Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

J.1011

(09/2016)

СЕРИЯ J: КАБЕЛЬНЫЕ СЕТИ И ПЕРЕДАЧА СИГНАЛОВ ТЕЛЕВИЗИОННЫХ 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; архитектура, определения и обзор

Рекомендация МСЭ-Т J.1011

ITU-T

Международный союз электросвязи

Рекомендация МСЭ-Т J.1011

Встроенный общий интерфейс для заменяемых решений CA/DRM; архитектура, определения и обзор

Резюме

В Рекомендации МСЭ-Т J.1011 определена архитектура 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-Т J.1011	02.09.2016 г.	9-я	11.1002/1000/12773

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 2018

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.
1	Сфера применения	1
2	Справочные документы	1
3	Определения	1
3.1	Термины, определенные в других документах	1
3.2	Термины, определенные в настоящей Рекомендации	1
4	Сокращения и акронимы	2
5	Условные обозначения	3
6	Архитектура заменяемых встроенных решений CA/DRM	3
6.1	Общие замечания	3
6.2	Техническая концепция системы ECI	5
7	Доверительная среда	11
7.1	Необходимые функциональные рабочие процессы	12
Дополнение I – Внедрение совместимой с ECI доверительной системы		15
Библиография		17

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. Если, по существу, CA сосредоточен на механизмах доступа к защищенному контенту, распределяемому по сети поставщиком услуг, то 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, телевидения на основе протокола Интернет (IPTV) или новых услуг на базе технологии over-the-top (OTT), 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 более дешевыми 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 эффектам "жесткой привязки" оборудования, что серьезно ограничивает свободу многих участников рынка цифрового мультимедийного контента. Благодаря техническому прогрессу 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.1011

Встроенный общий интерфейс для заменяемых решений CA/DRM; архитектура, определения и обзор

1 Сфера применения

Цель данной Рекомендации – определить функциональные объекты архитектуры для заменяемого встроенного общего интерфейса, что позволит загружать в CPE любую необходимую систему CA/DRM. Процесс загрузки осуществляется в условиях безопасной среды и позволяет принимать защищенный контент, передаваемый на различные виды оконечного оборудования посредством радиовещания и/или широкополосной связи в соответствии с правами конечного пользователя на приобретаемый контент. Настоящая Рекомендация является одной из ряда Рекомендаций, определяющих экосистему встроенного общего интерфейса (ECI) в целом.

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.

[ETSI GS ECI 001-1] ETSI GS ECI 001-1 (2014), *Embedded Common Interface (ECI) for exchangeable CA/DRM solutions; 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 усовершенствованная система безопасности (advanced security): Функция устройства CPE, соответствующего спецификации ECI, обеспечивающая повышенный уровень безопасности (оборудования и программного обеспечения) для клиента ECI. Следует отметить, что подробная информация приведена в [b-ETSI GS ECI 001-5].

3.2.2 ECI (встроенный CI) (ECI (embedded CI)): Архитектура и система, определяемая в ETSI ISG "встроенный CI", которая позволяет разрабатывать и внедрять программно заменяемые клиенты ECI в комплекты оборудования в помещении пользователя (CPE), тем самым обеспечивая функциональную совместимость устройств CPE с интерфейсом ECI.

3.2.3 клиент ECI (клиент встроенного CI) (ECI client (embedded CI client)): Практическая реализация клиента CA/DRM, соответствующая спецификациям встроенного интерфейса CI. Следует отметить, что данным термином обозначается программный модуль в оборудовании CPE, который обеспечивает возможность безопасного получения контента и контроля за осуществлением прав или привилегий потребителя в отношении этого контента, предоставляемого его поставщиком или оператором. Кроме того, этот модуль получает информацию об условиях, согласно которым право или привилегия могут быть использованы потребителем, а также ключи для расшифровки различных сообщений и контента.

3.2.4 загрузчик клиента ECI (ECI client loader): Часть программного модуля хоста ECI, которая позволяет загружать, проверять и устанавливать новое программное обеспечение для клиента ECI в контейнере ECI хоста ECI.

3.2.5 контейнер ECI (контейнер встроенного CI) (ECI container (embedded CI container)): Абстрактное понятие, определяющее изолированную среду, состоящую из виртуальной машины и отдельного клиента ECI.

3.2.6 хост ECI (ECI host): Аппаратная и программная система в составе CPE, которая реализует ряд относящихся к ECI функций и связана с клиентом ECI специальными интерфейсами. Следует отметить, что хост ECI – это часть прошивки устройства CPE. Хост ECI отвечает за изоляцию каждого контейнера ECI и обеспечивает аутентифицированную загрузку клиентов ECI.

3.2.7 загрузчик хоста ECI (ECI host loader): Программный модуль, который позволяет загружать, проверять и устанавливать (новое) программное обеспечение хоста ECI в устройство CPE. Следует отметить, что в конфигурации многоступенчатой загрузки данный термин используется для обозначения всех критичных с точки зрения безопасности функций загрузки, задействованных при загрузке хоста ECI.

3.2.8 доверительный орган (trust authority (TA)): Организация, определяющая все правила и регуляторные положения, применяемые при внедрении ECI. Следует отметить, что доверительный орган должен являться юридическим лицом с правом подачи исковых заявлений. Доверительный орган должен быть объективен ко всем лицам, имеющим отношение к доступной для скачивания экосистеме CA/DRM.

3.2.9 доверенная третья сторона (trusted third party (TTP)): Поставщик услуг по техническому обслуживанию, который выдает сертификаты и ключи производителям соответствующих компонентов системы ECI под контролем доверительного органа (TA).

