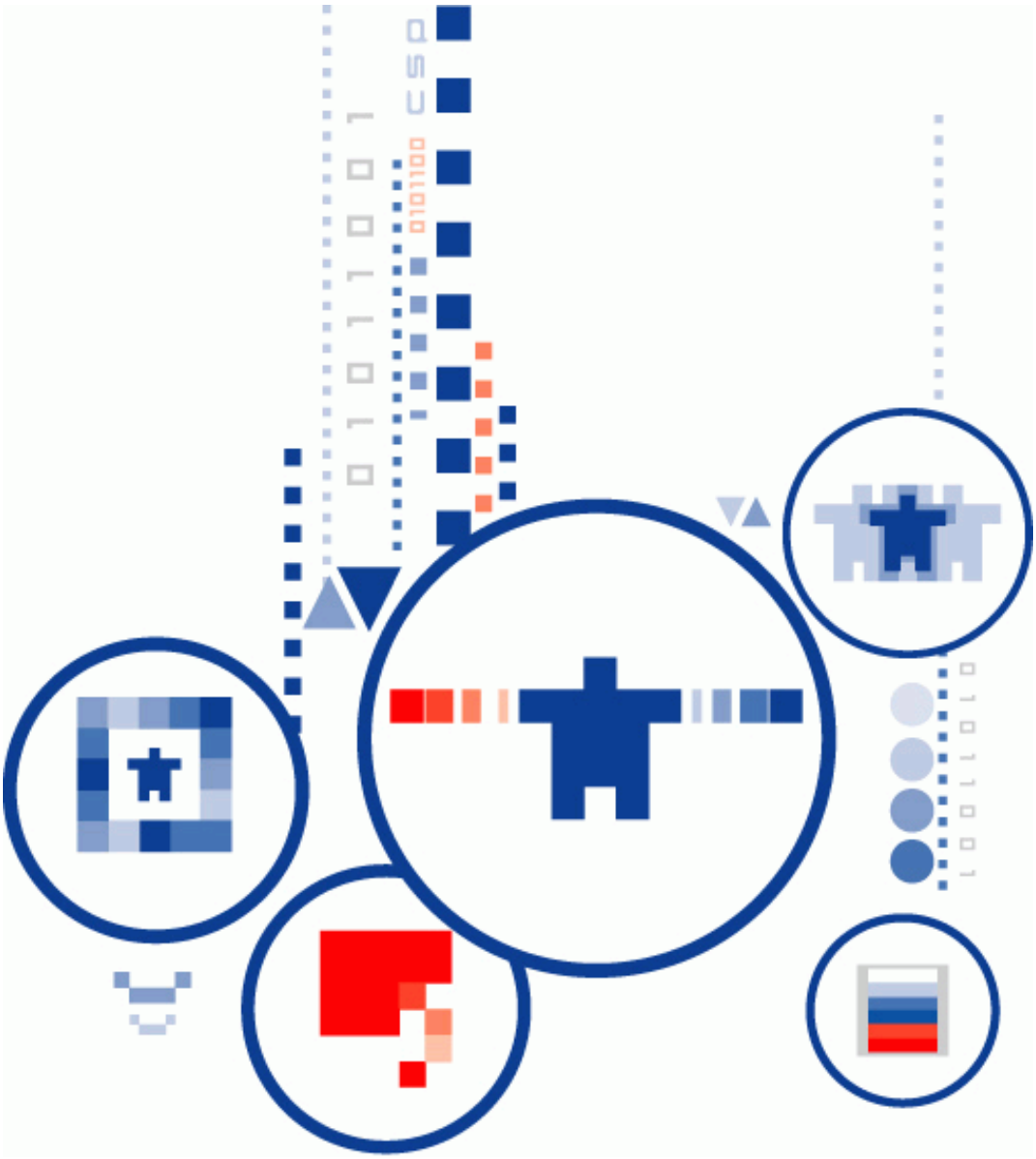

Программно-аппаратный комплекс

«КриптоПро DSS» версии 3.0

Общее описание

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CAdES	—	Расширенная версия стандарта электронной подписи CMS (CMS Advanced Electronic Signatures)
CRL	—	Список отзыва сертификатов (Certificate Revocation List)
CSP	—	Криптопровайдер (Cryptographic Service Provider)
HSM	—	Аппаратный модуль системы безопасности (Hardware security module)
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 актуального статуса сертификата (Online Certificate Status Protocol)
OTP	—	Пароль, действительный только для одного сеанса аутентификации (One-Time Password)
PAdES	—	Расширенная версия стандарта электронной подписи PDF-документов (PDF Advanced Electronic Signatures)
REST	—	Архитектурный стиль построения распределенного приложения (Representational State Transfer)
SDK	—	Набор программных компонентов для использования в мобильных приложениях (Software development kit)
TLS	—	Протокол защиты транспортного уровня (Transport Layer Security)
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)
XAdES	—	Расширенная версия стандарта электронной подписи XML-документов (XML Advanced Electronic Signatures)
АРМ	—	Автоматизированное рабочее место
БД	—	База данных
ЗПС	—	Замкнутая программная среда
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

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 сервисом 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

Настоящий документ содержит описание программно-аппаратного комплекса (ПАК) «КриптоПро DSS» версии 3.0 (далее — КриптоПро DSS). КриптоПро DSS позволяет создавать электронную подпись и шифровать документы различных форматов, что обеспечивает их конфиденциальность, целостность и аутентичность (подлинность и защиту от подделки). Выполнение криптографических операций реализуется при участии ПАКМ «КриптоПро HSM», СКЗИ «КриптоПро CSP», а также библиотеки программных компонентов для мобильных приложений DSS SDK и мобильных приложений, созданных на ее основе.

В данном документе приведено назначение ПАК «КриптоПро DSS» версии 3.0 и основные решаемые им задачи, описаны входящие в него компоненты и их функциональные характеристики, а также логическая архитектура программного комплекса.

Документ предназначен для руководителей и администраторов как ознакомительный материал перед установкой и эксплуатацией ПАК «КриптоПро DSS» версии 3.0.

2. Общие сведения

2.1. Назначение КриптоПро DSS

ПАК «КриптоПро DSS» предназначен для:

- Выполнения криптографических операций при различных вариантах хранения и защиты ключей Пользователей (в соответствии с выбранным режимом хранения ключей, см. раздел 6);
- 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 и защиты от подделки) 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.

Работа с учетными записями:

- регистрация Пользователей;
- ведение реестра зарегистрированных Пользователей
- удаление Пользователей.

Выполнение криптографических операций:

- аутентификация Пользователей и Операторов;
- генерация ключей ЭП, ключей проверки ЭП, закрытых и открытых ключей шифрования (см. 6);
- формирование запросов на сертификаты;
- создание и проверка ЭП;
- подтверждение операций.

Другое:

- аудит событий, связанных с эксплуатацией программного комплекса;
- оповещение Пользователей о событиях о операциях в КриптоПро DSS с использованием SMS-сообщений, сообщений электронной почты и PUSH-уведомлений в соответствии с описанием схемы размещения компонентов (см. раздел 7.5);
- получение и отправка документов, с которыми выполняются криптографические операции;
- визуализация (конвертация и отображение) документов для Пользователей перед выполнением операции с данными документами.

2.4. Исполнения КриптоПро DSS

В данном разделе перечислены доступные исполнения и группы исполнений. Дополнительно установлено соответствие групп исполнений типам хранения ключей подписи пользователей (см. также 6).

КриптоПро DSS в зависимости от набора используемых компонентов предоставлен в следующих исполнениях.

