ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 57450— 2017/ IEC/TS 62224: 2013

СЕРВЕРНЫЕ ДОМАШНИЕ СИСТЕМЫ МУЛЬТИМЕДИА

Концептуальная модель цифрового управления правами

(IEC/TS 62224:2013, IDT)

Издание официальное

Москва
Стандартинформ
2018

Предисловие

1 ПОДГОТОВЛЕН Автономной некоммерческой организацией «Научно-технический центр сертификации электрооборудования» «ИСЭП» (АНО «НТЦСЭ «ИСЭП») на основе собственного перевода на русский язык англоязычной версии документа, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартам ТК 452 «Безопасность аудио-, видео-, электронной аппаратуры, оборудования информационных технологий и телекоммуникационного оборудования»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 21 апреля 2017 г. № 296-ст

4 Настоящий стандарт идентичен международному документу IEC/TS 62224:2013 «Серверные домашние системы мультимедиа. Концептуальная модель цифрового управления правами» (IEC/TS 62224:2013 «Multimedia home server systems — Conceptual model for digital rights management», IDT).

Международный стандарт разработан техническим сектором 8 «Мультимедийные домашние серверные системы» Технического комитета ТК 100 «Аудио-, видео- и мультимедийные системы и оборудование» Международной электротехнической комиссии (IEC).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 ПЕРЕИЗДАНИЕ. Ноябрь 2018 г.

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Предисловие к международному документу

1) Международная электротехническая комиссия (МЭК) представляет собой международную организацию по стандартизации, объединяющую все национальные электротехнические комитеты (национальные комитеты МЭК). Задача МЭК — продвижение международного сотрудничества во всех вопросах, касающихся стандартизации в области электротехники и электроники. Результатом этой работы, в дополнение к другой деятельности МЭК, является издание международных стандартов, технических требований, технических отчетов, публично доступных технических требований (PAS) и руководств (в дальнейшем именуемых «публикации МЭК»). Их подготовка поручена техническим комитетам. Любой национальный комитет МЭК, заинтересованный в объекте рассмотрения, с которым имеет дело, может участвовать в предварительной работе. Международные, правительственные и неправительственные организации, сотрудничающие с МЭК, также принимают участие в этой подготовке. МЭК близко сотрудничает с Международной организацией по стандартизации (ИСО) в соответствии с условиями, определенными соглашением между этими двумя организациями.

2) В формальных решениях или соглашениях МЭК выражено положительное решение технических вопросов, практически консенсус на международном уровне в соответствующих областях, так как в составе каждого технического комитета есть представители национальных комитетов МЭК.

3) Публикации МЭК принимаются национальными комитетами МЭК в качестве рекомендаций. Приложены максимальные усилия для того, чтобы гарантировать правильность технического содержания публикаций МЭК, однако МЭК не может отвечать за порядок их использования или за неверное толкование конечным пользователем.

4) В целях содействия международной гармонизации национальные комитеты МЭК обязуются применять публикации МЭК в их национальных и региональных публикациях с максимальной степенью приближения к исходным. Любое расхождение между любой публикацией МЭК и соответствующей национальной или региональной публикацией должно быть четко обозначено в последней.

5) МЭК не устанавливает процедуры маркировки знаком одобрения и не берет на себя ответственность за любое оборудование, о котором заявляют, что оно соответствует публикации МЭК.

6) Все пользователи должны быть уверены, что они используют последнее издание этой публикации.

7) МЭК или ее директора, служащие или агенты, включая отдельных экспертов и членов ее технических комитетов и национальных комитетов МЭК, не несут никакой ответственности за причиненные телесные повреждения, материальный ущерб, или другое повреждение любой природы вообще, как прямое, так и косвенное, или за затраты (включая юридические сборы) и расходы, проистекающие ввиду использования публикации МЭК, или ее разделов, или другой публикации МЭК.

8) Следует обратить внимание на нормативные ссылки, указанные в настоящем стандарте. Использование ссылочных международных стандартов является обязательным для правильного применения настоящего стандарта.

9) Следует обратить внимание на то, что имеется вероятность того, что некоторые из элементов настоящего стандарта могут быть объектом патентных прав. МЭК не несет ответственности за идентификацию любых таких патентных прав.

Основной задачей технических комитетов МЭК является подготовка международных стандартов. В исключительных случаях технический комитет может предложить опубликовать техническую спецификацию:

- если, несмотря на неоднократные попытки, не может быть получена необходимая поддержка для публикации международного стандарта, или
- вопрос все еще находится на стадии технической проработки, или если по какой-то другой причине существует предполагаемая в будущем (но в данный момент отсутствующая) возможность соглашения на публикацию международного стандарта.

Техническая спецификация является предметом пересмотра в течение трех лет с даты опубликования для принятия решения относительно возможности ее трансформирования в международные стандарты.

Настоящий международный документ, который является технической спецификацией, подготовлен техническим сектором 8 «Мультимедийные домашние серверные системы» Технического комитета 100 МЭК «Аудио-, видео- и мультимедийные системы и оборудование».

Настоящее издание международного документа отменяет и заменяет первое издание, опубликованное в 2007 году, и является его техническим пересмотром.

Настоящее издание международного документа содержит следующие существенные технические изменения относительно предыдущего издания:

a) введен метод Диффи — Хеллмана (Diffie — Hellman), касающийся модели протокола безопасного лицензионного соглашения (SLTP);

b) исключена модель формата защищенного контента (PCF), зависящая от каждой службы/услуги;

c) добавлено описание, относящееся к МЭК 62227;

d) введена классификация сертификационных органов.

Текст настоящего международного документа основан на следующих документах:

Проект спецификации	Отчет о голосовании
100/2005/DTS	100/2060/RVC

Полную информацию о голосовании по одобрению настоящего международного документа можно найти в отчете о голосовании, указанном в приведенной выше таблице.

Настоящая публикация разработана в соответствии с Директивами ИСО/МЭК, часть 2.

Комитет принял решение, что содержание настоящей публикации останется неизменным до конечной даты сохранения, указанной на сайте МЭК с адресом http://webstore.iec.ch, в данных, касающихся конкретной публикации. К этой дате публикация будет:

- переведена в статус международного стандарта;
- подтверждена заново;
- аннулирована;
- заменена пересмотренным изданием или
- изменена.

Введение

Благодаря современным тенденциям возрастающей популярности мобильных телефонов и Интернета, а также реализации передачи данных с высокой скоростью и носителей записей (регистрирующих сред) данных большого объема развиваются службы распределения высококачественного контента и повсеместной доставки информации и на рынке постепенно появляются службы доставки информации и совместного использования сети нового типа. Также существует возможность использования домашних серверов терабайтового уровня в частных домах.

При распространении контента по совместно используемым сетям становится критичным введение технологий цифрового управления правами (DRM) с целью защиты контента от несанкционированного копирования и использования. Эти вопросы имеют большую социальную значимость.

Целью управления посредством DRM-технологии является введение цифрового лицензирования, например авторского права. По существу такие лицензии должны быть не только защищены, но и при этом способствовать новому творчеству/рекреативности и широко использоваться в качестве собственности, совместно используемой по всему земному шару. Таким образом, лицензиями с такими характеристиками следует управлять и защищать с помощью системы DRM, которая отвечает открытым интероперабельным (функционально совместимым) спецификациям, используемым по всему миру.

Открытая интероперабельная спецификация, соответствующая настоящему стандарту, может формировать широко распространенную инфраструктуру открытых ключей (PKI), основанную на DRM, нацеленную на использование между системами, с учетом расширения услуг распределения современного контента и клиентов (аудио-/видеооборудование консольного/пультового типа, ПК, терминал мобильных телефонов, автомобильный телематический терминал и т. д.). Настоящий стандарт представляет собой протокол спецификаций для обмена лицензионной (лицензируемой) информацией между модулями DRM, описание спецификаций для лицензионной (лицензируемой) информации и формат зашифрованного контента.

При разработке данной модели большое внимание уделено использованию контентов в электронном оборудовании пользователя, подключаемом к домашним серверам. Помимо этого, особое внимание направлено на распространение, хранение, обмен и использование контента между дистрибутивными серверами и оконечной системой клиента/клиентской системой назначения, учитывая при этом условия, одобренные держателем прав, но без нарушения удобства для пользователей. Стандартизация и ее популяризация, основанная на данной модели, позволят осуществлять взаимодействие между модулями DRM, гарантирующее строгую защиту контентов в разных системах с общим использованием сети контентов или в службах распространения контента по Интернету и сетям мобильных телефонов.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

СЕРВЕРНЫЕ ДОМАШНИЕ СИСТЕМЫ МУЛЬТИМЕДИА

Концептуальная модель цифрового управления правами

Multimedia home server systems.
Conceptual model for digital rights management

Дата введения — 2018—03—01

1 Область применения

Настоящий стандарт устанавливает концептуальную модель протокола спецификации для обмена лицензионной информацией между модулями цифрового управления правами (DRM). В настоящем стандарте рассмотрены модели, которые следует определять как стандартные, а также приведены стандартные смысловые значения (в основном с точки зрения информационной безопасности в среде распространения, включая системы домашних серверов).

2 Нормативные ссылки

Для применения настоящего стандарта необходимы следующие ссылочные документы. Для датированных ссылок применяют только указанное издание ссылочного документа, для недатированных ссылок применяют последнее издание ссылочного документа (включая любые изменения).