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

API	Application Programming Interface	Интерфейс прикладного программирования
CA	Conditional Access	Условный доступ
CENC	Common Encryption	Общее шифрование
CI	Common Interface	Общий интерфейс
CPE	Customer Premises Equipment	Оборудование в помещении пользователя
DRM	Digital Rights Management	Управление цифровыми правами
DVB	Digital Video Broadcasting	Цифровое телевизионное вещание
ECI	Embedded Common Interface	Встроенный общий интерфейс
HD	High Definition	Высокая четкость
HTTP	Hypertext Transfer Protocol	Протокол передачи гипертекста
iDTV	integrated Digital TV	Интегрированное цифровое телевидение
IP	Internet Protocol	Протокол Интернет
IPTV	Internet Protocol Television	Телевидение на основе протокола Интернет
LA	License Agreement	Лицензионное соглашение
MPEG	Motion Picture Experts Group	Экспертная группа по движущимся изображениям
OS	Operating System	Операционная система
OSD	On Screen Display	Отображение на экране
OTT	Over-The-Top	Технология OTT (доставка контента пользователю интернета напрямую через протокол HTTP)
PIN	Personal Identification Number	Персональный идентификационный номер

PVR	Personal Video-Recorder	Персональный видеомагнитофон
ROM	Read Only Memory	Постоянное запоминающее устройство
SI	Service Information	Служебная информация
STB	Set-Top Box	Абонентская приставка
TA	Trust Authority	Доверительный орган
TTP	Trusted Third Party	Доверенная третья сторона
TV	Television	Телевидение
UI	User Interface	Пользовательский интерфейс
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 этой Рекомендации;

ключевое слово "рекомендуется" означает требование, которое рекомендуется, но не является абсолютно необходимым. Таким образом, для заявления о соответствии данное требование не является обязательным;

ключевое слово "запрещается" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии этой Рекомендации;

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

В тексте настоящей Рекомендации и приложений к ней иногда встречаются слова *должен, не должен, следует* и *может*, и в таком случае их следует понимать как *требуется, чтобы, запрещается, 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 Архитектура заменяемых встроенных решений CA/DRM

6.1 Общие замечания

Архитектура, определения и обзор ECI, рассматриваемые в настоящей рамочной Рекомендации, являются частью стандарта (состоящего из нескольких частей), определяющего системную архитектуру для программных, встроенных и заменяемых систем CA/DRM общего назначения, которые могли бы стать наиболее подходящим и перспективным решением, способным преодолеть раздробление рынка и обеспечить функциональную совместимость. Предлагаемый подход к защите контента обладает следующими ключевыми преимуществами:

– гибкость и масштабируемость, возможные благодаря реализации на основе программного обеспечения;

– заменяемость, позволяющая применять перспективные и инновационные технические решения;

– возможность применения для распределения контента по сетям радиовещания и широкополосной связи, включая технологию OTT;

– поддержка многоэкранной среды;

– отсутствие "жесткой привязки" оборудования, стимулирующее рынок для операторов платформ, поставщиков сетей/услуг и потребителей;
– спецификация открытой экосистемы, способствующая развитию рынка.

Целью внедрения систем ECI является заменяемость систем CA и DRM в устройствах CPE на всех соответствующих уровнях и во всех аспектах, обеспечивая минимально возможные затраты для потребителей и минимальные ограничения для поставщиков систем CA и DRM при продвижении намеченной к выпуску продукции на рынке платного телевидения. Ключевой функцией системы ECI является организация интерфейса между клиентом программно реализуемой системы CA/DRM и центральной системой (хостом). Таким образом система ECI обладает, помимо прочего, следующими функциональными возможностями:

– программный контейнер для ядра CA и, соответственно, DRM (далее именуемый клиентом ECI), оборудованный:
  • стандартизированными интерфейсами для подключения ко всем необходимым функциям устройства CPE;
  • стандартизированной виртуальной машиной (VM), под управлением которой работает система;
– поддержка систем, работающих без смарт-карт, а также систем на базе смарт-карт;
– к устройству CPE могут подключаться несколько таких контейнеров, каждый из которых работает под управлением собственной копии VM;
– установка клиента ECI независимо от другого программного обеспечения CPE с использованием концепции надежного и стандартизированного загрузчика;
– усовершенствованная система безопасности, известная как система защиты на уровне набора микросхем, позволяющая обеспечить защиту контента на современном уровне;
– меры по максимально эффективному использованию средств защиты, обеспечиваемых аппаратурой;
– методы, позволяющие пользователю обнаружить подходящую программу клиента ECI для загрузки;
– методы частичного или полного аннулирования функциональных возможностей клиента ECI и устройства CPE;
– поддержка традиционного цифрового радиовещания, IPTV и современных систем на базе технологии OTT.

Хотя система ECI обладает некоторым сходством с уже применяемыми техническими решениями, между ними есть существенные различия:

1) клиентский модуль CA/DRM является уже полностью программным, а не аппаратным. Таким образом при замене системы CA или DRM потребитель не понесет дополнительных расходов;
2) в одном и том же устройстве CPE может быть установлено несколько параллельных клиентов ECI, при этом дополнительные затраты не требуются;
3) эти клиенты могут функционировать одновременно на одном устройстве.

В результате значительно упрощается замена компонентов CA или DRM, что дает возможность конечному пользователю сменить оператора либо воспользоваться услугами различных операторов на своем устройстве CPE без необходимости замены дорогостоящих модулей.

Полный стандарт, состоящий из группы спецификаций, включает основную (структурную) спецификацию в сочетании с несколькими базовыми спецификациями:

– часть 1: Architecture, Definitions and Overview (Архитектура, определения и обзор) [ETSI GS ECI 001-1];
– часть 2: Use cases and requirements (Сценарии использования и требования) [ETSI GS ECI 001-2];
– часть 3: CA/DRM Container, Loader, Interfaces, Revocation (Контейнер, загрузчик, интерфейсы, аннулирование сертификатов CA/DRM) [b-ETSI GS ECI 001-3];

– часть 4: The Virtual Machine (VM) (Виртуальная машина) [b-ETSI GS ECI 001-4];

– часть 5: The Advanced Security System (Усовершенствованная система безопасности) [b-ETSI GS ECI 001-5];

– часть 6: Trust Environment (Доверительная среда) [b-ETSI GS ECI 001-6];

– часть 7: Extended Requirements (Расширенные требования) [b-ETSI GS ECI 001-7],

которые в совокупности формируют решение, позволяющее в любое время осуществлять замену клиентов ECI путем загрузки клиентов ECI по запросу конечного пользователя. Клиенты ECI устанавливаются в стандартный программный контейнер устройства CPE при помощи отдельного загрузчика с использованием отдельных алгоритмов обеспечения безопасности и ключей для защиты клиентов ECI от несанкционированных действий, связанных с нарушением целостности и заменой сообщений, независимо от других программ, установленных в устройстве CPE. Контейнер соединен с CPE через интерфейсы широкого применения, описываемые в [b-ETSI GS ECI 001-3], что дает возможность клиенту ECI взаимодействовать с различными функциями в устройстве CPE и за его пределами.

Клиенты ECI работают под управлением копии виртуальной машины, описываемой в [b-ETSI GS ECI 001-4].

