Подходы к удаленной идентификации и аутентификации для задач PKI: как совместить цифровую экономику и безопасность

Смышляев Станислав Витальевич, к.ф.-м.н.,
директор по информационной безопасности

Смирнов Павел Владимирович, к.т.н.,
руководитель департамента разработок

PKI-Форум Россия 2018

1 Введение
2 “Облачная” подпись
3 Удаленное получение сертификатов
4 Безопасный способ совмещения технологий
5 Повышение безопасности совмещенного решения

Обсуждения перспектив биометрической идентификации и аутентификации для задач PKI

Светлое будущее после построения “цифровой экономики”

Смешение в дискуссиях двух независимых понятий:

- удаленная идентификация и аутентификация для получения возможности использования КЭП без личной явки в УЦ;
- технология “облачной” подписи.

Обсуждения перспектив биометрической идентификации и аутентификации для задач PKI

Опасное упрощенное понимание

- На сервере — некое самодостаточное СКЗИ, осуществляется хранение ключей пользователей.
- В любой момент с любого устройства можно аутентифицироваться на сервер с помощью только биометрических технологий.

- СКЗИ на сервере, хранение ключей пользователей.
- Аутентификация на сервер по биометрии в любой момент.

Критика и причины неодобрения

- Вероятность ложной аутентификации с помощью биометрии существенно выше вероятности подделки ЭП.
- Незрелость мат. аппарата, используемого для получения даже слабых оценок стойкости биометрической аутентификации.
- При биометрической аутентификации часты ложные отказы $\Rightarrow$ неуместны строгие ограничения по числу попыток — в отличие от криптографически стойких методов аутентификации.
- Удаленное получения сертификата можно сделать отложенным — а запрос на подпись нельзя.

При разделении анализа серверного СКЗИ и компонент аутентификации нарушится принцип равнопрочности криптографических систем.

Неконтролируемый процесс продвижения удобных технологий чреват небезопасными решениями — при отсутствии альтернативы.

Цель

Важно детальное обсуждение возможности развития обоих направлений и возможности их безопасного совместного применения — для выработки этой альтернативы.

План

- Рассмотрим по отдельности “облачную” подпись и удаленное получение сертификатов.
- Переформулируем задачу: как при допустимости удаленного получения сертификатов сохранить равенство безопасности “облачной” подписи и ключей на персональных носителях.
- Предложим путь решения задачи.
- Доп. меры, повышающие безопасность совместных решений.

Неконтролируемый процесс продвижения удобных технологий чреват небезопасными решениями — при отсутствии альтернативы.

Цель

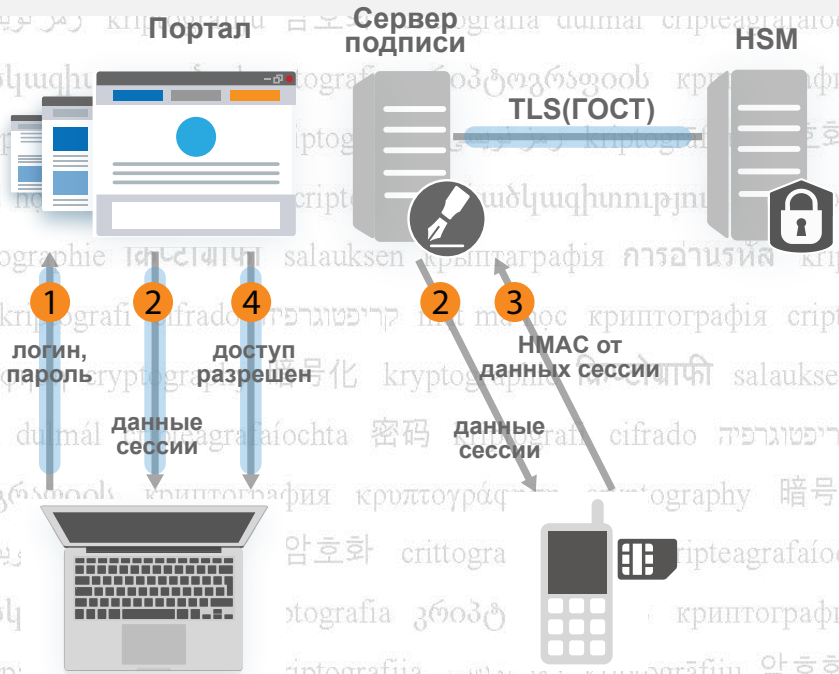
Важно детальное обсуждение возможности развития обоих направлений и возможности их безопасного совместного применения — для выработки этой альтернативы.

