КриптоПро Ключ

Описание функциональных характеристик

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CRL	—	Список отзыва сертификатов (Certificate Revocation List)
CSP	—	Криптопровайдер (Cryptographic Service Provider)
HSM	—	Аппаратный модуль системы безопасности (Hardware security module)
OAuth	—	Открытый протокол авторизации, который позволяет предоставить третьей стороне ограниченный доступ к защищенным ресурсам пользователя без необходимости передавать ей (третьей стороне) логин и пароль (Open Authorization)
OCSP	—	Протокол получения статуса сертификата в реальном времени (Online Certificate Status Protocol)
REST	—	Архитектурный стиль построения распределенного приложения (Representational State Transfer)
SDK	—	Набор программных компонентов для использования в мобильных приложениях (Software development kit)
TLS	—	Протокол защиты транспортного уровня (Transport Layer Security)
URL	—	Единый указатель ресурсов (Uniform Resource Locator)
АРМ	—	Автоматизированное рабочее место
БД	—	База данных
ИС	—	Информационная система
НСД	—	Несанкционированный доступ
МП	—	Мобильное приложение
МЭ	—	Межсетевой экран
ОС	—	Операционная система
ПАК	—	Программно-аппаратный комплекс
ПАКМ	—	Программно-аппаратный криптографический модуль
ПО	—	Программное обеспечение
ППО	—	Прикладное программное обеспечение
СКЗИ	—	Средство криптографической защиты информации
СУБД	—	Система управления базой данных
УЦ	—	Удостоверяющий Центр
ЭП	—	Электронная подпись

Аннотация

В данном документе приведено назначение КриптоПро Ключ, его функциональные характеристики и основные компоненты. Дополнительно приведено описание основных процессов, реализующих перечисленные функции.

1. Общие сведения

1.1. Назначение КриптоПро Ключ

Программный комплекс КриптоПро Ключ (далее — КриптоПро Ключ) предназначен для:

- Централизованного, распределенного и гибридного защищенного хранения закрытых ключей Пользователей (в соответствии с выбранным режимом хранения ключей, см. раздел 4);
- Удаленного выполнения операций Пользователей по созданию электронной подписи;
- Удаленного выполнения операций Пользователей по шифрованию и расшифрованию документов;
- Удаленного выполнения операций Пользователей по проверке электронной подписи.

1.2. Цели КриптоПро Ключ

Целями использования КриптоПро Ключ являются:

- Обеспечение конфиденциальности документов;
- Обеспечение целостности документов;
- Обеспечение аутентичности (подлинности) документов;
- Обеспечение юридически значимого электронного документооборота за счет использования электронной подписи документов.

1.3. Задачи КриптоПро Ключ

Для выполнения поставленных целей КриптоПро Ключ решает следующие задачи:

- Ведение реестра зарегистрированных Пользователей:
- Выполнение процедуры регистрации Пользователя в централизованном режиме с прибытием регистрируемого Пользователя в офис обслуживания;
- Выполнение процедуры удаления Пользователей из реестра Пользователей по запросам Оператора Сервера Электронной Подписи;
- Выполнение процедуры аутентификации Пользователей;
- Выполнение процедуры генерации ключей ЭП, их сохранения в защищенном виде и установки в мобильное приложение или на отчуждаемый носитель (если необходимо);
- Аудит событий, связанных с эксплуатацией программного комплекса.
- Реализацию системы оповещения Пользователей с использованием SMS-сообщений, сообщений электронной почты и PUSH-уведомлений в соответствии с описанием схемы размещения компонентов.
- Оповещение Пользователей о событиях при взаимодействии с КриптоПро Ключ (аутентификация, смена пароля на вход и т.д.);
- Оповещение Пользователей об операциях с ключами ЭП (генерация ключей, создание ЭП документа и т.д.);
- Визуализация (конвертация и отображение) документа для Пользователя перед выполнением операции с документом.

2. Описание КриптоПро Ключ

2.1. Состав КриптоПро Ключ

КриптоПро Ключ включает в себя следующие компоненты:

- Центр Идентификации (ЦИ, см. раздел 2.2.1):
  - Веб-интерфейс ЦИ;
  - Служба управления Пользователями;
  - Служба маркеров безопасности;
  - Сервис рассылки уведомлений;
  - БД ЦИ.
- Сервис Подписи (см. раздел 2.2.2):
  - ПО Сервиса Подписи;
  - КриптоПро TSP Client (Компонент из состава ПАК «Службы УЦ 2.0», используется опционально и при наличии действующего сертификата, выданного ФСБ России);
  - КриптоПро OCSP Client (Компонент из состава ПАК «Службы УЦ 2.0», используется опционально и при наличии действующего сертификата, выданного ФСБ России);
  - КриптоПро HSM Client;
  - БД Сервиса Подписи.
- Веб-интерфейс Пользователя (см. раздел 2.2.3);
- Сервис Аудита (см. раздел 2.2.4):
  - ПО Сервиса Аудита;
  - Веб-интерфейс Сервиса Аудита;
  - БД Сервиса Аудита.
- Сервис Обработки Документов (см. раздел 2.2.5);
- Сервис взаимодействия с мобильным приложением (МП) (см. раздел 2.2.7);
- ПАКМ «КриптоПро HSM» (см. раздел 2.2.6);
- Клиентские компоненты (см. раздел 2.2.8):
  - КриптоПро CSP/JCP/Cloud CSP;
  - КриптоПро SDK для встраивания в мобильное приложение;

Не все указанные компоненты являются обязательными. В минимальную конфигурацию КриптоПро Ключ входят Сервис Подписи, Центр Идентификации, Сервис Аудита и ПАКМ «КриптоПро HSM». Веб-интерфейс Пользователя может быть заменен интерфейсом информационной системы, с которой интегрируется КриптоПро Ключ. Сервис Обработки Документов, Сервис Взаимодействия с МП является опциональным компонентом. Установщик КриптоПро Ключ позволяет выбрать и установить нужные компоненты. КриптоПро CSP, TSP Client, OCSP Client и HSM Client входят в комплект поставки. ПАКМ «КриптоПро HSM» поставляется отдельно.