В [b-ETSI GS ECI 001-5] описывается механизм работы усовершенствованной системы безопасности по защите ключа доступа к контенту в процессе его поступления в устройство дешифровки контента, входящее в состав микросхемы процессора CPE.

В настоящей Рекомендации рассматривается архитектура и дается обзор соответствующих спецификаций интерфейса в целях внедрения функционально совместимых систем CA/DRM в устройства CPE.

Спецификация ECI может применяться исключительно к процессу приема и дальнейшей обработки контента, контролируемого системой условного доступа и/или системой управления цифровыми правами и зашифрованного поставщиком услуг. Контент, не контролируемый системой условного доступа и/или системой DRM, не рассматривается в настоящей Рекомендации.

Групповая спецификация ECI предназначена для использования совместно с договорной базой (лицензионным соглашением), правилами соответствия и обеспечения устойчивости, а также установленным порядком сертификации (см. Примечание) под контролем доверительного органа [b-ETSI GS ECI 001-6]. Следует отметить, что договорная база (лицензионное соглашение), правила соответствия и обеспечения устойчивости, а также установленный порядок сертификации не входят в перечень работ по стандартизации, выполняемых в ISG ECI.

6.2 Техническая концепция системы ECI

6.2.1 Основные принципы

Настоящая Рекомендация в сочетании с частями 2–5 и 7 спецификаций ([ETSI GS ECI 001-2], [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4], [b-ETSI GS ECI 001-5] и [b-ETSI GS ECI 001-7]) определяет архитектуру, которая позволяет загружать, устанавливать, обновлять, удалять и заменять клиентов ECI в любой момент независимо от других клиентов ECI, работающих на том же хосте, системных программ или приложений хоста CPE, работающих на этом хосте. Хост ECI должен быть способен разместить и обеспечить работу среды исполнения для как минимум двух или для максимально возможного (с учетом ресурсных возможностей по обработке) количества клиентов ECI. Клиенты ECI должны запускаться на хосте параллельно, обеспечивая одновременное дешифрование и повторное шифрование разнообразных потоков контента от различных операторов.

Техническая концепция, описываемая в настоящей Рекомендации и определяемая в [ETSI GS ECI 001-2], [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] и [b-ETSI GS ECI 001-5], может применяться как к системам CA, совместимым с DVB Multicrypt, так и к системам DRM, совместимым с общими алгоритмами шифрования (CENC).

На устройстве CPE устанавливается загрузчик, предназначенный специально для клиентов ECI и обладающий функциями безопасности, необходимыми для защиты целостности и аутентичности клиентов ECI. Этот загрузчик может быть вызван и запущен в любое время для загрузки и проверки

нового клиента ECI. Загрузчик и связанные с ним средства обеспечения безопасности описываются в [b-ETSI GS ECI 001-3].

Согласно данной технической концепции каждый клиент ECI устанавливается в отдельный программный контейнер с собственной копией виртуальной машины (VM), как указано в [b-ETSI GS ECI 001-4]. Контейнер ECI определяется только для набора функций CA/DRM, приведенного в [b-ETSI GS ECI 001-3]. Интерфейс связи с CPE, подробно описываемый в [b-ETSI GS ECI 001-3], позволяет отправлять запросы и обмениваться данными, необходимыми для работы различных функций CA/DRM. Такие запросы и обмены данными могут осуществляться между клиентом ECI и хостом, между двумя клиентами ECI, работающими на одном хосте, или двумя клиентами ECI, работающими на разных хостах.

ТВ-ориентированные устройства по определению обладают встроенной в набор микросхем функцией обработки транспортного потока MPEG-2. Согласно требованиям ECI данные наборы микросхем должны реализовывать функциональные возможности усовершенствованной системы безопасности, соответствующие ECI. В [b-ETSI GS ECI 001-5] определяется порядок использования механизмов усовершенствованной системы безопасности в выборах микросхем, таких как защита ключа, связанного с контентом, в процессе его передачи для обработки функцией дешифровки контента, встроенной в процессор CPE. Концепция усовершенствованной системы безопасности позволяет всем клиентам ECI, использующим данную функцию, при необходимости работать одновременно и независимо друг от друга.

Программное обеспечение устройств, предназначенных для работы в других условиях, в особенности устройств IPTV, планшетов, смартфонов и т. д., как правило, обладает более широким набором функций и обеспечивает двустороннюю связь по IP. Это позволяет задействовать особые, новые виды механизмов повышения уровня безопасности. В наборы микросхем, используемые в данных устройствах, встроены элементы, обеспечивающие функции безопасной обработки. При этом, согласно требованиям ECI, для соответствия спецификациям ECI необходима аппаратная реализация специальных функций обеспечения безопасности и устойчивости. Таким образом спецификация [b-ETSI GS ECI 001-3] включает методы, позволяющие клиенту ECI по мере необходимости получать соответствующие параметры технических и функциональных возможностей хоста, включая возможную поддержку усовершенствованной системы безопасности, как указано в [b-ETSI GS ECI 001-5].

Функциональные возможности усовершенствованной системы безопасности одновременно доступны для всех клиентов ECI, функционирующих в устройстве CPE. Клиенты ECI могут также устанавливаться на платформах с системами CA, совместимыми с DVB, или системами DRM, совместимыми с CENC, работающими в режиме Simulcrypt или Multicrypt, при условии, что со стороны сервера эти системы совместимы с соответствующими внутренними стандартами DVB/CENC.

6.2.2 Общие сведения о структуре

Система ECI позволяет поставщикам CA/DRM реализовывать решения, касающиеся условного доступа (CA) и управления цифровыми правами (DRM), в пределах зоны размещения отдельного пользователя. На рисунке 1 приведена эталонная конфигурация, которая полностью поддерживается установленной системой ECI.

В целях поддержки многоэкранных сред в пределах зоны размещения отдельного пользователя клиенты ECI в рамках этой зоны могут связываться друг с другом или использовать двустороннее сетевое соединение с поставщиком услуг в зависимости от доступности надлежащих сетей или дополнительных функциональных возможностей в системах CA/DRM и их клиентах ECI. Более подробная информация содержится в [b-ETSI GS ECI 001-3].

Клиент ECI может быть выполнен таким образом, чтобы обеспечивалась его работа в качестве шлюза, в том числе для клиентов, несовместимых с ECI. Соответствующие программные процедуры описаны в [b-ETSI GS ECI 001-5]. Конкретные протоколы и возможная реализация проприетарных клиентов выходят за рамки спецификаций ECI.

