Обеспечение безопасности систем дистанционного формирования электронной подписи в условиях слабодоверенного окружения

П.В. Смирнов, С.В. Смышляев

***Аннотация*— В работе рассматривается задача обеспечения безопасности систем дистанционного формирования электронной подписи («облачной» подписи) в случае использования пользователем клиентских компонент с устройств, для которых невозможно гарантировать наличие полностью доверенного окружения: в первую очередь, смартфонов с операционными системами iOS и Android. Данная задача стала особенно актуальной в последние годы: пользователи привыкли выполнять (или, как минимум, подтверждать) свои операции с помощью смартфона, но использование таким образом электронной подписи еще только развивается. Рассматриваются основные проблемы, функциональные требования, а также пути создания систем формирования и проверки электронной подписи с использованием устройств, в которых криптографические средства функционируют не в полностью доверенном окружении. Далее рассматривается вопрос о реализации в таких системах также и процесса удаленной выдачи сертификатов ключей проверки электронной подписи – процесса, который позволяет всю работу с электронной подписью, с самого начала, вести полностью дистанционным образом, без личной явки на каком-либо из этапов. С учетом функциональных требований и требований по информационной безопасности вырабатывается сценарий, применение которого позволяет решать данную задачу.**

***Ключевые слова*—электронная подпись, прикладные аспекты криптографии.**

I. Введение

Важность задачи обеспечения возможности использования ключей электронной подписи (ЭП) с использованием мобильных устройств вряд ли нуждается в комментариях: все основные программные технологии мигрируют на мобильные устройства, в первую очередь как раз те, что, как и работа с электронной подписью, предполагают повседневное использование.

При переносе привычных программных средств в условия мобильного использования требуется сформировать ответы на два основных вопроса: каковы функциональные требования к порядку их использования (с учетом ограничений мобильных устройств) и какая архитектура программных средств должна быть выбрана для обеспечения безопасной и эффективной работы на таких устройствах.

Ответ на первый вопрос в случае электронной подписи представляется относительно простым: важно дать пользователю инструмент, позволяющий с помощью его мобильного телефона (по возможности, произвольного, а не только смартфона на основе операционной системы iOS или Android) из любого места, где есть сотовая связь, воспользоваться своим ключом ЭП для формирования подписи документа (созданного либо на том же мобильном устройстве, либо на настольном компьютере, либо в размещенной в сети Интернет информационной системе с последующей передачей на устройство некоторым удобным образом).

Со вторым вопросом всё существенно сложнее: в ряде аспектов, важных для средств электронной подписи с учетом российских требований в области криптографической защиты, среда функционирования программных средств, работающих на мобильных устройствах, существенно отличается от привычной, а конкурирующих подходов к решению задачи можно выделить несколько.

II. Подходы к решению задачи по работе с электронной подписью с мобильных устройств

Первый из возможных подходов связан с хранением ключа электронной подписи непосредственно в памяти устройства (при использовании мобильного приложения для iOS или Android) или SIM-карты (при использовании Java-апплета на SIM-карте). Второй предполагает централизованное хранение ключей на отдельном защищенном сервере HSM (Hardware Security Module, программно-аппаратный криптографический модуль) сервиса электронной подписи и аутентификацию операций с ними с использованием хранимых на мобильном устройстве (аналогично, в памяти устройства или на SIM-карте) ключей доступа.

С учетом желаемой возможности обеспечить работу не только со смартфона, но и с телефона с произвольной операционной системой, отметим ряд особенностей каждого из двух подходов в случае реализации с использованием ключей, хранящихся на SIM-карте.

Статья получена 29 сентября 2020.
П.В. Смирнов – ООО «КРИПТО-ПРО» (e-mail: spv@cryptopro.ru)
С.В. Смышляев – ООО «КРИПТО-ПРО» (e-mail: svs@cryptopro.ru).