- **Исполнение 1 (класс защиты КС3)** — содержит серверные компоненты КриптоПро DSS (см. 3.1);
- **Исполнение 2 (класс защиты КС1)** — содержит клиентские компоненты КриптоПро DSS, представляющие собой мобильные приложения и средства для их разработки (см. 3.2.10);
- **Исполнение 3 (класс защиты КС1), Исполнение 4 (класс защиты КС2), Исполнение 5 (класс защиты КС3)** — содержат клиентские компоненты, представляющие собой КриптоПро CSP/JCP и ПО «КриптоПро ЭЦП Browser plug-in» (см. 3.2.10).

Группы исполнений позволяют соотнести исполнения КриптоПро DSS с типами хранения ключей подписи Пользователей. Существуют следующие группы исполнений.

- **Группа исполнений 1** — включает в себя Исполнения 1 и 2. Ключи Пользователей хранятся **распределенно** (на мобильном устройстве с дополнительной защитой Пользовательских ключей с помощью серверного компонента).
- **Группа исполнений 2** — включает в себя Исполнения 1 и 2. Ключи Пользователей хранятся на клиентском компоненте (**мобильное приложение**) с защитой Пользовательских ключей средствами только этого клиентского компонента.
- **Группа исполнений 4** — включает в себя Исполнения 1 и 3–5. Ключи Пользователей хранятся **на клиентском компоненте** (**стационарное устройство**) с автономной защитой Пользовательских ключей.

3. Описание КриптоПро DSS

3.1. Состав КриптоПро DSS

КриптоПро DSS включает в себя следующие компоненты:

- Центр Идентификации (ЦИ, см. раздел 3.2.1):
  - Служба управления Пользователями;
  - Служба маркеров безопасности;
  - База данных (БД) ЦИ.
- Сервис Подписи (см. раздел 3.2.2):
  - ПО Сервиса Подписи;
  - БД Сервиса Подписи;
- Веб-интерфейс (см. раздел 3.2.3);
- Сервис Аудита (см. раздел 3.2.4):
  - ПО Сервиса Аудита;
  - БД Сервиса Аудита.
- Сервис Обработки Документов (см. раздел 3.2.5);
- Сервис взаимодействия с SDK (SDK API Gateway, см. раздел 3.2.7);
- Сервис PUSH-уведомлений;
- Сервис DSS Lite (см. раздел 3.2.8);
- ПАКМ «КриптоПро HSM» (см. раздел 3.2.6);
- СКЗИ КриптоПро CSP (требуется установка на сервере для обеспечения работы компонентов).
- Клиентские компоненты (см. раздел 3.2.10):
  - КриптоПро CSP/JCP;
  - ПО «КриптоПро ЭЦП Browser plug-in»;
  - КриптоПро TSP Client (компонент из состава СКЗИ «КриптоПро CSP», используется опционально);
  - КриптоПро OCSP Client (компонент из состава СКЗИ «КриптоПро CSP», используется опционально);
  - DSS SDK для встраивания в мобильное приложение:
    - DSS Client SDK;
    - myDSS 3.0 SDK;
    - мобильное приложение «DSS Client»;
    - мобильное приложение «myDSS 3.0».

Веб-интерфейс Пользователя может быть заменен интерфейсом информационной системы, с которой интегрируется КриптоПро DSS. Сервис DSS Lite является опциональным компонентом (см. пункт 3.2.8). КриптоПро CSP, TSP Client, OCSP Client и HSM Client входят в комплект поставки. ПАКМ «КриптоПро HSM» поставляется отдельно. DSS SDK поставляется отдельно.

3.2. Описание компонентов КриптоПро DSS

3.2.1. Центр Идентификации

Компонент Центр Идентификации предназначен для регистрации, аутентификации Пользователей и Операторов, а также управления информацией, содержащейся в их учетных записях. В случае успешной аутентификации Центр Идентификации выдает электронный идентификатор (маркер безопасности), который затем может быть использован для доступа к другим компонентам КриптоПро DSS или

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

К функциям ЦИ относятся:

- регистрация Пользователей;
- ведение реестра зарегистрированных Пользователей
- удаление Пользователей;
- аутентификация Пользователей и Операторов;
- 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, информация о PUSH-адресе привязанных мобильных устройств и т.п.);
  - данные об Операторах;
- формирование записей о событиях, связанных с работой ЦИ, и отправка их для регистрации в Сервис Аудита (см. раздел 3.2.4).

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

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 маркеров безопасности является обособленной частью Центра Идентификации и отвечает за аутентификацию Пользователей и Операторов при обращении к КриптоПро DSS.

3.2.2. Сервис Подписи

Компонент КриптоПро DSS Сервис Подписи предназначен для управления сертификатами Пользователей, выполнения операций по шифрованию документов и созданию электронной подписи различных форматов.

К функциям Сервиса Подписи относятся:

- создание электронной подписи документов, загружаемых Пользователем;
- шифрование и расшифрование документов, загружаемых Пользователем;
- взаимодействие с КриптоПро HSM при выполнении криптографических операций;
- взаимодействие с УЦ для создания запросов на сертификат и управления сертификатами Пользователей;
- ведение БД, содержащей сведения о сертификатах Пользователей и их ключах (дополнительная информация об управлении ключами пользователей содержится в разделе 6);
- обеспечение доступа к Сервису Подписи внешним приложениям через REST API;
- формирование записей о событиях, связанных с работой Сервисом Подписи, и отправка их для регистрации в Сервис Аудита.

3.2.3. Веб-интерфейс Пользователя

Компонент КриптоПро DSS Веб-интерфейс Пользователя предназначен для организации интерактивного взаимодействия Пользователей и Операторов с компонентами КриптоПро DSS, а также с другими внешними компонентами (например, службой проверки сертификатов и электронной подписи КриптоПро SVS 2.0 «из состава ПАК «Службы УЦ 2.0»). Произведенные Пользователями действия на веб-формах с помощью REST API передаются в другие компоненты КриптоПро DSS и обрабатываются их серверными программными модулями.

В своем личном кабинете на Веб-интерфейсе Пользователя Пользователь при наличии у него соответствующих прав доступа может изменять информацию профиля и настройки аутентификации. При наличии установленного и настроенного компонента «Сервис Аудита» Пользователю доступен просмотр журнала операций, совершенных им в системе.

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

- **Документы.** В данном разделе Пользователь может создать новую или усовершенствовать (дополнить) существующую электронную подпись документа, выполнить процедуры шифрования и расшифрования. Для этого в данном разделе предусмотрена загрузка одного или нескольких документов, выбор необходимых для выполнения операции сертификатов и параметров подписи. Подробнее о поддерживаемых типах подписи см. раздел 11, о форматах шифрования — раздел 12. Также в данном разделе отображается загруженный документ в сценариях, требующих его отображения на Веб-интерфейсе Пользователя.
- **Проверка подписи.** В данном разделе Пользователь может загрузить подписанный документ и/или сертификат и получить сведения о действительности данной подписи и/или сертификата. 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 ПАК «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.
- **Журнал.** 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.
- **Профиль.** В данном разделе отображаются сведения об учетной записи Пользователя — сведения, включаемые в запрос на сертификат (например, ФИО и адрес Пользователя), контактная информация, настройки аутентификации (в разрешенном в соответствии с настройками сервиса объеме), настройки оповещения о событиях и сведения о выданных маркерах безопасности от ЦИ клиентским компонентам. К подразделу настроек аутентификации Пользователя может получить доступ Оператор, если уполномочен выполнять для него настройки аутентификации.

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.