2.2. Описание компонентов КриптоПро Ключ

2.2.1. Центр Идентификации

Компонент Центр Идентификации предназначен для регистрации и аутентификации Пользователей, а также подтверждения волеизъявления Пользователя об операциях с его ключами. В случае успешной аутентификации выдается электронный идентификатор, который затем может быть использован для доступа к Сервису Подписи

или для управления Центром Идентификации. Взаимодействие с Центром Идентификации осуществляется с использованием REST API.

К функциям ЦИ относятся:

- Регистрация Пользователей в личном кабинете Оператором.
- Обеспечение аутентификации Пользователей и Операторов при обращении к КриптоПро Ключ.
- Ведение базы данных, содержащей информацию о Пользователях ЦИ:
  - данные о Пользователях, включаемые в сертификаты;
  - данные о Пользователях, не включаемые в сертификаты (номер мобильного телефона, идентификатор OTP-токена (one-time password см. «Используемые сокращения и обозначения») и т.п.).
- Генерация событий для Сервиса Аудита (см. раздел 2.2.4).

Центр Идентификации состоит из нескольких компонентов, которые реализуют перечисленные функции.

Веб-интерфейс ЦИ

Центр Идентификации имеет собственный веб-интерфейс, на котором осуществляется регистрация и/или аутентификация Пользователя и Оператора. У Пользователя и у Оператора есть личный кабинет.

В своем личном кабинете Пользователь может изменять информацию профиля и настраивать методы первичной и вторичной аутентификации. При наличии установленного и настроенного компонента «Сервис Аудита» Пользователю доступен просмотр операций, совершенных им в системе.

Оператор в своем личном кабинете может добавлять и удалять Пользователей, генерировать запросы к УЦ на сертификаты для них, изменять информацию о профилях Пользователей и настраивать способы их аутентификации. При наличии установленного и настроенного компонента «Сервис Аудита» Оператору доступен просмотр операций всех Пользователей, относящихся к группам, Оператором которых он является.

Служба управления Пользователями

Служба управления Пользователями является обособленной частью Центра Идентификации и отвечает за регистрацию Пользователей и Операторов КриптоПро Ключ, а также за запись, хранение, обработку и удаление данных их учетных записей.

Служба маркеров безопасности

Служба управления Пользователями является обособленной частью Центра Идентификации и отвечает за аутентификацию Пользователей и Операторов при обращении к КриптоПро Ключ.

Сервис рассылки уведомлений

Сервис рассылки уведомлений является центральным узлом, где обрабатываются события, поступающие от других компонентов КриптоПро Ключ. В зависимости от

настроек, Сервис рассылки уведомлений формирует SMS-, Email- и PUSH-уведомления, рассылаемые Пользователям и Операторам.

2.2.2. Сервис Подписи

Компонент КриптоПро Ключ Сервис Подписи предназначен для выполнения операций по шифрованию документов, созданию электронной подписи и ее проверки. Взаимодействие с Сервисом Подписи осуществляется с использованием REST API.

К функциям Сервиса Подписи относятся:

- Обращение к HSM для создания ключа.
- Создание запроса к УЦ на сертификат.
- Создание электронной подписи под документами, загружаемыми Пользователем.
- Шифрование и расшифрование документов, загружаемых Пользователем.
- Ведение БД, содержащей зашифрованные закрытые ключи и сертификаты открытых ключей зарегистрированных в системе Пользователей (при соответствующем режиме хранения ключей).
- Обеспечение доступа к Сервису Подписи внешним приложениям через SOAP-интерфейс на базе HTTP(S).
- Генерация событий для сервиса Аудита.

Сервис Подписи состоит из нескольких компонентов, которые реализуют перечисленные функции.

ПО Сервиса Подписи

ПО Сервиса Подписи предоставляет Пользователям программный интерфейс для создания запросов на сертификат, установки сертификатов, подписи и шифрования документов.

КриптоПро TSP Client

Клиент служб штампов времени «КриптоПро TSP Client» предназначен для обращения к серверу «КриптоПро TSP Server» по протоколу TSP поверх HTTP, получения от него штампов времени (меток времени), обработки и работы с запросами на штампы времени и непосредственно со штампами времени. Подробная информация о TSP-клиенте содержится в составе документации на ПАК «КриптоПро УЦ 2.0».

КриптоПро OCSP Client

Клиент служб актуальных статусов сертификатов «КриптоПро OCSP Client» предназначен для обращения к серверу «КриптоПро OCSP Server» по протоколу OCSP поверх HTTP, получения от него OCSP-ответов, обработки и работы с OCSP-запросами и OCSP-ответами. Подробнее о OCSP-клиенте можно прочитать в составе документации на ПАК «КриптоПро УЦ 2.0».

КриптоПро HSM Client

Операции создания электронной подписи, шифрования и расшифрования документов выполняются Сервисом Подписи при взаимодействии с ПАКМ «КриптоПро HSM» посредством клиента ПАКМ «КриптоПро HSM» по отдельному сегменту

локальной сети с использованием защищенного сетевого протокола. Компонент «КриптоПро HSM Client» является ответной частью, устанавливаемой на рабочие станции и серверы, необходимой для трансляции криптографических вызовов к ПАКМ «КриптоПро HSM».