Начнем с вопроса о надежном хранении ключей на SIM-карте и криптографически безопасных механизмах работы с ними. В первую очередь важно отметить следующий аспект российской действительности: отечественный стандарт электронной подписи ГОСТ Р 34.10-2012, в отличие от алгоритма RSA (использование которого на SIM-картах по умолчанию закладывалось для граждан в некоторых зарубежных системах, см. [1, 2]), как и все схемы подписи, родственные схеме Эль-Гамаля, требует доверенного источника случайности для каждой операции формирования подписи, его сбой немедленно приводит к компрометации ключа (см. [3]). При этом данная ситуация в большинстве случаев не будет детектироваться на принимающей стороне, ведь подпись может остаться совершенно корректной и успешно проверяться. Кроме того, российские схемы электронной подписи предполагают работу в структурах эллиптических кривых, реализации процедур вычисления кратной точки в которых в случае низкоресурсных вычислителей (таких, как SIM-карты) требуют существенных мер по защите от атак по побочным каналам (см. [4]) – причем не только от тех, что требуют анализа с использованием специального оборудования с физическим доступом к устройству, но и от куда более доступных атак по времени, которые зачастую осуществимы удаленно. Отметим также и следующий аспект: массово поставляемые в Россию SIM-карты лишены криптосопроцессоров, микрокод которых допустимо считать доверенным в соответствии с российскими требованиями. В настоящее время отечественными специалистами (см. [5]) проводятся работы, направленные на решение данной проблемы, однако массовая замена всех SIM-карт граждан на специальные вряд ли возможна в ближайшем будущем. На массовых же SIM-картах безопасные реализации криптографических процедур возможны только на уровне апплетов, что в случае криптографии с открытым ключом может приводить к времени вычисления подписи, составляющем несколько минут.

Таким образом, безопасная реализация процедур вычисления электронной подписи непосредственно на массовой SIM-карте существенно затруднена. Все обозначенные проблемы вытекают из повышенных требований к ресурсам любых стойких алгоритмов криптографии с открытым ключом – такова цена за возможность пользоваться преимуществами асимметричных схем. Однако действительно ли в рассматриваемом случае есть смысл платить эту цену?

В случае использования телефона с произвольной операционной системой (не позволяющего, в общем случае, отображать документ непосредственно в приложении на экране) передача информации на вход модулям SIM-карты в любом случае возможна только по SMS/сервисным сообщениям, обработка которых возможна с использованием SIM-карт. За исключением нескольких отдельных вариантов использования, подписываемые сообщения не могут умещаться в такие сообщения ввиду технических ограничений. А значит, подпись на SIM в любом случае может использоваться исключительно для подтверждения соответствия отображаемого на мобильном устройстве текста (выжимки, хэша – любого набора уникальных идентификаторов документа) подписываемому документу – сам же документ необходимо безопасным образом отобразить пользователю на некотором другом устройстве, что заведомо требует доверенных серверных компонент, взаимодействующих как с этим устройством, так и с SIM-картой пользователя. К этим серверным компонентам не может не требоваться полное доверие – ведь наличие злоумышленника, имеющего к ним доступ, немедленно приводит к угрозе подмены подписываемого сообщения.

Таким образом, использование ключа ЭП, хранимого на SIM-карте, в любом случае предполагает взаимодействие с доверенным сервером, компрометация которого незамедлительно приводит к нарушению безопасности подписи. Но в таком случае пропадает и основная причина использовать на мобильном устройстве криптографию с открытым ключом – ведь это имеет смысл в первую очередь тогда, когда ответная часть взаимодействия доверенной стороной не является. Таким образом, аутентификацию сообщений между мобильным устройством и серверной стороной можно осуществлять с использованием симметричных алгоритмов обеспечения имитозащиты – таких, например, как HMAC_GOSTR3411_2012_256, стандартизированный в рекомендациях по стандартизации Росстандарта Р 50.1.113–2016 "Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования", разработанных Техническим комитетом по стандартизации «Криптографическая защита информации» (ТК 26). Задача безопасной реализации данного алгоритма на SIM-карте является беспроблемно выполнимой – производительности базовой (то есть, без криптосопроцессора) архитектуры совершенно достаточно, учесть необходимость противодействия атакам по побочным каналам можно без вреда для эффективности вычислений, а сбои в работе источников случайных чисел не опасны для компрометации ключей.

Вектор аутентификации пользователя при этом может диверсифицироваться (например, с использованием механизма, описанного в рекомендациях по стандартизации Р 50.1.113–2016 «Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования») из мастер-ключа, хранящегося на сервере, а также служебной информации. Существует две копии вектора аутентификации: одна хранится в апплете на SIM-карте, вторая – на серверной части. Обе копии вектора аутентификации служат для вычисления и проверки кода аутентификации сообщения по алгоритму HMAC_GOSTR3411_2012_256.