План

- Рассмотрим по отдельности “облачную” подпись и удаленное получение сертификатов.
- Переформулируем задачу: как при допустимости удаленного получения сертификатов сохранить равенство безопасности “облачной” подписи и ключей на персональных носителях.
- Предложим путь решения задачи.
- Доп. меры, повышающие безопасность совместных решений.

1 Введение
2 “Облачная” подпись
3 Удаленное получение сертификатов
4 Безопасный способ совмещения технологий
5 Повышение безопасности совмещенного решения

“Облачная” подпись



- Единое решение: серверная и клиентская компоненты.
- Серверная компонента — защищенное хранение ключей в неизвлекаемом виде, реализация операций по аутентифицированным запросам от клиентских компонент.
- Клиентская компонента — визуализация, аутентификация и подтверждение операций, защищенный канал.

“Облачная” подпись

Преимущества: удобство

- 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.
- Средство аутентификации налагает существенно меньшее количество требований к окружению, чем средство ЭП, что позволяет упростить порядок установки и распространения, расширить перечень устройств.
- Пользователь имеет возможность доступа к своим ключам ЭП с нескольких устройств, что удобно для «мобильных» сотрудников и для руководителей высшего звена.
- Высокопроизводительные кластеризуемые аппаратные решения на стороне сервера — высокая скорость подписания пакетов документов.

„Облачная“ подпись

Преимущества: безопасность

- Повреждение/утеря устройства аутентификации не приводит к утере ключей ЭП, в случае утери доступ к ключам блокируется мгновенно на серверной стороне.
- Журнал аудита на сервере при нештатной ситуации позволяет установить, был ли несанкционированный доступ к ключу подписи.
- Возможность прямого взаимодействия серверных компонент средства „облачной“ подписи с ИС позволяет по желанию владельца ключа ограничить допустимое множество документов, поступающих ему на подпись.

Сертифицированнное средство „облачной“ ЭП

- КриптоПро DSS с Крипто Про HSM 2.0: в августе 2018 получены сертификаты на 11 исполнений.
- В том числе, с компонентами аутентификации в виде мобильных приложений (iOS, Android) и апплета на SIM-карте.

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3481 от "10" августа 2018 г.

Действителен до "10" августа 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие «Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (исполнения 3)» (исполнения «DSS + nyDSS», «DSS + AirKey Lite») в комплектации согласно формуляру ЖТЯИ.00096-02 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1, Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографически аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-003001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЯИ.00096-02 30 01.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России А.М. Шойтов

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3480 от "10" августа 2018 г.

Действителен до "10" августа 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие «Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (исполнения 3)» (исполнения «DSS + SIM (O2M)») в комплектации согласно формуляру ЖТЯИ.00096-02 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1, Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографически аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-003001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЯИ.00096-02 30 01.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России А.М. Шойтов

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3479 от "10" августа 2018 г.

Действителен до "10" августа 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие «Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (исполнения 3)» (исполнение «DSS + JCP версия 2.0 исполнение 2») в комплектации согласно формуляру ЖТЯИ.00096-02 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1, Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1, и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, вычисление значения хэш-функции для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографически аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-003001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЯИ.00096-02 30 01.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России А.М. Шойтов

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3478 от "10" августа 2018 г.

Действителен до "10" августа 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие «Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)» (исполнения «DSS + CSP версия 4.0 исполнение 1-Base», «DSS + CSP версия 4.0 исполнение 2-Base», «DSS + CSP версия 4.0 исполнение 3-Base») в комплектации согласно формуляру ЖТЯИ.00096-02 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения «DSS + CSP версия 4.0 исполнение 1-Base»), класса КС2 (для исполнения «DSS + CSP версия 4.0 исполнение 2-Base»), класса КС3 (для исполнения «DSS + CSP версия 4.0 исполнение 3-Base»). Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения «DSS + CSP версия 4.0 исполнение 1-Base»), класса КС2 (для исполнения «DSS + CSP версия 4.0 исполнение 2-Base»), класса КС3 (для исполнения «DSS + CSP версия 4.0 исполнение 3-Base»), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографически аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-003001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЯИ.00096-02 30 01.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России А.М. Шойтов

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3477 от "10" августа 2018 г.

