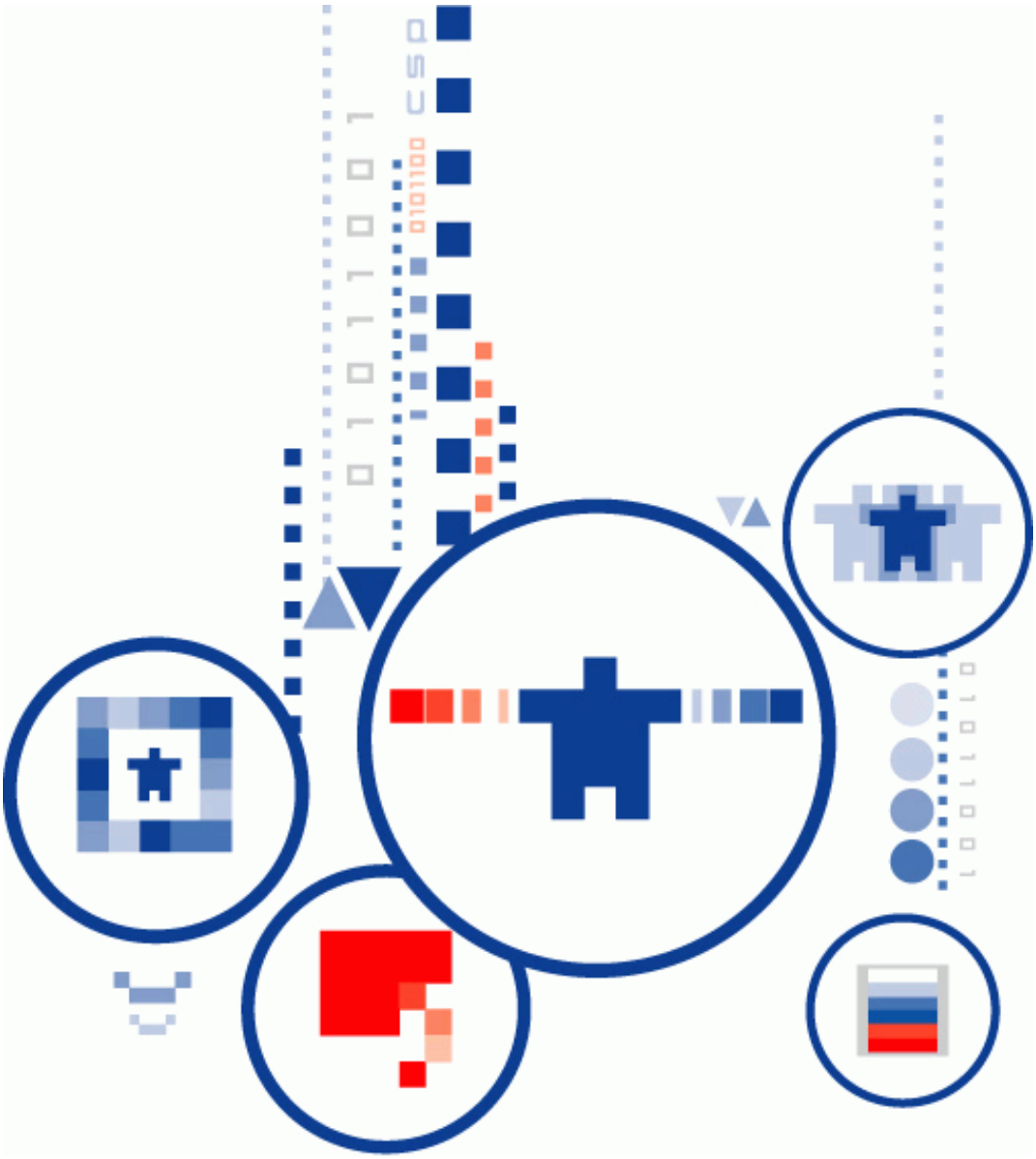

Сервер Электронной Подписи

«КриптоПро DSS»

Компонент ПАКМ «КриптоПро HSM»

Общее описание

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CAdES	—	Расширенная версия стандарта электронной подписи CMS (CMS Advanced Electronic Signatures)
CMIS	—	Сервисы взаимодействия при управлении контентом (Content Management Interoperability Services)
CRL	—	Список отзыва сертификатов (Certificate Revocation List)
CSP	—	Криптопровайдер (Cryptographic Service Provider)
HSM	—	Аппаратный модуль системы безопасности (Hardware security module)
HOTP	—	алгоритм защищенной аутентификации с использованием одноразового пароля. (HMAC-Based One-Time Password Algorithm)
IIS	—	Набор серверов от компании Microsoft (Internet Information Services)
OATH	—	Набор алгоритмов аутентификации с использованием одноразовых паролей
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)
OTP	—	Пароль, действительный только для одного сеанса аутентификации (One-Time Password)
REST	—	Архитектурный стиль построения распределенного приложения (Representational State Transfer)
RFC	—	Рекомендация Internet Engineering Task Force (Request for Comments)
SAML	—	Язык разметки декларации безопасности, язык разметки, основанный на языке XML (Security Assertion Markup Language)
SDK	—	Набор программных компонентов для использования в мобильных приложениях (Software development kit)
SOAP	—	Простой протокол доступа к объектам (Simple Object Access Protocol)
SSL	—	Протокол защиты сокетов (Secure Sockets Layer)
TLS	—	Протокол защиты транспортного уровня (Transport Layer Security)
TOTP	—	OATH-алгоритм создания одноразовых паролей для защищенной аутентификации, генерирующий пароль на основе времени. (Time-based One Time Password Algorithm)
URL	—	Единый указатель ресурсов (Uniform Resource Locator)
АРМ	—	Автоматизированное рабочее место
БД	—	База данных
ИС	—	Информационная система
НСД	—	Несанкционированный доступ
МЭ	—	Межсетевой экран
ОС	—	Операционная система
ПАК	—	Программно-аппаратный комплекс
ПАКМ	—	Программно-аппаратный криптографический модуль
ПО	—	Программное обеспечение
СКЗИ	—	Средство криптографической защиты информации
СУБД	—	Система управления базой данных
СЭП	—	Сервер электронной подписи
УЦ	—	Удостоверяющий Центр
ЭП	—	Электронная подпись

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Апплет	—	Программный компонент в двоичном коде виртуальной машины Java.
Владелец сертификата открытого ключа	—	лицо, которому в установленном Федеральным законом (№63-ФЗ от 06.04.2011 г. «Об электронной подписи») порядке выдан сертификат открытого ключа.
Закрытый ключ	—	уникальная последовательность символов, предназначенная для шифрования.
Квалифицированный сертификат открытого ключа (квалифицированный сертификат)	—	сертификат открытого ключа, выданный аккредитованным удостоверяющим центром или доверенным лицом аккредитованного удостоверяющего центра либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи.
Ключ проверки электронной подписи	—	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи.
Ключ электронной подписи	—	уникальная последовательность символов, предназначенная для создания электронной подписи
Мобильное устройство	—	смартфон или планшет, являющийся собственностью Пользователя КриптоПро DSS.
Средства электронной подписи	—	шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций - создание электронной подписи, проверка электронной подписи, создание закрытого и открытого ключей.
Сертификат открытого ключа	—	электронный или бумажный документ, содержащий открытый ключ, информацию о владельце ключа, области применения ключа, подписанный выдавшим его Удостоверяющим центром и подтверждающий принадлежность открытого ключа владельцу.
Удостоверяющий центр	—	юридическое лицо или индивидуальный предприниматель, осуществляющие функции по созданию и выдаче сертификатов открытых ключей, а также иные функции, предусмотренные Федеральным законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи».
Учетная запись	—	Набор сведений о Пользователе КриптоПро DSS, содержащий необходимое и достаточное для работы с DSS количество информации.
Электронная подпись	—	информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

1. Аннотация

В настоящее время почти каждая организация использует электронный документооборот — как внешний, так и внутренний. Информация пересылается внутри ИС, используемых компанией, по электронной почте и даже иногда посредством некоторых внешних сервисов. В случае перехвата злоумышленником передаваемой информации, ее конфиденциальность, целостность и аутентичность могут быть нарушены. Определить истинное авторство документа и убедиться в том, что он не был изменен в процессе передачи по каналам связи позволяет использование электронной цифровой подписи, а шифрование обеспечивает конфиденциальность документов.

Настоящий документ содержит описание Сервера Электронной Подписи (СЭП) «КриптоПро DSS». КриптоПро DSS используется для создания электронной подписи, шифрования документов, а также для централизованного защищенного хранения закрытых ключей Пользователей. Для хранения в КриптоПро DSS сертификатов и закрытых ключей Пользователей в зашифрованном виде, а также для реализации криптографических операций используется ПАКМ «КриптоПро HSM».

В данном документе приведено назначение СЭП и основные решаемые им задачи, описаны входящие в него компоненты и архитектура предлагаемого решения. Описаны системные требования к продукту и возможности интеграции с другими ИС.

Документ предназначен для руководителей и администраторов как ознакомительный материал перед установкой и эксплуатацией программного обеспечения КриптоПро DSS.

2. Общие сведения

2.1. Назначение КриптоПро DSS

Сервер Электронной Подписи «КриптоПро DSS» (далее — КриптоПро DSS) предназначен для:

- Централизованного защищенного хранения закрытых ключей Пользователей (в соответствии с выбранным режимом хранения ключей);
- 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.

2.2. Цели КриптоПро DSS

Целями использования КриптоПро DSS являются:

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

2.3. Задачи КриптоПро DSS

Для выполнения поставленных целей КриптоПро DSS 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;
- 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 (см. раздел 7.4):
- Оповещение Пользователей о событиях при взаимодействии с КриптоПро DSS (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.

2.4. Исполнения КриптоПро DSS

Подключение к серверу КриптоПро DSS со стороны пользователя должно осуществляться исключительно с использованием клиентских компонент, определенных

для соответствующего исполнения. Подключение к серверу КриптоПро DSS иными способами не допускается. Существуют следующие исполнения КриптоПро DSS:

- КриптоПро DSS + КриптоПро CSP версия 4.0 Исполнение 1-Base, уровень защиты КС1.
- КриптоПро DSS + КриптоПро CSP версия 4.0 Исполнение 2-Base, уровень защиты КС2.
- КриптоПро DSS + КриптоПро CSP версия 4.0 Исполнение 3-Base, уровень защиты КС3.
- КриптоПро DSS + КриптоПро CSP версия 4.0 Исполнение 1-Lic, уровень защиты КС1.
- КриптоПро DSS + КриптоПро CSP версия 4.0 Исполнение 2-Lic, уровень защиты КС2.
- КриптоПро DSS + КриптоПро CSP версия 5.0 Исполнение 1-Base, уровень защиты КС1.
- КриптоПро DSS + КриптоПро CSP версия 5.0 Исполнение 2-Base, уровень защиты КС2.
- КриптоПро DSS + КриптоПро CSP версия 5.0 Исполнение 3-Base, уровень защиты КС3.
- КриптоПро DSS + КриптоПро JCP версия 2.0 Исполнение 2, уровень защиты КС1.
- КриптоПро DSS + SIM (QES), уровень защиты КС1.
- КриптоПро DSS + SIM (M2M), уровень защиты КС1.
- КриптоПро DSS + myDSS, уровень защиты КС1.
- КриптоПро DSS + AirKey Lite, уровень защиты КС1.
- myDSS SDK, уровень защиты КС1.
- Сбербанк myDSS SDK, уровень защиты КС1.
- DSS Client SDK, уровень защиты КС1.

3. Описание КриптоПро DSS

3.1. Состав КриптоПро DSS

КриптоПро DSS включает в себя следующие компоненты:

- Центр Идентификации (ЦИ, см. раздел 3.2.1):
  - Веб-интерфейс ЦИ;
  - Модуль аутентификации myDSS;
  - Служба управления Пользователями;
  - Служба маркеров безопасности;
  - Сервис рассылки уведомлений;
  - БД ЦИ.
- Сервис Подписи (см. раздел 3.2.2):
  - 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 3.2.3);
- Сервис Аудита (см. раздел 3.2.4):
  - ПО Сервиса Аудита;
  - Веб-интерфейс Сервиса Аудита;
  - БД Сервиса Аудита.
- Сервис Обработки Документов (см. раздел 3.2.5);
- Сервис взаимодействия с DSS SDK (см. раздел 3.2.7);
- ПАКМ «КриптоПро HSM» (см. раздел 3.2.6);
- Клиентские компоненты (см. раздел 3.2.8):
  - КриптоПро CSP/JCP/Cloud CSP;
  - Мобильное приложение myDSS/AirKey Lite;
  - DSS SDK для встраивания в мобильное приложение;
  - Апплет на SIM-карте.

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

3.2. Описание компонентов КриптоПро DSS

3.2.1. 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 DSS (см. раздел 4).
- 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 3.2.4).

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. Подробнее о ролях в КриптоПро DSS см. раздел 10.

Модуль аутентификации myDSS

Модуль аутентификации myDSS для КриптоПро DSS является обособленной частью Центра Идентификации и позволяет подтверждать волеизъявление Пользователя о выполнении различных операций с помощью мобильного приложения, а также может применяться при вспомогательной аутентификации. Модуль используется в КриптоПро DSS только в исполнениях КриптоПро DSS «DSS + myDSS» и «DSS + AirKey Lite», уровень защиты КС1. (см. раздел 2.4).

Модуль аутентификации myDSS имеет следующую структуру:

1. Серверная часть:

1.1. Сервис взаимодействия с ЦИ.

Интегрируется с ЦИ КриптоПро DSS и выполняет следующие функции:

- генерация и обновление ключевой информации Пользователей myDSS при взаимодействии с ЦИ КриптоПро DSS;
- управление процессом подтверждения операций.

1.2. Сервис взаимодействия с мобильным приложением myDSS.

Выполняет функции по взаимодействию с мобильными приложениями, включая:

- регистрацию устройств Пользователей для отправки PUSH-уведомлений;
- отправку PUSH-уведомлений;
- предоставление информации о операциях, необходимых для подтверждения Пользователем;
- прием и проверку кодов подтверждения при помощи Сервиса взаимодействия с ЦИ.

2. Клиентская часть:

Клиентская часть представлена мобильным приложением myDSS, доступным в операционных системах iOS и Android (см. раздел 3.2.7).

Схема взаимодействия компонентов, отображающая описанные логические компоненты myDSS и их взаимодействие с другими компонентами и продуктами, приведена в разделе 7.2.

Служба управления Пользователями

Служба управления Пользователями является обособленной частью Центра Идентификации и отвечает за регистрацию Пользователей и Операторов КриптоПро DSS, 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 DSS.

Сервис рассылки уведомлений

Сервис рассылки уведомлений является центральным узлом, где обрабатываются события, поступающие от других компонентов КриптоПро DSS. В зависимости от настроек, Сервис рассылки уведомлений формирует SMS-, Email- и PUSH-уведомления, рассылаемые Пользователям и Операторам.

3.2.2. Сервис Подписи

Компонент КриптоПро DSS 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».

3.2.3. Веб-интерфейс Пользователя

Компонент КриптоПро DSS Веб-интерфейс Пользователя предназначен для организации интерактивного взаимодействия Пользователей с компонентами КриптоПро DSS, а также с другими внешними компонентами. Произведенные Пользователями действия на веб-формах с помощью REST API передаются в другие компоненты КриптоПро DSS 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. Подробнее о типах подписи см. раздел 11.
- **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). Подробнее о типах подписи см. раздел 11.
- **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 DSS. 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 DSS.