Для создания электронной подписи ключом пользователя выполняются следующие шаги:

1. Документ передается на серверную часть. Каналы

связи от компьютера пользователя до серверных компонент защищаются с помощью протокола TLS в соответствии с Р 1323565.1.020-2018 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)».

При этом обеспечение строгой криптографической аутентификации пользователя на данном этапе не является критичным – достаточно TLS с односторонней (то есть, серверной) аутентификацией.

2. На экране в рамках TLS-сессии у пользователя для документа, который он хочет подписать, отображается уникальный идентификатор документа.

На мобильное устройство пользователя пересылается информация о документе, включая идентификатор документа, идентификатор пользователя и идентификатор его ключа.

Каждому документу в момент загрузки на сервер присваивается индивидуальный идентификатор документа. В системе не может существовать двух документов с одинаковыми идентификаторами документа

3. На мобильном устройстве пользователя отображается полученная информация о документе.

4. В случае совпадения информации, отображаемой на экране компьютера и мобильном устройстве, пользователь вводит пароль доступа к вектору аутентификации.

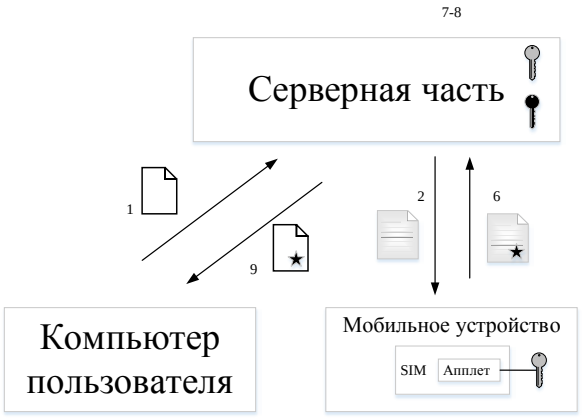
5. На результат операции и информацию о документе вычисляется код аутентификации в соответствии с HMAC_GOSTR3411_2012_256 с помощью вектора аутентификации пользователя (обозначен на схеме значком ключа серого цвета).

6. Производится передача вышеперечисленных данных на серверную часть.

7. На серверной части производится проверка кода аутентификации.

8. В случае корректности кода аутентификации производится подпись документа личным ключом пользователя, хранящимся на серверной части (обозначен на схеме значком ключа черного цвета).

9. Подписанный документ пересылается пользователю.



Безопасность при этом обеспечивается благодаря уникальности идентификатора документа, однозначной привязке этого идентификатора к конкретному документу на стороне сервера, а также включения его в имитозащищаемые данные при подтверждении со стороны SIM-карты. Для успешной атаки злоумышленнику необходимо, чтобы пользователь подтвердил операцию с идентификатором, соответствующим подменяемому документу. Но пользователь не сделает это, так как в рамках своей сессии с компьютера не увидит данный идентификатор в качестве привязанного к предназначенному им для подписи документу.

Доверенные SIM-карты с возможностью быстрого и безопасного вычисления электронной подписи по ГОСТ Р 34.10-2012 без труда добавляются в данную схему: требуется лишь использовать на шаге 5 вместо HMAC_GOSTR3411_2012_256 электронную подпись по ГОСТ Р 34.10-2012, а на шаге 7 проверять ее. При этом все перечисляемые далее преимущества технологии остаются в силе.

В целом технология, предполагающая хранение ключей электронной подписи на серверной стороне, часто называется «облачной» подписью. В терминологии принятого в конце 2019 года Федерального закона от 27.12.2019 N 476-ФЗ технология определяется как хранение ключей квалифицированных электронных подписей для дистанционного использования с созданием электронной подписи по поручению владельца квалифицированного сертификата.

