О видах ключевых носителей и форматах ключей электронной подписи простыми словами

В этой статье мы хотим помочь разобраться, какие бывают ключевые носители, и как тип устройства определяет степень безопасности закрытого ключа электронной подписи (ЭП).

Для этого рассмотрим практическую разницу форматов контейнеров ЭП и способы работы ключевых носителей.

Термины

Часть терминов в статье подается в упрощенном виде для простоты понимания.

Используя термин **ЭП**, мы подразумеваем квалифицированную электронную подпись (КЭП). Это электронная подпись, которая полностью соответствует всем требованиям 63-ФЗ и Приказу ФСБ России № 796 к средствам ЭП и хранится на персональном защищенном ключевом носителе.

Ключи ЭП — закрытый и открытый ключи, которые вместе составляют ключевую пару. Создание (генерация) ключевой пары выполняется криптографическим программным обеспечением , оно может быть установлено в точке выдачи УЦ, у вас на компьютере и в самом ключевом носителе.
Закрытый ключ никому разглашать нельзя. Если его кто-то узнал, то он может подписать любой документ от вашего имени.
Открытый ключ можно показывать всем. Его значение (это просто длинное число) заносится в сертификат ключа проверки электронной подписи (он же просто «сертификат»), который потом используется при проверке вашей подписи под документом.

Сертификат ЭП выдает Удостоверяющий Центр (УЦ). Форма сертификата КЭП соответствует требованиям Приказа ФСБ РФ № 795.
Главная задача УЦ — достоверно определить, что вы – это вы. Для того, чтобы при обмене документами в электронном виде люди точно знали, что подпись, сделанная с использованием вашего сертификата — поставлена именно вами.

Ключи ЭП вместе с сертификатом составляют контейнер ЭП (ключевой контейнер).

Разновидность ключей электронной подписи

Извлекаемые ключи ("пассивные контейнеры")

Создаются с помощью программного ГОСТ-криптопровайдера, который устанавливается в операционную систему (ОС).

Контейнеры ГОСТ-криптопровайдеров можно хранить в виде файлов на флеш-накопителях, жестком диске и реестре компьютера или на специализированном ключевом носителе, защищенном PIN-кодом.

Когда ключевые контейнеры хранятся как обычные файлы, возможности анализа, копирования или удаления никак не ограничены, а значит скопировать и удалить их может кто угодно. Поэтому безопаснее хранить ключевые контейнеры на специализированном, защищенном ключевом носителе (смарт-карте или токене), защищенном PIN-кодом. Именно этот вариант мы и будем рассматривать дальше.

Чтобы криптопровайдер (СКЗИ) смог получить доступ к содержимому защищенного ключевого носителя, нужно физически иметь в распоряжении ключевой носитель и знать PIN-код. Все операции с закрытым ключом выполняются в оперативной памяти компьютера.

Т. е. во время операций с закрытым ключом, после ввода правильного PIN-кода, закрытый ключ временно извлекается в оперативную память компьютера.

Таким образом, извлекаемые **экпортируемые** ключи — это ключи, которые можно скопировать на другой носитель средствами программного криптопровайдера.

А извлекаемые **неэкспортируемые** ключи — это ключи с запретом копирования стандартными средствами программного криптопровайдера.

Защита от копирования реализуется внутренними программными механизмами самого криптопровайдера. При этом техническая возможность скопировать контейнер (закрытый ключ) остается. При формировании или импорте контейнера на ключевой носитель может быть установлен запрет на процедуру копирования, такие контейнеры (и закрытые ключи в них) называются неэкспортируемыми. Впоследствии этот параметры изменить нельзя.

Неизвлекаемые ключи ("активные контейнеры")

Создаются с использованием встроенных аппаратных криптографических механизмов внутри специализированных ключевых носителей. Для генерации ключей используется криптографическое ядро внутри микроконтроллера устройства. Такие ключи ЭП хранятся не просто в защищенной памяти с доступом по PIN-коду, но и в специальном типе файлов, с которым умеет работать только криптоядро устройства. При работе с подписью все операции производятся внутри токена, и закрытый ключ никогда не копируется из памяти микроконтроллера.

Неизвлекаемые ключи бывают разного формата: **PKCS#11 и “ФКН-ключ”**.

Используя стандартизированный программный интерфейс (API) библиотеки **PKCS#11,** приложение, или программный криптопровайдер, напрямую работает с криптоядром ключевого носителя.

У носителей, которые называются ФКН (функциональный ключевой носитель) есть возможность работать с неизвлекаемыми **“ФКН-ключами”.** Такие носители и криптопровайдер на компьютере, для передачи PIN-кода и другого обмена (в т.ч. данными, которые подписываются), строят защищенный канал. Для этого используется протокол SESPAKE (протокол выработки общего ключа с аутентификацией на основе пароля). Выработка ключа -- задача устройства ФКН и криптопровайдера на компьютере, поэтому на компьютере также должна быть установлена версия КриптоПро CSP, поддерживающая SESPAKE.

Неэкспортируемый ключ ≠ неизвлекаемый ключ.

Неэкспортируемые ключи ЭП ненадолго извлекаются в оперативную память компьютера при работе с ними программного криптопровайдера. При этом копирование неизвлекаемых ключей полностью исключено.