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.

3.2.4. Сервис Аудита

Компонент Сервис Аудита предназначен для аудита событий, поступающих с компонентов КриптоПро DSS. 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 DSS (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.

3.2.5. Сервис Обработки Документов

Сервис Обработки Документов (СОД) предназначен для работы с документами, отправленными на подпись или шифрование/расшифрование в КриптоПро DSS. 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.

3.2.6. 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 DSS 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.

3.2.7. Сервис Взаимодействия с DSS SDK

Сервис взаимодействия с DSS SDK для мобильного приложения (DSS Api Gateway) предоставляет доступ к компонентам КриптоПро DSS при взаимодействии с ними через КриптоПро DSS SDK.

Схема взаимодействия компонентов, отображающая взаимодействие DSS Api Gateway с другими компонентами и продуктами, приведена в разделе 7.3.

Сервис взаимодействия с DSS SDK используется в исполнениях «myDSS SDK», «Сбербанк myDSS SDK» и «DSS Client SDK» (см. раздел 2.4).

3.2.8. Клиентские компоненты

КриптоПро CSP/JCP/Cloud CSP

СКЗИ «КриптоПро CSP» может применяться Пользователем для установления безопасного соединения с серверами КриптоПро DSS при аутентификации по логину и паролю, а также по сертификату (см. разделы 4.1–4.2). КриптоПро CSP необходимо использовать на стороне Пользователя в исполнениях «DSS + CSP» всех версий и Исполнений, приведенных в разделе 2.4.

Аналогично, СКЗИ «КриптоПро JCP» может применяться Пользователем для установления безопасного соединения с серверами КриптоПро DSS при аутентификации по логину и паролю, а также по сертификату (см. разделы 4.1–4.2). КриптоПро JCP необходимо использовать на стороне Пользователя в исполнении «DSS + JCP версия 2.0 Исполнение 2» (см. раздел 2.4).

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 DSS, а также генерировать ключи Пользователей и создавать запросы на сертификат. Дополнительно Cloud CSP предоставляет возможность использовать ключи, хранимые в КриптоПро DSS, для аутентификации клиента в рамках взаимодействия по протоколу TLS во всех сценариях, поддерживаемых КриптоПро CSP версии 5.0.

Мобильное приложение myDSS/AirKey Lite

Мобильное приложение myDSS/AirKey Lite является клиентской частью модуля аутентификации myDSS (см. раздел 3.2.1) и доступно для операционных систем iOS и Android.

Приложение myDSS/AirKey Lite выполняет следующие функции:

- управление ключевой информацией Пользователя (считывание, хранение, использование, обновление, удаление);
- получение информации для подтверждения от серверной части в режиме онлайн или офлайн;
- отображение подтверждаемой информации на экране мобильного телефона;
- выработка кода подтверждения на основе данных транзакции, ключа Пользователя, времени выработки и (опционально) отпечатка устройства;
- отправка кода подтверждения в серверную часть в режиме онлайн или отображение Пользователю в режиме офлайн.

Способы аутентификации Пользователя при помощи мобильного приложения myDSS/AirKey Lite приведены в разделах 4.5–4.6.

Схема взаимодействия компонентов, отображающая взаимодействие myDSS/AirKey Lite с другими компонентами и продуктами, приведена в разделе 7.2.

Использование мобильного приложения myDSS/AirKey Lite допускается в исполнениях КриптоПро DSS «DSS + myDSS» и «DSS + AirKey Lite» (см. раздел 2.4).

DSS SDK для встраивания в мобильное приложение

DSS 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 DSS, инициированные другими способами. Возможности создания мобильных приложений на базе DSS SDK описаны в разделе 3.3.

Способы аутентификации Пользователя при помощи мобильного приложения на базе DSS SDK приведены в разделах 4.7–4.8.

Схема взаимодействия компонентов, отображающая взаимодействие мобильного приложения на базе DSS SDK с другими компонентами и продуктами, приведена в разделе 7.3.

Использование мобильного приложения на базе DSS SDK допускается в исполнениях КриптоПро DSS «myDSS SDK», «Сбербанк myDSS SDK» и «DSS Client SDK» (см. раздел 2.4).

Апплет на SIM-карте

Апплет на SIM-карте представляет собой программный компонент, который устанавливается на SIM-карту при ее производстве (см. раздел 4.11.2). Пользователь, на SIM-карте которого находится апплет, установленный и настроенный для работы с КриптоПро DSS, может использовать способы аутентификации, описанные в разделах 4.4 и 4.5.

Требования к SIM-картам и необходимая для установки и настройки апплета информация приводятся в документе «ЖТЯИ.00096-02 98 02 КриптоПро DSS. Технические условия для записи апплета на SIM-карту».

Способы аутентификации Пользователя при помощи апплета на SIM-карте приведены в разделах 4.3, 4.4 и 4.9.

Использование апплета на SIM-карте допускается в исполнениях КриптоПро DSS «DSS + SIM (QES)» и «DSS + SIM (M2M)» (см. раздел 2.4).

3.3. Возможности создания мобильных приложений, использующих КриптоПро DSS

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

1. Обмен данными между мобильным приложением на базе DSS SDK и КриптоПро DSS 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 DSS SDK, каждое из которых может использоваться для подтверждения операций.
8. В мобильном приложении возможно управление сертификатами Пользователя.

Использование мобильного приложения на базе DSS SDK допускается в исполнениях КриптоПро DSS «myDSS SDK», «Сбербанк myDSS SDK» и «DSS Client SDK» (см. раздел 2.4).

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

4. Аутентификация в КриптоПро DSS

При входе в КриптоПро DSS, а также операциях, требующих доступа к ключевой информации, в DSS предусмотрена аутентификация Пользователей. В настоящем разделе описаны методы аутентификации. Срок жизни всех векторов аутентификации, упоминаемых в данном разделе, составляет 1 год и 3 месяца.

В случае со способами, описанными в разделах 4.1, 4.2, 4.3 и 4.5, для аутентификации на рабочей станции Пользователя требуется наличие сертифицированного ФСБ России СКЗИ КриптоПро CSP версии 3.9, 4.0 или КриптоПро JCP версии 2.0.

4.1. Аутентификация по логину и паролю

Данный метод требует установки защищенного TLS-соединения с односторонней аутентификацией (просмотр и подтверждение операции с загруженным на сервер документом производятся в рамках взаимодействия по защищенному каналу). Аутентификация производится по паролю, хранимому в БД Центра Идентификации КриптоПро DSS. При этом должно быть обеспечено отсутствие подключений (прямых или опосредованных) компонентов к сетям общего пользования.

Описанный метод аутентификации реализуется в исполнениях, приведенных в разделе 2.4 и соответствующих классу защиты КС1.

4.2. Аутентификация по сертификату

Данный метод требует установки защищенного TLS-соединения с двусторонней аутентификацией (просмотр и подтверждение операции с загруженным на сервер документом производятся в рамках взаимодействия по защищенному каналу). Аутентификация производится с использованием пары ключей, закрытая часть которой хранится у Пользователя, а сертификат открытого ключа должен быть доверенным для КриптоПро DSS.

Аутентификация по сертификату реализуется в исполнениях «DSS + CSP» всех версий и Исполнений, приведенных в разделе 2.4, а также в исполнении «DSS + JCP версия 2.0 Исполнение 2».

4.3. Аутентификация по логину и паролю с подтверждением операций с помощью апплета на SIM-карте

Данный метод аналогичен методу, описанному в разделе 4.1, с тем лишь отличием, что отсутствие подключений к сетям общего пользования необязательно.

Кроме аутентификации по паролю, данный метод аутентификации подтверждает операции с помощью апплета на SIM-карте. Подписываемый документ отображается в Веб-интерфейсе DSS. КриптоПро DSS генерирует для этого документа уникальный идентификатор, который отображается как в Веб-интерфейсе DSS, так и в сервисном сообщении на мобильном устройстве. Пользователь сравнивает идентификаторы и в случае их совпадения подтверждает операцию, после чего ему требуется ввести ПИН-код. Такой метод подтверждения применим для создания ЭП любых документов.

Описанный метод аутентификации реализуется в исполнении КриптоПро DSS «DSS + SIM (QES)» (см. раздел 2.4).

4.4. Аутентификация с помощью апплета на SIM-карте

При данном методе аутентификации Пользователь не имеет прямого доступа к Веб-Интерфейсу DSS. Интегрированная с КриптоПро DSS информационная система инициирует операцию создания ЭП документа, после чего подписываемый документ отображается в сервисном сообщении на мобильном устройстве. Пользователь просматривает его, убеждается, что хочет выполнить операцию именно с этим документом, и подтверждает ее, после чего ему требуется ввести ПИН-код. Такой метод подтверждения применим для создания ЭП коротких текстовых документов, длина которых не превышает 300 символов.

Описанный метод аутентификации реализуется в исполнении КриптоПро DSS «DSS + SIM (QES)» (см. раздел 2.4).

4.5. Аутентификация по логину и паролю и подтверждением операций с помощью мобильного приложения myDSS

Данный метод аналогичен методу, описанному в разделе 4.1, с тем лишь отличием, что отсутствие подключений к сетям общего пользования необязательно.

Кроме аутентификации по паролю, данный метод аутентификации подтверждает операции с помощью мобильного приложения myDSS следующими способами:

- С помощью отображения самого документа.

Документ, для которого планируется создать электронную подпись, отображается в мобильном приложении myDSS. Пользователь просматривает его, убеждается, что хочет выполнить операцию именно с этим документом, и подтверждает ее путем нажатия соответствующей кнопки в myDSS, после чего ему требуется ввести ПИН-код в мобильном приложении. В этом случае для обеспечения конфиденциальности передаваемых документов требуется защищать канал связи дополнительными средствами (например, VPN-решениями соответствующего класса защиты).

- С помощью сравнения уникального идентификатора.

КриптоПро DSS генерирует для подписываемого документа, отображаемого в Веб-интерфейсе DSS, уникальный идентификатор, который отображается как в Веб-интерфейсе DSS, так и в мобильном приложении. Пользователь сравнивает идентификаторы и в случае их совпадения подтверждает операцию путем нажатия соответствующей кнопки в myDSS, после чего ему требуется ввести ПИН-код в мобильном приложении. Такой метод подтверждения применим для создания ЭП любых документов.

Если у мобильного устройства Пользователя отсутствует подключение к сети, операцию можно подтвердить в офлайн-режиме. В этом случае Пользователь, используя мобильное приложение myDSS, сканирует QR-код, отображающийся в Веб-интерфейсе DSS. После этого ему необходимо ввести ПИН-код для доступа к вектору аутентификации и сверить уникальные идентификаторы аналогично онлайн-сценарию подтверждения. После нажатия кнопки подтверждения в myDSS отобразится код, который необходимо ввести в Веб-интерфейс DSS для завершения операции.

Описанные в данном разделе способы аутентификации реализуются в исполнениях КриптоПро DSS «DSS + myDSS» и «DSS + AirKey Lite», уровень защиты КС1. (см. раздел 2.4).

4.6. Аутентификация с помощью мобильного приложения myDSS

Интегрированная с КриптоПро DSS информационная система инициирует операцию создания ЭП документа, после чего подписываемый документ отображается в мобильном приложении myDSS. Пользователь просматривает его, убеждается, что хочет выполнить операцию именно с этим документом, и подтверждает ее путем нажатия соответствующей кнопки в myDSS, после чего ему требуется ввести ПИН-код в мобильном приложении. В этом случае для обеспечения конфиденциальности передаваемых документов требуется защищать канал связи дополнительными средствами (например, VPN-решениями соответствующего класса защиты). При данном методе аутентификации Пользователь не имеет прямого доступа к Веб-Интерфейсу DSS.

Описанный метод аутентификации реализуется в исполнениях КриптоПро DSS «DSS + myDSS» и «DSS + AirKey Lite» (см. раздел 2.4).

4.7. Аутентификация по логину и паролю и подтверждением операций при помощи мобильного приложения на базе DSS SDK

Данный метод аналогичен методу, описанному в разделе 4.1, с тем лишь отличием, что отсутствие подключений к сетям общего пользования необязательно.

Кроме аутентификации по паролю, данный метод аутентификации подтверждает операции с помощью мобильного приложения, использующего DSS SDK.

- С помощью отображения одного или нескольких документов.

Документ или несколько документов, для которых планируется создать электронную подпись, отображаются в мобильном приложении на базе DSS SDK. Дополнительно может быть настроено отображение краткой информации о документах и/или их печатной формы. Пользователь просматривает документы, убеждается, что хочет выполнить операцию именно с ними, и подтверждает свои действия путем нажатия соответствующей кнопки, после чего ему требуется ввести ПИН-код в мобильном приложении.

- С помощью сравнения уникального идентификатора.

КриптоПро DSS генерирует для подписываемого документа, отображаемого в Веб-интерфейсе DSS, уникальный идентификатор, который отображается как в Веб-интерфейсе DSS, так и в мобильном приложении на базе DSS SDK. Пользователь сравнивает идентификаторы и в случае их совпадения подтверждает операцию путем нажатия соответствующей кнопки в мобильном приложении, после чего ему требуется ввести ПИН-код. Такой метод подтверждения применим для создания ЭП любых документов.

Если у мобильного устройства Пользователя отсутствует подключение к сети, операцию можно подтвердить в офлайн-режиме. В этом случае Пользователь, используя мобильное приложение на базе DSS SDK, сканирует QR-код, отображающийся в Веб-интерфейсе DSS. После этого ему необходимо ввести ПИН-код для доступа к вектору аутентификации и сверить уникальные идентификаторы аналогично онлайн-сценарию подтверждения. После нажатия кнопки подтверждения в мобильном приложении отобразится код, который необходимо ввести в Веб-интерфейс DSS для завершения операции.

Обмен данными между DSS SDK и КриптоПро DSS осуществляется через защищенное соединение, что дает возможность подписывать конфиденциальные документы.

Описанные в данном разделе способы аутентификации реализуются в исполнениях КриптоПро DSS «myDSS SDK», «Сбербанк myDSS SDK» и «DSS Client SDK», уровень защиты КС1. (см. раздел 2.4).

4.8. Аутентификация с помощью мобильного приложения на базе DSS SDK

Пользователь в мобильном приложении или интегрированная с КриптоПро DSS информационная система инициирует операцию создания ЭП документа или нескольких документов, после чего подписываемые документы отображаются в мобильном приложении на базе DSS SDK. Дополнительно может быть настроено отображение краткой информации о документах и/или их печатной формы. Пользователь просматривает документы, убеждается, что хочет выполнить операцию именно с ними, и подтверждает свои действия путем нажатия соответствующей кнопки, после чего ему требуется ввести ПИН-код в мобильном приложении. При данном методе аутентификации Пользователь не имеет прямого доступа к Веб-Интерфейсу DSS.

Обмен данными между DSS SDK и КриптоПро DSS осуществляется через защищенное соединение, что дает возможность подписывать конфиденциальные документы.

Описанные в данном разделе способы аутентификации реализуются в исполнениях КриптоПро DSS «myDSS SDK», «Сбербанк myDSS SDK» и «DSS Client SDK», уровень защиты КС1. (см. раздел 2.4).

