Международный союз электросвязи

МСЭ-Т J.1015.1

(04/2020)

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; усовершенствованная система безопасности – блок лестницы ключей: аутентификация информации о правилах использования контрольных слов и связанных с ними данных 1

Рекомендация МСЭ-Т J.1015.1

ITU-T

Международный союз электросвязи

Рекомендация МСЭ-Т J.1015.1

Встроенный общий интерфейс для заменяемых решений CA/DRM; усовершенствованная система безопасности – блок лестницы ключей: аутентификация информации о правилах использования контрольных слов и связанных с ними данных 1

Резюме

Рекомендация МСЭ-Т J.1015.1 является частью серии рекомендаций, составляющих спецификацию блока лестницы ключей усовершенствованной системы безопасности встроенного общего интерфейса заменяемых решений для условного доступа и управления цифровыми правами (CA/DRM).

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т J.1015.1	23.04.2020	9-я	11.1002/1000/13837

Ключевые слова

Условный доступ, CA, управление цифровыми правами, DRM, замена.

* 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/.

СОДЕРЖАНИЕ

Введение

Целью настоящей Рекомендации[1] является содействие повышению функциональной совместимости и развитию конкуренции в сфере услуг электронной связи, в частности на рынке радиовещательных и аудиовизуальных устройств. Однако существуют и другие технологии, которые также могут оказаться подходящими и полезными в зависимости от ситуации в Государствах-Членах.

Поставщик контента шифрует свой цифровой контент и использует **систему защиты контента**[2] для его защиты от несанкционированного доступа. Для доступа к защищенному контенту потребитель использует **приемник контента**. **Приемник контента** содержит набор микросхем, выполняющий одну или несколько операций дешифрования контента. Для защиты переноса ключей дешифрования контента из **системы защиты контента** в набор микросхем используется протокол создания криптографических ключей. Шаги данного протокола, реализованные в этом наборе микросхем, называют "лестница ключей".

Лестница ключей и протокол также могут использоваться для безопасной передачи ключей шифрования контента в набор микросхем. Такие ключи необходимы в тех случаях, когда набор микросхем повторно шифрует контент. С этой целью набор микросхем может выполнять одну или несколько операций шифрования контента. Типичными примерами случаев использования повторного шифрования контента служат персональная видеозапись и экспорт защищенного контента в другую **систему защиты контента**. В настоящей Рекомендации ключи дешифрования контента и ключи шифрования контента называются **контрольными словами** (CW).

В настоящей Рекомендации также описывается механизм аутентификации. Этот механизм тесно связан с лестницей ключей и может использоваться для аутентификации объекта; иными словами, данный механизм можно использовать для аутентификации набора микросхем.

Лестница ключей и механизм аутентификации, определенные в настоящей Рекомендации, не зависят ни от **системы защиты контента**, ни от **поставщика контента**. Это позволяет **поставщику контента** применять любую совместимую **систему защиты контента**, а потребителю использовать **приемник контента** для доступа к контенту любого **поставщика контента**, применяющего такую совместимую **систему**.

Сертификатом открытого ключа каждого набора микросхем в механизмах, описанных в настоящей Рекомендации, управляет **орган по сертификации**. В частности, **орган по сертификации** распространяет такие сертификаты и информацию об отзыве сертификатов среди **поставщиков контента**, желающих использовать лестницу ключей и/или механизм аутентификации. **Поставщики контента** используют сертификаты и информацию об отзыве сертификатов в качестве входных данных для своей совместимой **системы защиты контента**; как подробно описано в разделе 7 [ITU-T J.1015], знание открытого ключа сертификата набора микросхем позволяет **системе защиты контента** создавать подходящие входные сообщения для лестницы ключей и механизма аутентификации этого набора микросхем.

---

[1] В Дополнении I определен ряд тематических областей для дальнейшей разработки.

[2] Полужирным шрифтом в тексте настоящей Рекомендации выделены термины, определения которых в контексте встроенного общего интерфейса могут отличаться от общеупотребительных.

Рекомендация МСЭ-Т J.1015.1

Встроенный общий интерфейс для заменяемых решений CA/DRM; усовершенствованная система безопасности – блок лестницы ключей: аутентификация информации о правилах использования контрольных слов и связанных с ними данных 1

1 Сфера применения

В настоящей Рекомендации описан блок лестницы ключей для реализации в наборе микросхем **приемника контента**. Блок лестницы ключей содержит лестницу ключей для безопасного переноса **контрольных слов** в набор микросхем и механизм аутентификации. В настоящей Рекомендации также рассматриваются аспекты персонализации совместимого набора микросхем.

