Международный союз электросвязи

МСЭ-Т J.1010

(09/2016)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ J: КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ И ЗВУКОВЫХ ПРОГРАММ И ДРУГИХ МУЛЬТИМЕДИЙНЫХ СИГНАЛОВ

Условный доступ и защита – Заменяемые встроенные решения для обеспечения условного доступа и управления цифровыми правами

Встроенный общий интерфейс для заменяемых решений CA/DRM; сценарии использования и требования

Рекомендация МСЭ-Т J.1010

ITU-T

Международный союз электросвязи

Рекомендация МСЭ-T J.1010

Встроенный общий интерфейс для заменяемых решений CA/DRM; сценарии использования и требования

Резюме

В Рекомендации МСЭ-T J.1010 определены сценарии использования и требования для заменяемых встроенных решений условного доступа/управления цифровыми правами (CA/DRM), поддерживающих оборудование в помещении потребителя (CPE), которое может принимать вещательный и широкополосный контент, с тем чтобы загружать клиентов CA/DRM в надежной среде. Используя услугу, позволяющую загружать несколько CA/DRM, обладающие правами пользователи могут потреблять вещательный и широкополосный контент, контролируемый DRM и/или системами условного доступа (CA), даже если CPE не имеет требуемого относящегося к контенту клиента CA/DRM, доступного путем его загрузки из надежного источника в разные типы CPE, включая абонентские приставки (STB), "умные" телевизоры, ПК, смартфоны и/или смарт-планшеты.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-T J.1010	02.09.2016 г.	9-я	11.1002/1000/12772

Ключевые слова

CA/DRM, заменяемый встроенный общий интерфейс, продаваемое в розницу CPE.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним с целью стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" ("shall") или некоторые другие обязывающие выражения, такие как "обязан" ("must"), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности, независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу: http://www.itu.int/ITU-T/ipr/.

© ITU 2017

Все права сохранены. Ни одна из частей данной публикации не может быть воспроизведена с помощью каких бы то ни было средств без предварительного письменного разрешения МСЭ.

СОДЕРЖАНИЕ

Стр.

Введение

Защита услуг и контента, которая обеспечивается с помощью условного доступа (CA) и управления цифровыми правами (DRM), имеет важнейшее значение в быстро развивающейся области цифрового радиовещания и широкополосной связи, включая контент, услуги, сети и оборудование в помещении клиента (CPE), для защиты бизнес-моделей владельцев контента, операторов сетей и операторов платного ТВ. По существу, CA сосредоточен на механизмах доступа к защищенному контенту, распределяемому по сети поставщиком услуг, а DRM изначально содержит описание типа и степени прав на использование согласно контракту абонента.

Операторы платного ТВ создали платформы цифрового ТВ, в которых внедрены стандарты для базовых функций, расширенные проприетарными элементами. Большинство систем CA и DRM, используемых для услуг классического цифрового радиовещания, IPTV или новых услуг OTT (over-the-top), охватывают оборудование в помещении потребителя (CPE), увязывая его с проприетарными элементами, которые относятся к безопасности. В результате оборудование в помещении потребителя, конфигурированное для использования в сети или платформе A, не может использоваться в сети или платформе B и наоборот. Таким образом, рынок бытовой электроники для цифрового ТВ все еще является фрагментированным, поскольку спецификации различаются не только в зависимости от той или иной страны, но и от платформы. Съемные модули CA/DRM предлагают лишь частичное решение: такие модули опять-таки являются проприетарными для системы CA/DRM, они не являются менее дорогими и используются в основном для кабельного или спутникового ТВ и не применимы в оборудовании современного типа, таком как планшеты, в силу отсутствия необходимых физических интерфейсов.