4.9. Аутентификация для автоматического создания ЭП с помощью апплета на SIM-модуле

Данный метод аутентификации используется для автоматического подписания информации, поступающей с устройств, оснащенных SIM-модулем. Если при функционировании такого устройства возникает необходимость подписания данных, устройство при помощи специального апплета в SIM-модуле в автоматическом режиме вычисляет на основании этих данных код аутентификации и передает данные и код в интегрируемую информационную систему. ИС инициирует процедуру создания ЭП в КриптоПро DSS, передавая туда необходимую информацию и код аутентификации. КриптоПро DSS проверяет целостность полученной информации, проверяя полученный код аутентификации. В случае успешной проверки КриптоПро DSS подписывает данные. Такой метод аутентификации допустим только для создания усиленной неквалифицированной ЭП.

Описанный метод аутентификации реализуется в исполнении КриптоПро DSS «DSS + SIM (M2M)» (см. раздел 2.4).

4.10. Дополнительные способы аутентификации

При использовании аутентификации только по логину и паролю (раздел 4.1) или аутентификации по сертификату (раздел 4.2) возможно назначить дополнительные способы аутентификации:

- аутентификация с использованием одноразового пароля, доставляемого через SMS-сообщение (OTP-via-SMS).

При использовании данного метода для подтверждения входа и операций у Пользователя дополнительно будет запрашиваться ввод одноразового пароля, доставляемого в SMS-сообщении на телефон Пользователя.

- аутентификация с использованием одноразового пароля, доставляемого через EMAIL (OTP-via-EMAIL).

При использовании данного метода для подтверждения входа и операций дополнительно у Пользователя будет запрашиваться ввод одноразового пароля, доставляемого по электронной почте.

Дополнительные способы аутентификации в КриптоПро DSS являются **вспомогательными** и не ослабляют требований, описанных в разделах 4.1–4.9.

4.11. Механизм аутентификации с помощью мобильного приложения или апплета на SIM-карте

4.11.1. Процесс подтверждения операций

Подтверждение операций с помощью мобильного приложения или апплета на SIM-карте основано на вычислении кода аутентификации от набора данных, содержащего служебные данные и данные о подтверждаемой операции, по алгоритму HMAC_GOSTR3411_2012_256, описанному в Рекомендациях по стандартизации ТК 26 Р 50.1.113-2016, с использованием вектора аутентификации Пользователя, хранящегося на его мобильном устройстве.

Аутентификация Пользователя при создании ЭП документа происходит следующим образом: Пользователь или интегрируемая с КриптоПро DSS информационная система инициируют процесс создания ЭП, передавая документ в DSS. КриптоПро DSS обрабатывает полученный документ и подготавливает данные для аутентификации Пользователя. В исполнениях «DSS + SIM» эти данные содержат либо сообщение о выполняемой операции (например, ЭП), либо подписываемый документ (см. раздел 4.4). В исполнениях «DSS + myDSS» и всех исполнениях DSS SDK (см. раздел 2.4) эти данные содержат как сообщение о выполняемой операции, так и сам документ (см. разделы 4.5–4.8).

Пользователь просматривает сообщение и/или документ, убеждается, что хочет выполнить данную операцию, и подтверждает ее, после чего ему требуется ввести ПИН-код. После ввода ПИН-кода апплет, либо мобильное приложение получают доступ к вектору аутентификации Пользователя, хранящемуся на его мобильном устройстве, и вычисляют код аутентификации, который потом отправляется в КриптоПро DSS. КриптоПро DSS «на лету» вырабатывает вектор аутентификации Пользователя из Мастер-ключа, хранящегося в КриптоПро HSM, вычисляет код аутентификации и проверяет полученный код аутентификации. В случае их совпадения КриптоПро DSS успешно подписывает документ.

4.11.2. Установка вектора аутентификации в мобильное приложение или апплет на SIM-карте

Векторы аутентификации Пользователей генерируются ПАКМ «КриптоПро HSM» из Мастер-ключа в момент создания Администратором DSS партии карт, либо по запросу Пользователя на использование мобильного приложения (myDSS или приложения на базе DSS SDK). Вектор аутентификации является секретом Пользователя и хранится либо в апплете на SIM-карте Пользователя, либо в мобильном приложении. В HSM таким образом хранятся только Мастер-ключи, используемые для генерации векторов аутентификации.

Вектор аутентификации может передаваться в апплет на SIM-карте или в мобильное приложение защищенным на коде активации. Коды активации создаются и сохраняются в КриптоПро DSS при регистрации партии SIM-карт или при выработке векторов аутентификации для Пользователей модуля myDSS/DSS SDK. Чтобы подтверждать операции при помощи апплета на SIM-карте или мобильного приложения, Пользователю следует ввести код активации. После этого он придумывает ПИН-код, на котором теперь будет защищен вектор аутентификации.

Доставка вектора аутентификации в мобильное устройство Пользователя происходит следующим образом:

- Для DSS + SIM – при производстве SIM-карты.

Администратор DSS регистрирует партию SIM-карт в КриптоПро DSS и передает сведения о них в файле персонализации производителю SIM-карт[1]. При этом в КриптоПро DSS сохраняются их серийные номера и коды активации. Файл персонализации содержит серийные номера SIM-карт, контейнеры с ключевой информацией и векторы инициализации для смены вектора аутентификации. При изготовлении SIM-карты в апплет записывается контейнер с ключевой информацией вектора аутентификации, а также вектор инициализации. Срок допустимого использования одной SIM-карты составляет 6 лет.

SIM-карта с апплетом и вектором аутентификации передается Пользователю из рук в руки Оператором DSS после идентификации Пользователя. При этом Оператор DSS осуществляет привязку выданной SIM-карты к учетной записи Пользователя по серийному номеру данной SIM-карты.

Чтобы подтверждать операции при помощи апплета на SIM-карте, апплет нужно активировать. Оператор DSS или Пользователь инициирует процедуру активации в КриптоПро DSS. DSS связывается с апплетом на SIM-карте, после чего Пользователю предлагается ввести код активации в его мобильном устройстве. Если введенный код верен, Пользователю требуется придумать ПИН-код для доступа к вектору аутентификации. После этого вектор аутентификации перезаписывается под защитой ПИН-кода, а апплет считается активированным и готовым к дальнейшему использованию.

[1] Производитель SIM-карт должен обладать Лицензией на производство (тиражирование) шифровальных (криптографических) средств (п. 7 приложения ППРФ № 313 от 16.04.2012).

- Для DSS + myDSS и DSS + AirKey Lite – сканированием QR-кода, содержащего вектор аутентификации.

Если Пользователь аутентифицируется в КриптоПро DSS с помощью методов, описанных в разделах 4.1, 4.2 и 4.5, он может самостоятельно получить QR-код, содержащий вектор аутентификации, в своем личном кабинете. В этом случае QR-код с вектором аутентификации отображается в Веб-интерфейсе Пользователя.

При использовании других методов аутентификации создание вектора аутентификации возможно только с участием Оператора DSS при личном визите Пользователя в офис обслуживания. В этом случае Оператор DSS инициирует процедуру создания вектора аутентификации в DSS. DSS генерирует QR-код, содержащий вектор аутентификации, который должен быть передан Пользователю способом, исключающим возможность несанкционированного ознакомления с ним Оператора.

Пользователю необходимо отсканировать QR-код, используя мобильное приложение myDSS.

Вектор аутентификации, передаваемый в QR-коде, может быть дополнительно защищен на коде активации (защита настраивается Администратором). Код активации доставляется Пользователю в SMS-сообщении или в сообщении электронной почты. При сканировании QR-кода с вектором аутентификации мобильное приложение предложит Пользователю ввести код активации. Если введенный код верен, Пользователь может придумать ПИН-код для доступа к вектору аутентификации. После этого вектор аутентификации перезаписывается под защитой ПИН-кода.

Если планируется создание **только** усиленной неквалифицированной подписи, QR-код может быть передан Пользователю в сообщении электронной почты.

- Для myDSS SDK, Сбербанк myDSS SDK и DSS Client SDK — инициализацией мобильного приложения на базе DSS SDK.

Установка вектора аутентификации в мобильное приложение на базе DSS SDK является частью процедуры инициализации мобильного приложения и привязки мобильного устройства Пользователя к его учетной записи. Данный процесс может быть организован различными способами (см. раздел 5).

4.11.3. Смена вектора аутентификации на мобильном устройстве Пользователя

Смена вектора аутентификации на мобильном устройстве Пользователя происходит следующим образом:

- Для DSS + SIM – вводом цифровой последовательности.

Для смены вектора аутентификации в апплете на SIM-карте Пользователь должен получить цифровую последовательность доверенным образом. Оператор DSS или Пользователь инициирует в КриптоПро DSS процесс смены вектора аутентификации. КриптоПро DSS связывается с апплетом на SIM-карте Пользователя для начала процедуры смены ключа. Получив запрос на смену ключа, апплет предлагает Пользователю ввести ПИН-код для доступа к действующему вектору аутентификации. После этого Пользователю следует ввести в диалоговом окне на своем мобильном устройстве полученную цифровую последовательность. На ее основе и с использованием

вектора инициализации, хранящегося на SIM-карте, апплет вырабатывает новый вектор аутентификации.

Для проверки корректности введенных данных апплет вычисляет проверочный код аутентификации на новом ключе и отправляет его в КриптоПро DSS. КриптоПро DSS «на лету» вырабатывает вектор аутентификации Пользователя из Мастер-ключа, хранящегося в КриптоПро HSM, и проверяет полученный код аутентификации. При успешной проверке вектор аутентификации считается измененным и готовым к дальнейшему использованию.

Активация апплета после смены ключа не требуется.

- Для DSS + myDSS и DSS + AirKey Lite – сканированием QR-кода, содержащего новый вектор аутентификации.

Процедура смены и активации вектора аутентификации Пользователя для мобильного приложения myDSS аналогична действиям и требованиям, описанным для DSS + myDSS и DSS + AirKey Lite в разделе 4.11.2.

- Для myDSS SDK, Сбербанк myDSS SDK и DSS Client SDK — инициализацией мобильного приложения на базе DSS SDK.

Процедура смены и активации вектора аутентификации Пользователя для мобильного приложения на базе DSS SDK аналогична действиям и требованиям, описанным для myDSS SDK, Сбербанк myDSS SDK и DSS Client SDK в разделе 4.11.2.

5. Способы инициализации мобильного приложения на базе DSS SDK

Мобильное устройство Пользователя, на котором установлено мобильное приложение на базе DSS SDK, должно быть инициализировано (привязано) к учетной записи Пользователя в КриптоПро DSS.

Существуют следующие способы инициализации (привязки) мобильного устройства:

- при помощи сверки уникального идентификатора (раздел 5.1);
- при помощи выбранного идентификатора с дополнительной защитой QR-кодом (раздел 5.2);
- при помощи QR-кода с начальным вектором аутентификации (раздел 5.3);
- при помощи самостоятельного получения сертификата (раздел 5.4).

Пользователь КриптоПро DSS, использующий аутентификацию при помощи мобильного приложения на базе DSS SDK (см. разделы 4.7–4.8), может привязать к своей учетной записи еще одно мобильное устройство без визита к Оператору. Данная процедура описана в разделе 5.5.

5.1. Инициализация мобильного устройства при помощи сверки уникального идентификатора

Данный способ инициализации заключается в подтверждении учетной записи Пользователя в КриптоПро DSS и привязке к ней мобильного устройства при помощи уникального идентификатора и обладает следующими особенностями:

- необходима предварительная регистрация мобильного устройства Пользователя;
- уникальный идентификатор вектора аутентификации создается средствами КриптоПро DSS, и Пользователю нет необходимости его запоминать.
- уникальный идентификатор вектора аутентификации должен содержаться в заявительных документах Пользователя;
- для привязки мобильного устройства нет необходимости сканировать QR-код.

Сценарий состоит из следующих этапов.

1. Предварительная регистрация мобильного устройства.
2. Привязка Оператором DSS мобильного устройства к учетной записи Пользователя.
3. Подтверждение Пользователем привязки мобильного устройства к учетной записи.

На первом этапе Пользователь из мобильного приложения на базе DSS SDK отправляет запрос на регистрацию мобильного устройства в КриптоПро DSS. В ответ КриптоПро DSS отправляет в мобильное приложение вектор аутентификации (ВА) и уникальный идентификатор ВА. Уникальный идентификатор генерируется в КриптоПро DSS и является 12-символьной строкой, состоящей из цифр и латинских букв. Полученные данные сохраняются в мобильном приложении, Пользователь может защитить ВА с помощью ПИН-кода.

На втором этапе требуется визит Пользователя или его Доверенного лица к Оператору DSS.

Оператор DSS выполняет следующие действия.

- Идентифицирует Пользователя.

- Проверяет наличие учетной записи Пользователя в DSS по уникальным признакам (СНИЛС, ИНН и т.п.). Если учетная запись отсутствует, Оператор DSS создает ее.
- Готовит и передает Пользователю на подпись, либо получает от Пользователя подписанные заявительные документы, необходимые для начала обслуживания Пользователя в DSS (если учетная запись ранее не существовала) и для привязки мобильного устройства Пользователя к его учетной записи, проверяет их. В заявительных документах обязательно присутствует идентификатор ВА, который Пользователь видит в мобильном приложении на базе DSS SDK и вписывает в эти документы, либо сверяет, если идентификатор там уже содержится.
- Находит по идентификатору ВА неподтверждённое мобильное устройство Пользователя и привязывает его к учетной записи.

На третьем этапе Пользователю следует подтвердить данные учетной записи в мобильном приложении на своем мобильном устройстве. Подтверждение данных учетной записи может быть инициировано Пользователем или мобильным приложением.

Для подтверждения учетной записи мобильное приложение отображает Пользователю сведения об учетной записи и предоставляет возможность подтвердить их или отказаться. Привязка мобильного устройства Пользователя к учетной записи в DSS будет завершена после получения подтверждения. Если Пользователь не согласился с полученными учетными данными, ему следует отказаться от их подтверждения и обратиться к Оператору DSS.

5.2. Инициализация мобильного устройства при помощи выбранного идентификатора с дополнительной защитой QR-кодом

Данный способ инициализации заключается в подтверждении учетной записи Пользователя в КриптоПро DSS и привязке к ней мобильного устройства при помощи уникального идентификатора и QR-кода, что является развитием сценария, описанного в разделе 5.1. Способ обладает следующими особенностями:

- необходима предварительная регистрация мобильного устройства Пользователя;
- уникальный идентификатор вектора аутентификации может выбрать Пользователь или создать само мобильное приложение;
- уникальный идентификатор вектора аутентификации может быть устно назван Пользователем Оператору;
- для привязки мобильного устройства Пользователь должен отсканировать QR-код в мобильном приложении.

Сценарий состоит из следующих этапов.

1. Предварительная регистрация мобильного устройства.
2. Привязка Оператором DSS мобильного устройства к учетной записи Пользователя.
3. Подтверждение Пользователем привязки мобильного устройства к учетной записи.

На первом этапе Пользователь из мобильного приложения на базе DSS SDK отправляет запрос на регистрацию мобильного устройства в КриптоПро DSS, содержащий выбранный идентификатор вектора аутентификации. КриптоПро DSS проверяет уникальность идентификатора и в случае положительного результата проверки отправляет в мобильное приложение Пользователя вектор аутентификации. Полученный вектор аутентификации сохраняется в мобильном приложении, Пользователь может защитить его с помощью ПИН-кода.

