КРИПТОПРО

Программный комплекс «КриптоПро Ключ»

Техническое описание решения

2025 г.

Оглавление

1 Введение 3

2 Назначение и цели использования КриптоПро Ключ 4

3 Основные возможности КриптоПро Ключ 5

4 Компоненты КриптоПро Ключ 8

5 Взаимодействие компонентов КриптоПро Ключ 13

6 Режимы хранения ключей 14

7 Системное окружение 16

8 Типовые структурные схемы комплекса технических средств Сервиса электронной подписи на базе ПК «КриптоПро Ключ» 17

8.1 Схема системы электронной подписи в базовой конфигурации 17

8.2 Схема системы электронной подписи в базовой конфигурации с горячим резервированием 18

8.3 Схема системы электронной подписи в кластерной конфигурации 21

9 Сценарии реализации возможностей КриптоПро Ключ 24

9.1 Регистрация пользователя и настройка учетной записи 24

9.2 Инициализация мобильного приложения на базе Ключ SDK 25

9.3 Создание ключа и запроса на сертификат 29

9.4 Подписание электронного документа 31

9.5 Проверка подписи и Проверка сертификата ЭП 34

9.6 Шифрование электронного документа 35

9.7 Расшифрование электронного документа 35

9.8 Аудит событий и формирование отчетов 36

10 Основные преимущества использования КриптоПро Ключ 37

11 Возможные варианты использования КриптоПро Ключ 38

12 Полезные ссылки для ознакомления с функционалом КриптоПро Ключ 39

13 Контактная информация 40

1 Введение

В условиях стремительной цифровизации общества и постоянного роста количества услуг, предоставляемых в электронном виде, электронная подпись становится все более популярной. Крупные организации и предприятия, стремящиеся предоставлять дистанционные сервисы и оказывать цифровые услуги, нуждаются в надежной инфраструктуре электронной подписи, которая должна отвечать следующим требованиям:

– обеспечить юридически значимый электронный документооборот;

– использовать отечественные криптографические алгоритмы для защиты информации;

– функционировать в импортозамещенном окружении;

– обеспечить централизованное управление ключами и сертификатами;

– предоставлять различные способы хранения и применения пользовательских ключей;

– поддержать возможность работы на мобильных устройствах;

– предоставлять гибкий и простой интерфейс для интеграции в различные бизнес-процессы;

– соответствовать требованиям регулирующих органов.

Для решения этих задач предлагается создать систему электронной подписи на основе продуктов компании КриптоПро, главным компонентом которой является Программный комплекс (далее – ПК) «КриптоПро Ключ», который успешно прошел сертификационные испытания и получил сертификат соответствия ФСБ России.

В данном документе представлено техническое описание ПК «КриптоПро Ключ», а также описаны его особенности и подходы, позволяющие организовать эффективную систему электронной подписи с использованием других продуктов компании.

Документ предназначен для руководителей и технических специалистов ИТ и ИБ подразделений, стремящихся к построению надежной инфраструктуры электронной подписи.

2 Назначение и цели использования КриптоПро Ключ

ПК «КриптоПро Ключ» предназначен для:

– обеспечения возможности локального, мобильного и (или) распределенного защищенного хранения и использования ключей подписи Пользователей, включая подписание и шифрование/расшифрование электронных документов;

– удаленной проверки электронной подписи (далее – ЭП) различных форматов;

– интеграции с корпоративными информационными системами.

Целями использования ПК «КриптоПро Ключ» являются:

– обеспечение юридической значимости электронного документооборота, в том числе целостности и аутентичности (подлинности и защиты от подделки) электронных документов за счет использования электронной подписи документов;

– обеспечение конфиденциальности электронных документов.

3 Основные возможности КриптоПро Ключ

Список основных возможностей КриптоПро Ключ:

– Создание, защищенное хранение и использование ключей Пользователей ЭП в различных режимах[1]:

- в мобильном приложении;
- в распределенном виде (в мобильном приложении с дополнительной защитой пользовательских ключей с помощью серверного компонента);
- на отчуждаемом (съёмном) ключевом носителе (токене) совместно с мобильными устройствами и автоматизированными рабочими местами (далее – АРМ) Пользователей.

– Управление учетными записями Пользователей с возможностью разделения на группы с различными настройками и политиками.

– Выполнение криптографических операций с применением отечественных алгоритмов:

- аутентификация Пользователей и Операторов;
- генерация ключей ЭП, ключей проверки ЭП, закрытых и открытых ключей шифрования;
- формирование запросов на сертификаты;
- создание и проверка ЭП;
- шифрование и расшифрование.

– Поддержка различных форматов подписи[2]:

- необработанная подпись по ГОСТ Р 34.10-2012;
- подпись в формате CMS (CAdES-BES);
- усовершенствованная ЭП (CAdES-T, CAdES-X Long Type 1);
- подпись XML-документов (XMLDSig);
- усовершенствованная ЭП (XadES-BES, XadES-T);
- подпись PDF-документов (PAdES-B-B, PAdES-B-T, PAdES с включением доказательств проверки).

[1] Подробнее о режимах хранения ключей в «ЖТЯИ.00118-01 96 01 КриптоПро Ключ. Общее описание» (Раздел 6). Централизованный режим хранения ключей подписи с использованием ПАКМ «КриптоПро HSM» реализован в ПАК «КриптоПро DSS»

[2] Подробнее о типах ЭП и форматах документах в «ЖТЯИ.00118-01 96 01 КриптоПро Ключ. Общее описание» (Раздел 11) и в онлайн документации

– Пакетное подписание (нескольких документов за одно подтверждение операции).

– Подписание документов в асинхронном режиме с возвращением результата (Callback) в вызывающую систему по завершении операции.

– Реализация множества способов аутентификации Пользователей, в том числе:

- по логину и паролю с защитой канала по протоколу TLS с односторонней аутентификацей;
- по сертификату с защитой канала по протоколу TLS с двусторонней аутентификацией (возможно использование USB-токенов и смарт-карт);
- аутентификация пользователей по алгоритму HMAC, описанным в Рекомендациях по стандартизации ТК 26 Р-50.1.113-2016, в мобильном приложении на базе ***КриптоПро Ключ SDK***;
- подтверждение операций в мобильном приложении на базе ***КриптоПро Ключ SDK***;
- вспомогательная аутентификация при помощи одноразовых паролей (OTP), доставляемых в SMS-сообщениях или по электронной почте.

– Интеграция со сторонними центрами идентификации по протоколу OAuth 2.0 (в т.ч. с корпоративным доменом на базе MS AD (посредством ADFS) и OpenLDAP).

– Интеграция с удостоверяющим центром (далее – УЦ) на базе ПАК «КриптоПро УЦ» для автоматизации создания запросов на сертификаты.

– Визуализация (конвертация и отображение) электронных документов форматов, перечисленных в «ЖТЯИ.00118-01 96 01 КриптоПро Ключ. Общее описание», перед выполнением операции с ними[3].

– Добавление в PDF-документы видимой подписи (штампа) (отображение произвольных изображений, логотипов и текстов на штампе).

– Предоставление веб-интерфейса для Пользователей и Операторов.

– Предоставление программного интерфейса (REST API) для интеграции в бизнес-процессы.

– Предоставление SDK для встраивания в мобильные приложения.

– Реализация системы оповещений Пользователей о событиях и операциях с их ключами ЭП:

- PUSH – уведомления;
- SMS – сообщения;

[3] Подробнее о поддерживаемых форматах документов для их отображения в «ЖТЯИ.00118-01 96 01 КриптоПро Ключ. Общее описание» (Раздел 13)

- E-mail – сообщения.

– Ведение аудита событий, связанных с действиями Пользователей, Операторов и эксплуатацией программного комплекса.

4 Компоненты КриптоПро Ключ

Для реализации указанного функционала в разделе 3 необходимо создать систему электронной подписи (далее – СЭП) на базе ПК «КриптоПро Ключ». В ряде сценариев потребуется использовать дополнительные компоненты и продукты КриптоПро.

Состав ПК «КриптоПро Ключ»:

- Центр Идентификации;
- Сервис Подписи;
- Веб-интерфейс;
- Сервис Аудита;
- Сервис Обработки Документов;
- ПАКМ «КриптоПро HSM»[4].

Для расширения функциональных возможностей и сценариев работы КриптоПро Ключ применяются следующие дополнительные компоненты:

- Сервис рассылки PUSH – уведомлений;
- Сервис Ключ Lite[5];
- Сервис Взаимодействия с SDK для мобильных приложений [6];
- Клиентские компоненты:
  - Средство криптографической защиты информации (далее – СКЗИ) КриптоПро CSP/JCP;
  - КриптоПро TSP Client (компонент из состава СКЗИ «КриптоПро CSP», используется опционально);
  - КриптоПро OCSP Client (компонент из состава СКЗИ «КриптоПро CSP», используется опционально);
  - Ключ SDK для встраивания в мобильное приложение:
    - КриптоПро Ключ SDK;
    - КриптоКлюч SDK;
    - мобильное приложение «КриптоПро Ключ»;
    - мобильное приложение «КриптоКлюч».

[4] ПАКМ приобретается отдельно

[5] Может использоваться как самостоятельный продукт совместно с СКЗИ КриптоПро CSP на АРМ Пользователей

[6] Использование Модулей аутентификации (SDK) лицензируется дополнительно

Для расширения функциональных возможностей и сценариев работы СЭП применяются следующие программные продукты КриптоПро:

– КриптоПро УЦ;
– КриптоПро Службы УЦ;
– КриптоПро Центр мониторинга.

Описание основных компонентов ПК «КриптоПро Ключ»

Компонент «***Центр Идентификации***» предназначен для регистрации и аутентификации Операторов и Пользователей, а также управления информацией, содержащейся в их учетной записи.

Компонент «***Сервис Подписи***» предназначен для выполнения операций по созданию подписи и ее проверке, а также шифрования и расшифрования документов, загружаемых Пользователями. «***Сервис подписи»*** используется при создании ключей и запросов на сертификаты.

Компонент «***Веб-интерфейс***» предназначен для организации интерактивного взаимодействия Пользователей и Операторов с компонентами ПК КриптоПро Ключ.

В веб-интерфейсе Пользователю доступны операции создания, усовершенствования и проверки ЭП, шифрования и расшифрования электронных документов, создания запросов на сертификаты и их установка, настройка профиля и просмотр списка своих операций.

В веб-интерфейсе Оператора возможно управлять учетными данными пользователей, настраивать им способы аутентификации, просматривать журнал аудита и создавать отчеты.

Для доступа Пользователей и Операторов к функциям ПК КриптоПро Ключ может использоваться интерфейс прикладных информационных систем Пользователя, интегрированных с компонентами ПК КриптоПро Ключ по REST API [7].

Компонент «***Сервис Аудита***» предназначен для доверенного аудита событий, поступающих с компонентов КриптоПро Ключ.

Компонент «***Сервис Обработки Документов***» предназначен для работы с электронными документами. Компонент «Сервис Обработки Документов» выполняет преобразование документов в различные форматы для их отображения в разных сценариях работы. Сервис осуществляет временное хранение электронных документов при создании подписи в асинхронном режиме.

[7] REST API Сервиса Подписи

Компонент «***Сервис Взаимодействия с SDK для мобильных приложений***» (SDK API Gateway) предназначен для организации взаимодействия между SDK мобильных приложений (Ключ SDK) и компонентами КриптоПро Ключ.

ПАКМ «КриптоПро HSM»[8] предназначен для создания и обеспечения защищенного хранения ключей безопасности и электронной подписи и выполнения криптографических операций с их использованием. Программно-аппаратный криптографический модуль выполняет хранение ключевой информации серверных компонентов и осуществляет криптографические операции над пользовательскими данными.