В Веб-интерфейсе Оператору могут быть доступны следующие разделы:

- **Пользователи.** В данном разделе Оператору доступен список Пользователей, принадлежащих к группам в ведении данного Оператора. Оператор может выполнять поиск нужного Пользователя при помощи фильтров и переходить в разделы личного кабинета Пользователя, доступные ему для редактирования. Также в данном разделе Оператор может зарегистрировать новую учетную запись Пользователя.
- **Средства аутентификации.** В данном разделе Оператору доступны зарегистрированные в КриптоПро DSS в разное время средства аутентификации с возможностью поиска средств, связанных с определенным Пользователем, серийным номером и/или лицензией. Данная информация может быть необходима Оператору при настройке аутентификации Пользователей.
- **Оповещения.** В данном разделе Оператору доступен список событий, о которых он может получать оповещения. Возможность настройки оповещения может быть доступна при наличии соответствующих настроек.
- **Журнал.** В данном разделе Оператору доступны записи аудита об операциях, совершенных Пользователями, принадлежащими к группам в ведении данного Оператора. К списку операций можно применять фильтры по логину пользователя, коду и/или дате события.
- **Отчеты.** В данном разделе Оператору доступен список зарегистрированных шаблонов отчетов и возможность создания отчетов о работе пользователей за определенный период времени и с учетом параметров, предопределенных конкретным шаблоном.

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 и расшифрованных документов из БД Сервиса Обработки Документов.

Подробнее о поддерживаемых форматах см. раздел 13.

3.2.6. ПАКМ «КриптоПро HSM»

Программно-аппаратный криптографический модуль (ПАКМ) «КриптоПро HSM» предназначен для хранения и использования ключевой и криптографически опасной информации серверных компонентов КриптоПро DSS, а также для выполнения криптографических операций над пользовательскими данными и обеспечения защиты пользовательских ключей в зависимости от выбранного режима (см. раздел 6).

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».

ПАКМ «КриптоПро HSM» выполняет следующие функции.

- Создание электронной подписи в соответствии с ГОСТ Р 34.10–2012 (34.10–2018).
- Проверка электронной подписи в соответствии с ГОСТ Р 34.10–2012 (34.10–2018) и ГОСТ Р 34.10–2001.
- Вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11–2012 (34.11–2018).
- Шифрование и расшифрование данных и вычисление имитовставки в соответствии с ГОСТ 28147–89, ГОСТ Р 34.12–2015 (34.12–2018), ГОСТ Р 34.13–2015 (34.13–2018).
- Генерация и защищенное хранение ключевой информации (см. раздел 6).
- Управление учетными записями Пользователей ПАКМ.

3.2.7. Сервис Взаимодействия с SDK

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

Схема взаимодействия компонентов, отображающая взаимодействие SDK API Gateway с другими компонентами и продуктами, приведена в разделе 7.2.

Сервис взаимодействия с SDK используется в исполнениях группы 1 и 2 (см. раздел 2.4).

3.2.8. Сервис DSS Lite

Сервис DSS Lite предназначен для выполнения криптографических операций подписи и хэширования с ключами, хранимыми на устройстве Пользователя (например, на отчуждаемом носителе, как это описано в разделе 6). В случае использования DSS Lite КриптоПро DSS не хранит ключи ЭП Пользователей. Сервис предоставляет следующие режимы работы:

- **веб-интерфейс Lite**. В данном режиме сохраняются остальные сервисы КриптоПро DSS (см. подраздел 3.1), но при этом используется особый режим работы Сервиса Подписи. Аутентификация Пользователей и иные способы взаимодействия компонентов КриптоПро DSS аналогичны процессам, описанным

в разделе 7. Возможна настройка отображения документов перед подписью и аудит событий. Доступно создание электронной подписи всех форматов, поддерживаемых КриптоПро DSS (см. раздел 11). Доступно расшифрование документов только формата CMS типа «конверт данных» (см. Р 1323565.1.025–2019). На стороне Пользователя требуется наличие КриптоПро CSP. Для работы в браузере требуется наличие на стороне Пользователя КриптоПро ЭЦП Browser plug-in;

- **REST-сервис Lite**. В данном режиме сервис DSS Lite предоставляет программный интерфейс, позволяющий выполнять вычисление хэш-значения для подписанного документа и формировать структуру подписи необходимого формата. Вычисление значения подписи происходит непосредственно на устройстве Пользователя. Доступно создание электронной подписи всех форматов, поддерживаемых КриптоПро DSS (см. раздел 11). На стороне Пользователя требуется наличие КриптоПро CSP.

Поддерживаемые форматы электронной подписи соответствуют форматам, поддерживаемым в КриптоПро DSS (см. 11). Сервис также предоставляет возможности по усовершенствованию подписей CAdES и XAdES в рамках поддерживаемых форматов.

Сервис DSS Lite не работает с подтверждением операций (например, в мобильном приложении). Формирование подписи документа происходит при помощи средства ЭП пользователя, не входящего в состав DSS Lite. Для хранения ключа подписи необходимо использовать КриптоПро CSP или другое СКЗИ, имеющее действующий сертификат соответствия ФСБ России.

3.2.9. Сервис PUSH-уведомлений

Сервис PUSH-уведомлений позволяет отправлять PUSH-уведомления на мобильные устройства Пользователей. КриптоПро DSS позволяет гибко настраивать список событий, о которых необходимо оповещать пользователей для каждого зарегистрированного на сервере мобильного приложения. Ввиду того, что рассылка PUSH-уведомлений производится через внешние PUSH-серверы, Сервис PUSH уведомлений может быть размещен в выделенном сегменте сети (DMZ), как это описано в 7.3.

3.2.10. Клиентские компоненты

КриптоПро CSP/JCP

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).

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).

СКЗИ «КриптоПро CSP» дополнительно может предоставлять возможность (если она заявлена в документации на данное СКЗИ) любому приложению, использующему вызовы Microsoft CryptoAPI 2.0, подписывать электронные документы и выполнять другие криптографические операции на ключах Пользователей, созданных с использованием КриптоПро DSS.

ПО «КриптоПро ЭЦП Browser plug-in»

ПО КриптоПро ЭЦП Browser plug-in позволяет выполнять сценарии на страницах Веб-интерфейса Пользователя и необходимо для установки на устройство (рабочее место) Пользователя при использовании с компонентом Сервис DSS Lite (см. 3.2.8) в режиме веб-интерфейса. Для работы ПО «КриптоПро ЭЦП Browser plug-in» на АРМ Пользователя необходимо также иметь установленный СКЗИ «КриптоПро CSP».

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 СКЗИ «КриптоПро CSP».

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. Подробная информация о OCSP-клиенте содержится в составе документации на СКЗИ «КриптоПро CSP».

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».

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 выполнять операции подписи, управлять сертификатами, а также подтверждать операции Пользователя в КриптоПро DSS, инициированные другими способами.

В составе КриптоПро DSS доступны готовые мобильные приложения на базе DSS SDK: DSS Client и myDSS 3.0. Возможности создания собственных мобильных приложений с DSS SDK описаны в разделе 3.3.

Способы аутентификации Пользователя при помощи мобильного приложения на базе DSS SDK приведены в разделах 4.3–4.4.

Схема взаимодействия компонентов, отображающая взаимодействие мобильного приложения на базе DSS SDK с другими компонентами и продуктами, приведена в разделе 7.2.

Использование мобильного приложения на базе DSS SDK допускается в исполнениях группы 1 и 2 (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 в мобильное приложение с мобильного устройства или со стороны сервера (в том числе через интегрированную информационную систему).
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 групп 1 и 2 (см. раздел 2.4).

DSS SDK встраивается в мобильное приложение в соответствии с руководствами разработчика из комплекта документации на выбранное исполнение. 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, 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 подразделах 4.1, 4.2, 4.3 и 4.5, для аутентификации на рабочей станции Пользователя требуется наличие сертифицированного ФСБ России СКЗИ КриптоПро CSP версии 5.0 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 подразделе 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 во всех исполнениях, приведенных в подразделе 2.4.