Внедряемые в настоящее время решения, связанные со встроенным или съемным аппаратным обеспечением, приводят к последствиям "привязки". Это серьезно ограничивает свободу многих участников рынков цифрового мультимедийного контента. В связи с техническим прогрессом становятся осуществимыми инновационные решения CA/DRM на основе программного обеспечения. Максимально увеличивая функциональную совместимость, при этом поддерживая высокий уровень безопасности, они сулят соответствие будущим запросам рынка, создание возможностей для новых направлений бизнеса и расширение выбора для потребителей.

Потребители заинтересованы в том, чтобы можно было продолжать использовать приобретенное ими CPE, например, после ухода или изменения поставщика сети, или даже использовать устройства для услуг различных коммерческих видео-порталов. Это может быть обеспечено только благодаря функциональной совместимости CPE в отношении CA и DRM на основе надлежащей архитектуры безопасности. Можно избежать дальнейшей фрагментации рынка CPE и содействовать конкуренции только путем обеспечения заменяемости систем CA и DRM дружественным для потребителей и зависимым от контекста образом.

Рекомендация МСЭ-Т J.1010

Встроенный общий интерфейс для заменяемых решений CA/DRM; сценарии использования и требования

1 Сфера применения

Цель настоящей Рекомендации заключается в установлении набора базовых требований к заменяемому встроенному общему интерфейсу для загрузки любой необходимой системы CA/DRM в CPE. Процесс загрузки осуществляется в надежной среде и позволяет потреблять защищенный контент, доставляемый через радиовещание и/или широкополосные соединения с различными видами оконечного оборудования в соответствии с приобретенными правами конечного пользователя на контент. Данная Рекомендация является одной из серии Рекомендаций, где определяется вся экосистема ECI.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие справочные документы содержат положения, которые путем ссылок на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие справочные документы могут подвергаться пересмотру; поэтому всем пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других справочных документов, перечисленных ниже. Перечень действующих на настоящий момент Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статус Рекомендации. Приведенные далее справочные документы являются обязательными при использовании данного документа.

[ETSI GS ECI 001-1] ETSI GS ECI 001-1: 2014, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions (ECI); Part 1: Architecture, Definitions and Overview*.

[ETSI GS ECI 001-2] ETSI GS ECI 001-2: 2014, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 2: Use cases and requirements*.

3 Определения

3.1 Термины, определенные в других документах

Отсутствуют.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации определяются следующие термины.

3.2.1 встроенный общий интерфейс (ECI): Архитектура и система, определяемые в ETSI ISG "Встроенный CI", который дает возможность разработки и внедрения сменных клиентов ECI на базе программного обеспечения в оборудование в помещении клиента (CPE) и таким образом обеспечивает функциональную совместимость устройств CPE в отношении ECI.

3.2.2 клиент встроенного общего интерфейса (клиент ECI): Ввод в действие клиента CA/DRM, совместимого с запланированными спецификациями встроенного CI. Следует отметить, что это модуль программного обеспечения в CPE, который обеспечивает все средства для получения защищенным образом разрешений и прав потребителя, касающихся контента, который распределяется дистрибьютором контента или оператором. В нем также содержатся условия, при которых то или иное право или разрешение может использоваться потребителем, а также ключи для расшифровки различных сообщений и контента. Клиент встроенного CI может иметь соответствующую смарт-карту.

3.2.3 хост встроенного общего интерфейса (ECI): Система аппаратного и программного обеспечения CPE, которая охватывает функциональные возможности, относящиеся к ECI, и имеет интерфейсы с клиентом ECI. Следует отметить, что хост ECI является одной из частей микропрограммного обеспечения CPE.

3.2.4 защищенный контент: Все виды защищенных носителей, в частности A/V, и соответствующие метаданные, доставляемые на приложение потребителя средствами либо линейной, либо нелинейной доставки.