Описание дополнительных компонент

Компонент «***Сервис рассылки PUSH-уведомлений***» – предназначен для отправки PUSH-уведомлений на мобильные устройства Пользователей.

Компонент «***Сервис Ключ Lite***» (Ключ Lite) позволяет Пользователям выполнять криптографические операции с использованием закрытых ключей на своих стационарных устройствах и внешних носителях. Ключ Lite может использоваться в режиме веб-интерфейса (Сервиса Подписи) и в режиме программного интерфейса.

«Сервис Ключ Lite» в режиме веб-интерфейса является специализированным режимом работы компонента Сервис Подписи ПК «КриптоПро Ключ». При работе в данном режиме Пользователю доступны следующие операции:

– аутентификация пользователя (аналогично общим правилам аутентификации в КриптоПро Ключ);

– создание ЭП документов различных форматов, поддерживаемых Сервисом Подписи ПК «КриптоПро Ключ»;

– шифрование и расшифрование документов (только в формате Enveloped CMS);

– управление сертификатами ключей проверки ЭП пользователей (формирование запросов на создание и аннулирование сертификатов, установка полученных сертификатов).

В режиме программного интерфейса «***Сервис Ключ Lite***» предоставляет возможность интеграции прикладных информационных систем по REST API для создания электронной подписи документов с использованием СКЗИ «КриптоПро CSP», установленного на рабочем месте (компьютере) пользователя.

Ключи подписи Пользователей формируются и хранятся непосредственно на персональных (стационарных или переносных) устройствах пользователей (в т.ч. с помощью

[8] ПАКМ «КриптоПро HSM» - сертифицированное СКЗИ класса КВ2

съёмных ключевых носителей), где выполняются криптографические операции с использованием СКЗИ КриптоПро CSP.

Для корректной работы режимов «Сервис Ключ Lite» на персональное устройство Пользователя устанавливается сертифицированное СКЗИ «КриптоПро CSP» с лицензией для рабочего места и совместимый браузер (поддерживающий работу с КриптоПро ЭЦП Browser plug-in [9]).

Лицензии на ПО «КриптоПро Ключ Lite» и СКЗИ «КриптоПро CSP» для пользователей сервиса приобретаются дополнительно.

Для предоставления информации о статусе сертификатов ключей проверки подписи и меток времени, а также для проверки подписей и сертификатов по запросам Пользователей используется программно-аппаратный комплекс (ПАК) «Службы УЦ». Кроме того, Службы УЦ необходимы для сбора доказательств для усовершенствования подписи CAdES-BES до форматов CAdES-T и CAdES-X Long Type 1, подписи XadES-BES до формата XadES-T.

В составе СЭП могут использоваться следующие компоненты ПАК «Службы УЦ»:

– программный компонент «КриптоПро OCSP Server»;
– программный компонент «КриптоПро TSP Server»;
– Служба проверки сертификатов и электронной подписи «КриптоПро SVS».

Клиентские компоненты

СКЗИ «КриптоПро CSP» предоставляет Пользователю возможность устанавливать безопасное соединение с серверными компонентами ПК «КриптоПро Ключ» по протоколу TLS ГОСТ, обеспечивая как двустороннюю, так и одностороннюю аутентификацию. Первичная аутентификация может осуществляться с использованием логина и пароля, а также по клиентскому сертификату.

Кроме того, СКЗИ «КриптоПро CSP» (или СКЗИ «КриптоПро JCP») устанавливается на серверы информационных систем, которые интегрируется с серверными компонентами ПК «КриптоПро Ключ» для защиты передаваемых данных по протоколу TLS(ГОСТ).

***«Ключ SDK»* для встраивания в мобильное приложение**

В дополнительный компонент «Модуль аутентификации мобильных приложений» будет входить «***Ключ SDK***», который позволяет осуществлять работу с компонентами КриптоПро Ключ в собственных мобильных приложениях. «Ключ SDK» представляет собой набор программных библиотек (включая СКЗИ «КриптоПро CSP») для встраивания в мобильные приложения, позволяющие выполнять операции создания ЭП и управления

[9] Рекомендуемые браузеры, поддерживающе работы с КриптоПро ЭЦП Browser plug-in - https://cryptopro.ru/products/cades/plugin

сертификатами Пользователей, а также подтверждать операции Пользователя в КриптоПро Ключ, инициированные другими способами.

5 Взаимодействие компонентов КриптоПро Ключ

На рисунке 1 изображена схема взаимодействия компонентов КриптоПро Ключ. Слева от пунктирной линии отображаются компоненты и сервисы, которые непосредственно связаны с организацией СЭП, а также связи между ними. Продукты для расширения функциональных возможностей и сценариев работы СЭП, а также сторонние продукты, расположены справа от границы, обозначенной пунктиром.

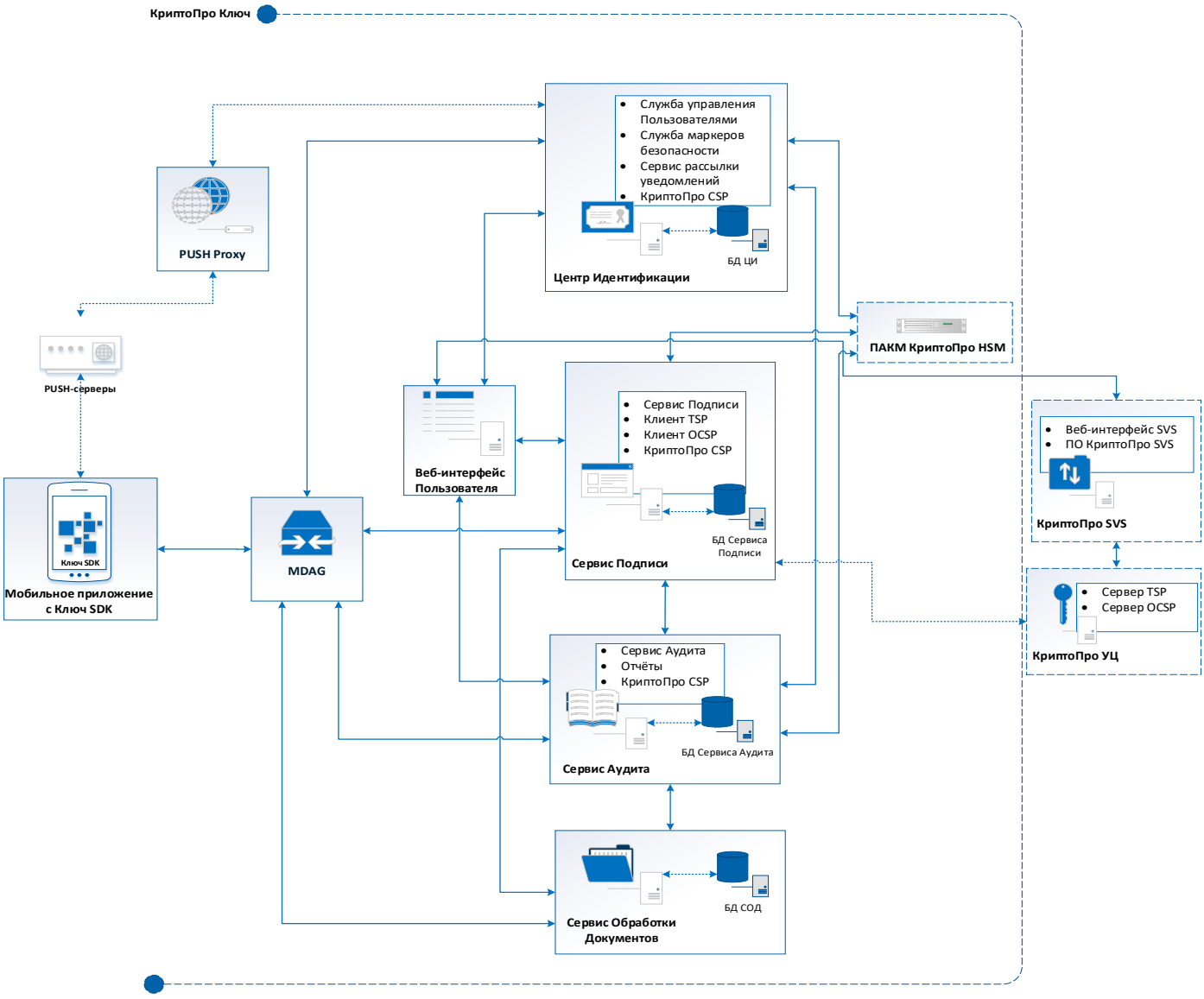

Рисунок 1 – Взаимодействие компонентов СЭП на базе ПК «КриптоПро Ключ»

6 Режимы хранения ключей

ПК «КриптоПро Ключ» позволяет использовать несколько режимов хранения ключей ЭП Пользователей в защищенном виде[10]:

– непосредственно в мобильных приложениях на базе «***Ключ SDK***»;

– в распределенном виде в мобильном приложении с дополнительной защитой пользовательских ключей с помощью ПАКМ «КриптоПро HSM»;

– на отчуждаемых ключевых носителях[11], поддерживаемых СКЗИ «КриптоПро CSP», включая на мобильные устройства (в т.ч. по протоколу NFC).

Режим хранения ключей подписи в мобильном приложении включает создание или перенос ключей подписи Пользователей и их защищенное хранение с использованием «Ключ SDK» в мобильном приложении на устройстве Пользователя. С помощью «Ключ SDK» также возможно использование съёмных ключевых носителей, в том числе носителей с поддержкой протокола NFC. Данные ключи могут дополнительно защищены ПИН-кодом.

Защищенное хранение ключей подписи в распределенном режиме подразумевает защищенное хранение ключей ЭП в мобильных устройствах, которое обеспечивается с помощью ключей защиты, находящихся на серверной стороне в ПАКМ «КриптоПро HSM» в неизвлекаемом виде. Дополнительно ключ Пользователя защищен ПИН-кодом в мобильном приложении на устройстве Пользователя.

Реализация режима хранения ключей подписи на съёмных ключевых носителях возможна следующими способами:

– использование ключей подписи на АРМ Пользователя (в Web-интерфейсе или в консольном приложении интегрированной ИС) с помощью сервиса Ключ Lite;

– использование ключей подписи аналогично режиму хранения ключей в мобильном приложении на базе Ключ SDK за тем исключением, что контейнер с ключом подписи хранится в неизвлекаемом виде на ключевом носителе (ФКН) типа Рутокен ЭЦП[11], в т.ч. с поддержкой протокола NFC. Использование ключа подписи возможно посредством мобильного приложения на базе Ключ SDK и на АРМ Пользователя.

Срок хранения ключей подписи Пользователей в мобильном приложении в гибридном виде составляет максимум 15 месяцев. На отчуждаемых носителях (ФКН) типа Рутокен с поддержкой протокола NFC ключи подписи Пользователей имеют ограничения срока

[10] О режимах хранения ключей в ««ЖТЯИ.00118-01 96 01 КриптоПро Ключ. Общее описание» (Раздел 6). Централизованный с использованием ПАКМ «КриптоПро HSM» режим хранения ключей подписи реализован в ПАК «КриптоПро DSS».

[11] Подробнее про поддерживаемые отчуждаемых ключевых носителях в «ЖТЯИ.00118-01 30 01 Формуляр»

действия максимум 36 месяцев (в соответствии с «ЖТЯИ.00118-01 95 01. КриптоПро Ключ. Правила пользования»).