2.2.3. Веб-интерфейс Пользователя

Компонент КриптоПро Ключ Веб-интерфейс Пользователя предназначен для организации интерактивного взаимодействия Пользователей с компонентами КриптоПро Ключ, а также с другими внешними компонентами. Произведенные Пользователями действия на веб-формах с помощью REST API передаются в другие компоненты КриптоПро Ключ и обрабатываются их серверными программными модулями. Также для Веб-интерфейса Пользователя доступно взаимодействие с помощью программного интерфейса.

В Веб-интерфейсе Пользователя Пользователю могут быть доступны следующие разделы:

- **Подписать.** В данном разделе Пользователь может создать электронную подпись документа, выбрать сертификат для этой подписи, а также загрузить сам подписываемый документ.
- **Усовершенствовать подпись.** В данном разделе можно усовершенствовать уже имеющуюся ЭП – добавить к ней штамп времени (CAdES-T), либо штамп времени и доказательство подлинности подписи (CAdES-X Long Type 1).
- **Зашифровать.** В данном разделе Пользователь может загрузить документ и выбрать сертификат, на котором будет производиться шифрование.
- **Расшифровать.** В данном разделе можно расшифровать зашифрованный документ. Требуется загрузить подлежащий расшифрованию документ, а система автоматически произведет поиск сертификата(-ов), на котором(-ых) можно расшифровать документ, из имеющихся у Пользователя.
- **Проверить подпись.** В данном разделе Пользователь может загрузить подписанный документ и узнать статус его подписи (действительна/недействительна), а также узнать сведения о сертификате, на котором подписывался документ. Возможность проверки ЭП доступна только при условии настроенного взаимодействия со службой проверки сертификатов и электронной подписи КриптоПро SVS 2.0 (может использоваться опционально при наличии продукта Службы УЦ версии 2.0).
- **Проверить сертификат.** В данном разделе Пользователь может загрузить сертификат, статус которого ему нужно проверить. Возможность проверки сертификата доступна только при условии настроенного взаимодействия со службой проверки сертификатов и электронной подписи КриптоПро SVS 2.0 (может использоваться опционально при наличии продукта Службы УЦ версии 2.0).
- **Сертификаты.** В данном разделе Пользователю доступен список имеющихся у него сертификатов. Также он может устанавливать и удалять сертификаты, генерировать запрос на создание нового. К этому разделу Веб-интерфейса получает доступ Оператор, если создает сертификат за Пользователя.
- **Аудит.** В данном разделе отображаются операции, совершенные Пользователем в КриптоПро Ключ. Каждый Пользователь видит только свои операции. К списку операций можно применять фильтры по коду и/или дате события. Возможность просмотра событий аудита доступна только после установки и настройки Администратором компонента Сервис Аудита в КриптоПро Ключ.

Оператор взаимодействует с Веб-интерфейсом Пользователя только во время генерации запроса на сертификат от имени Пользователя. При выборе этой опции в личном кабинете Оператора происходит перенаправление на веб-форму Веб-интерфейса Пользователя, где Оператор заполняет поля сертификата и отправляет запрос в УЦ.

2.2.4. Сервис Аудита

Компонент Сервис Аудита предназначен для аудита событий, поступающих с компонентов КриптоПро Ключ. Сервис Аудита состоит из службы записей событий аудита, веб-интерфейса аудита и БД аудита. Служба записей событий аудита получает список записей аудита с других компонентов КриптоПро Ключ (в зависимости от настроек сбора событий) и записывает эти события в БД. С помощью веб-интерфейса аудита Пользователи и Операторы аудита могут просматривать события аудита, а также формировать специализированные отчеты.

2.2.5. Сервис Обработки Документов

Сервис Обработки Документов (СОД) предназначен для работы с документами, отправленными на подпись или шифрование/расшифрование в КриптоПро Ключ. Сервис Обработки Документов выполняет следующие задачи:

- обработка документов для отображения полного текста документа в мобильном приложении;
- преобразование документов в различные форматы:
  - преобразование документов для отображения печатной формы документа;
  - преобразование документов для отображения краткой информации о документе;
- загрузка и хранение документов в БД Сервиса Обработки Документов;
- выгрузка подписанных (зашифрованных, расшифрованных) документов из БД Сервиса Обработки Документов.

2.2.6. ПАКМ «КриптоПро HSM»

Программно-аппаратный криптографический модуль (ПАКМ) «КриптоПро HSM» предназначен для выполнения криптографических операций над данными.

ПАКМ «КриптоПро HSM» является необходимым элементом архитектуры КриптоПро Ключ и должен устанавливаться в соответствии с процедурой, описанной в документе «ЖТЯИ.00096-02 95 01 КриптоПро HSM. Правила пользования», входящем в комплект поставки ПАКМ «КриптоПро HSM».

К функциям ПАКМ «КриптоПро HSM» относятся:

- Создание и проверка электронной цифровой подписи в соответствии с ГОСТ Р 34.10–2001 и ГОСТ Р 34.10–2012.
- Вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11–2012 и ГОСТ Р 34.11–94.
- Шифрование и расшифрование блоков данных в соответствии с ГОСТ 28147–89.
- Вычисление имитовставки блоков данных в соответствии с ГОСТ 28147–89.
- Генерация и защищенное хранение ключевой информации.
- Управление учетными записями Пользователей ПАКМ.