3.2.5 хранилище программного обеспечения: Набор интерфейсов программного обеспечения для хоста и для клиента, в котором четко разделяются клиент и хост CA/DRM. Предоставление интерфейсов обеспечивает заменяемость клиентов CA/DRM.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AES	Advanced Encryption Standard	Усовершенствованный стандарт шифрования
CA	Conditional Access	Условный доступ
CA/DRM	Conditional Access/Digital Rights Management	Условный доступ/Управление цифровыми правами
CE	Consumer Electronics	Бытовая электроника
CPE	Customer Premises Equipment	Оборудование в помещении клиента
CSA	Common Scrambling Algorithm	Общий алгоритм скремблирования
DECE	Digital Entertainment Content Ecosystem	Экосистема цифрового развлекательного контента
DRM	Digital Rights Management	Управление цифровыми правами
DVB	Digital Video Broadcasting	Цифровое телевизионное радиовещание
ECI	Embedded Common Interface	Встроенный общий интерфейс
IP	Internet Protocol	Протокол Интернет
IPTV	TV services delivered via IP protocol	Услуги телевидения на основе IP-протокола
OMA	Open Mobile Access	Открытый мобильный доступ
OTT	Over The Top (over the open Internet)	Технология OTT (доставка поверх открытого интернета)
PVR	Personal Video Recorder	Персональный видеомагнитофон
TTP	Trusted Third Party	Доверенная третья сторона
URI	Usage Rights Information	Информация о правах на использование
VM	Virtual Machine	Виртуальная машина

5 Условные обозначения

В настоящей Рекомендации:

Ключевые слова "**требуется, чтобы**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу.

Ключевые слова "**рекомендуется, чтобы**" означают требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии этому документу это требование не является обязательным.

Ключевые слова "**запрещается**" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этому документу.

Ключевые слова "**может факультативно**" означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Этот термин не означает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и функция может быть активирована по желанию оператора сети/поставщика услуг. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии спецификации.

В тексте настоящего документа и его приложениях иногда встречаются слова *должен*, *не должен*, *следует* и *может*. В этом случае их следует понимать как *требуется, чтобы*; *запрещено*; *рекомендуется* и *может факультативно*, соответственно. Появление таких фраз или ключевых слов в дополнении или материалах, однозначно помеченных, как *информативные*, должно пониматься, как не несущее нормативного смысла.

6 Требования для заменяемых встроенных решений CA/DRM

6.1 Общие замечания

Групповая спецификация базовых требований **ECI**, рассматриваемых в настоящей Рекомендации, является частью многотомной итоговой документации, в которой определена архитектура системы для общих целей, основанные на программном обеспечении встроенные и заменяемые системы CA/DRM, которые будут наиболее подходящим и перспективным решением для преодоления фрагментации рынка и обеспечения возможности функциональной совместимости. Важнейшими преимуществами предусматриваемого подхода для обеспечения безопасности контента являются:

- гибкость и масштабируемость благодаря реализации на базе программного обеспечения;
- заменяемость, содействующая перспективным решениям и способствующая инновациям;
- применимость к контенту, распределяемому через радиовещание и широкополосную связь, включая OTT;
- поддержка многоэкранной среды;
- стимулирование рынка для операторов платформ, поставщиков сетей/услуг и потребителей путем недопущения "привязки";
- спецификация открытой экосистемы, способствующей развитию рынка.

Система **ECI** направлена на обеспечение заменяемости систем CA и DRM в CPE на всех соответствующих уровнях и по всем аспектам по наиболее низким, насколько это возможно, ценам для потребителей и при минимальных ограничениях для поставщиков CA или DRM по разработке своих целевых продуктов для рынка платного ТВ. В связи с этим ECI обладает, в том числе, нижеследующими функциональными возможностями.

- Хранилище программного обеспечения для CA относительно ядра DRM (далее: **клиент ECI**) которое имеет:
  - стандартизированные интерфейсы для всех соответствующих функциональных возможностей CPE;
  - стандартизированную **виртуальную машину (VM)** для работы.
- Поддержка систем без смарт-карт, а также использование систем на базе смарт-карт.
- Включение множества таких хранилищ программного обеспечения в CPE, при этом каждое хранилище работает на основе своего экземпляра **VM**.
- Установка **клиента ECI** независимо от другого программного обеспечения CPE с использованием концепции надежного и стандартизированного загрузчика.
- **Повышенная безопасность**, известная также под названием набор микросхем в области безопасности, для поддержки защиты контента и предупреждения несанкционированного доступа к контенту.
- Методы, с помощью которых пользователь может обнаружить правильного **клиента ECI** для загрузки.
- Методы отмены функциональной возможности (или ее части) **клиента ECI** и функциональной возможности CPE.
- Подходит для классического цифрового радиовещания, IPTV или современных систем на базе OTT.