Настоящая Рекомендация предназначена для использования производителями микросхем.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса Рекомендации.

[ITU-T J.1015] Recommendation ITU-T J.1015 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The advanced security system – Key ladder block.*

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 орган по сертификации (certification authority) – сторона, ответственная за управление сертификатами открытых ключей в **экосистеме** встроенного общего интерфейса **(ECI)**. Все остальные стороны системы доверяют органу по сертификации выполнение операций, связанных с сертификатами.

3.2.2 идентификатор набора микросхем (chipset-ID) – несекретный номер, используемый для идентификации набора микросхем в **экосистеме ECI**.

3.2.3 система защиты контента (content protection system) – система в **экосистеме ECI**, использующая криптографические методы для управления доступом к контенту и услугам. Вместо этого термина нередко может использоваться термин "система защиты услуг", с которым они являются взаимозаменяемыми. Типичными системами такого рода являются системы условного доступа (CA) или системы управления цифровыми правами (DRM).

3.2.4 поставщик контента (content provider) – сторона, передающая цифровой контент **приемнику контента** в **экосистеме ECI**.

3.2.5 приемник контента (content receiver) – устройство, используемое для доступа к цифровому контенту в **экосистеме ECI**. **Приемник контента** содержит набор микросхем с **дескремблером контента**.

3.2.6 дескремблер контента (content descrambler) – компонент в наборе микросхем **экосистемы ECI**, способный дешифровывать контент. Дескремблер контента может также поддерживать шифрование контента (для целей его повторного шифрования). В настоящей Рекомендации для шифрования и дешифрования контента используется **схема симметричного шифрования**. Шифрование и дешифрование контента MPEG-2 также называют соответственно скремблированием и дескремблированием.

3.2.7 контрольное слово (control word) – секретный ключ, используемый для шифрования и дешифрования контента в **экосистеме ECI**. В системах управления цифровыми правами контрольное слово обычно называется ключом контента.

3.2.8 криптографическая хеш-функция (cryptographic hash function) – криптографическая функция без ключа в **экосистеме ECI**, принимающая на входе данные произвольного размера (сообщение) и возвращающая на выходе блок данных фиксированного размера, который называют дайджестом сообщения. В настоящей Рекомендации предполагается, что **криптографическая хеш-функция** ведет себя как случайная функция, устойчивая к нахождению второго прообраза.

3.2.9 схема цифровой подписи (digital signature scheme) – асимметричная криптографическая схема с ключом, применяемая для обеспечения аутентичности данных в **экосистеме ECI**. **Схема цифровой подписи** состоит из алгоритма генерирования ключей, операции формирования подписи и операции проверки подписи. Ключи генерируются в виде пар, состоящих из секретного (закрытого) и открытого ключей. Данные подписывают секретным (закрытым) ключом, а соответствующий открытый ключ используют для проверки подписи. **Схема цифровой подписи**, описанная в настоящей Рекомендации, используется для проверки аутентичности сообщений, как определено в [b-ROEL]; в частности, в настоящей Рекомендации не предусмотрено использование этой схемы для обеспечения невозможности отказа от авторства или аутентификации источника.

3.2.10 экосистема ECI (ECI ecosystem) – функционирующая на коммерческой основе система, состоящая из доверительного органа, ряда платформ и **ECI**-совместимого оборудования, установленного в помещении пользователя.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

AD1	Associated Data 1	Связанные данные 1
AK	Authentication Key	Ключ аутентификации
CA	Conditional Access	Условный доступ
CW	Control Word	Контрольное слово
DRM	Digital Rights Management	Управление цифровыми правами
ECI	Embedded Common Interface	Встроенный общий интерфейс
ID	Identifier	Идентификатор
LK	Link Key	Ключ связи
SHA	Secure Hash Algorithm	Защищенный алгоритм хеширования
SIM	Signed Input Message	Подписанное входное сообщение
SPK	Sender Public Key	Открытый ключ отправителя
SSK	Sender Secret/private Key	Секретный/закрытый ключ отправителя
T	Tag	Признак
URI	Usage Rules Information	Информация о правилах использования

5 Соглашения

Полужирным шрифтом в тексте настоящей Рекомендации выделены термины, определения которых в контексте встроенного общего интерфейса могут отличаться от общеупотребительных.