IEC 62224:2008 Multimedia home server systems — Digital rights permission code Amendment 1:2012 (Мультимедийные системы домашних серверов. Код доступа к цифровым правам. Изменение 1:2012)

ISO/IEC 7498-1:1994 Information technology — Open systems interconnection — Basic reference model: The basic model (Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель)

ISO/IEC 9594-8:2008 Information technology — Open systems interconnection — The Directory: Public-key and attribute certification framework (Информационная технология. Взаимодействие открытых систем. Руководство: схема сертификации по свойствам/атрибутам и с инфраструктурой открытых ключей)

ISO/IEC 15408-1:2009 Information technology — Evaluation criteria for IT security — Part 1: Introduction and general model (Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель)

ITU-T Recommendation X.509:1997 Information technology — Information technology — Open systems interconnection — The Directory: Public-key and attribute certification framework (Информационная технология. Взаимодействие открытых систем. Руководство. Схема сертификации по свойствам/атрибутам и с инфраструктурой открытых ключей)

RFC 3280 R. Housley (RSA Laboratories), W. Ford (VesiSign), W. Polk (NIST), D. Solo (Citicorp) Request for comments: 3280 — Internet X.509 Public-key Infrastructure certificate and certificate revocation list (CRL) profile, Category: Standards track» (April 2002), http://rfc.slim.summitmedia.co.uk/rfc2380.html [Запрос на отзывы: 3280. Сертификат инфраструктуры открытых ключей Интернет X.509 и профиль списка аннулированных (отозванных) сертификатов (CRL). Категория: Трек стандартов (апрель 2002), http://rfc.slim.summitmedia.co.uk/rfc2380.html]

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 9594-8:2008, а также следующие термины с соответствующими определениями:

3.1 **условие доступа** (access condition): Информация, представляющая условия использования контента.

Примечание 1 — Условие доступа представляет условные правила, ограничивающие возможность манипулирования информацией контента у пользователя, и является частью информации об авторизации/разрешении в лицензии для контента.

3.2 **политика работы с сертификатом** (certificate policy): Именованный набор правил, указывающих на применимость сертификата для конкретного сообщества и/или класса приложения с общими требованиями по безопасности/защите.

Пример — Конкретная политика работы с сертификатом может означать применимость типа сертификата к аутентификации/проверке подлинности транзакций обмена электронными данными при торговле товарами в пределах заданного ценового диапазона.

[ИСО/МЭК 9594-8:2008, 3.4.10, модифицированное определение, т. е. соотнесенное с новыми требованиями к терминам и определениям]

3.3 **сертификационный орган; CA** (certification authority, CA): Орган, которому доверено с привлечением одним или несколькими пользователями создавать и передавать сертификаты инфраструктуры открытых ключей.

Примечание 1 — Сертификационный орган может по выбору создавать/устанавливать ключи пользователей.

3.4 **список аннулированных (отозванных) сертификатов; список отозванных сертификационных органов; CARL** (certificate revocation list; certificate authority, revocation list, CARL): Список отзывов, содержащий перечень сертификатов инфраструктуры открытых ключей, выпущенных для сертификационных органов, которые «издатель» сертификата перестал считать действенными.

[ИСО/МЭК 9594-8:2008, 3.4.18]

3.5 **идентификатор контента** (content identifier): Идентификатор, представляющий собой уникальное значение, назначаемое каждому контенту, который является единицей информации, доставляемой держателем контента.

3.6 **ключ к контенту** (content key): Ключ шифрования контента, уникальный для каждого контента.

Примечание 1 — Ключ к контенту — это ключ в системе шифрования с использованием симметричного криптографического ключа.

3.7 **конкатенация (сцепление) данных** (data concatenation): Соединение двух битовых потоков в один битовый поток.

Примечание 1 — Первый бит 2-го исходного потока соседствует с последним битом 1-го исходного потока.

3.8 **TREM**[1)] **декодера** (decoder TREM): TREM, в котором зашифрованный контент может быть дешифрован и воспроизведен.

3.9 **TREM назначения** (destination TREM): TREM, получающий лицензию.

3.10 **управление правами на цифровой продукт** (digital rights management): Технология, или функции по защите прав, касающихся цифрового контента (например, копирования), или система, или модуль, обеспечивающие эти функции.

Примечание 1 — В рамках такой системы или модуля происходит управление условиями доступа к контенту и функционирование при этих условиях.

3.11 **зашифрованный контент** (encrypted content): Зашифрованные данные контента с относящимися к ним метаданными, например контентом вещания, контентом загрузки, контентом формирования потока и т. п.

3.12 **входной TREM** (entry TREM): TREM с функцией генерации новой лицензии в соответствии с указанием/индикацией извне и работой в качестве исходного TREM.

Примечание 1 — Входной TREM находится на сервере распределения лицензий и т. п.

[1)] См. определение 3.33.

3.13 **хэш-функция** (hash function): Математическая функция, отображающая значения из большой (вероятно, очень большой) области в более маленькой зоне.

Примечание 1 — «Хорошая» хэш-функция — это функция, при которой результат применения функции к (большому) ряду значений в данной области будет равномерно (и, очевидно, случайным образом) распределен по зоне.

[ИСО/МЭК 9594-8:2008, 3.4.35, модифицированное определение, т. е. соотнесенное с новыми требованиями к терминам и определениям]

3.14 **лицензия** (license): Информация, включающая один ключ к контенту или более, и информация об авторизации, подобная условиям доступа и т. п.

Примечание 1 — Если она находится вне TREM, она должна быть защищенной лицензией, которая защищена ключом сеанса связи (сеансовым ключом), генерируемым в соответствии с протоколом безопасного лицензионного соглашения (SLTP).

3.15 **идентификатор лицензии** (license identifier): Идентификатор, являющийся уникальным значением, присваиваемым каждой лицензии.

3.16 **передача лицензии** (license move): Передача лицензии от одного TREM другому.

Примечание 1 — Если происходит передача лицензии, она удаляется из исходного TREM. Передача лицензии с зашифрованным контентом приравнивается к передаче контента.

3.17 **модуль переключения (коммутации) лицензии;** LRM (license relay module, LRM): Система или модуль, переключающие защищенную лицензию между TREM посредством сеанса протокола безопасного лицензионного соглашения (SLTP).

Примечание 1 — LRM является конечной точкой соединения протокола переключения лицензии (LRP) и имеет функцию управления внутренней шиной и сетью/схемой для переключения защищенной лицензии через соединение LRP.

3.18 **протокол переключения (коммутации) лицензии**; LRP (license relay protocol, LRP): Протокол между LRM.

Примечание 1 — По этому протоколу реализован протокол безопасного лицензионного соглашения (SLTP) для интернетной среды. Для SLTP протокол LRP обеспечивает функции управления транзакциями, рестарта отключенного сеанса SLTP, согласования протокола и передачи информации, касающейся авторизации/наделения разрешением пользователя или управления учетом сетевых ресурсов.

3.19 **сервер системы лицензирования** (license server): Серверная система, имеющая TREM и LRM, которая способствует передаче (трансляции) лицензии, выпущенной TREM.

3.20 **транзакция лицензии** (license transaction): Элемент (единица) обработки данных для распределения, передачи или копирования лицензии.

3.21 **трансфер лицензии** (license transfer): Передача или копирование лицензии из одного TREM в другой TREM.

3.22 **промежуточный TREM** (mediator TREM): TREM, основная роль которого служить промежуточным звеном при трансфере лицензии.

Примечание 1 — Он выполняет две роли: TREM назначения и исходный TREM.

3.23 **защищенная лицензия** (protected license): Информация о лицензионных операциях, защищенная при трансфере между TREM.

Примечание 1 — Защищенная лицензия включает ключи к зашифрованному контенту и защищенную информацию об авторизации.

3.24 **криптографическая система с открытым ключом** (public key cryptosystem): Криптографическая система, в которой ключ шифрования отличается от ключа расшифровки.

Примечание 1 — При маскировке/скрытии данных ключ, используемый для шифрования, находится в открытом доступе. Хорошо известны такие криптографические системы с открытым ключом, как RSA (алгоритм Ривеста — Шамира — Адлемана/алгоритм асимметричного шифрования с использованием перемножения двух случайно выбранных простых чисел) и криптографическая система с эллиптической кривой.

3.25 **протокол безопасного лицензионного соглашения**; SLTP (secure license transaction protocol, SLTP): Протокол безопасного трансфера информации о лицензионных операциях между TREM.

Примечание 1 — Настоящий протокол включает форматы информации, обмениваемой между TREM, и спецификацию смены состояний TREM, которые необходимо реализовать.

3.26 **личный (скрытый) сеансовый ключ** (session private key): Временный личный (скрытый) ключ, применяемый при совместном использовании симметричного сеансового ключа между TREM в каждом сеансе SLTP.

3.27 **открытый сеансовый ключ** (session public key): Временный открытый ключ, применяемый при совместном использовании симметричного сеансового ключа между TREM в каждом сеансе SLTP.

3.28 **симметричный сеансовый ключ** (session symmetric key): Временный симметричный ключ, совместно используемый между TREM в каждом сеансе SLTP.

3.29 **сеанс SLTP** (SLTP session): Безопасный сеанс, создаваемый между TREM в соответствии с SLTP для трансфера лицензии.

Примечание 1 — В каждом сеансе SLTP есть симметричный сеансовый ключ, используемый совместно обеими сторонами TREM.

3.30 **исходный TREM** (source TREM): TREM в качестве TREM, выпускающего лицензию.

3.31 **система шифрования с использованием симметричного криптографического ключа** (symmetric key criptosystem): Система шифрования, в которой для шифрования и дешифровки данных используют один и тот же ключ.

Примечание 1 — Хорошо известной криптографической системой с криптографическим ключом является улучшенный стандарт шифрования (AES), принятый NIST в США.

3.32 **модуль, устойчивый к вмешательству**; TRM (tamper resistant module, TRM): Модуль для защиты от исследования или модификации информации и ее обработки.

Примечание 1 — См. [FIPS (Федеральный стандарт обработки информации, США), 140-2].

3.33 **устойчивый к вмешательству модуль принудительного применения права**; TREM (tamper resistant rights enforcement module, TREM): Система или модуль, имеющие функции управления правами на цифровой продукт.

Примечание 1 — TREM построен как модуль, устойчивый к вмешательству. TREM имеет функции принудительного осуществления прав, управления лицензией и процессом трансфера лицензии в соответствии с SLTP.

3.34 **идентификатор транзакции** (transaction identifier): Идентификатор, назначаемый для каждой транзакции лицензии.