Хотя ECI имеет некоторое сходство с уже развернутыми решениями, но есть и существенные различия:

1) модули включены в программное обеспечение, а более не в аппаратное обеспечение, таким образом нет необходимости в затратах потребителей на замену системы CA или DRM;

2) в одно и то же CPE может быть включено несколько параллельных **клиентов ECI** без повышения соответствующей стоимости;

3) эти клиенты могут работать одновременно в одном устройстве.

В результате компонент CA или DRM может заменяться гораздо проще, позволяя конечному пользователю менять оператора или получать услуги от различных операторов на свое CPE, без необходимости замены дорогих модулей.

Полная многотомная документация включает группу спецификаций, в том числе групповую спецификацию по сценариям использования и требованиям, в сочетании с лежащими в основе спецификациями:

− Часть 1: Архитектура, определения и обзор [ETSI GS ECI 001-1]

− Часть 2: Сценарии использования и требования [ETSI GS ECI 001-2]

− Часть 3: Хранилище, загрузчик, интерфейсы, отмена CA/DRM [b- ETSI GS ECI 001-3]

− Часть 4: Виртуальная машина (VM) [b- ETSI GS ECI 001-4]

− Часть 5: Система повышенной безопасности [b- ETSI GS ECI 001-5]

− Часть 6: Среда доверия [b- ETSI GS ECI 001-6]

− Часть 7: Расширенные требования [b- ETSI GS ECI 001-7]

Эти спецификации совместно описывают решение, позволяющее заменить **клиентов ECI** в любое время, просто загрузив **клиентов ECI**, запрашиваемых конечным потребителем. **Клиенты ECI** устанавливаются в стандартном хранилище программного обеспечения в CPE с помощью отдельного загрузчика, с отдельными алгоритмами безопасности и ключами для защиты **клиентов ECI** от атак на целостность и от действий посредством замены независимо от всего другого программного обеспечения в CPE. Интерфейсы хранилищ и CPE являются общими и определены в GS ECI 001-3 [b- ETSI GS ECI 001-3], позволяя **клиенту ECI** взаимодействовать с различными функциями в CPE и вне CPE.

Клиенты ECI работают на основе экземпляра виртуальной машины, который определен в GS ECI 001-4 [b- ETSI GS ECI 001-4].

В GS ECI 001-5 [b- ETSI GS ECI 001-5] указан механизм повышенной безопасности для защиты ключа к контенту во время его передачи в устройство расшифровки контента в микросхеме процессора CPE.

В настоящей Рекомендации рассматриваются сценарии использования и требования в качестве основы для внедрения функционально совместимых систем CA/DRM в CPE.

Спецификация **ECI** применяется только к получению и последующей обработке контента, контролируемого системой условного доступа и/или управления цифровыми правами и скремблированного поставщиком услуг. В настоящей Рекомендации не рассматривается контент, который не контролировался системой условного доступа и/или DRM.

Групповая спецификация **ECI** предназначена для использования в сочетании с договорной базой (лицензионным соглашением), правилами соответствия и устойчивости, а также соответствующим процессом сертификации (см. примечание) под контролем **доверительного органа**, GS ECI 001-6 [b- ETSI GS ECI 001-6].

Сквозная безопасность совместимой с ECI системы CA/DRM является предметом не одних лишь технических спецификаций. Технология ECI − это только один элемент совместимой с ECI экосистемы, GS ECI 001-1 [ETSI GS ECI 001-1], которая должна быть создана доверительным органом с учетом также нормативно-правовой базы, сертификации устройств и других вопросов. Указанные ниже требования основаны на сценариях использования, которые приводятся в Приложении A.