6 Аутентификация информации о правилах использования контрольных слов и связанных данных 1

В разделе 7 [ITU-T J.1015] подробно описывается ряд элементов входных данных для блока лестницы ключей, в том числе CW-URI, AD1, τ_b, SPK-URI, SPK_i, шифрованный ключ связи (LK) и подписанный идентификатор набора микросхем (Chipset-ID). Некоторые из этих входных данных, например LK и идентификатор набора микросхем, шифруются и применяются вместе со схемой цифровой подписи. С другой стороны, CW-URI, AD1, τ_b, SPK-URI и SPK доставляются без применения криптографических схем. Аутентифицируются эти входные данные неявным образом: если значение какого-либо из переданных на вход элементов данных не является подлинным, то результат вычисления CW будет неверен и дескремблировать контент не удастся.

При рассмотрении характеристик входных данных может оказаться, что SPK, SPK-URI и τ_b можно передавать без применения каких-либо криптографических схем. В частности, τ_b можно проверить с помощью процедур проверки связанных данных, так что применения схемы явной аутентификации не требуется.

При необходимости поставщики услуг могут применить дополнительный метод явной аутентификации для CW-URI и AD1, подаваемых на вход блока лестницы ключей. Эта функция может предоставить дополнительные удобства для пользователей и эксплуатационные преимущества для поставщиков услуг.

В настоящей Рекомендации описывается способ применения схемы аутентификации к CW-URI и AD1, подаваемым на вход блока лестницы ключей. В частности, это можно реализовать, применив схему цифровой подписи, которая в соответствующих случаях уже используется для идентификатора набора микросхем || E(SPK, LK) с SSK. Операторы услуг могут по отдельности или коллективно аутентифицировать CW-URI или AD1.

Если операторы услуг хотят защитить CW-URI и/или AD1, им необходимо использовать схему, определенную в настоящей Рекомендации.

См. рисунок 1.

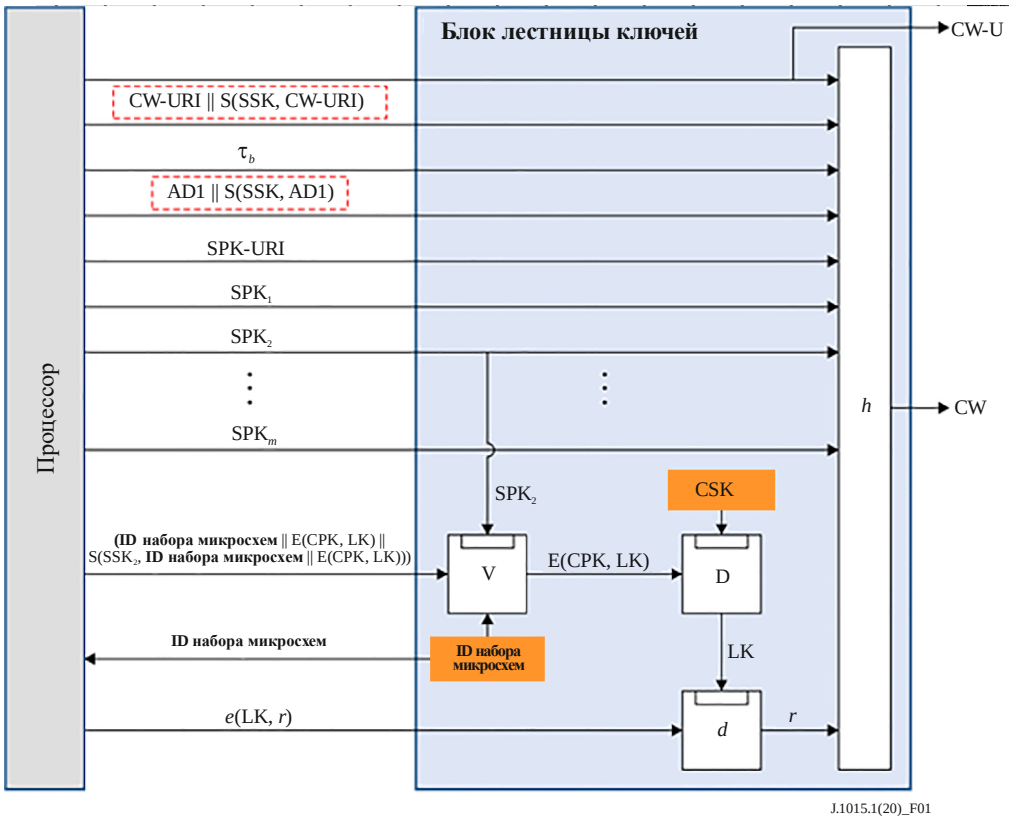

Рисунок 1 – Аутентификация информации о правилах использования контрольных слов и связанных с ними данных 1