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

Данный метод аналогичен методу, описанному в подразделе 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.

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.

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

Описанные в данном подразделе способы аутентификации реализуются в исполнениях групп 1 и 2 (см. подраздел 2.4).

4.4. 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 КриптоПро DSS.

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

Описанные в данном подразделе способы аутентификации реализуются в исполнениях групп 1 и 2 (см. подраздел 2.4).

4.5. Дополнительные способы аутентификации

При использовании аутентификации только по логину и паролю (подраздел 4.1) или аутентификации по сертификату (подраздел 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 подразделах 4.1–4.4.

4.6. Механизм аутентификации с помощью мобильного приложения

4.6.1. Процесс подтверждения операций

Подтверждение операций с помощью мобильного приложения 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 (см. 6).

Аутентификация Пользователя при создании ЭП документа происходит следующим образом: Пользователь или интегрируемая с КриптоПро DSS информационная система инициируют процесс создания ЭП, передавая документ в КриптоПро DSS. обрабатывает полученный документ и подготавливает данные для аутентификации Пользователя. В исполнениях с SDK (см. подраздел 2.4) эти данные содержат как сообщение о выполняемой операции, так и сам документ (см. подразделы 4.3–4.4).

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 мобильное приложение получает доступ к вектору аутентификации Пользователя, хранящемуся на его мобильном устройстве, и вычисляет 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 при участии DSS SDK успешно подписывает документ.

4.6.2. Установка вектора аутентификации в мобильное приложение

Векторы аутентификации Пользователей генерируются ПАКМ «КриптоПро HSM» из Мастер-ключа по запросу Пользователя на использование мобильного приложения на базе DSS SDK. Вектор аутентификации является секретом Пользователя и хранится в мобильном приложении (см. 6). В HSM таким образом хранятся только Мастер-ключи, используемые для генерации векторов аутентификации.

Доставка вектора аутентификации в мобильное устройство Пользователя происходит путем инициализации мобильного приложения на базе DSS SDK и его привязки к учетной записи Пользователя. Данный процесс может быть организован различными способами (см. 5).

Если Пользователь аутентифицируется в КриптоПро DSS с помощью методов, описанных в подразделах 4.1, 4.2, он может самостоятельно получить в своем личном кабинете и отсканировать в мобильном приложении QR-код, содержащий вектор аутентификации. В этом случае QR-код с вектором аутентификации отображается в Веб-интерфейсе Пользователя. Пользователю необходимо отсканировать QR-код, используя мобильное приложение на базе DSS SDK.

Вектор аутентификации, передаваемый в QR-коде, может быть дополнительно защищен на коде активации (защита настраивается Администратором). Коды активации создаются и сохраняются в КриптоПро DSS при выработке векторов аутентификации для Пользователей модуля DSS SDK. 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.

Одноразовый QR-код может быть передан Пользователю в сообщении электронной почты с учетом требований к передаче QR-кода, описанных в подразделе 5.3.

При использовании других методов аутентификации создание вектора аутентификации возможно только с участием Оператора при личном визите Пользователя в офис обслуживания либо при наличии у Пользователя ранее зарегистрированного устройства или квалифицированного сертификата (см. 5).

4.6.3. Смена вектора аутентификации на мобильном устройстве Пользователя

Смена вектора аутентификации на мобильном устройстве Пользователя происходит при помощи новой инициализации мобильного приложения на базе DSS SDK (см. 5).

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 (подраздел 5.1);
- при помощи выбранного идентификатора с дополнительной защитой QR-кодом (подраздел 5.2);
- при помощи QR-кода с начальным вектором аутентификации (подраздел 5.3);
- при помощи самостоятельного получения сертификата (подраздел 5.4);
- при помощи привязанного ранее устройства (подраздел 5.5).

Пользователь КриптоПро DSS, использующий аутентификацию при помощи мобильного приложения на базе DSS SDK (см. подразделы 4.3–4.4), может привязать к своей учетной записи еще одно мобильное устройство без визита к Оператору. Данная процедура описана в подразделе 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 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 КриптоПро DSS.

Оператор КриптоПро DSS выполняет следующие действия.

- Идентифицирует Пользователя.

- Проверяет наличие учетной записи Пользователя в КриптоПро DSS по уникальным признакам (СНИЛС, ИНН и т.п.). Если учетная запись отсутствует, Оператор создает ее.
- Готовит и передает Пользователю на подпись, либо получает от Пользователя подписанные заявительные документы, необходимые для начала обслуживания Пользователя в КриптоПро 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 КриптоПро DSS будет завершена после получения подтверждения. Если Пользователь не согласился с полученными учетными данными, ему следует отказаться от их подтверждения и обратиться к Оператору КриптоПро 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 подразделе 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 КриптоПро 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 КриптоПро DSS.

Оператор КриптоПро DSS выполняет следующие действия.

- Идентифицирует Пользователя.
- Проверяет наличие учетной записи Пользователя в КриптоПро DSS по названному Пользователем уникальному идентификатору ВА. Если учетная запись отсутствует, Оператор КриптоПро DSS создает ее.
- Готовит и передает Пользователю на подпись, либо получает от Пользователя подписанные заявительные документы для начала обслуживания Пользователя в КриптоПро 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 КриптоПро 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 подразделе 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 КриптоПро DSS и обладает следующими особенностями:

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

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

- Идентифицирует Пользователя.
- Проверяет наличие учетной записи Пользователя в КриптоПро DSS по уникальным признакам (СНИЛС, ИНН и т.п.). Если учетная запись отсутствует, Оператор КриптоПро DSS создает ее.
- Готовит и передает Пользователю на подпись, либо получает от Пользователя подписанные заявительные документы для начала обслуживания Пользователя в КриптоПро 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 одноразовый QR-код с начальным ВА, который должен быть передан Пользователю (либо его Доверенному лицу), способом, исключающим возможность несанкционированного ознакомления с ним 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.

Для того чтобы привязывать другие мобильные устройства к той же учетной записи, необходимо генерировать новые одноразовые QR-коды. Администратор может настроить КриптоПро DSS таким образом, что один QR-код может использоваться несколько раз. В этом случае QR-код должен быть передан Пользователю (либо его Доверенному лицу), способом, исключающим возможность несанкционированного ознакомления с ним как третьих лиц, так и Оператора КриптоПро DSS.

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.

Дальнейшие действия по подтверждению сведений об учетной записи Пользователем аналогичны описанным в подразделе 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 КриптоПро 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. В ответ КриптоПро DSS отправляет в мобильное приложение Пользователя на базе DSS SDK вектор аутентификации. Полученные данные сохраняются в мобильном приложении, Пользователь может защитить ВА с помощью ПИН-кода.

Далее Пользователь предъявляет в мобильном приложении полученный им ранее сертификат. В случае если сертификат отсутствует, возможно создание запроса на сертификат в процессе инициализации мобильного устройства. Если установленный сертификат является квалифицированным, Оператор КриптоПро 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 подразделе 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. подразделы 4.3–4.4), 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 КриптоПро DSS.

6. Управление ключами Пользователей

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

- в мобильном приложении;
- в гибридном («распределенном») виде — в мобильном приложении с дополнительной защитой пользовательских ключей с помощью серверного компонента;
- на отчуждаемом носителе, считываемом при помощи мобильного приложения (бесконтактно либо с использованием совместимого коннектора);
- в ПАКМ HSM;
- в БД Сервиса Подписи.

