقي مجفر في نهاية كل رزمة رسالة إدارة الأحقية (EMM) ورسالة مراقبة الأحقية (ECM).
- ولإدارة إيصال أوامر (رسالة إدارة الأحقية (EMM) ورسالة مراقبة الأحقية (ECM)) يمكن على السواء استعمال الموارد الإضافية لعرض نطاق تدفق الإذاعة الفيديوية الرقمية (DVB) واحتياطات السرعة البنيوية (الإطناب البنيوي) لتدفق نقل الإذاعة الفيديوية الرقمية.
- *معدات الاستقبال*: هناك نمطان ممكنان من نظام النفاذ المشروط "Roscrypt" على جانب الاستقبال:
- وحدة أمن مدمجة في الوحدة الطرفية للمشترك، تشمل خوارزمية فك تجفير المفتاح في مفاتيح الأمن ووحدة إزالة التخليط.
- وحدة نفاذ مشروط (CAM) قابلة للنزع تشمل وحدتي الأمن وإزالة التخليط، وتتواصل مع جهاز الاستقبال عبر سطح بيني مشترك (CI) مقيّس. ويمكن لوحدة نفاذ مشروط واحدة إعادة المكونات المخلّطة لتدفق نقل الدخل إلى أصلها في الوقت نفسه.

2.1 السمات الأخرى:

- يمكن لمجموعة واحدة من معدات إرسال "Roscrypt" أن تجفر محتوى العديد من الموردين المستقلين. وتُستعمل هذه الخاصية لفائدة مشغلي الإذاعة الساتلية والإذاعة للأرض.
- ويتيح نظام التحكم والمراقبة المشترك التحكم في نفاذ المشترك إلى المحتوى.
- ويتيح نظام التحكم والمراقبة المشترك تشغيلاً مركزياً عن بعد ومراقبة مجموعة معدات إرسال "Roscrypt" في كل أنحاء الشبكة. وتُستعمل هذه الخاصية لفائدة مشغلي الإذاعة الساتلية والإذاعة للأرض.

2 وصف نظام النفاذ المشروط أثناء استقبال الإشارة (CAS-R)

1.2 الغرض من النظام

يسخّر معيار رابطة الصناعات ومشاريع الأعمال الراديوية – B25 (ARIB STD-B25) نظام التحكم بالنفاذ المشروط لاستعماله في الإذاعة الرقمية، ويعرّف التخليط ومواصفات المعلومات المصاحبة له فضلاً عن مواصفات الاستقبال ذات الصلة لنظام يوفر التحكم أثناء استقبال الإشارة (يدعى "CAS-R" من الآن فصاعداً).

ويوصّف هذا المعيار أنظمة النفاذ المشروط (CAS) لأنظمة الإذاعة الرقمية للأرض والإذاعة الرقمية الساتلية المستعملة حالياً في اليابان.

2.2 متطلبات نظام CAS-R وأنظمته المتداولة

يوصّف معيار ARIB STD-B25 أنظمة النفاذ المشروط (CAS) لتلبي المتطلبات التالية:

1 أكبر عدد من المشتركين

يمكن توسيع النظام ليوفر وظائف إدارة العملاء لجميع الأسر في منطقة التغطية.

2 عمر النظام:

يمكن إدارة النظام بدعم وسائط الإذاعة المعمول بها.

3 مكافحة القرصنة:

يوفر النظام وظائفية أمنية متقدمة ويمكنه اتخاذ تدابير في حال تعرضه لهجوم الأمني.

4 الأنظمة قابلة للتطبيق على جميع أنظمة الإذاعة الرقمية في منطقة معينة.

5 أنماط الاستقبال:

أ) استقبال في الوقت الفعلي يشمل تدفق الإشارة السمعية/الفيديوية (A/V) وإذاعة البيانات باستعمال نسق الملفات (CAS-R).

ب) استقبال محفوظ (استقبال في غير الوقت الفعلي).

ج) استقبال مسجل (بما فيه الاستقبال المحجوز).