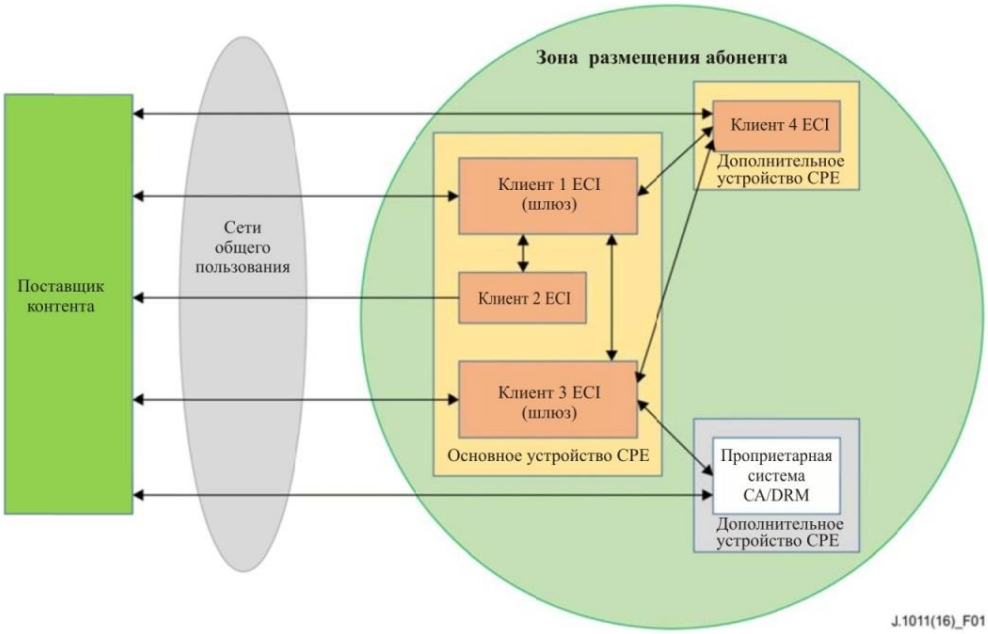

Рисунок 1 – Клиенты ECI в пределах зоны размещения отдельного пользователя

Спецификации ECI, помимо прочего, определяют интерфейс между контейнером ECI и хостом ECI. На рисунке 2 показана блок-схема CPE с контейнерами ECI, а также другие функции хоста ECI, с которым связываются или могут связаться контейнеры ECI. Некоторые из этих функций являются необязательными. В процессе установки клиента ECI и в процессе его запуска хост определяет, какие из его функций доступны для клиента ECI.

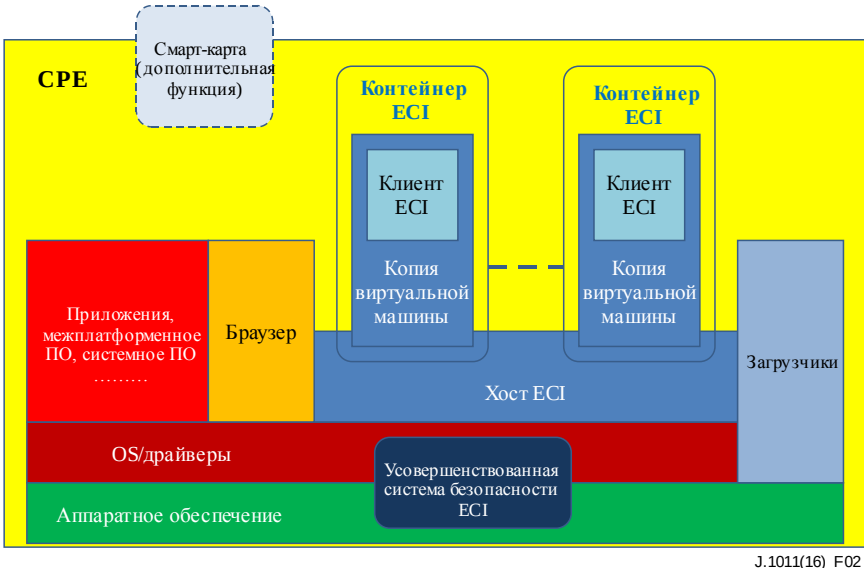

Рисунок 2 – Блок-схема CPE со встроенными клиентами ECI, каждый из которых имеет собственный контейнер ECI и копию виртуальной машины

Рассматриваемая концепция основывается прежде всего на иерархической системе загрузки (см. рисунок 3), состоящей из загрузчика на базе микросхем, загрузчика системного программного обеспечения и загрузчика клиента ECI.

Загрузчик хоста ECI загружает программное обеспечение хоста ECI. Помимо прочего, эта операция включает виртуальную машину, доступ к компонентам усовершенствованной системы безопасности

и загрузчик клиента ECI. Хост ECI может загружать несколько клиентов ECI в отдельные копии виртуальной машины, которые запускаются раздельно и изолированы друг от друга.

При загрузке клиента ECI в данную систему создается копия виртуальной машины, в которую загружается клиент ECI. Эта копия VM играет роль "песочницы" между клиентом ECI и хостом. Интерфейс между клиентом ECI и копией VM является основным типом интерфейса, определяемым посредством групповой спецификации (GS). Помимо этого, интерфейс определяет информационный поток/протокол между несколькими копиями такого клиента ECI и другими функциями внутри CPE, например усовершенствованной системой безопасности, дисплеем и т. д. Следует отметить, что другой клиент ECI не обязательно должен находиться на том же самом хосте ECI. Этот интерфейс и протокол связи описываются в [b-ETSI GS ECI 001-3].

Сам по себе хост ECI зависит от конфигурации, заданной производителем. Он связан интерфейсом с операционной системой и уровнем драйверов и обеспечивает все наборы функций, определяемые спецификациями интерфейса клиента ECI. Хост ECI не определяется системой ECI, однако в целях соответствия спецификациям интерфейса клиента ECI он должен быть сертифицирован доверительным органом (TA).

