ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 55811 — 2013

УПРАВЛЕНИЕ СЕРТИФИКАТАМИ ДЛЯ ФИНАНСОВЫХ УСЛУГ

Сертификаты открытых ключей

Издание официальное

Москва
Стандартинформ
2014

Предисловие

1 ПОДГОТОВЛЕН Федеральным бюджетным учреждением «Консультационно-внедренческая фирма в области международной стандартизации и сертификации – «Фирма «ИНТЕРСТАНДАРТ» (ФБУ «КВФ «ИНТЕРСТАНДАРТ») совместно с Центральным банком Российской Федерации (Банком России) на основе аутентичного перевода на русский язык стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 122 «Стандарты финансовых операций» и ТК 26 «Криптографическая защита информации»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Федерального агентства по техническому регулированию и метрологии от 22 ноября 2013 № 1714-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО 15782-1:2009 «Управление сертификатами для финансовых услуг. Часть 1. Сертификаты открытых ключей» (ISO 15782-1:2009 «Certificate management for financial services – Part 1: Public key certificates»)

5 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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 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 (gost.ru)

Содержание

Введение

В настоящем стандарте приведены требования для сферы финансовых услуг, а также определены процедуры управления сертификатами ключей проверки электронной подписи и элементы данных этих сертификатов.

Несмотря на то, что методы, указанные в настоящем стандарте предназначены для обеспечения целостности сообщений, имеющих финансовое назначение, и поддержки их неотказуемости, применение настоящего стандарта не гарантирует, что конкретная реализация обеспечит полную безопасность.

Связь между идентификационными данными владельца ключа проверки электронной подписи и этим ключом документируется, чтобы доказать право собственности на соответствующий ключ электронной подписи. Эта документированная связь устанавливается сертификатом ключа проверки электронной подписи. Сертификаты ключей проверки электронной подписи формируются доверенной организацией – удостоверяющим центром.

Надлежащее выполнение требований настоящего стандарта призвано обеспечить уверенность в соответствии идентификационных данных юридических или физических лиц ключу, используемому этими юридическими или физическими лицами для подписания документов, в том числе банковских переводов и контрактов.

Методы, определяемые в настоящем стандарте, могут быть использованы при установлении деловых отношений между юридическими лицами.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

УПРАВЛЕНИЕ СЕРТИФИКАТАМИ ДЛЯ ФИНАНСОВЫХ УСЛУГ

Сертификаты открытых ключей

Certificate management for financial services –Public key certificates

Дата введения — 2014—08—01

1 Область применения

Настоящий стандарт определяет систему управления сертификатами ключей проверки электронной подписи для использования в сфере финансовой деятельности юридическими и физическими лицами, включающую:

- содержание (данные) запроса на сертификат ключа проверки электронной подписи;
- типы систем удостоверяющих центров;
- создание, распределение, проверку, замену и продление сертификатов ключей проверки электронной подписи;
- приостановку, восстановление и прекращение действия сертификатов ключей проверки электронной подписи;
- цепочки сертификатов ключей проверки электронной подписи;
- процедуры аннулирования.

В настоящем стандарте также даны рекомендации относительно некоторых процедур (например, механизмов распределения, критериев приемлемости предоставленных свидетельств), полезных для практической деятельности.

Реализация настоящего стандарта также должна учитывать риски бизнеса и правовые нормы.

В настоящем стандарте не рассматриваются:

- сообщения, используемые между участниками процесса управления сертификатами ключей проверки электронной подписи;
- требования относительно нотариальной и временно́й отметки;
- требования к практикам создания сертификатов ключей проверки электронной подписи и политикам применения сертификатов ключей проверки электронной подписи;
- сертификаты атрибутов.

В настоящем стандарте не затрагивается создание или транспортировка ключей, используемых для шифрования.

Примечание – Использование полужирного шрифта без засечек, такого как **CertReqData** или **CRLEntry**, обозначает использование абстрактной синтаксической нотации (ASN.1), как определено в стандартах ГОСТ Р ИСО/МЭК 8824-1, ГОСТ Р ИСО/МЭК 8824-2–2001, ГОСТ Р ИСО/МЭК 8824-3–2002, ГОСТ Р ИСО/МЭК 8824-4–2003, ГОСТ Р ИСО/МЭК 8825-1–2003, ГОСТ Р ИСО/МЭК 8825-2.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 8824-1–2001 Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 1. Спецификация основной нотации

ГОСТ Р ИСО/МЭК 8824-2–2001 Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 2. Спецификация информационного объекта

ГОСТ Р ИСО/МЭК 8824-3–2002 Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 3. Спецификация ограничения

ГОСТ Р ИСО/МЭК 8824-4–2003 Информационная технология. Абстрактная синтаксическая нотация версии один (АСН.1). Часть 4. Параметризация спецификации АСН.1

Издание официальное

ГОСТ Р ИСО/МЭК 8825-1–2003 Информационная технология. Правила кодирования АСН.1. Часть 1. Спецификация базовых (BER), канонических (CER) и отличительных (DER) правил кодирования

ГОСТ Р ИСО/МЭК 8825-2–2003 Информационная технология. Правила кодирования АСН.1. Часть 2. Спецификация правил уплотненного кодирования (PER)

ГОСТ Р ИСО/МЭК 9594-8–98 Информационная технология. Взаимосвязь открытых систем. Справочник. Часть 8. Основы аутентификации

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

Для целей данного документа используются следующие термины и определения.

Стандартизованные термины и их краткие формы, представленные аббревиатурой, набраны полужирным шрифтом, а синонимы – курсивом. Заключенная в круглые скобки часть термина может быть опущена при использовании термина, при этом не входящая в круглые скобки часть термина образует его краткую форму.

3.1 **владелец сертификата ключа проверки электронной подписи;** *владелец сертификата* (public key certificate subject): Юридическое или физическое лицо, которому выдан сертификат ключа проверки электронной подписи.

3.2 **восстановление действия сертификата (ключа проверки электронной подписи)** (public key certificate release): Восстановление удостоверяющим центром действия сертификата ключа проверки электронной подписи, действие которого было приостановлено этим удостоверяющим центром.

3.3 **данные запроса на сертификат (ключа проверки электронной подписи)** (request data on public key certificate): Подписанная информация в запросе на сертификат ключа проверки электронной подписи, включающая ключ проверки электронной подписи физического или юридического лица, идентификационные данные этого лица и другую информацию, включаемую в сертификат.

3.4 **двойной контроль** (dual control): Процесс совместного участия двух или более юридических или физических лиц, действующих в общих целях обеспечения защиты важных функций или информации.

Примечание – Эти лица несут равную ответственность за обеспечение защиты информации, задействованной в уязвимых операциях. Ни одно из этих лиц в отдельности не может получить доступ к информации (например, криптографическому ключу) или использовать ее.

3.5 **доверенный ключ проверки электронной подписи** (trusted certification authority public key): Ключ проверки электронной подписи, полученный доверенным образом и используемый для проверки первого сертификата ключа проверки электронной подписи в цепочке сертификатов ключей проверки электронной подписи при проверке цепочки сертификатов.

Пример – Корневой ключ в иерархической системе удостоверяющих центров или ключ локального удостоверяющего центра в сетевой системе удостоверяющих центров (см. приложение Б).

3.6 **журнал аудита** (audit journal): Хронологическая запись системной активности, достаточная, чтобы позволить реконструкцию, анализ и изучение последовательности условий и действий, окружающих или приводящих к каждому событию в ходе транзакции от ее начала и до вывода окончательных результатов.

3.7 **замена сертификата (ключа проверки электронной подписи)** (public key certificate re-

key): Процесс, при котором владелец сертификата ключа проверки электронной подписи получает новый сертификат ключа проверки электронной подписи на новый ключ проверки электронной подписи после создания новой пары ключей.

3.8 **ключ проверки электронной подписи** (public key): Уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.

Примечание – В настоящем стандарте в целях сохранения терминологической преемственности по отношению к действующим национальным правовым и нормативным документам, регулирующих отношения по использованию электронной подписи (например [1, 2]), и опубликованным научно-техническим изданиям установлено, что термины «ключ проверки электронной подписи» и «открытый ключ» являются синонимами.

3.9 **ключ электронной подписи** (private key): Уникальная последовательность символов, предназначенная для создания электронной подписи.

3.10 **ключевая информация** (keying material): Данные, необходимые для выполнения криптографических операций, например изготовления ключей.

3.11 **конечный владелец сертификата ключа проверки электронной подписи:** *конечный владелец сертификата* (end entity): Владелец сертификата ключа проверки электронной подписи, за исключением удостоверяющего центра, использующий свой ключ электронной подписи для целей, отличных от подписания сертификатов ключей проверки электронной подписи.

3.12 **криптографический ключ** (cryptographic key): Параметр, который определяет работу криптографической функции.

Примечание – Криптографическая функция позволяет осуществить:
- преобразование обычного текста в шифрованный текст и наоборот;
- создание ключевой информации;
- создание или проверку электронной подписи.

3.13 **кросс-сертификация** (cross-certification): Процесс, при котором два удостоверяющих центра взаимно подтверждают ключи проверки электронных подписей друг друга.

3.14 **модуль ASN.1** (ASN.1 module): Совокупность идентифицируемых видов и значений абстрактной синтаксической нотации (ASN.1).

3.15 **отличительное имя** (distinguished name): Уникальный идентификатор владельца сертификата ключа проверки электронной подписи.

Примечание – Методы определения глобальной уникальности имени выходят за рамки настоящего стандарта.

3.16 **пара ключей** (key pair): Совокупность ключа проверки электронной подписи и соответствующего ему ключа электронной подписи.

3.17 **политика применения сертификатов (ключей проверки электронных подписей)** (public key certificate policy): Поименованный набор правил, определяющий порядок применения сертификата ключа проверки электронной подписи, для определенной совокупности и (или) отдельного класса бизнес-приложений с едиными требованиями безопасности.

Примечания:

1 Политика применения сертификатов ключей проверки электронных подписей должна использоваться пользователем сертификата ключа проверки электронной подписи при принятии решения о том, стоит ли признавать связь между владельцем сертификата и ключом проверки электронной подписи.

2 Конкретная политика применения сертификатов ключей проверки электронных подписей может указывать на условия применимости сертификата ключа проверки электронной подписи к аутентификации электронного обмена данными при транзакциях по торговле товарами в пределах данного ценового диапазона.

3.18 **пользователь сертификата** (relying party): Юридическое или физическое лицо, использующее сертификат ключа проверки электронной подписи для проверки электронной подписи.

3.19 **приостановка действия сертификата (ключа проверки электронной подписи)** (public key certificate suspension): Временное прекращение удостоверяющим центром действия сертификата ключа проверки электронной подписи.

3.20 **продление сертификата (ключа проверки электронной подписи)** (public key certificate renewal): Процесс, при котором юридическому или физическому лицу выдается новый сертификат существующего ключа проверки электронной подписи с новым сроком действия.

3.21 **разделенное знание** (split knowledge): Метод хранения криптографического ключа, при

котором два (или более) физических или юридических лица по отдельности, имеют части ключа, которые, по отдельности, не дают никаких сведений о результирующем криптографическом ключе.

3.22 **регламент выдачи сертификатов ключей проверки электронных подписей; РВС** (public key certification practice statement): Совокупность правил, регулирующих порядок выдачи и управления сертификатами ключей проверки электронных подписей удостоверяющим центром на протяжении их жизненного цикла.

3.23 **реестр сертификатов (ключей проверки электронных подписей)** (public key certificate register): Совокупность данных, включающая список выданных удостоверяющим центром сертификатов ключей проверки электронных подписей и информацию, содержащуюся в этих сертификатах, а также информацию о датах прекращения действия или аннулирования сертификатов ключей проверки электронных подписей и об основаниях таких прекращений или аннулирований.

3.24 **сертификат ключа проверки электронной подписи** (public key certificate): Электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу данного сертификата ключа проверки электронной подписи.

3.25 **сертификат ключа проверки электронной подписи удостоверяющего центра;** *сертификат УЦ* (certification authority public key certificate): Сертификат ключа проверки электронной подписи, владельцем которого является удостоверяющий центр, чей ключ электронной подписи используется для подписания сертификатов ключей проверки электронной подписи.

3.26 **система удостоверяющих центров;** *система УЦ* (certification authority system): Совокупность удостоверяющих центров, которые управляют сертификатами ключей проверки электронных подписей (включая соответствующие им ключи проверки электронных подписей и ключи электронных подписей) на протяжении жизненного цикла сертификата ключа проверки электронной подписи.

3.27 **список недействительных сертификатов ключей проверки электронных подписей; САС** (public key certificate revocation/non-action list): Список сертификатов ключей проверки электронных подписей, объявленных недействительными.

Примечание – Недействительными сертификатами являются сертификаты срок действия которых истек, приостановленные сертификаты и сертификаты, аннулированные по решению суда.

3.28 **уведомление по дополнительному каналу** (out-of-band notification): Уведомление с использованием средств связи, независимых от основных средств связи.

3.29 **удостоверяющий центр; УЦ** (certification authority): Юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные национальным законодательством.

3.30 **управление ключами** (key management): Обращение с ключевой информацией и ключами на протяжении их жизненного цикла в соответствии с политикой безопасности.

3.31 **часть ключа** (key fragment): Фрагмент ключа, переданный на хранение юридическому или физическому лицу для реализации метода разделения знаний.

3.32 **хэш-функция** (hash-function): Функция, отображающая строки бит в строки бит фиксированной длины и удовлетворяющая следующим свойствам:

1) по данному значению функции сложно вычислить исходные данные, отображаемые в это значение;

2) для заданных исходных данных сложно вычислить другие исходные данные, отображаемые в то же значение функции;

3) сложно вычислить какую-либо пару исходных данных, отображаемых в одно и то же значение.

[ГОСТ Р 34.11–2012, пункт 3.1.6]

Примечание – Применительно к области использования электронной подписи свойство по перечислению подразумевает, что:

1) по известной электронной подписи невозможно восстановить исходное сообщение; свойство по перечислению

2) для заданного подписанного сообщения трудно подобрать другое (фальсифицированное) сообщение, имеющее ту же электронную подпись; свойство по перечислению

3) трудно подобрать какую-либо пару сообщений, имеющих одну и ту же подпись.

3.33 **центр регистрации; ЦР** (registration authority): Служба (подразделение) УЦ, которая отвечает за регистрацию, идентификацию и аутентификацию владельцев сертификатов, и является

частью УЦ, но не создает и не выдает сертификаты.

Примечание – ЦР может участвовать в процессе получения сертификата ключа проверки электронной подписи, процессе прекращения действия сертификата ключа проверки электронной подписи, или в том и другом.

3.35 **цепочка сертификатов ключей проверки электронных подписей**; *цепочка сертификатов* (public key certification path): Упорядоченная последовательность сертификатов ключей проверки электронных подписей, которая, исходя из условия доверия первому сертификату ключа проверки электронной подписи этой цепочки (сертификату удостоверяющего центра), позволяет установить доверие конечному сертификату ключа проверки электронной подписи этой цепочки.

3.36 **электронная подпись** (digital signature): Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

Примечания:

1 Виды электронной подписи определены в [1].

2 Применение соответствующего вида электронной подписи определяется на основе правовых и нормативных актов уполномоченных органов или договорными отношениями между участниками электронного взаимодействия (см. [1]).

4 Инфраструктура открытых ключей

4.1 Обзор

Инфраструктура открытых ключей (PKI) – это термин, используемый для описания технической, юридической и коммерческой инфраструктуры, которая делает возможным широкое применение технологии открытого ключа.