6.2 Общие требования

[R 01] **Встроенный CI** должен быть применимым к любым услугам радиовещания, широкополосной связи и гибридным услугам (означающим сочетание радиовещания и широкополосной связи), обеспечивающим доставку защищенного контента через соответствующую сеть доступа любого типа до применимого устройства любого типа.

[R 02] **Встроенный CI** должен определять **хранилище программного обеспечения** для программного обеспечения ядра ECI, тесно связанного с функциональными возможностями программного обеспечения CA/DRM и четко отделенного от остальных элементов программного обеспечения CPE.

[R 03] **Встроенный CI** должен обеспечивать функции повышенной безопасности, совместимые с функциями имеющихся в настоящее время новейших систем CA/DRM.

[R 04] **Встроенный CI** должен дать возможность разработки реализаций безопасных систем CA/DRM, которые могут эксплуатироваться и поддерживаться в течение долгого времени, в любом случае не менее пяти лет.

6.3 Требования, связанные с универсальностью

[R 05] **Встроенный CI** должен поддерживать включение более одного клиента CA/DRM в CPE, что обеспечивает решение для одновременной обработки по меньшей мере двух различных случаев **защищенного контента**.

[R 06] Архитектура должна обеспечивать возможность того, чтобы различные клиенты ECI в CPE могли распознавать друг друга, установить взаимное доверие и передавать друг другу контент и соответствующую **URI**.

[R 07] Архитектура должна обеспечивать возможность того, чтобы **клиенты ECI** могли доверять **хосту ECI**, с которым они соединены, и защищенным образом передавать **URI** в **хост ECI**.

[R 08] **Встроенный CI** должен обеспечивать соответствие национальным нормативно-правовым требованиям, например по защите конфиденциальности данных и защите несовершеннолетних.

[R 09] **Встроенный CI** должен поддерживать экспорт приобретенного законным образом **защищенного контента** в другие терминалы (включая мобильные оконечные устройства) в рамках базового домена или домашней сети. Это предполагает, что архитектура обеспечивает необходимые интерфейсы, что клиент ECI в CPE может разговаривать с другим клиентом ECI по тому же устройству. Это будет возможным только в соответствии с правами на использование, выданными соответствующими владельцами контента.

[R 10] Клиент ECI может быть включен таким образом, что он может экспортировать **защищенный контент** в устройство, не совместимое с ECI. Это будет возможным только в соответствии с правами на использование, выданными соответствующими владельцами контента.

6.4 Требования, связанные с применимостью

[R 11] **Встроенный CI** должен обеспечивать API для внедрения пользовательских интерфейсов, обеспечивающих большое удобство использования и простоту регулирования пользовательского взаимодействия.

[R 12] **Встроенный CI** не должен добавлять заметной задержки по сравнению с сопоставимыми решениями CA/DRM, даже если два затрагиваемых канала (услуги) используют различные системы CA/DRM. Следует отметить, что не предполагается, что система CA/DRM должна заменяться во время регулярного изменения канала (услуги).

[R 13] Все связанные с ECI направления деятельности (например, обычная работа, загрузка **клиента ECI**) не должны оказывать заметного **воздействия** на опыт пользователя и показатели деятельности.

6.5 Требования, связанные с заменой клиента ECI

[R 14] **Встроенный CI** должен обеспечивать возможность перейти к новому поставщику услуг без необходимости получения согласия от производителя CA/DRM, производителя устройства, платформы или оператора услуги.

[R 15] В случае замены клиента ECI время прекращения услуг должно быть ограничено до минимума.

[R 16] После замены **клиента ECI** потребление **защищенного контента** (например, скремблированного контента PVR), приобретенного законным образом перед заменой, должно быть возможным без необходимости каких-либо сложных действий со стороны пользователя.