6 يمكن تطبيق النظام على هياكل الرسوم التالية: (الموحدة/الطبقية، والدفع مقابل كل مشاهدة، والدفع التفاعلي مقابل كل مشاهدة (IPPV)، والمجاني.

3.2 متطلبات وحدة الأمن

1 تجفير المعلومات المصاحبة:

يستعمل نظام التجفير معمارية ثلاثية الطبقات بمفاتيح تكافئ معيار تجفير البيانات (DES) ومفاتيح خاصة. ومن منظور تنفيذ بطاقة ذكية، ينبغي لنظام التجفير أن يضم برنامجاً صغيراً يمكّن المعالجة السريعة بواسطة معالج تحكم صغري بثماني بتات على الأقل.

2 وظائفية الإدارة:

يمكن للنظام أن يغيّر بروتوكول التجفير لمكافحة أعمال القرصنة.

3 ينبغي تنفيذ استيقان متبادل بين البطاقة الذكية وجهاز الاستقبال:

تُستعمل البطاقة الذكية في نظام النفاذ المشروط لاستبعاد أجهزة الاستقبال التي لا تستجيب لمعلومات حماية الحقوق في التطبيقات التي تستعمل نظام النفاذ المشروط هذا كتكنولوجيا لحماية الحقوق في الإذاعة الرقمية. ويتوفر عندئذ نظام للاستيقان المتبادل بين هذه البطاقة الذكية وجهاز الاستقبال.

4.2 يرد وصف مفصل للنظام في الوثيقة التالية

ترد مواصفات نظام النفاذ المشروط ARIB STD B-25 على العنوان الإلكتروني:
http://www.arib.co.jp/english/html/overview/doc/6-STD-B25v5_0-E1.pdf

3 وصف "معيار اللجنة الكهرتقنية الدولية 62455 (IEC 62455) في أنظمة الإذاعة الفيديوية الرقمية"

يوصّف معيار اللجنة الكهرتقنية الدولية 62455 (IEC 62455) نظاماً معيارياً للتحكم في النفاذ إلى خدمات إذاعية قائمة على تدفق نقل MPEG2. كما يوصّف معيار IEC 62455 الكيفية التي يمكن فيها استعمال النظام نفسه للتحكم في النفاذ إلى خدمات إذاعية قائمة على بروتوكول الإنترنت (IP). ومن ثم فإن التوصيف يسري على مختلف الأنظمة الإذاعية على نطاق واسع، بما فيها الأنظمة التي تتعذر فيها الحماية على رزم تدفق نقل MPEG2 (مثل الخدمات القائمة على بروتوكول الإنترنت المقدمة عبر شبكات لا تستند إلى MPEG2).

ولأنظمة الإذاعة ذات النفاذ المشروط، يقدم معيار IEC 62455 سطحاً بينياً موصّفاً بالكامل ما بين الطرفين المرسل والمستقبل. وباستعمال هذا السطح البيني الموصّف بالكامل، يمكن لباعة المخدّم والمستقبِل على السواء أن ينفذوا الدعم لنظام الحماية على نحو مستقل، بدلاً من الاضطرار للاعتماد على بائع خدمة أمنية واحد لتسهيل التنفيذ على المخدم والمستقبل كليهما. وهكذا فإن تبلور النظام يغني عن الارتباط ببائع خدمة أمنية ويتيح تغيير بائع أي عنصر في نظام نفاذ مشروط موصّف دون تغيير العناصر الأخرى أو باعتها.

ويغطي توصيف IEC 62455 جميع الطبقات التالية للنظام، بيد أنه يحيل إلى المواصفات القائمة كلما أمكن ذلك:

- طبقة التسجيل
- طبقة إدارة الحقوق
- طبقة تدفق المفتاح
- طبقة الحركة.