Эта технология предполагает централизованное защищенное хранение ключей пользователей на серверной стороне с выполнением операций формирования электронной подписи по аутентифицированному запросу пользователя с помощью некоторых хранимых пользователем в секрете аутентифицирующих данных, векторов аутентификации. Ее применение решает ряд задач, связанных с обеспечением удобства использования электронной подписи:

- Повреждение устройства аутентификации (телефона с SIM-картой со специальным апплетом, смартфона с мобильным приложением, токена доступа) не приводит к утере ключей – только к временной утере доступа к ним (восстанавливается за один визит к оператору системы).
- Пользователь имеет возможность доступа к своим ключам подписи сразу с нескольких устройств, что удобно для «мобильных» сотрудников и для руководителей высшего звена.
- Средство аутентификации налагает существенно меньшее количество требований к окружению, чем полное средство электронной подписи, что позволяет упростить порядок установки и распространения средств аутентификации, расширить перечень поддерживаемых устройств.
- Благодаря высокопроизводительным кластеризуемым аппаратным решениям на стороне сервера достигается существенно более высокая скорость подписания пакетов документов.

При этом решается также ряд задач, связанных с безопасностью системы.

• В случае утери устройства доступ злоумышленника к ключам блокируется мгновенно на серверной стороне, что позволяет обеспечить вывод ключа из действия существенно оперативнее и безопаснее, чем механизм отзыва сертификата (что не исключает возможность совместного применения двух механизмов).

• Наличие журналов аудита на сервере, аутентичность которых защищена благодаря хранению с помощью цепной записи данных с использованием средств HSM позволяет гарантированно установить (с привлечением в случае конфликтной ситуации администратора аудита), был ли осуществлен несанкционированный доступ к ключу подписи.

• Возможность прямого взаимодействия серверных компонент средства облачной подписи с информационными системами позволяет по желанию владельца ключа ограничить допустимое множество документов, поступающих ему на подпись, – например, если владелец ключа регулярно подписывает своим ключом справки и отчетность, но не хотел бы, чтобы с помощью его ключа можно было продать его квартиру или заключить многомиллионную сделку.

Отметим, что описанная выше схема для аутентификации с использованием SIM-карт без существенных изменений переносится для использования в смартфоне с операционной системой iOS или Android. При этом также существенно расширяются возможности по визуализации документов перед подписанием: возможен показ документа непосредственно в мобильном приложении.

Схема взаимодействия пользователя с серверной частью при этом остается аналогичной описанной выше для случая SIM-карты, со следующими уточнениями.

1. На мобильное устройство передается сам документ, а не его идентификатор – соответственно, пользователю для подтверждения операции требуется не сравнивать идентификаторы документа на компьютере и на мобильном устройстве, а проверить сам отображаемый документ.
2. Благодаря возможностям мобильного приложения документ доставляется на мобильное устройство по защищенному с использованием протокола TLS каналу связи.
3. Так как строгое криптографическое подтверждение операции с документом производится с мобильного устройства после просмотра самого документа целиком, в случае неконфиденциальных документов первичную загрузку документов на серверные компоненты можно совершать и без защиты канала связи.

Федеральный закон от 27.12.2019 N 476-ФЗ дает право удостоверяющим центрам после прохождения соответствующей процедуры аккредитации осуществлять хранение ключа электронной подписи, ключ проверки которой содержится в квалифицированном сертификате, с обеспечением его защиты от компрометации и (или) несанкционированного использования, в том числе создание при помощи указанного ключа подписи по поручению владельца квалифицированного сертификата. При этом соответствующие механизмы работы с хранимым ключом подписи должны удовлетворять четырем группам требований по:

а) хранению ключей квалифицированной электронной подписи и автоматическому созданию такой подписи с их использованием по поручению соответствующих владельцев квалифицированных сертификатов;

б) аутентификации владельцев квалифицированных сертификатов, по поручению которых аккредитованный удостоверяющий центр создает и проверяет квалифицированную электронную подпись;

в) защите информации, передаваемой по каналу взаимодействия между владельцем квалифицированного сертификата и аккредитованным удостоверяющим центром, осуществляющим создание и проверку квалифицированной электронной подписи по поручению такого владельца;

г) доказательству невозможности отказа владельца квалифицированного сертификата от поручения на создание квалифицированной электронной подписи.

Рассмотрим, как в описанной схеме выполняются указанные требования.

Хранение ключей квалифицированной электронной подписи и автоматическое создание ЭП по поручению владельцев на серверной части производится с использованием высокозащищенного программно-аппаратного модуля HSM, реализующего функционал создания, использования и уничтожения ключевой информации, предполагающий хранение ключей в неизвлекаемом виде в продолжение всего их жизненного цикла.