[R 17] **Встроенный CI** не должен неоправданно ограничивать возможности поставщиков CA/DRM по разработке различных функционально совместимых/сменных **клиентов ECI** в соответствии с потребностями рынка.

6.6 Требования, связанные с безопасностью систем ECI

[R 18] Необходимо, чтобы можно было безопасным образом загрузить, установить и заменить **клиента ECI** для CPE и чтобы делать это можно было стандартизированным образом. Загрузка и установка **клиента ECI** должны осуществляться только на основе стандартизированных решений.

[R 19] CPE должно обеспечивать **хранилище программного обеспечения**, которое должно предоставлять единый уровень абстракции для любого клиента ECI. Следует отметить, что единый уровень абстракции − это то, что виртуальная машина будет обеспечивать клиенту ECI.

[R 20] **Клиенты ECI** и система **хоста** должны быть способны в любое время доказать и подтвердить свою надежность.

[R 21] **Встроенный CI** должен обеспечивать разработку и создание **доверительного органа**.

[R 22] **Встроенный CI** не должен зависеть от того или иного специального аппаратного обеспечения (компонента) или конкретной представляемой операционной системы. Это требование как правило не запрещает передовые средства защиты, пока спецификации таких средств общедоступны и соответствуют сегодняшним архитектурам безопасности соответствующих поставщиков микросхем CPE. Следует отметить, что передовые системы безопасности, указанные в том или ином общедоступном документе, не рассматриваются в качестве специального аппаратного обеспечения.

[R 23] Система **встроенного CI** не должна позволять переход существующего DVB/ETSI, совместимого с системами CA/DRM, к этой новой системе **встроенного CI**. Следует отметить, что это подразумевает, что оператор с существующей у него системой CA/DRM может работать как с традиционными устройствами, так и с новыми совместимыми с ECI устройствами, управляя клиентом ECI, совместимым с существующей системой CA/DRM.

[R 24] **Встроенный CI** должен обеспечивать добавочные блоки, позволяющие дальнейшую разработку **встроенного CI** и реализаций ECI с обратной совместимостью. Должна существовать возможность того, чтобы существующие реализации ECI могли учитывать права на использование, введенные будущими расширениями характеристик возможностей CPE или возможностей клиента ECI.

[R 25] **Встроенный CI** должен поддерживать обе реализации системы со смарт-картами и без них в качестве устройств защиты и должен обеспечивать ресурсы для обоих типов решений.

[R 26] **Встроенный CI** должен обеспечивать необходимые функциональные возможности для всех уровней безопасности контента, требуемой для различных приложений систем CA/DRM. Он должен быть применимым к массовым рынкам и ко всему диапазону платных продуктов − от продуктов нижнего ценового сектора до продуктов с премиальной наценкой.

[R 27] В случае замены клиента ECI **встроенный CI** не должен требовать замены какого бы то ни было компонента аппаратного обеспечения. Однако, согласно этому требованию, замена смарт-карты систем CA/DRM на базе смарт-карт, как правило, не рассматривается в качестве замены компонента аппаратного обеспечения.

[R 28] **Встроенный CI** не должен требовать существенно больше ресурсов (вычислительной мощности, памяти и т. д.) устройства CPE, чем совместимые, имеющиеся на текущий момент встроенные системы CA/DRM, а реализация системной архитектуры не должна подразумевать существенно более высокую/дополнительную стоимость.

[R 29] **Встроенный CI** должен поддерживать по меньшей мере DVB CSA и системы скремблирования усовершенствованного стандарта шифрования (AES), а хост должен поддерживать по меньшей мере транспортный поток MPEG (ISO/IEC 13818-1 [b- ITU-T H.222.0]) и ISOBMFF (ISO/IEC 14496-12 [b- ISO/IEC 14496-12:2012], включая Поправку 3, в соответствии с сигнализацией, определенной в общепринятой схеме шифрования, которая описана в документации ISO/IEC 23001-7 [b- ISO/IEC 23001-7:2011], но потенциально с разным алгоритмом шифрования). Следует отметить, что поддержка этого требования будет совместимой с DRM, которые в настоящее время используются в DECE, и обеспечит стандартный формат для других случаев DRM, принятых для поддержки **встроенного CI**.