2.2.7. Сервис Взаимодействия с МП

Сервис взаимодействия с МП для мобильного приложения (DSS Api Gateway) предоставляет доступ к компонентам КриптоПро Ключ при взаимодействии с ними через мобильное приложение на базе КриптоПро SDK.

2.2.8. Клиентские компоненты

КриптоПро CSP/JCP/Cloud CSP

СКЗИ «КриптоПро CSP» может применяться Пользователем для установления безопасного соединения с серверами КриптоПро Ключ при аутентификации по логину и паролю, а также по сертификату.

Аналогично, СКЗИ «КриптоПро JCP» может применяться Пользователем для установления безопасного соединения с серверами КриптоПро Ключ при аутентификации по логину и паролю, а также по сертификату.

Модуль Cloud CSP входит в состав КриптоПро CSP версии 5.0. Cloud CSP предоставляет возможность любому приложению, использующему вызовы Microsoft CryptoAPI 2.0, подписывать электронные документы и выполнять другие криптографические операции на ключах Пользователей, находящихся в КриптоПро Ключ, а также генерировать ключи Пользователей и создавать запросы на сертификат. Дополнительно Cloud CSP предоставляет возможность использовать ключи, хранимые в КриптоПро Ключ, для аутентификации клиента в рамках взаимодействия по протоколу TLS во всех сценариях, поддерживаемых КриптоПро CSP версии 5.0.

КриптоПро SDK для встраивания в мобильное приложение

КриптоПро SDK для встраивания в мобильное приложение представляет собой набор программных компонентов для использования в мобильных приложениях, который позволяет производить удаленное выполнение операций подписи и управление сертификатами, а также подтверждать операции Пользователя в КриптоПро Ключ, инициированные другими способами. Возможности создания мобильных приложений на базе КриптоПро SDK описаны в разделе 2.3.

2.3. Возможности создания мобильных приложений, использующих КриптоПро Ключ

Использование КриптоПро SDK подразумевает встраивание в мобильное приложение, что позволяет осуществлять работу с КриптоПро Ключ в собственных приложениях. КриптоПро SDK предоставляет разработчикам мобильных приложений возможность работы с КриптоПро Ключ следующим образом.

1. Обмен данными между мобильным приложением на базе КриптоПро SDK и КриптоПро Ключ осуществляется через защищенное соединение, что дает возможность подписывать конфиденциальные документы без защиты канала дополнительным средствами (например, VPN-решениями соответствующего класса защиты).
2. Подтверждение операций требует ввода ПИН-кода Пользователем. Данный код может быть введен один раз за сеанс работы с приложением.

3. Документы для создания ЭП могут быть загружены как с мобильного устройства Пользователя, так и со стороны сервера.
4. Возможна подпись нескольких документов в составе единого пакета. При этом Пользователь имеет возможность просмотреть каждый из документов в пакете, а подтвердить операцию требуется только один раз.
5. Перед подтверждением подписи документов Пользователь просматривает краткие сведения о документах и имеет возможность увидеть печатную форму каждого документа, а также его исходный вид.
6. Многостраничные документы загружаются по одной странице. Данная особенность позволяет снизить нагрузку на каналы связи и упростить работу с приложением.
7. К одной учетной записи Пользователя могут быть привязаны несколько мобильных устройств с установленным и инициализированным приложением на базе КриптоПро SDK, каждое из которых может использоваться для подтверждения операций.
8. В мобильном приложении возможно управление сертификатами Пользователя.

Использование КриптоПро SDK осуществляется следующим образом. DSS SDK встраивается в мобильное приложение в соответствии с руководствами разработчика из комплекта документации. Встраивание должно производиться с учетом ограничений, описанных в «ЖТЯИ.00096-02 95 01. КриптоПро HSM. Правила пользования». Мобильное приложение на базе КриптоПро SDK должно предоставлять Пользователю информацию о всех мобильных устройствах, привязанных к его учетным записям в КриптоПро Ключ.

3. Описание процессов в КриптоПро Ключ

В данном разделе представлено описание основных процессов, обеспечиваемых КриптоПро Ключ. Основными процессами являются:

- Регистрация Пользователя и создание запроса на сертификат (см. раздел 3.1);
- Подпись документа (см. раздел 3.2);
- Шифрование документа (см. раздел 3.3);
- Расшифрование документа (см. раздел 3.4);
- Аудит событий и формирование отчетов (см. раздел 3.5).

Описание наиболее сложных процессов, где присутствует несколько участников или большое количество операций, дополнено функциональными диаграммами, иллюстрирующими основные этапы взаимодействия участников.

Диаграммы актуальны при условии использования компонента «Веб-интерфейс Пользователя» и наличия ПАКМ «КриптоПро HSM».

3.1. Регистрация Пользователя и создание запроса на сертификат

Работа с КриптоПро Ключ доступна только зарегистрированным Пользователям. Для этого Пользователь проходит регистрацию в Центре Идентификации самостоятельно (при наличии соответствующих административных настроек), либо получает учетные данные для входа от своего Оператора, который уже зарегистрировал Пользователя в системе. Также на данном этапе необходимо настроить для Пользователя способ аутентификации. По окончании регистрации сведения о профиле Пользователя и данные аутентификации заносятся в БД ЦИ.