وتقوم طبقة إدارة الحقوق على معيار إدارة الحقوق الرقمية OMA DRM 2.0 لتحالف الخدمات المتنقلة المفتوحة، وهو معيار راسخ ومعتمد تجارياً على نطاق واسع. وتتولى هذه الطبقة مسؤولية إيصال الحقوق والقيود المتصلة بها إلى أجهزة الاستقبال، فضلاً عن المفاتيح طويلة الأجل، أي مفتاح تجفير الخدمة (SEK) أو مفتاح تجفير البرنامج (PEK)، تبعاً لما إذا النفاذ ممنوحاً على أساس اشتراك أو كل برنامج على حدة.

وفي الأسلوب التفاعلي، أي عند توفر قناة اتصال بالاتجاهين بين جهاز الاستقبال ومورّد الخدمة، يُستعمل معيار OMA DRM 2.0 كما هو. أما في التشغيل الإذاعي أحادي الاتجاه الذي تغيب فيه قناة التفاعل، فقد عُزز النظام بنُسخ اثنينية من أغراض حقوق OMA DRM 2.0 (تدعى أغراض حقوق بتشفير اثنيني أو BCRO) من شأنها توفير عرض النطاق، وبطريقة لحمايتها عند تقديمها عبر القناة الإذاعية. وتشمل عنونة أغراض الحقوق بتشفير اثنيني مختلف أساليب العنونة مما يزيد من تقليص عرض النطاق اللازم لتوزيع أغراض الحقوق. وتعتمد طريقة الحماية على تجفير إذاعة الرسالة الصفرية، مما يضمن أن اختراقاً أمنياً في أحد أجهزة الاستقبال لا يتيح نفاذاً إلى مفاتيح أو حقوق مقدمة لأية أجهزة استقبال أخرى. ويراعى إلى حد كبير الاستعمال الأمثل لعرض نطاق الإذاعة.

ويجري إيصال مجموعة المفاتيح اللازمة للتشغيل بأسلوب الإذاعة إلى جهاز الاستقبال أثناء التسجيل على الخدمة عبر قناة الإذاعة. وللتسجيل على خدمة، ما على المستعمل إلا موافاة مورّد الخدمة بالرقم الذي ينفرد به جهاز الاستقبال (UDN)، فيستخرج مورّد الخدمة شهادة جهاز الاستقبال من قاعدة بيانات الشهادات. إذ أن الشهادة تحوي المفتاح العمومي المستعمل لحماية مجموعة المفاتيح أثناء العبور.

ولحماية تدفق نقل MPEG-2، يستخدم تجفير (تخليط) المحتوى الفعلي للخدمة شفرات تجفير رائجة من قبيل DVB-CSA أو AES-128 كما يوصّفها معيار IEC 62455، الذي يوصّف أيضاً دعماً لمعايير تجفير أخرى مثل IPsec وSRTP وISMAcryp لتسهيل الحماية القائمة على ما يغاير رزم تدفق نقل MPEG2.

وتسهيلاً للتغيير المتكرر لمفاتيح تجفير الحركة (TEK) المستعملة لحماية محتوى الخدمة، يوصّف معيار IEC 62455 طبقة تدفق مفتاح تعمل بين طبقة إدارة الحقوق وطبقة الحركة. ويدعم النظام إتاحة النفاذ إلى التدفق نفسه عبر أغراض حقوق الخدمة والبرنامج على السواء. فإذا ما أراد مورد الخدمة تمكين النفاذ إلى كل برنامج على حدة في حالة توفر البرنامج عن طريق الاشتراك كذلك، ستحمل رسالة تدفق المفتاح مفتاح تجفير برنامج (PEK) مجفراً مع مفتاح تجفير الخدمة (SEK) بالإضافة إلى مفتاح TEK مجفراً بمفتاح PEK. كما يمكن لطبقة تدفق المفتاح أن تحمل بعض المعلومات الأخرى مثل معايير النفاذ أو قيمة فئة الأذونات التي يمكن استعمالها للانتقاء بين الحقوق المختلفة في غرض حقوق الخدمة المتصل بجزء من التدفق الذي تنطبق عليه رسالة تدفق المفتاح. ويتيح ذلك امتلاك حقوق مختلفة في برامج مختلفة حتى وإن كان النفاذ قائماً على الاشتراك في خدمة مكونة من برامج متتالية متعددة.

_____