3.35 **журнал транзакций** (transaction log): Регистрируемые данные, представляющие статус транзакции трансфера лицензии и лицензии, выпускаемой в данной транзакции.

Примечание 1 — Он безопасно хранится в TREM.

3.36 **личный (скрытый) ключ TREM; отдельный личный (скрытый) ключ TREM** (TREM private key; TREM individual private key): Ключ, тайно хранимый каждым TREM отдельно.

3.37 **открытый ключ TREM; отдельный открытый ключ TREM** (TREM public key; TREM individual public key): Открытый ключ, соответствующий личному/скрытому (отдельному) ключу TREM.

4 Сокращения

В настоящем стандарте использованы следующие сокращения:

AES — улучшенный стандарт шифрования, стандарт AES;

CA — сертификационный орган;

CCI — информация о возможности копирования;

CRL — список аннулированных (отозванных) сертификатов;

DES — стандарт шифрования данных;

DRM — управление цифровыми правами/правами на цифровой продукт;

EC-DH — план соглашения о ключах в криптографической системе с эллиптической кривой, метод Диффи — Хеллмана (Diffie — Hellman);

EC-DSA — упрощенная проверка методом эллиптической кривой, версия DSA (алгоритм цифровой подписи);

ID — идентификатор;

LRM — модуль переключения/коммутации лицензии;

LRP — протокол переключения/коммутации лицензии;

PCF — формат защищенного контента;

SLTP — протокол безопасного лицензионного соглашения;

T-DES — шифр стандарта DES с трехкратным шифрованием;

TID — идентификатор транзакции;

TREM — устойчивый к вмешательству модуль принудительного применения права;

TRM — модуль, устойчивый к вмешательству.

5 Условные обозначения

5.1 Цифровые значения (величины)

В настоящем стандарте использованы выражения цифровых значений, приведенных в таблице 1.

Таблица 1 — Представление цифровых значений

Система счисления	Символы, используемые для обозначения значения	Приложенный символ	Пример
Двоичная система счисления (BIN)	«0» ~ «1»	Отсутствует	11001000 (или 11001000b)
Десятичная система счисления (DEC)	«0» ~ «9»	Отсутствует (или «b»)	200
Шестнадцатеричная система счисления (HEX)	«0» ~ «9», «A» ~ «F»	«h»	C8h

5.2 Перечень условных обозначений

В настоящем стандарте использованы условные обозначения, приведенные в таблице 2.

Таблица 2 — Условные обозначения, используемые в модели, рассматриваемой в настоящем стандарте

Наименование	Обозначение	Описание
Шифрование	E (K, D)	Результат шифрования информации «D» с ключом «K»
Хэш	H (D)	Результат хэша информации «D»
Сцепление	A || B	Результат сцепления данных «A» и «B»
Ключ контента	Kc	Ключ шифрования контента, относящийся к каждому контенту
Корневой скрытый ключ	KR	Скрытый ключ, скрытно поддерживаемый корневым сертификационным органом (CA)
Корневой открытый ключ	KPR	Открытый ключ, соответствующий KR
Скрытый ключ CA	KCi	Скрытый ключ, скрытно поддерживаемый сертификационным органом «i», который является издателем сертификата органа более низкого уровня или сертификата системы открытого ключа TREM. (Сюда не входит корневой скрытый ключ)
Открытый ключ CA	KPCi	Открытый ключ, соответствующий KCi. (Сюда не входит корневой открытый ключ)
Скрытый ключ TREM для обнаружения вмешательства в сообщение SLTP	KTdk	Ключ, который TREM «k» хранит отдельно и скрытно. Этот ключ используют для генерации цифровой подписи при обнаружении вмешательства в сообщение SLTP
Открытый ключ TREM для обнаружения вмешательства в сообщения SLTP	KPTdk	Открытый ключ, соответствующий KTdk. Данный ключ используют для проверки цифровой подписи, которая генерируется за счет использования KTdk
Скрытый ключ TREM для совместного использования симметричного сеансового ключа с другим TREM	KTsk	Ключ, который TREM «k» хранит отдельно и скрытно. Данный ключ используют для совместного использования симметричного сеансового ключа с другим TREM

Окончание таблицы 2

Наименование	Обозначение	Описание
Открытый ключ TREM для совместного использования симметричного сеансового ключа с другим TREM	KPTsk	Открытый ключ, соответствующий KTsk. Данный ключ используют для совместного использования симметричного сеансового ключа с другим TREM
Соответствующая информация	Ir	Информация, относящаяся к корневому CA
	Ici	Информация, относящаяся к «i» CA, не являющемуся корневым CA
	Itxx	Информация, относящаяся к открытому ключу TREM KPTxx
Сертификат	C (KR, KPR || Ir)	Сертификат корневого открытого ключа KPR KPR || Ir || E (KR,H (KPR || Ir))
	C (KR, KPCi || Ici)	Сертификат открытого ключа KPCi, издаваемый корневым CA, скрытый ключ которого KR KPCi || Ici || E(KR, H(KPCi || Ici))
	C (KCi, KPCj || Icj)	Сертификат открытого ключа KPCj, издаваемый «i» CA, скрытый ключ которого KCi KPCj || Icj || E(KCi, H(KPCj || Icj))
	C (KCj, KPTxx || Itxx)	Сертификат открытого ключа KPTxx, издаваемый «j» CA, скрытый ключ которого KCj KPTxx || Itxx || E(KCj, H(KPTxx || Itxx))
Сеансовый скрытый ключ	KTTkn	Временный скрытый ключ, генерируемый в «k» TREM в каждый сеанс «n» SLTP. Используют для совместного использования сеансового симметричного ключа между TREM в сеансе «n» SLTP
Сеансовый открытый ключ	KPTTkn	Временный открытый ключ, соответствующий KTTkn. Используют для совместного применения сеансового симметричного ключа между TREM в сеансе «n» SLTP
Сеансовый симметричный ключ, совместно используемый между TREM	KSk1k2n	Временный симметричный ключ, который совместно используют между TREM «k1» и TREM «k2» в сеансе «n» SLTP посредством применения шифросистемы с открытым ключом
Список отметок времени обновления CRL	CRLUpdates	Дата и время обновления CRL
Идентификатор контента	CID	Значение уникального идентификатора, назначаемого каждому контенту
Метод Диффи — Хеллмана (Diffie — Hellman)	DH (KPTTk1n,KPTTk2n, epx) = DH (KPTTk2n,KPTTk1n, exp)	Сеансовый симметричный ключ, который совместно используют TREM «k1» и TREM «k2» в сеансе «n» SLTP при применении метода Диффи — Хеллмана epx: параметр шифрования «x» шифросистемы с открытым ключом

6 Требования

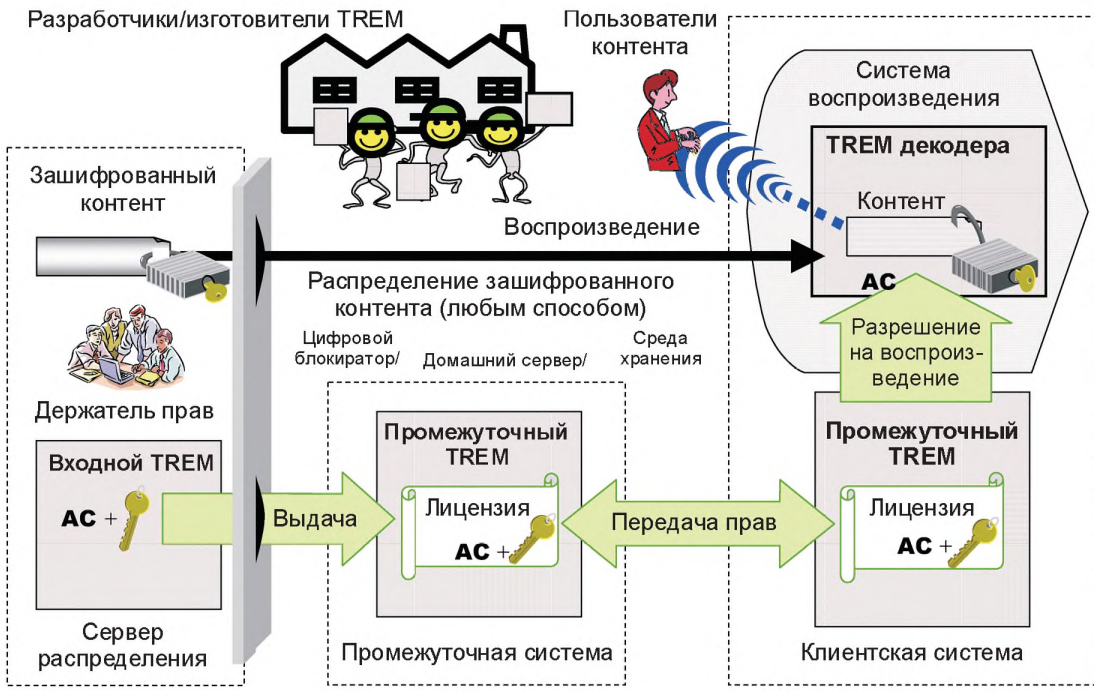
6.1 Модель лицензионного обслуживания

6.1.1 Общие положения

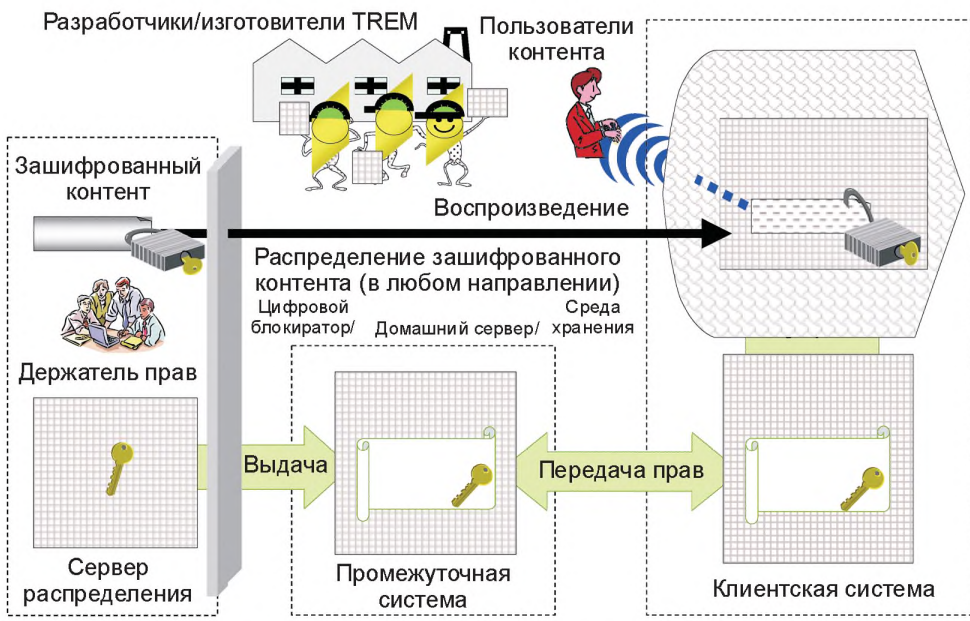
К модели лицензионного обслуживания установлены следующие функциональные требования, представленные на рисунке 1:

a) контент шифруют и распространяют любым способом;

b) информация о лицензионных операциях включает ключи к контенту и условия доступа (AC);