Технология открытого ключа используется для создания электронной подписи и управления симметричными ключами. В криптографии с асимметричным ключом используются два ключа: один скрытно хранится у пользователя, а другой становится публично доступным (открытым). Подписанное или обработанное с помощью одного ключа может быть проверено на действительность с помощью дополняющего его ключа. Раскрытие открытого ключа не компрометирует дополняющий его ключа.

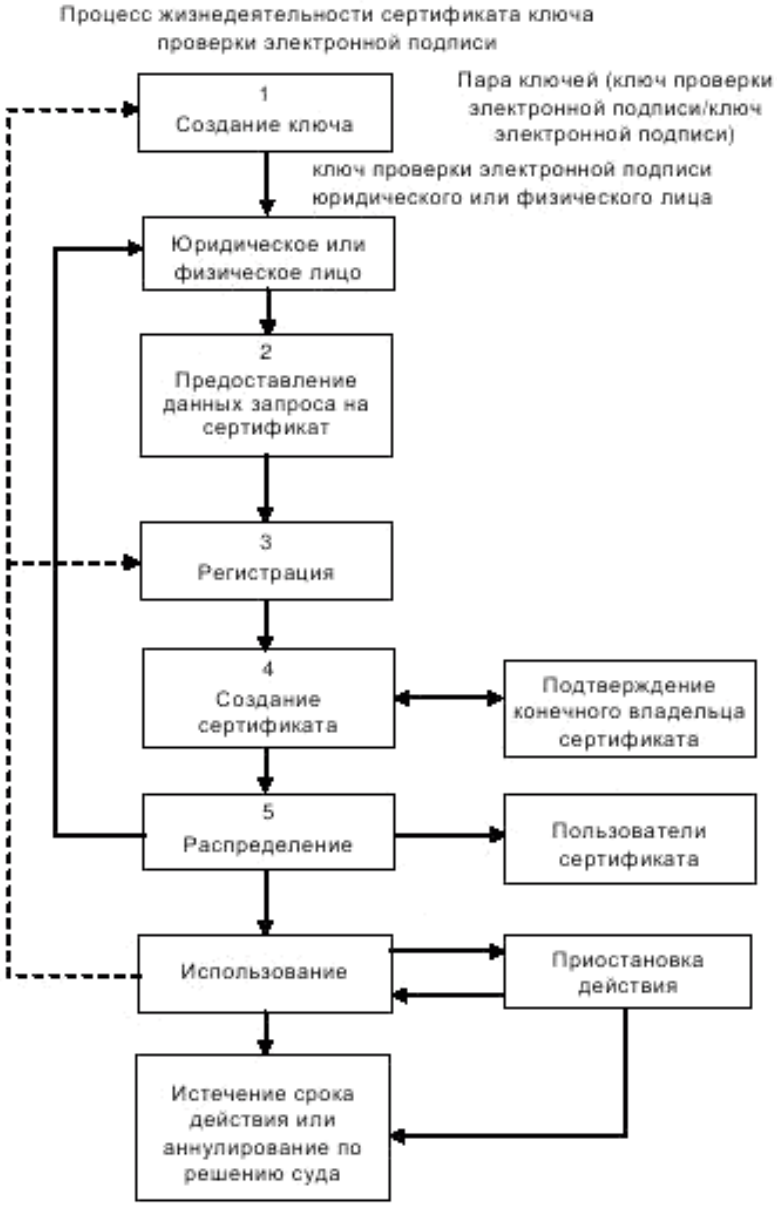
Аутентификация ключей проверки электронной подписи является необходимым условием, и поэтому такие ключи находятся в сертификатах ключей проверки электронной подписи. Сертификат ключа проверки электронной подписи содержит ключ проверки электронной подписи и идентификационные данные, а также электронную подпись УЦ. Настоящий стандарт основан на ГОСТ Р ИСО/МЭК 9594-8 в части аутентификации в открытых системах.

4.2 Процесс управления инфраструктурой открытых ключей

Обязанностями, услугами и процедурами, необходимыми для управления инфраструктурой открытых ключей, являются:

- создание ключей;
- регистрация;
- создание сертификатов;
- распределение;
- использование;
- приостановка, восстановление;
- прекращение срока действия;
- продление;
- замена.

Основные этапы процесса управления инфраструктурой открытых ключей показаны на рисунке 1.



Примечание – Цифры соответствуют этапам процессов, детализированных на рисунках 2

Рисунок 1 – Типовой процесс управления инфраструктурой открытых ключей

4.3 Удостоверяющий центр

УЦ создает сертификаты ключей проверки электронной подписи. Юридические и физические лица (в том числе УЦ) могут использовать сертификаты ключей проверки электронной подписи, чтобы аутентифицировать себя для пользователей сертификатов.

После того как сертификат ключа проверки электронной подписи создан, целостность его содержания защищается электронной подписью удостоверяющего центра. Настоящий стандарт не требует обеспечения конфиденциальности сертификатов ключей проверки электронной подписи. Учитывая, что пользователи сертификатов доверяют УЦ, это делает возможной проверку связи между ключом проверки электронной подписи юридического или физического лица, идентификационными данными этого лица и другой необходимой, содержащейся в сертификате ключа проверки электронной подписи информацией.

Цепочка сертификатов может быть составлена для двух основных архитектур: иерархической и сетевой.

В иерархической системе УЦ полномочия подстраиваются под головной УЦ, который создает и

выдает сертификаты ключей проверки электронной подписи для УЦ, непосредственно ему подчиненных. Эти подчиненные УЦ могут выдавать сертификаты ключей проверки электронной подписи подчиненным им УЦ или конечным владельцам сертификатов. В иерархической архитектуре ключ проверки электронной подписи головного УЦ выступает в качестве доверенного ключа проверки электронной подписи и известен каждому пользователю сертификатов. Действительность сертификата ключа проверки электронной подписи любого юридического или физического лица может быть проверена посредством проверки цепочки сертификатов, которая ведет от проверяемого сертификата ключа проверки электронной подписи обратно к доверенному ключу проверки электронной подписи (ключу проверки электронной подписи головного УЦ). В этой системе УЦ головной УЦ является общей точкой доверия для всех пользователей сертификатов.

Головной УЦ для связи за пределами своей области ответственности должен кросс-сертифицироваться с УЦ желаемой удаленной области. Проверка цепочки сертификатов предполагает создание последовательности сертификатов ключей проверки электронной подписи от удаленного физического или юридического лица до головного УЦ с помощью кросс-сертифицированного удаленного УЦ.

В сетевой системе УЦ, независимые УЦ могут кросс-сертифицировать друг друга посредством выдачи сертификатов ключей проверки электронной подписи друг другу. Это приводит к общей схеме доверительных отношений между УЦ и позволяет каждой группе (например, клиринговой палате, финансовому учреждению или его подразделениям) иметь собственный УЦ. Юридическое или физическое лицо использует ключ проверки электронной подписи выбранного УЦ как доверенный ключ проверки электронной подписи. Цепочка сертификатов состоит из тех сертификатов ключей проверки электронной подписи, которые идут в обратной последовательности от проверяемого на действительность сертификата ключа проверки электронной подписи до УЦ, ключ проверки электронной подписи которого получен пользователем сертификата доверенным образом.

Компрометация ключа электронной подписи УЦ компрометирует все сертификаты ключей проверки электронной подписи, выданных данным УЦ, поскольку злоумышленники с помощью скомпрометированного ключа электронной подписи могут создавать фальшивые сертификаты ключей проверки электронной подписи, а затем выдавать себя за одного или нескольких конечных владельцев сертификатов.

Жизненный цикл сертификата ключа проверки электронной подписи конечного владельца сертификата показан на рисунке 1.

4.4 Центр регистрации

ЦР отвечает за регистрацию, идентификацию и аутентификацию владельцев сертификатов, но не выполняет функции УЦ, и, следовательно, не создает и не выдает сертификаты. ЦР может способствовать процессу получения сертификата, процессу прекращения его действия, или тому и другому.

4.5 Конечный владелец сертификата

Конечный владелец сертификата использует свой ключ электронной подписи для целей, отличных от подписания сертификатов ключей проверки электронной подписи.

5 Системы УЦ

5.1 Общая информация

ЦР (в случае его наличия) является службой (подразделением) УЦ, действующей в рамках регламента выдачи сертификатов ключей проверки электронных подписей данного УЦ. Регистрация юридических и физических лиц с соблюдением всех требуемых мер безопасности может быть поручена ЦР или может быть частью услуг, предоставляемых УЦ.

При использовании ЦР взаимодействие ЦР с остальными службами УЦ должно быть аутентифицировано. Для этого процесса может быть использована электронная подпись.

5.2 Ответственность в системах УЦ

5.2.1 Ответственность и характеристики УЦ

5.2.1.1 УЦ несет ответственность за:

а) обеспечение безопасности ключа электронной подписи, связанного с ключом проверки

электронной подписи, содержащимся в сертификате ключа проверки электронной подписи УЦ;

б) обеспечение уверенности в том, что ключи проверки электронной подписи, сертификаты которых созданы УЦ, являются уникальными в области действия этого УЦ;

в) обеспечение отсутствия дублирования отличительного имени запрашивающей стороны с именем любого другого физического или юридического лица, сертификат ключа проверки электронной подписи которого был создан этим УЦ;

г) создание сертификатов ключа проверки электронной подписи с применением алгоритма электронной подписи к информации, указанной в сертификате ключа проверки электронной подписи;

д) поддержание механизма прекращения действия сертификатов и проверки, приемлемого для владельцев и пользователей сертификатов;

е) создание и распределение САС (см. приложение Д);

ж) создание пар ключей в соответствии с подробным сценарием процедуры создания ключей удостоверяющим центром и требованиями РВС;

з) разработку РВС и обеспечение его доступности для всех юридических и физических лиц;

и) обеспечение уверенности в том, что он владеет и управляет своими ключами электронной подписи;

к) замену пары ключей (проверки электронной подписи / электронной подписи) УЦ через интервалы времени, соответствующие рискам бизнеса.

Работа УЦ должна осуществляться в соответствии с РВС и соответствующими политиками применения сертификатов. УЦ несет ответственность за создание сертификатов и должен иметь возможность представлять информацию, содержащуюся в сертификатах ключей проверки электронной подписи, в форме, пригодной для чтения человеком.

Требования к распределению УЦ ключей проверки электронной подписи определены в 5.3.5.

5.2.1.2 Рекомендуется, чтобы УЦ обладал следующими характеристиками:

а) имел достаточно ресурсов для поддержания своей деятельности в соответствии со своими обязанностями;

б) был способен в достаточной мере принять свой риск ответственности перед конечными владельцами сертификатов и пользователями сертификатов, как это диктуется политикой применения сертификатов;

в) применял кадровую политику, которая обеспечивает доверие к деятельности УЦ;

г) использовал для реализации функций УЦ средства, удовлетворяющие нормативным требованиям уполномоченных органов. Средства УЦ должны быть соответствующим образом защищены.

Примечание – Классы средств электронной подписи и средств УЦ определены в [2]. Необходимый класс разрабатываемых (модернизируемых) средств УЦ определяется заказчиком (разработчиком) средств УЦ на основе [2].

д) обеспечивал доступность своих сертификатов ключей проверки электронной подписи, ключа проверки электронной подписи и САС для пользователей сертификатов;

е) определял и документально оформлял внутренние политики функционирования для области действия УЦ и обеспечивал их доступность заинтересованным лицам;

ж) обеспечивал уверенность в соответствии всем надлежащим нормативным требованиям.

Система УЦ должна обеспечить уверенность в том, что обязанности УЦ и ЦР (при его наличии) были определены.

5.2.2 Ответственность, которая должна быть возложена на УЦ или на ЦР

УЦ или ЦР (при его наличии) необходимо осуществлять следующее:

а) проверять действительность идентификационных данных юридического или физического лица, запрашивающего сертификат ключа проверки электронной подписи как будущий владелец данного сертификата;

б) проверять действительность идентификационных данных юридического или физического лица, запрашивающего сертификат ключа проверки электронной подписи, как доверенное лицо;

в) извещать о создании сертификата ключа проверки электронной подписи сторону, указанную в сертификате ключа проверки электронной подписи (при необходимости);

г) осуществлять передачу этого извещения способом, отличным от любых способов, используемых для передачи сертификата ключа проверки электронной подписи юридического или физического лица. Примерами таких способов передачи являются обычные почтовые письма для систем с низким уровнем риска (розничная торговля) и заказные письма для частных банковских систем. Реализация этой функциональности определяется риском бизнеса;

д) осуществлять аудит процесса выдачи сертификатов ключей проверки электронной

подписи в течение времени, определенного требованиями к сохранению записей;

е) осуществлять в соответствии с требованиями безопасности регистрацию аутентифицированных юридических и физических лиц;

ж) предоставлять своим конечным владельцам сертификатов руководство по безопасному управлению ключом электронной подписи конечного владельца сертификата;

з) информировать конечного владельца сертификата о том, что его работа определяется как скомпрометированная, если его ключ электронной подписи используется каким-либо другим юридическим или физическим лицом;

и) использовать соответствующие средства, чтобы убедиться в том, что конечный владелец сертификата понимает обязанности, сформулированные в 5.2.3, и в состоянии их выполнять;

к) в случае компрометации ключа электронной подписи УЦ незамедлительно информировать об этом владельцев и пользователей сертификатов в области действия УЦ;

л) осуществлять обработку запросов от юридических и физических лиц на выдачу, продление и замену сертификата, на прекращение и восстановление действия сертификата, а также (по решению суда) аннулирование сертификата.

Распределение указанных функций между ЦР и другими службами УЦ определяется при реализации системы УЦ.

Приложение В содержит рекомендуемые требования для приема данных запроса на сертификат. На предмет обеспечения требований контроля и уверенности в качестве безопасности см. 5.4.

5.2.3 Ответственность конечного владельца сертификата

К конечному владельцу сертификата предъявляются следующие требования:

а) обеспечивать уверенность в том, что ключ электронной подписи конечного владельца сертификата:

- хранится в контролируемой зоне, установленной для средства, реализующего криптографические функции;
- используется только уполномоченным лицом с применением надлежащих мер и средств контроля и управления доступом (например, пароля), согласно соответствующему РВС;

б) обеспечивать уверенность в том, что резервная копия ключа электронной подписи хранится в контролируемой зоне, установленной для средства, реализующего криптографические функции, тогда как сами средства хранятся в защищенном хранилище.

Требования безопасности для резервного копирования ключей электронной подписи могут быть основаны на 5.3.1.1. Ключ электронной подписи следует транспортировать безопасным способом;

в) предпринимать действия по обеспечению конфиденциальности ключа электронной подписи для предотвращения несанкционированного использования и компрометации ключа в течение его жизненного цикла;

г) предпринимать действия по незамедлительному уведомлению УЦ, когда конечный владелец сертификата знает или подозревает о потере, раскрытии или иного рода компрометации своего ключа электронной подписи;

д) обеспечить уверенность в том, что после компрометации или отзыва ключа электронной подписи конечного владельца сертификата использование этого ключа электронной подписи незамедлительно и окончательно прекращается;

е) обеспечить уверенность в том, что ключ электронной подписи какого-либо конечного владельца сертификата, который был ранее утерян или скомпрометирован, а затем найден, будет уничтожен;

ж) обеспечить уверенность в том, что в случае прекращения деятельности (например, ликвидации юридического лица) конечного владельца сертификата, существует назначенная ответственная сторона, обеспечивающая уничтожение ключа конечного владельца сертификата и уведомление системы УЦ;

з) обеспечить уровень безопасности, требуемый РВС и определенный соответствующим договорным соглашением;

и) предоставлять точные и полные данные для запроса на сертификат;

к) сообщать в УЦ/ЦР о любых неточностях или изменениях в содержании сертификата ключа проверки электронной подписи (например, изменение фамилии и т. д.).