6.2.3 Функциональные возможности, обязательные для устройств, совместимых с ECI

Система ECI охватывает ряд сценариев использования (см. рисунок 1). Следовательно, интерфейс ECI должен взаимодействовать с самыми разными устройствами, такими как iDTV, STB, персональные видеомагнитофоны (PVR), IPTV, планшеты, смартфоны и т. п. Эти устройства отличаются своими функциональными возможностями, при этом интерфейс ECI обеспечивает согласованную защищенную структуру. ECI различает TB-ориентированные устройства и устройства, предназначенные для работы в других условиях, в том числе устройства IPTV и планшеты.

TB-ориентированные устройства по определению обладают функцией обработки транспортного потока MPEG-2 внутри набора микросхем. Согласно требованиям ECI данные наборы микросхем должны выполнять функции усовершенствованной системы безопасности, совместимой с ECI. Совместимые с ECI TB-ориентированные устройства CPE должны поддерживать функции, указанные в спецификациях [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] и [b-ETSI GS ECI 001-5].

Программное обеспечение устройств, предназначенных для работы в других условиях, в особенности IPTV, компьютеров, планшетов, как правило, реализует более широкий набор функций и обеспечивает двустороннюю связь по IP. Это позволяет использовать различные типы механизмов обеспечения безопасности. В наборы микросхем, используемые в данных устройствах, встроены элементы, обеспечивающие различные функции защищенной обработки; в этих микросхемах согласно требованиям ECI необходима аппаратная реализация специальных функций безопасности и устойчивости. Механизмы, необходимые для использования этих функций, определяются в [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] и [b-ETSI GS ECI 001-5].

6.2.4 Необходимые интерфейсы между хостом ECI и клиентом ECI

Контейнер ECI – это техническое понятие, объединяющее виртуальную машину и клиента ECI с целью изолировать и экранировать VM и клиента ECI от остальной части CPE. Виртуальная машина – это функциональный элемент хоста ECI. Загружая клиент ECI, хост ECI создает копию виртуальной машины. Виртуальная машина обеспечивает подключение к клиенту ECI через нужные интерфейсы и соединяет их с хостом ECI. Спецификация ECI определяет интерфейс между VM и клиентом ECI. См. также на рисунке 2 архитектуру высокого уровня для совместимого с ECI устройства. Интерфейс обеспечивает работу конкретных интерфейсов прикладного программирования (API), а также формирует защищенный канал связи.

В нижеследующем списке перечислены важнейшие программные интерфейсы:

– интерфейс передачи информации о пропускной способности клиенту ECI от хоста ECI и наоборот;
– интерфейс с устройством обработки входных и выходных сигналов CPE;
– интерфейс с блоком оборудования/драйверов усовершенствованной системы безопасности;
– интерфейс с функциями загрузчика;

– интерфейс для поддержки взаимодействия с пользователем;
– интерфейс с функциями шифрования и дешифрования;
– интерфейс с дополнительным считывающим устройством для смарт-карт;
– интерфейс со специальными функциями защиты, например методом снятия отпечатков пальцев и технологией встраивания водяных знаков;
– интерфейс с локальным хранилищем данных.

Все интерфейсы клиента ECI обеспечиваются при помощи виртуальной машины.

Наряду с интерфейсами существуют дополнительные протоколы связи, обеспечивающие безопасное соединение. В частности определяется протокол для соединения, устанавливаемого между клиентами ECI как внутренними, так и внешними.

CPE может подключаться к сети любого типа, а также к нескольким сетям одновременно как по одностороннему, так и по двустороннему соединению. Устройство не обязательно должно быть подключено к какой-либо сети (загруженному/сохраненному контенту).

6.2.5 Минимальный набор функций пользовательского интерфейса и отображения информации

Для контейнеров ECI должен быть обеспечен минимальный набор функций пользовательского интерфейса (UI) и отображения на экране (OSD), позволяющий устанавливать соединение с пользователем. Эти функции описываются в [b-ETSI GS ECI 001-3]. Они используются для отображения сообщений пользователям, сформированных или отправленных при помощи системы CA/DRM. Кроме того, эти функции позволяют пользователю вводить информацию, например персональный идентификационный номер (PIN). Более подробное описание приводится в [b-ETSI GS ECI 001-3].

Локальное взаимодействие пользователей с системой CA/DRM обеспечивается посредством клиента ECI.

6.2.6 Виртуальная машина

Клиент ECI работает под управлением стандартизированной виртуальной машины (VM). Этот компонент описывается в [b-ETSI GS ECI 001-4]. Каждый установленный клиент ECI должен иметь свою собственную копию VM. Копия VM обеспечивает безопасную среду для запуска приложений ядра системы условного доступа или клиента системы управления цифровыми правами. VM формирует интерфейсы API, при этом ресурсы среды хоста ECI доступны в стандартном режиме.

6.2.7 Функция "усовершенствованная система безопасности"

ECI определяет минимальный набор функций, необходимый для создания безопасной системы защиты контента. Для ECI требуется расширение технических возможностей на основе элементов оборудования. В ТВ-ориентированных устройствах это реализуется за счет специальных функций усовершенствованной системы безопасности. В системах-на-чипе (SoC) данная функция называется "Key Ladder Block" (многозвенный блок ключей). Важной задачей усовершенствованной системы безопасности является обеспечение безопасности ключей защиты контента в процессе их перенаправления от клиента ECI на модуль расшифровки контента в CPE или в процессе передачи защищенного контента от одного клиента ECI другому клиенту ECI (см. рисунок 1). Усовершенствованная система безопасности, описанная в [b-ETSI GS ECI 001-5], поддерживает различные параллельные потоки контрольных слов и нескольких клиентов ECI, одновременно посылающих ей запросы на обслуживание. Более того, функция усовершенствованной системы безопасности играет ключевую роль в процессе верификации загружаемого программного обеспечения для хоста и клиентов ECI.

Программное обеспечение устройств, предназначенных для работы в других условиях, в особенности IPTV, компьютеров и планшетов, как правило, реализует более широкий набор функциональных возможностей и обеспечивает двустороннюю связь по IP. ECI определяет те же принципы и механизмы усовершенствованной системы безопасности, однако порядок их применения к архитектурам безопасности устройств отличается [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4] и [b-ETSI GS ECI 001-5].

Информация о наличии усовершенствованной системы безопасности в устройстве CPE передается клиенту ECI в процессе ее установки и запуска.