Действителен до "10" августа 2021 г.

Выдан Обществу с ограниченной ответственностью «КРИПТО-ПРО».

Настоящий сертификат удостоверяет, что изделие «Программно-аппаратный криптографический модуль «КриптоПро HSM» версия 2.0 (комплектация 3)» (исполнения «DSS + CSP версия 3.9 исполнение 1», «DSS + CSP версия 3.9 исполнение 2», «DSS + CSP версия 3.9 исполнение 3») в комплектации согласно формуляру ЖТЯИ.00096-02 30 01

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения «DSS + CSP версия 3.9 исполнение 1»), класса КС2 (для исполнения «DSS + CSP версия 3.9 исполнение 2»), класса КС3 (для исполнения «DSS + CSP версия 3.9 исполнение 3»). Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, установленным для класса КС1 (для исполнения «DSS + CSP версия 3.9 исполнение 1»), класса КС2 (для исполнения «DSS + CSP версия 3.9 исполнение 2»), класса КС3 (для исполнения «DSS + CSP версия 3.9 исполнение 3»), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, вычисление имитовставки для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений, криптографически аутентификация абонентов при установлении соединения, реализация функций электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «КРИПТО-ПРО»

сертификационных испытаний образца продукции № 789А-003001.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями эксплуатационной документации согласно формуляру ЖТЯИ.00096-02 30 01.

Временно исполняющий обязанности начальника Центра защиты информации и специальной связи ФСБ России А.М. Шойтов

Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию, сертификации и защите государственной тайны ФСБ России А.В. Парфенов

Конкретные сертифицированные средства (КриптоПро DSS) явно определяют порядок получения СКПЭП и аутентификаторов.

Но сама технология „облачной“ подписи

- не привязана к способу первичного получения СКПЭП и аутентификаторов к соответствующим ключам;
- лишь предполагает, что
  - СКПЭП выдаются с доверенной аутентификацией пользователя,
  - аутентификаторы к хранимым на сервере ключам получаются безопасным способом.

Конкретные сертифицированные средства (КриптоПро DSS) явно определяют порядок получения СКПЭП и аутентификаторов.

Но сама технология „облачной“ подписи

- не привязана к способу первичного получения СКПЭП и аутентификаторов к соответствующим ключам;
- лишь предполагает, что
  - СКПЭП выдаются с доверенной аутентификацией пользователя,
  - аутентификаторы к хранимым на сервере ключам получаются безопасным способом.

В настоящее время средства „облачной“ подписи предназначены для использования следующим образом.

1. Пользователь лично является к Оператору сервера подписи, запрашивает генерацию нового ключа на сервере „облачной“ подписи, получает аутентификатор и запрос на сертификат.
2. Пользователь лично обращается в УЦ, передает полученный запрос на сертификат.
3. УЦ выпускает квалифицированный сертификат на данного пользователя, передает его пользователю.
4. Пользователь передает полученный сертификат на сервер „облачной“ подписи для привязки сертификата к ключу.
5. Пользователь использует свой ключ в „облачном“ средстве ЭП с помощью своего аутентификатора.

Личная явка на шаге 1 обеспечивает:

(a) безопасную передачу аутентификатора пользователю;

(b) собственноручную подпись владельцем согласия на получение услуг по хранению ключа ЭП на сервере „облачной“ подписи при выполнении оператором правил пользования.

Ключ после шага 1 является криптографическим объектом под контролем владельца без возможности использования от его лица — идентификация является избыточной.

Таким образом, свойство (a) возможно достичь и с помощью установления защищенного канала с односторонней аутентификацией.

1 Введение
2 “Облачная” подпись
3 Удаленное получение сертификатов
4 Безопасный способ совмещения технологий
5 Повышение безопасности совмещенного решения

Удаленное получение сертификатов

Получение сертификатов без личного присутствия с помощью аутентификации в ЕСИА и ЕБС. Возможность пользователю, так или иначе создавшему ключ ЭП, получить квалифицированный СКПЭП без личной явки в УЦ.

- Технология направлена на отмену необходимости личной явки для идентификации при выдаче сертификата.
- Никак не привязана к способу хранения и использования самих ключей ЭП пользователями.
- Лишь предполагает, что ключи хранятся и используются под контролем владельца сертификата.
  - Под физическим контролем с наличием ключевого носителя «в кармане».
  - Обеспечиваемым безопасностью системы, в рамках которой у владельца присутствует аутентификатор.