AC: Условие доступа (условие использования) ※ Количество промежуточных TREM может быть 0 или более



AC: Условие доступа (условие использования) ※ Количество промежуточных TREM может быть 0 или более

Рисунок 1 — Модель лицензионного обслуживания для рассмотрения угроз

c) единожды созданный держателем прав зашифрованный контент и защищенную лицензию дешифруют только в TREM (устойчивом к вмешательству модуле принудительного применения права);

d) информацию о лицензионных операциях защищают путем шифрования вне TREM, и ее следует передавать среди них в соответствии с условиями доступа;

e) TREM, издающий и передающий лицензию, называют исходным TREM, а TREM, получающий и передающий лицензию, — TREM назначения;

f) TREM обрабатывает запрос пользователя в соответствии с условиями доступа, указанными в лицензии;

g) входной TREM (см. 3.12), находящийся в таком сервере, как сервер «управления/распределения контента», может принимать данные простого контента и информацию о простой лицензии и создавать зашифрованный контент и информацию о защищенной лицензии, действуя в качестве исходного TREM;

h) промежуточный TREM (см. 3.22) в системе промежуточной работы с контентом/лицензией действует и как исходный TREM, и как TREM назначения;

i) TREM декодера (см. 3.8), например в системе воспроизведения, может получать лицензию от другого TREM и производить дешифровку зашифрованных контентов в соответствии с условиями доступа, включенными в лицензию.

6.1.2 Угрозы и контрмеры

6.1.2.1 Общие положения

В таблице 3 приведены угрозы, существующие в среде лицензионного обслуживания, которые представлены в 6.1, и меры, применяемые в отношении каждой угрозы.

Таблица 3 — Угрозы и контрмеры в модели лицензионного обслуживания

<table>
<tr><th>Субъект</th><th colspan="2">Угроза (попытка нарушения защиты)</th><th colspan="2">Контрмеры</th></tr>
<tr><td rowspan="4">Пользователь TREM и пользователь сети</td><td colspan="2">Разбор-анализ TREM</td><td colspan="2">a) Изготовление TREM как TRM</td></tr>
<tr><td rowspan="2">Комуфляж (дезориентация)</td><td>Комуфляж TREM назначения. Атака методом записи и повторной передачи блоков шифрованного текста (комуфляж исходного TREM)</td><td colspan="2">b) Шифрование с сеансовым ключом, используемым совместно, после взаимного признания подлинности по сертификатам TREM назначения и исходного TREM</td></tr>
<tr><td>Комуфляж отключения сеанса транзакции лицензии</td><td colspan="2">c) Сравнение регистраций в каждом TREM</td></tr>
<tr><td colspan="2">Утечка скрытного ключа для CA или TREM</td><td rowspan="3">d) Выдача CRL</td><td>Обновление ключа</td></tr>
<tr><td rowspan="2">Изготовитель TREM</td><td colspan="2">Незаконное изготовление</td><td rowspan="2">Прекращение действия взломанного или незаконного TREM</td></tr>
<tr><td colspan="2">Утечка информации о ключе</td></tr>
</table>

6.1.2.2 Изготовление TREM в качестве TRM

Для того чтобы уберечь пользователя контента от взлома TREM и похищения из него секретных ключей, TREM должен быть TRM (модулем, устойчивым к вмешательству).

6.1.2.3 Шифрование с сеансовым ключом

В услуге распространения лицензий персонация (выдача себя за другое лицо) TREM, например атака методом записи и повторной передачи блоков шифрованного текста путем дезориентации TREM отправителя лицензии, вызывает незаконное неограниченное копирование контента. Поэтому, чтобы уберечь кого-либо от разработки модуля, персонирующего исходный TREM (отправитель) или TREM назначения (получатель), платная лицензия должна быть зашифрована с сеансовым ключом, используемым совместно после взаимной аутентификации TREM назначения и исходного TREM с помощью открытых ключей TREM при определении вмешательства в сообщение SLTP.

6.1.2.4 Сравнение регистраций

Необходимо, чтобы журналы транзакций лицензий хранились безопасно в TREM. Когда сеанс по трансферу/передаче лицензии отключается и для отсылки лицензии необходимо вновь восстановить сеанс, журнал TREM назначения должен скрытно быть передан в исходный TREM для сравнения журналов исходного TREM и TREM назначения с целью подтверждения, была ли получена лицензия TREM назначения или нет. В ином случае кто-либо может закомуфлировать несанкционированную копию лицензии с восстановлением сеанса.

Существует много возможностей неожиданных прерываний, которые могут происходить в процессе покупки лицензий через сети связи. Это часто происходит в мобильных беспроводных сетях. Если

никаких мер против этого типа вмешательства не существует, дистрибьютор может только повторно выслать лицензии ложному TREM, закомуфлированному под законно отключенный TREM. Так как может происходить не только отключение/прерывание, но может быть так, что нет очевидности получения лицензии, исходный TREM должен, конечно, предоставить лицензию в место назначения в обмен на предоставление отчета/учета ресурсов или уменьшение прав.

6.1.2.5 Выдача CRL

Для прекращения использования незаконных или взломанных ключей и TREM можно использовать CRL (список отозванных/аннулированных сертификатов, указанный в Рекомендации X.509 МСЭ и в ИСО/МЭК 9594-8). Описание CRL приведено в документе RFC 3280.

6.1.3 Критерии оценки

Для реализации защитной среды безопасного контента необходимо определить критерии оценки безопасности для TREM. Критерии безопасности для защиты контента должны соответствовать ИСО/МЭК 15408-1 и включать следующее:

- функции безопасности для защиты контента, указанные в 6.1.2;
- указатели, информирующие о реализации должным образом необходимых алгоритмов криптографической системы/шифросистемы, хэш-функции и функции генерации случайных чисел;
- указатели, относящиеся к устойчивости TRM для TREM, например уровня безопасности TRM в соответствии с документом FIPS 140-2;
- описание процесса проектирования, разработки и изготовления TREM.

7 Вопросы проектирования

7.1 Общие положения

В настоящем разделе приведены следующие концептуальные модели, отвечающие требованиям, указанным в разделе 6:

a) модель безопасности;

b) модель взаимодействия;

c) модель информации о лицензионных операциях.

7.2 Модель безопасности

7.2.1 Общие положения

В настоящем подразделе приведена модель безопасности, отвечающая требованиям, указанным в 6.1.2.

7.2.2 Рассмотрение модели безопасности

В модели безопасности (см. рисунок 2) данной концептуальной модели подлежащий защите контент шифруют и распространяют любым способом. В данной модели ключ шифрования контента и информация о правах, включая условия доступа (AC) к контенту, также защищены посредством использования TRM и криптографической системы и имеют следующий жизненный цикл в качестве лицензии:

a) лицензия создается во входном TREM;

b) лицензия является первоначально изданной в качестве защищенной лицензии из входного TREM;

c) лицензия передается в TREM декодера через промежуточные TREM, количество которых больше 0;

d) лицензия используется для дешифровки контента в соответствии с условиями доступа (AC) в TREM декодера.

7.2.3 Функции TREM

TREM должен иметь следующие функции:

a) функцию устойчивости к вмешательству, предотвращающую утечку информации о лицензионных операциях, в качестве TRM;

b) функцию создания и поддержания сеанса SLTP;

c) функцию передачи лицензии между TREM всегда при использовании сеанса SLTP;

d) в случае промежуточного TREM — функцию дешифровки лицензии и трансфера/передачи ее другому TREM в соответствии с условиями доступа к защищенному промежуточному TREM;

e) в случае TREM декодера — функцию дешифровки лицензии и дешифровки контента с дешифровальным ключом, соответствующим условию доступа к защищенному декодеру.