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

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

Режим хранения ключей **на отчуждаемом носителе** подразумевает использование ключей одним из следующих способов:

- использование ключей на стороне Пользователя (в браузере или интегрированном программном или веб-интерфейсе некоторой ИС) при использовании сервиса DSS Lite (см. пункт 3.2.8);
- аналогично режиму хранения ключей в мобильном приложении за тем исключением, что контейнер с ключом находится на отчуждаемом носителе (в том числе ФКН). Для доступа к ключу необходимо использовать мобильное приложение.

Закрытые ключи Пользователей, хранимые в мобильном приложении, распределенно и на отчуждаемых носителях, также имеют ограниченный срок действия, по умолчанию равный 15 месяцам (36 месяцев при хранении в ФКН в неизвлекаемом виде). После окончания срока действия закрытый ключ Пользователя не может больше использоваться для создания подписи, шифрования и расшифрования и должен быть удален.

Режим хранения ключей **в HSM** подразумевает, что ПАКМ КриптоПро HSM является криптопровайдером для КриптоПро DSS и именно в нем хранятся ключи Пользователей. Срок действия ключей составляет 36 месяцев.

Режим хранения ключей **в БД Сервиса Подписи** подразумевают защиту данных ключей при помощи их шифрования на ключе, вырабатываемом с помощью HSM из Мастер-ключа Сервиса Подписи и секрета Пользователя (ПИН-кода). Срок действия ключей составляет 15 месяцев.

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. На Рис. 1 отражено соотношение сроков действия Мастер-ключа и ключей Пользователей в БД Сервиса Подписи. 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	В HSM	В БД Сервиса Подписи	В мобильном приложении	Рапределенно	На внешнем носителе
Что хранится	Все закрытые ключи Пользователей хранятся в ПАКМ HSM.	Все закрытые ключи Пользователей хранятся в БД Сервиса Подписи в зашифрованном виде, в HSM хранится Мастер-ключ.	Все закрытые ключи Пользователей хранятся в мобильном приложении в защищенном виде.	Все закрытые ключи Пользователей хранятся в мобильном приложении в защищенном виде и не могут быть использованы без вектора защиты, соответствующего каждому ключу и хранимому в HSM.	Все закрытые ключи Пользователей хранятся на отчуждаемом носителе в защищенном виде и могут быть использованы при помощи мобильного приложения или на АРМ Пользователя.

Критерий/ Режим	В HSM	В БД Сервиса Подписи	В мобильном приложении	Рапределенно	На внешнем носителе
Срок жизни ключа	36 месяцев.	**Мастер-ключ:** 36 месяцев, 21 месяц пригоден для создания новых ключей. **Ключи Пользователей:** 15 месяцев.	15 месяцев.	15 месяцев	36 месяцев (для неизвлекаемых ключей).

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.

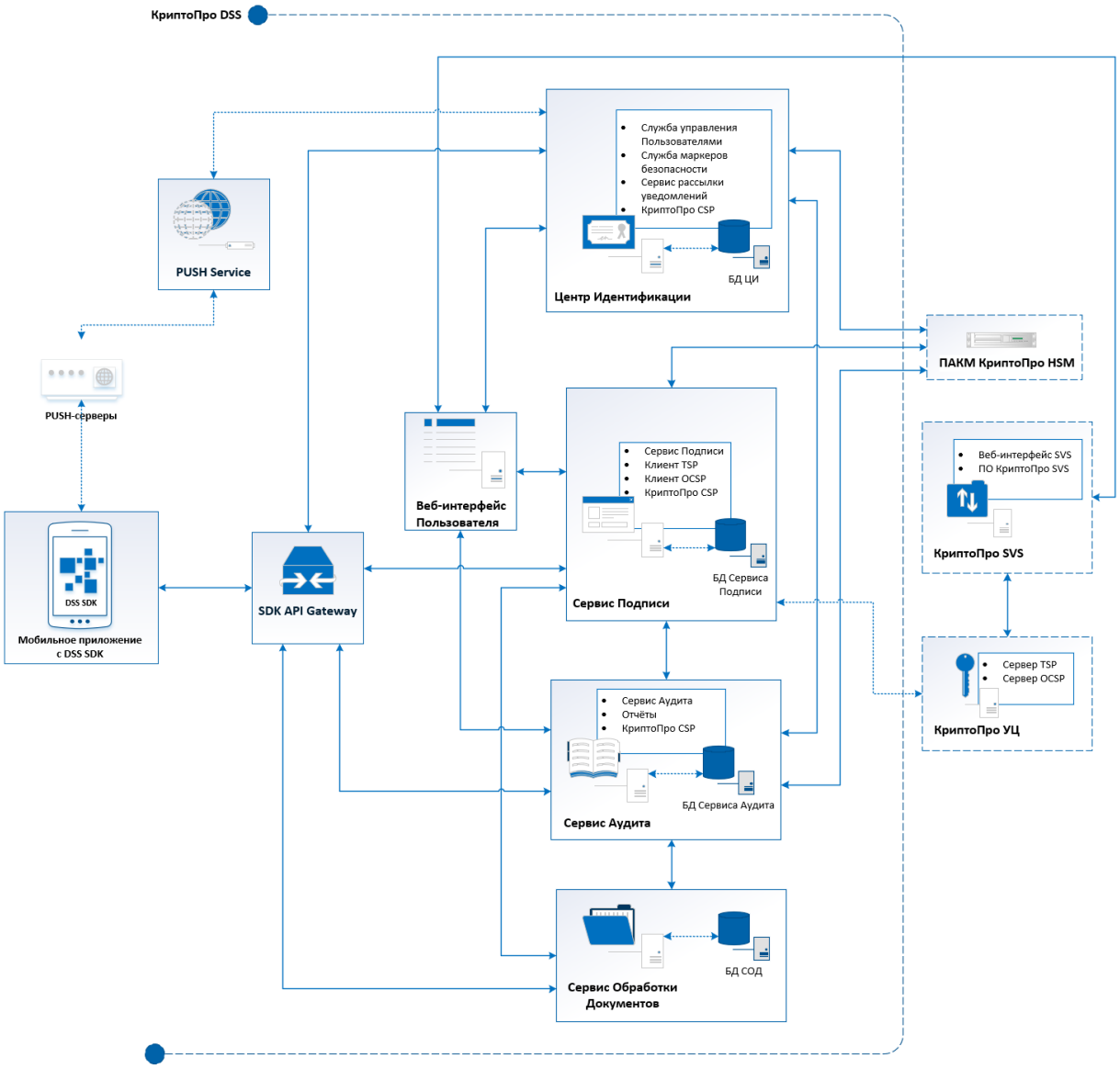

Рис. 2 — Схема взаимодействия компонентов КриптоПро DSS

7.2. Взаимодействие компонентов с Сервисом взаимодействия с мобильным приложением (SDK API Gateway)

Компонент SDK API Gateway осуществляет взаимодействие с другими компонентами КриптоПро DSS в соответствии со схемой взаимодействия компонентов,

приведенной на Рис. 3. Настоящая схема отображает только логические компоненты, непосредственно участвующие во взаимодействии с SDK API Gateway.

Сервер, на котором развернут SDK 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 SDK API Gateway через Сервис PUSH-уведомлений (см. подраздел 7.3).