На втором этапе требуется визит Пользователя или его Доверенного лица к Оператору DSS.

Оператор DSS выполняет следующие действия.

- Идентифицирует Пользователя.
- Проверяет наличие учетной записи Пользователя в DSS по названному Пользователем уникальному идентификатору ВА. Если учетная запись отсутствует, Оператор DSS создает ее.
- Готовит и передает Пользователю на подпись, либо получает от Пользователя подписанные заявительные документы для начала обслуживания Пользователя в DSS (если учетная запись ранее не существовала) и для привязки мобильного устройства Пользователя к его учетной записи, проверяет их. В заявительных документах обязательно присутствует идентификатор ВА, придуманный Пользователем на первом этапе.
- Находит по идентификатору ВА неподтверждённое мобильное устройство Пользователя и привязывает его к учетной записи.

На третьем этапе Оператор DSS создаёт для Пользователя QR-код, необходимый для подтверждения владения мобильным устройством, и передает его непосредственно Пользователю или Доверенному лицу Пользователя.

Пользователю следует отсканировать полученный QR-код в мобильном приложении на базе DSS SDK. Дальнейшие действия по подтверждению данных учетной записи аналогичны описанным в разделе 5.1.

5.3. Инициализация мобильного устройства при помощи QR-кода с начальным вектором аутентификации

Данный способ инициализации заключается в подтверждении учетной записи Пользователя в КриптоПро DSS и привязке к ней мобильного устройства при визите Пользователя (или его Доверенного лица) к Оператору DSS и обладает следующими особенностями:

- не требуется предварительная регистрация мобильного устройства, т.е. Пользователь может совершить все необходимые действия во время визита к Оператору DSS;
- уникальный идентификатор вектора аутентификации не используется;
- необходимо исключить возможность несанкционированного доступа к QR-коду Оператора и третьих лиц.

Оператор DSS при визите к нему Пользователя или его Доверенного лица выполняет следующее:

- Идентифицирует Пользователя.
- Проверяет наличие учетной записи Пользователя в DSS по уникальным признакам (СНИЛС, ИНН и т.п.). Если учетная запись отсутствует, Оператор DSS создает ее.
- Готовит и передает Пользователю на подпись, либо получает от Пользователя подписанные заявительные документы для начала обслуживания Пользователя в DSS (если учетная запись ранее не существовала) и для привязки мобильного устройства Пользователя к его учетной записи, проверяет их.
- Создает QR-код для первичной аутентификации мобильного устройства Пользователя и последующего получения вектора аутентификации (ВА).

КриптоПро DSS генерирует QR-код с начальным ВА, который должен быть передан Пользователю (либо его Доверенному лицу), способом, исключающим возможность

несанкционированного ознакомления с ним Оператора и третьих лиц. Начальный ВА, передаваемый в QR-коде, может быть дополнительно защищен на коде активации (защита настраивается отдельно Администратором). Код активации доставляется Пользователю в SMS-сообщении или в сообщении электронной почты.

Пользователь сканирует QR-код при помощи мобильного приложения на базе DSS SDK и вводит код активации, если он используется. Мобильное приложение связывается с КриптоПро DSS, аутентифицируя себя с помощью начального ВА, после чего мобильное приложение привязывается к учетной записи и в него устанавливается вектор аутентификации. Пользователь может защитить ВА с помощью ПИН-кода.

Администратор может настроить DSS таким образом, что QR-код может использоваться только один раз. В этом случае привязка других мобильных устройств к той же учетной записи будет возможна только путем генерации новых QR-кодов.

Дальнейшие действия по подтверждению сведений об учетной записи Пользователем аналогичны описанным в разделе 5.1.

5.4. Инициализация мобильного устройства при помощи самостоятельного получения сертификата

Данный способ инициализации заключается в подтверждении учетной записи Пользователя и привязке к ней мобильного устройства при помощи самостоятельно полученного сертификата и обладает следующими особенностями:

- необходима предварительная регистрация мобильного устройства Пользователя;
- визит к Оператору DSS необязателен при использовании квалифицированного сертификата;
- уникальный идентификатор вектора аутентификации не используется;
- QR-код для привязки мобильного устройства не используется.

Пользователь из мобильного приложения на базе DSS SDK отправляет запрос на регистрацию мобильного устройства в КриптоПро DSS и создание запроса на сертификат. В ответ КриптоПро DSS отправляет в мобильное приложение Пользователя на базе DSS SDK вектор аутентификации и готовый запрос на сертификат. Полученные данные сохраняются в мобильном приложении, Пользователь может защитить ВА с помощью ПИН-кода.

Далее Пользователю необходимо самостоятельно обратиться в УЦ и выпустить сертификат на основании полученного запроса. Сертификат, полученный таким образом, может быть установлен в КриптоПро DSS самим Пользователем через мобильное приложение или через программный интерфейс КриптоПро DSS.

Если установленный в КриптоПро DSS указанными способами сертификат является квалифицированным, Оператор DSS на основании информации из сертификата может идентифицировать владельца соответствующего ключа подписи.

Сведения об учетной записи Пользователя заполняются из установленного сертификата. Дальнейшие действия по подтверждению сведений об учетной записи Пользователем аналогичны описанным в разделе 5.1. Если учетная запись Пользователя уже существует, то новый сертификат и мобильное устройство могут быть привязаны к ней автоматически.

5.5. Инициализация дополнительного мобильного устройства при помощи привязанного ранее устройства

Пользователь КриптоПро DSS, использующий аутентификацию при помощи мобильного приложения на базе DSS SDK (см. разделы 4.7–4.8), может привязать к своей учетной записи еще одно мобильное устройство без визита к Оператору. Для этого в мобильном приложении на новом устройстве Пользователь запрашивает привязку. При этом ему требуется ввести свой идентификатор учетной записи (например, логин). Если данные введены верно, в мобильном приложении на новом устройстве отобразится QR-код для подтверждения привязки данного устройства.

Далее Пользователь на имеющемся привязанном мобильном устройстве сканирует QR-код при помощи мобильного приложения. Приложение отображает сведения о новом подключаемом устройстве: имя устройства, тип ОС, идентификатор учетной записи. Пользователь просматривает данную информацию, убеждается в ее корректности и подтверждает привязку. В этом случае новое мобильное устройство считается привязанным и в него устанавливается новый вектор аутентификации. Если отображаемая информация некорректна, Пользователю следует отказаться от привязки и обратиться к Оператору DSS.

6. Управление ключами Пользователей

КриптоПро DSS позволяет использовать один из двух режимов хранения закрытых ключей Пользователей: непосредственно в ПАКМ HSM и в БД Сервиса Подписи. 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). Мастер-ключ хранится в HSM. Этот процесс выглядит следующим образом:

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.

Закрытые ключи Пользователей 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. 1 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.

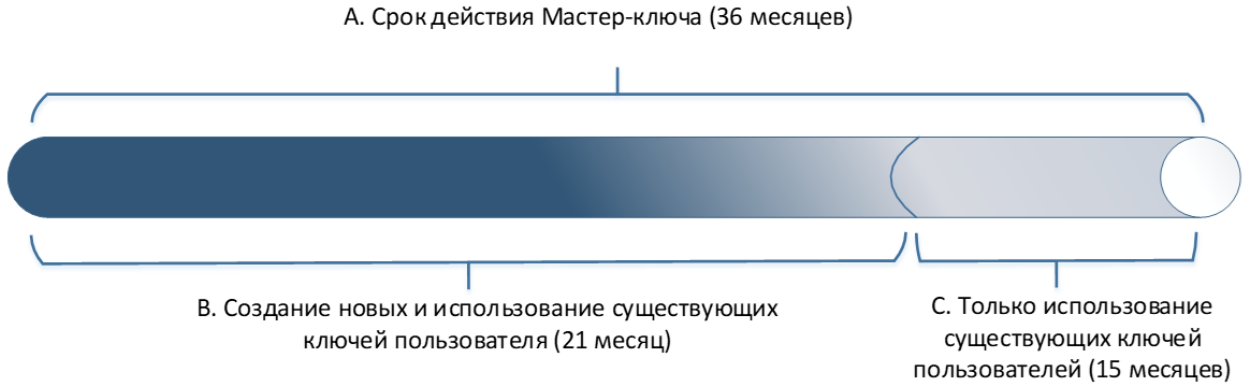

Рис. 1 — Сроки действия Мастер-ключа и ключей Пользователей

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

Таблица 1 — Режимы хранения ключей

Критерий/Режим	Хранение ключей в HSM	Хранение ключей в БД Сервиса Подписи
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.
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.
Возможности репликации БД	Только ручная репликация.	Обычная репликация БД, ручной перенос Мастер-ключа.

Из представленной таблицы можно видеть, что с точки зрения повышения отказоустойчивости и производительности удобно хранить закрытые ключи Пользователей в зашифрованном виде в БД Сервиса Подписи — повышаются производительность и отказоустойчивость системы за счет простоты автоматической репликации основной БД и ручной репликации одного только Мастер-ключа, а также отсутствует жесткое ограничение по количеству ключей Пользователей. Минусом является то, что время жизни ключа уменьшается чуть больше, чем вдвое.

7. Архитектура решения КриптоПро DSS

7.1. Взаимодействие компонентов КриптоПро DSS

На Рис. 2 изображена схема взаимодействия компонентов КриптоПро DSS. Слева от пунктирной линии отображаются компоненты и сервисы, непосредственно входящие в состав продукта, а также связи между ними. Сторонние продукты расположены справа от границы, обозначенной пунктиром. Их присутствие на схеме необходимо для полного видения связей и зависимостей компонентов КриптоПро DSS от внешних компонентов. Клиентские компоненты аутентификации и схемы взаимодействия с ними изображены на Рис. 3–Рис. 4).

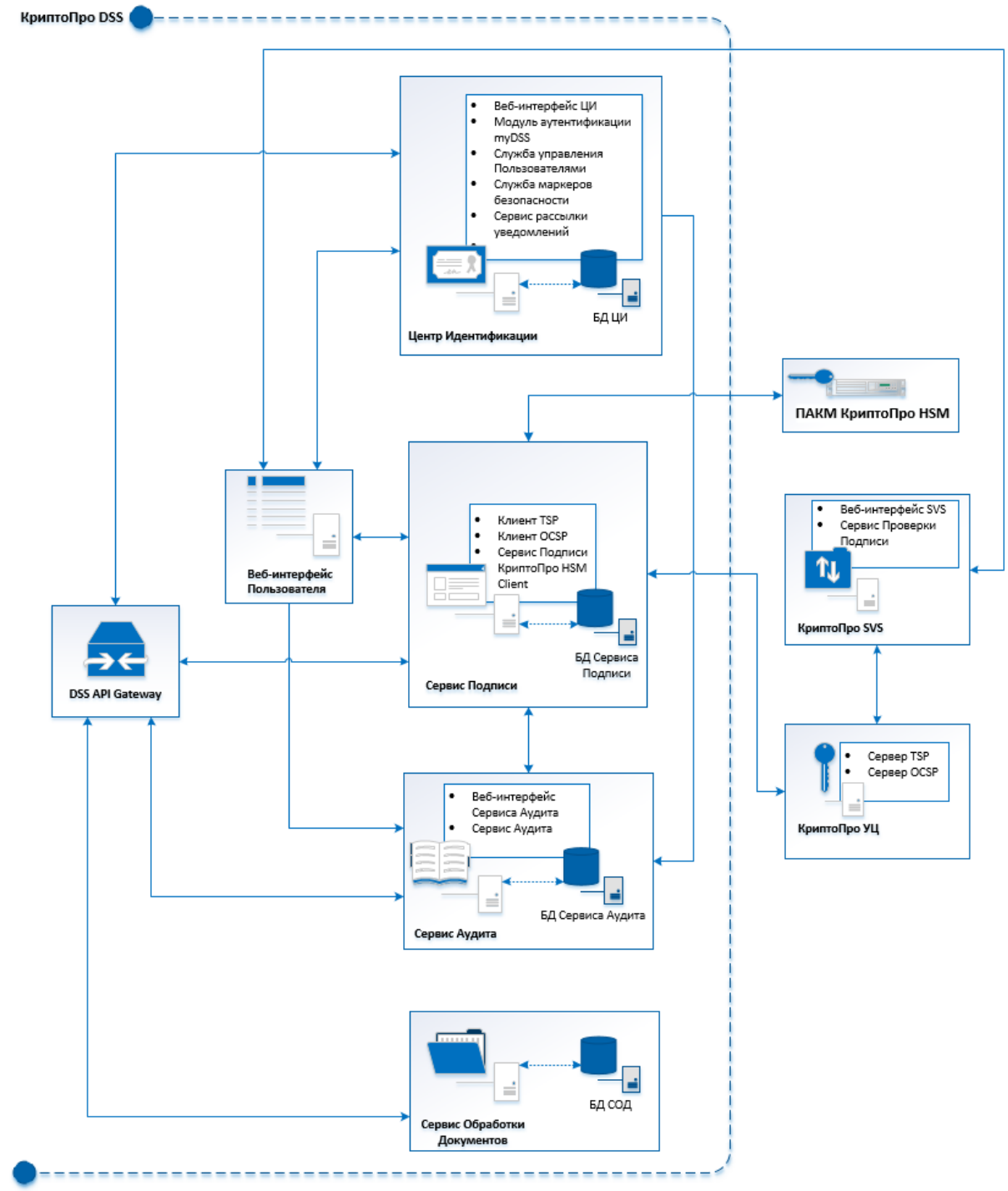

Рис. 2 — Схема взаимодействия компонентов КриптоПро DSS

7.2. Взаимодействие компонентов с myDSS

Компонент myDSS осуществляет взаимодействие с КриптоПро DSS через ЦИ КриптоПро DSS в соответствии со схемой взаимодействия компонентов, приведенной на Рис. 3. Настоящая схема отображает только логические компоненты и продукты (ПАКМ «КриптоПро HSM»), непосредственно участвующие во взаимодействии с серверной и клиентской частью myDSS.

Сервер внешнего взаимодействия myDSS должен быть установлен в выделенном сегменте сети (DMZ). Доступ к функциям Сервера внешнего взаимодействия со стороны КриптоПро DSS не осуществляется. С ним взаимодействуют с одной стороны Сервер внутреннего взаимодействия, с другой – мобильное приложение myDSS и PUSH-сервер.

На Сервере внутреннего взаимодействия находится КриптоПро HSM Client, позволяющий взаимодействовать с ПАКМ «КриптоПро HSM».