Доступ к закрытому ключу

Для доступа к ключевому контейнеру при работе с любыми защищенными ключевыми носителями **обязательно требуется ввести правильный PIN-код Пользователя**. PIN-код может не быть длинным и сложным – это компенсируется требованием физического владения устройством и ограничениями на перебор PIN-кода. После определенного количества неудачных попыток ввода PIN-кода доступ к содержимому токена или смарт-карты блокируется. Это защищает от случайного подбора PIN-кода. Очень важно установить уникальный PIN-код, который будет сложно подобрать.

Теперь поговорим о том, какие бывают ключевые носители.

Виды защищенных ключевых носителей

Пассивные ключевые носители

Выступают в роли защищенного хранилища для извлекаемых ключей. То есть программный криптопровайдер генерирует ключи, записывает их в защищенную PIN-кодом память устройства и впоследствии работает с ними. Пример такого носителя – **Рутокен Lite**.

Активные ключевые носители

Могут выступать в роли пассивного ключевого носителя, что снижает безопасность использования ключа ЭП. Но главное их отличие в том, что они являются самостоятельным СКЗИ, если использовать функции аппаратного криптоядра устройства -- встроенного микрокомпьютера. Ключи сгенерированные в криптоядре - неизвлекаемые и вся работа с закрытым ключом (в т. ч. формирование ЭП) будет производиться внутри носителя. Активные ключевые носители еще называют криптографическими ключевыми носителям

Пример активного носителя — **Рутокен ЭЦП 3.0 3220**.

Функциональный ключевой носитель (ФКН)

Это активный носитель, дополнительно имеющий реализацию протокола SESPAKE для построения защищенного канала между криптопровайдером и токеном.

Пример такого устройства — **Рутокен ЭЦП 3.0 3220**, который также поддерживает активный и пассивный режимы.

Важно понимать

1) Криптографические возможности активных и ФКН-носителей ≠ встроенный КриптоПро CSP. Если требуется работа с КриптоПро CSP, нужно приобрести лицензию на этот продукт. Вне зависимости от вида ключевого носителя и формата ключей ЭП на нем.

2) Конвертация ключей из одного формата в другой невозможна. Если ключи были созданы извлекаемыми, то их нельзя перевести в формат неизвлекаемых ключей и наоборот.

Средства генерации ключевых пар

Рассмотрим с помощью каких средств криптографической защиты информации (СКЗИ) можно генерировать и использовать разные форматы ключей, на примере устройств Рутокен:

Извлекаемые ключи ("пассивные контейнеры")

- **СКЗИ КриптоПро CSP версии 4.0 и новее**. При генерации нужно выбрать "режим CSP". Ключи будут созданы в защищённой памяти любой из моделей Рутокен.
- При использовании **СКЗИ VipNet CSP или Signal-COM CSP**, режим выбирать не надо: извлекаемые ключи будут созданы на пассивных ключевых носителях.

Неизвлекаемые ключи ("активные контейнеры")

Генерируются на активных и ФКН носителях, с использованием стандартизированного программного интерфейса (API) библиотеки PKCS#11.
Например, вся линейка продуктов Рутокен ЭЦП 3.0 содержит в себе возможности аппаратной криптографии.

Для генерации ключей формата **PKCS#11** можно использовать инструменты от компании Актив:

- **Генератор запроса на сертификат** из комплекта Драйверов Рутокен.
- **Рутокен SDK,** содержащий примеры использования кроссплатформенной библиотеки rtpkcs11ecp).

Или воспользоваться программными ГОСТ-криптопровайдерами:

- **СКЗИ КриптоПро CSP версии 5.0 R2 и новее** - при генерации ключей надо выбрать режим "Активный токен".
- **СКЗИ Signal-COM CSP** или **VipNet CSP** - на активные ключевые носители из линейки Рутокен ЭЦП 3.0 автоматически генерируются неизвлекаемые ключи.

ФКН-ключи

Для того, чтобы сгенерировать ключи ФКН с защитой канала нужно использовать модели линейки Рутокен ЭЦП 3.0 - именно эти модели имеют поддержку протокола SESPAKE. Важно так же, что для работы и генерации ключей в таком формате подойдет версия **КриптоПро CSP 5.0 и новее**.

Сертификация устройств

Немного о сертификации ключевых носителей.

Для того, чтобы электронная подпись юридически считалась квалифицированной, средство криптографической защиты информации (СКЗИ), с помощью которого производится генерация ключей и последующая работа с ключами ЭП, должно быть сертифицировано в ФСБ России.

Чтобы проще было запомнить:

- ФСТЭК России сертифицирует средство защиты информации (устройство).
- ФСБ России сертифицирует средство криптографической защиты информации (СКЗИ).

Таким образом, в случае с **извлекаемыми ключами**, сгенерированными с помощью программного СКЗИ, в ФСБ России должен быть сертифицирован именно программный ГОСТ-криптопровайдер. А пассивный носитель Рутокен должен быть сертифицирован во ФСТЭК России.

В **случае с неизвлекаемыми ключами** на активном или ФКН-носителе, так как при генерации ключей используется аппаратная криптография, сертифицированным в ФСБ России должен сам носитель.

Заключение

Для надежной защиты ключей ЭП от копирования и перехвата мы рекомендуем использовать активные носители с возможностью генерации неизвлекаемых ключей на "борту", такие как Рутокен ЭЦП 3.0 3220. Так ваша электронная подпись будет максимально защищена.