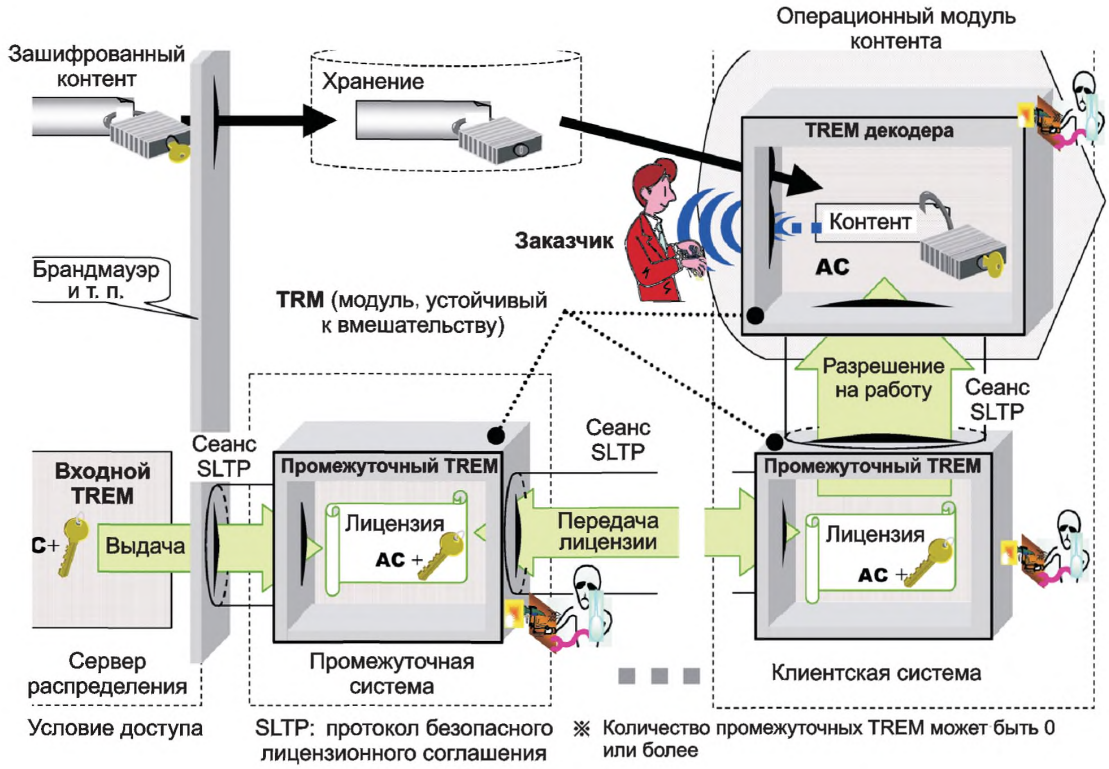


Рисунок 2 — Модель безопасности при защите контента

7.2.4 Модель протокола безопасного лицензионного соглашения SLTP

В настоящем пункте приведена модель SLTP, отвечающая требованиям, указанным в разделе 6, в качестве примера наиболее простого протокола безопасного лицензионного соглашения между TREM. Также в качестве контрмер, особенно указанных в 6.1.2.3 и 6.1.2.4, необходимы стандартизация и реализация SLTP.

SLTP является протоколом скрытной передачи информации о лицензионных операциях между TREM. Этот протокол включает форматы информации, которой обмениваются TREM между собой, и спецификацию смены состояний в рамках TREM.

В основной стандартной последовательности модели SLTP происходят обмен следующими сообщениями в соответствии с определенными шагами (см. рисунок 3) для генерации сеанса SLTP в качестве контрмер, приведенных в 6.1.2.3, и скрытная передача секретных данных в сеансе SLTP:

а) генерация сеанса SLTP:

- подготовка к обнаружению вмешательства в сообщение SLTP.

Для обнаружения вмешательства в сообщение SLTP из TREM-отправителя сообщения в TREM-получатель сообщения высылается сертификат открытого ключа TREM, и происходит его проверка на TREM-получателе.

Например, из TREM-отправителя в TREM-получатель высылаются сообщения: C(KR,KPCi || Ici), C(KCi,KPCj || Icj) и C(KCj,KPTdk || Itdk), где C(KR,KPCi || Ici),C(KCi,KPCj || Icj) — сертификаты, создающие PkiPath, а C(KCj,KPTdk || Itdk) — сертификат TREM-отправителя (TREM-отправитель — «k» TREM).

Тогда между TREM-отправителем и TREM-получателем генерируется среда для обнаружения вмешательства в сообщение за счет использования цифровой подписи;

- совместное использование сеансового симметричного ключа. Исходный TREM и TREM назначения совместно используют сеансовый симметричный ключ. Существует несколько методов совместного использования. Ниже приведены их основные примеры:

1) за счет использования скрытого ключа TREM и открытого ключа при совместном использовании временного ключа.

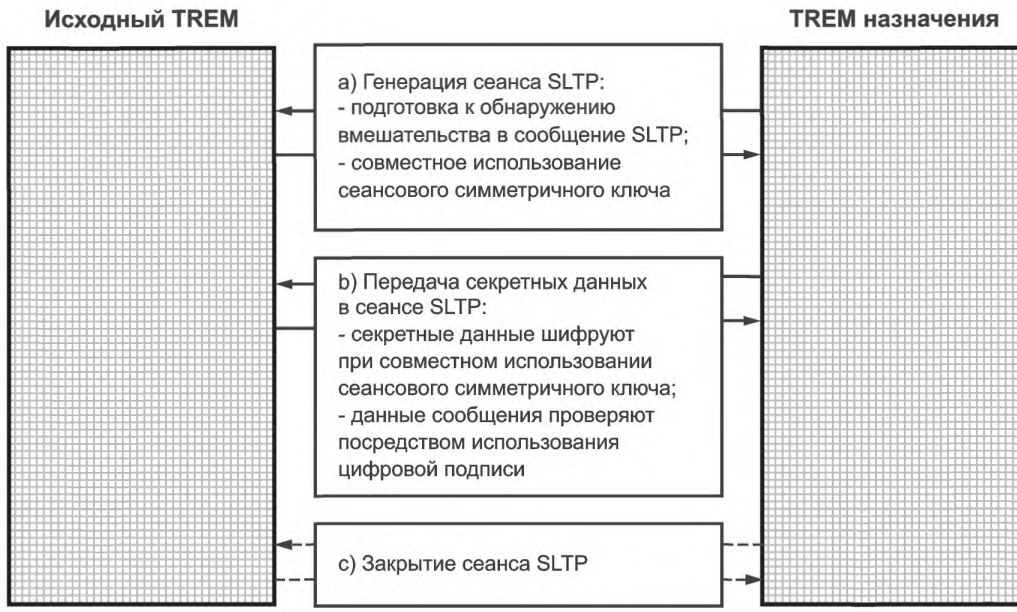


Рисунок 3 — Основная процедура модели SLTP

Сначала исходный TREM получает сертификаты C(KR,KPCi || Ici),C(KCi,KPCj || Icj) и C(KCj,KPTsk1 || Itsk1) от TREM назначения «k1» и проверяет эти сертификаты. Затем исходный TREM «k2» формирует сеансовый симметричный ключ KSk1k2n и шифрует его с KPTsk1. В итоге исходный TREM посылает зашифрованный сеансовый симметричный ключ в TREM назначения;

2) за счет использования сеансового скрытого ключа и сеансового открытого ключа.

TREM назначения «k1» формирует сеансовый открытый ключ «KPTTk1n» и сеансовый скрытый ключ «KTTk1n», и аналогичным образом исходный TREM «k2» формирует сеансовый открытый ключ «KPTTk2n» и сеансовый скрытый ключ «KTTk2n». Затем оба эти TREM получают общий сеансовый симметричный ключ «KSk1k2n» путем обмена сеансовыми открытыми ключами каждого из них при использовании метода Диффи — Хеллмана (Diffie — Hellman).

Исходный TREM «k2»: DH(KPTTk1n, KTTk2n, epx)

↓

KSk1k2n

↑

TREM назначения «k1»: DH(KPTTk2n, KTTk1n , epx);

b) передача/трансфер секретных данных в сеансе SLTP:

- секретные данные шифруют при совместном использовании сеансового симметричного ключа:

- секретные данные шифруют при совместном использовании сеансового симметричного ключа в TREM-отправителе, а из него эти зашифрованные секретные данные посылают в TREM-получатель.

E(KSk1k2n, SD)

SD: Секретные данные

- данные сообщения проверяют посредством использования цифровой подписи:

- данные сообщения добавляют/присоединяют к цифровым подписям TREM-отправителя, а TREM-получатель проверяет их

MD || E(KTdk1, H(MD))

KTdk1: Скрытый ключ TREM для обнаружения вмешательства в сообщение SLTP TREM «k1»

MD: Данные сообщения;

c) закрытие сеанса SLTP.

Произведенный сеанс SLTP закрывают в явном или неявном виде [например, закрывают блокировкой по превышению лимита времени («time out») или при новом запросе от того же TREM].

Для использования случайного числа в качестве сеансового ключа это случайное число следует формировать достаточно секретно. Секретные случайные числа должны быть особыми/разными по способу генерации и по значениям, а также трудно определимыми для хакеров за приемлемый период времени.

Если принимаемая информация не может быть должным образом интерпретирована в TREM, TREM немедленно ее отклоняет, чтобы не допустить любые возможные взломы, использующие нестабильность модуля.

Для безопасного восстановления сеанса SLTP необходимо предпринять контрмеры, указанные в 6.1.2.4.

7.2.5 Сертификационный орган

Для того чтобы определенный класс TREM мог участвовать в условиях услуг распространения контента, изготовитель (разработчик или компоновщик) класса TREM должен создавать пару открытых ключей класса и скрытых ключей класса и применять их к открытому ключу класса с соответствующей информацией для CA.

Если CA убедился, что информация приложения корректна и TREM, отвечающий критериям безопасности/секретности, выполнен (или построен) должным образом, CA формирует сертификат на открытый ключ данного класса TREM и соответствующую ему информацию согласно [RFC 3280]. К сертификату добавляют цифровую подпись со скрытым ключом CA, а затем сертификат предоставляют изготовителю.

Изготовитель TREM вкладывает в TREM сертификат и соответствующий скрытый ключ класса, и после этого TREM может принять лицензию, передаваемую от TREM другого класса, который уже авторизован тем же CA (см. рисунок 4).