5.3 Требования к жизненному циклу сертификата ключа проверки электронной подписи

5.3.1 Создание

5.3.1.1 Средства УЦ, реализующие криптографические функции с ключом электронной подписи, должны быть соответствующим образом защищены и недоступны для какого-либо другого

юридического или физического лица. Ключ электронной подписи УЦ также должен быть соответствующим образом защищен, поскольку обладание им позволит злоумышленнику замаскироваться под УЦ и сформировать ложные сертификаты ключей проверки электронной подписи.

Требования безопасности к ключу электронной подписи УЦ следующие:

а) порядок создания, использования, хранения и уничтожения ключа электронной подписи УЦ определяется в соответствии с требованиями эксплуатационной документации на средства УЦ, реализующие криптографические функции, и нормативными требованиями соответствующих уполномоченных органов (например, требованиями [2]);

б) процесс создания ключа проверки электронной подписи / ключа электронной подписи должен обеспечивать уверенность в том, что ключевая информация соответствует требованиям к ключу проверки электронной подписи;

в) только УЦ должен иметь доступ к своему ключу электронной подписи;

г) при переходе функций УЦ к другому уполномоченному юридическому или физическому лицу, ключ электронной подписи УЦ должен быть экспортирован безопасным способом, например:

- под двойным контролем с разделением знания; или
- в зашифрованном виде, при этом криптографическая стойкость шифрования должна соответствовать уровню защиты экспортируемого ключа электронной подписи УЦ;

д) после истечения срока действия ключа все копии ключа электронной подписи УЦ (и частей ключа, если они существуют) должны оставаться надежно защищенными или должны быть уничтожены безопасным образом.

5.3.1.2 При создании пары ключей для конечного владельца сертификата также необходимо соблюдать соответствующие требования. В частности создание пары ключей конечному владельцу сертификата может осуществляться средствами конечного владельца сертификата, реализующими криптографические функции, или средствами УЦ. Порядок создания, использования, хранения и уничтожения ключевой информации (пары ключей) конечного владельца сертификата определяется в соответствии с требованиями эксплуатационной документации на средства, реализующие криптографические функции конечного владельца сертификата, и нормативными требованиями соответствующих уполномоченных органов (например, требованиями [2]).

Если пара ключей создается УЦ, то применимы следующие дополнительные требования:

а) УЦ должен обеспечить уверенность в том, что ключ электронной подписи конечного владельца сертификата не раскрывается никому, кроме владельца ключа;

б) УЦ не должен сохранять копию какого-либо ключа электронной подписи, как только этот ключ доставлен конечному владельцу сертификата;

в) УЦ должен обеспечить безопасный канал доставки пары ключей конечному владельцу сертификата. При этом необходимо обеспечить конфиденциальность и целостность ключа электронной подписи конечного владельца сертификата.

5.3.2 Предоставление данных запроса на сертификат ключа проверки электронной подписи

Данные запроса на сертификат конечный владелец сертификата предоставляет в ЦР (а при отсутствии ЦР – в УЦ). Эти данные включают отличительное имя конечного владельца сертификата и другую информацию, позволяющую ЦР (УЦ) проверить идентификационные данные конечного владельца сертификата в соответствии с требованиями РВС.

Запрос на сертификат ключа проверки электронной подписи должен быть подписан ключом электронной подписи юридического или физического лица (в отношении соответствующих форм проверки идентификационных данных см. приложение В). ЦР (УЦ) необходимо проверить подпись в данных запроса на сертификат, чтобы обеспечить уверенность:

а) в целостности отличительного имени юридического или физического лица, ключа проверки электронной подписи и другой информации, подписанной с использованием ключа электронной подписи этого юридического или физического лица;

б) в том, что ключ проверки электронной подписи в данных запроса на сертификат соответствует ключу электронной подписи этого юридического или физического лица.

После создания ключа, но до его использования, конечный владелец сертификата должен:

- подготовить данные запроса на сертификат, включая отличительное имя конечного владельца сертификата и вновь созданный ключ проверки электронной подписи;
- поставить электронную подпись под данными запроса на сертификат с использованием ключа электронной подписи, связанного с ключом проверки электронной подписи, содержащимся в данных запроса на сертификат;
- предоставить подписанные данные запроса на сертификат и другую информацию в соответствии с требованиями РВС для ЦР (УЦ).

5.3.3 Регистрация

Когда ЦР обращается в службу (подразделение) УЦ, осуществляющую непосредственно создание сертификатов ключей проверки электронных подписей, за сертификатом ключа проверки электронной подписи от имени юридического или физического лица, запрашивающего сертификат ключа проверки электронной подписи, то он должен:

а) проверить действительность идентификационных данных юридического или физического лица, запрашивающего сертификат в соответствии с РВС УЦ (рекомендации по приему данных запроса на сертификат содержатся в приложении В);

б) проверить действительность владения юридическим или физическим лицом ключом электронной подписи, соответствующим ключу проверки электронной подписи, для которого запрашивается сертификат ключа проверки электронной подписи;

в) принять данные запроса на сертификат от юридического или физического лица, если его идентификационные данные действительны;

г) проверить данные запроса на сертификат в отношении ошибок или упущений;

д) проверить действительность электронной подписи юридического или физического лица в данных запроса на сертификат;

е) предоставить для юридического или физического лица копию ключа проверки электронной подписи УЦ в соответствии с требованиями 5.3.5, а также копию сертификата ключа проверки электронной подписи конечного владельца сертификата;

ж) предоставить юридическому или физическому лицу уведомление, подтверждающее успешную регистрацию и выдачу сертификата ключа проверки электронной подписи, используя метод уведомления по дополнительному каналу;

з) в зависимости от риска бизнеса, записывать свои действия в журнал аудита (см. приложение А).

При отсутствии ЦР указанные выше действия должен осуществлять УЦ.

Процесс выдачи сертификата ключа проверки электронной подписи с использованием только УЦ показан на рисунке 2. Процесс выдачи сертификата ключа проверки электронной подписи с использованием ЦР, входящего в состав УЦ, приведен на рисунке 3.

Рисунок 2 – Выдача сертификата только удостоверяющим центром

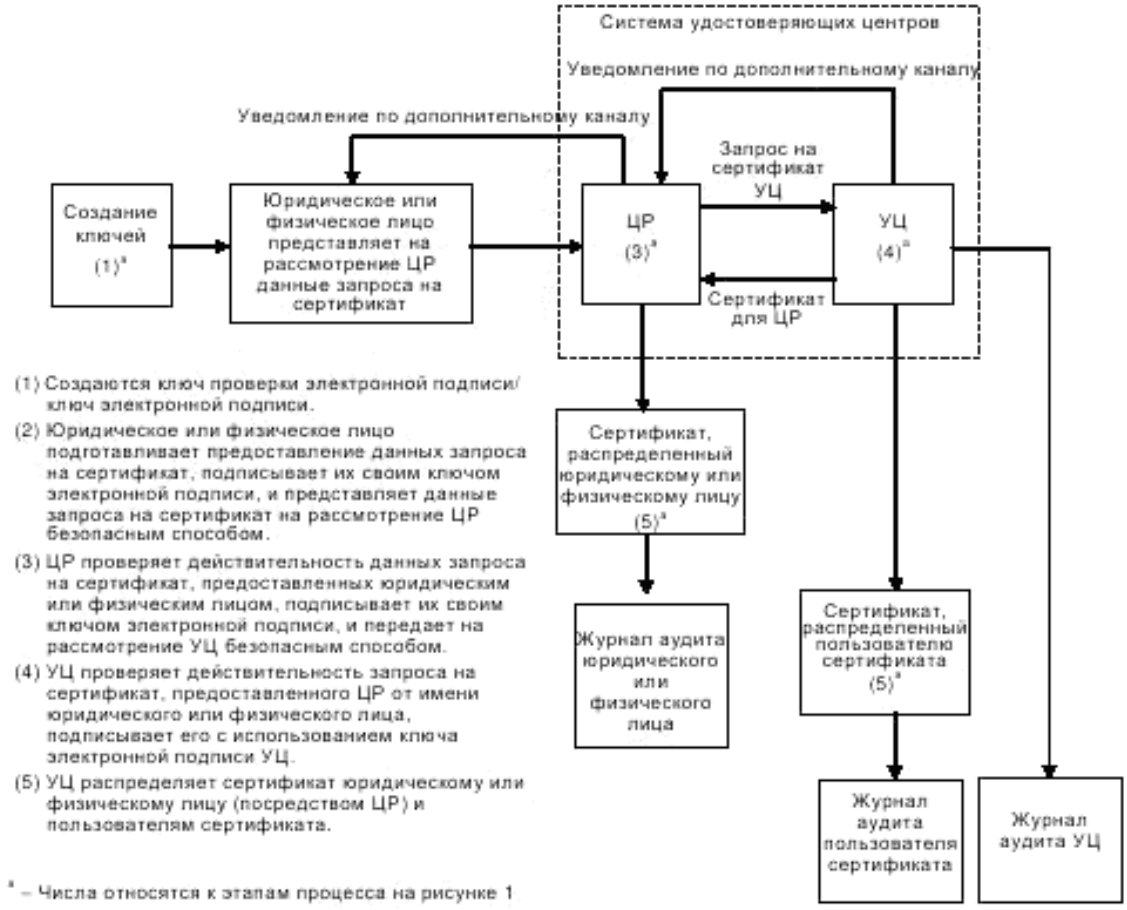


Рисунок 3 – Выдача сертификата удостоверяющим центром, использующим ЦР

5.3.4 Создание сертификата ключа проверки электронной подписи

Для новых запросов на сертификат ключа проверки электронной подписи УЦ должен:

а) проверить аутентичность представления юридического или физического лица, запрашивающего сертификат, или аутентичность ЦР (при его наличии);

б) проверить действительность подписи в предоставленных данных запроса на сертификат;

в) обеспечить уверенность в отсутствии дублирования отличительных имен запрашивающего и какого-либо другого юридического или физического лица, сертификат ключа проверки электронной подписи которого ранее был создан в УЦ;

г) обеспечить уверенность в уникальности ключа проверки электронной подписи, предоставленного для создания сертификата ключа проверки электронной подписи в области действия УЦ;

д) при обнаружении дубликатов ключей проверки электронной подписи УЦ должен:

1) прекратить действие всех сертификатов ключей проверки электронной подписи, содержащие дублированный ключ проверки электронной подписи;

2) отклонить запрос на получение сертификата ключа проверки электронной подписи.

Если какая-либо из этих проверок будет неудачной, УЦ должен отклонить запрос на сертификат ключа проверки электронной подписи.

В отношении запроса на сертификат ключа проверки электронной подписи УЦ также должен:

- обеспечить уверенность в соответствии информации в полях сертификата ключа проверки электронной подписи, информации, содержащейся в данных запроса на сертификат, РВС УЦ и, при необходимости, дополнить или изменить информацию в полях сертификата ключа проверки электронной подписи для достижения соответствия;
- включить дополнительные поля в сертификат ключа проверки электронной подписи для пополнения информации (при необходимости);
- использовать один или несколько ключей электронной подписи УЦ для подписания информации сертификата ключа проверки электронной подписи, тем самым создавая один или

несколько сертификатов ключа проверки электронной подписи в зависимости от действующей модели бизнеса;

- проверить свою электронную подпись сертификата ключа проверки электронной подписи до его выдачи;
- предоставить копию ключа (ключей) проверки электронной подписи УЦ в соответствии с требованиями 5.3.5, а также копию сертификата(ов) ключа проверки электронной подписи конечного владельца сертификата в ЦР[1)] (при его наличии) или непосредственно конечному владельцу сертификата, в зависимости от структуры системы УЦ (см. рисунки 2, 3);
- при наличии ЦР уведомить его безопасным способом (используя, при необходимости, возможности дополнительного канала), что были созданы один или несколько сертификатов ключа проверки электронной подписи;
- записать свои действия в журнал аудита.

Примечание – Создаваемые УЦ сертификаты ключей проверки электронной подписи и САС должны соответствовать международным рекомендациям МСЭ-Т X.509 [3]. Все поля и дополнения, включаемые в сертификат ключей проверки электронной подписи и в САС, должны быть заполнены в соответствии с рекомендациями X.509. При использовании альтернативных форматов сертификатов ключей проверки электронной подписи должны быть определены требования к протоколам создания и прекращения действия сертификатов ключей проверки электронной подписи и указаны в ТЗ на разработку (модернизацию) средств УЦ [2].

5.3.5 Распределение ключей проверки электронной подписи

Система УЦ должна предоставлять владельцам и пользователям соответствующих сертификатов один или несколько доверенных ключей проверки электронной подписи и соответствующие параметры, которые эти лица могут использовать для проверки первого сертификата ключа проверки электронной подписи в цепочке сертификатов.

УЦ может распределять по нескольку ключей проверки электронной подписи для обеспечения замены ключа проверки электронной подписи по истечении срока действия указанной пары ключей (проверки электронной подписи / электронной подписи), а также для их резервирования и восстановления.

Целостность ключа проверки электронной подписи УЦ и любых связанных с ним параметров играет важную роль. Когда существует единственная цепочка сертификатов, целостность цепочки сертификатов зависит от целостности ключа проверки электронной подписи и конфиденциальности ключа электронной подписи каждого УЦ в этой цепочке.

УЦ должен распределять свой ключ проверки электронной подписи и связанные с ним параметры, включающие срок действия ключ проверки электронной подписи и отличительное имя УЦ, а также обеспечивать уверенность в целостности и аутентичности этого ключа в процессе распределения. Метод распределения выбирается в зависимости от риска бизнеса, например:

а) доверенные ключи проверки электронной подписи могут изначально распределяться с использованием, например:

- машиночитаемых носителей (например, USB-носители);
- встраивания в клиентские средства, реализующие криптографические функции;
- и др.

б) если у юридического или физического лица, обращающегося за сертификатом ключа проверки электронной подписи, или пользователя сертификата уже имеется заверенная копия доверенного ключа проверки электронной подписи, новый доверенный ключ проверки электронной подписи может распределяться посредством, например:

- прямой электронной передачи от УЦ;
- любых методов начального распределения.

Целостность и аутентичность доверенного ключа проверки электронной подписи должны быть обеспечены независимо от способа передачи. Это может быть достигнуто использованием, например, одного из нижеперечисленных или эквивалентных им методов:

- распределение носителей информации под двойным контролем с разделенным знанием и подтверждением получения. Этот метод неприменим к прямой электронной передаче;
- подписание нового доверенного ключа проверки электронной подписи с использованием существующего доверенного ключа электронной подписи. При использовании этого метода получатель должен проверить действительность подписи. Этот метод не используется, если ключ

[1)] ЦР нет необходимости получать ключ проверки электронной подписи УЦ по каждому запросу сертификата ключа проверки электронной подписи.

электронной подписи УЦ скомпрометирован.

Ключ УЦ может быть включен в сертификат ключа проверки электронной подписи, подписанный другим УЦ, и быть частью цепочки сертификатов. В этом случае действительность ключа может быть проверена с помощью ключа проверки электронной подписи из предыдущего сертификата ключа проверки электронной подписи в цепочке.

Чтобы проверить действительность цепочки, включающей несколько сертификатов ключей проверки электронной подписи удостоверяющих центров, действительность начального сертификата ключа проверки электронной подписи в цепочке проверяется с помощью доверенного ключа проверки электронной подписи, который может быть распределен одним из методов, описанных в настоящем стандарте.

Проверяющий должен убедиться, что этот доверенный ключ проверки электронной подписи в настоящее время является действительным.

5.3.6 Распределение сертификатов ключей проверки электронной подписи

Сертификаты ключей проверки электронной подписи могут быть распределены пользователям сертификатов с использованием, например, следующих методов:

- вложением сертификатов ключей проверки электронной подписи в электронное сообщение;
- вложением в электронное сообщение указания о месте нахождения (хранилища) сертификатов ключей проверки электронной подписи.