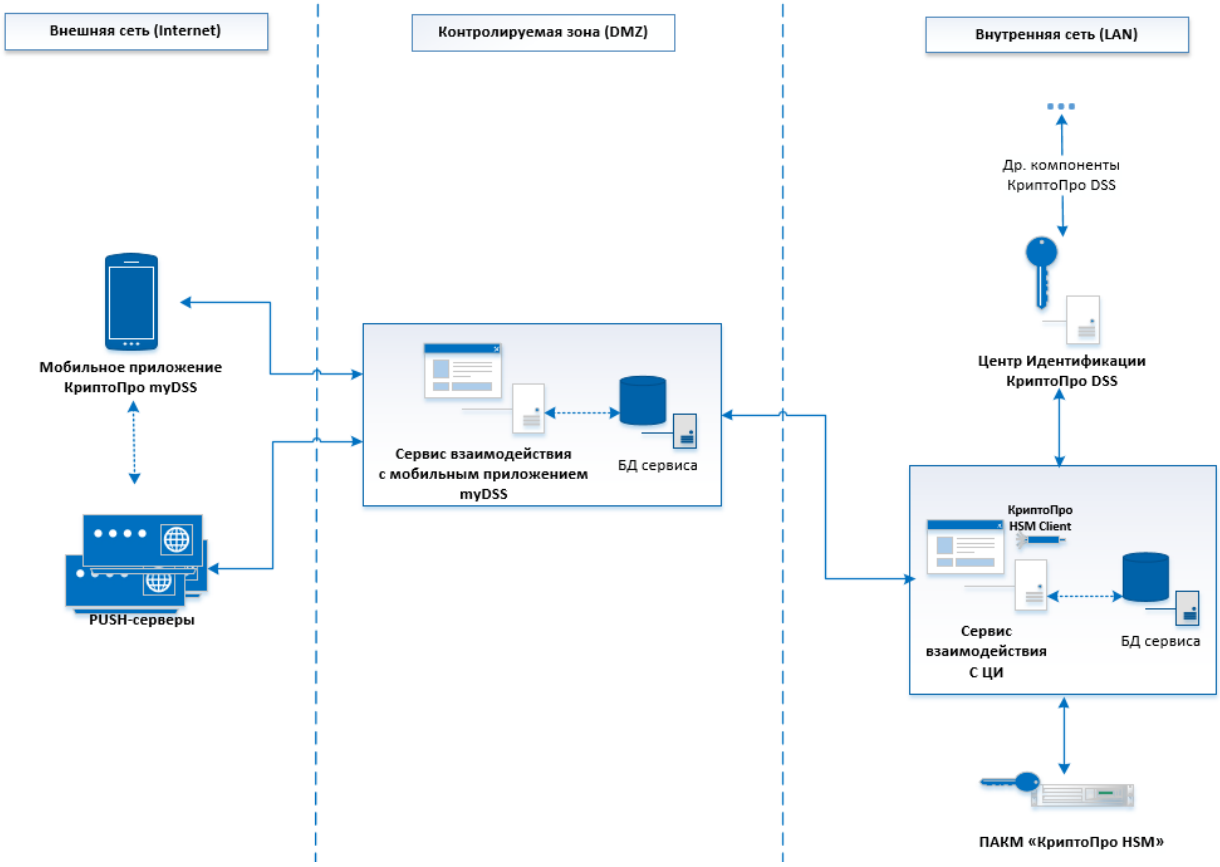

Рис. 3 — Схема взаимодействия компонентов при использовании myDSS

7.3. Взаимодействие компонентов с DSS Api Gateway

Компонент DSS Api Gateway осуществляет взаимодействие с другими компонентами КриптоПро DSS в соответствии со схемой взаимодействия компонентов, приведенной на Рис. 4. Настоящая схема отображает только логические компоненты, непосредственно участвующие во взаимодействии с DSS Api Gateway.

Сервер, на котором развернут DSS Api Gateway, должен быть установлен в выделенном сегменте сети (DMZ). С ним взаимодействуют с одной стороны мобильное приложение с на базе DSS SDK, с другой — другие компоненты КриптоПро DSS. При этом взаимодействие с серверами PUSH-уведомлений производится без участия

DSS Api Gatewayчерез Сервис рассылки уведомлений (входит в состав ЦИ КриптоПро DSS).

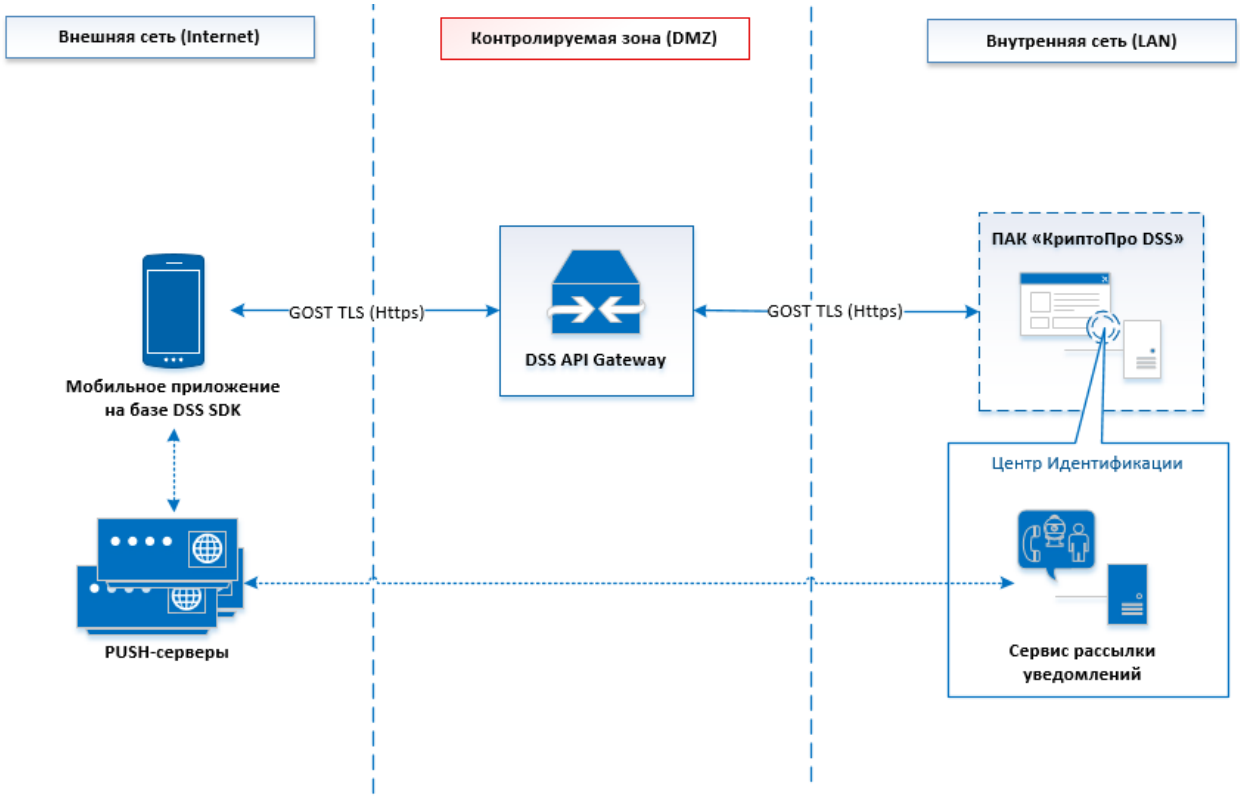

Рис. 4 — Схема взаимодействия компонентов при использовании mDAG

7.4. Размещение компонентов КриптоПро DSS

Типовая схема размещения компонентов КриптоПро DSS представлена на Рис. 5. Взаимодействие между компонентами КриптоПро DSS осуществляется по защищенному протоколу TLS. При развертывании необходимо размещать сервера за сертифицированным ФСБ России межсетевым экраном не ниже класса 4.

Организация защищенных каналов со стороны КриптоПро DSS осуществляется с помощью СКЗИ «КриптоПро CSP». Со стороны клиента необходимо использовать сертифицированное ФСБ России СКЗИ КриптоПро CSP.

Уровень защиты при использовании КриптоПро DSS с подключением по протоколу TLS с двусторонней аутентификацией определяется уровнем защиты клиентских компонентов, используемых для TLS-соединения с сервером КриптоПро DSS.

При использовании КриптоПро DSS с подключением по протоколу TLS с односторонней аутентификацией обеспечивается уровень защиты КС1. При этом в случае использования исполнений, отличных от «DSS + myDSS» и «DSS + SIM (QES)» обязательно отсутствие подключений серверных компонентов к сетям общего пользования.

На данной схеме рассмотрен случай, когда используется компонент «Веб-интерфейс Пользователя». В случае, если Сервис Подписи интегрирован непосредственно с интерфейсом сторонней ИС, она обращается к нему напрямую через МЭ с использованием защищенного соединения (см. раздел 9).

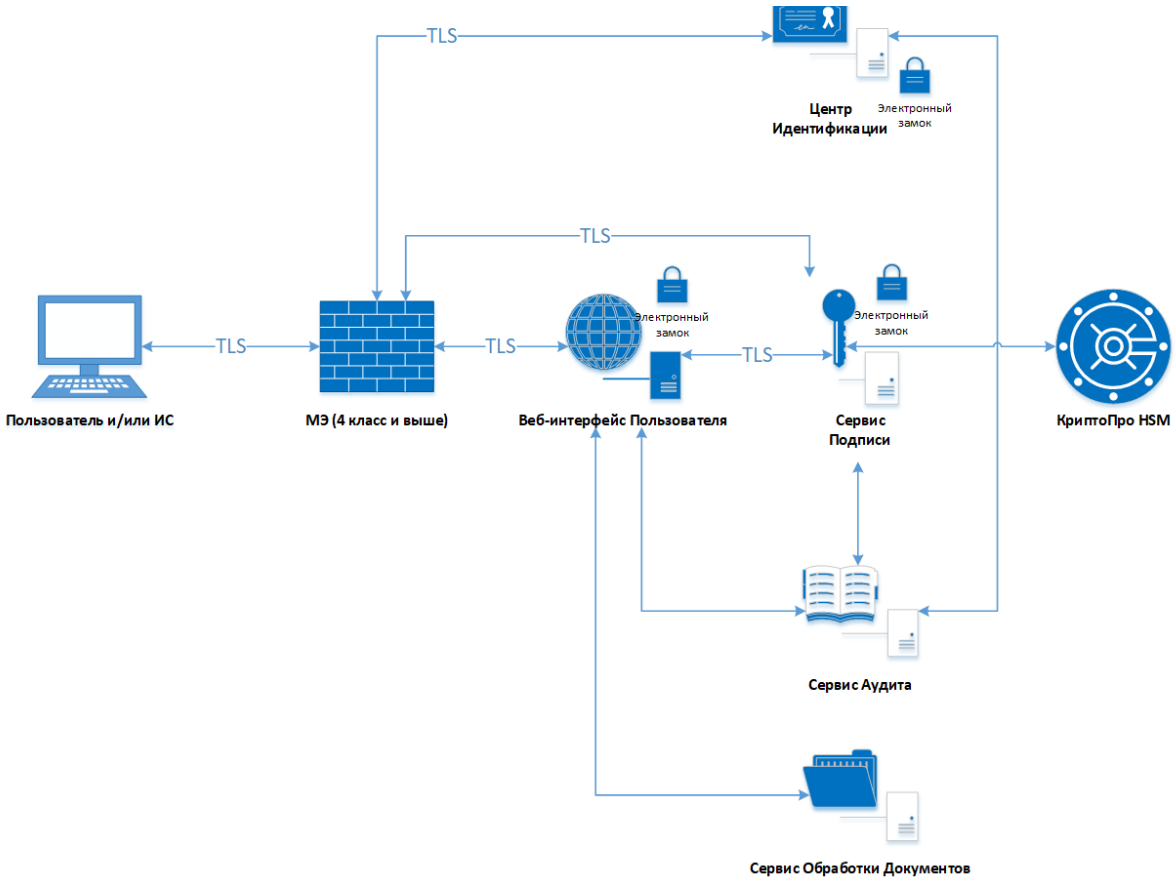

Рис. 5 — Схема размещения компонентов КриптоПро DSS

При использовании различных методов аутентификации (см. раздел 4) требуется настроить взаимодействие КриптоПро DSS с внешними системами для доставки сообщений Пользователям. На Рис. 6 изображены компоненты КриптоПро DSS, взаимодействующие с такими системами. В зависимости от выбранного способа доставки возможна рассылка сообщений по электронной почте, посредством SMS или PUSH-уведомлений (только для модуля аутентификации myDSS и взаимодействия с мобильным приложением на основе DSS SDK).

ЦИ КриптоПро DSS может быть подключен к почтовому серверу или SMS-шлюзу для доставки Пользователям QR-кодов и одноразовых паролей, использующихся при вспомогательной аутентификации (см. раздел 4.10) и/или для оповещения Пользователей о действиях, совершенных с их учетными записями и ключами аутентификации. Также ЦИ взаимодействует с PUSH-серверами для оповещения Пользователей в мобильном приложении на базе DSS SDK о необходимости подтверждения операций (см. разделы 4.7–4.8).

Модуль аутентификации myDSS взаимодействует с PUSH-серверами (см. разделы 3.2.7 и 7.2) для оповещения Пользователей в мобильном приложении myDSS о необходимости подтверждения операций.

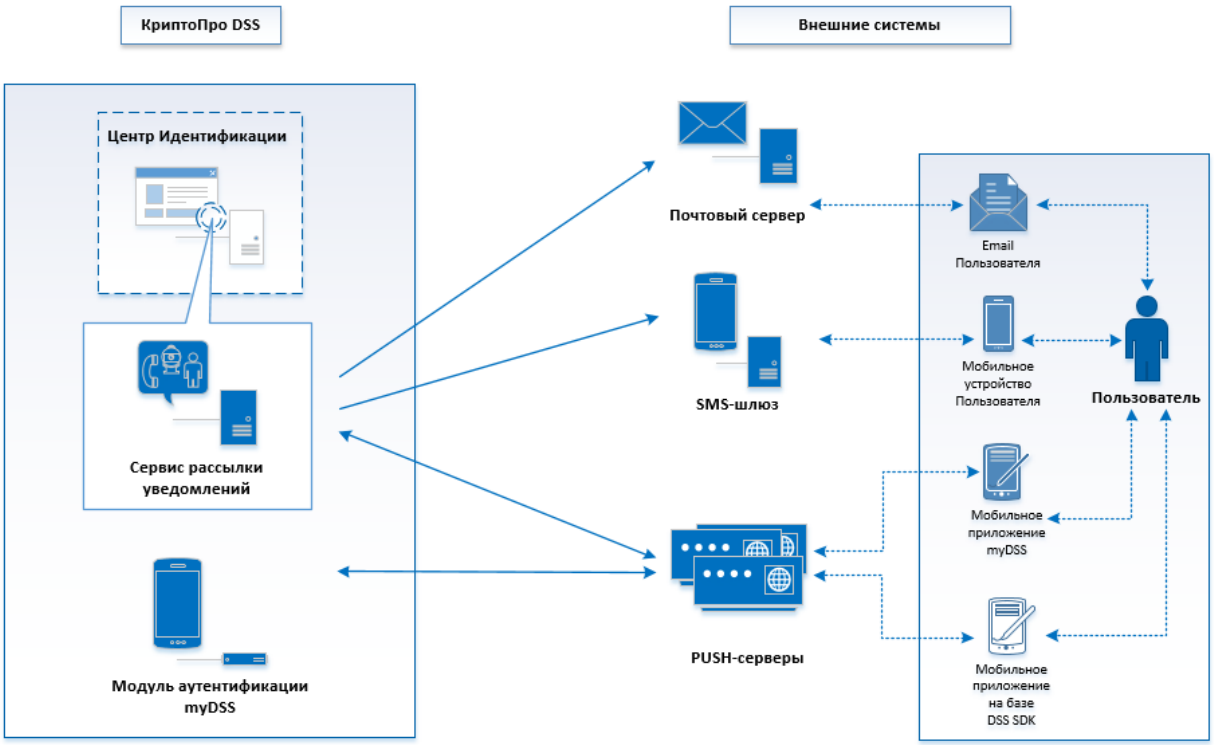

Рис. 6 — Доставка сообщений Пользователям

7.5. Описание процессов КриптоПро DSS

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

- Регистрация Пользователя и создание запроса на сертификат (см. раздел 7.5.1);
- Подпись документа (см. раздел 7.5.2);
- Проверка подписи (см. раздел 7.5.3);
- Проверка сертификата (см. раздел 7.5.4);
- Шифрование документа (см. раздел 7.5.5);
- Расшифрование документа (см. раздел 7.5.6);
- Аудит событий и формирование отчетов (см. раздел 7.5.7).