Для аутентификации владельцев квалифицированных сертификатов используется механизм HMAC_GOSTR3411_2012_256, имеющий стойкость аналогичную используемому алгоритму электронной подписи.

Защита информации, передаваемой по каналу взаимодействия с владельцем квалифицированного сертификата, обеспечивается с помощью протокола TLS.

Доказательство невозможности отказа владельца квалифицированного сертификата от поручения на создание квалифицированной электронной подписи обеспечивается с помощью механизма HMAC_GOSTR3411_2012_256, а также с помощью реализуемого HSM доверенного аудита всех операций с ключами ЭП, не допускающего искажений оператором или администратором безопасности информации журнала, который содержит сведения о совершенных каждым пользователем операциях, – в том числе не допускает изъятия информации о тех или иных операциях (например, с помощью использования механизмов цепной записи данных).

III. Удаленная идентификация и аутентификация

Федеральный закон от 27.12.2019 N 476-ФЗ вводит и

еще одну норму, имеющую прямое отношение к упрощению работы с электронной подписью для массового пользователя: к традиционным способам идентификации заявителя при выдаче сертификата ключа проверки электронной подписи (лично или с помощью ранее выданного сертификата) добавляются дистанционные: посредством идентификации заявителя без его личного присутствия путем предоставления сведений из единой системы идентификации и аутентификации (ЕСИА) и информации из единой биометрической системы (ЕБС), а также с помощью заграничного паспорта нового поколения. Реализация таких возможностей также требует проработки технических и криптографических вопросов.

При обсуждении технологий удаленной идентификации (в частности, с использованием биометрических решений) при получении сертификатов ключей электронной подписи зачастую смешиваются два независимых понятия: удаленная идентификация/аутентификация для получения возможности использования квалифицированной электронной подписи без личной явки в удостоверяющий центр и технология «облачной» подписи. Из-за подобной путаницы в понятиях зачастую «облачная» подпись представляется как решение, позволяющее пользователям путем исключительно биометрической аутентификации получать доступ к операциям с хранимым на сервере ключом электронной подписи – что вызывает справедливую критику со стороны специалистов по информационной безопасности (см. [6]). При этом разработки в части обоих данных понятий действительно важны для повышения удобства использования технологий PKI, поэтому представляется полезным детальное обсуждение возможности развития обоих направлений – в том числе и возможности их безопасного совместного применения.

Рассмотрим оба этих понятия несколько подробнее для того, чтобы обсудить возможность их совместного использования при обеспечении информационной безопасности.

Отметим, что сама по себе технология «облачной» подписи не привязана к тому или иному способу первичного получения сертификатов ключей электронной подписи и векторов аутентификации к соответствующим ключам (хранимым на серверной стороне) – лишь предполагает, что сертификаты выдаются некоторым порядком, обеспечивающим доверенную идентификацию пользователя, а векторы аутентификации к хранимым на сервере ключам пользователя получаются пользователем безопасным способом, исключающим их перехват злоумышленником.

Базовым способом регистрации пользователя средств «облачной» подписи является следующий:

1. Пользователь лично является к оператору, запрашивает генерацию нового ключа на сервере «облачной» подписи с получением вектора аутентификации к нему, а также запроса на сертификат.

2. Пользователь лично обращается в удостоверяющий центр (УЦ), передает полученный на предыдущем шаге запрос на сертификат в УЦ.

3.УЦ выпускает квалифицированный сертификат на данного пользователя, передает его пользователю.

4. Пользователь передает (любым образом, доверенный канал не обязателен благодаря ЭП УЦ в сертификате) полученный на шаге 3 сертификат на сервер «облачной» подписи для привязки сертификата к ключу при совпадении открытых ключей.

5. Пользователь использует свой ключ в «облачном» средстве ЭП обычным образом, аутентифицируясь на него с помощью своего вектора аутентификации.

Личная явка на шаге 1 обеспечивает безопасную передачу вектора аутентификации пользователю. При этом идентификация пользователя, вообще говоря, не является обязательной: ключ после шага 1 является сугубо криптографическим объектом, под контролем владельца, но без возможности использования от его лица – с учетом этого замечания, данное свойство можно достичь и с помощью установления защищенного канала с односторонней аутентификацией (аутентификацией сервера) с достаточной стойкостью как в части обеспечения конфиденциальности, так и имитозащиты.