ЦР также может распределять сертификаты ключей проверки электронной подписи пользователям сертификатов. Средства распределения в настоящем стандарте не рассматриваются.

5.3.7 Использование сертификатов ключей проверки электронной подписи

5.3.7.1 Использование сертификатов ключей проверки электронной подписи должно соответствовать требованиям, изложенным в 5.3.7.2 и 5.3.7.3.

5.3.7.2 Для того чтобы проверить действительность сертификата ключа проверки электронной подписи и получить действительный ключ проверки электронной подписи для немедленного использования, пользователь сертификата должен проверить:

а) срок действия сертификатов ключей проверки электронной подписи в цепочке (следует обратить внимание на то, что синхронизация часов отправителя, получателя и всех УЦ в цепочке является проблемой, и решения должны быть основаны на риске бизнеса);

б) статус всех сертификатов ключей проверки электронной подписи в цепочке сертификатов с использованием CAC или других соответствующих механизмов;

в) действительность подписей на всех сертификатах ключей проверки электронной подписи в цепочке сертификатов.

Решение относительно того, принять или отклонить сообщение, должно приниматься пользователем сертификата в зависимости от рисков бизнеса.

5.3.7.3 Всякий раз, когда происходит сбой проверки, должны быть предприняты следующие действия:

а) для бизнес-приложений с высокой степенью риска пользователи сертификата должны регистрировать в журнале аудита выявленные сбои проверки;

б) пользователи сертификата должны сохранять записи, связанные со сбоями проверки за период времени, в соответствии с требованиями правовых и нормативных актов и требованиями бизнеса. Эти записи должны включать:

- сообщение, которое не прошло проверку;
- цепочку сертификатов, связанную с этим сообщением;
- CAC или результаты использования других стандартных протоколов проверки статуса сертификата ключа проверки электронной подписи.

Сертификат ключа проверки электронной подписи должен быть использован только для целей, изложенных в политике применения сертификата.

Должна быть обеспечена уверенность в целостности любого ключа проверки электронной подписи и связанных с ним параметров, сохраняемых для дальнейшего использования. Например, это может быть достигнуто хранением всего сертификата ключа проверки электронной подписи и проверки его по мере необходимости, или извлечением и хранении ключа проверки электронной подписи для оперативного использования, обеспечивая его защиту от случайной или преднамеренной модификации.

В соответствии с 5.3.3 и 5.3.4, требуется, чтобы юридическому или физическому лицу был предоставлен:

- либо ключ проверки электронной подписи УЦ, который подписывает сертификат ключа проверки электронной подписи юридического или физического лица;
- либо ключ проверки электронной подписи любого УЦ в возможной цепочке сертификатов

между отправителем и получателем подписанной информации.

Ключ проверки электронной подписи УЦ пользователя сертификата используется, чтобы развернуть цепочку сертификатов от УЦ пользователя сертификата к УЦ отправителя и до отправителя.

Если ключ проверки электронной подписи другого УЦ в этой цепочке является доверенным, то цепочка может быть сокращена. Например, использование доверенного ключа проверки электронной подписи головного УЦ позволяет проверять цепочку от этого головного УЦ к отправителю, без необходимости проверки цепочки от пользователя сертификата к головному УЦ. Некоторые примеры таких альтернативных моделей доверия представлены в приложении Б.

5.3.8 Прекращение срока действия, приостановка действия или аннулирование сертификата ключа проверки электронной подписи

5.3.8.1 Прекращение или приостановка действия сертификата могут быть запрошены самим владельцем сертификата или ЦР (при его наличии), связанным с этим владельцем сертификата. Связь с ЦР устанавливается в момент запроса сертификата ключа проверки электронной подписи в соответствии с политикой применения сертификатов УЦ и ЦР. Там, где требуется предотвращение отказа в обслуживании, запрос на прекращение или приостановку действия сертификата должен быть аутентифицирован. В этом случае может быть использована электронная подпись.

Действие сертификата ключа проверки электронной подписи может быть прекращено или приостановлено только УЦ, выдавшим сертификат ключа проверки электронной подписи. Это может произойти по целому ряду причин, например:

- компрометация ключа электронной подписи конечного владельца сертификата;
- компрометация ключа электронной подписи УЦ;
- ключ проверки электронной подписи заменен другим;
- истек срока действия сертификат ключа проверки электронной подписи;
- прекращение деятельности УЦ без перехода его функций другому УЦ.

УЦ (или ЦР) должен проверить подлинность идентификационных данных юридического или физического лица, запрашивающего прекращение или приостановку действия сертификата, согласно практике бизнеса, с учетом относительного риска несанкционированного прекращение действия или приостановки.

5.3.8.2 Должны применяться процедуры и средства оперативной связи для содействия безопасному и аутентифицированному прекращению или приостановке действия:

- одного или нескольких сертификатов ключей проверки электронной подписи одного или нескольких юридических или физических лиц;
- всех сертификатов ключей проверки электронной подписи, выданных УЦ на основе единственной пары ключей (ключ проверки электронной подписи/ключ электронной подписи), используемой УЦ для создания сертификатов ключей проверки электронной подписи;
- всех сертификатов ключей проверки электронной подписи, выданных УЦ, независимо от используемой пары ключей (ключ проверки электронной подписи/ключ электронной подписи).

Независимо от того, истек ли срок действия сертификатов ключей проверки электронной подписи, было ли их действие прекращено или приостановлено, копии этих сертификатов ключей проверки электронной подписи и прошлые версии САС должны быть сохранены УЦ на период времени, требуемый законодательством, разумными практиками бизнеса и нормами. Требования для ведения записей САС, касающихся сертификатов ключей проверки электронной подписи с истекшим сроком действия, указаны в 5.3.8.3.

В случае прекращения действия сертификата ключа проверки электронной подписи действие всех сертификатов ключей проверки электронной подписи, содержащих тот же ключ проверки электронной подписи, должно быть немедленно прекращено.

5.3.8.3 Сертификаты ключей проверки электронной подписи, действие которых было прекращено или приостановлено, следует вносить в САС с отметкой времени, указывающей, когда связь между ключом проверки электронной подписи и идентификационными данными юридического или физического лица была прекращена или приостановлена.

После прекращения действия сертификата, юридическое или физическое лицо, чей сертификат ключа проверки электронной подписи прекратил действие, не может создавать подписи с помощью ключа электронной подписи, соответствующего ключу проверки электронной подписи в этом сертификате ключа проверки электронной подписи.

В отношении САС УЦ должен:

- создавать и подписывать САС, чтобы пользователи сертификатов могли проверить их целостность и дату выдачи;
- распределять САС на регулярной основе, даже если с момента последней выдачи не произошло никаких изменений;

- обеспечить доступность САС для всех пользователей сертификатов.

Периодичность и сроки выдачи САС необходимо определить в РВС. Записи САС, определяющие сертификаты ключей проверки электронной подписи, действие которых прекращено, должны оставаться в САС до окончания срока действия этих сертификатов ключей проверки электронной подписи.

В отношении способов распределения САС см. также ГОСТ Р ИСО/МЭК 9594-8.

5.3.8.4 Действие сертификата ключа проверки электронной подписи определяется сроком действия, указанным в сертификате ключа проверки электронной подписи, но который может быть ограничен УЦ согласно политике применения сертификатов.

УЦ может приостановить действие сертификата. Причинами таких действий являются:

а) желание уменьшить ответственность за ошибки при прекращении действия сертификата, когда предоставленной в УЦ информации недостаточно, чтобы определить, является ли запрос на прекращение действия сертификата действительным;

б) другие потребности бизнеса, такие как приостановка действия сертификата юридического или физического лица по результатам аудита или в процессе расследования.

Действие сертификата ключа проверки электронной подписи приостанавливается путем создания соответствующей записи в САС с указанием кода причины **certificatehold**.

5.3.8.5 Содействуя запрашивающему юридическому или физическому лицу в процессе приостановки действия сертификата, ЦР должен:

- проверить идентификационные данные и полномочия юридического или физического лица, запрашивающего приостановку действия сертификата;
- представить УЦ запрос на приостановку действия сертификата надлежащим способом;
- предоставить запрашивающему юридическому или физическому лицу письменное подтверждение приостановки действия сертификата.

5.3.8.6 После того как действие сертификата ключа проверки электронной подписи приостановлено, УЦ может выполнить одно из трех действий в отношении данного сертификата ключа проверки электронной подписи:

а) оставить его в САС без изменений;

б) заменить приостановку действия сертификата на прекращение действия того же самого сертификата ключа проверки электронной подписи;

в) восстановить действие сертификата, удалив соответствующую запись из САС.

Сертификат ключа проверки электронной подписи может быть использован после восстановления его действия. Действие сертификата ключа проверки электронной подписи восстанавливается посредством невнесения в следующий САС.

5.3.8.7 При прекращении действия сертификата ключа проверки электронной подписи УЦ должен:

а) проверить идентификационные данные и полномочия юридического или физического лица, запрашивающего прекращение действия сертификата ключа проверки электронной подписи;

б) подтвердить действительность запроса на прекращение действия сертификата;

в) подготовить уведомление о прекращении действия сертификата, подписать его своим ключом электронной подписи и отправить его запрашивающему юридическому или физическому лицу;

г) внести изменения в САС и подписать своим ключом электронной подписи;

д) обеспечить уверенность в доступности информации о статусе сертификата ключа проверки электронной подписи для всех пользователей сертификатов;

е) записать свои действия в журнал аудита.

УЦ должен предоставить юридическому или физическому лицу аутентифицированное подтверждение прекращения действия сертификата ключа проверки электронной подписи, а также может распределять уведомления о прекращении действия сертификата ключа проверки электронной подписи другим юридическим и физическим лицам, обратившимся в УЦ, и пользователям сертификатов.

5.3.8.8 ЦР (при его наличии) содействуя юридическому или физическому лицу в процессе прекращения действия сертификатов ключей проверки электронной подписи, должен:

- проверить идентификационные данные и полномочия юридического или физического лица, запрашивающего прекращение действия сертификата ключа проверки электронной подписи;
- представить УЦ запросы на прекращение действия сертификатов ключей проверки электронной подписи надлежащим способом, как того требует РВС;
- получить и проверить подтверждение того, что УЦ получил запрос на прекращение действия сертификата ключа проверки электронной подписи;
- предоставить запрашивающему юридическому или физическому лицу

аутентифицированное подтверждение прекращение действия сертификата ключа проверки электронной подписи;

- обеспечить уверенность в доступности информации о статусе сертификата ключа проверки электронной подписи для всех пользователей сертификатов;
- записать свои действия в журнал аудита.

ЦР также должен предоставить юридическому или физическому лицу аутентифицированное подтверждение прекращения действия сертификатов ключей проверки электронной подписи, как того требует РВС.

5.3.8.9 Действия, которые должны быть предприняты при прекращении или приостановке действия сертификата, определены в таблице 1.

Таблица 1 – Действия, которые должны предприниматься при прекращении или приостановке действия сертификата по какой-либо причине

Юридическое или физическое лицо	Действия
Владелец сертификата ключа проверки электронной подписи или ЦР	Владелец сертификата или ЦР могут: 1 запросить, чтобы УЦ прекратил, приостановил или восстановил действие сертификата, указывая **CertificateSerialNumber** для идентификации сертификата ключа проверки электронной подписи и запрошенный **CRLEntry reasonCode**; 2 отправить пользователям сертификата уведомление о приостановке (прекращении) действия сертификата; 3 обновлять журнал аудита для отражения предпринятых действий и причин их осуществления. Приостановленные сертификаты ключей проверки электронной подписи или сертификаты, действие которых прекращено, должны быть отмечены в журнале аудита
УЦ	УЦ должен удостовериться в действительности запроса на прекращение или приостановку действия сертификата в соответствии с РВС УЦ и выполнить следующие действия: 1 обновить САС. В случае прекращения действия сертификата ключа проверки электронной подписи, он должен оставаться в САС, как минимум, до выпуска первого САС после даты прекращения срока действия указанного в этом сертификате ключа проверки электронной подписи. В случае приостановки действия сертификата, он должен оставаться в САС до тех пор, пока не будет или явного восстановления его действия, истечения срока приостановки или срока действия сертификата (что наступит раньше); 2 отправить (опционально) пользователям сертификата уведомление о прекращении действия сертификата (приостановке); 3 обновить журнал аудита для отражения предпринятых действий и причин их осуществления. Сертификаты ключей проверки электронной подписи, действие которых приостановлено или прекращено, должны быть отмечены в журнале аудита
Пользователь сертификата ключа проверки электронной подписи	Пользователь сертификата должен: 1 отвергать любое сообщение, подписанное после даты прекращения действия соответствующего сертификата ключа проверки электронной подписи; 2 обновлять журнал аудита для отражения предпринятых действий и причин этих действий. Сертификаты ключей проверки электронной подписи, действие которых приостановлено или прекращено, должны быть зарегистрированы в журнале аудита. Дополнительно могут быть уведомлены и другие лица. В таблице 6 определены дополнительные действия, предпринимаемые в случае прекращения или приостановки действия сертификатов, используемых для защиты обмена ключами симметричного алгоритма.

5.3.8.10 Дополнительные действия, которые должны быть предприняты в зависимости от причины прекращения или приостановки действия сертификата, определены в таблицах 2 – 6.

Дальнейшими дополнительными действиями, которые могут быть предприняты юридическим или физическим лицом или ЦР (при его наличии), запрашивающим приостановку действия сертификата, являются следующие:

- юридическое или физическое лицо или ЦР могут запросить, чтобы УЦ, выдавший подлежащий приостановке сертификат ключа проверки электронной подписи, выполнил приостановку действия сертификата, указав **CertificateSerialNumber** для идентификации сертификата ключа проверки электронной подписи и опциональное значение приостановки **certificateHold** для поля **CRLEntry reasonCode**;
- если подлежащий приостановке сертификат ключа проверки электронной подписи является сертификатом ключа проверки электронной подписи УЦ, то САС УЦ, осуществляющего приостановку, должен содержать записи обо всех сертификатах ключей проверки электронной

подписи (выданных УЦ, действие сертификата которого приостанавливается), действие которых прекращено или приостановлено, выданных УЦ, действие сертификата которого приостанавливается.

Таблица 2 – Дополнительные действия, предпринимаемые в случае компрометации или подозрения на компрометацию ключа электронной подписи юридического или физического лица

Юридическое или физическое лицо	Действия
Владелец сертификата ключа проверки электронной подписи или ЦР	Владелец сертификата или ЦР могут направить в УЦ запрос на прекращение действия сертификата ключа проверки электронной подписи, указывая **CertificateSerialNumber** для идентификации сертификата ключа проверки электронной подписи и опциональное значение **keyCompromise** или **caCompromise** для поля **CRLEntry reasonCode**. Если владельцем сертификата является УЦ, то действие всех сертификатов ключей проверки электронной подписи, выпущенных на скомпрометированном ключе после даты возможной компрометации, должно быть прекращено и САС самого УЦ могут содержать записи всех сертификатов ключей проверки электронной подписи подозрительного УЦ с опциональным значением **caCompromise** для поля **reasonCode**
УЦ	УЦ, выдающий сертификаты ключей проверки электронной подписи, должен обновить САС. **CRLEntry** в САС может опционально содержать значение **keyCompromise** или **caCompromise** для поля **reasonCode**, соответственно
Пользователь сертификата ключа проверки электронной подписи	Прекратить использование всей ключевой информации, когда-либо отправленной или защищенной этим сертификатом ключа проверки электронной подписи

Таблица 3 – Дополнительные действия, предпринимаемые по причине прекращения деятельности

Юридическое или физическое лицо	Действия
Владелец сертификата ключа проверки электронной подписи или ЦР	Владелец сертификата или ЦР могут направить в УЦ запрос на прекращение действия сертификата ключа проверки электронной подписи, указывая **CertificateSerialNumber** для идентификации сертификата ключа проверки электронной подписи, а также **CRLEntry** и опционально значение **cessationOfOperation** для поля **reasonCode**. Если владельцем сертификата является УЦ, то действие всех выданных им сертификатов должно быть прекращено. Запрос может быть представлен юридическим или физическим лицом или его законным представителем
УЦ	УЦ должен обновить САС, указывая опционально значение **cessationOfOperation** для поля **reasonCode**.