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».

7.5.1. Регистрация Пользователя и создание запроса на сертификат

Работа с КриптоПро DSS 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 (см. раздел 4). По окончании регистрации сведения о профиле Пользователя и данные аутентификации заносятся в БД ЦИ.

Для создания электронной подписи и выполнений других операций в КриптоПро DSS Пользователю необходим сертификат. КриптоПро DSS 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 DSS генерирует запрос на сертификат.

Пример последовательности шагов процесса регистрации Пользователя и создания запроса на сертификат представлен на Рис. 7. В данном случае предполагается, что регистрацию Пользователя и заполнение полей запроса на сертификат выполняет Оператор.

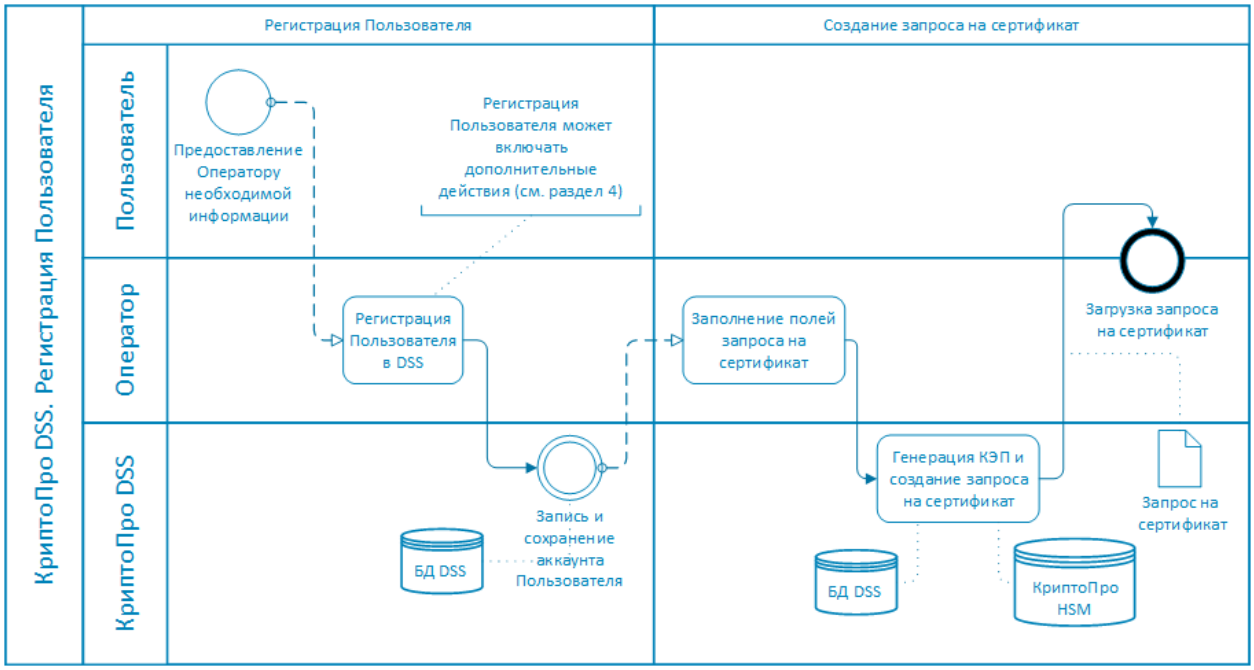

Рис. 7 — Регистрация Пользователя и создание запроса на сертификат

7.5.2. Подпись документа

Подпись документов является одним из основных процессов, поддерживаемых КриптоПро DSS. 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 DSS). Особенности каждого из этих вариантов описаны в разделе 9. При выполнении операции подписи могут быть использованы различные способы аутентификации. В данном разделе приведено описание процесса подписи документа с аутентификацией с помощью мобильного приложения myDSS (см. разделы 4.5–4.6).

Пользователь инициирует операцию подписи при помощи кнопки «Подписать» на Веб-интерфейсе Пользователя или программного интерфейса интегрируемой системы, выбирает нужный сертификат ЭП, подписываемый документ, параметры и формат подписи. Данная информация отправляется в КриптоПро DSS. КриптоПро DSS 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 документов и подтверждает операцию. Подробнее механизм и варианты подтверждения операции описаны в разделах 4.5, 4.6 и 4.11.1. Если операция подтверждена Пользователем, КриптоПро DSS подписывает документ и возвращает его Пользователю. В общем виде шаги процесса подписи с подтверждением при помощи мобильного приложения myDSS представлены на Рис. 8.

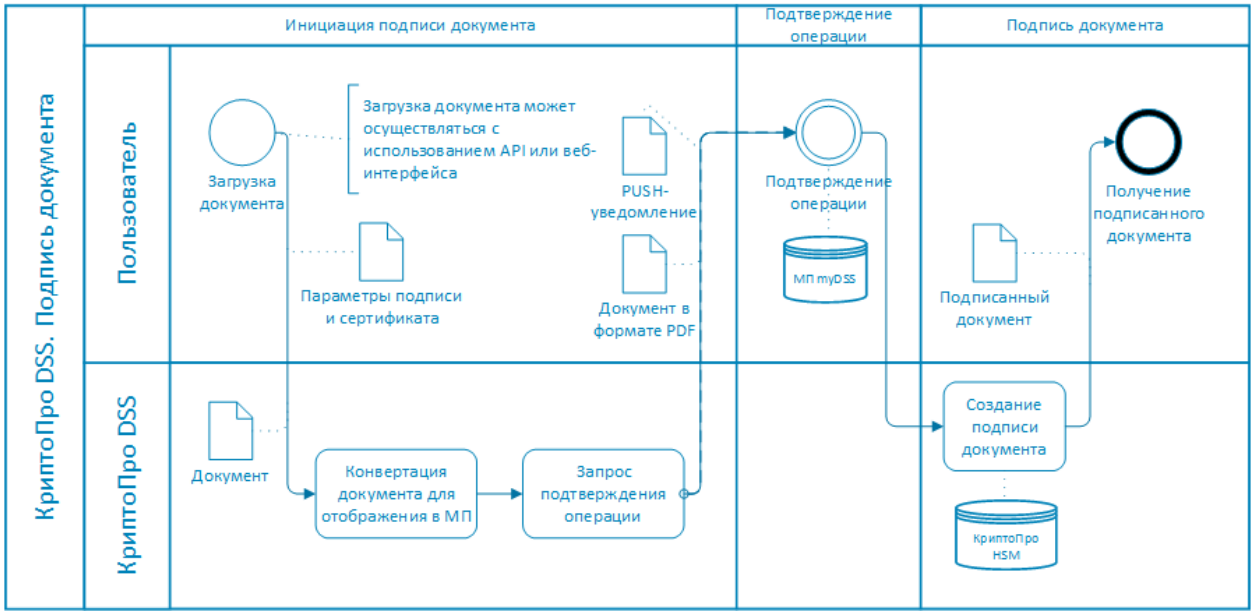

Рис. 8 — Подпись документа

7.5.3. Проверка подписи

Проверка подписи возможна при наличии КриптоПро SVS 2.0 (компонент из состава ПАК «Службы УЦ 2.0», используется опционально и при наличии действующего сертификата, выданного ФСБ России).

Для того чтобы проверить подпись документа, Пользователь в соответствующем разделе «Проверить подпись» выбирает нужный файл, после чего веб-форма пытается определить формат подписи (см. раздел 11). Если формат определить автоматически не удается, его можно переопределить вручную. Затем подписанный документ отправляется на КриптоПро SVS 2.0, где производятся криптографические операции по проверке/снятию ЭП. После окончания проверки Сервис Проверки Подписи возвращает Пользователю информацию о действительности/недействительности подписи, информацию о сертификате, на котором она была создана, а также документ в открытом виде, если данная опция была выбрана в начале процесса. Аналогичные действия могут быть выполнены через программный интерфейс КриптоПро SVS 2.0.

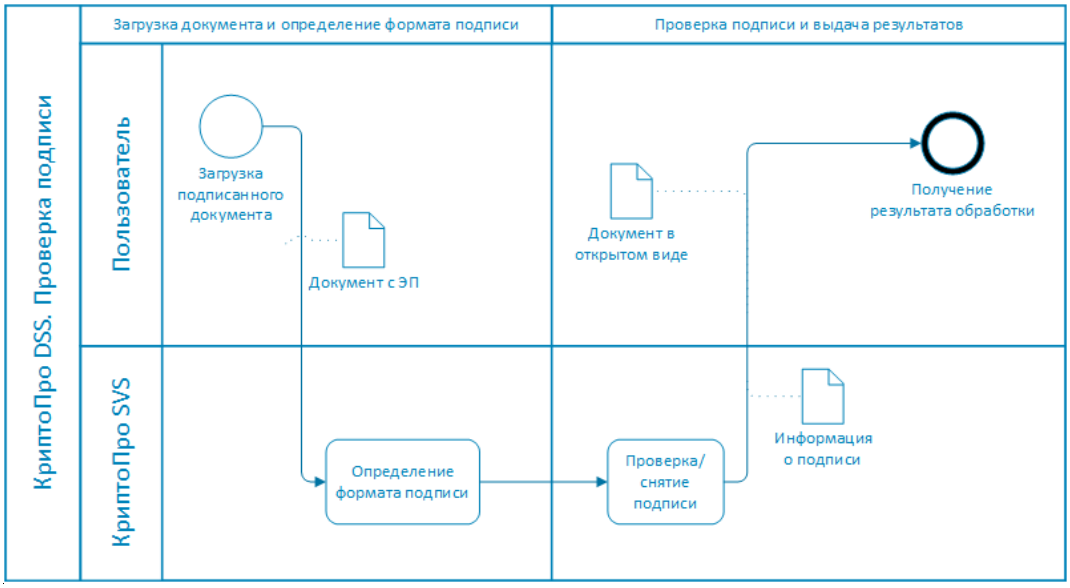

Рис. 9 — Проверка электронной подписи

7.5.4. Проверка сертификата

Проверка сертификата возможна при наличии КриптоПро SVS 2.0 (компонент из состава ПАК «Службы УЦ 2.0», используется опционально и при наличии действующего сертификата, выданного ФСБ России).

Для того, чтобы проверить статус своего сертификата, Пользователь загружает его на веб-форму в соответствующем разделе «Проверить сертификат». Сертификат отправляется на Сервис Проверки Подписи, где обрабатывается в соответствии с правилами проверки сертификата – формируется цепочка сертификатов, проверяется наличие данного сертификата в списке CRL и т.д. Результатом является выдача Пользователю информации о самом сертификате (когда, где, кому и кем выдан, срок действия и т.п.), а также информации о действительности/недействительности этого сертификата. Аналогичные действия могут быть выполнены через программный интерфейс КриптоПро SVS 2.0.

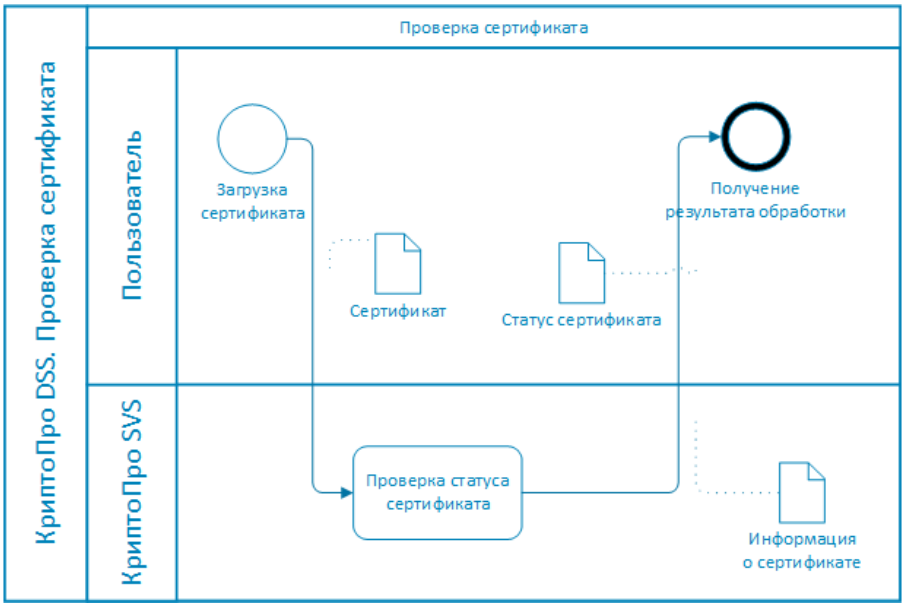

Рис. 10 — Проверка сертификата

7.5.5. Шифрование документа

Шифрование документов является одним из основных процессов, поддерживаемых в КриптоПро DSS. 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 DSS). Особенности каждого из этих вариантов описаны в разделе 9.

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.

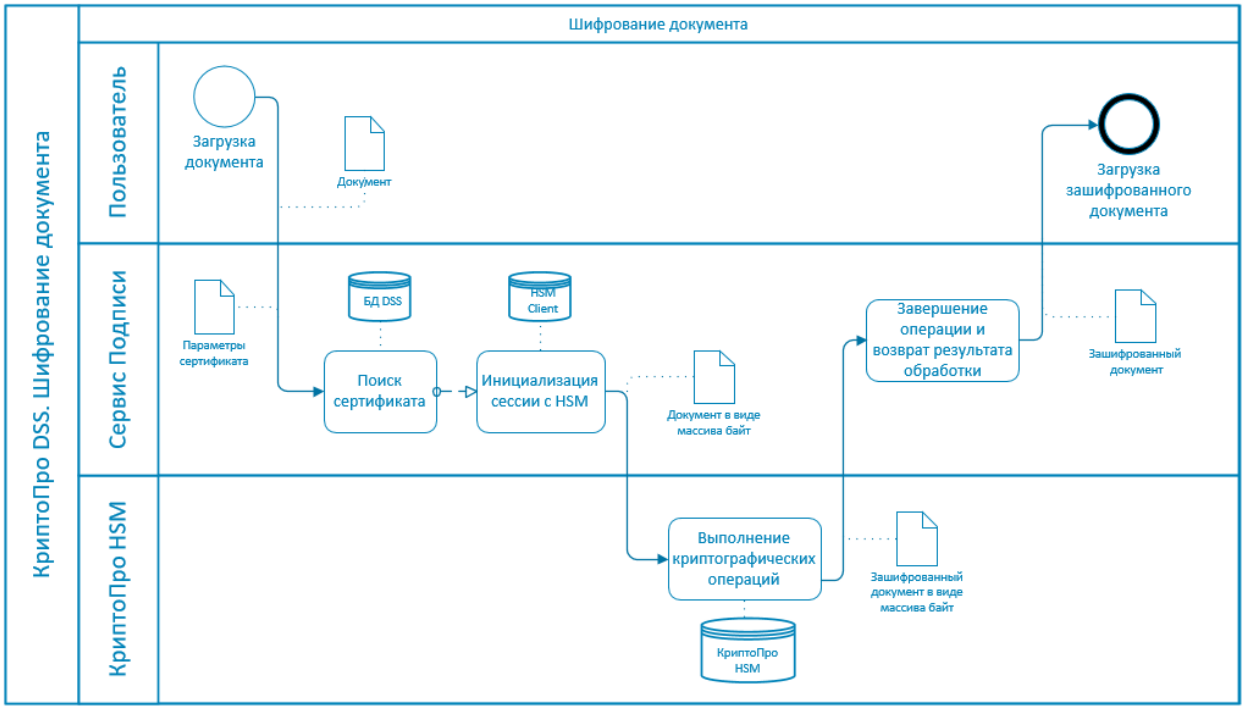

Рис. 11 — Шифрование документа

7.5.6. 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.