Для создания электронной подписи и выполнения других операций в КриптоПро Ключ Пользователю необходим сертификат. КриптоПро Ключ позволяет создавать запрос на сертификат, который впоследствии может быть загружен и/или распечатан для последующей его передачи в удостоверяющий центр. Запрос на сертификат для Пользователя заполняет Оператор в личном кабинете, либо сам Пользователь при помощи специальной формы на Веб-интерфейсе Пользователя в разделе «Сертификаты». В процессе заполнения полей запроса на сертификат необходимо заполнить компоненты имени (возможно автоматическое заполнение некоторых полей при условии наличия нужной информации в профиле Пользователя), а также выбрать УЦ и шаблон сертификата. На основе введенных данных КриптоПро Ключ генерирует запрос на сертификат.

Пример последовательности шагов процесса регистрации Пользователя и создания запроса на сертификат представлен на Рис. 1. В данном случае предполагается, что регистрацию Пользователя и заполнение полей запроса на сертификат выполняет Оператор.

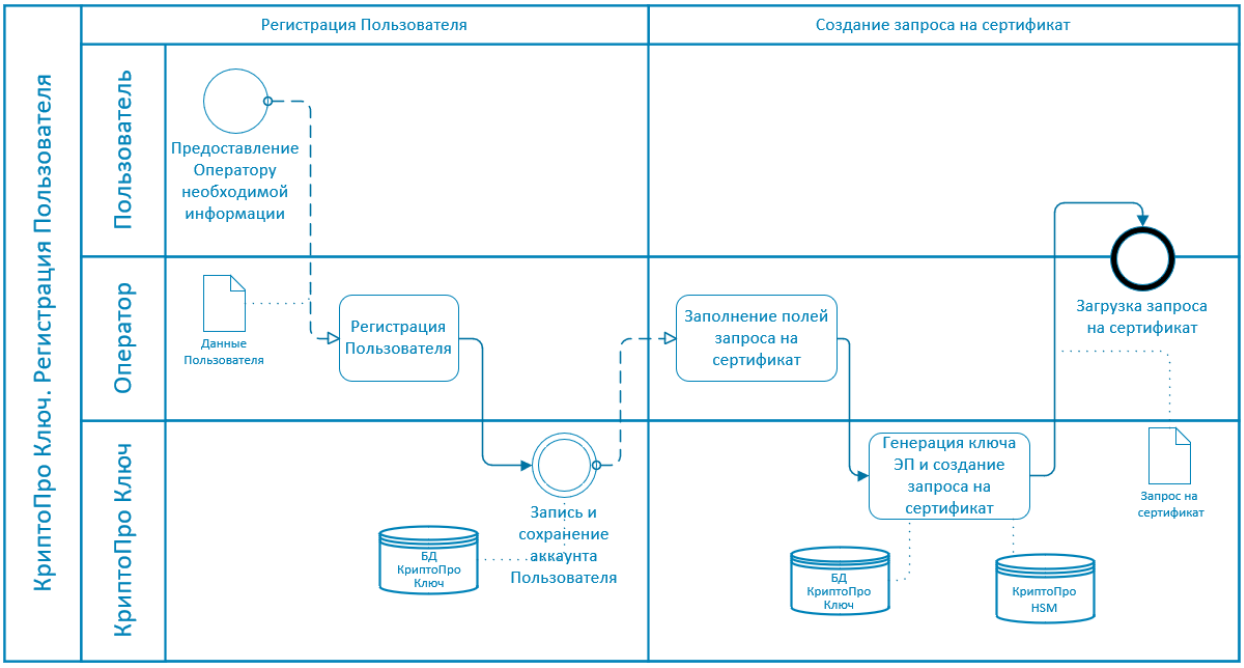

Рис. 1 — Регистрация Пользователя и создание запроса на сертификат

3.2. Подпись документа

Подпись документов является одним из основных процессов, поддерживаемых КриптоПро Ключ. В зависимости от настроек, подпись может выполняться как с использованием HTTP-API (в этом случае необходимо использовать компонент Веб-интерфейс Пользователя), так и посредством SOAP/REST (в этом случае используется программный интерфейс КриптоПро Ключ). При выполнении операции подписи могут быть использованы различные способы аутентификации. В данном разделе приведено описание процесса подписи документа с аутентификацией с помощью мобильного приложения.

Пользователь инициирует операцию подписи при помощи кнопки «Подписать» на Веб-интерфейсе Пользователя, в мобильном приложении или при помощи программного интерфейса интегрируемой системы, выбирает нужный сертификат ЭП, подписываемый документ, параметры и формат подписи. Данная информация отправляется в КриптоПро Ключ. КриптоПро Ключ проверяет полученные данные, подготавливает документ для дальнейших действий и отправляет в мобильное приложение PUSH-уведомление с просьбой подтвердить операцию. Пользователь убеждается, что хочет выполнить действия с нужным документом и подтверждает операцию. Если операция подтверждена Пользователем, КриптоПро Ключ (при участии мобильного приложения, если ключ хранится в нем, см. раздел 4) подписывает документ и возвращает его Пользователю в веб-интерфейсе или мобильном приложении. В общем виде шаги процесса подписи с подтверждением при помощи мобильного приложения представлены на Рис. 2.