Личная явка на шаге 3 обеспечивает доверенную привязку открытого ключа из запроса на сертификат к владельцу, после которой соответствующий ключ ЭП становится возможно использовать от лица владельца.

Технологии получения сертификатов без личного присутствия, допускаемые Федеральным законом от 27.12.2019 N 476-ФЗ, предполагают возможность пользователю, так или иначе создавшему ключ электронной подписи, получить квалифицированный сертификат соответствующего ключа проверки электронной подписи без личной явки в удостоверяющий центр.

Отметим следующий принципиальный момент: данная технология направлена на отмену необходимости личной явки для идентификации гражданина при выдаче сертификата, но она сама по себе никак не привязана к тому или иному способу хранения и использования самих ключей электронной подписи пользователями – лишь предполагает, что ключи электронной подписи, на которые выдаются сертификаты, хранятся и используются под контролем владельца сертификата (физическим контролем с наличием ключевого носителя «в кармане» либо обеспечиваемым безопасностью распределенной системы, в рамках которой у владельца присутствует вектор аутентификации).

Рассмотрим базовый сценарий получения сертификата ключа проверки электронной подписи без личного присутствия – для простоты предположим, что речь идет о персональном ключевом носителе и локальном средстве ЭП.

1. Пользователь с помощью уже имеющегося у него средства ЭП создает ключ электронной подписи на своем ключевом носителе и соответствующий ему запрос на сертификат.

2. Пользователь обращается в УЦ, аутентифицируется через ЕСИА/ЕБС или с применением загранпаспорта,

после чего в качестве уже идентифицированного лица пересылает по созданному защищенному каналу полученный на предыдущем шаге запрос на сертификат в УЦ.

3. УЦ выпускает квалифицированный сертификат на данного пользователя, передает его пользователю.

4. Пользователь использует свое средство ЭП и сертификат обычным образом.

IV. Добавление «облачной» подписи в сценарий с удаленным получением сертификатов

Оценим теперь возможность введения «облачной» подписи в данную схему, считая необходимым условие недопустимости снижения безопасности по сравнению с описанным выше базовым сценарием.

1. Пользователь по защищенному каналу (обеспечивающему как конфиденциальность, так и имитозащиту необходимого уровня стойкости) с односторонней аутентификацией (т.е. аутентифицированному только со стороны сервера) обращается к серверу «облачной» подписи, запрашивает у сервера «облачной» подписи генерацию нового ключа (пока не снабженного сертификатом, т.е. только как криптографического объекта) с получением вектора аутентификации к нему, а также запроса на сертификат.

2. Пользователь обращается в УЦ, аутентифицируется посредством ЕСИА/ЕБС или с помощью загранпаспорта, после чего в качестве уже идентифицированного лица пересылает по созданному защищенному каналу полученный на предыдущем шаге запрос на сертификат в УЦ.

3.УЦ выпускает квалифицированный сертификат на данного пользователя, передает его пользователю.

4. Пользователь аутентифицируется на сервере «облачной» подписи с использованием полученного на шаге 1 вектора аутентификации, пересылает полученный на шаге 3 сертификат на сервер «облачной» подписи.

5. Пользователь использует свой ключ в «облачном» средстве ЭП обычным образом, аутентифицируясь на нем с помощью своего вектора аутентификации.

Отметим, что в конце первого шага сервер «облачной» подписи не имеет никакой (по крайней мере, доверенно подтвержденной) информации о принадлежности созданного ключа некоторому лицу. Всё, что обеспечивается после первого шага: тот пользователь (вообще говоря, пока совершенно анонимный для сервера), что создал себе в «облачном» средстве ключ (только криптографический объект, еще не привязанный к владельцу в юридическом смысле), гарантированно имеет полный и исключительный контроль над этим ключом благодаря переданному ему вектору аутентификации. То есть, уже обеспечивается, что ключ находится под полным контролем владельца, но пока не обеспечивается какой-либо привязки ключа к тому или иному лицу (точь-в-точь, как и после первого шага в базовом сценарии – на носителе создан ключ, он «в кармане» у владельца под его полным контролем, но пока это лишь криптографический объект, никак не привязанный к какому-либо лицу).