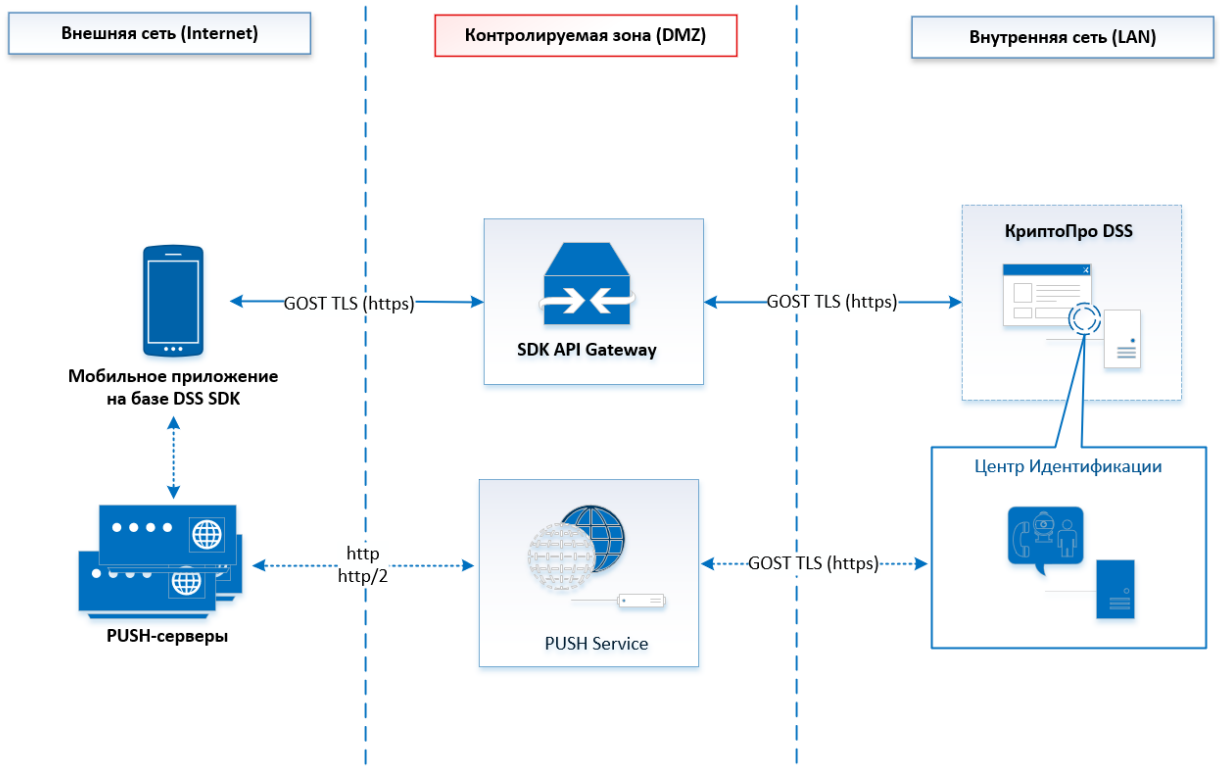

Рис. 3 — Схема взаимодействия компонентов при использовании SDK API Gateway

7.3. Взаимодействие компонентов при оповещении Пользователей

Сервис PUSH-уведомлений (PUSH Service) позволяет отправлять PUSH-уведомления на мобильные устройства Пользователей. КриптоПро DSS позволяет гибко настраивать список событий, о которых необходимо оповещать пользователей для каждого зарегистрированного на сервере мобильного приложения. Ввиду того, что рассылка PUSH-уведомлений производится через внешние PUSH-серверы, Сервис PUSH уведомлений может быть размещен в DMZ (см. Рис. 4).

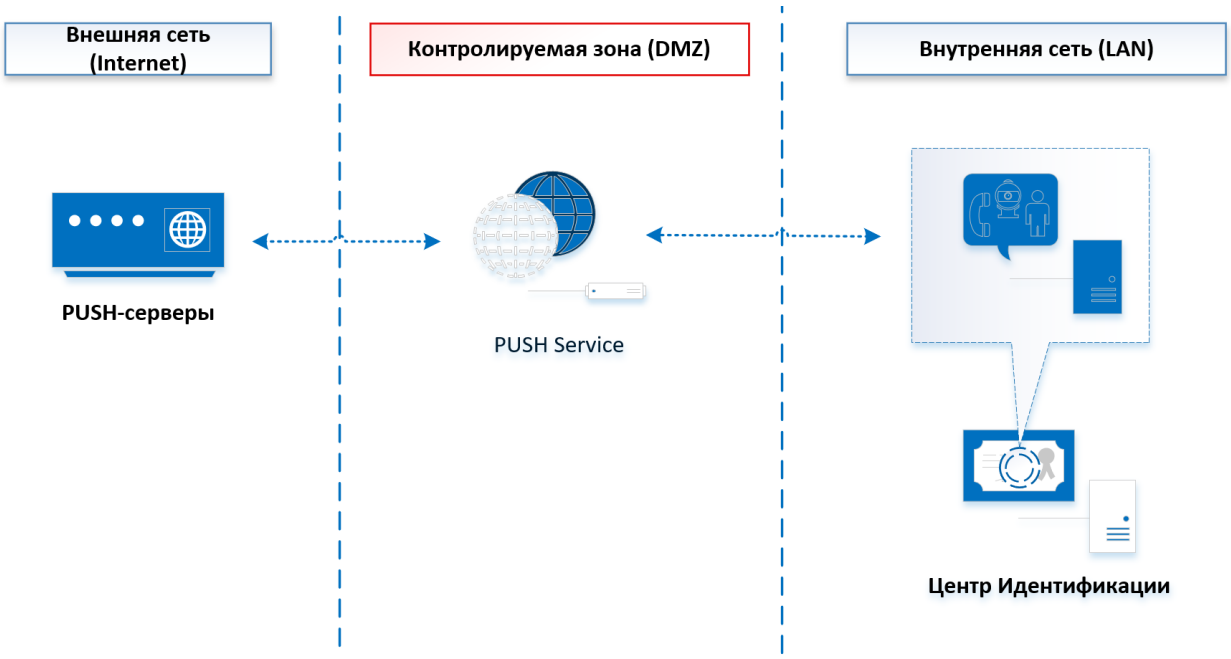

Рис. 4 — Оповещение Пользователей

7.4. Взаимодействие компонентов при использовании DSS Lite

На Рис. 5 изображена схема взаимодействия компонентов КриптоПро DSS при использовании DSS Lite. 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.

Красным цветом отмечены новые взаимодействия, появляющиеся у Пользователя, использующего ключ ЭП, хранимый на его стороне (например, на отчуждаемом носителе, как это описано в 6), и работающего в режиме **REST-сервиса** Lite.

Зеленым цветом отмечены новые взаимодействия (и режим работы Сервиса Подписи), появляющиеся у Пользователя, использующего ключ ЭП, хранимый на его стороне (например, на отчуждаемом носителе, как это описано в 6), и работающего в режиме **веб-интерфейса** Lite.

Синим цветом отмечены взаимодействия компонентов КриптоПро DSS, порядок работы которых не изменяется при условии использования DSS Lite.