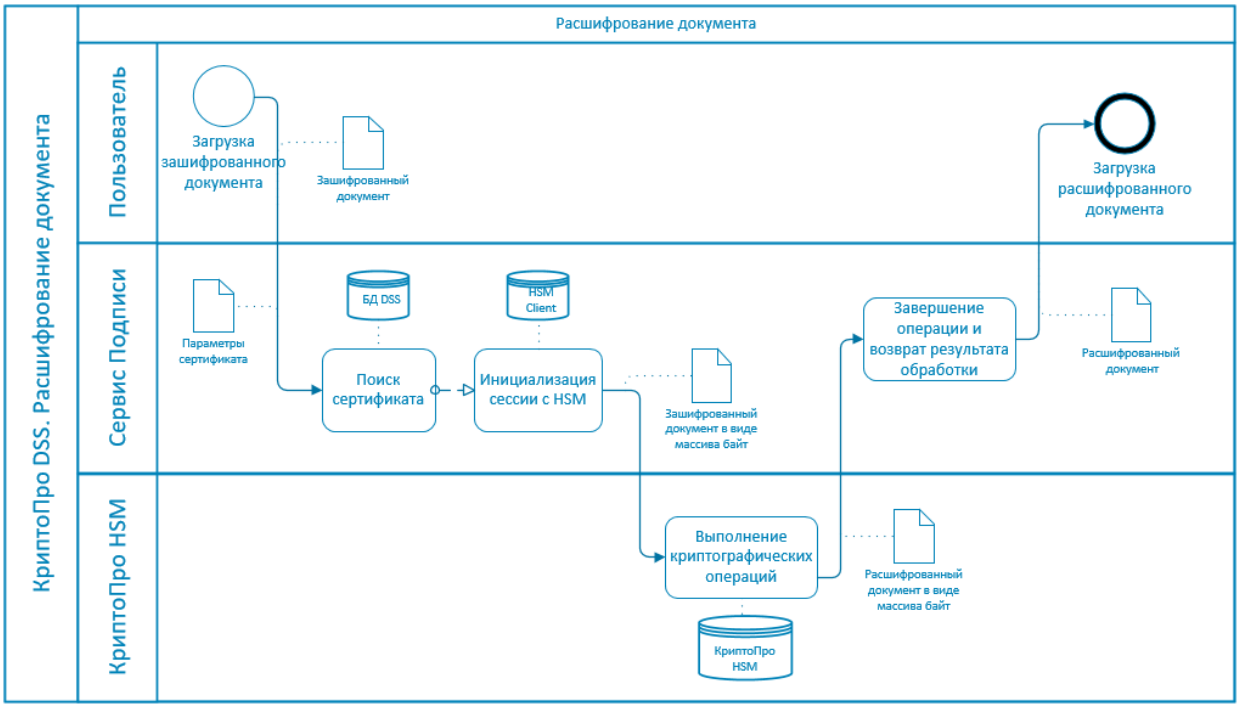

Рис. 12 — Расшифрование документа

7.5.7. Аудит событий и формирование отчетов

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

- 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 DSS 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.

8. Системные требования

8.1. Аппаратное обеспечение

Аппаратные требования к техническим средствам, на которых размещаются программные компоненты КриптоПро DSS, зависят от количества зарегистрированных Пользователей и требований по производительности всего комплекса.

В данном документе приведены рекомендуемые минимальные требования к техническим средствам, которые обеспечивают установку и работу компонентов при 1000 Пользователях:

Таблица 2 — Требования к аппаратному обеспечению

Оборудование	Минимальные требования
Центральный процессор	64-разрядный двухъядерный процессор с тактовой частотой 1,86 ГГц.
Оперативная память	4 ГБ ОЗУ.
Жесткий диск	4 ГБ свободного места.
Сетевые адаптеры	Один сетевой адаптер, совместимый с операционной системой компьютера, для взаимодействия с внутренней сетью.

8.2. Программное обеспечение

КриптоПро DSS представляет собой набор веб-сервисов, как уже было сказано ранее. Поэтому ко всем его компонентам предъявляются одинаковые системные требования:

- Microsoft Windows Server 2008 R2/2012/2012R2/2016/2019 (x64);
- SQL Server 2008 R2/2012/2014/2016/2017/2019.

SQL Server не требуется только для тех компонентов, которые не имеют собственной БД. В настоящий момент таким компонентом является Веб-интерфейс Пользователя. При тестировании КриптоПро DSS можно использовать СУБД MS SQL Express, однако при эксплуатации необходимо использовать СУБД Microsoft SQL Server 2008 R2/2012/2014/2016/2017/2019.

9. Интеграция с внешними ИС

КриптоПро DSS предоставляет программные интерфейсы автоматизации, которые позволяют интегрировать использование сервера электронной подписи в существующие бизнес-процессы и системы. На Рис. 13 и Рис. 14 представлены типовые схемы использования КриптоПро DSS с интегрируемой ИС (например, ДБО).

В приведенных примерах иллюстрируется работа КриптоПро DSS с подтверждением операции посредством отправки одноразового пароля в SMS-сообщении (OTP-via-SMS). О других способах аутентификации см. раздел 4.

9.1. Использование HTTP-API

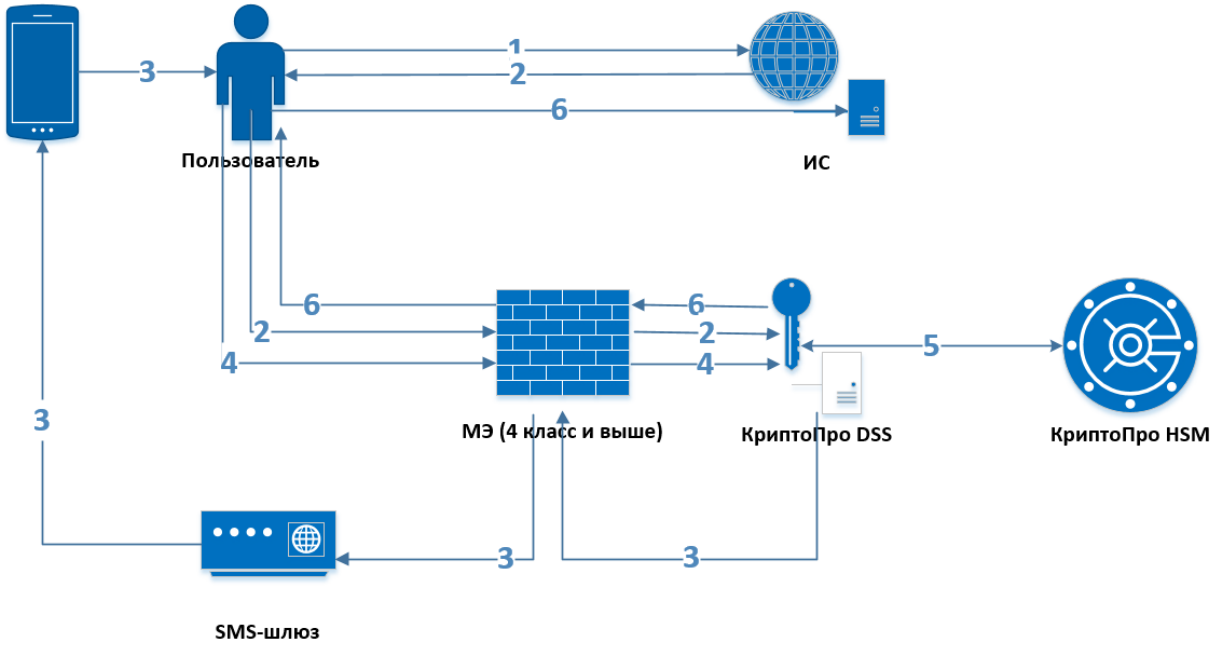

Рис. 13 — Взаимодействие с КриптоПро DSS с использованием HTTP-API

Сценарий взаимодействия:

4. Пользователь отправляет сформированный документ в Информационную Систему (ИС).
5. ИС, используя штатные документированные механизмы КриптоПро DSS, перенаправляет Пользователя на Веб-Интерфейс КриптоПро DSS, передавая в этом перенаправлении подписанный маркер доступа, содержащий информацию о Пользователе (имя Пользователя, номер мобильного телефона и т.п.), и подписываемый документ.
6. Для подтверждения подписания документа КриптоПро DSS направляет Пользователю SMS-сообщение, содержащее код подтверждения подписания и значимые поля документа (например, получатель, сумма и т.п.), на номер мобильного телефона, полученный в маркере доступа.
7. Пользователь вводит полученный код подтверждения в поле формы Веб-Интерфейса.

8. Сервис Подписи КриптоПро DSS, используя документированные функции ПАКМ «КриптоПро HSM», отправляет запрос на подписание документа с использованием закрытого ключа Пользователя и получает подписанный документ.
9. КриптоПро DSS перенаправляет Пользователя на веб-интерфейс ИС, передавая в перенаправлении подписанный документ.

9.2. Использование SOAP/REST

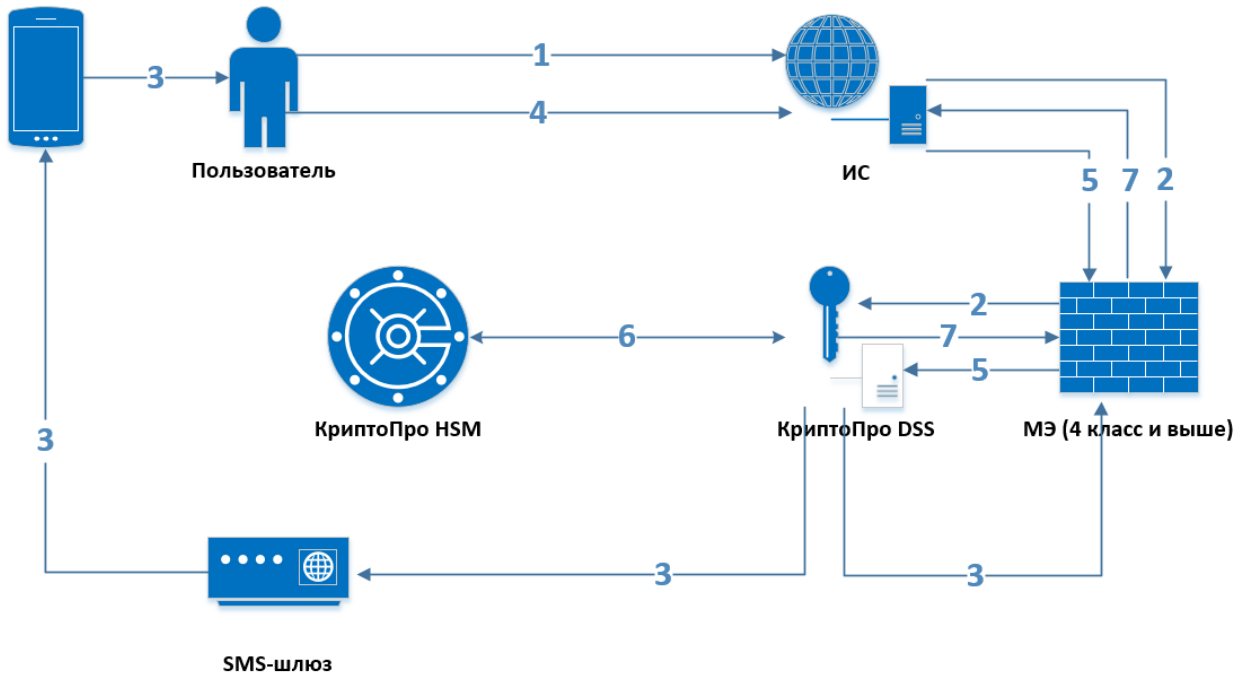

Рис. 14 — Взаимодействие с КриптоПро DSS с использованием SOAP

Сценарий взаимодействия:

1. Пользователь отправляет сформированный документ в Информационную Систему (ИС).
2. Информационная Система, используя штатные документированные механизмы, передает подписываемый документ и подписанный маркер доступа, содержащий информацию о Пользователе (имя Пользователя, номер мобильного телефона и т.п.).
3. Для подтверждения подписания документа КриптоПро DSS направляет Пользователю SMS-сообщение, содержащее код подтверждения подписания и значимые поля документа (например, получатель, сумма и т.п.), на номер мобильного телефона, полученный в маркере доступа.
4. Пользователь вводит полученный код подтверждения в поле формы веб-интерфейса ИС.
5. ИС передает полученный код подтверждения в КриптоПро DSS.
6. Сервис Подписи, используя документированные функции ПАКМ «КриптоПро HSM», отправляет запрос на подписание документа с использованием закрытого ключа Пользователя и получает подписанный документ.
7. Сервис Подписи передает подписанный документ в ИС.

10. Система ролей в КриптоПро DSS

Система ролей в КриптоПро DSS позволяет разграничить права доступа лиц, работающих с КриптоПро DSS. Существуют следующие роли:

- Пользователь;
- Оператор;
- Оператор Аудита;
- Администратор;
- Системный Администратор.

Логическая структура ролей в КриптоПро DSS изображена на Рис. 15.