7 Системное окружение

ПК «КриптоПро Ключ» представляет собой набор веб-сервисов, поэтому ко всем его компонентам предъявляются одинаковые системные требования.

Для функционирования серверной части в *nix-системах:

– ОС СН Astra Linux Special Edition версии 1.7 Смоленск (РУСБ. 10015-01);

– СКЗИ из состава компонентов выбранного исполнения (см. ЖТЯИ.00118-01 30 01. КриптоПро Ключ. Формуляр);

– СУБД PostgreSQL 11 и выше, Jatoba 4 Platform V или Pangolin SE 6;

– веб-сервер nginx 1.18.0 и выше.

Для функционирования серверной части в ОС Windows:

– ОС Microsoft Windows Server 2016/2019/2022 (x64);

– СКЗИ из состава компонентов выбранного исполнения (см. ЖТЯИ.00118-01 30 01. КриптоПро Ключ. Формуляр);

– СУБД SQL Server 2016/2017/2019/2022;

– веб-сервер IIS, соответствующий используемой ОС.

Для функционирования пользовательского АРМ:

– операционная система, поддерживаемая СКЗИ КриптоПро CSP/JCP;

– СКЗИ из состава компонентов выбранного исполнения (см. ЖТЯИ.00118-01 30 01. КриптоПро Ключ. Формуляр);

– веб-браузер с установленным плагином КриптоПро Browser plug-in (Chromium Gost, Яндекс.Браузер, Opera, Firefox) (опционально).

Для функционирования пользовательского мобильного устройства:

– мобильная ОС iOS версии не ниже 13 (при использовании Ключ SDK) либо 15 (при использовании мобильных приложений), Android версии не ниже 8;

– мобильное приложение на базе Ключ SDK.

СУБД не требуются для клиентских компонентов и серверных компонентов, которые не имеют собственной БД. В настоящий момент такими компонентами являются Веб-интерфейс Пользователя и Сервис взаимодействия с SDK, а также Ключ Lite.

8 Типовые структурные схемы комплекса технических средств Сервиса электронной подписи на базе ПК «КриптоПро Ключ»

8.1 Схема системы электронной подписи в базовой конфигурации

Система электронной подписи в базовой конфигурации представлена на рисунке 2 и состоит из одного выделенного сегмента, защищённого межсетевым экраном (не ниже 4 класса защиты по требованиям ФСБ России или межсетевым экраном уровня веб-сервера (тип "Г"), сертифицированного ФСТЭК России и соответствующего 4 классу защиты требований к межсетевым экранам), системой обнаружения вторжений (сертифицированной ФСТЭК России и соответствующей 4 классу защиты или выше требований к системам обнаружения вторжений) или средством обнаружения атак, сертифицированным ФСБ России, и включает:

– Сервер с компонентами ПК «КриптоПро Ключ» (1 шт.);

– ПАКМ «КриптоПро HSM» (1 шт.);

– Сервер с компонентами ПАК «Службы УЦ» (1 шт.) (ПО «КриптоПро TSP Server» и «КриптоПро OCSP Server», «КриптоПро SVS») – опционально (в случае необходимости создания ЭП усовершенствованного формата без подключения к внешним Службам УЦ).

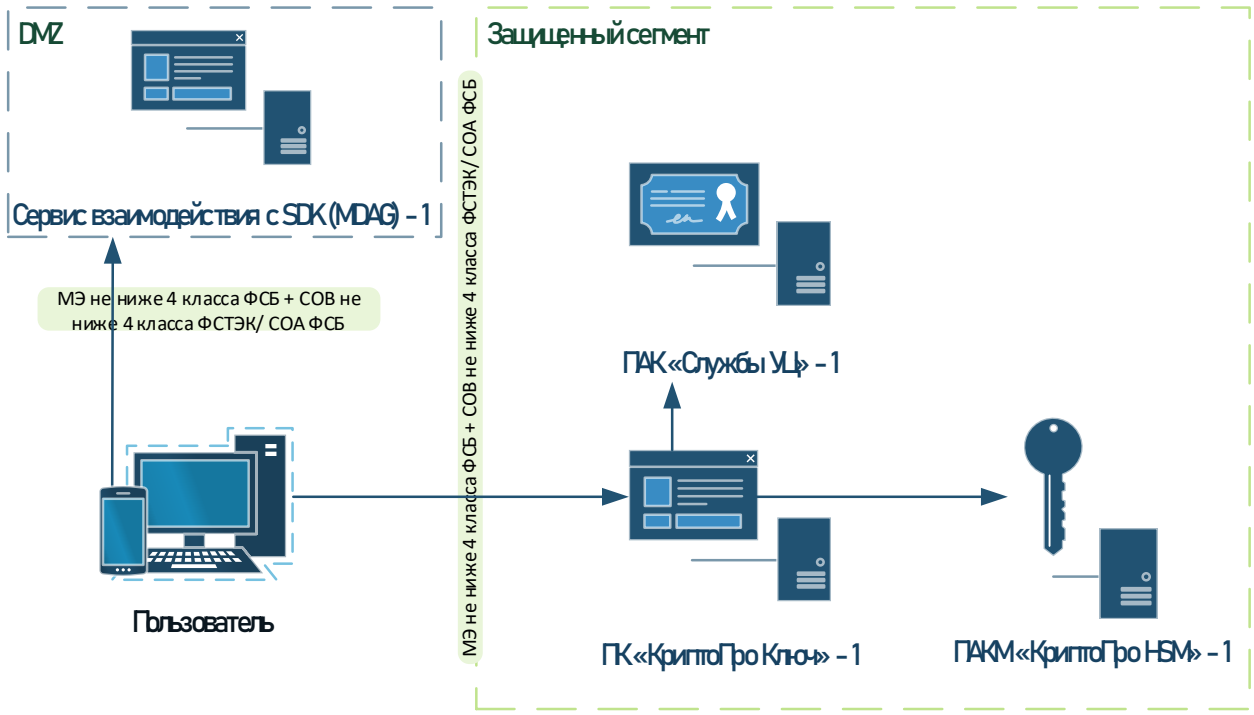

Рисунок 2 – Типовая схема СЭП в базовой конфигурации

Перечень основных компонентов представлен в таблице 1 ниже.

Таблица 1 – Основные компоненты

Компонент	Назначение компонента	Класс защиты СКЗИ
Сервер с основными компонентами ПК «КриптоПро Ключ»	Для выполнения основных криптографических операций, связанных с электронной подписью, с шифрованием и пр.	КС3
Сервер с дополнительными компонентами ПК «КриптоПро Ключ»	– MDAG – сервис взаимодействия с мобильным приложением; – Push Service – сервис уведомлений	КС3
ПАКМ «КриптоПро HSM» версии 2.0[12]	Для обеспечения высокого уровня безопасности криптографических операций, связанных с обработкой, хранением и использованием криптографических ключей и цифровых подписей	КВ2
Информационная система	Для обеспечения взаимодействия Пользователя и СЭП	
Мобильное устройство (МУ)	Для пользования услугами СЭП с мобильного устройства	
АРМ Пользователя	Для пользования услугами СЭП	

Перечень дополнительных компонентов представлен в таблице 2 ниже.

Таблица 2 – Дополнительные компоненты

Компонент	Назначение компонента	Класс Защиты СКЗИ
ПАК «Службы УЦ»	Для предоставления штампов времени, информации о статусе сертификатов ключей проверки ЭП, а также проверки сертификатов и электронной подписи	КС2

8.2 Схема системы электронной подписи в базовой конфигурации с горячим резервированием

Система электронной подписи в базовой конфигурации с горячим резервированием представлена на рисунке 3 и состоит из одного выделенного сегмента, защищённого межсетевым экраном (не ниже 4 класса защиты по требованиям ФСБ России или межсетевым экраном уровня веб-сервера (тип "Г"), сертифицированного ФСТЭК России и

[12] ПАКМ «КриптоПро HSM»

соответствующего 4 классу защиты требований к межсетевым экранам), системой обнаружения вторжений (сертифицированной ФСТЭК России и соответствующей 4 классу защиты или выше требований к системам обнаружения вторжений) или средством обнаружения атак, сертифицированным ФСБ России, и включает:

– Сервер с компонентами ПК «КриптоПро Ключ» (1 шт.);

– ПАКМ «КриптоПро HSM» (2 шт.);

– Сервер с компонентами ПАК «Службы УЦ» (1 шт.) (ПО «КриптоПро TSP Server» и «КриптоПро OCSP Server», «КриптоПро SVS») – опционально (в случае необходимости создания ЭП усовершенствованного формата без подключения к внешним Службам УЦ).

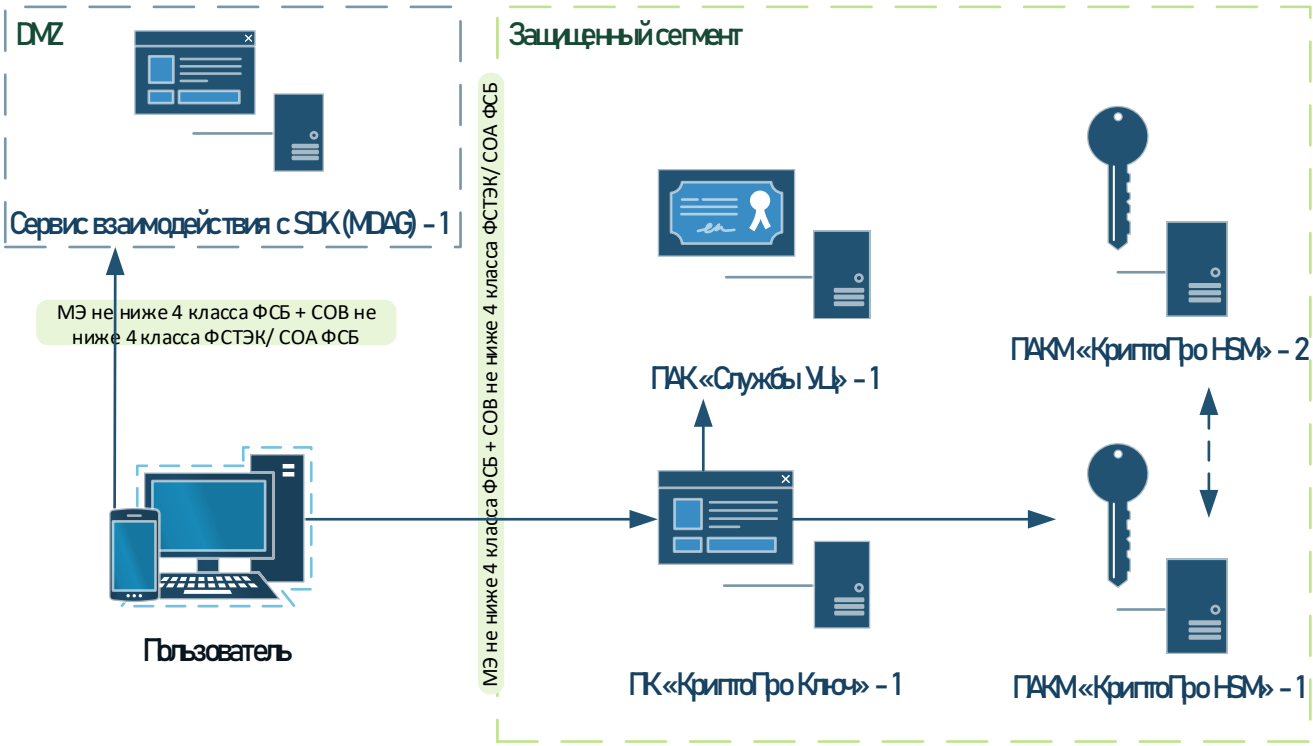

Рисунок 3 – Типовая схема СЭП в базовой конфигурации с горячим резервированием

Перечень основных компонентов представлен в таблице 3 ниже.