6.1 Аутентификация информации о правилах использования контрольных слов

Вычисление CW-URI || подпись (отправитель)

1) Подписать битовую строку CW-URI, используя SSK_i; подпись обозначается как S(SSK_i, CW-URI).

2) Добавить эту подпись в конец битовой строки CW-URI.

Извлечение CW-URI (блок лестницы ключей)

1) Проверить длину входных данных. Если длина CW-URI составляет 64 бита, то блок лестницы ключей выполняет обычный процесс, определенный в пункте 7.3.1 [ITU-T J.1015], и прекращает процесс аутентификации CW-URI. В противном случае, то есть если длина превышает 64 бита, выполнить процедуру аутентификации CW-URI и перейти к следующему шагу.

2) Убедиться, что SPK-URI и правила использования, определенные в пункте 7.3.2 [ITU-T J.1015], позволяют V использовать SPK_i для проверки подписи. Если это не разрешено, блок лестницы ключей прерывает вычисления.

3) Проверить подпись, используя полученное сообщение (CW-URI || подпись) и SPK_i. Если подпись недействительна, блок лестницы ключей прерывает вычисления.

4) Извлечь CW-URI.

6.2 Проверка связанных данных 1

Вычисление AD1 || подпись (отправитель)

1) Подписать битовую строку AD1, используя SSK_i; подпись обозначается как S(SSK_i, AD1).

2) Добавить эту подпись в конец битовой строки AD1.

Извлечение связанных данных 1 (блок лестницы ключей)

1) Проверить длину входных данных. Если длина AD1 составляет 256 битов, то блок лестницы ключей выполняет обычный процесс, определенный в пункте 7.3.1 [ITU-T J.1015], и прекращает процесс аутентификации AD1. В противном случае, то есть если длина превышает 256 битов, выполнить процедуру аутентификации AD1 и перейти к следующему шагу.

2) Убедиться, что SPK-URI и правила использования, определенные в пункте 7.3.2 [ITU-T J.1015], позволяют V использовать SPK_i для проверки подписи. Если это не разрешено, блок лестницы ключей прерывает вычисления.

3) Проверить подпись, используя полученное сообщение (AD1 || подпись) и SPK_i. Если подпись недействительна, блок лестницы ключей прерывает вычисления.

4) Извлечь AD1.

Дополнение I

Тематические области, требующие доработки

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации.)

Определено, что настоящая Рекомендация нуждается в доработке и валидации, с тем чтобы обеспечить ее соответствие требованиям, установленным в [b-ITU-T J.1010], и что необходимо обновить Рекомендацию [b-ITU-T J.1010], отразив в ней требования спецификации системы расширенной защиты контента MovieLabs (ECP) [b-ECP]. Рекомендации [b-ITU-T J.1011], [b-ITU-T J.1012], [b-ITU-T J.1013], МСЭ-Т J.1014, [b-ITU-T J.1015] и [b-ITU-T J.1015.1] следует в дальнейшем обновить, отразив в них указанные изменения в [b-ITU-T J.1010].

Ряд Государств – Членов МСЭ наряду с заинтересованными сторонами со всего мира, представляющими самые разные отрасли, включая производителей устройств и электронных компонентов, владельцев и лицензиатов авторских прав на контент, поставщиков услуг over-the-top (OTT) и линейного телевидения, а также поставщиков решений для систем условного доступа (CAS) и управления цифровыми правами (DRM), выразили обеспокоенность тем, что встроенный общий интерфейс (ECI) не в полной мере отвечает требованиям ECP и требованиям к защите контента, предъявляемым в более широком круге отраслей.