Также отметим следующее: не предполагается большего доверия к биометрической идентификации/аутентификации, чем в первой схеме – как и в ней, биометрическая аутентификация происходит лишь единожды, при получении сертификата. Всё взаимодействие с сервером «облачной» подписи производится с использованием векторов аутентификации, обеспечивающих соответствующий ключу ЭП уровень стойкости, без какого-либо доверия к биометрическим механизмам.

Таким образом, в предположении допустимости получения сертификатов ключей ЭП с помощью биометрической идентификации/аутентификации использование «облачной» ЭП без личной явки к оператору «облачной» ЭП не приводит к какому-либо дополнительному снижению информационной безопасности по сравнению с базовым сценарием.

Благодаря трем дополнительным преимуществам «облачной» подписи в части безопасности, перечисленным ранее (возможность мгновенной блокировки ключа в случае утери устройства или сомнений в сохранности вектора аутентификации в тайне; максимально доверенный и подробный аудит; возможность ограничить сферу применения своего ключа ЭП благодаря настройкам серверной стороны), защищенность пользователя от злоумышленников повышается, что становится особенно важным в случае появления легитимного способа получения сертификата с помощью биометрической идентификации.

Кроме того, при использовании средств «облачной» подписи (в частности, с возможностью получения квалифицированного сертификата удаленным образом) представляется важным обеспечить следующий набор организационно-технических мер.

1. Выдачу новых векторов аутентификации на ключ, хранимый на сервере «облачной» подписи, производить только в случае аутентификации с использованием уже существующих векторов аутентификации – то есть, криптографически стойкими методами, а не путем аутентификации с помощью сторонних методов, таких как аутентификация через ЕСИА/ЕБС. Данная мера защищает от возможных угроз, связанных с получением злоумышленником векторов аутентификации на уже выданные ключи.

2. При выдаче нового вектора аутентификации на уже выданный ключ необходимо извещать владельца ключа с помощью доступных каналов взаимодействия.

Опционально при взаимодействии с сервером «облачной» подписи можно использовать биометрическую аутентификацию в качестве дополнительного средства защиты (например, для того, чтобы подтвердить согласие на хранение ключа в облаке) – в описанной выше схеме намеренно сделан акцент на отсутствии ее использования при работе с сервером «облачной» подписи для демонстрации того, что на ней не базируется обеспечиваемое аутентификацией доверие.

Сертификаты ключей проверки электронной подписи, выданные при аутентификации с использованием

ЕСИА/ЕБС или загранпаспорта (без личной явки), уместно снабжать соответствующими идентификаторами, а в информационных системах учитывать данную информацию для возможного требования дополнительных способов подтверждения личности.

При получении сертификата с помощью идентификации/аутентификации через ЕСИА/ЕБС возможно уведомлять владельца о данном действии с использованием доступных (благодаря информации в ЕСИА/ЕБС) каналов связи, а сам сертификат выдавать с задержкой, чтобы обеспечить возможность лицу отменить выдачу ему сертификата, если он не запрашивал сертификат (в случае ложной аутентификации злоумышленником).

Протокол OpenID Connect ([7]) в версии, применяемой в ЕСИА/ЕБС (см. [8]), позволяет передавать в скалярном виде информацию о степени схожести аутентифицирующегося лица с эталоном. В случае получения сертификата ключа проверки электронной подписи возможно использовать повышенные требования к данным параметрам.

V. Заключение

С учетом ограничений, накладываемых мобильными устройствами, разумным представляется их использование для аутентификации и волеизъявления на выполнение операции с ключом ЭП в рамках схем «облачной» подписи. Рассмотрены преимущества использования данных схем, а также описаны два протокольных решения, в настоящее время уже реализованные получивших подтверждение соответствия требованиям к действующим средствам электронной подписи решениях. Принимая во внимание нормы о возможных путях проведения удаленной идентификации, введенные в Федеральном законе от 27.12.2019 N 476-ФЗ, важной является задача интеграции решений по удаленной идентификации при выдаче сертификатов ключей проверки электронной подписи с решениями, реализующими дистанционное хранение и использование ключей электронной подписи. Описаны основные требования к решению данной задачи, а также предложен сценарий, в полной мере решающий её с учетом этих требований.