Таблица 3 – Основные компоненты

Компонент	Назначение компонента	Класс защиты СКЗИ
Сервер с основными компонентами ПК «КриптоПро Ключ»	Для выполнения основных криптографических операций, связанных с электронной подписью, с шифрованием и пр.	КС3

Компонент	Назначение компонента	Класс защиты СКЗИ
Сервер с дополнительными компонентами ПК «КриптоПро Ключ»	– MDAG – сервис взаимодействия с мобильным приложением; – Push Service – сервис уведомлений	КС3
ПАКМ «КриптоПро HSM» версии 2.0[13]	Для обеспечения высокого уровня безопасности криптографических операций, связанных с обработкой, хранением и использованием криптографических ключей и цифровых подписей	КВ2
Информационная система	Для обеспечения взаимодействия Пользователя и СЭП	
Мобильное устройство (МУ)	Для пользования услугами СЭП с мобильного устройства	
АРМ Пользователя	Для пользования услугами СЭП	

Перечень дополнительных компонентов представлен в таблице 4 ниже.

Таблица 4 – Дополнительные компоненты

Компонент	Назначение компонента	Класс Защиты СКЗИ
ПАК «Службы УЦ»	Для предоставления штампов времени, информации о статусе сертификатов ключей проверки ЭП, а также проверки сертификатов и электронной подписи	КС2

[13] ПАКМ «КриптоПро HSM»

8.3 Схема системы электронной подписи в кластерной конфигурации

Система электронной подписи в кластерной конфигурации представлена на рисунке 4 и обеспечивает высокий уровень доступности и непрерывность функционирования за счет резервирования всех основных компонентов системы и равномерного распределения по ним нагрузки в период высокой интенсивности запросов Пользователей.

Система электронной подписи в кластерной конфигурации может состоять из одного или нескольких выделенных сегментов, защищённых межсетевым экраном (не ниже 4 класса защиты по требованиям ФСБ России или межсетевым экраном уровня веб-сервера (тип "Г"), сертифицированным ФСТЭК России и соответствующим 4 классу защиты требований к межсетевым экранам), системой обнаружения вторжений (сертифицированной ФСТЭК России и соответствующей 4 классу защиты или выше требований к системам обнаружения вторжений) или средством обнаружения атак, сертифицированным ФСБ России, и включает:

– Сервер с компонентами ПК «КриптоПро Ключ» (2 шт.);
– ПАКМ «КриптоПро HSM» (2 шт.);
– Сервер с компонентами ПАК «Службы УЦ» (ПО «КриптоПро TSP Server» и «КриптоПро OCSP Server», «КриптоПро SVS») (2 шт.)– опционально (в случае необходимости создания ЭП усовершенствованного формата без подключения к внешним Службам УЦ).

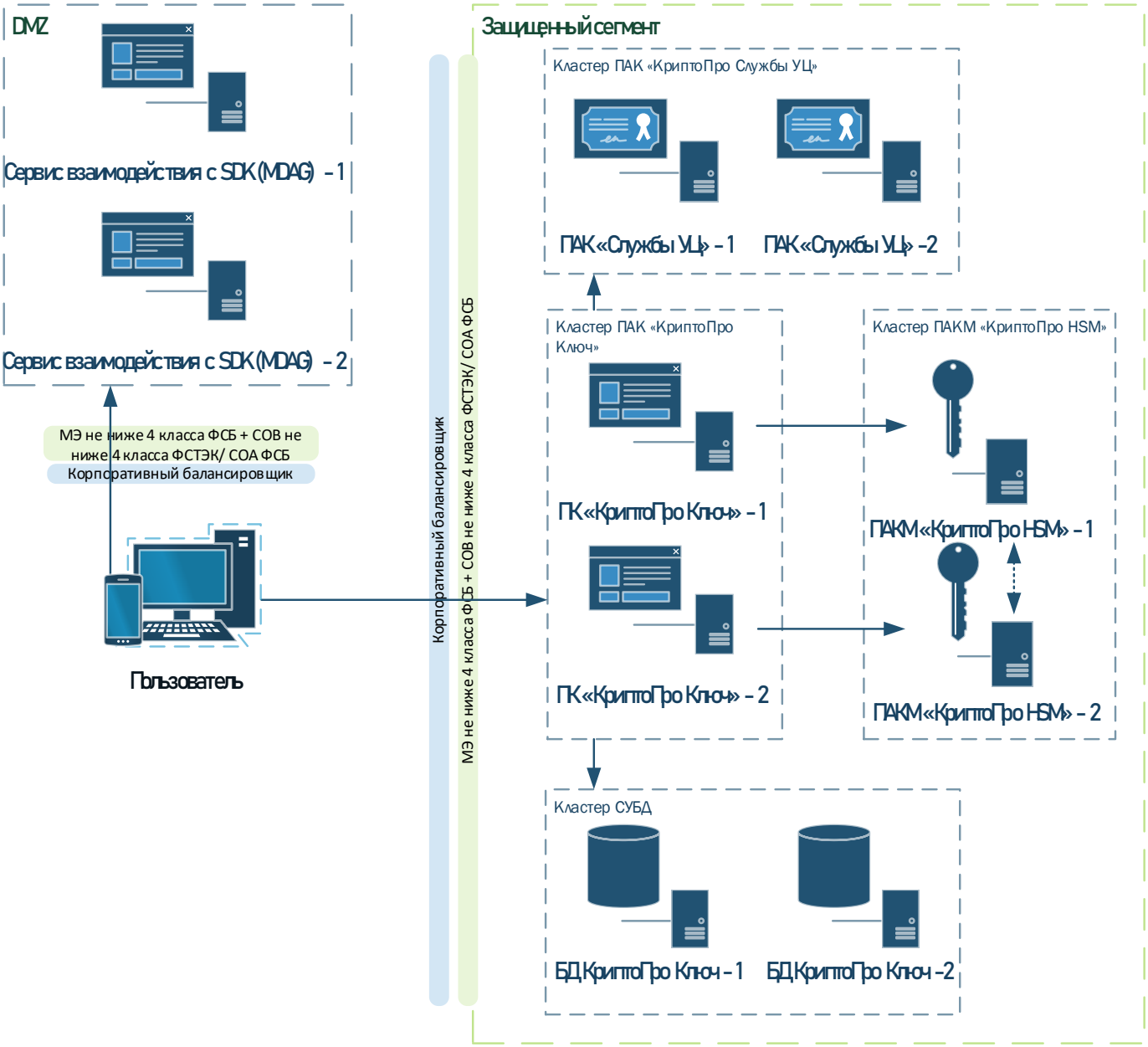

Рисунок 4 – Типовая схема СЭП в кластерной конфигурации с горячим резервированием

Перечень основных компонентов представлен в таблице 5 ниже.

Таблица 5 – Основные компоненты

Компонент	**Назначение компонента**	**Класс защиты СКЗИ**
Сервер с основными компонентами ПК «КриптоПро Ключ»	Для выполнения основных криптографических операций, связанных с электронной подписью, с шифрованием и пр.	КС3

Компонент	Назначение компонента	Класс защиты СКЗИ
Сервер с дополнительными компонентами ПК «КриптоПро Ключ»	– MDAG – сервис взаимодействия с мобильным приложением; – Push Service – сервис уведомлений	КС3
ПАКМ «КриптоПро HSM» версии 2.0[14]	Для обеспечения высокого уровня безопасности криптографических операций, связанных с обработкой, хранением и использованием криптографических ключей и цифровых подписей	КВ2
Информационная система	Для обеспечения взаимодействия Пользователя и СЭП	
Мобильное устройство (МУ)	Для пользования услугами СЭП с мобильного устройства	
АРМ Пользователя	Для пользования услугами СЭП	

Перечень дополнительных компонентов представлен в таблице 6 ниже.

Таблица 6 – Дополнительные компоненты

Компонент	Назначение компонента	Класс Защиты СКЗИ
ПАК «Службы УЦ»	Для предоставления штампов времени, информации о статусе сертификатов ключей проверки ЭП, а также проверки сертификатов и электронной подписи	КС2

[14] ПАКМ «КриптоПро HSM»

9 Сценарии реализации возможностей КриптоПро Ключ

9.1 Регистрация пользователя и настройка учетной записи

Взаимодействие с КриптоПро Ключ доступно только зарегистрированным Пользователям. Процесс регистрации предоставлен на рисунке 5. В процессе регистрации создается учетная запись Пользователя и настраивается способ его аутентификации. Пользователь может зарегистрироваться самостоятельно при наличии соответствующих административных настроек, либо с помощью Оператора.

К самостоятельной регистрации относятся следующие сценарии регистрации Пользователем:

– Самостоятельная регистрация Пользователем с использованием компонента «Веб-интерфейс» из состава КриптоПро Ключ;

– Самостоятельная регистрация Пользователем по квалифицированному сертификату в мобильном приложении[15]. В этом случае Пользователь должен иметь действующий квалифицированный сертификат, чтобы Оператор КриптоПро Ключ смог идентифицировать владельца соответствующего ключа подписи. Сведения в учетной записи Пользователя заполняются из установленного сертификата.

К регистрации Пользователя Оператором КриптоПро Ключ относятся следующие сценарии регистрации:

– Регистрация Пользователя Оператором КриптоПро Ключ, либо информационной системой, выступающей в роли Оператора КриптоПро Ключ;

– Регистрация Пользователя с использованием стороннего Центра Идентификации (далее – СЦИ), интегрированного с КриптоПро Ключ по протоколу OpenID или SAML (например, корпоративного каталога AD посредством ADFS или Keycloak, или СЦИ из состава интегрированной корпоративной ИС).

Ниже представлен один из методов регистрации Пользователя Оператором КриптоПро Ключ, либо информационной системой, выступающей в роли Оператора КриптоПро Ключ. Учетную запись Пользователя создает Оператор.

[15] Подробнее про самостоятельную регистрацию Пользователем по квалифицированному сертификату в мобильном приложении на рисунке 9, в разделе «Инициализация мобильного приложения на базе Ключ SDK»

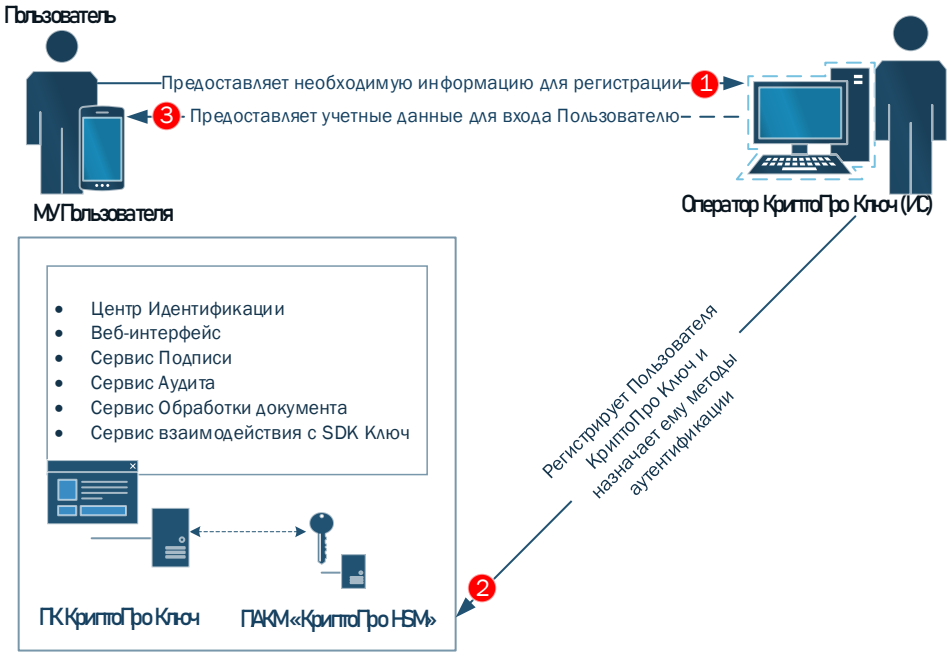

Рисунок 5 – Процесс регистрации Пользователя Оператором КриптоПро Ключ

9.2 Инициализация мобильного приложения на базе Ключ SDK

Перед использованием КриптоПро Ключ мобильное устройство Пользователя, на котором установлено мобильное приложение, должно быть привязано к учетной записи Пользователя для выполнения операций в КриптоПро Ключ.