Оставим «за скобками» вопросы безопасности существующих технологий биометрической идентификации и аутентификации.

Предположим, что получение квалифицированных сертификатов без личной явки в УЦ стало легитимным (и считающимся обладающим допустимым для области применения квалифицированной ЭП уровнем безопасности) в РФ.

Базовый сценарий работы с ЭП при удаленном получении сертификата

1. Пользователь с помощью сертифицированного средства ЭП создает ключ ЭП на своем носителе и запрос на сертификат.
2. Пользователь обращается в УЦ, аутентифицируется и авторизуется через ЕСИА/ЕБС, после чего пересылает по созданному защищенному каналу 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.

CRYPTOPRO

1 Введение
2 “Облачная” подпись
3 Удаленное получение сертификатов
4 Безопасный способ совмещения технологий
5 Повышение безопасности совмещенного решения

Введем „облачную“ подпись, считая необходимым условие недопустимости снижения безопасности по сравнению с описанным выше базовым сценарием.

1. Пользователь по защищенному каналу с односторонней аутентификацией обращается к серверу „облачной“ подписи, запрашивает генерацию нового ключа с получением аутентификатора к нему, а также запроса на сертификат.
2. Пользователь обращается в УЦ, аутентифицируется и авторизуется через ЕСИА/ЕБС, после чего пересылает по созданному защищенному каналу запрос на сертификат в УЦ.
3. УЦ выпускает квалифицированный сертификат на данного пользователя, передает его пользователю.
4. Пользователь пересылает полученный сертификат на сервер.
5. Пользователь использует свой ключ в „облачном“ средстве ЭП обычным образом с помощью своего аутентификатора.

Обеспечивается после первого шага:

1. Пользователь, что создал себе в „облачном“ средстве ключ, имеет исключительный контроль над этим ключом, благодаря переданному ему аутентификатору.
2. Ключ под полным контролем владельца, но пока нет какой-либо привязки ключа к тому или иному лицу — как и после первого шага в базовом сценарии.

Не предполагается большего доверия к биометрической идентификации/аутентификации, чем в базовом сценарии — биометрическая аутентификация тоже происходит единожды, при получении сертификата.

Всё взаимодействие с сервером „облачной“ подписи с использованием аутентификаторов, обеспечивающих соответствующий ключу ЭП уровень стойкости, без какого-либо доверия к биометрическим механизмам.

1 Введение
2 “Облачная” подпись
3 Удаленное получение сертификатов
4 Безопасный способ совмещения технологий
5 Повышение безопасности совмещенного решения

Преимущества „облачной“ подписи в части безопасности

- Возможность мгновенной блокировки ключа.
- Максимально доверенный аудит.
- Возможность ограничить сферу применения ключа.

$\Rightarrow$ защищенность пользователя повышается, что особенно важно в случае легитимного способа получения сертификата с помощью биометрической идентификации.

Дополнительно усилить безопасность

- Выдачу новых аутентификаторов на ключ — только с использованием уже существующих аутентификаторов.
- При выдаче нового аутентификатора на существующий ключ извещать владельца с помощью доступных каналов взаимодействия.

Общие дополнительные меры защиты при получении сертификатов посредством удаленной идентификации

СКПЭП, выданные без личной явки, снабжать соответствующими идентификаторами, а в ИС принимать с учетом моделей угроз.

OpenID Connect в версии ЕСИА/ЕБС позволяет передавать степень схожести — в случае получения СКПЭП повысить требования к ней.

Общие дополнительные меры защиты при получении сертификатов посредством удаленной идентификации

При дистанционном получении сертификата уведомить владельца с использованием доступных (по информации в ЕСИА) каналов связи, а сертификат выдавать с задержкой.

CRYPTOPRO

Спасибо за внимание!

Вопросы?

- Материалы, вопросы, комментарии:
  svs@cryptopro.ru
  spv@cryptopro.ru

Способ подтверждения согласия на услугу хранения ключа на серверной стороне

Опционально при взаимодействии с сервером „облачной“ подписи можно использовать биометрическую аутентификацию в качестве дополнительного средства защиты (например, для того, чтобы подтвердить готовность на услугу хранения 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.