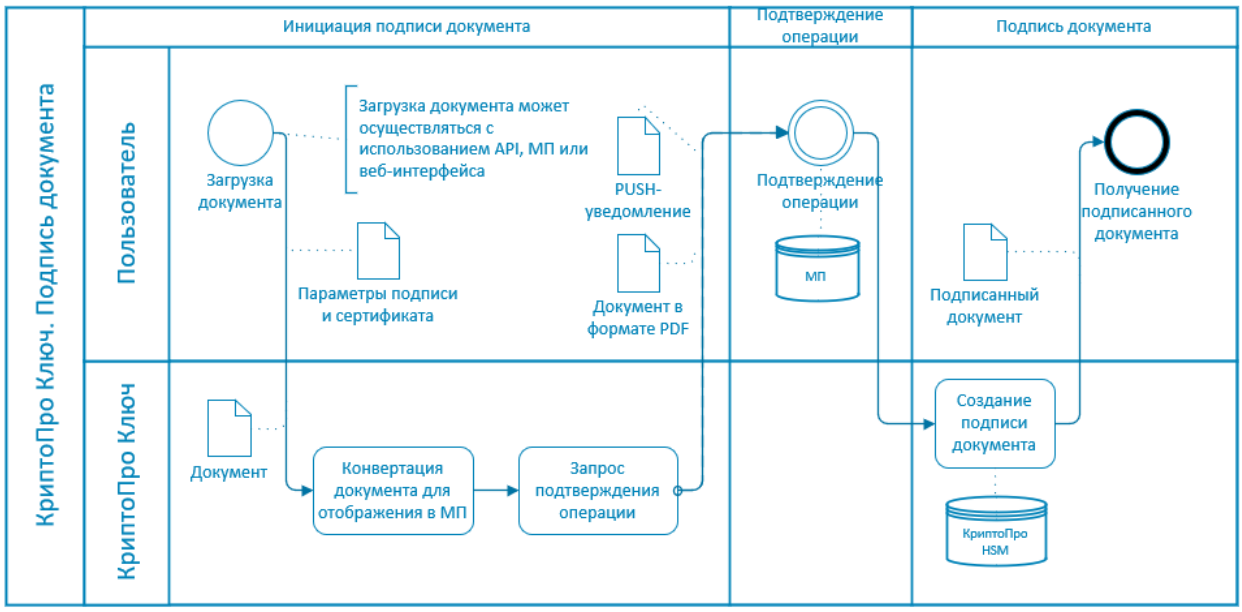

Рис. 2 — Подпись документа

3.3. Шифрование документа

Шифрование документов является одним из основных процессов, поддерживаемых в КриптоПро Ключ. В зависимости от настроек, шифрование может выполняться как с использованием HTTP-API (в этом случае необходимо использовать компонент Веб-интерфейс Пользователя), так и посредством SOAP/REST (в этом случае используется программный интерфейс КриптоПро Ключ).

Как и в случае с подписью документа, Пользователь инициирует операцию шифрования при помощи кнопки «Зашифровать» на Веб-интерфейсе Пользователя или при помощи программного интерфейса интегрируемой системы, выбирает нужный сертификат ЭП и документ, после чего происходит обращение к Сервису Подписи. Сервис Подписи находит сертификат в своей БД и инициализирует сессию с HSM с помощью КриптоПро HSM Client. КриптоПро HSM Client передает в HSM документ в виде массива байт, а HSM зашифровывает документ и возвращает на Сервис Подписи. Сервис Подписи отправляет зашифрованный документ Пользователю.