6.2.8 Повторное скремблирование

Защищенный контент, принимаемый совместимым с ECI устройством CPE, может не использоваться непосредственно в момент получения. Для устройств, совместимых с ECI, доступны следующие функциональные возможности:

– локальное хранилище:
  - под контролем CPE;
  - под контролем клиента CA или DRM;
– шлюз:
  - передача элемента защищенного контента на внешнее устройство под контролем клиента DRM;
  - передача элемента защищенного контента другому клиенту ECI, установленному на том же устройстве CPE или работающему на другом совместимом с ECI устройстве CPE.

В целях поддержки перечисленных функций ECI-совместимое устройство способно выполнять повторное скремблирование контента. Система ECI не определяет ни механизмы транспортирования, ни доступные функциональные возможности DRM для хранения или передачи защищенного контента на другие устройства. Необходимые интерфейсы между хостом ECI и клиентом ECI определяются в [b-ETSI GS ECI 001-5].

6.2.9 Функциональные возможности загрузчика ECI

Совместимое с ECI устройство CPE должно осуществлять функции загрузчика, позволяющие производить загрузку и установку, а также обеспечить защиту целостности и защиту от подмены соответствующих программных модулей системы ECI.

Вначале загрузчик, интегрированный в микросхему, загружает программу-загрузчик системного программного обеспечения (ПО). Встроенный загрузчик должен обеспечивать возможность установки и запуска лишь сертифицированного загрузчика системного ПО. Загрузчик системного ПО включает загрузчик хоста ECI, следовательно, загрузчик системного ПО должен быть заверен доверительным органом. Загрузчик системного ПО может содержать загрузчики другого системного ПО, не относящегося к функциональным возможностям ECI и не связанного с элементами безопасности системы. Программное обеспечение хоста ECI включает загрузчик клиента ECI, который способен по запросу загружать клиента ECI.

В процессе установки в собственный контейнер ECI, а также в процессе своего запуска клиент ECI получает от хоста ECI информацию об имеющихся у него функциональных элементах, таких как устройства записи, устройства HD, устройство считывания смарт-карт, снятия отпечатков пальцев и нанесения водяных знаков, сети, а также информацию о соответствии требованиям основной спецификации (настоящей Рекомендации), [b-ETSI GS ECI 001-3], [b-ETSI GS ECI 001-4], [b-ETSI GS ECI 001-5] и, возможно, [b-ETSI GS ECI 001-6].

Загрузчик ECI и соответствующие средства обеспечения безопасности описываются в [b-ETSI GS ECI 001-3].

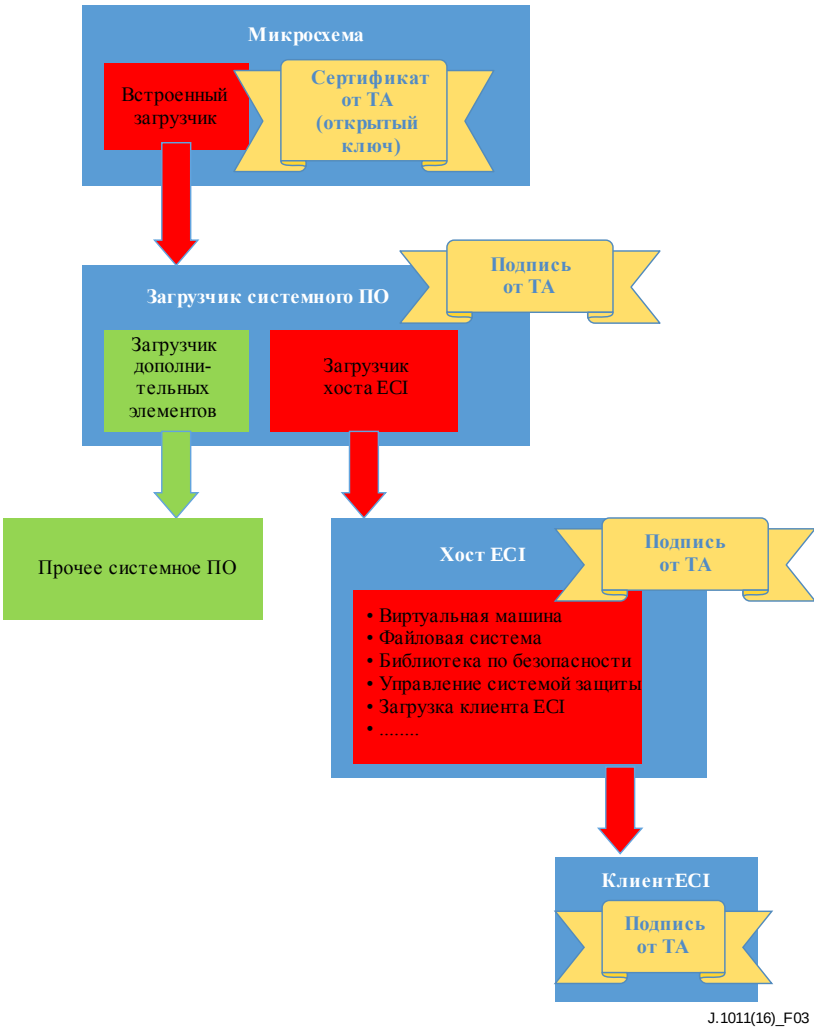

Рисунок 3 – Иерархическая концепция работы загрузчика

6.2.10 Аннулирование

Доверительный орган может принять решение о внесении какого-либо устройства CPE, ряда устройств CPE, того или иного типа устройств CPE или всех устройств CPE от конкретного производителя в "черный" список. Поставщик контента или оператор могут отозвать одно или несколько упомянутых устройств CPE из своего пункта распределения услуг. Применяемые методы позволяют другим операторам и поставщикам контента по своему усмотрению продолжать предоставление услуг владельцам данных устройств CPE.

В результате аннулирования могут быть заблокированы все услуги оператора или поставщика контента, предоставляемые упомянутым устройствам CPE или подгруппе служб. Этот процесс регулируется функциональными возможностями соответствующей системы CA и DRM и не входит в сферу применения настоящей Рекомендации.

Процесс аннулирования описывается в [b-ETSI GS ECI 001-3].

7 Доверительная среда

Для создания системы, основанной на встроенном CI, должна быть сформирована доверительная среда. Подробное описание доверительной среды выходит за рамки спецификаций ECI**.** Тем не менее принципы, приведенные в [b-ETSI GS ECI 001-6], необходимы для полного понимания механизма работы ECI.