Таблица 4 – Дополнительные действия, предпринимаемые в связи с изменением принадлежности юридического или физического лица

Юридическое или физическое лицо	Действия
Владелец сертификата ключа проверки электронной подписи или ЦР	Владелец сертификата или ЦР могут направить в УЦ запрос на прекращение действия сертификата ключа проверки электронной подписи, указывая **CertificateSerialNumber** для идентификации сертификата ключа проверки электронной подписи с опциональным запрашиваемым значением **affiliationChanged** для поля **CRLEntry reasonCode**. Если владельцем сертификата является УЦ, передающий функции другому УЦ, то САС нового УЦ должен включить все записи обо всех сертификатах ключей проверки электронной подписи, действие которых прекращено УЦ, передающим свои функции.
УЦ	УЦ должен обновлять САС, указывая опционально значение **affiliationChanged** для поля **reasonCode**.

Таблица 5 – Дополнительные действия, предпринимаемые в случае прекращения действия сертификата ключа проверки электронной подписи по причинам, отличным от компрометации ключа, прекращения деятельности или изменения принадлежности

Юридическое или физическое лицо	Действия
Владелец сертификата ключа проверки электронной подписи или ЦР	Владелец сертификата или ЦР могут направить в УЦ запрос на прекращение действия сертификата ключа проверки электронной подписи, указывая **CertificateSerialNumber** для идентификации сертификата ключа проверки электронной подписи и опциональное значение **superseded** или **unspecified** для поля **CRLEntry reasonCode** в САС.
УЦ	УЦ должен обновлять САС, указывая опциональное значение **superseded** или **unspecified** для поля **reasonCode** соответственно

Таблица 6 – Дополнительные действия, предпринимаемые в случае прекращения или приостановки действия сертификатов, используемых для защиты обмена ключами симметричного алгоритма

Причина прекращения или приостановки действия сертификата	Действия, которые должны быть предприняты пользователями сертификата
Компрометация или подозрение на компрометацию ключа электронной подписи юридического или физического лица	Использование всей ключевой информации, когда-либо присланной и защищенной с помощью этого сертификата ключа проверки электронной подписи должно быть прекращено. Если владельцем сертификата, действие которого прекращено или приостановлено, является УЦ, то в процессе замены ключевой информации должен быть использован другой УЦ
Истечение срока действия или прекращение действия сертификата ключа проверки электронной подписи по причинам, не являющимся фактической компрометацией или подозрением на компрометацию	Замена всей ключевой информации, отправленной и защищенной с помощью этого сертификата, как только это станет возможно
Действие сертификата ключа проверки электронной подписи приостановлено по причинам, не являющимся фактической компрометацией или подозрением на компрометацию	Когда действие сертификат ключа проверки электронной подписи приостановлено по причинам, не являющимся фактической компрометацией или подозрением на компрометацию, возможно прекращение использования или замены всей ключевой информации, отправленной и защищенной с помощью этого сертификата ключа проверки электронной подписи, как только это станет возможно

5.3.8.11 Сертификат ключа проверки электронной подписи может быть аннулирован по решению суда, в частности, если установлено, что сертификат ключа проверки электронной подписи содержит недостоверную информацию.

УЦ должен в течение не более чем одного рабочего дня аннулировать сертификат ключа проверки электронной подписи путем внесения записи о его аннулировании в реестр сертификатов по решению суда, вступившему в законную силу.

Использование аннулированного сертификата ключа проверки электронной подписи не влечет юридических последствий, за исключением тех, которые связаны с его аннулированием. До внесения в реестр сертификатов информации об аннулировании сертификата ключа проверки электронной подписи УЦ обязан уведомить владельца сертификата об аннулировании его сертификата ключа проверки электронной подписи путем направления документа на бумажном носителе или электронного документа.

5.3.9 Продление сертификатов ключей проверки электронной подписи

5.3.9.1 Сертификат ключа проверки электронной подписи имеет срок действия, указанный в сертификате ключа проверки электронной подписи.

До истечения срока действия сертификата конечный владелец сертификата может запросить продление сертификата посредством запроса на продление срока его действия (т. е., запрашивая дату **notAfter** более позднюю, чем дата **notAfter** существующего сертификата ключа проверки электронной подписи). Тем не менее, дата начала (дата **notBefore**) в продленном сертификате ключа проверки электронной подписи должна быть той же самой, что в исходном сертификате ключа проверки электронной подписи. Продленный сертификат ключа проверки электронной подписи будет иметь ту же пару ключей, что и исходный сертификат ключа проверки электронной подписи.

Сертификаты ключей проверки электронной подписи могут быть продлены только УЦ,

выдавшим данные сертификаты.

Конечный владелец сертификата, запрашивающий продление сертификата, должен собрать данные для продления своего сертификата и предоставить их в ЦР (при отсутствии ЦР – в УЦ, который ранее сформировал этот сертификат ключа проверки электронной подписи). Данные для продления сертификата должны предоставлять ЦР (УЦ) достаточно информации, позволяющей ЦР (УЦ) проверить идентификационные данные конечного владельца сертификата и определить сертификат ключа проверки электронной подписи для продления. Они включают:

а) отличительное имя конечного владельца сертификата;

б) серийный номер сертификата ключа проверки электронной подписи;

в) запрашиваемый срок действия сертификата.

Конечный владелец сертификата должен поставить электронную подпись под данными запроса на продление сертификата.

5.3.9.2 УЦ для продления сертификатов должен:

а) подтвердить действительность подписи на данных, представленных для продления сертификата;

б) проверить наличие и действительность сертификата ключа проверки электронной подписи, подлежащего продлению;

в) проверить, что запрашиваемый срок действия сертификата содержит ту же самую дату **notBefore**, что и дата **notBefore** в исходном сертификате ключа проверки электронной подписи, и что дата **notAfter** является более поздней, чем дата **notAfter** в существующем сертификате ключа проверки электронной подписи;

г) проверить, что запрашиваемый срок действия сертификата отвечает требованиям, определенным в политике применения сертификатов.

Если все эти проверки окажутся успешными, УЦ должен сформировать и подписать новый сертификат существующего ключа проверки электронной подписи, отличающийся от предыдущего сертификата только сроком действия, серийным номером сертификата ключа проверки электронной подписи и подписью УЦ. Если какая-либо проверка будет неудачной, УЦ должен отклонить запрос на продление сертификата.

УЦ должен сделать новый сертификат ключа проверки электронной подписи доступным для конечного владельца сертификата в соответствии с политикой применения сертификатов. Результатом продления сертификата будет существование двух сертификатов ключа проверки электронной подписи с одним и тем же ключом проверки электронной подписи. Это подразумевает, что:

- продление сертификата не требует прекращения действия предыдущего сертификата ключа проверки электронной подписи;
- при пересечении сроков действия сертификатов ключей проверки электронных подписей может быть использован любой из двух сертификатов ключа проверки электронной подписи.

5.3.10 Замена сертификата ключа проверки электронной подписи

5.3.10.1 Ключ проверки электронной подписи имеет срок действия, который может отличаться от срока действия, указанного в сертификате ключа проверки электронной подписи. Перед окончанием срока действия ключа проверки электронной подписи или всякий раз, когда возникает риск компрометации ключа электронной подписи, конечный владелец сертификата может запросить замену сертификата ключа проверки электронной подписи с созданием новой пары ключей. Этот новый сертификат ключа проверки электронной подписи будет иметь срок действия, установленный в соответствии с политикой применения сертификатов. Если замена сертификата ключа проверки электронной подписи была запрошена вследствие компрометации ключа электронной подписи, то действие старого сертификата ключа проверки электронной подписи должно быть прекращено.

Конечный владелец сертификата, запрашивающий замену действующего в настоящее время сертификата ключа проверки электронной подписи, должен собрать данные для замены своего сертификата ключа проверки электронной подписи и предоставить их в ЦР (при отсутствии ЦР – в УЦ, который ранее сформировал этот сертификат ключа проверки электронной подписи). Данные для замены сертификата должны предоставлять ЦР (УЦ) достаточно информации, позволяющей ЦР (УЦ) проверить идентификационные данные конечного владельца сертификата и утвердить сертификат ключа проверки электронной подписи для замены. Они включают:

а) отличительное имя конечного владельца сертификата;

б) серийный номер заменяемого сертификата ключа проверки электронной подписи;

в) запрашиваемый срок действия нового сертификата ключа проверки электронной подписи;

г) новый ключ проверки электронной подписи (если новая пара ключей создана конечным владельцем сертификата).

5.3.10.2 В процессе запроса на замену сертификата должен использоваться ключ электронной

подписи юридического или физического лица для подписания данных для замены сертификата, а ЦР (УЦ) должен подтвердить действительность подпись данных для замены сертификата, чтобы обеспечить уверенность:

а) в целостности отличительного имени конечного владельца сертификата, нового ключа проверки электронной подписи и другой информации во время применяемого процесса, используя новый ключ электронной подписи;

б) в том, что ключ проверки электронной подписи в данных для замены сертификата соответствует новому ключу электронной подписи юридического или физического лица;

в) в том, что в процессе создания и передачи ключа не было никаких ошибок.

5.3.10.3 После создания ключа и до его использования конечный владелец сертификата должен:

- собрать данные для замены сертификата, включая отличительное имя конечного владельца сертификата и заново созданный ключ проверки электронной подписи;
- подписать электронной подписью данные для замены сертификата, используя новый ключ электронной подписи, который связан с новым ключом проверки электронной подписи, содержащимся в данных для замены сертификата;
- представить подписанные данные для замены сертификата и другую информацию, как этого требует РВС, в ЦР (УЦ).

5.3.10.4 Для замены сертификатов ключа проверки электронной подписи УЦ должен:

а) подтвердить действительность подписи данных, представленных для замены сертификата;

б) проверить наличие и действительность сертификата ключа проверки электронной подписи, который должен быть заменен;

в) проверить, что запрос, включая запрашиваемый срок действия сертификата, отвечает требованиям, определенным в политике применения сертификатов.

Если все эти проверки являются успешными, УЦ должен сформировать и подписать новый сертификат ключа проверки электронной подписи (с новым серийным номером сертификата ключа проверки электронной подписи). Если какая-либо проверка будет неудачной, УЦ должен отклонить запрос на замену сертификата.

УЦ должен обрабатывать запрос на замену только в том случае, если предыдущий сертификат ключа проверки электронной подписи является действительным (т. е. не истек срок действия и его действие не прекращено).

Замена сертификата может осуществляться только УЦ, выдавшим данный сертификат ключа проверки электронной подписи.

5.4 Обеспечение безопасности и требования контроля

5.4.1 Требования к ведению журнала аудита

В системе УЦ необходимо вести журналы аудита, с целью предоставления достаточно подробной информации для восстановления событий, обеспечения и удовлетворения правовых и нормативных требований. Все записи в журналах аудита должны быть датированы и иметь отметку времени. Хотя журналы аудита, как правило, создаются и поддерживаются системой УЦ, некоторые журналы аудита могут, при необходимости, заполняться вручную. Требования контроля должны быть указаны в РВС УЦ.

Журнал аудита УЦ должен содержать записи обо всех операциях с сертификатами ключей проверки электронной подписи и обо всех операциях по управлению ключами, таких как создание, резервирование, восстановление и уничтожение ключей, вместе с идентификационными данными лица, разрешающего операцию, и лиц, работающих с любой ключевой информацией (например, частями ключей или ключами, хранящимися в портативных устройствах или на носителях информации). Изменения в хранении ключей электронной подписи и связанных с ними параметров, а также устройств и носителей, на которых хранятся ключи, необходимо регистрировать в журналах аудита. В журналы аудита не допускается записывать открытым текстом значения каких-либо ключей электронной подписи, но можно указывать значения хэш-функции, как средство идентификации ключей и проверки их корректности, а также ключи проверки электронной подписи, полученные из ключей электронной подписи посредством односторонней функции.

Перечень содержимого журнала аудита приведен в приложении А.

Журналы аудита должны вестись в форме, предотвращающей их несанкционированную модификацию или уничтожение. Автоматизированные журналы аудита должны быть защищены от модификации или замены, например с использованием хэш-функции или электронной подписи. Пара ключей, используемых для подписания журнала аудита, не должна использоваться для других целей.

Кроме того, журнал аудита должен быть доступен только уполномоченным лицам и при наличии веских причин, касающихся бизнеса и безопасности.

5.4.2 Обеспечение безопасности

Документированные процессы и процедуры по обеспечению безопасности необходимы как часть системы внутреннего контроля безопасности в процессе управления сертификатами ключей проверки электронной подписи. Журнал аудита должен просматриваться регулярно (например, ежедневно) согласно установленным требованиям обеспечения безопасности. Просмотр должен включать подтверждение целостности журнала аудита, а также выявление и наблюдение за несанкционированной или подозрительной деятельностью (например, доступ в необычное время или из необычных источников, неожиданное увеличение потребления системных ресурсов).

Масштабы и частота просмотра, а также требования к усилению управления должны быть определены с учетом риска бизнеса. Для бизнес-приложений с высокой степенью риска или для выполнения правовых и нормативных требований, или и того и другого, может потребоваться, чтобы конечные владельцы и пользователи сертификатов вели журнал аудита.

5.4.3 Проверка УЦ и ЦР

Проверки соответствия УЦ и ЦР требованиям безопасности должны являться обязанностью органа независимого контроля (внутреннего, внешнего или обоих) с установленной периодичностью (например, ежегодно). Проверка должна охватывать соблюдение политики применения сертификатов и РВС, руководств по процедурам и спецификации по конфигурации используемых средств. Результаты проверки должны быть официально оформлены и предоставлены проверяемым для устранения замечаний и реализации рекомендаций.

5.4.4 Проверка конечных владельцев сертификатов

В бизнес-приложениях с высокой степенью риска проверке могут подвергнуться также конечные владельцы и пользователи сертификатов.

5.5 Планирование непрерывности бизнеса

Требования к планированию непрерывности бизнеса зависят от потребностей в доступности и непрерывности приложений бизнеса, поддерживаемых УЦ. В основном бизнес-приложения с высокой степенью риска и высокой доступностью требуют более надежных процессов и методов обеспечения непрерывности бизнеса, чем бизнес-приложения с низким уровнем риска и низкой доступностью.

Как минимум, планирование непрерывности бизнеса должно включать процессы аварийного восстановления для всех критических компонентов систем УЦ, таких как аппаратные средства, программные средства и ключи в случае отказа одного или нескольких таких компонентов.

Варианты аварийного восстановления деятельности УЦ могут включать переустановку соответствующих средств, используемых УЦ, и повторную выдачу всех сертификатов ключей проверки электронной подписи, использование резервных средств УЦ (частичное резервирование, «холодный» или «горячий» узел).

Процессы аварийного восстановления деятельности УЦ также требуются в случае компрометации одного из важнейших компонентов безопасности. Компрометация или подозрение на компрометацию ключа электронной подписи УЦ следует рассматривать как инцидент безопасности. Все сертификаты ключей проверки электронной подписи, подписанные с помощью этого ключа после даты компрометации (если она известна), должны рассматриваться как подозрительные и, следовательно, действие их должно быть прекращено. Меры безопасности, реализуемые УЦ для защиты ключа электронной подписи УЦ, должны обеспечивать уверенность в том, что вероятность компрометации этого ключа является пренебрежимо малой.

Когда УЦ должен заменить или восстановить свой ключ электронной подписи, подлежат применению процедуры безопасного и аутентифицированного прекращения действия всех сертификатов ключей проверки электронной подписи, выданных УЦ с использованием этого ключа электронной подписи.

Примеры процедур аварийного восстановления деятельности УЦ описаны в приложении Г.

Юридическое или физическое лицо может иметь один или несколько действительных сертификатов ключей проверки электронной подписи на случай предполагаемых перемен или восстановления деятельности УЦ. Эти сертификаты ключей проверки электронной подписи обеспечивают непрерывность работы (услуги) по истечении срока действия сертификата ключа проверки электронной подписи, отказа средства, реализующего криптографические функции, или компрометации ключа электронной подписи.

Приложение А
(обязательное)

Содержание и использование журнала аудита УЦ

А.1 Содержание и защита журнала аудита УЦ и ЦР

А.1.1 Общая информация

Записи журнала аудита должны быть идентифицированы в отношении источника, даты и номера записи. В журнал аудита следует вносить только подтверждаемую и необходимую для журнала аудита информацию.

Большинство записей заносится в журнал аудита автоматически, однако некоторые важные, связанные с безопасностью, события могут вноситься вручную.

Также должны быть учтены положения 5.4.1 (последний абзац).

А.1.2 Элементы, подлежащие включению во все записи журнала аудита

Во все записи журнала должны быть включены следующие элементы:

а) дата и время записи;

б) регистрационный или порядковый номер записи;

в) тип записи;

г) источник (терминал, порт, местонахождение, клиент и т. д.);

д) идентификационные данные юридического или физического лица, делающего запись в журнале.

Записи, сделанные в журнале вручную, должны, при необходимости, включать следующее:

- идентификационные данные юридического или физического лица, санкционирующего операцию, и юридических или физических лиц, обрабатывающих любую ключевую информацию (например, части ключей или ключи, хранящиеся в портативных устройствах или на носителях информации);
- сведения об устройствах или носителях, на которых хранятся ключи.

А.1.3 Информация о применении сертификата ключа проверки электронной подписи, подлежащая внесению в журнал аудита ЦР или УЦ

В журнал аудита должна быть включена следующая информация:

а) тип идентификационного(ых) документа(ов), представленного юридическим или физическим лицом, обратившимся в УЦ;

б) запись уникальных идентификационных данных, номеров или их комбинации (например, номер документа, удостоверяющего юридическое или физическое лицо, обратившееся в УЦ), если это необходимо;

в) место хранения копий заявок на сертификат (на его создание, продление и т. п.) и идентификационных документов;

г) идентификационные данные лица, принявшего заявку на сертификат;

д) метод, используемый для проверки идентификационных документов, если таковые имеются;

е) наименование УЦ (ЦР), непосредственно принявшего запрос на сертификат ключа проверки электронной подписи от конечного владельца сертификата;

ж) о принятии владельцем сертификата ключа проверки электронной подписи пользовательского договора;

з) о согласии юридического или физического лица, обратившегося в УЦ, на ведение УЦ записей, содержащих персональные данные, и передачу этой информации указанным третьим сторонам; а также публикацию сертификатов ключей проверки электронной подписи (когда это требуется в соответствии с законодательством).

А.1.4 События, подлежащие внесению в журнал аудита

В журнале необходимо регистрировать следующие события, касающиеся ключевой информации:

а) создание ключей;

б) установка криптографических ключей вручную и ее результаты (с идентификационными данными оператора);

в) резервное копирование;

г) хранение;

д) восстановление;

е) изъятие ключевой информации из обслуживания;

ж) условное депонирование;

з) архивирование;

и) уничтожение;

к) формирование сертификатов;

л) получение запросов на сертификат(ы) ключа проверки электронной подписи, включая первичные запросы, запросы на продление и запросы на замену;

м) запросы на прекращение и приостановку действия сертификата;

н) прекращение, приостановка и восстановление действия сертификата;

о) получение, формирование и отправление САС;

п) распределение ключа проверки электронной подписи УЦ;

р) предоставление ключей проверки электронной подписи для сертификатов ключей проверки

электронной подписи;

с) действия, принятые при компрометации ключа электронной подписи.

А.1.5 События, важные по отношению к безопасности и подлежащие регистрации в журнале аудита

Записи журнала аудита должны содержать информацию, необходимую для анализа. Поэтому в журнале необходимо регистрировать следующие события, важные по отношению к безопасности или касающиеся чувствительной информации:

а) чтение или запись конфиденциальных файлов или документов;

б) действия с критически важными по отношению к безопасности данными;

в) изменения в профиле безопасности;

г) использование механизмов идентификации и аутентификации, как успешное, так и неудачное (включая многократные неудачные попытки аутентификации);

д) важные по отношению к безопасности нефинансовые транзакции (например, изменения учетной записи или имени/адреса и т. п.);

е) отказ системы, сбои аппаратных средств и другие нештатные ситуации;

ж) действия, предпринимаемые лицами, исполняющими доверенные роли: операторов компьютеров, системных администраторов и должностных лиц, обеспечивающих информационную безопасность систем;

з) изменение принадлежности юридического или физического лица;

и) доступ к журналу аудита;

к) действия, связанные с обходом процессов или процедур шифрования/аутентификации;

л) доступ к системе УЦ или какому-либо из ее компонентов.

А.1.6 Сообщения и данные, подлежащие внесению в журнал аудита

В журнал аудита должны быть включены следующие сообщения и данные:

а) все сообщения/данные (в электронном виде), входящие (исходящие) в (из) УЦ (включая САС);

б) все сформированные сертификаты ключей проверки электронной подписи;

в) идентификационные данные используемых криптографических ключей и их хэш (где это применимо)[1)];

г) идентификационные данные лиц, получающих части ключей.

А.2 Резервное копирование журнала аудита

Данные журнала аудита УЦ и ЦР должны подвергаться резервному копированию через соответствующие промежутки времени, а созданные копии следует хранить вне места эксплуатации.

А.3 Использование журнала аудита

Ручные и автоматизированные процедуры должны быть доступными для упрощения использования, просмотра и поддержки журнала аудита. Процедуры должны определять, когда о выявленных нарушении(ях) должно быть доложено руководству.

К примерам условий, требующих анализа и возможных действий, относятся:

а) необычное потребление системных ресурсов;

б) внезапное, неожиданное увеличение объема трафика и т. п.;

в) доступ в необычное время из необычных мест.

[1)] Контрольные числа, полученные из криптографических ключей с использованием функции хэширования, должны быть внесены в журнал аудита в качестве средства идентификации ключей и проверки их корректности.

Приложение Б
(справочное)

Альтернативные модели доверия

Б.1 Общая информация

Модели доверия определяют, как доверие делегируется между УЦ. Для проверки сертификата ключа проверки электронной подписи пользователь сертификата находит доверенную (надежную) цепочку сертификатов, от сертификата ключа проверки электронной подписи, проверяемого на действительность, до сертификата ключа проверки электронной подписи УЦ, которому юридическое или физическое лицо доверяет. Юридическое или физическое лицо одного УЦ может не владеть (или не доверять) ключом проверки электронной подписи УЦ, подписавшего сертификат ключа проверки электронной подписи другому юридическому или физическому лицу.

Различные модели доверия определяют механизмы построения цепочки сертификатов по иерархии УЦ. Эти модели доверия имеют общую характеристику, заключающуюся в том, что пользователю сертификата необходимо доверять ключу проверки электронной подписи только одного УЦ, чтобы получать и проверять сертификат ключа проверки электронной подписи юридического или физического лица. Доверенным ключом, как правило, является ключ головного УЦ (иерархическая система УЦ) или УЦ, выдавшего сертификат ключа проверки электронной подписи юридическому или физическому лицу (сетевая система УЦ).

Иерархическая системе УЦ показана на рисунке Б.1. Сетевая система УЦ показана на рисунке Б.2. Смешанная система УЦ обсуждается в Б.4 и показана на рисунке Б.3. Преимущества и недостатки модели доверия каждой системы УЦ приведены в таблице Б.1.

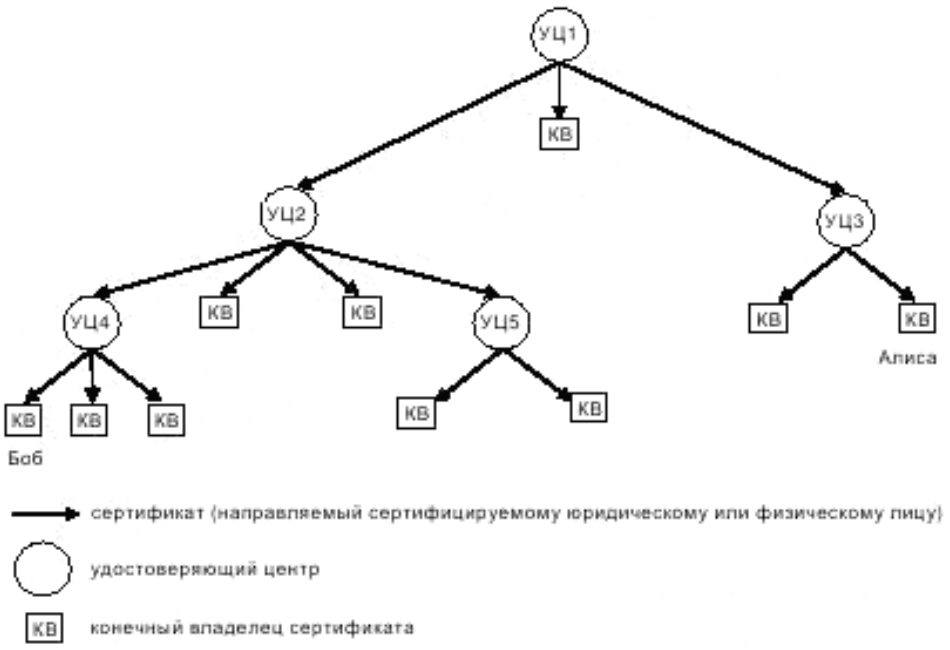


Рисунок Б.1 – Иерархическая система УЦ

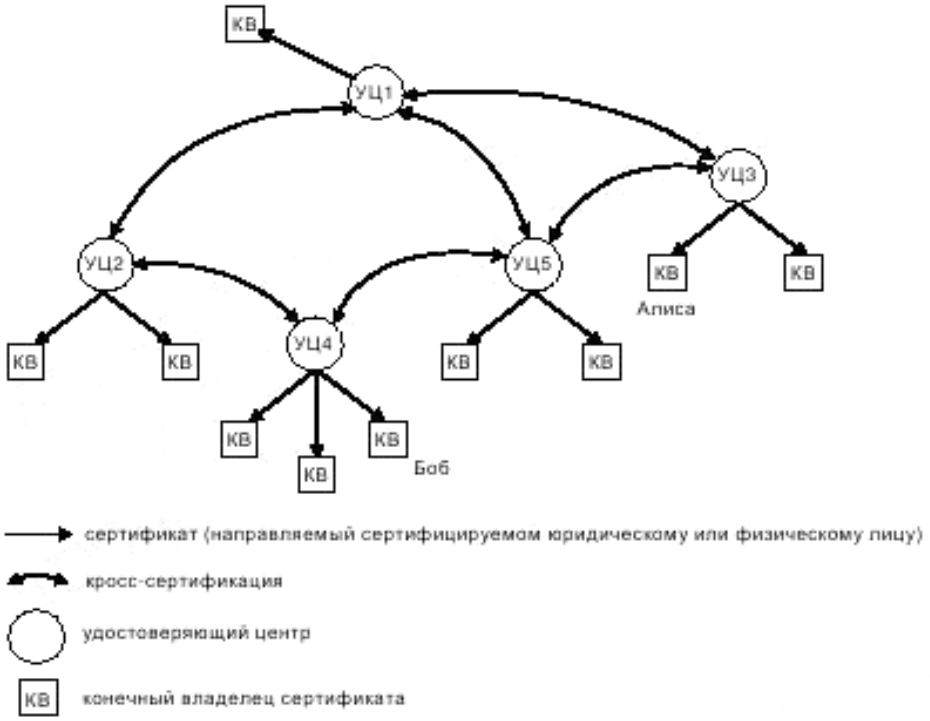


Рисунок Б.2 – Сетевая система УЦ

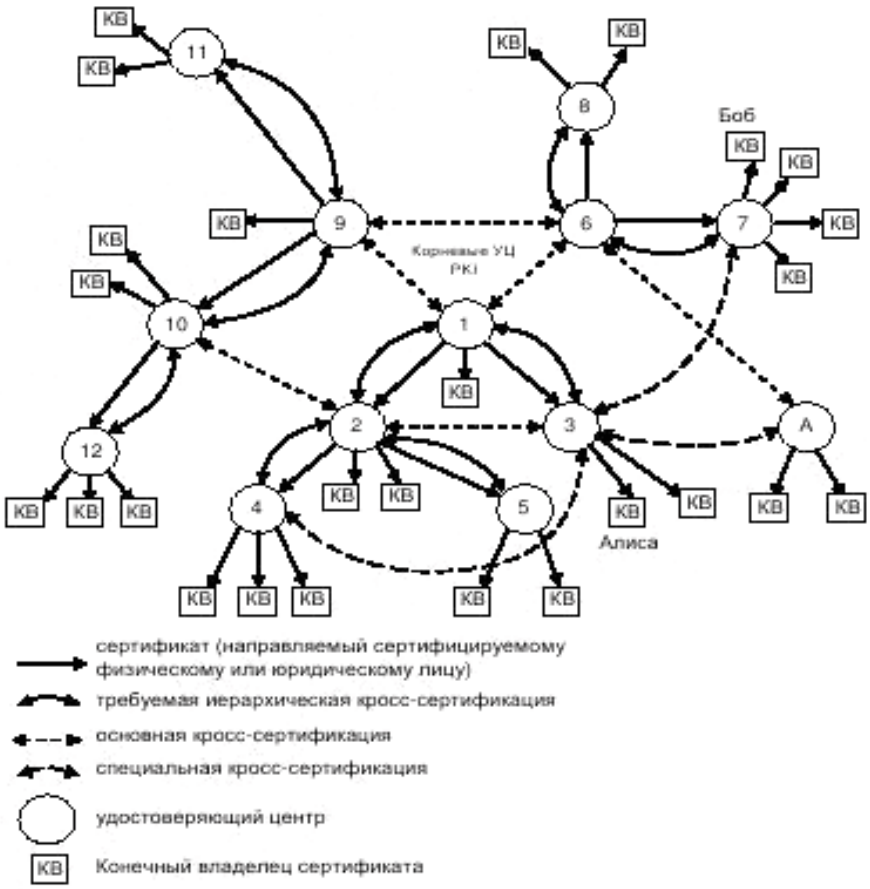


Рисунок Б.3 – Система УЦ смешанного типа

Таблица Б.1 – Преимущества и недостатки модели доверия различных систем УЦ

Система УЦ	Преимущества	Недостатки
Иерархическая	- Организационная структура управления многих организаций большей частью является иерархической. Отношения доверия часто выстраиваются в соответствии с организационной структурой, поэтому естественным является согласование цепочки сертификатов с организационной структурой. - Стратегия поиска цепочки сертификатов является простой. - Некоторые существующие системы спроектированы иерархическим образом. - У каждого юридического или физического лица имеется цепочка сертификатов, ведущая обратно к головному УЦ. Указанное юридическое или физическое лицо может предоставить свою цепочку сертификатов любому другому юридическому или физическому лицу, а любое другое юридическое или физическое лицо может проконтролировать эту цепочку сертификатов, поскольку все юридические и физические лица знают ключ проверки электронной подписи головного УЦ	- Маловероятно, что будет существовать единственный головной УЦ для всемирной PKI. - Коммерческие и деловые доверительные отношения не обязательно являются иерархическими. - Компрометация головного ключа электронной подписи является чрезвычайным происшествием, и его восстановление требует безопасного распределения нового ключа проверки электронной подписи для каждого юридического и физического лица. Однако компрометация ключа электронной подписи УЦ, выдающего сертификаты ключей проверки электронной подписи, делает недействительными только сертификаты ключей проверки электронной подписи, выданные этим УЦ
Сетевая	- Она является гибкой, способствует произвольным связям и доверительным отношениям, а также отражает двусторонние отношения доверия бизнеса. - Некое юридическое или физическое лицо как минимум доверяет УЦ, выдавшему ему сертификат ключа проверки электронной подписи в какой-либо PKI, поэтому рационально сделать этот УЦ основой всех отношений доверия. - Организационно удаленные УЦ, конечные владельцы сертификатов, которых сотрудничают с высокой степенью доверия, могут быть напрямую кросс-сертифицированы в соответствии с политикой высокого доверия, которая не распространяется на другие и расположенные выше УЦ, которые могли бы быть в более длинной иерархической цепочке сертификатов. - Она делает возможной прямую кросс-сертификацию УЦ, юридические или физические лица которых часто общаются, уменьшая нагрузку, связанную с обработкой цепочки сертификатов. - Восстановление после компрометации ключа электронной подписи какого-либо УЦ требует только того, чтобы новый Ключ проверки электронной подписи (и сертификаты ключей проверки электронной подписи, подписанные с помощью соответствующего нового ключа электронной подписи) безопасно распределялся держателям сертификатов этого УЦ	- Стратегии поиска цепочки сертификатов могут быть более сложными. - Некое юридическое или физическое лицо не может предоставить единственную цепочку сертификатов, которая является гарантированной, чтобы сделать возможным подтверждение ее подписей всеми другими юридическими и физическими лицами PKI
Смешанная	- Реализует иерархическую сеть доверия, которая предоставляет для каждого пользователя цепочку сертификатов, ведущей обратно к головному УЦ. - Делает возможной прямую кросс-сертификацию УЦ, пользователи которых часто общаются, уменьшая нагрузку, связанную с обработкой цепочки сертификатов. - Отражает двусторонние отношения доверия бизнеса. - Выравнивание цепочки сертификатов с организационной структурой.	- Стратегии поиска цепочки сертификатов могут быть намного более сложными. - Кросс-сертификация между подчиненными УЦ представляет риск.

Б.2 Иерархическая система УЦ

В иерархической системе УЦ уровень доверия к любому действительному сертификату ключа проверки электронной подписи является фактически уровнем доверия к ключу проверки электронной подписи головного УЦ. В этой системе УЦ ключ проверки электронной подписи головного УЦ не сертифицирован, поскольку явно отсутствует юридическое или физическое лицо, чтобы сертифицировать его ключ проверки электронной подписи. В иерархической системе УЦ ключ проверки электронной подписи головного УЦ рекомендуется распределять с помощью средств дополнительного канала доставки (например, курьером, застрахованным соответствующим образом). Это требует использования иерархической системы УЦ создания сертификатов, при которой юридическое или физическое лицо не обязано иметь доверенную копию ключа проверки электронной подписи своего УЦ.

В иерархической системе УЦ головной УЦ выдает сертификаты ключей проверки электронной подписи подчиненным УЦ. Эти УЦ могут выдавать сертификаты ключей проверки электронной подписи УЦ, расположенным ниже их в иерархии, или юридическим и физическим лицам. Иерархическая система УЦ показана на рисунке Б.1.

В иерархической системе УЦ:

а) ключ проверки электронной подписи головного УЦ известен каждому юридическому и физическому лицу;

б) сертификат ключа проверки электронной подписи какого-либо юридического или физического лица может быть проверен на действительность с помощью проверки цепочки сертификатов, ведущей обратно к головному УЦ.

Далее приведен пример проверки цепочки сертификатов для иерархической системы УЦ

П р и м е р :
Алиса
- проверяет сертификат ключа проверки электронной подписи Боба, выданный УЦ4; затем
- сертификат ключа проверки электронной подписи УЦ4, выданный УЦ2; а затем
- сертификат ключа проверки электронной подписи т УЦ2, выданный головным УЦ1, ключ проверки электронной подписи которого она знает.

Проверка цепочки сертификатов осуществляется только в направлении от головного УЦ к владельцу проверяемого сертификата и проверки цепочки сертификатов в обратном направлении (от владельца проверяемого сертификата к головному УЦ) не требуется.

Б.3 Сетевая система УЦ

В сетевой системе УЦ независимые УЦ кросс-сертифицируют друг друга (т. е. выдают сертификаты друг другу), результатом этого является общая сеть доверительных отношений между УЦ. На рисунке Б.2 показана сетевая система УЦ. Некое юридическое или физическое лицо доверяет ключу проверки электронной подписи, как правило, того УЦ, который выдал ему сертификат ключа проверки электронной подписи и проверяет сертификаты других юридических или физических лиц посредством проверки сертификатов в цепочке сертификатов, которая ведет обратно к этому УЦ.

Пример:
– Алиса знает ключ проверки электронной подписи УЦ3, и
– Боб знает ключ проверки электронной подписи УЦ4.
Существует несколько цепочек сертификатов, ведущих от Боба к Алисе, но Алисе нужна кратчайшая, чтобы подтвердить:
– сертификат ключа проверки электронной подписи Боба, выданный УЦ4, затем
– сертификат ключа проверки электронной подписи УЦ4, выданный УЦ5 и, наконец
– сертификат ключа проверки электронной подписи УЦ5, выданный УЦ3.
УЦ3 является УЦ Алисы, она доверяет УЦ3 и знает его ключ проверки электронной подписи.

Б.4 Смешанная система УЦ

Смешанная система УЦ включает в себя характеристики как иерархической, так и сетевой системы УЦ. Основной конструктивный блок представляет собой иерархию, которая включает головные УЦ, подчиненные УЦ и конечных владельцев сертификатов. Головные УЦ создают сертификаты ключей проверки электронной подписи подчиненным УЦ и осуществляют кросс-сертификацию с другими головными УЦ. Каждому УЦ, не являющемуся головным УЦ, соответствует цепочка сертификатов, направленная к головному УЦ. Таким образом, образуется иерархическая цепочка сертификатов, проходящую от головного УЦ к своим подчиненным УЦ, и от каждого из этих УЦ к их соответствующим подчиненным УЦ.

Пары кросс-сертификатов ключей проверки электронной подписи подобны сертификатам ключей проверки электронной подписи, иерархически соединяющим УЦ с головным УЦ. Эти сравнимые пары кросс-сертификатов ключей проверки электронной подписи, показанные на рисунке Б.3 двусторонними стрелками, позволяют бизнес-приложениям осуществляющим проверку цепочки сертификатов от проверяемого «родительского» (головного) УЦ, использующего пары кросс-сертификатов ключей проверки электронной подписи, вести работу с любым УЦ.

Это делает возможным осуществление кросс-сертификации с другими областями не только на верхнем (головной УЦ) уровне, но и среди подчиненных УЦ.

В смешанной системе УЦ определяют три вида кросс-сертификатов ключей проверки электронной подписи: иерархический, общий и специальный.

Иерархические кросс-сертификаты ключей проверки электронной подписи подобны иерархической цепочке сертификатов, направленной к головному УЦ. Они обеспечивают уверенность в том, что пользователи сертификатов, которые доверяют своему локальному УЦ (в отличие от головного УЦ), всегда могут найти цепочку сертификатов к любому другому юридическому или физическому лицу в системе УЦ.

Общие кросс-сертификаты ключей проверки электронной подписи дополняют иерархию создания сертификатов ключей проверки электронной подписи и делают возможными более короткие цепочки сертификатов. Правила, касающиеся использования общих кросс-сертификатов ключей проверки электронной подписи, позволяют распространить доверие с таким же ограничением, как и распространение доверия при использовании наименее ограниченной цепочки сертификатов от головного УЦ пользователя сертификата к проверяемому на действительность сертификату ключа проверки электронной подписи.

Специальные кросс-сертификаты ключей проверки электронной подписи обеспечивают цепочки сертификатов, которые могут не соответствовать ограничениям, предписываемым иерархически по цепочке из головных УЦ. Специальные кросс-сертификаты ключей проверки электронной подписи могут быть созданы между «листовыми» УЦ. Листовыми являются УЦ, которые имеют иерархическую цепочку сертификатов, направленную к головному УЦ, длина которой ограниченна «0». Это делает возможным дальнейшее распространение доверия к другим УЦ по иерархической цепочке сертификатов. Специальные кросс-сертификаты ключей проверки электронной подписи адекватны тогда, когда каждый из двух УЦ действует в соответствии с политиками применения сертификатов, делающими возможным более высокий уровень доверия или меньшие ограничения, чем те, которые были бы позволены в любом другом случае.

На рисунке Б.3 Алиса показана в иерархии, не являющейся иерархией Боба в рамках системы УЦ. Если Алиса пожелает подтвердить подпись Боба, она может сделать свой выбор из целого ряда цепочек сертификатов, чтобы установить доверие к своему непосредственному УЦ (УЦ3) или к своему головному УЦ (УЦ1). В процессе подтверждения подлинности цепочки сертификатов клиента Алисы отыскивается, по крайней мере, одна цепочка сертификатов, соответствующая политике применения сертификатов или другим критериям, которые требуются Алисе для проверки сертификата ключа проверки электронной подписи Боба.

Приложение В
(справочное)

Рекомендации по принятию данных запроса на сертификат ключа проверки электронной подписи

В.1 Общая информация

Это приложение содержит рекомендации по принятию данных запроса на сертификат от физического или юридического лица в различных ситуациях. Рекомендации носят общий характер и предназначены, чтобы показать, что уровень усилий, необходимых для принятия данных запроса, должен быть пропорционален риску, связанному с принятием недействительного запроса на создание сертификата ключа проверки электронной подписи (например, если лицо, запрашивающее сертификат ключа проверки электронной подписи, представило сфальсифицированные документы, удостоверяющие личность). Фактические требования будут определяться политикой безопасности УЦ и политикой безопасности бизнес-приложений.

Эта процедура не препятствует УЦ использовать ЦР для проверки идентификационных данных юридического или физического лица, обратившегося в УЦ, на основе его личного присутствия или представления идентификационных полномочий (доверенности от него).

Требования, представленные в настоящем приложении, являются только одним из факторов, определяющим, насколько следует доверять сертификатам ключей проверки электронной подписи, выданным УЦ. Другие факторы включают операционную политику, процедуры, а также меры и средства контроля и управления безопасностью УЦ, политику конечного владельца сертификата и процедуры для работы с ключами электронной подписи и т. д. Ответственность, которую берут на себя УЦ, выдающие сертификаты ключей проверки электронной подписи, и конечные владельцы сертификатов, также играет определенную роль в степени доверия. Сертификат ключа проверки электронной подписи может содержать политики применения сертификатов; это позволяет пользователю сертификата решить, насколько можно доверять связыванию идентификационных данных юридического или физического лица с его ключом проверки электронной подписи. Как правило, конкретные политики и механизмы безопасности, которые реализуют их, определяются в документе с детальными инструкциями, который обычно именуется как «Регламент выдачи сертификатов ключей проверки электронной подписи».

В.2 Принятие данных запроса на сертификат ключа проверки электронной подписи от физического лица

В.2.1 Для бизнес-приложений с низкой степенью риска

Пример – Розничные банковские кредитные карточки и торговые терминалы.

Принятие данных запроса на сертификат должно быть основано на идентификации физического лица, подающего заявку на сертификат ключа проверки электронной подписи. Что касается бизнес-приложений с низкой степенью риска, данные запроса на сертификат необязательно должны быть представлены лично. Средство для идентификации физического лица должно соответствовать традиционным деловым практикам.

В.2.2 Для бизнес-приложений со средней степенью риска

Пример – Недорогие/небольшого объема бизнес-приложения по электронному обмену данными или персональные системы по управлению активами.

Принятие данных запроса на сертификат должно быть основано на одном или нескольких механизмах идентификации физического лица, подающего заявку на сертификат ключа проверки электронной подписи. Эти методы могут значительно отличаться в зависимости от того, представлена ли заявка лично и представлена ли от имени личности с применением традиционных деловых практик для идентификации физического лица. Механизмы, которые могут быть использованы, в совокупности включают:

- использование и подтверждение действительного идентификатора и пароля пользователя;
- процедуры повторного вызова;
- коды аутентификации сообщений (MAC);
- электронные карты или жетоны с микросхемами.

В.2.3 Для бизнес-приложений с высокой степенью риска

Пример – Частная банковская система.

Принятие данных запроса на сертификат должно быть основано на личном присутствии физического лица (или уполномоченного лица), подающего заявку на сертификат ключа проверки электронной подписи, и использовании традиционных деловых практик для идентификации физического лица (или, если это требуется, уполномоченного указанного физического лица). Это может включать проверку личности физического лица

(доверенного юридического или физического лица), например, инспектором по банковским счетам или юридической фирмой, утвержденной финансовым учреждением.

В.3 Принятие данных запроса на сертификат ключа проверки электронной подписи от юридического лица

В.3.1 Для одноуровневого финансового учреждения

Пример – Клиринговые расчетные палаты (например, CHIPS[1], CHAPS[2]) и системы автоматизированных расчетов центральных банков.

Принятие данных запроса на сертификат должно быть основано на личной доставке данных запроса на сертификат представителем юридического лица, и на:

- сопроводительном письме на фирменном бланке с подписью и печатью (при необходимости) старшего должностного лица юридического или физического лица, уполномоченного подать заявку на сертификат ключа проверки электронной подписи;
- средстве идентификации представителя, доставившего данные запроса на сертификат, которое соответствует традиционным деловым практикам.

В.3.2 Для бизнес-клиентов финансового учреждения

Принятие данных запроса на сертификат должно быть основано на личной доставке данных запроса на сертификат двумя или несколькими представителями юридического лица, и на:

- заявке на сертификат ключа проверки электронной подписи на фирменном бланке, заверенной подписью и печатью (при необходимости);
- использование традиционных деловых практик для идентификации подписи и печати (при необходимости) физического лица;
- средстве идентификации представителя, доставившего данные запроса на сертификат, которое соответствует традиционным деловым практикам.

---

[1] CHIPS (The Clearing House Interbank Payments System) – частная электронная система денежных переводов в США.

[2] CHAPS (The Clearing House Automated Payment System) – система клиринговых расчётов в Великобритании.

Приложение Г
(справочное)

Методы, применяемые УЦ для восстановления своей деятельности после потери или компрометации ключа электронной подписи УЦ

Г.1 Общая информация

Потеря или компрометация ключа электронной подписи УЦ рассматривается как чрезвычайное происшествие, так как сертификаты ключей проверки электронной подписи, подписанные с помощью этого ключа электронной подписи, вызывают сомнение в их истинности. Надлежащее восстановление деятельности УЦ после подобного чрезвычайного происшествия (бедствия) включает прекращение действия и переоформление всех сертификатов ключей проверки электронной подписи, которые были подписаны с помощью ключа электронной подписи УЦ.