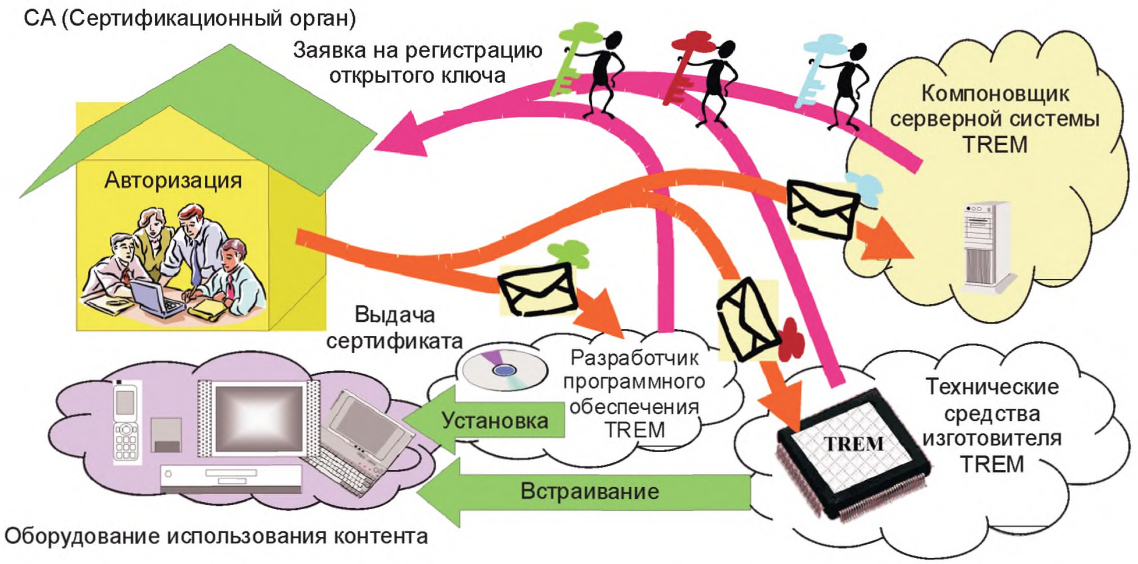


Рисунок 4 — Общее представление выдачи сертификатов классу TREM

7.2.6 Отмена ключа и окончание действия TREM

В данной безопасной модели следует поддерживать отмену ключа и окончание действия TREM через CRL (список отозванных/аннулированных сертификатов, указанный в Рекомендации X.509 МСЭ и в ИСО/МЭК 7498-1) в соответствии с требованиями, приведенными в 6.1.2.5.

CRL — это список идентификаторов отозванных сертификатов с цифровой подписью от CA. CRL используют следующим образом:

a) после выдачи CRL сертификационным органом этот CRL вкладывается в TREM, особенно во входные TREM;

b) если TREM назначения высылает отозванный сертификат в исходный TREM (т. е. в CRL опознается идентификатор сертификата для TREM назначения), передача лицензии отменяется.

7.3 Модель взаимодействия

7.3.1 Основная модель взаимодействия

В данной модели взаимодействия (см. рисунок 5) модуль переключения лицензии LRM переключает лицензию, защищенную посредством сеанса SLTP, между TREM. LRM — это система или модуль, которые управляют внутренней шиной и сетью/схемой для коммутации защищенной лицензии между TREM посредством сеанса SLTP. Однако защищенная лицензия не может ни дешифроваться, ни интерпретироваться LRM.

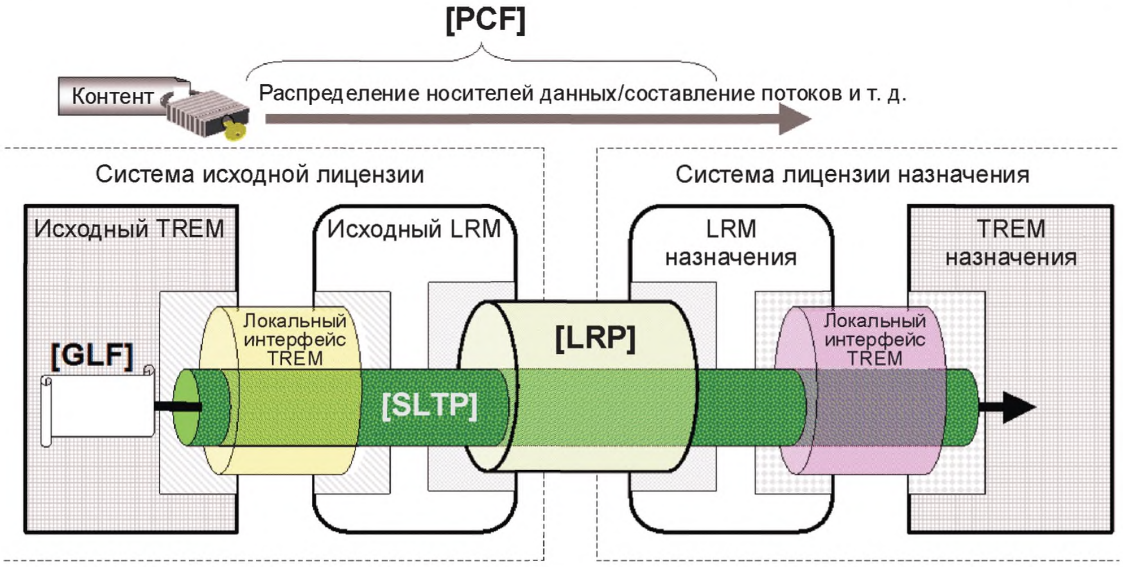


Рисунок 5 — Основная модель взаимодействия при защите контента

Исходные LRM и LRM назначения находятся перед каждым TREM в каждой системе обмена лицензиями и коммутируют защищенную лицензию за счет использования протокола между LRM, называемого LRP (протокол переключения лицензии). При SLTP протокол LRP обеспечивает такие функции, как управление транзакцией, рестарт отключенного сеанса SLTP, согласование протоколов и трансфер/передача информации, касающейся аутентификации пользователя или управления учетом сетевых ресурсов.

LRM и LRP отделены от TREM и SLTP по следующим причинам:

a) протоколы более низких уровней (например, интерфейса локальной шины) каждого класса локальных TREM отличаются друг от друга и весьма разнообразны. Поэтому, если требуется произвести обмен лицензией между TREM разных классов, необходимо, чтобы локальный протокол более низкого уровня преобразовывался с помощью LRM (в случае обмена по Интернету с использованием LRP);

b) в целях бизнеса большинство TREM следует изготавливать так же дешево и надежно, как TRM. Поэтому они не могут иметь многих функций, поддерживаемых в LRM;

c) при отделении изготовитель может только произвести заявку на выдачу TREM в CA. Поэтому, даже если расширены или изменены только функции LRM, изготовителю не требуется подавать ее снова.

SLTP не зависит от типа формата описания лицензии, передаваемого им. Можно использовать разные выражения прав, например XrML, CCI (информацию о возможности копирования) и другие.

SLTP, LRP не зависят от метода распространения и вида зашифрованного контента. Их также можно применить к разным услугам, например к обменам в носителях записей и услугам загрузки и составления потока. Также можно использовать разные типы защищенного контента от соответствующих служб/услуг распределения.

7.3.2 Модель протокола переключения лицензии LRP

7.3.2.1 Общие положения

LRP имеет не только функцию переключения сообщения SLTP, но также следующие функции:

a) управление и восстановление транзакции лицензии;

b) согласование протоколов между TREM;

c) взаимодействие по аутентификации пользователя и учету сетевых ресурсов.

7.3.2.2 Управление и восстановление транзакции лицензии

LRM придает множественные идентификаторы транзакций каждой транзакции передачи лицензии в соответствии с SLTP и управляет ими. При необходимости восстановления транзакции лицензии LRM автоматически запускает сеанс восстановления для данной транзакции с помощью функции восстановления SLTP. После завершения транзакции выполняется сбор ненужных данных ресурсов транзакции.

7.3.2.3 Согласование протоколов

LRP поддерживает следующие функции согласования для SLTP:

a) согласование версии: функция для согласования версий SLTP, LRP и формата лицензии, используемого в сеансе SLTP;

b) согласование криптографической системы/шифросистемы: функция для согласования алгоритмов для шифросистемы открытого ключа и симметричной шифросистемы, используемой в сеансе SLTP;

c) согласование хэш-алгоритмов: функция для согласования алгоритмов для хэш-функции, используемой в сеансе SLTP;

d) согласование набора кодов символов: функция для согласования набора кодов символов, используемого в сеансе SLTP;

e) согласование сценария прав: функция для согласования языка или формы описания прав, передаваемых посредством сеанса SLTP.

7.3.2.4 Взаимодействие по аутентификации пользователя и учету сетевых ресурсов

LRM назначения лицензии может послать информацию по аутентификации пользователя в исходный LRM лицензии в качестве параметра сообщения LRP, добавленного к сообщению «сертификации назначения» SLTP. Исходный LRM лицензии может выполнить этот процесс для взаимодействия с функцией управления пользователя или с функцией учета сетевых ресурсов при использовании информации по аутентификации пользователя.

7.3.3 Модель реализации взаимодействия

Система трансфера/передачи лицензии, основанная на LRP, включающем SLTP, может быть реализована на базе различных протоколов связи через их соответствующие интерфейсы, реализуемые агентом, запрашивающим лицензию, и агентом, выдающим лицензию (см. рисунок 6).