Существуют следующие способы привязки мобильного устройства:

– Инициализация мобильного устройства при помощи сверки уникального идентификатора. В данном случае необходима предварительная регистрация мобильного устройства Пользователя. Данный процесс представлен на рисунке 6;

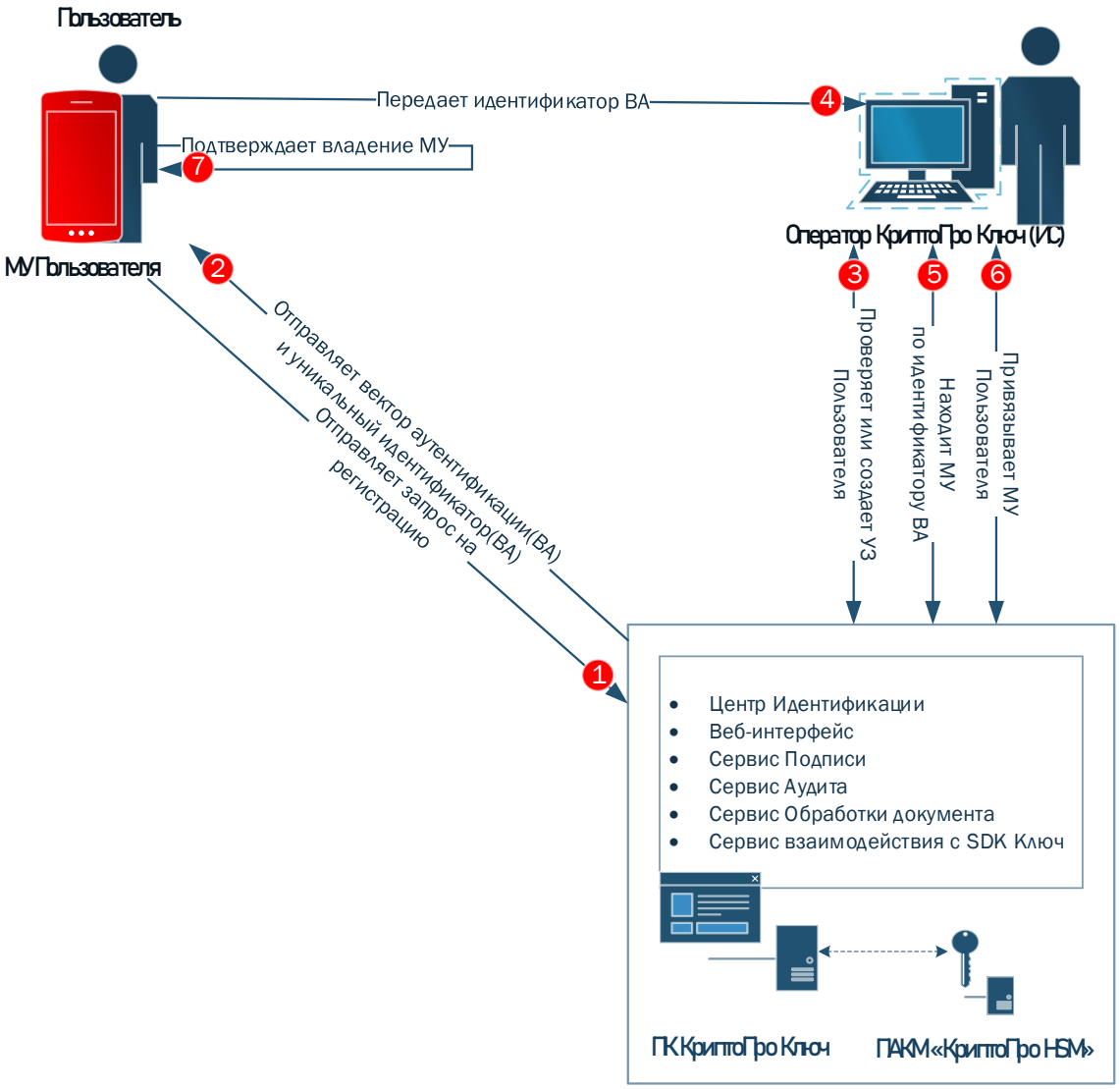

Рисунок 6 – Процесс привязки МУ Пользователя при помощи сверки уникального идентификатора

– Инициализация мобильного устройства при помощи выбранного идентификатора с дополнительной защитой QR-кодом. В данном случае необходима предварительная регистрация мобильного устройства Пользователя. Данный процесс представлен на рисунке 7;

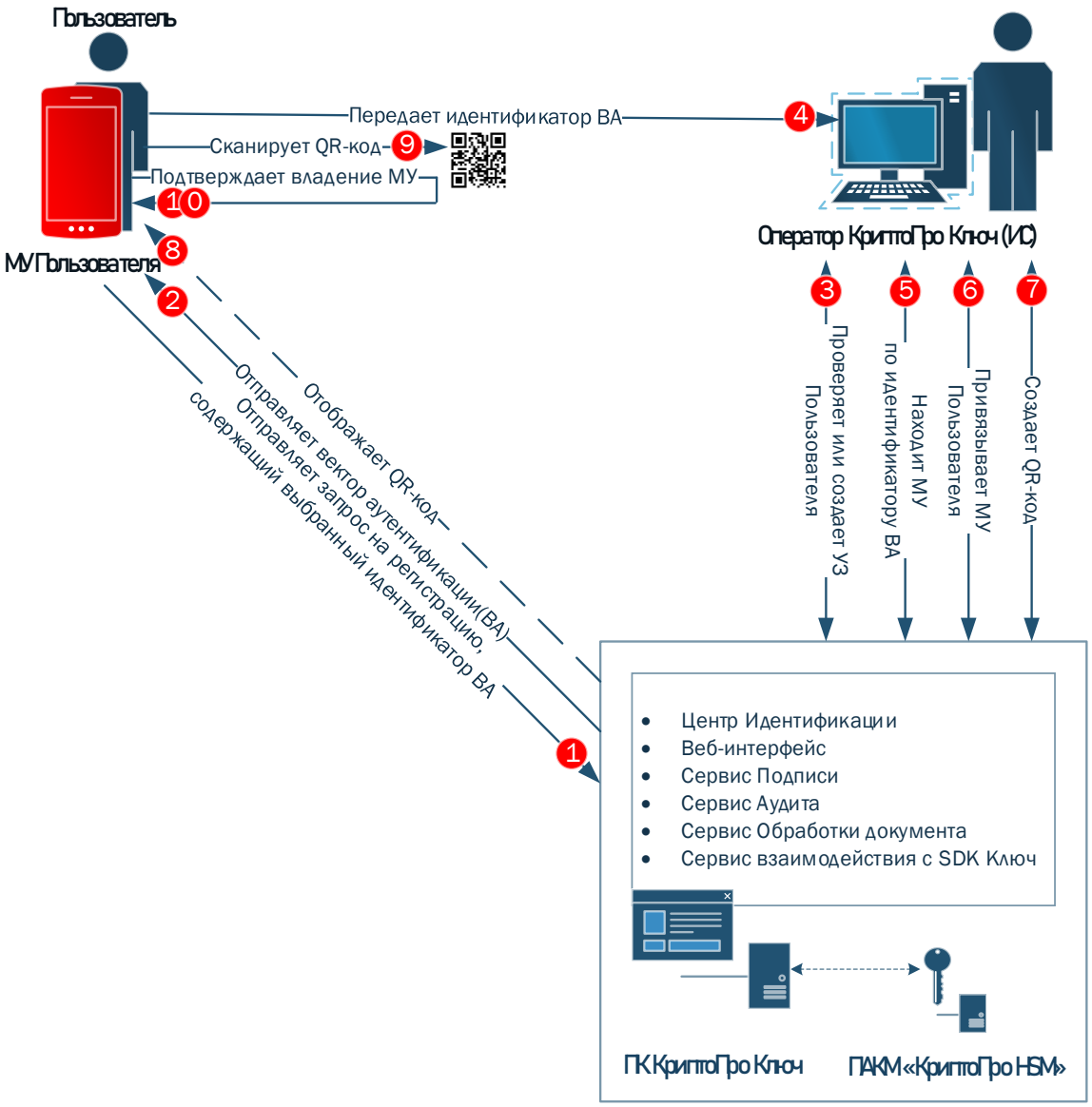

Рисунок 7 – Процесс привязки МУ Пользователя при помощи выбранного идентификатора с дополнительной защитой QR-кодом

– Инициализация мобильного устройства при помощи QR-кода с начальным вектором аутентификации. Данный процесс представлен на рисунке 8;