Доверительный орган (TA) – это организация, определяющая все правила и регуляторные положения, применяемые при внедрении архитектуры ECI. Доверительный орган должен быть юридическим

лицом с правом подачи исковых заявлений. Доверительный орган должен быть объективен в отношении всех лиц, имеющих отношение к доступной для скачивания экосистеме CA/DRM. В их число входят:

– производители оборудования CPE;
– производители систем CA/DRM (клиентов ECI);
– производители наборов микросхем, компоненты которых включают постоянные ключи и сертификаты защищенных процессоров, необходимые для взаимодействия между хостом и совместимой системой CA/DRM;
– операторы платформ; оператор платформы – это участник, осуществляющий контроль над всеми необходимыми элементами системы CA/DRM. К примеру, операторами платформы могут быть поставщики услуг или операторы сетей;
– поставщики приложений (если это применимо).

Доверенная третья сторона (TTP) – поставщик услуг по техническому обслуживанию, который выдает сертификаты и ключи производителям соответствующих компонентов системы ECI. Надежность таких ключей и сертификатов подтверждается доверительным органом (TA**)**, у которого хранится корневой сертификат.

Доверительный орган и доверенная третья сторона формируют основу цепочки доверия и таким образом включаются во все процессы – от производства (микросхем и устройств CPE) и рабочих процедур (защищенной загрузки и активации клиента ECI) до мероприятий по контролю и управлению (например, аннулированию).

Доверительный орган как юридическое лицо обеспечивает функционирование доверительной среды на основе договорной базы, называемой также лицензионным соглашением, в рамках действия которого различные заинтересованные стороны могут принять на себя обязательства и распределить ответственность. В соответствии с лицензионным соглашением доверительный орган/доверенная третья сторона генерируют и предоставляют пары ключей, сертификаты, тестовые параметры доступа, идентификационные коды оператора и т. д.

Доверительные отношения между всеми участниками рынка определяются одним TA. Какой-либо другой TA не может определять доверительные отношения повторно для той же среды. При этом несколько TA могут существовать, например, в пределах страны, региона, сегментов, экосистем.

В случаях, когда несколько доверительных органов функционируют параллельно, необходимым предварительным условием является установление доверительных отношений между доверительным органом *A* и доверительным органом *B*, при которых устройства, зарегистрированные в доверительном органе *A*, могут использоваться в сфере действия доверительного органа *B*.

7.1 Необходимые функциональные рабочие процессы

В данном разделе приведены общие сведения о необходимых функциональных рабочих процессах, удовлетворяющих потребности различных участников рынка в целях развития бизнеса на основе технологий ECI. Кроме того, указанные рабочие процессы основываются на обязательных технических элементах, необходимых для внедрения системы ECI. На рисунке 4 показаны взаимосвязи между этими техническими компонентами и соответствующими участниками рынка.

ПРИМЕЧАНИЕ. – Данное описание является обобщенным и не связано с каким-либо из существующих проприетарных технических решений или проводимой в настоящее время деятельностью по стандартизации.

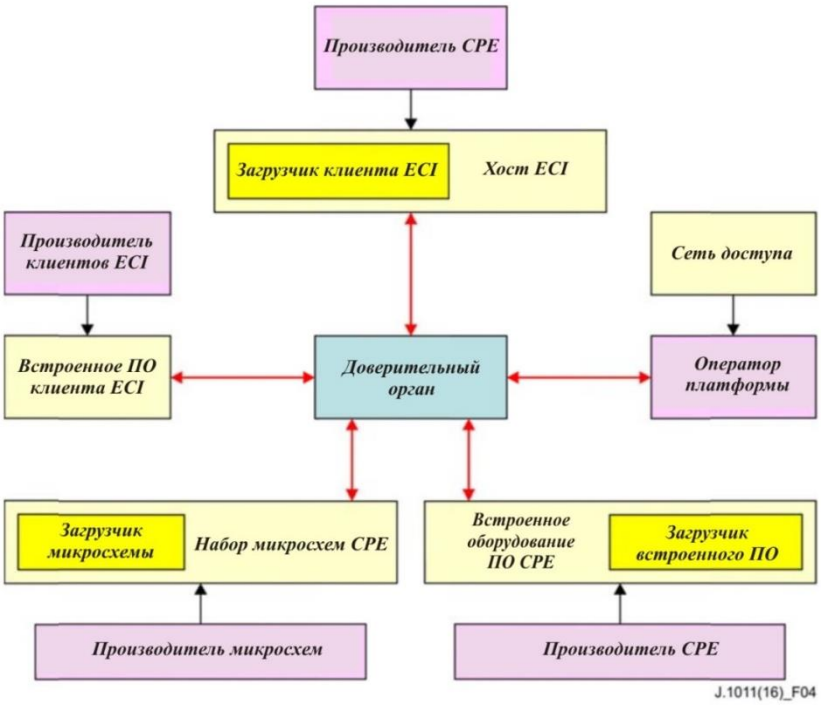

Рисунок 4 – Схема управления, необходимая для формирования доверительных отношений между доверительным органом (TA) и соответствующими участниками рынка

Эксплуатационные и соответствующие правовые аспекты (см. стрелки красного цвета на рисунке 4), необходимые для формирования доверительной среды.

1) Целостность

Целостность – это требование, согласно которому один из участников рынка имеет возможность проверки аппаратных/программных компонентов, предоставленных другим участником рынка, на предмет несанкционированной модификации и соответствия спецификациям и правилам обеспечения устойчивости. Данное требование может быть выполнено на основе надлежащих регистрационных данных, подписей и проверочных процедур, базирующихся на тестовых параметрах доступа, предоставленных доверительным органом/доверенной третьей стороной.

2) Аутентичность

Аутентичность означает, что любой аппаратный/программный компонент, предоставленный партнером по договору доверительного органа и прошедший необходимые этапы верификации и сертификации, может однозначно иметь отношение к данному партнеру по договору и, следовательно, может быть отличим от любых копий этого компонента. Аутентичность любого рассматриваемого аппаратного/программного компонента подтверждается любой системой ECI.

3) Договорная основа

Договорная основа, которую формирует доверительный орган как юридическое лицо, должна охватывать порядок соответствия спецификациям и обеспечения устойчивости, а также процедуры сертификации в целях создания условий для внедрения систем ECI.

4) Устранение проблем

В случае если аппаратные/программные компоненты системы ECI более не соответствуют спецификациям, доверительный орган устанавливает для поставщика данного компонента особые процедуры, позволяющие в приемлемые сроки восстановить целостность экосистемы.