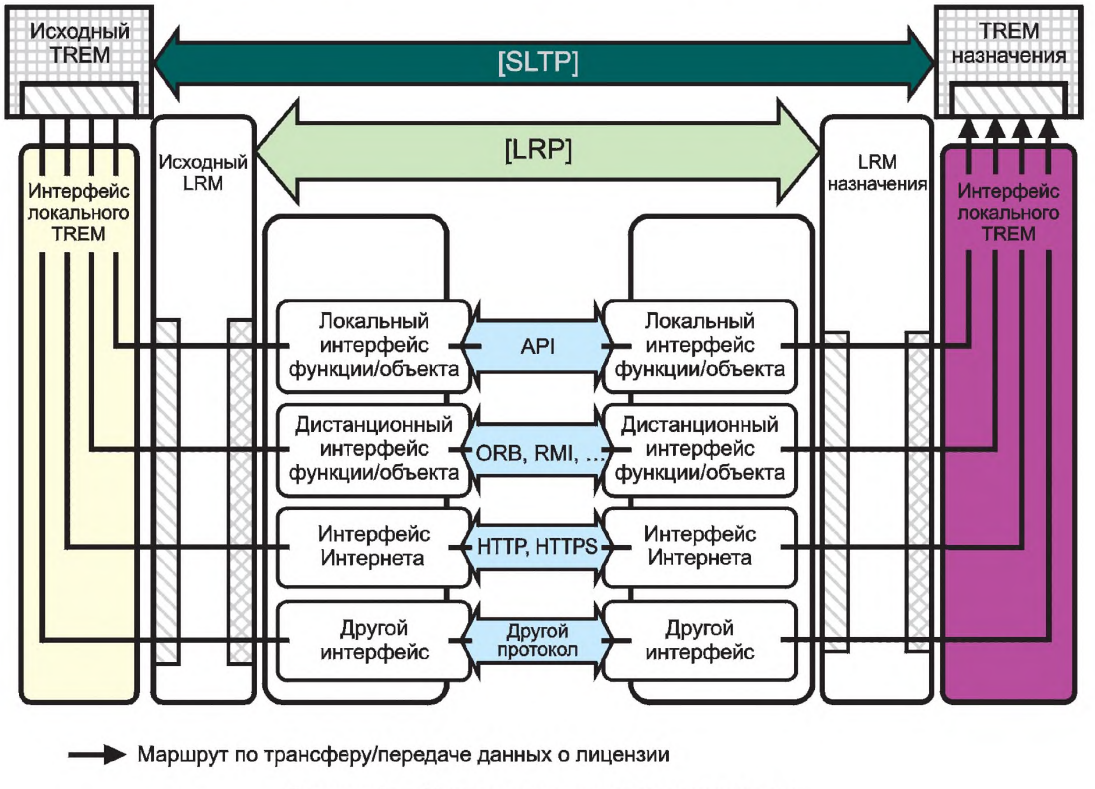


Рисунок 6 — Модель реализации взаимодействия

Агент, запрашивающий лицензию, и агент, выдающий лицензию, получают и выдают сообщение LRP (которое включает сообщение SLTP) с LRM назначения и исходным LRM соответственно, и эти агенты обмениваются сообщением LRP между собой, выполняя процедуры, указанные LRP.

Один агент может обмениваться сообщением LRP с другим агентом через различные интерфейсы (например, локальный интерфейс функции/объекта, дистанционный интерфейс функции/объекта, интерфейс Интернета и т. п.), так как сообщение LRP не зависит от каких-либо протоколов связи.

В данной модели реализации (см. рисунок 6) агент, запрашивающий лицензию, и агент, выдающий лицензию, реализуют следующие функции:

- интерфейсы протоколов связи для трансфера/передачи сообщений LRP;
- процедуру обмена сообщениями LRP, указанную LRP.

LRM реализует интерфейсы для сообщений LRP, поэтому LRM транслирует сообщение LRP во входные параметры локальных интерфейсов TREM и транслирует выходные данные локальных интерфейсов TREM в сообщения LRP.

7.4 Модель информации о лицензиях

7.4.1 Общие положения

Данные на полномочие обладания цифровыми правами/правами на цифровой продукт — это код или язык выражений, имеющий разные наборы разрешительной информации и разрешающих условий для передачи/трансляции цифрового контента. Данные на полномочие обладания цифровыми правами/правами на цифровой продукт и информация о лицензионных операциях могут распространяться в системы клиентов независимо.

Данные на полномочие обладания цифровыми правами/правами на цифровой продукт должны опознаваться вне зависимости от того, были они или нет фальсифицированы кем-либо, поэтому данные формата распространения должны включать цифровую подпись. Цифровые сертификаты на открытый ключ, соответствующий скрытому ключу, используемому для цифровой подписи, должны распределяться CA. CA может быть корневым CA или промежуточным CA, относящимся к его корневому CA. Каждый TREM должен проверять цифровую подпись на основании цифровых сертификатов. Цифровые сертификаты могут быть проверены путем отсылки к корневому CA. Конкретный стандарт подписи должен зависеть от каждой сервисной системы.

7.4.2 Данные на полномочие обладания цифровыми правами/правами на цифровой продукт

Данные на полномочие обладания цифровыми правами/правами на цифровой продукт имеют некоторые составляющие и элементы при этих составляющих. Пример такого синтаксиса представлен в МЭК 62227.

8 Аспекты, подлежащие стандартизации

Для реализации систем DRM, соответствующих модели, приведенной на рисунке 1, необходимо определить следующие аспекты с учетом того, что спецификации обрабатываются в оборудовании, например в основных бытовых устройствах, персональных компьютерах, домашних серверах, мобильных телефонах и т. п.:

a) SLTP;

b) LRP;

c) критерии оценки для TREM (посредством которых CA решает, является ли TREM авторизованным или нет).

Указанные выше спецификации должны отвечать требованиям, приведенным в разделе 6.

Приложение А
(справочное)

Пример алгоритмов для криптографической системы и случайных данных (хэш)

В SLTP не установлены алгоритмы криптографических систем и хэш-данных. В случае реализации такой модели необходимо определить критерии оценки безопасности для алгоритмов. Например, можно использовать указанные ниже алгоритмы криптографических систем и хэш-данных.

Криптографическая система симметричного ключа:

- криптографическая система с шифром стандарта DES с трехкратным шифрованием с двумя ключами, EDE и режимом внешнего сцепления шифрованных блоков CBC, указанным в [1][1)], [2] и [3];
- режим CBC AES (см. [7]).

Криптографическая система открытого ключа:

- криптосистема с использованием эллиптической кривой по рекомендованным NIST параметрам в двоичном поле (163 бита) (см. [8]);
- криптосистема с использованием эллиптической кривой по рекомендованным NIST параметрам в первичном поле (256 бит) (см. [6]);
- криптосистема открытого ключа с алгоритмом цифровой подписи Райвеста — Шамира — Эдельмана (RSA) (см. [10]).

Хэш-алгоритм:

- SHA-1, SHA-256, SHA-384, SHA-512 (см. [5]).

Для реализации шифрования, дешифровки и функции цифровой подписи с использованием криптосистемы с эллиптической кривой можно применять следующие алгоритмы:

- шифрование и дешифровка: EC-DH и стандарт DES с трехкратным шифрованием или AES, указанный в [8];
- цифровая подпись: алгоритм цифровой подписи на базе EC-DSA, указанный в [8].

В данной модели рекомендуется следующая длина ключа для каждой криптосистемы:

- криптосистема симметричного ключа — более 112 бит;
- криптосистема открытого ключа:
    - криптосистема с эллиптической кривой — более 160 бит;
    - криптосистема RSA: более 1024 бит.

[1)] Цифры в квадратных скобках относятся к первоисточникам, приведенным в разделе «Библиография».

Приложение В
(справочное)

Пример преобразования информации о правах в DRM, основанном на SLTP, в информацию существующего DRM

SLTP — это открытая (имеющая возможность к взаимодействию) спецификация и инструмент реализации хорошо расширяемых элементов управления цифровыми правами/правами на цифровой продукт DRM на базе инфраструктуры открытых ключей PKI, поэтому изготовители существующих DRM могут реализовывать TREM, который трансформирует информацию о правах в DRM SLTP в информацию существующего DRM. TREM, трансформирующий информацию о правах, должен реализовывать как SLTP, так и протокол существующего DRM.

На рисунках В.1 и В.2 приведены примеры преобразования/трансформации информации о правах.

Пример преобразования/трансформации информации о правах в DRM на базе SLTP в информацию существующего DRM.

1) Статическое преобразование.

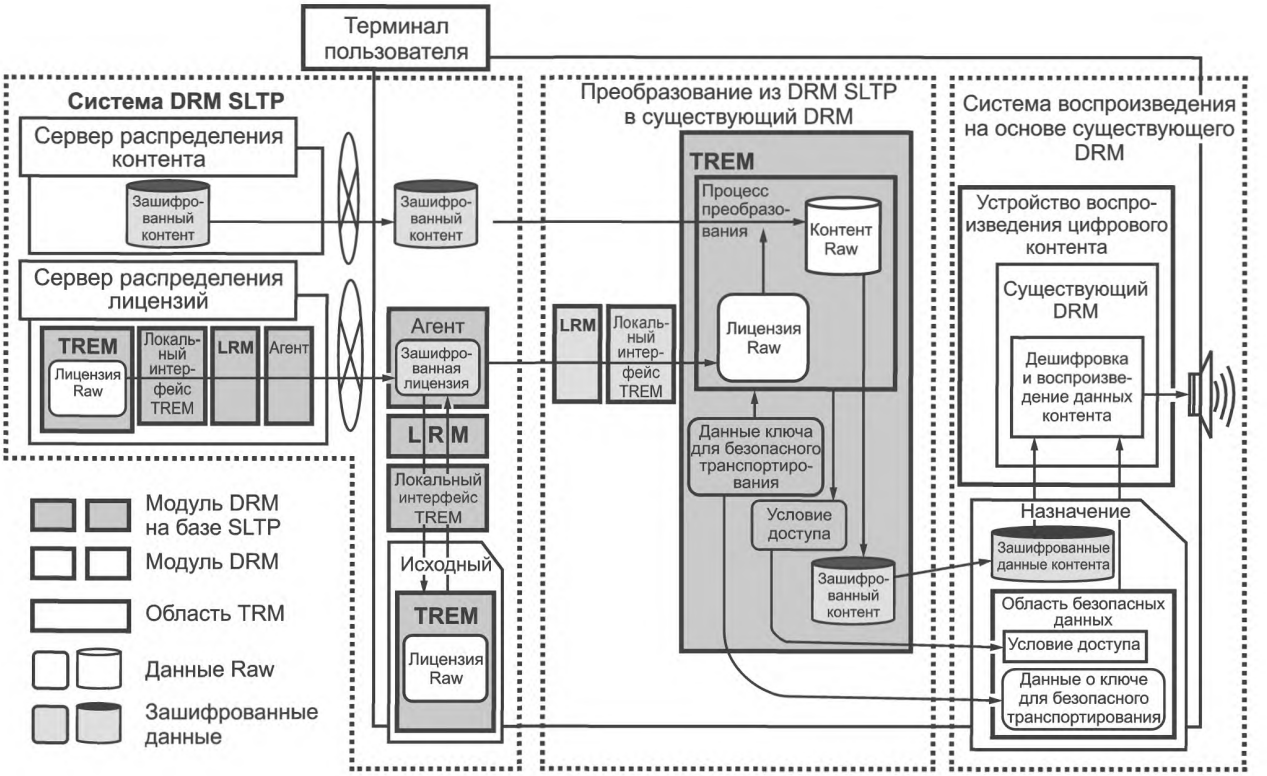


Рисунок В.1 — Пример статического преобразования информации о правах

На рисунке В.1 приведен пример статического преобразования информации о правах. Первоначально информация о правах (лицензия) распространяется от сервера лицензий SLTP и хранится в TREM, который реализован в запоминающей среде/на носителе данных через LRP, включающий SLTP. Затем информация о правах (лицензия) транспортируется из этого TREM в запоминающую среду/носитель данных другого TREM, реализующего преобразование через LRP, включающий SLTP. В итоге информация о правах преобразуется в информацию существующего DRM в TREM, реализующем это преобразование.