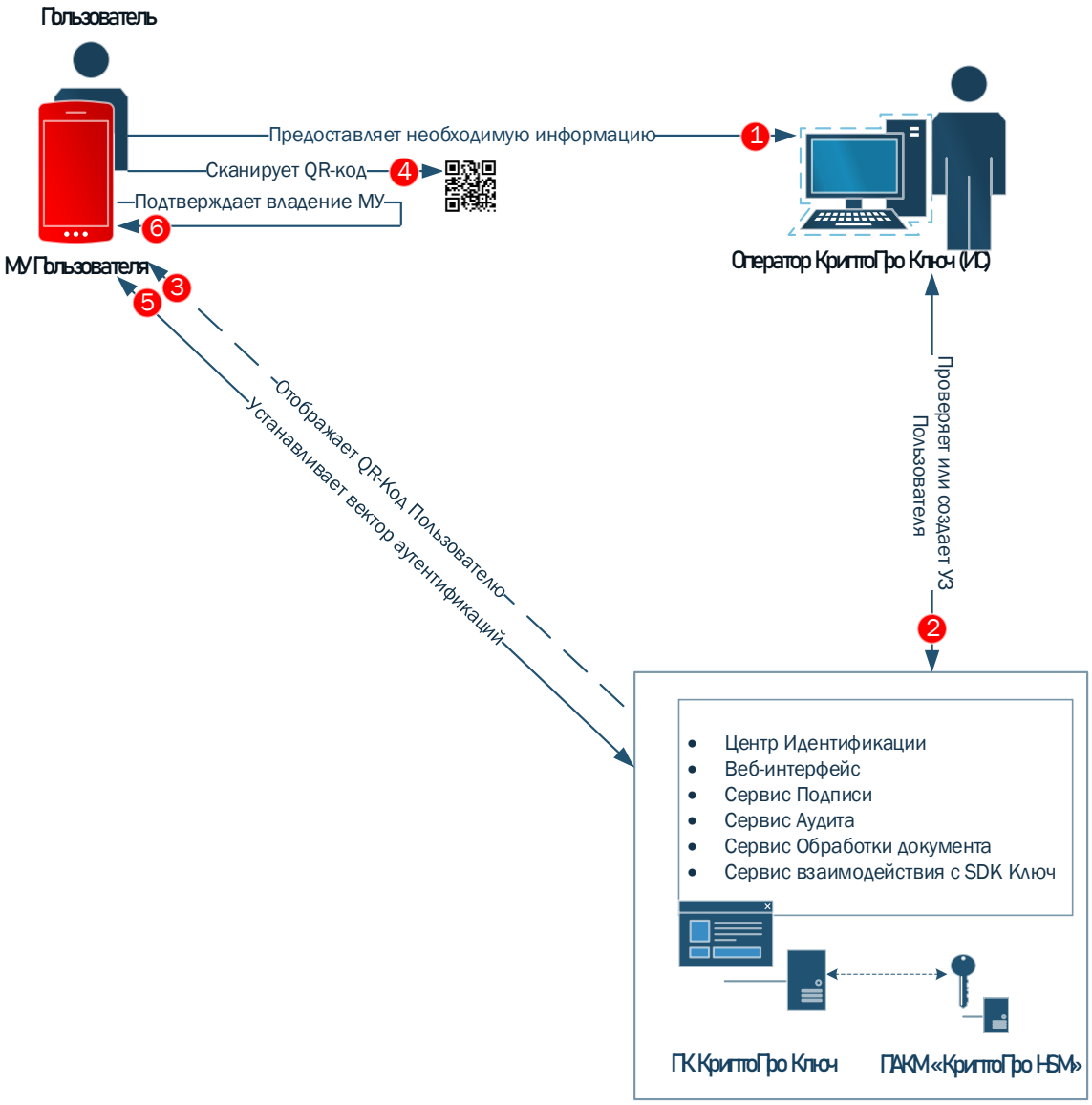

Рисунок 8 – Процесс привязки МУ Пользователя при помощи QR-кода с начальным вектором аутентификации

– Инициализация мобильного устройства при помощи самостоятельного получения сертификата. В данном случае необходима предварительная регистрация мобильного устройства Пользователя. Данный процесс представлен на рисунке 9;

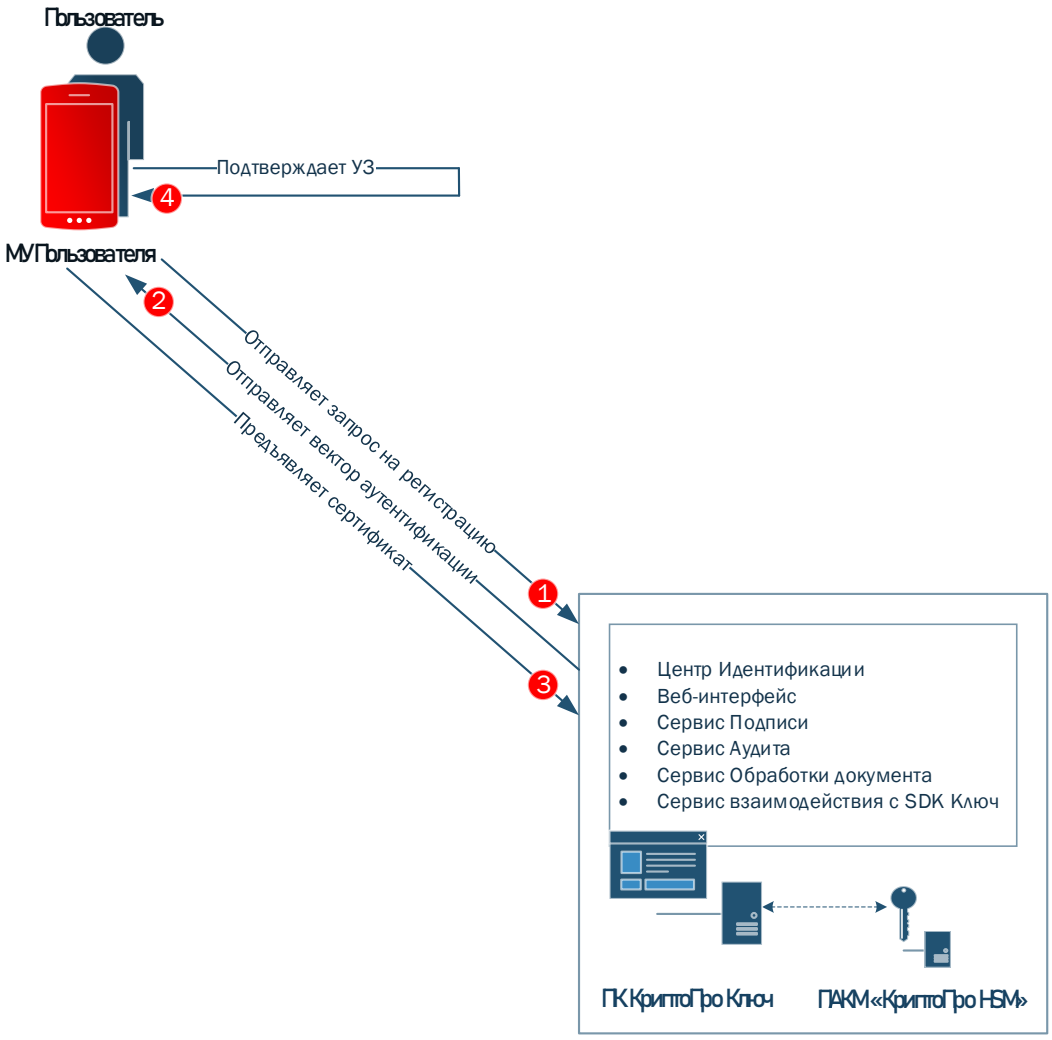

Рисунок 9 – Процесс привязка МУ Пользователя при помощи ранее полученного квалифицированного сертификата

9.3 Создание ключа и запроса на сертификат

Для выполнения криптографических операций у Пользователя в КриптоПро Ключ должны быть ключ подписи и сертификат ключа проверки электронной подписи (далее – сертификат). Ниже приведены варианты создания ключа подписи и запроса на сертификат в зависимости от выбранного режима хранения ключа подписи.

Создание запроса на сертификат может осуществляться самостоятельно с использованием устройства Пользователя (АРМ Пользователя или мобильное устройство) или с помощью Оператора.

При самостоятельном создании запроса на сертификат Пользователь, находясь под своей учетной записью, например, в мобильном приложении, отправляет запрос на выпуск сертификата, выбирая место хранения ключа. В веб-интерфейсе Оператор КриптоПро Ключ

выгружает запрос на сертификат. Оператор УЦ выпускает сертификат Пользователю. Далее Оператор КриптоПро Ключ/ Пользователь в веб-интерфейсе КриптоПро Ключ устанавливает сертификат в учетную запись Пользователя. Также Пользователь может самостоятельно установить сертификат в мобильном приложении.

Для генерации ЭП и создания запроса на сертификат необходима предварительная регистрация. Ниже на рисунке 10 схематично изображен процесс создания запроса на сертификат и выпуск сертификата.

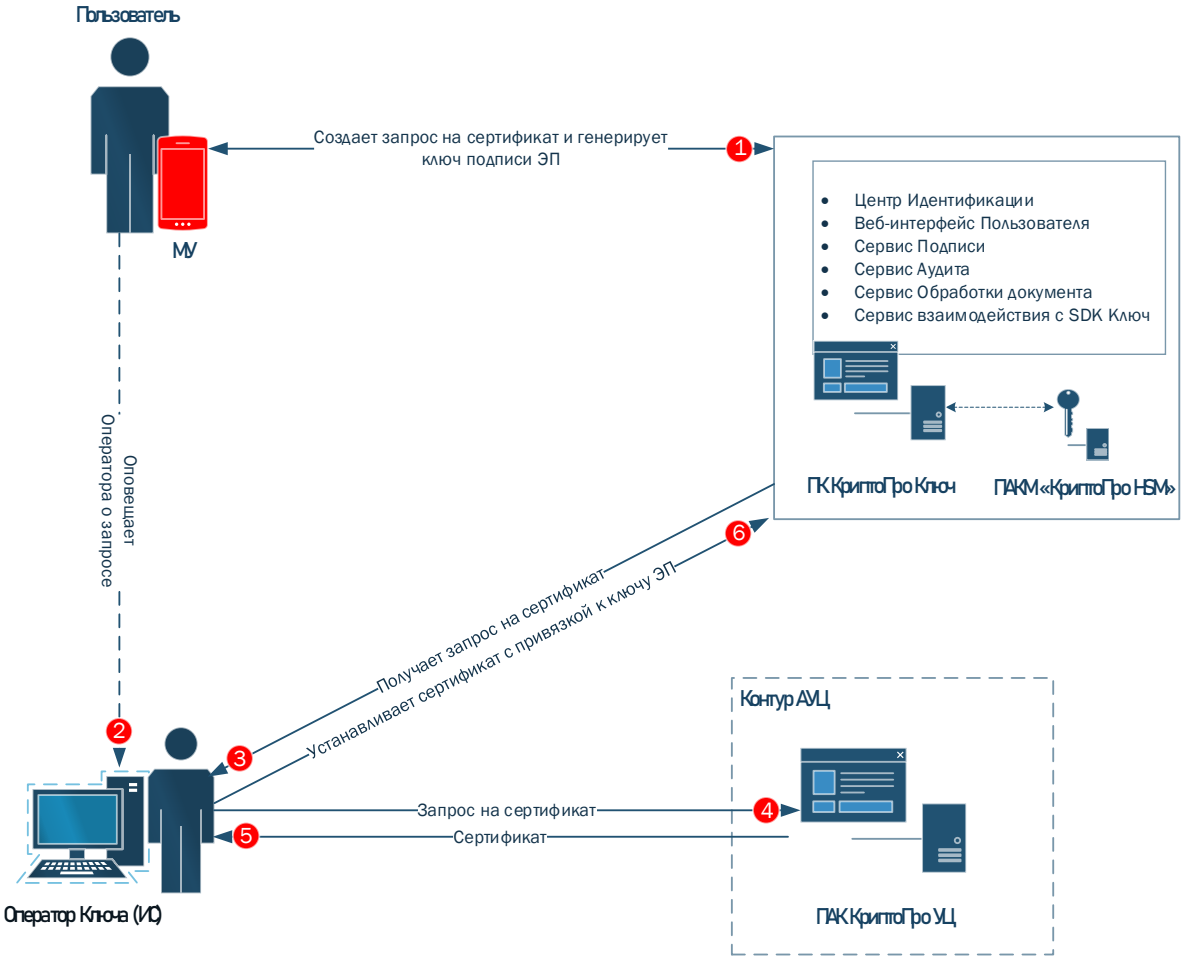

Рисунок 10 – Процесс создания и хранения ключа подписи в мобильном приложении Пользователем

При создании запроса на сертификат Оператором, Оператор КриптоПро Ключ заходит под своей учетной записью в веб – интерфейс КриптоПро Ключ и создает неподписанный запрос на сертификат с операцией подписания запроса на сертификат через мобильное устройство Пользователя. Далее Пользователю необходимо подписать запрос на сертификат и выбрать место расположения ключа подписи Пользователя. В веб-интерфейсе Оператор

КриптоПро Ключ выгружает запрос на сертификат. Оператор УЦ выпускает сертификат Пользователю. Далее Оператор КриптоПро Ключ/Пользователь в веб-интерфейсе КриптоПро Ключ устанавливает сертификат Пользователю.

Для генерации ЭП и создания запроса на сертификат необходима предварительная регистрация. Ниже на рисунке 11 схематично изображен процесс создания запроса на сертификат и выпуск сертификата.