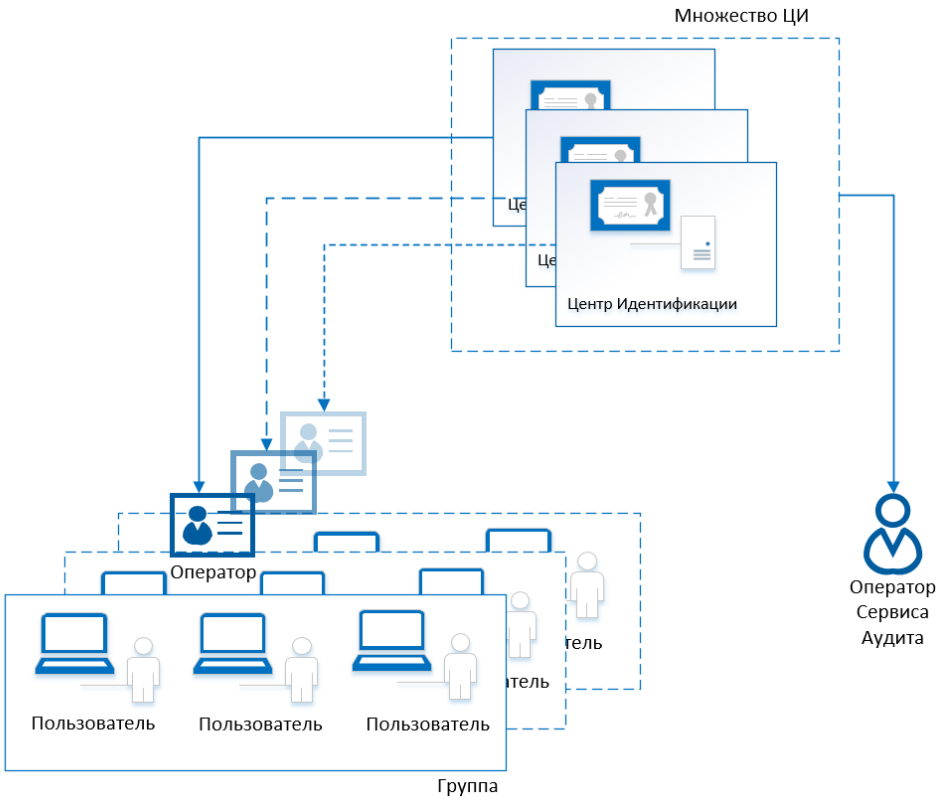

Рис. 15 — Логическая структура ролей в КриптоПро DSS

Пользователь КриптоПро DSS — любой пользователь, получивший учетные данные для входа от Оператора. Ему доступен основной функционал КРИПТОПРО DSS и личный кабинет, где он может просмотреть свой профиль и настроенные для него способы аутентификации (см. раздел 4). Редактирование личных данных и способов аутентификации осуществляется в основном Оператором, однако в системе есть возможность выдачи Пользователю прав на такие действия.

Управление учетными записями Пользователей в КриптоПро DSS может осуществляться только через веб-интерфейс (Оператором и частично самим Пользователем).

Пользователи, прошедшие процедуру аутентификации, объединены вокруг своего экземпляра Центра Идентификации. Для них могут быть включены общие настройки аутентификации, подтверждения операций, а также политика компонентов имени, в

которой указывается, какие компоненты имени обязательно должны присутствовать при регистрации Пользователя.

Пользователи, вне зависимости от того, к какому экземпляру ЦИ они относятся, могут быть разделены на группы под управлением Операторов. Пользователю может быть назначена только одна группа. Группа Пользователей также характеризуется различными общими настройками и политиками, действующими для всех входящих в нее Пользователей и Операторов. Это могут быть правила входа, вторичной аутентификации (подтверждение входа и подтверждение операций). Если в Центре Идентификации разрешена самостоятельная регистрация, то при создании Пользователем своей учетной записи он будет включен в группу по умолчанию.

Для каждого Пользователя индивидуально могут быть заданы способы аутентификации и подтверждения входа и операций (см. раздел 4). Однако изменение этих настроек должно соответствовать настройкам экземпляра ЦИ, в котором Пользователь создан.

Оператор КриптоПро DSS — привилегированный пользователь, имеющий право на создание, редактирование и удаление учетных записей Пользователей, а также на управление сертификатами Пользователей DSS. Оператор может быть включен в одну и более групп. Оператор может управлять учетными записями и сертификатами Пользователей только в рамках своей группы (групп). При создании учетной записи Оператора ему назначается группа по умолчанию. В дальнейшем можно изменить набор групп, в которые включен Оператор.

В целях обеспечения безопасности Центр Идентификации не имеет предустановленной встроенной учетной записи Оператора. Поэтому создание учетной записи Оператора возможно только локально на сервере, где установлен Центр Идентификации КриптоПро DSS. Роль Оператора назначается Администратором путем выдачи Оператору сертификата с расширенными правами и клиентской аутентификацией.

Оператор КриптоПро DSS обеспечивает выполнение следующих задач:

- Регистрация Пользователей КриптоПро DSS;
- Управление (редактирование, удаление) учетными записями зарегистрированных Пользователей КриптоПро DSS;
- Настройка аутентификации Пользователей;
- Прием заявлений на регистрацию средств аутентификации Пользователей (средства аутентификации представлены в разделе 4);
- Просмотр средств аутентификации, зарегистрированных в ЦИ КриптоПро DSS;
- Создание запросов на сертификаты Пользователей КриптоПро DSS;
- Выдача сертификатов Пользователям;
- Просмотр и печать событий аудита назначенных Оператору групп.

Роль **Оператора Аудита** КриптоПро DSS предназначена для мониторинга событий, поступающих от компонентов КриптоПро DSS и Пользователей, и формирования отчетов по данным событиям. Оператору Аудита доступны события всех Пользователей внутри определенного Центра Идентификации, в отличие от других ролей, которым события доступны только в фильтрованном по группе/Пользователю виде. Оператор Аудита существует только в пределах Сервиса Аудита и не имеет доступа к другим компонентам КриптоПро DSS

В целях обеспечения безопасности Центр Идентификации не имеет предустановленной встроенной учетной записи Оператора Аудита. Поэтому создание учетной записи Оператора Аудита возможно только локально на сервере, где установлен

Центр Идентификации КриптоПро DSS. Роль Оператора Аудита назначается Администратором путем выдачи Оператору Аудита сертификата с клиентской аутентификацией.

Администратор КриптоПро DSS — это лицо, имеющее доступ к БД компонентов КриптоПро DSS и к управлению КриптоПро DSS при помощи командлетов. Его задачами являются:

- Администрирование специального программного обеспечения;
- Настройка экземпляров компонентов КриптоПро DSS;
- Управление (создание, редактирование, удаление) учетными записями Операторов КРИПТОПРО DSS;
- Управление лицензиями КриптоПро DSS.

Роль Администратора логически не зависит от других ролей, групп и экземпляров ЦИ. Данная роль создается на каждом экземпляре компонента КриптоПро DSS, имеющем БД, для получения прав на выполнение управляющих командлетов. Поэтому на схеме логической структуры ролей она не отображается.

Системный Администратор КриптоПро DSS занимается администрированием сервера(-ов) с КриптоПро DSS. Он обеспечивает выполнение следующих задач:

- Установка общесистемного и специального программного обеспечения компонентов КриптоПро DSS;
- Создание, удаление и обновление экземпляров компонентов КриптоПро DSS;
- Администрирование общесистемного программного обеспечения;
- Архивирование и восстановление настроек общесистемного программного обеспечения;
- Установка и конфигурирование дополнительных программно-аппаратных средств, обеспечивающих контроль целостности программных средств;
- Администрирование программно-аппаратных средств, реализующих меры защиты от НСД на компонентах КриптоПро DSS.

Роль Системного Администратора логически не зависит от других ролей, групп и экземпляров ЦИ. Поэтому на схеме логической структуры ролей она не отображается.

В целях обеспечения безопасности необходимо, чтобы роли Администратора, Системного Администратора, Оператора и Оператора Аудита принадлежали разным людям из независимых структурных подразделений организации, что позволит исключить возможность сговора и компрометации данных Пользователей КриптоПро DSS.

Рекомендуется также назначать указанные роли материально ответственным лицам и лицам из руководящего состава организации.

11. Поддерживаемые типы ЭП и форматы документов

11.1. Усовершенствованная подпись (CMS Advanced Electronic Signature)

КриптоПро DSS позволяет формировать усовершенствованную подпись, формат которой основан на стандарте ETSI TS 101 733 («CMS Advanced Electronic Signature, CAdES»).

Усовершенствованная электронная подпись позволяет:

- Обеспечить доказательное подтверждение момента создания ЭП;
- Обеспечить доказательное подтверждение действительности сертификата открытого ключа на момент создания ЭП;
- Обеспечить отсутствие необходимости сетевых обращений при проверке ЭП;
- Обеспечить архивное хранение электронных документов.
- Доказательно подтвердить момент создания ЭП позволяет полученный на нее штамп времени.
- Доказательно подтвердить действительность сертификата открытого ключа на момент создания подписи позволяет информация о статусе сертификата, полученная в режиме реального времени.

Данный формат подписи позволяет сформировать криптографическое сообщение, являющееся полностью самодостаточным для его открытия и выполнения всех необходимых операций. С этой целью в сообщении размещается информация об исходном документе, алгоритмах хэширования и подписи, параметрах алгоритмов, времени подписи, сертификате закрытого ключа, цепочки сертификации.

КриптоПро DSS оперирует тремя форматами электронной подписи:

- **CAdES Basic Electronic Signature (CAdES-BES).**

Представляет собой подпись формата Cryptographic Message Syntax (RFC 5652). CAdES-BES требует обязательного наличия в подписанном сообщении подписанного атрибута SigningCertificateV2. Данный атрибут идентифицирует сертификат подписывающего и позволяет дополнить подпись до формата CAdES-X Long Type 1.

Также в подписанное сообщение добавляется подписанный атрибут signingTime – отметка о времени создания подписи (время в атрибуте указывается по часам сервера).

Два следующих типа электронной подписи, доступных в КриптоПро DSS, являются усовершенствованным вариантами CAdES-BES.

- **CAdES-T (Timestamp).**

Представляет собой электронную подпись с доверенным временем Timestamp. Подходит для ситуации, в которой использованные сертификаты, будучи действительными на момент генерации подписи, были отозваны после этого. Поэтому для доказательства того, что данные были подписаны до отзыва сертификатов и что эти данные существовали на определенный момент времени, используются штампы времени, подписанные службой проверки штампов времени до истечения срока действия хотя бы одного сертификата. Это дает ценность подписи при ее проверке.

- **CAdES with Extended Long validation data Type 1 (CAdES-X Long Type 1).**

Данный формат представляет собой усовершенствованную подпись, позволяющую обеспечить участников электронного документооборота всей необходимой доказательной базой (причем собранной в самой ЭП в качестве реквизитов электронного

документа), связанной с установлением момента подписи и статуса сертификата открытого ключа на момент подписи.

В зависимости от наличия исходного документа в самом сообщении, выделяют два типа CMS-подписи:

- Присоединенная подпись (attached).

Получатель такого сообщения может проверить полученную подпись даже при отсутствии исходного подписанного документа.

- Отделенная подпись (detached).

Получатель сообщения этого типа для проверки подписи должен иметь исходный документ, для которого была сформирована подпись.

11.2. Подпись XML-документов (XML Digital Signature, XMLDSig)

Данный формат подписи реализует рекомендации W3C.

Отличительной особенностью данного формата подписи является то, что подпись представляет собой XML-узел, помещаемый внутрь подписываемого документа или являющийся самостоятельным документом.

В КриптоПро DSS реализована поддержка трех типов XML-подписи:

- Вложенная XML-подпись (enveloped). XML-подпись находится внутри подписываемого узла.
- Присоединенная XML-подпись (enveloping). Подписываемый узел находится внутри структуры XML-подписи.
- XML-подпись по шаблону. Происходит подпись документа, содержащего шаблон подписи с незаполненными значениями подписи. В процессе подписания данные значения вычисляются и заносятся в структуру подписи.

11.3. Электронная подпись ГОСТ Р 34.10–2001 и ГОСТ Р 34.10–2012 (Необработанная ЭП)

Данный формат предназначен для вычисления электронной подписи данных по алгоритмам ГОСТ Р 34.10–2001 и ГОСТ Р 34.10–2012.

КриптоПро DSS поддерживает два типа подписи:

- Подпись данных. В качестве входных данных для формирования подписи используется исходный документ.
- Подпись значения хэш-функции. Возвращает значение электронной подписи от переданного значения функции хэширования ГОСТ Р 34.11–94 и ГОСТ Р 34.11-2012.

11.4. Подпись документов Microsoft Office

Данный формат подписи позволяет формировать электронную подпись для обеспечения юридической значимости электронных документов Word и Excel из состава Microsoft Office 2007/2010/2013.

После формирования электронной подписи подписанный документ будет доступен только для чтения. Если в подписанный документ нужно внести изменения, то все созданные подписи следует удалить из документа, поскольку они станут недействительными.

КриптоПро DSS формирует неотображаемую подпись документа.

11.5. Подпись PDF-документов

Данный формат подписи позволяет формировать электронную подпись для обеспечения юридической значимости электронных документов, формируемых в формате PDF – стандарта обмена электронными документами.

В КриптоПро DSS реализовано три типа подписи данного формата:

- Подпись PDF документа с использованием формата CMS. В документ будет добавлена подпись в формате CMS. Для проверки такой подписи в программах Adobe Acrobat и Adobe Reader необходим плагин КриптоПро PDF.
- Подпись PDF документа с использованием формата CAdES-T. В документ будет добавлена подпись в формате CAdES-T, то есть подпись, содержащая штамп времени. Проверить такую подпись можно с помощью плагина КриптоПро PDF.
- Подпись PDF документа с использованием CAdES-XLT1 формата. В документ будет добавлена подпись в формате CAdES-XLT1, то есть содержащая штамп времени и ответы службы актуальных статусов сертификатов. Проверить такую подпись можно с помощью плагина КриптоПро PDF.

12. Поддерживаемый формат шифрования документов

КриптоПро DSS позволяет зашифровывать и расшифровывать документы в формате CMS Enveloped Data (RFC 5652, ТК-026).

Данный формат предназначен для создания криптографического сообщения, состоящего из зашифрованных данных и зашифрованных сессионных ключей, с помощью которых были зашифрованы данные.

Сессионные ключи зашифровываются с помощью транспортных ключей, вырабатываемых на основе открытых ключей, содержащихся в сертификатах получателей сообщения. Данные могут быть зашифрованы для нескольких получателей.

СВЕДЕНИЯ О РАЗРАБОТЧИКЕ

Компания КриптоПро создана в 2000 году и в настоящее время занимает лидирующее положение по распространению средств криптографической защиты информации и электронной цифровой подписи.

Основное направление деятельности компании – разработка средств криптографической защиты информации и развитие Инфраструктуры Открытых Ключей (Public Key Infrastructure) на основе использования международных рекомендаций и российских криптографических алгоритмов.

Компания разработала полный спектр программных и аппаратных продуктов для обеспечения целостности, авторства и конфиденциальности информации с применением ЭП и шифрования для использования в различных средах (Windows, Unix, Java). Новое направление продуктов компании – программно-аппаратные средства криптографической защиты информации и использованием смарт-карт и USB ключей, позволяющих существенно повысить безопасность систем, использующих ЭП.

Компания КриптоПро является разработчиком и поставщиком средств применения ЭП в автоматизированных информационных системах. Кроме этого, компания оказывает консультационные услуги по обеспечению деятельности удостоверяющих центров и применению ЭП в автоматизированных информационных системах предприятий различных форм собственности.

Удостоверяющий центр компании КриптоПро предоставляет организациям (юридическим лицам) услуги по изготовлению и управлению открытыми и закрытыми ключами пользователей информационных систем, включая процедуру подачи и обработки запросов на сертификаты, верификацию запросов на сертификаты, формирования сертификатов, их получения, использования и отзыва. Также Удостоверяющим центром предоставляются иные сервисные функции, связанные с использованием электронных подписей, шифрованием, обеспечением электронного юридически-значимого документооборота.

Контакты:

ООО «КРИПТО-ПРО»

127018, Москва, ул. Сущевский вал, 18

Телефон: (495) 995 4820

Факс: (495) 995 4820

URL: http://www.CryptoPro.ru

E-mail: info@CryptoPro.ru