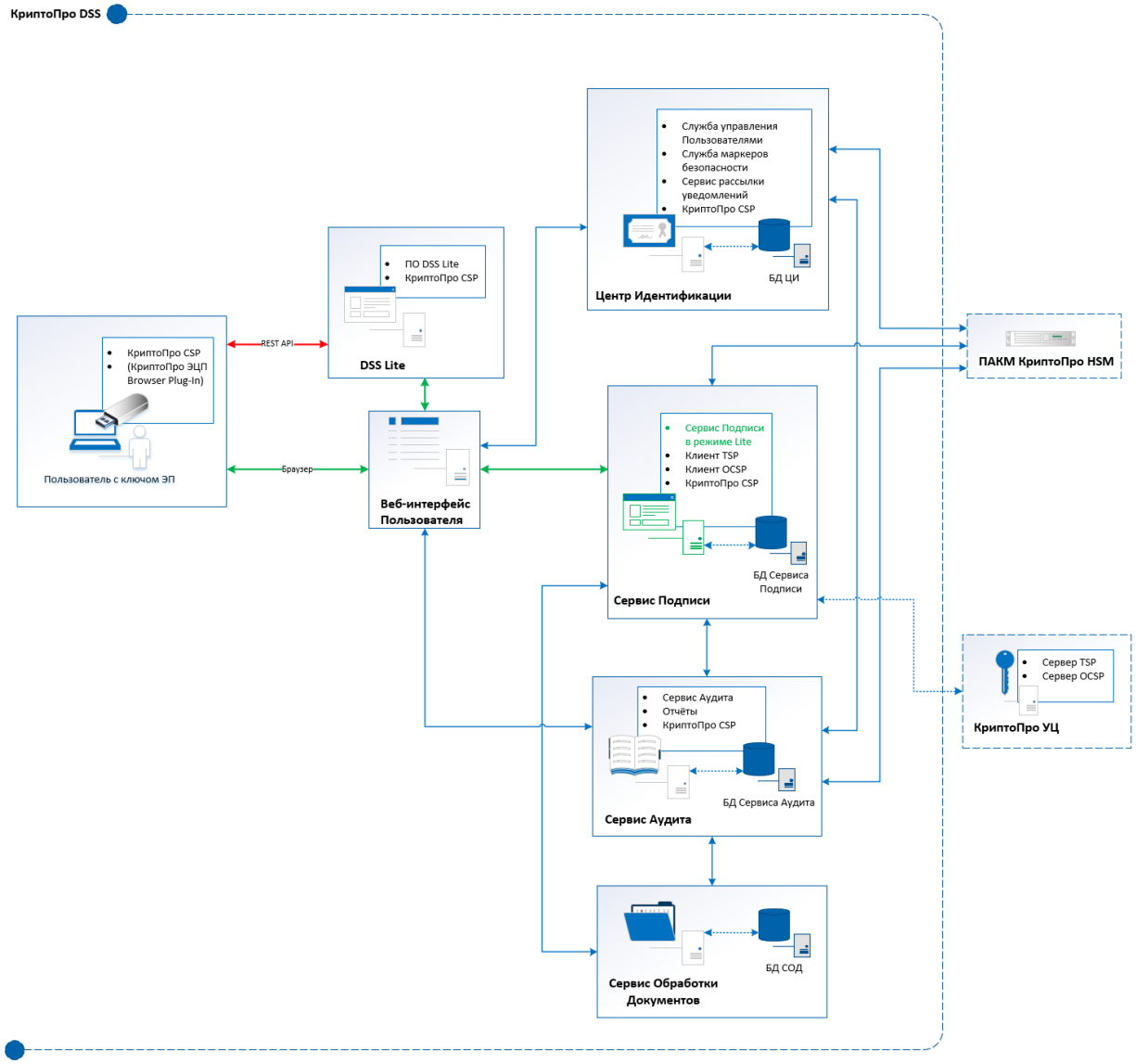

Рис. 5 — Схема взаимодействия компонентов при использовании DSS Lite

7.5. Размещение компонентов КриптоПро DSS

Типовая схема размещения компонентов КриптоПро DSS представлена на Рис. 6. 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.

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. 9).

В случае использования БД, размещенных на удаленных от сервисов КриптоПро DSS серверах, необходимо использовать на данных серверах режим замкнутой программной среды (ЗПС) Astra Linux, электронные замки. Соединение с серверами, на которых расположены серверные компоненты КриптоПро DSS, должно происходить по протоколу TLS с односторонней аутентификацией.

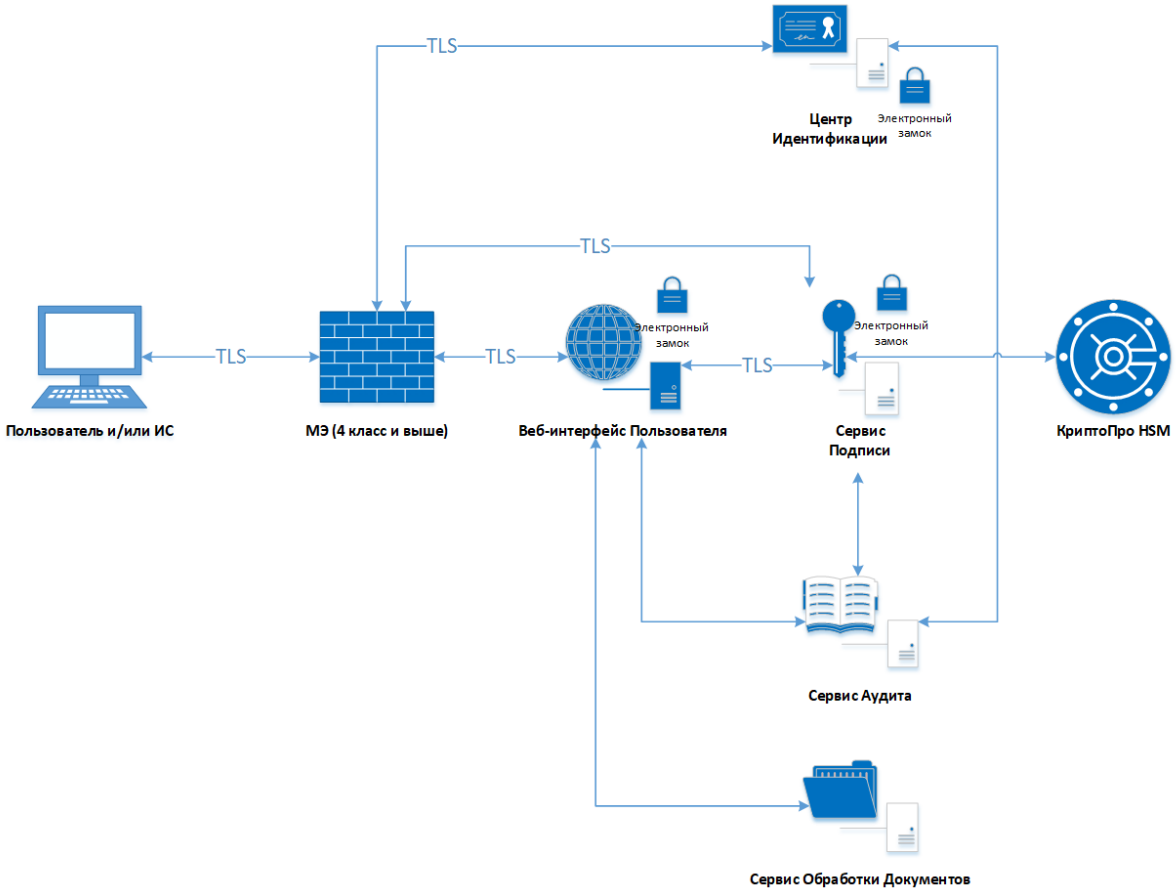

Рис. 6 — Схема размещения компонентов КриптоПро DSS

При использовании различных методов аутентификации (см. 4) требуется настроить взаимодействие КриптоПро DSS с внешними системами для доставки сообщений Пользователям. На Рис. 7 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 взаимодействия с мобильным приложением на базе 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. подраздел 4.5) и/или для оповещения Пользователей о действиях, совершенных с их учетными записями и ключами аутентификации. Также ЦИ взаимодействует с PUSH-серверами посредством Сервиса PUSH-уведомлений (PUSH Service) для оповещения Пользователей в мобильном приложении на базе DSS SDK о необходимости подтверждения операций (см. подразделы 4.3–4.4).