Ключевые технические компоненты (на рисунке 4 обозначены желтыми прямоугольниками).

1) Набор микросхем CPE

Набор микросхем CPE – это основной компонент в составе оборудования CPE. В таком оборудовании, как правило, используются однокристалльные системы SoC, что обусловлено существующими требованиями операторов платформ и поставщиков контента. Кроме того, в микросхему CPE обычно входит загрузчик микросхемы.

2) Оборудование CPE

Ключевыми аспектами являются: безопасное внедрение набора микросхем CPE, предотвращение любого несанкционированного доступа к запоминающим устройствам (Flash, ROM) и защита интерфейсов.

3) Другие загрузчики

Загрузчик микросхем загружает различные дополнительные загрузчики в зависимости от аппаратной/программной конфигурации CPE.

4) Встроенное программное обеспечение CPE

Существуют различные каналы взаимодействия встроенного ПО устройств CPE с клиентом ECI и всеми соответствующими аппаратными интерфейсами CPE. Безопасность обеспечивается подробными спецификациями, а также подходящими правилами соответствия и обеспечения устойчивости.

5) Клиент ECI

Клиент ECI извлекает относящуюся к CA и DRM информацию, передаваемую внешними интерфейсами CPE, и инициирует соответствующие настройки в устройстве CPE (дескремблер, интерфейсы). Очевидно, что данный процесс требует тесного и безопасного взаимодействия со встроенным ПО устройства CPE.

Дополнение I

Внедрение совместимой с ECI доверительной системы

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В Дополнении I приведены общие сведения о необходимых функциональных рабочих процессах, удовлетворяющих потребности различных участников рынка в целях развития бизнеса на основе технологий ECI. На рисунке I.1 приводится общая схема рабочего процесса. Кроме того, указанные рабочие процессы основываются на обязательных технических элементах, необходимых для внедрения системы ECI. На рисунке 4 в разделе 7.1 показаны взаимосвязи между техническими компонентами и соответствующими участниками рынка.

ПРИМЕЧАНИЕ. – Доверенная третья сторона (TTP) и испытательный центр являются партнерами по договору доверительного органа (TA) в вопросах сертификации и генерации ключей.

Рисунок I.1 – Общая схема рабочего процесса

Правовая/договорная основа

Безопасное управление доверительными отношениями может осуществляться только в рамках четко определенной правовой и договорной основы, ключевым элементом которой является лицензионное соглашение (LA). TA заключает лицензионные соглашения с любым лицом, желающим внедрить спецификацию(и), будь то производители устройств CPE, поставщики систем CA/DRM, производители микросхем, поставщики прочих технологий, операторы платформ и т. д.

Таким образом, лицензионное соглашение является важнейшим инструментом, позволяющим TA формировать, поддерживать и представлять на горизонтальном рынке безопасный и в то же время удобный для пользователя метод получения и активации всех требуемых ключей и других необходимых материалов и информации, связанных с обеспечением безопасности, при подключении устройств CPE к выбранным поставщикам услуг, руководствующимся соответствующими правилами использования контента. Аналогичным образом рамки лицензионного соглашения позволяют TA производить надлежащее аннулирование всех материалов, связанных с обеспечением безопасности, в случае если пользователь отключен поставщиком услуг (при наличии технической и финансовой возможности).

Лицензионное соглашение позволяет согласованно и на постоянной основе применять прочие элементы договорной основы, такие как технические спецификации, правила соответствия и обеспечения устойчивости, обязательства и ответственность сторон, тестирование и сертификация, указания по внедрению и т. д.

На рисунке I.2 представлены компоненты лицензионного соглашения:

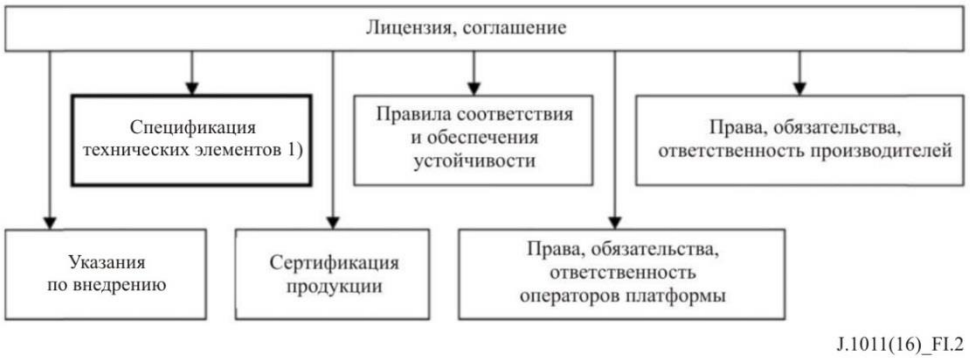

Рисунок I.2 – Компоненты лицензионного соглашения

Эти спецификации будут разрабатываться в ETSI ISG ECI как групповые спецификации.

Библиография

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

[b-CENELEC EN 50221] CENELEC EN 50221 (1997), *Common Interface Specification for Conditional Access and other Digital Video Broadcasting Decoder Applications.*

[b-CI Plus Specification] CI Plus Specification (V1.3.1) (2011), *Content Security Extensions to the Common Interface*.

[b-ETSI EN 300 468] ETSI EN 300 468 V1.13.1 (2012), *Digital Video Broadcasting (DVB); Specification for Service Information (SI) in DVB systems.*

[b-ETSI ISG ECI] ETSI ISG ECI White Paper (2014), *Industry Specification Group on Embedded Common Interface for exchangeable CA/DRM solutions*.
www.etsi.org/deliver/etsi.../ECI/.../gs_ECI00101v010101p.pdf

[b-ETSI TS 101 699] ETSI TS 101 699 V1.1.1 (1999), *Digital Video Broadcasting (DVB); Extensions to the Common Interface Specification*.
http://webstore.ansi.org/RecordDetail.aspx?sku=ETSI+TS+101+699-v1.1.1-1999-11

[b-ETSI TS 103 162] ETSI TS 103 162 V1.1.1 (2010), *Access, Terminals, Transmission and Multiplexing (ATTM); Integrated Broadband Cable and Television Networks; K-LAD Functional Specification.*

[b-ETSI TS 103 205] ETSI TS 103 205 V1.1.1 (2014), *Digital Video Broadcasting (DVB); Extensions to the CI PlusTM Specification.*

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, 2018 г.