[R 30] **Встроенный CI** должен поддерживать широкий диапазон прав на использование путем обеспечения надлежащих функциональных возможностей интерфейса между хранилищем ECI и хостом.

[R 31] Встроенный CI должен быть способен описать права на использование и возможности использования клиенту ECI или различным клиентам ECI.

[R 32] Встроенный CI должен обеспечивать надежный канал связи между клиентами ECI либо по одному и тому же устройству, либо по различным устройствам.

Приложение A

Сценарии использования

(Данное Приложение является неотъемлемой частью настоящей Рекомендации.)

Список сценариев использования, рассматриваемых в Приложении A, не является исчерпывающим.

A.1 Сценарий использования 1

В бизнес-среде цифрового ТВ могут возникать различные причины, по которым требуется поменять систему CA/DRM в оборудовании CPE.

- Поставщик цифрового мультимедийного контента может решить изменить систему CA/DRM в CPE для своих клиентов. Причины могут быть следующими:
  - Различные технические или коммерческие причины, такие как требования, касающиеся расширенных функциональных возможностей CA/DRM, более высоких уровней безопасности или более высоких показателей работы системы, или же случай глубокого хакерского проникновения в существующую систему.
  - Привлечение новых клиентов в ту или иную сеть, которая использовалась для доступа к услугам конкурента.
- Оператор платформы может решить изменить систему CA/DRM в CPE в рамках своей платформы. Причины могут быть следующими:
  - Различные технические или коммерческие причины, такие как требования, касающиеся расширенных функциональных возможностей CA/DRM, более высоких уровней безопасности или более высоких показателей работы системы, или же случай глубокого хакерского проникновения в существующую систему.
  - Согласование технологий после приобретения сети.
- Поставщик CA/DRM привлекает нового клиента, который эксплуатирует платформу, где конкурент уже установил свою систему CA, или поставщик CA/DRM сменяет другого поставщика CA/DRM и хочет согласовать технологии обеспечения безопасности.
- Конечный пользователь приобрел CPE в том или ином магазине и подключил его к сети в сети доступа поставщика A. По этой сети свои услуги предлагают один или несколько поставщиков услуг. Конечный пользователь может выбрать любую из этих услуг и загрузить свою систему CA/DRM, если он зарегистрирован (включая аутентификацию и авторизацию) у соответствующего поставщика услуг. Через некоторое время этот же конечный пользователь решает подключиться к сети в сети доступа поставщика B. Он подключает свое CPE к этой сети. Если его CPE поддерживает требуемые технологии приема (например, DVB-C/C2, -S/S2, -T/T2, Ethernet, xDSL), по этой сети свои услуги могут предоставлять один или более поставщиков услуг. Конечный пользователь может выбрать любую из этих услуг и соответствующим образом поменять/заменить системы CA/DRM, если он зарегистрирован (включая аутентификацию и авторизацию) у соответствующего поставщика услуг.
- Производитель CE хочет представить на розничном рынке CPE, которое поддерживает как бесплатное, так и платное ТВ. Но CPE может быть адаптировано для использования с конкретными услугами платного ТВ путем обновления программного обеспечения с согласия конечного пользователя.

A.2 Сценарий использования 2

В настоящее время, если система CA установленной базы CPE операционной платформы CA должна быть заменена (по какой бы то ни было причине), в этом всегда задействованы четыре стороны:

- нынешний поставщик CA;
- оператор платформы или поставщик цифрового мультимедийного контента;
- производитель CPE;
- новый поставщик CA.