Пример преобразования/трансформации информации о правах в DRM на базе SLTP в информацию существующего DRM.

2) Динамическое преобразование.

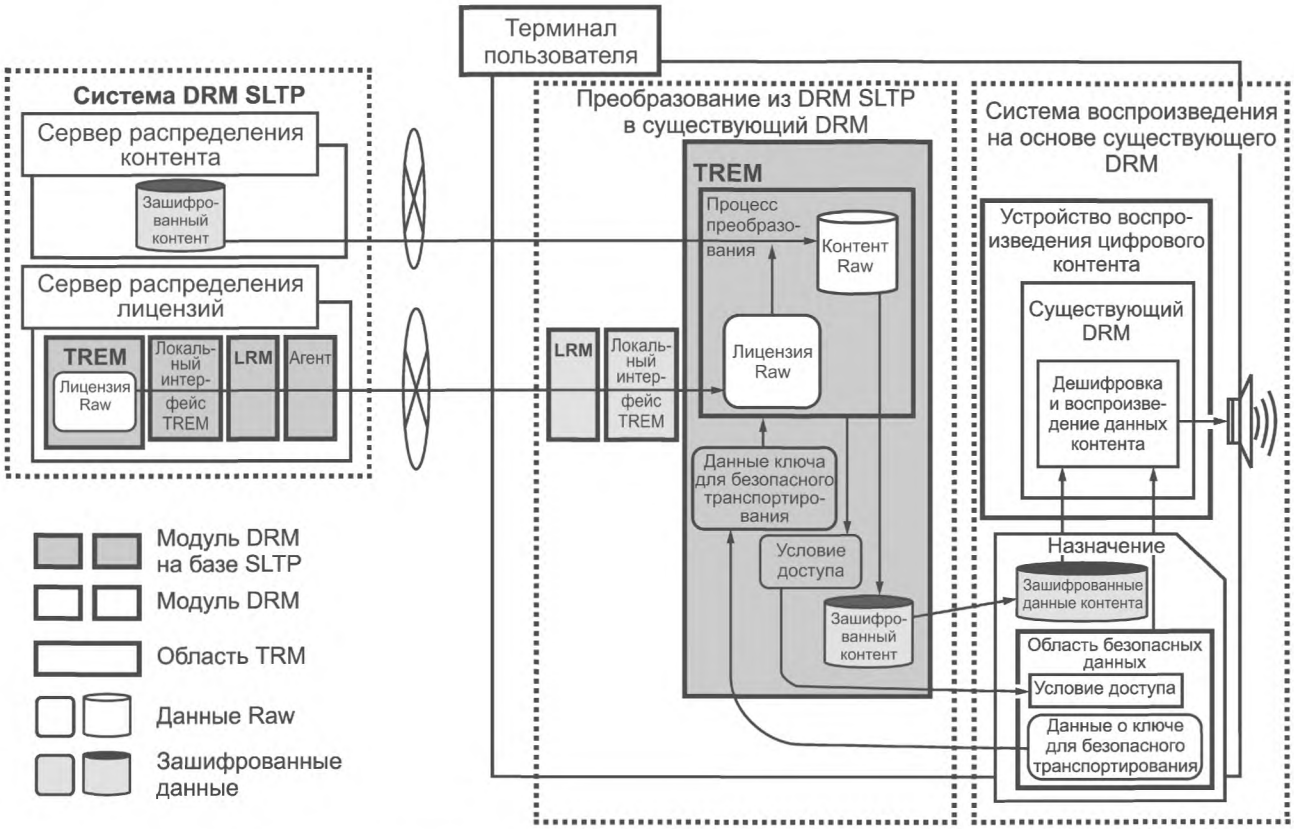


Рисунок В.2 — Пример динамического преобразования информации о правах

На рисунке В.2 приведен пример динамического преобразования информации о правах. Информация о правах (лицензия) распространяется от LRP, включающего сервер лицензий SLTP в TREM, реализующий преобразование, и информация о правах динамично преобразуется в информацию существующего DRM в этом TREM.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
IEC 62224:2008	—	*
ISO/IEC 7498-1:1994	IDT	ГОСТ Р ИСО/МЭК 7498-1—99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель»
ISO/IEC 9594-8:2008	—	*
ISO/IEC 15408-1:2009	IDT	ГОСТ Р ИСО/МЭК 15408-1—2012 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель»
ITU-T Recommendation X.509:1997	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

При подготовке настоящего стандарта в качестве ссылок использованы следующие документы:

[1] NIST — «Federal information processing standards publication 46-3: Data encryption standard (DES)», 1999 October 25 («Публикация 46-3. Федеральные стандарты по обработке информации. Стандарты на шифрование данных (DES)», 25 октября 1999 г.)

[2] NIST — «Federal information processing standards publication 81: DES modes of operation», 1980 December («Публикация 81. Федеральные стандарты по обработке информации. Режимы работы DES», декабрь 1980 г.)

[3] FIPS Publication Change Notice — FIPS PUB 81 — «DES modes of operation» — Change No: 2, 1996 May 31 («Режимы работы DES», изменение № 2, 31 мая 1996 г.)

[4] NIST: FIPS PUB 140-2 — «Federal information processing standards publication — Security requirement for cryptographic modules», 2001 May 25 («Публикация 140-2. Федеральные стандарты по обработке информации. Требования к безопасности криптографических модулей», 25 мая 2001 г.)

[5] NIST — «Federal information processing standards publication 180-2: Secure hash standard», 2002. Available at <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf> («Публикация 180-2. Федеральные стандарты по обработке информации. Стандарт на безопасность хэш-модулей», 2002. Доступ на сайте <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>)

[6] NIST — «Federal information processing standards publication 186-2: Digital signature standards (DSS)», January 27, 2000 Available at <http://csrc.nist.gov/publications/fips/ fips186-2/fips186-2-change1.pdf> («Публикация 186-2. Федеральные стандарты по обработке информации. Стандарты на цифровую подпись (DSS)», 27 января 2000 г. Доступ на сайте <http://csrc.nist.gov/ publications/fips/fips186-2/fips186-2-change1.pdf>)

[7] NIST — «Federal information processing standards publication 197: Advanced encryption standards (AES)», November 26, 2001 Available at <http://csrc.nist.gov/ publications/fips/fips197/fips-197.pdf> («Публикация 197. Федеральные стандарты по обработке информации. Усовершенствованный стандарт на шифрование (AES)», 26 ноября 2001 г. Доступ на сайте <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>)

[8] IEEE P1363 — «Standard specifications for public key cryptography» («Стандартные спецификации для криптографии с открытым ключом»)

[9] Request for comments:1945 — «Hypertext transfer protocol — HTTP/1.0», T. Berners-Lee (MIT/LCS), R. Fielding (UC Irvine), H. Frystyk (MIT/LCS), May 1996 («Протокол передачи гипертекста. HTTP/1.0», T. Berners-Lee (Массачусетский технологический институт/LCS), R. Fielding (UC Irvine), H. Frystyk (Массачусетский технологический институт/LCS)

[10] PKCS #1 v2.1 — «RSA cryptography standard, RSA laboratories», June 14, 2002 («Стандарт на шифрование методом Ривеста, Шамира и Адлемана (RSA)», лаборатории RSA, 14 июня 2002 г.)

[11] Request for comments:3280 — «Internet X.509 Public key infrastructure certificate and certificate revocation list (CRL) profile, Category: Standards track», R. Housley (RSA laboratories), W. Ford (VeriSign), W. Polk (NIST), D. Solo (Citicorp), April 2002 («Интернет X.509. Сертификат инфраструктуры с открытым ключом и профиль списка отозванных сертификатов (CRL). Категория: Предложенный стандарт», R. Housley (Лаборатории RSA), W. Ford (VeriSign), W. Polk (Национальный институт стандартов и технологий США), D. Solo (корпорация «Ситигруп», апрель 2002 г.)

[12] Request for comments:2246 — «The TLS protocol version 1.0, Category: Standards track», January 1999, T. Dierks (Certicom), C. Allen (Certicom) [«Протокол защиты (безопасности) транспортного уровня (TLS)]. Версия 1.0. Категория: Предложенный стандарт», январь 1999 г. T. Dierks (Certicom), C. Allen (Certicom)

УДК 621.377:006.354 ОКС 33.160.60
35.100.01 ОКП

Ключевые слова: безопасность, доступ, идентификатор, лицензия, мультимедиа, контент, ключ, право, сервер, транзакция, трансфер, угроза, хэш, TREM

Редактор *Л.С. Зимилова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 12.11.2018. Подписано в печать 28.11.2018. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,95.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,

117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru