ВЕСТНИК ВОЕННОГО ИННОВАЦИОННОГО ТЕХНОПОЛИСА «ЭРА», 2023, том 4, № 4, с. 383–386

ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

УДК 004.738.2

ИССЛЕДОВАНИЕ ВОЗМОЖНОСТИ ПЕРЕДАЧИ УПРАВЛЕНИЯ СЕРТИФИКАТАМИ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ МЕЖДУ УДОСТОВЕРЯЮЩИМИ ЦЕНТРАМИ ПРИ ОРГАНИЗАЦИИ ИЕРАРХИЧЕСКОЙ И СЕТЕВОЙ (ОДНОРАНГОВОЙ) МОДЕЛЕЙ ИНФРАСТРУКТУРЫ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ ПРИ ВЫХОДЕ ИЗ СТРОЯ ОДНОГО ИЗ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ

© 2023 г. Е. О. Шмаков[1], М. И. Заховаев[1], В. А. Щербаков[1], Д. В. Леонов[1,*], Д. В. Харланов[1]

[1]Краснодарское высшее военное училище имени генерала армии С.М. Штеменко, Краснодар, Россия

*****E-mail: ragecountry@mail.ru*

Поступила в редакцию 20.11.2023 г.
После доработки 20.11.2023 г.
Принята к публикации 26.11.2023 г.

Исследована возможность реализации передачи управления сертификатами ключей проверки электронной подписи между удостоверяющими центрами при выходе из строя одного из удостоверяющих центров. Рассмотрены преимущества и недостатки иерархической и сетевой (одноранговой) моделей инфраструктуры управления между удостоверяющими центрами, а также проведен анализ нормативно-правовой базы, связанной с вопросами порядка и условий передачи управления между удостоверяющими центрами. На основе проведенного анализа выделены недостатки в нормативно-правовой базе, которые отрицательно сказываются на скорости передачи управления между удостоверяющими центрами при прекращении работы одного из них.

DOI: 10.56304/S2782375X23040137

ВВЕДЕНИЕ

В соответствии с планом мероприятий по переходу организаций на безбумажный электронный документооборот проводится работа по внедрению и модернизации системы электронной подписи в автоматизированной информационной системе электронного документооборота и дальнейшей ее интеграции с создаваемой в Российской Федерации системой межведомственного электронного взаимодействия. Основной компонент системы электронной подписи – удостоверяющий центр (**УЦ**), задачами которого являются предоставление пользователям удостоверяющего центра услуг, связанных с применением электронных подписей в соответствии с законодательством Российской Федерации (создание и выдача ключей электронной подписи и ключей проверки электронной подписи должностным лицам МО РФ и т.д.).

В связи с этим для увеличения отказоустойчивости системы УЦ рассмотрим возможность передачи управления сертификатами ключей проверки электронной подписи между удостоверяющими центрами при выходе из строя одного из них, используя сетевые и иерархические модели организации их инфраструктуры.

МОДЕЛИ ИНФРАСТРУКТУРЫ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ

Для определения преимуществ и недостатков моделей инфраструктуры удостоверяющих центров нужно провести исследование таких моделей построения, как иерархическая и сетевая (одноранговая).

Перед тем как приступить к подробному рассмотрению моделей инфраструктуры УЦ, была проанализирована нормативно-правовая база и выявлены следующие проблемы.

В соответствии со статьей 15, п. 4 Федерального закона от 06.04.2011 г. № 63-ФЗ (ред. от 02.07.2021 г.) “Об электронной подписи”, в случае принятия решения о прекращении своей деятельности аккредитованный удостоверяющий центр обязан:

– сообщить об этом в уполномоченный федеральный орган не позднее чем за один месяц до даты прекращения своей деятельности;

– передать в уполномоченный федеральный орган в установленном порядке реестр выданных этим аккредитованным удостоверяющим центром квалифицированных сертификатов;

– передать на хранение в уполномоченный федеральный орган в установленном порядке информацию, подлежащую хранению в аккредитованном удостоверяющем центре. Ключи электронной подписи, хранимые аккредитованным удостоверяющим центром по поручению владельцев квалифицированных сертификатов электронной подписи, подлежат уничтожению в порядке, установленном федеральным органом исполнительной власти в области обеспечения безопасности.

В случае прекращения деятельности удостоверяющего центра с переходом его функций другим лицам он должен уведомить об этом в письменной форме владельцев сертификатов ключей проверки электронных подписей, которые выданы этим удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана лицу, к которому перешли функции удостоверяющего центра, прекратившего свою деятельность [1].

В случае прекращения деятельности УЦ с переходом его функций к другим воинским частям он должен уведомить об этом в письменной форме владельцев сертификатов, которые выданы удостоверяющим центром и срок действия которых не истек, не менее чем за один месяц до даты передачи своих функций. В указанном случае после завершения деятельности удостоверяющего центра информация, внесенная в реестр сертификатов, должна быть передана воинской части, к которой перешли функции удостоверяющего центра [2].

Вместе с передачей управления сертификатами ключей проверки электронной подписи пользователей удостоверяющего центра необходимо осуществить передачу сертификатов служб удостоверяющего центра TSA/OCSP. При этом требуется обеспечить санкционированные возможности удостоверяющего центра, которому передается управление, отзывать действующие сертификаты ключей проверки электронной подписи, изготовленные удостоверяющим центром, передающим управление; обеспечить санкционированную возможность удостоверяющего центра, которому передается управление, выпускать списки отозванных сертификатов, содержащие сертификаты ключей проверки электронной подписи, изготовленные удостоверяющим центром, передающим управление; обеспечить возможность доверия пользователей удостоверяющего центра, передающего управление, к спискам отозванных сертификатов, выпускаемых удостоверяющим центром, которому передается управление.

ИЕРАРХИЧЕСКАЯ АРХИТЕКТУРА

Удостоверяющие центры организуются иерархически под управлением так называемого корневого удостоверяющего центра, который выпускает самоподписанный сертификат и сертификаты для подчиненных удостоверяющих центров. Подчиненные удостоверяющие центры могут выпускать сертификаты для удостоверяющих центров, находящихся ниже них по уровню иерархии, или для пользователей. Другими словами, головной центр распределяет свои полномочия по нижестоящим УЦ в иерархии. В иерархической модели каждая доверяющая сторона знает открытый ключ подписи корневого УЦ.

Любой сертификат может быть проверен путем выстраивания цепочки сертификатов от корневого удостоверяющего центра и ее верификации, т.е. проверки связанности субъекта сертификата и его открытого ключа [3].

При выходе из строя головного удостоверяющего центра, заранее считая, что сертификат ключа проверки электронной подписи не скомпрометирован, полномочия и управление передаются УЦ 2. При выходе из строя УЦ 2 и головного УЦ управление сертификатами переходит УЦ 3. Но для качественного управления УЦ, идущими ниже по иерархии, все удостоверяющие центры, стоящие выше, должны иметь средства передачи данных в нижестоящие центры. Чтобы остальные УЦ знали о состоянии работоспособности других УЦ, должен существовать механизм проверки. Если все УЦ работают в штатном режиме, данные средства передачи информации не используются [3].

СЕТЕВАЯ АРХИТЕКТУРА

Сетевая модель (децентрализованная, распределенная модель) реализует альтернативный подход к формированию отношений доверия. Модель строится путем установления доверительных отношений между равноправными УЦ. При этом отношения могут быть односторонними или двусторонними. “Якорем” доверия в данном случае является локальный УЦ. Таких “якорей” доверия может быть много в зависимости от числа участвующих УЦ. Особенностью данной модели является то, что отношения доверия строятся, как правило, посредством перехода через границы областей доверия. Поэтому сертификаты, выпущенные для этих целей, называются кросс-сертификатами и имеют специальный вид. В составе кросс-сертификата по сравнению с обычным сертификатом присутствует информация преобразования политик безопасности. Удобство сете-

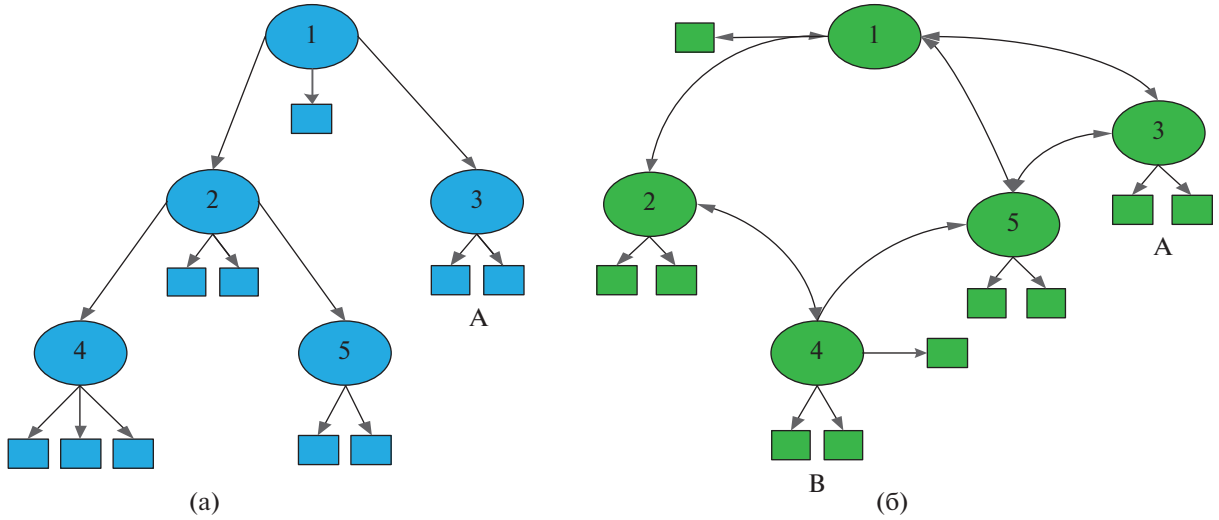

Рис. 1. Традиционные архитектуры PKI: а – иерархическая, б – сетевая. Окружностями с номерами обозначены удостоверяющие центры; квадратами – конечные пользователи.

вой модели заключается в том, что в результате кросс-сертификации на уровне корневых УЦ исчезает необходимость распространения корневого самоподписанного сертификата одной организации среди пользователей другой [4].

Данная модель имеет более гибкую систему передачи управления между удостоверяющими центрами. Например, если рассмотрим рис. 1б, то отправитель сообщения А знает открытый ключ подписи УЦ 3, в то время как получателю сообщения В известен открытый ключ УЦ 4. Существует несколько цепочек сертификатов. Самая короткая цепочка – отправитель сообщения проверяет сертификат получателя, выпущенный УЦ 4, затем сертификат УЦ 4, выпущенный УЦ 5, и, наконец, сертификат УЦ 5, выпущенный УЦ 3. УЦ 3 – это удостоверяющий центр, которому доверяет отправитель и знает его открытый ключ. Но если УЦ 5 уничтожен, то остается путь через УЦ 2, затем УЦ 1 и к конечному получателю УЦ 3.

В случае уничтожения более одного УЦ увеличивается вероятность потери связи остальных УЦ между собой. Например, если уничтожены УЦ 2 и УЦ 5, то связь с УЦ 4 будет потеряна для остальных УЦ. Для увеличения отказоустойчивости сетевой модели инфраструктуры необходимо увеличивать количество УЦ, но слишком большое количество УЦ окажет и обратный эффект, понизив тем сам надежность данной системы передачи управления.

Существует еще так называемая “гибридная” или мостовая модель доверия между УЦ. Она представляет объединение иерархической и сетевой моделей, но по своей сути больше относится к сетевой модели, так как основная ее структура за основу берет кросс-сертификацию с последующим расслоением дочерних УЦ по иерархии. Несмотря на то что все УЦ могут быть в тех или иных доменах доверия либо полностью доверять друг другу, всегда на уровне регламентов УЦ вводятся те или иные ограничения на сертификаты, такие как ограничения на имя сертификата, на количество звеньев в цепочке доверия, на использование в различных доменах доверия и т.п. [4].

Удостоверяющие центры поддерживают ряд дополнительных протоколов, которые дают возможность получать подробную информацию о цифровых сертификатах. Примерами таких протоколов являются протоколы OCSP и TSP. Рассмотрим их возможности более подробно.

ПРОТОКОЛ OCSP И TSP (TSA)

Online Certificate Status Protocol (**OCSP**) – протокол получения статуса сертификата в реальном времени применяется для предоставления пользователям УЦ актуальной информации о статусах сертификатов ключей подписи. По протоколу OCSP можно получить информацию об изменении статуса цифрового сертификата в реальном времени. Протокол OCSP необходим при работе с важной информацией.

Протокол OCSP работает по принципу “запрос–ответ”. OCSP-клиент генерирует OCSP-запрос и отправляет его на сервер. OCSP-сервер получает этот запрос, проверяет статус сертификата, генерирует OCSP-ответ и отсылает его клиенту. Рассмотрим подробнее структуру OCSP-запросов и ответов.

OCSP-запрос состоит из номера версии протокола, типа запроса на обслуживание и одного или нескольких идентификаторов сертификатов.

Идентификатор сертификата включает в себя хэш-коды отличительного имени и открытого ключа издателя сертификата, а также серийный номер сертификата. В запросе иногда могут присутствовать необязательные дополнения.

OCSP-ответ состоит из идентификатора сертификата, статуса сертификата (“нормальный”, “аннулированный” или “неизвестный”) и срока действия ответа, связанного с идентификатором каждого указанного в исходном запросе сертификата. Если сертификат имеет статус аннулированного, то отображается время аннулирования и может быть указана причина аннулирования (необязательно). Срок действия задается интервалом от текущего обновления до следующего обновления. Ответ может содержать необязательные дополнения, а также код ошибки, если обработка запроса не была завершена корректно.

Time-Stamping Protocol (**TSP**) – протокол представляет собой набор методов, позволяющих установить, является ли электронный документ созданным или подписанным в (или раньше) определенное время. На практике в большинстве случаев системы с метками времени используют в качестве доверенной третьей стороны – Time-Stamping Authority (**TSA**). TSA является доверенной третьей стороной, которая создает временную метку для того, чтобы указать, что данный документ существовал в определенный момент времени. Для того чтобы связать документ с конкретным моментом времени, должен быть использован сервис TSA.

Это может быть использовано, например, для проверки цифровой подписи, которая была применена к сообщению перед аннулированием сертификата, что позволяет отменить сертификат открытого ключа, который будет использоваться для проверки подписей, созданных до аннулирования.

Значение метки времени становится ясно, когда есть необходимость законного использования электронных документов длительное время. Без фиксации времени не можем доверять подписанным документам в тех случаях, когда они подписаны с помощью криптографических примитивов, которые стали ненадежными, и в тех случаях, когда подписавший сам отказывается от подписи, утверждая, что он случайно потерял свой ключ. В последние годы, особенно в контексте правового регулирования использования цифровых подписей, организационные и правовые аспекты временных меток стали предметом всемирного внимания. В дополнение к определению обязанностей владельца подписи обязанности и ответственность третьих лиц (TSA) тоже указаны. Следовательно, существует растущий интерес к системам с метками времени, которые должны доверять TSA [5].

ЗАКЛЮЧЕНИЕ

В результате проведенного исследования возможности передачи управления сертификатами ключей проверки электронной подписи между УЦ при организации сетевой и иерархической модели инфраструктуры выявлены их следующие отличительные преимущества. Преимуществом иерархической архитектуры является то, что не все стороны должны автоматически доверять всем удостоверяющим центрам. Фактически единственным удостоверяющим центром, которому необходимо доверять, является корневой удостоверяющий центр. Для сетевой архитектуры большим плюсом является то, что компрометация одного центра в сети удостоверяющих центров не обязательно ведет к утрате доверия ко всей Public Key Infrastructure (**PKI**).

Еще одной положительной характеристикой сетевой модели является то, что в результате кросс-сертификации на уровне корневых УЦ исчезает необходимость распространения корневого самоподписанного сертификата одной воинской части среди пользователей другой.

Анализ двух моделей инфраструктуры при выходе из строя одного из УЦ показал, что при организации иерархической и сетевой (одноранговой) моделей инфраструктуры удостоверяющих центров при уничтожении одного из УЦ, в принципе, возможна передача управления сертификатами ключей проверки электронной подписи, а также сертификатов служб TSA/OCSP между удостоверяющими центрами. Для этого необходимо разработать предложения в нормативно-правовую базу для обеспечения легитимности такой операции и разработать механизм ее реализации.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 02.07.2021) “Об электронной подписи”.
2. Приказ Министра обороны РФ от 30 июня 2022 г. № 380 “Об утверждении Порядка реализации Министерством обороны Российской Федерации функций удостоверяющего центра, осуществления его прав и исполнения обязанностей”.
3. *Горбатов В.С., Полянская О.Ю.* Основы технологии PKI. М.: Горячая линия-Телеком, 2004. 248 с.
4. *Котенко А.В., Нурдавлетова Д.Р.* // Электронные средства и системы управления. Материалы докладов Международной научно-практической конференции. Томский государственный университет систем управления и радиоэлектроники, 2013. № 2. С. 18.
5. *Мерзликин Н.Ю., Платонов В.Ю., Лукьянов В.С., Быков Д.В.* // Современные проблемы науки и образования. 2013. № 3. С. 15.