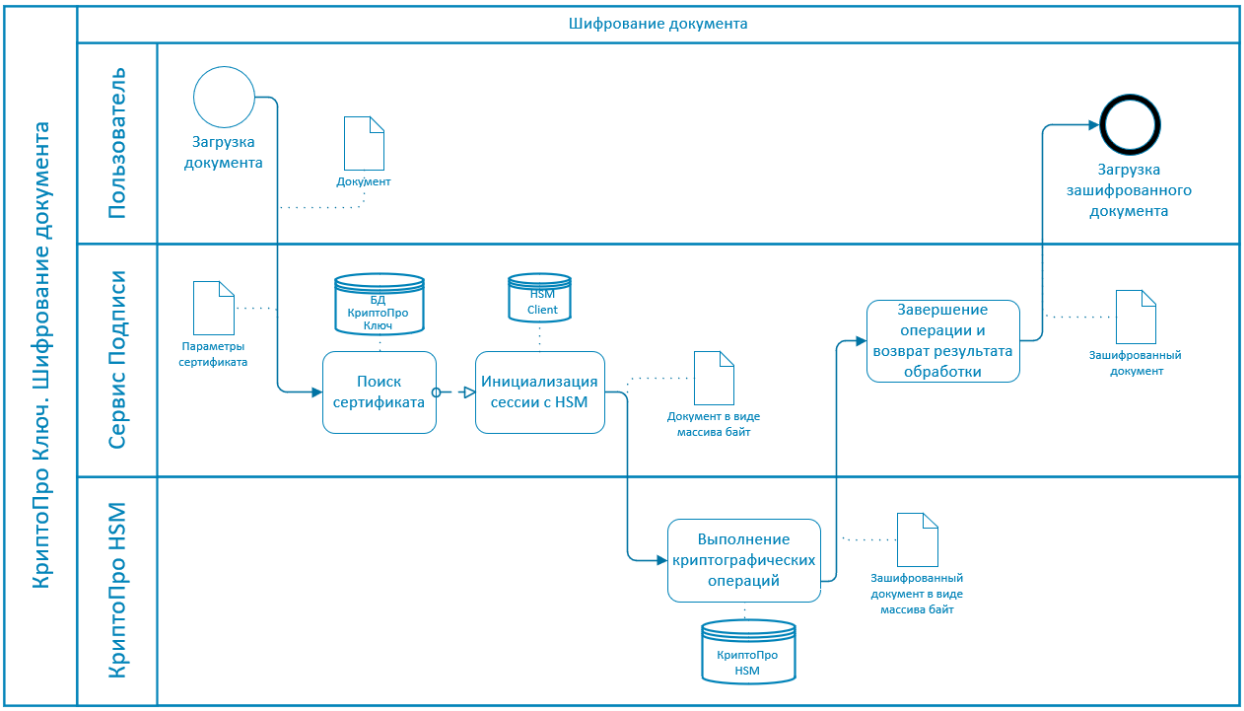

Рис. 3 — Шифрование документа

3.4. Расшифрование документа

Пользователь инициирует операцию расшифрования при помощи кнопки «Расшифровать» на Веб-интерфейсе Пользователя или при помощи программного интерфейса интегрируемой системы, выбирает нужный документ, после чего происходит обращение к Сервису Подписи, где осуществляется поиск сертификата(-ов) Пользователя, на которых документ можно расшифровать. После того, как Пользователь выбрал сертификат, на котором будет производиться расшифрование, Сервис Подписи инициализирует сессию с HSM с помощью КриптоПро HSM Client. КриптоПро HSM Client передает в HSM зашифрованный документ в виде массива байт, а HSM расшифровывает документ и возвращает на Сервис Подписи. Сервис Подписи отправляет документ Пользователю.

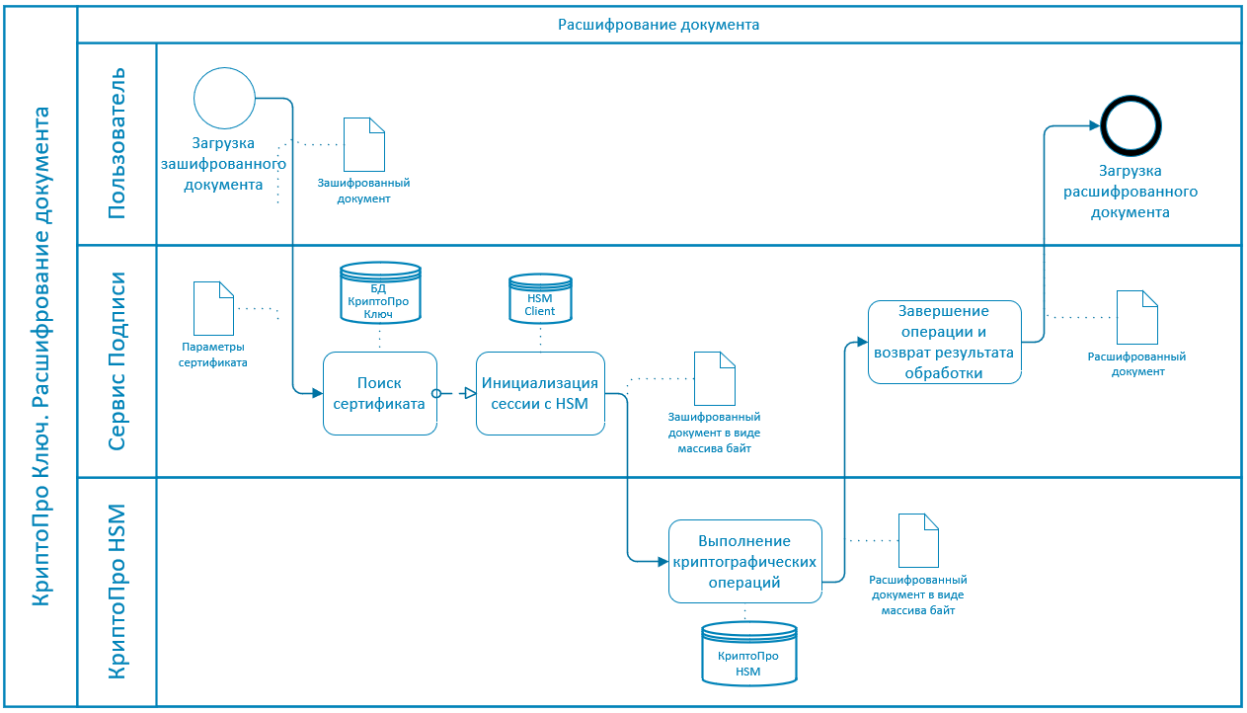

Рис. 4 — Расшифрование документа

3.5. Аудит событий и формирование отчетов

Аудит компонентов КриптоПро Ключ производится при помощи компонента Сервис Аудита. Доступен аудит следующих компонентов КриптоПро Ключ:

- Центр Идентификации;
- Сервис Подписи;
- Сервис Обработки Документов.

Аудит осуществляется без вмешательства Пользователя — его настраивает Администратор системы. Выбранные Администратором при настройке операции записываются в журналы, которые отсылаются в Сервис Аудита и записываются в его БД. Событиям назначаются коды, что упрощает их просмотр и фильтрацию на веб-интерфейсе.

Пользователю доступен только просмотр событий аудита и их сортировка по фильтру и/или датам. Оператору доступны к просмотру события Пользователей, включенных в группу (группы), назначенные данному Оператору. Оператору Аудита доступны события всех Пользователей внутри определенного Центра Идентификации и формирование отчетов по этим событиям.

Журнал аудита должен сохраняться в полном объеме за период, покрывающий срок действия ключей Пользователей, хранящихся в БД Сервиса Подписи. То есть, если ключ Пользователя на настоящий момент является действительным, необходимо, чтобы аудит сохранялся за все время жизни этого ключа.

4. Управление ключами пользователей

КриптоПро Ключ позволяет использовать несколько режимов хранения закрытых ключей Пользователей в защищенном виде:

- в ПАКМ HSM;
- в БД Сервиса Подписи;
- в мобильном приложении;
- в гибридном виде;
- на отчуждаемом носителе, считываемом при помощи мобильного приложения.

В первом случае HSM является криптопровайдером для КриптоПро DSS и именно в нем хранятся ключи Пользователей.