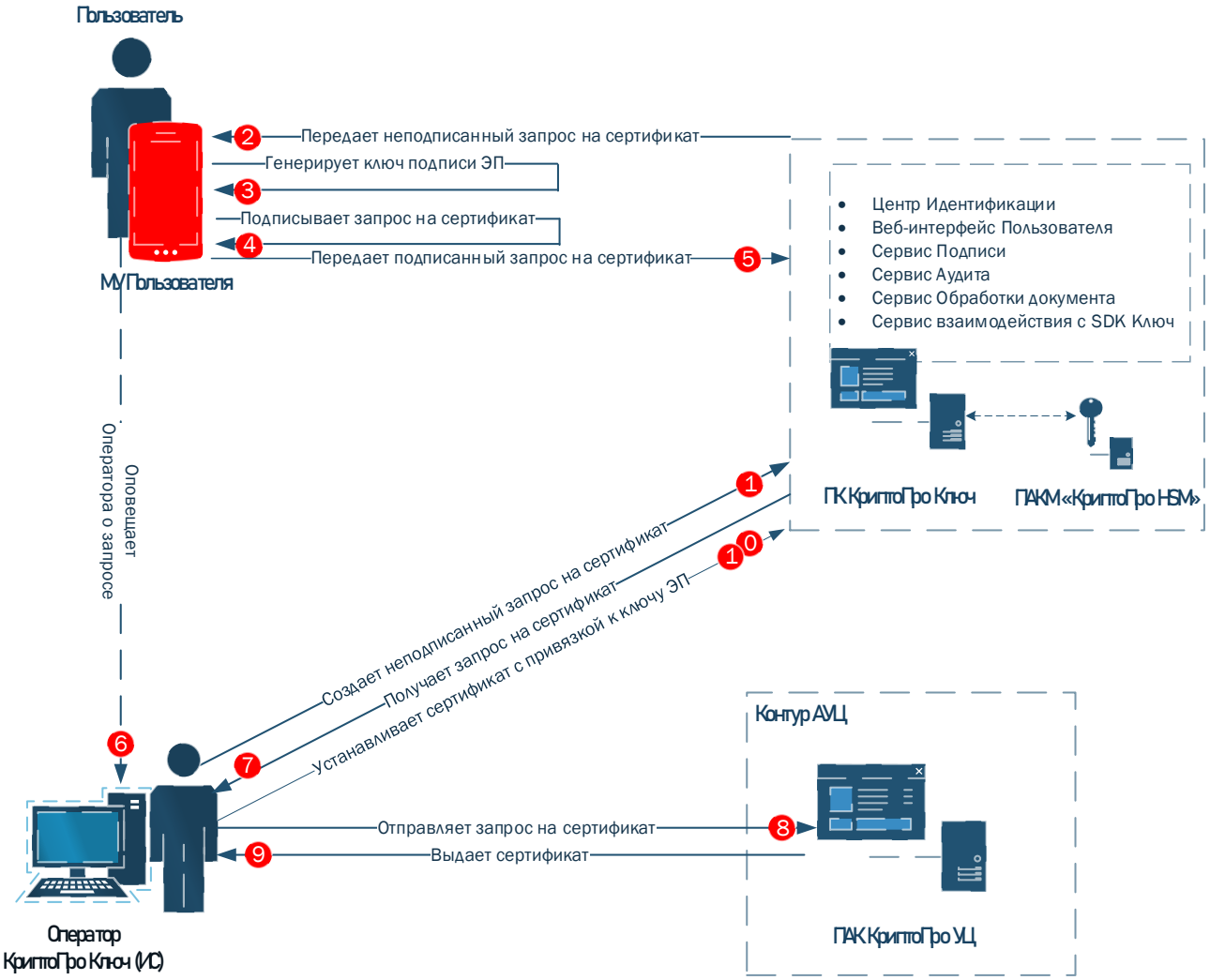

Рисунок 11 – Процесс создания и хранения ключа подписи в мобильном приложении при помощи Оператора

9.4 Подписание электронного документа

Одна из основных функций, поддерживаемых в КриптоПро Ключ – создание подписи электронных документов (далее – ЭД). Ниже приведено несколько вариантов подписания ЭД

в зависимости от выбранного режима хранения ключей подписи и настроек вторичной аутентификации.

Процесс подписания ЭД через мобильное приложение

Для подписания электронного документа Пользователю необходимо аутентифицироваться. Далее Пользователю в мобильном приложении необходимо выбрать нужный сертификат ЭП, подписываемый электронный документ, а также указать параметры и формат подписи (могут устанавливаться автоматически в соответствии с реализованной интеграцией прикладной информационной системы). В мобильном приложении КриптоПро Ключ отображается электронный документ перед выполнением операции с ним. После того, как Пользователь убедился, что хочет выполнить действия с нужным документом, выбирает кнопку «Подписать». Если операция подтверждена Пользователем, КриптоПро Ключ (при участии мобильного приложения, если ключ хранится в нем, на внешнем носителе или в распределенном виде) подписывает документ и возвращает его Пользователю в веб-интерфейсе, в мобильном приложении или при помощи интегрируемой системы. Данный процесс представлен на рисунке 12.

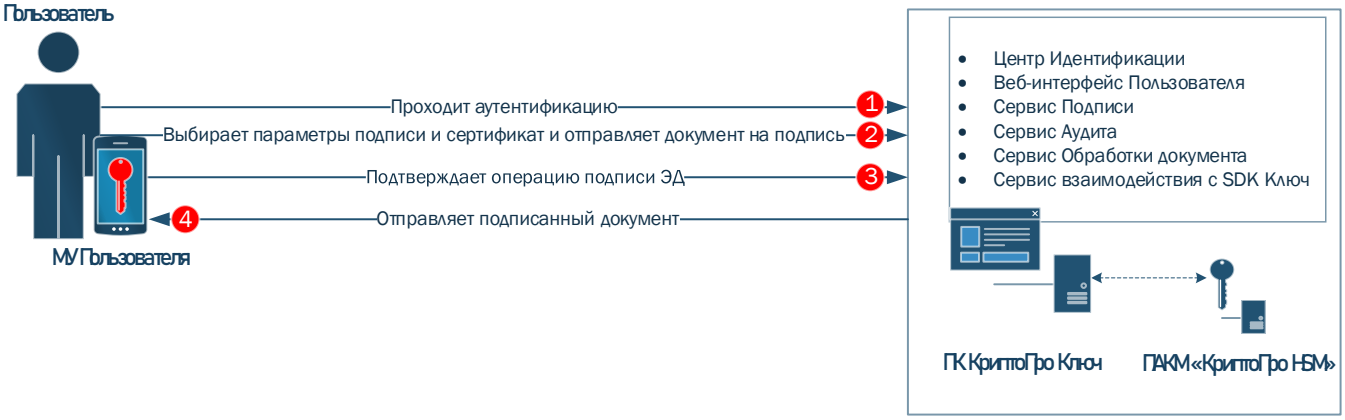

Рисунок 12 – Процесс подписания электронного документа через мобильное приложение, ключ хранится в мобильном приложении

Процесс подписания ЭД через веб-интерфейс интегрированной информационной системы

Для подписания электронного документа в веб-интерфейсе интегрированной информационной системы Пользователю необходимо выбрать сертификат и подписываемый

электронный документ, параметры и формат подписи устанавливаются в соответствии с реализованной интеграцией информационной системы. В мобильном приложении отображается электронный документ перед выполнением операции с ним. После того, как Пользователь убедился, что хочет выполнить действия с нужным документом, он выбирает кнопку «Подписать». Если операция подтверждена Пользователем, КриптоПро Ключ (при участии мобильного приложения, если ключ хранится в нем, на внешнем носителе или в распределенном виде) подписывает документ и возвращает его Пользователю в веб-интерфейсе, в мобильном приложении или при помощи интегрируемой системы. Данный процесс представлен на рисунке 13.

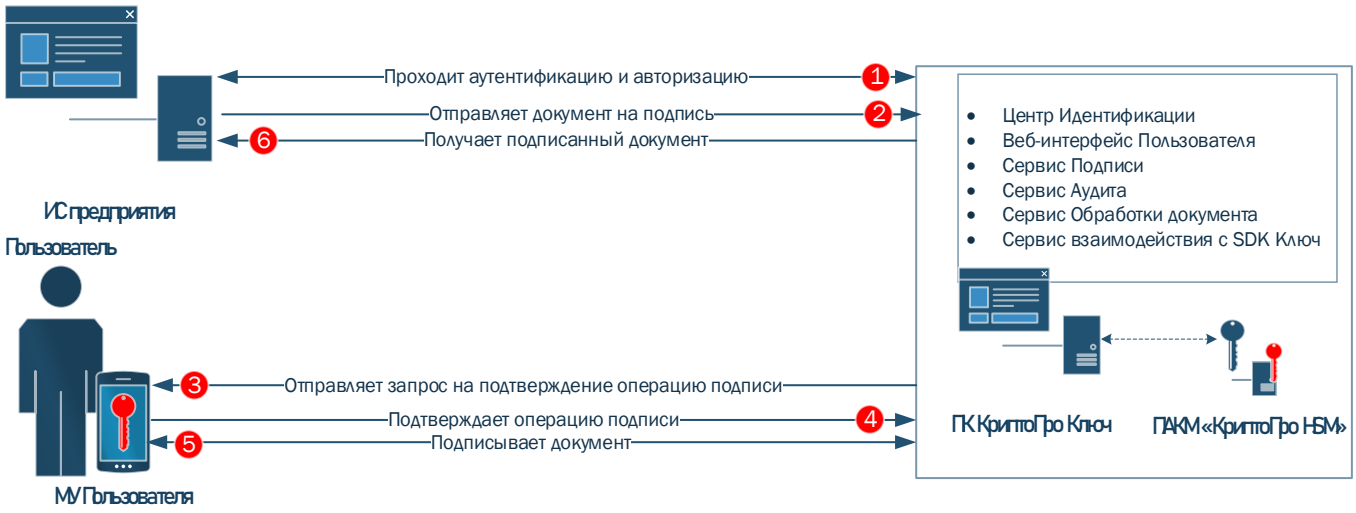

Рисунок 13 – Процесс подписания электронного документа через программный интерфейс интегрированной системы, ключ хранится в распределенном виде

Процесс подписания ЭД при использовании Ключ Lite

Пользователь, используя браузер, либо информационную систему отправляет в Ключ Lite документ, выбирает формат ЭП и нужный сертификат. Ключ Lite подготавливает документ к подписи, вычисляет от него хэш-значение и отправляет Пользователю. На стороне Пользователя происходит формирование электронной подписи полученного хэш-значения (средством ЭП Пользователя), после чего хэш-значение, его ЭП и сведения о ней передаются в Ключ Lite для завершения процедуры подписания. Ключ Lite формирует подписанный документ согласно выбранному формату подписи и возвращает его Пользователю. Данный процесс представлен на рисунке 14.