Соответствующие вопросы были, в частности, подняты во вкладах к собранию 9-й Исследовательской комиссии МСЭ-Т (ИК9) (16–23 апреля 2020 года). Во вкладах, представленных Израилем, Австралией, Членом Сектора МСЭ-Т компанией Samsung, а также Ассоциированными членами ИК9 компаниями Sky Group и MovieLabs, предлагалось внести ряд изменений в Рекомендации по тематике ECI, однако согласие по ним достигнуто не было. Эти предложения перечислены в [b-SG9 Report 17 Ann.1].

Они состояли, в частности, в следующем:

1) упростить систему ECI, ограничив сферу ее применения;
2) отказаться от DRM;
3) отказаться от повторного шифрования контента;
4) отказаться от управления программным обеспечением;
5) добавить интерфейсы API для защищенного хранения и криптографических операций;
6) предусмотреть возможность использования лестниц ключей, определяемых поставщиком;
7) установить требования к TEE, изложенные в Рекомендации J.1207;
8) включить в Рекомендации реализацию TEE для виртуальной машины;
9) применять более стойкие алгоритмы шифрования, например SHA-384;
10) использовать стандартные сертификаты, подобные приведенным в Рекомендации МСЭ-Т X.509;
11) пересмотреть обмен данными между клиентами;
12) организовать дополнительное взаимодействие с ETCИ;
13) провести дополнительное коллегиальное рассмотрение;
14) рассмотреть возможные альтернативы модели доверительного органа;
15) уточнить технические аспекты правил соответствия и обеспечения устойчивости ECI;
16) добавить требования об обеспечении технического разнообразия, например о рандомизации распределения адресного пространства;
17) добавить требования о проверке целостности данных на этапе выполнения.

Эти предложения отражают постоянную эволюцию защиты контента и способов ее нарушения. Первоначальный замысел ECI возник почти за десять лет до утверждения настоящей Рекомендации

МСЭ-Т. Системы, подобные ECI, необходимо регулярно оценивать на предмет стойкости к современным методам осуществления атак, а также соответствия отраслевым требованиям к защите.

Существуют и другие механизмы обеспечения функциональной совместимости. В частности, что касается применения DRM, большинство интернет-служб доставки видео внедрили другие решения, обеспечивающие функциональную совместимость наряду с решением стоящих перед этими службами задач.

Важной задачей является внесение большей ясности, так как многие Государства-Члены рассматривают стандарты МСЭ как авторитетные источники руководящих указаний по развитию их рынков и отраслей. Упомянутый выше список предложений призван способствовать тому, чтобы можно было в полной мере уяснить все последствия, связанные с настоящей Рекомендацией МСЭ-Т, при внедрении ECI на рынках этих государств и учесть все возможные вопросы при рассмотрении законодательных и нормативных актов и потребностей рынка, требующих обеспечения функциональной совместимости потребительского цифрового телевизионного оборудования. Он также позволяет производителям оборудования, предпочитающим брать за основу при проектировании особые наборы требований или иные стандарты, учитывать эти вопросы в процессе разработки продукции, предназначенной для различных рынков.

Библиография

[b-ITU-T J.1010] Рекомендация МСЭ-Т J.1010 (2016 год), *Встроенный общий интерфейс для заменяемых решений CA/DRM; сценарии использования и требования.*

[b-ITU-T J.1011] Рекомендация МСЭ-Т J.1011 (2016 год), *Встроенный общий интерфейс для заменяемых решений CA/DRM; архитектура, определения и обзор*.

[b-ITU-T J.1012] Recommendation ITU-T J.1012 (2020), *Embedded common interface for exchangeable CA/DRM solutions; CA/DRM container, loader, interfaces, revocation*.

[b-ITU-T J.1013] Recommendation ITU-T J.1013 (2020), *Embedded common interface for exchangeable CA/DRM solutions; The virtual machine*.

[b-ITU-T J.1014] Recommendation ITU-T J.1014 (2020), *Embedded common interface for exchangeable CA/DRM solutions; Advanced security – ECI-specific functionalities*.

[b-SG9 Report 17 Ann.1] ITU-T SG9 meeting report, SG9-R17-Annex 1 (2020), Annex 1 to Report 17 of the SG9 fully virtual meeting held 16-23 April 2020. https://www.itu.int/md/T17-SG09-R-0017/en

[b-ECP] MovieLabs Specification for Enhanced Content Protection – Version 1.2 Доступно по адресу: https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.2.pdf

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, 2020 г.