Во втором случае безопасность хранения ключей в БД Сервиса Подписи достигается шифрованием на ключе, вырабатываемом с помощью HSM из Мастер-ключа Сервиса Подписи и секрета Пользователя (ПИН-кода). При выборе режима хранения ключей в БД Сервиса Подписи в HSM создается Мастер-ключ. Созданный Мастер-ключ имеет ограниченный срок жизни, по умолчанию равный 36 месяцам. По истечении срока действия Мастер-ключа должен быть создан новый Мастер-ключ, то есть зарегистрирован новый криптопровайдер.

Режим хранения ключей в мобильном приложении подразумевает создание закрытых ключей пользователей и хранение их при помощи криптопровайдера на устройстве Пользователя в мобильном приложении в защищенном виде. Данные ключи могут быть дополнительно защищены ПИН-кодом.

Гибридный режим хранения закрытых ключей Пользователей подразумевает хранение части закрытого ключа при помощи криптопровайдера в мобильном приложении на устройстве пользователя. При этом ключ не может покидать устройство пользователя, не может быть представлен на нем в открытом виде, а также не может быть использован без выполнения криптографической операции с другой его частью – вектором защиты ключа, хранимой в серверной части КриптоПро Ключ, в HSM. Дополнительно ключ Пользователя защищен ПИН-кодом в мобильном приложении на устройстве Пользователя.

Режим хранения ключей на отчуждаемом носителе аналогичен режиму хранения ключей в мобильном приложении за тем исключением, что контейнер с ключом находится на бесконтактном отчуждаемом носителе (ФКН). Для доступа к ключу необходимо использовать мобильное приложение.

Закрытые ключи Пользователей, хранимые в мобильном приложении, гибридно и на отчуждаемых носителях, также имеют ограниченный срок действия, по умолчанию равный 15 месяцам. После окончания срока действия закрытый ключ Пользователя не может больше использоваться для создания подписи, шифрования и расшифрования и должен быть удален.

На Рис. 5 отражено соотношение сроков действия Мастер-ключа и ключей Пользователей. Интервал A обозначает полный срок действия Мастер-ключа, по истечении которого Мастер-ключ удаляется. Интервал B обозначает период, в течение которого Мастер-ключ может использоваться для создания новых ключей Пользователей. Интервал C обозначает период, в течение которого Мастер-ключ не может использоваться для создания новых ключей Пользователей, так как в противном случае сроки действия ключей Пользователя превысили бы срок действия Мастер-ключа. В

течение периода C Мастер-ключ используется только для работы с существующими ключами Пользователей.

Администратор КриптоПро DSS должен зарегистрировать новый криптопровайдер до наступления периода C. В противном случае, создание новых ключей Пользователей, то есть выпуск новых сертификатов, станет невозможным.

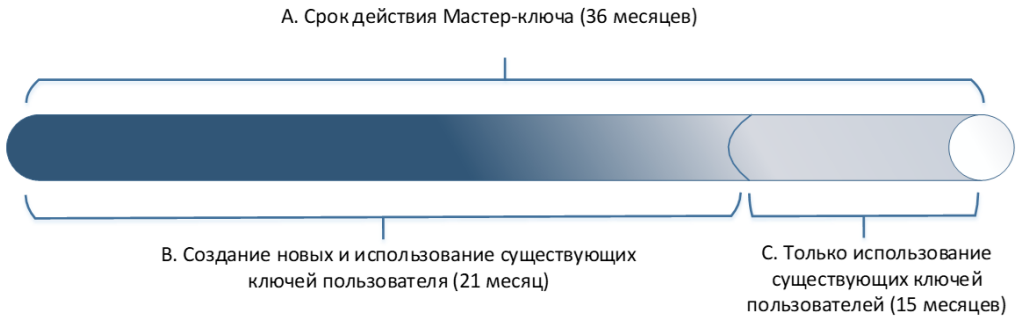

Рис. 5 — Сроки действия Мастер-ключа и ключей Пользователей

В сравнительной таблице (см. Таблица 1) ниже представлены особенности каждого из режимов хранения ключей:

Таблица 1 — Режимы хранения ключей

Критерий/ Режим	Хранение ключей в HSM	Хранение ключей в БД Сервиса Подписи	Хранение ключей в мобильном приложении	Гибридное хранение ключей	Хранение ключей на токене
Что хранится	Все закрытые ключи Пользователей хранятся в ПАКМ HSM.	Все закрытые ключи Пользователей хранятся в БД Сервиса Подписи в зашифрованном виде, в HSM хранится Мастер-ключ.	Все закрытые ключи Пользователей хранятся в мобильном приложении в защищенном виде.	Все закрытые ключи Пользователей хранятся в мобильном приложении в защищенном виде и не могут быть использованы без вектора защиты, соответствующего каждому ключу и хранимому в HSM.	Все закрытые ключи Пользователей хранятся на отчуждаемом носителе в защищенном виде и могут быть использованы при помощи мобильного приложения.
Емкость	10 000 ключей.	Ограничивается размерами дискового пространства Сервиса Подписи и производительностью сервера БД.	-	-	-.
Срок жизни ключа	36 месяцев.	Мастер-ключ: 36 месяцев, 21 месяц пригоден для создания новых ключей. Закрытые ключи Пользователей: 15 месяцев.	36 месяцев.	36 месяцев	36 месяцев.
Возможности репликации БД	Только ручная репликация.	Обычная репликация БД, ручной перенос Мастер-ключа.	Обычная репликация БД.	Обычная репликация БД.	Обычная репликация БД.