Текущий поставщик CA должен предоставить новому поставщику как техническую информацию для доступа в установленную базу CPE, так и лицензию на использования некоторых компонентов аппаратного обеспечения, протоколы или элементы программного обеспечения, внедренные в это CPE. В любом случае новый поставщик CA должен адаптировать свою систему CA к функциональным возможностям, ограничениям аппаратного/программного обеспечения и протоколам, имеющимся в CPE на местах. Производители CPE должны интегрировать новую систему CA в программное обеспечение различного установленного CPE. В наихудшем случае замена системы CA/DRM может даже оказаться нецелесообразным техническим/коммерческим вариантом. Для обеспечения большей функциональной совместимости такую ситуацию следует изменить.

Поскольку в настоящее время проприетарные модули безопасности являются неотъемлемой частью большинства современных систем CA, CPE производится по большей части для специализированных систем CA. Это может ограничивать уровень безопасности, который может обеспечиваться замененной системой CA для CPE на местах. Такую ситуацию следует изменить таким образом, чтобы любое усовершенствования в области безопасности было в полной мере переносимым.

A.3 Сценарий использования 3

Система ECI должна поддерживать только ориентированные на потребление приложения, в том числе доставку **защищенного контента** на вспомогательные устройства. К поддержке приложений вспомогательных устройств относятся два сценария использования:

- централизованное приложение: тип шлюза, CPE, совместимое с ECI, доставляет вспомогательному устройству информацию о правах на использование (URI) и зашифрованный контент;
- децентрализованное приложение: тип шлюза, CPE, совместимое с ECI, доставляет вспомогательному устройству только URI, а вспомогательное устройство извлекает зашифрованный контент из сети. Следует отметить, что в системе ECI не имеется требований в отношении включения клиента DRM во вспомогательное устройство. Для доставки защищенного контента от шлюза до вспомогательного устройства необходимо только, чтобы два клиента DRM могли безопасным образом осуществлять связь между собой и чтобы владелец контента поддерживал внедренную систему DRM.

A.4 Сценарий использования 4 (Сценарии использования, связанные с доверенной третьей стороной (TTP))

В настоящее время любые требуемые уникальные идентификаторы или сертификаты встроены в CPE проприетарным образом, определенным поставщиком системы CA/DRM. В аспекте функциональной совместимости это не является подходящим решением, поскольку поставщики, наиболее вероятно, не будут раскрывать механизмы доступа к своим уникальным идентификаторам или сертификатам. Например, консорциум CI plus продемонстрировал, что целесообразно передавать защищенное управление сертификатами "доверенной третьей стороне". Для функционально совместимых систем CA/DRM потребуются аналогичные решения.

Библиография

[b-ITU-T H.222.0] Рекомендация МСЭ-Т H.222.0 (2006 г.) | ISO/IEC 13818-1 (2007), *Информационная технология – Общее кодирование подвижных изображений и соответствующей аудиоинформации: Системы*.

[b-ETSI GS ECI 001-3] ETSI GS ECI 001-3, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 3: The CA/DRM Container: Loader, Interfaces, Revocation*.

[b-ETSI GS ECI 001-4] ETSI GS ECI 001-4, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 4: The Virtual Machine*.

[b-ETSI GS ECI 001-5] ETSI GS ECI 001-5, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 5: The Advanced Security System*.

[b-ETSI GS ECI 001-6] ETSI GS ECI 001-6, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 6: Trust Environment*.

[b-ETSI GS ECI 001-7] ETSI GS ECI 001-7, *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; Part 7: Extended Requirements*.

[b-ETSI ISG ECI] ETSI ISG ECI White Paper-v1_20 (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions*.

[b-ISO/IEC 14496-12] ISO/IEC 14496-12:2012, *Information Technology – Coding of Audio Visual Objects – Part 12: ISO Base Media file format*.

[b-ISO/IEC 23001-7] ISO/IEC 23001-7:2011, *Information technology – MPEG systems technologies – Part 7: Common encryption in ISO base media file format files*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	**Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов**
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	Сети передачи данных, взаимосвязь открытых систем и безопасность
Серия Y	Глобальная информационная инфраструктура, аспекты межсетевого протокола, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2017 г.