Библиография

[1] Estonian eID scheme: Mobiil-ID. Technical specifications and procedures for assurance level high for electronic identification. https://ec.europa.eu/cefdigital/wiki/download/attachments/62885749/EE%20eID%20LoA%20mapping%20-%20Mobiil-ID.pdf?version=1&modificationDate=1531759816924&api=v2#:~:text=Estonian%20eID%20is%20always%20issued,this%20document%20as%20Mobiil%2DID.&text=The%20identity%20documents%20database%20provides,validity%20of%20the%20provided%20document

[2] A. Parsovs. “Estonian Electronic Identity Card: Security Flaws in Key Management”, https://www.usenix.org/conference/usenixsecurity20/presentation/parsovs

[3] T. ElGamal, “A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, in *Proc. Crypto 84*, Springer-Verlag, New York, Heidelberg, Berlin, 1985, pp. 10–18.

[4] J.L. Danger, S. Guilley, P. Hoogvorst, C. Murdica, D. Naccache: “A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards”, in *Journal of Cryptographic Engineering*, 3(4), 2013, pp. 241–265.

[5] “Сотовые операторы начали переход на отечественную связь”, http://www.ipmce.ru/about/press/popular/sotsv/

[6] А.Г. Сабанов, “Анализ международных стандартов по идентификации и аутентификации“, доклад на X Уральском форуме “Информационная безопасность финансовой сферы“, 2018.

[7] OpenID Connect Core 1.0, https://openid.net/specs/openid-connect-core-1_0.html

[8] Единая биометрическая система. Методические рекомендации по работе с Единой биометрической системой для разработчиков. https://bio.rt.ru/documents/

Providing security to remote digital signature systems in case of semi-trusted secure environment

Pavel Smirnov, Stanislav Smyshlyaev

***Abstract*— The task of providing security to remote digital signature systems ("cloud" signature) for cases of end user running client-side components on devices without potential of ensuring trusted environment (most common examples of such devices are smartphones with iOS or Android operation systems) is considered. This task has become particularly topical recently: users are used to performing (or at least confirming) their operations with smartphones, however, such usage of digital signature is still evolving. Main issues and functional requirements are dealt with, ways to construct systems employing devices with cryptographic software running in weakly secure environment are discussed. The task of remote issuance of digital certificates is also considered: such a process can make completely remote usage of digital signature (from the very beginning, without even one personal appearance to a certification authority) possible. Taking functional and information security requirements into account, a scenario is developed in the current paper to solve the mentioned task.**

***Keywords*—digital signature, applications of cryptography**

REFERENCES

[1] Estonian eID scheme: Mobiil-ID. Technical specifications and procedures for assurance level high for electronic identification. https://ec.europa.eu/cefdigital/wiki/download/attachments/62885749/EE%20eID%20LoA%20mapping%20-%20Mobiil-ID.pdf?version=1&modificationDate=1531759816924&api=v2#:~:text=Estonian%20eID%20is%20always%20issued,this%20document%20as%20Mobiil%2DID.&text=The%20identity%20documents%20database%20provides,validity%20of%20the%20provided%20document.

[2] A. Parsovs. "Estonian Electronic Identity Card: Security Flaws in Key Management", https://www.usenix.org/conference/usenixsecurity20/presentation/parsovs

[3] T. ElGamal, "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", in *Proc. Crypto 84*, Springer-Verlag, New York, Heidelberg, Berlin, 1985, pp. 10–18.

[4] J.L. Danger, S. Guilley, P. Hoogvorst, C. Murdica, D. Naccache: "A synthesis of side-channel attacks on elliptic curve cryptography in smart-cards", in *Journal of Cryptographic Engineering*, 3(4), 2013, pp. 241–265.

[5] "Sotovye operatory nachali perehod na otechestvennuyu svyaz", http://www.ipmce.ru/about/press/popular/sotsv/ (in Russian)

[6] A.G. Sabanov, "Analiz mezhdunarodnyh standartov po identifikacii I autentifikacii", talk on the X Ural Forum "Information security of financial sphere", 2018 (in Russian).

[7] OpenID Connect Core 1.0, https://openid.net/specs/openid-connect-core-1_0.html

[8] Edinaya biometricheskaya sistema. Medodicheskiye rekomendacii po rabote s Edinoj biometricheskoj sistemoj dlya razrabotchikov. https://bio.rt.ru/documents/ (in Russian).