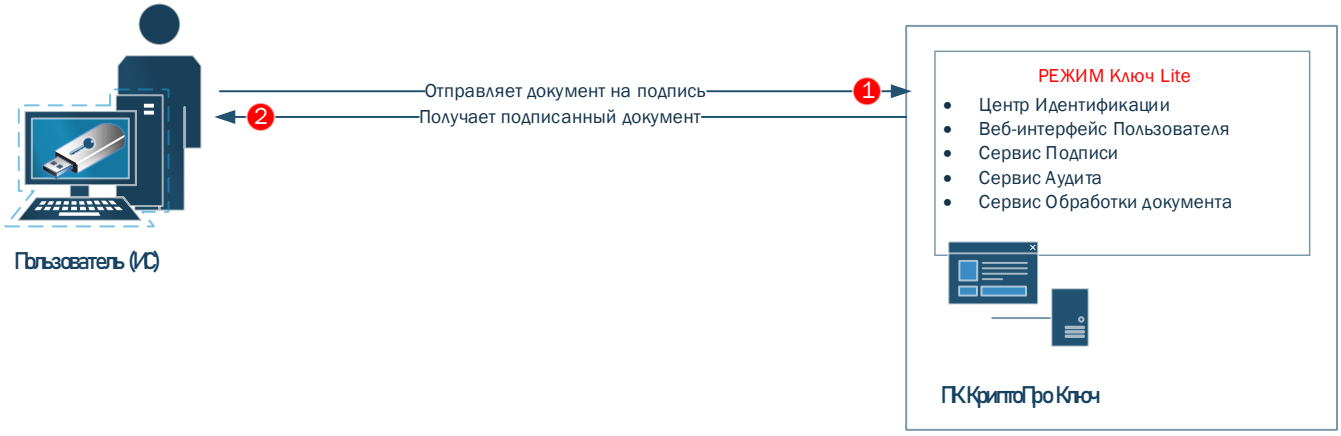

Рисунок 14 – Процесс подписания электронного документа при использовании Ключ Lite

9.5 Проверка подписи и Проверка сертификата ЭП

В КриптоПро Ключ реализована функция «Проверка электронной подписи» и «Проверка сертификата ЭП» с использованием ПО «Службы проверки сертификатов и электронной подписи «КриптоПро SVS»». Проверка подписи электронного документа и сертификата ЭП могут осуществляться Пользователем в интерактивном режиме как посредством штатного веб-интерфейса, так и интегрированной прикладной информационной системы по REST API.

Ниже на рисунке 15 продемонстрирован процесс «Проверка подписи» через веб-интерфейс Пользователя.

Рисунок 15 – Процесс проверки подписи

9.6 Шифрование электронного документа

В КриптоПро Ключ реализована функция «Шифрование ЭД», которая в зависимости от настроек может выполняться как с использованием веб-интерфейса, так и посредством программного интерфейса КриптоПро Ключ.

Пользователь инициирует операцию шифрования ЭД при помощи «Зашифровать» на веб-интерфейсе Пользователя или при помощи программного интерфейса интегрируемой системы, загружает или выбирает из списка имеющихся сертификат ЭП и документ, после чего происходит обращение к Сервису Подписи. Сервис Подписи находит сертификат в своей базе данных (далее – 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 Сервису Подписи. Сервис Подписи отправляет зашифрованный документ Пользователю. Данный процесс представлен на рисунке 16.

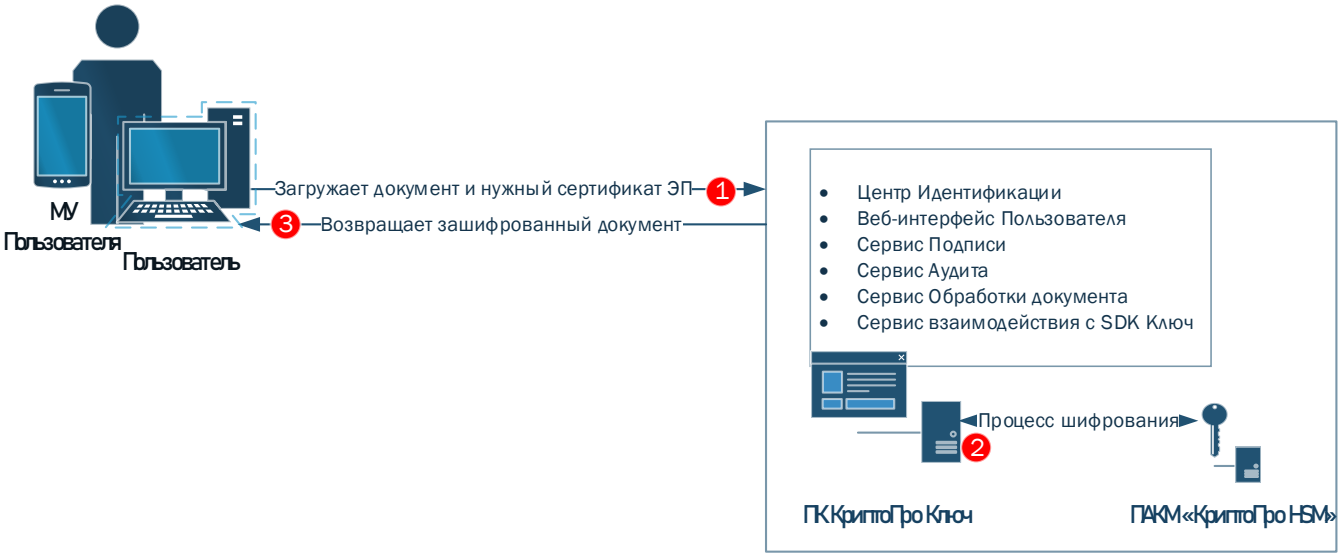

Рисунок 16 – Процесс шифрования документа

9.7 Расшифрование электронного документа

В КриптоПро Ключ реализована функция «Расшифрование ЭД», которая, в зависимости от настроек, может выполняться как с использованием веб-интерфейса, так и посредством программного интерфейса КриптоПро Ключ.

Пользователь инициирует операцию расшифрования ЭД при помощи «Расшифровать» на веб-интерфейсе Пользователя или при помощи программного интерфейса интегрируемой системы, загружает или выбирает из списка имеющихся сертификат и документ, после чего происходит обращение к Сервису Подписи. 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. Данный процесс представлен на рисунке 17.

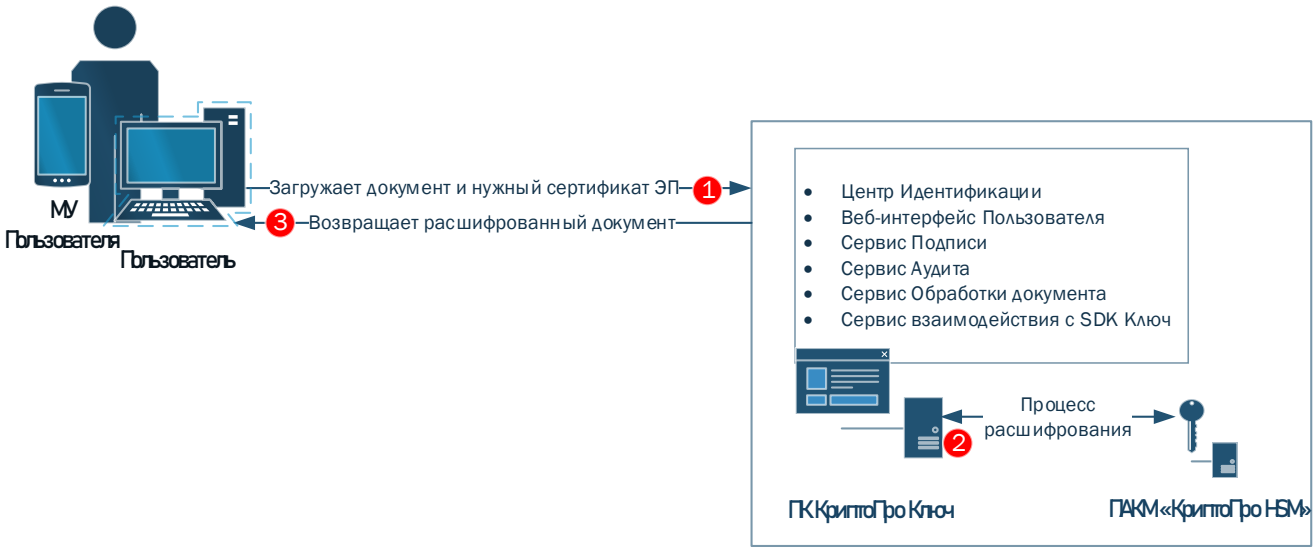

Рисунок 17 – Процесс расшифрования электронного документа

9.8 Аудит событий и формирование отчетов

Аудит компонентов КриптоПро Ключ производится при помощи компонента Сервиса Аудита. Аудит доступен для следующих компонентов КриптоПро Ключ:

– Центр Идентификации;

– Сервис Подписи;

– Сервис Обработки Документов.

Настройка аудита событий осуществляется Администратором системы. События записываются в журналы, которые отсылаются в Сервис Аудита и записываются в его БД.

Пользователю доступен только просмотр аудита событий и их сортировка по фильтру и/ или дате. Оператор может просматривать все действия Пользователя.

10 Основные преимущества использования КриптоПро Ключ

При использовании КриптоПро Ключ доступны следующие преимущества:

– централизованное управление сервисом ЭП в корпоративной ИТ – инфраструктуре;

– возможность разворачивания в импортозамещённой среде;

– использование отечественных криптографических алгоритмов;

– различные способы хранения и использования ключей ЭП - мобильная/распределенная/локальная подпись;

– множество схем аутентификации Пользователя для доступа к ключам;

– множество поддерживаемых видов и форматов подписи и шифрования документов;

– REST API для реализации различных сценариев работы;

– возможность работы как на десктопе, так и в мобильном приложении;

– возможность работы с ключами Пользователей на NFC-токене;

– обеспечение юридической значимости электронного документа в соответствии с требованиями законодательства Российской Федерации.

11 Возможные варианты использования КриптоПро Ключ

Компания ООО «КриптоПро» предлагает два варианта использования решения ПК «КриптоПро Ключ»:

– разворачивание решения в инфраструктуре вашего предприятия;

– использование Сервиса электронной подписи ООО «КРИПТО-ПРО».

В обоих случаях вы получаете полный доступ ко всем функциям продукта и можете использовать его для решения своих задач.

Для разворачивания решения в инфраструктуре вашего предприятия необходимо приобрести:

– серверное и сетевое оборудование;

– лицензии на системное и прикладное ПО;

– лицензии на продукты компании ООО «КРИПТО-ПРО»;

– техническое проектирование, разработку рабочей-эксплуатационной и организационно-распорядительной документации;

– услуги по внедрению и технической поддержке системы.

Для использования Сервиса электронной подписи компании ООО «КРИПТО-ПРО» на базе ПК «КриптоПро Ключ» и ПАКМ «КриптоПроHSM» необходимо приобрести:

– Лицензии компании ООО «КРИПТО-ПРО»;

– услуги сервиса электронной подписи;

– услуги удостоверяющего центра;

– услуги по разработке внутренних организационно-распорядительных документов, определяющих порядок эксплуатации сервиса ЭП.

12 Полезные ссылки для ознакомления с функционалом КриптоПро Ключ

Для ознакомления с функционалом системы вы можете воспользоваться нашим тестовым сервисом электронной подписи или самостоятельно установить виртуальную машину у себя.

Для интеграции с тестовым контуром СЭП на базе ПК «КриптоПро Ключ» следует подать Заявку на подключение для Оператора.

Для установки виртуального стенда загрузите готовую виртуальную машину на странице по ссылке https://cryptopro.ru/products/ca/2.0/howto

Также есть возможность пройти обучающие курсы от Учебного центра «Информзащита»:

- Т215 Порядок развертывания и применения ПК "КриптоПро Ключ" 1.0. на платформе Astra Linux.
- Т534 Порядок развертывания, применения и мониторинга инфраструктуры для усовершенствованной электронной подписи на основе ПК "КриптоПро Ключ" и технологий КриптоПро.

13 Контактная информация

По всем вопросам обращайтесь на почту: **info@cryptopro.ru**

Канал новостей: https://t.me/cryptopro_news

Сайт КриптоПро: https://www.cryptopro.ru/