Для переоформления сертификатов ключей проверки электронной подписи УЦ может использовать методы с применением двух пар ключей проверки электронной подписи, т. е. пары первичных ключей (ключ проверки электронной подписи P^1, ключ электронной подписи S^1) и пары вторичных ключей (P^2, S^2), например:

- уведомление с помощью пары вторичных ключей УЦ (CAC, подписанный с помощью вторичного ключа);
- переоформление сертификатов с помощью пары вторичных ключей УЦ;
- переоформление сертификатов ключей проверки электронной подписи с помощью пары новых первичных ключей УЦ;
- уведомление с помощью множества подписанных сертификатов ключей проверки электронной подписи.

Указанные методы рассматриваются в Г.2 - Г.5 с использованием следующей нотации:

- **$P=>E_p$**: для данного сертификата ключа проверки электронной подписи УЦ<<E>>, ключ проверки электронной подписи E_p проверяется на действительность ключом проверки электронной подписи P, принадлежащим УЦ. Следовательно, для УЦ<<E>>, P дает E_p;
- **$P^1=>E_p$**: Ключ проверки электронной подписи E проверяется на действительность первичным ключом проверки электронной подписи УЦ;
- **P^2=>Ep**: Ключ проверки электронной подписи E проверяется на действительность вторичным ключом проверки электронной подписи УЦ;
- **S^1<<E>>**: Первичный сертификат ключа проверки электронной подписи E подписывается с использованием первичного ключа электронной подписи УЦ;
- **S^2<<E>>**: Вторичный сертификат ключа проверки электронной подписи E подписывается с использованием вторичного ключа электронной подписи УЦ.

Примечание – Нотация, используемая в настоящем стандарте, является вариантом нотации X.509 [3] для сертификатов ключей проверки электронной подписи, цепочки сертификатов и взаимосвязанной информации.

Г.2 Уведомление с помощью пары вторичных ключей УЦ

Когда новый конечный владелец сертификатов (E) представляет свой ключ проверки электронной подписи (E_p) УЦ, УЦ формирует первичный сертификат ключа проверки электронной подписи $УЦ^1$<<E>>, подписанный с помощью первичного ключа электронной подписи УЦ, и вторичный сертификат ключа проверки электронной подписи $УЦ^2$<<E>>, подписанный с помощью вторичного ключа электронной подписи УЦ. До восстановления деятельности УЦ после бедствия пользователи сертификатов имеют оба сертификата ключа проверки электронной подписи и оба ключа проверки электронной подписи УЦ, но используют только первичный ключ УЦ для проверки первичного сертификата ключа проверки электронной подписи.

До восстановления деятельности УЦ после бедствия: $УЦ^1$<<E>>, $P^1=>E_p$ и $УЦ^2$<<E>>, P^2.

После восстановления деятельности УЦ после бедствия: $УЦ^1$<<E>>, P^1 и $УЦ^2$<<E>>, $P^2=>E_p$.

В тех случаях, когда первичный ключ электронной подписи УЦ скомпрометирован, восстановление деятельности УЦ после бедствия заключается в прекращении действия всех сертификатов ключей проверки электронной подписи, подписанных с помощью первичного ключа электронной подписи, и в уведомлении конечных владельцев сертификатов о переключении на вторичный сертификат ключа проверки электронной подписи. После восстановления деятельности УЦ после бедствия каждое юридическое или физическое лицо, обращающееся в УЦ, подтверждает действительность вторичных сертификатов ключей проверки электронной подписи конечных владельцев сертификатов, используя вторичный ключ проверки электронной подписи УЦ.

Данный метод восстановления деятельности УЦ может быть выполнен только единожды.

Разновидность этого метода используется, когда сертификаты ключей проверки электронной подписи распределяются через централизованную службу. В этом случае УЦ удаляет все недействительные первичные сертификаты ключей проверки электронной подписи и уведомляет конечных владельцев сертификатов о необходимости использования существующих вторичных сертификатов, которые по-прежнему остаются

действительными.

Г.3 Переоформление с помощью пары вторичных ключей УЦ

Когда новый конечный владелец сертификата (Е) представляет свой ключ проверки электронной подписи (E_p) УЦ, УЦ формирует сертификат ключа проверки электронной подписи $УЦ^1$<<Е>>, подписанный с помощью первичного ключа электронной подписи УЦ. До восстановления деятельности УЦ после бедствия пользователи сертификатов имеют только первичные сертификаты ключей проверки электронной подписи и оба ключа проверки электронной подписи УЦ, но используют только первичный ключ УЦ для проверки первичного сертификата ключа проверки электронной подписи.

До восстановления деятельности УЦ после бедствия: $УЦ^1$<<Е>>, P^1=>E_p и P^2.

После восстановления деятельности УЦ после бедствия: $УЦ^1$<<Е>>, P^1 и $УЦ^2$<<Е>>, P^2=>E_p.

В тех случаях, когда первичный ключ электронной подписи УЦ скомпрометирован, восстановление деятельности УЦ после бедствия заключается в прекращении действия всех первичных сертификатов ключей проверки электронной подписи и переоформлении вторичных сертификатов ключей проверки электронной подписи. После восстановления деятельности УЦ после бедствия каждый проверяющий подтверждает действительность вторичных сертификатов ключей проверки электронной подписи конечных владельцев сертификатов, используя вторичный ключ проверки электронной подписи УЦ.

Данный метод восстановления деятельности УЦ может быть выполнен только единожды.

Разновидность этого метода используется для централизованных служб распределения. В этом случае УЦ заменяет все недействительные первичные сертификаты ключей проверки электронной подписи новыми действительными вторичными сертификатами ключей проверки электронной подписи и уведомляет конечных владельцев сертификатов о необходимости использовать новые сертификаты ключей проверки электронной подписи.

Г.4 Переоформление с помощью новой пары первичных ключей УЦ

Когда новый конечный владелец сертификата (Е) представляет УЦ свой ключ проверки электронной подписи (E_p), УЦ формирует сертификат ключа проверки электронной подписи $УЦ^1$<<Е>>, подписанный с помощью первичного ключа электронной подписи УЦ. До восстановления деятельности УЦ после бедствия пользователи сертификатов имеют только первичные сертификаты ключей проверки электронной подписи и оба ключа проверки электронной подписи УЦ, но используют только первичный ключ УЦ для проверки первичного сертификата ключа проверки электронной подписи.

До восстановления деятельности УЦ после бедствия: $УЦ^1$<<Е>>, P^1=>E_p и P^2.

Во время восстановления деятельности УЦ после бедствия: $УЦ^1$<<Е>>, P^1 и $УЦ^2$<<P^3>>, P^2=>P^3.

После восстановления деятельности УЦ после бедствия: $УЦ^3$<<Е>>, P^3=>E_p и $УЦ^2$<<P^3>>, P^2=>P^3.

В тех случаях, когда первичный ключ электронной подписи УЦ скомпрометирован, восстановление деятельности УЦ после бедствия заключается в прекращении действия всех сертификатов ключей проверки электронной подписи, подписанных с помощью первичного ключа электронной подписи. Во время восстановления деятельности УЦ после бедствия УЦ создает новую пару первичных ключей проверки электронной подписи (P^3, S^3) и выдает новый сертификат ключа проверки электронной подписи $УЦ^2$<<P_3>> своего нового первичного ключа проверки электронной подписи (P^3), подписанный с помощью вторичного ключа электронной подписи УЦ (S^2). Каждое юридическое или физическое лицо, обращающееся в УЦ, подтверждает действительность нового сертификата ключа проверки электронной подписи УЦ, используя вторичный ключ проверки электронной подписи УЦ. Восстановление деятельности УЦ после бедствия завершается повторной выдачей сертификатов ключей проверки электронной подписи УЦ, подписанных с помощью нового первичного ключа электронной подписи УЦ. После восстановления деятельности УЦ после бедствия каждый конечный владелец сертификатов подтверждает действительность новых сертификатов ключей проверки электронной подписи конечных владельцев сертификатов, используя новый первичный ключ проверки электронной подписи УЦ.

Данный метод восстановления деятельности УЦ является повторяемым.

Разновидность этого метода используется, когда сертификаты ключей проверки электронной подписи распределяются не через централизованную службу. В этом случае УЦ добавляет свой собственный новый сертификат ключа проверки электронной подписи, заменяет все недействительные сертификаты ключей проверки электронной подписи конечных владельцев сертификатов новыми действительными сертификатами ключей проверки электронной подписи и уведомляет конечных владельцев сертификатов о необходимости проверить новый сертификат ключа проверки электронной подписи УЦ и начать использовать новые сертификаты ключей проверки электронной подписи конечных владельцев сертификатов.

Г.5 Переоформление с помощью очередной пары ключей УЦ

Когда новый конечный владелец сертификата (Е) представляет УЦ свой ключ проверки электронной подписи (E_p), УЦ формирует сертификат ключа проверки электронной подписи конечного владельца сертификата $УЦ^1$<<Е>>, подписанный с помощью первичного ключа электронной подписи УЦ. УЦ не распределяет свой вторичный ключ проверки электронной подписи, но его хэш содержится в самоподписанном сертификате его первичного ключа проверки электронной подписи, т. е. $УЦ^1$<<P^1, хэш(P^2)>>. До восстановления деятельности УЦ после бедствия пользователи сертификатов имеют только первичные сертификаты ключей проверки

электронной подписи конечных владельцев сертификатов и первичный сертификат ключа проверки электронной подписи УЦ, и используют первичный ключ УЦ для проверки первичного сертификата ключа проверки электронной подписи конечного владельца сертификата.

До восстановления деятельности УЦ после бедствия: УЦ^1<<E>>, P^1=>E_p и УЦ^1<<P^1, хэш(P^2)>>.

Во время восстановления деятельности УЦ после бедствия: УЦ^1<<E>>, P^1 и (P^1, хэш(P^2)) =>P^2.

После восстановления деятельности УЦ после бедствия: УЦ^2<<E>>, P^2=>E_p и УЦ^2<<P^2, хэш(P^3)>>.

В тех случаях, когда первичный ключ электронной подписи УЦ скомпрометирован, восстановление деятельности УЦ после бедствия сначала заключается в прекращении действия всех первичных сертификатов ключей проверки электронной подписи, а также в распределении вторичного ключа проверки электронной подписи УЦ. Вторичный ключ проверки электронной подписи УЦ распределяется в самоподписанном сертификате ключа проверки электронной подписи УЦ^2<<P^2, хэш (P^3)>>, который также содержит хэш своего следующего ключа проверки электронной подписи – третичный ключ проверки электронной подписи УЦ. Юридическое или физическое лицо, обращающееся в УЦ, подтверждает действительность нового сертификата ключа проверки электронной подписи удостоверяющего центра путем проверки самоподписанного сертификата и путем проверки того, что хэш ключа проверки электронной подписи P^2 действительно идентичен хэшу, содержащемуся в первичном сертификате ключа проверки электронной подписи удостоверяющего центра УЦ^1<<P^1, хэш(P^2)>>.

Восстановление деятельности УЦ после бедствия завершается повторной выдачей УЦ вторичных сертификатов ключей проверки электронной подписи конечных владельцев сертификатов. После восстановления деятельности УЦ после бедствия каждый конечный владелец сертификата подтверждает действительность новых сертификатов ключей проверки электронной подписи, используя новый ключ проверки электронной подписи УЦ.

Данный метод восстановления деятельности УЦ является повторяемым, и сертификаты ключей проверки электронной подписи конечных владельцев сертификатов, сформированные с помощью «будущих» ключей УЦ, могли бы быть, при необходимости, распределены, прежде чем будущий ключ УЦ станет «действующим» ключом УЦ.

Приложение Д
(справочное)

Распределение сертификатов ключей проверки электронной подписи и CAC

Д.1 Общая информация

В этом приложении обсуждаются механизмы распределения сертификатов ключей проверки электронной подписи юридическим или физическим лицам, которые не являются владельцем сертификата, и механизмы распределения CAC. Распределение CAC может осуществляться с помощью электронных средств или носителей информации, например, CD-ROM или печатных листов.

Д.2 Распространение сертификатов ключей проверки электронной подписи

Если юридическое или физическое лицо имеет несколько сертификатов ключей проверки электронной подписи, то в структуре подписи (или в подписываемых данных) желательно указать, какой сертификат ключа проверки электронной подписи должен быть использован для проверки подписи. По подписанному сообщению могут быть определены регистрационный номер сертификата ключа проверки электронной подписи и выдавший его УЦ. В случае с сертификатом ключа проверки электронной подписи, подписанным УЦ с несколькими сертификатами ключей проверки электронной подписи, пользователь сертификатов использует сертификат ключа проверки электронной подписи, поле **subjectUniqueIdentifier** которого совпадает с полем **issuerUniqueIdentifier** сертификата ключа проверки электронной подписи, подлежащего проверке.

Для транзакций, которые необходимо подписывать, существует ряд альтернатив по распространению сертификата ключа проверки электронной подписи, например:

- передача сертификата ключа проверки электронной подписи (или цепочки сертификатов) имеющего отношение к транзакции;
- передача указателя на сертификат ключа проверки электронной подписи, необходимого для проверки подписи, имеющего отношение к транзакции, например:
  - имя подписавшего (и, возможно, уникальный идентификатор подписавшего); или
  - регистрационный номер сертификата и УЦ, выдавший его.

Сертификаты ключа проверки электронной подписи, не переданные при транзакции, могут быть получены из справочника сертификатов соответствующего УЦ или с аналогичного сервера.

Д.3 Распространение CAC

CAC могут быть предоставлены владельцам и пользователям сертификатов. К механизмам распространения относятся следующие:

- сообщение от криптографической службы, содержащее CAC;
- включение в заголовок сообщения, как в случае с сертификатами ключей проверки электронной подписи;
- запрос юридическим или физическим лицом CAC УЦ или единичной записи. В этом случае ответ подписывается УЦ, обслуживающим данный CAC, для предотвращения отказа в обслуживании путем имитации недействительности сертификата ключа проверки электронной подписи. Запросы будут направляться к справочнику сертификатов соответствующего УЦ или аналогичному хорошо известному серверу;
- передача единичной записи CAC (подписанной УЦ). Этот механизм будет использоваться для обеспечения уведомления о прекращении действия «в реальном времени», тогда как весь CAC будет отправлен на плановой основе в соответствии со временем следующего обновления. Возможна отправка нового (внепланового) CAC полностью, когда действие сертификата ключа проверки электронной подписи прекращено.

Код причины может быть использован для определения того, распространять или не распространять уведомление о прекращении действия сертификата до **nextUpdate** (см. 5.3.8). Кроме того, несколько CAC с различной частотой обновления могут поддерживаться на основе **reasonCode**.

Библиография

[1] Федеральный закон от 6 апреля 2011г. №63-ФЗ «Об электронной подписи»

[2] Приказ Федеральной службы безопасности Российской Федерации от 27 декабря 2011 г. № 796, г. Москва «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра»

[3] Рекомендация МСЭ-Т X.509 (ITU-T Recommendation X.509) Информационные технологии. Взаимосвязь открытых систем. Справочник: Структуры сертификатов открытых ключей и атрибутов. 2008 (Information technology - Open systems interconnection - The Directory: Public-key and attribute certificate frameworks. 2008) http://www.itu.int/rec/T-REC-X.509-200811-i

УДК 681.3.06:006.354 ОКС 35.240.40

Ключевые слова: инфраструктура ключей проверки электронной подписи, сертификат ключа проверки электронной подписи, управление сертификатами, удостоверяющий центр, цепочка сертификатов, формирование сертификата, прекращение действия сертификата, продление сертификата, замена сертификата, управление ключами, ключ проверки электронной подписи, ключ электронной подписи

Подписано в печать 01.08.2014. Формат 60x84 1/8.
Усл. печ. л. 4,65. Тираж 40 экз. Зак. 2868.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ФГУП «СТАНДАРТИНФОРМ»

123995 Москва, Гранатный пер., 4.
www.gostinfo.ru info@gostinfo.ru