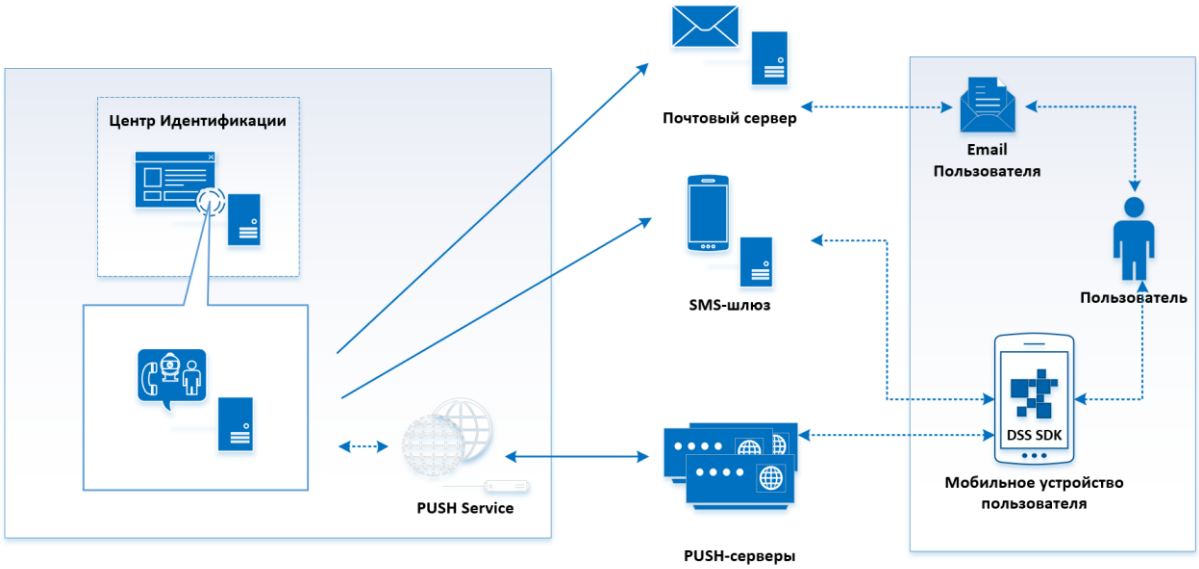

Рис. 7 — Доставка сообщений Пользователям

7.6. Описание процессов в КриптоПро DSS

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

- Регистрация Пользователя и создание запроса на сертификат (см. пункт 7.6.1);
- Подпись документа (см. пункт 7.6.2);
- Проверка подписи (см. пункт 7.6.3);
- Проверка сертификата (см. пункт 7.6.4);
- Шифрование документа (см. пункт 7.6.5);
- Расшифрование документа (см. пункт 7.6.6);
- Аудит событий и формирование отчетов (см. пункт 7.6.7).

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».

7.6.1. Регистрация Пользователя и создание запроса на сертификат

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

В случае, если для выполнения криптографических операций планируется использовать мобильное приложение и/или DSS SDK, Пользователю потребуется привязать свое мобильное устройство к учетной записи. В данном случае описан общий

случай, когда Пользователь предоставляет Оператору необходимую для регистрации информацию (данное действие может включать в себя предварительные действия в мобильном приложении), после чего Оператор регистрирует учетную запись Пользователя и привязывает к ней соответствующее мобильное устройство (при его использовании). Данная операция после подтверждения ее Пользователем позволяет перейти к созданию запроса на сертификат. В случае использования мобильного устройства возможно несколько сценариев его привязки к учетной записи (см. 5).

Сертификат в КриптоПро DSS необходим Пользователю для создания электронной подписи и выполнения других операций. КриптоПро DSS позволяет создавать запрос на сертификат, который впоследствии может быть загружен (дополнительно может быть представлена печатная форма) 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 или в мобильном приложении с DSS SDK в разделе «Сертификаты». В процессе заполнения полей запроса на сертификат необходимо указать 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 и/или мобильное приложение с DSS SDK генерируют запрос на сертификат, который впоследствии может быть установлен Оператором или Пользователем (в том числе в мобильном приложении при наличии соответствующих административных настроек).

Пример последовательности шагов процесса регистрации Пользователя и создания запроса на сертификат представлен на Рис. 8.

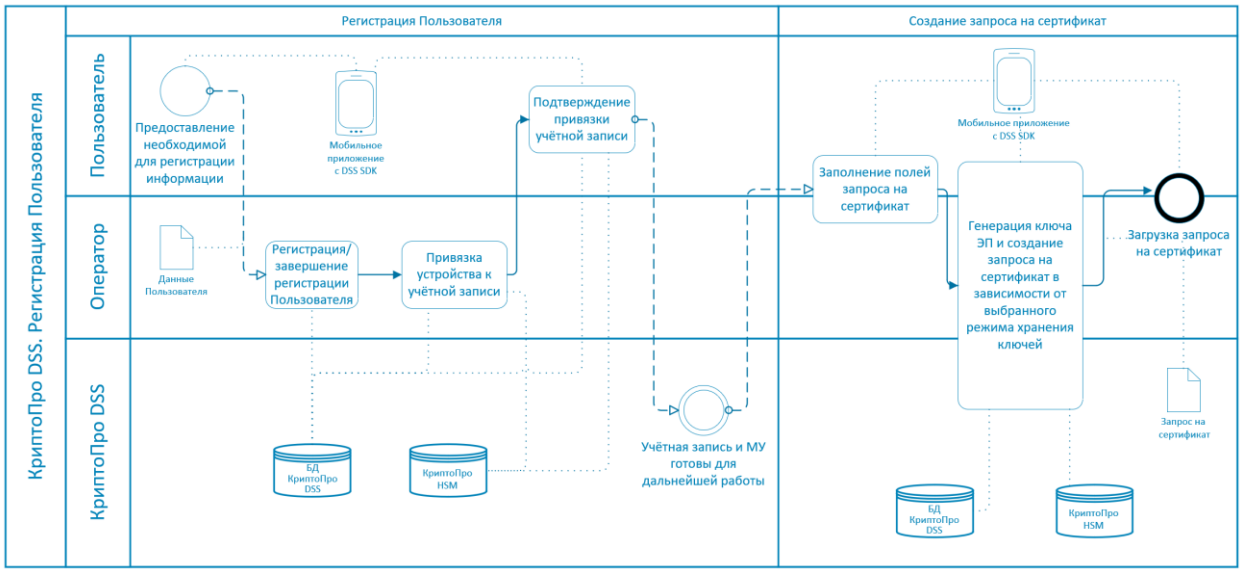

Рис. 8 — Регистрация Пользователя и создание запроса на сертификат

7.6.2. Подпись документа

Подпись документов является одним из основных процессов, обеспечиваемых КриптоПро DSS. При выполнении операции подписи могут быть использованы различные способы аутентификации. В данном пункте приведено описание процесса подписи документа с аутентификацией с помощью мобильного приложения с DSS SDK.

Пользователь инициирует операцию подписи при помощи кнопки «Подписать» на Веб-интерфейсе Пользователя, в мобильном приложении или при помощи программного

интерфейса интегрируемой системы, выбирает нужный сертификат ЭП, подписываемый документ, параметры и формат подписи. Данная информация отправляется в КриптоПро 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 документом и подтверждает операцию. Если операция подтверждена Пользователем, КриптоПро DSS (при участии мобильного приложения, если ключ хранится в нем, на внешнем носителе или в распределенном виде, см. 6) подписывает документ и возвращает его Пользователю в веб-интерфейсе, в мобильном приложении или при помощи интегрируемой системы. В общем виде шаги процесса подписи с подтверждением при помощи мобильного приложения с DSS SDK представлены на Рис. 9.

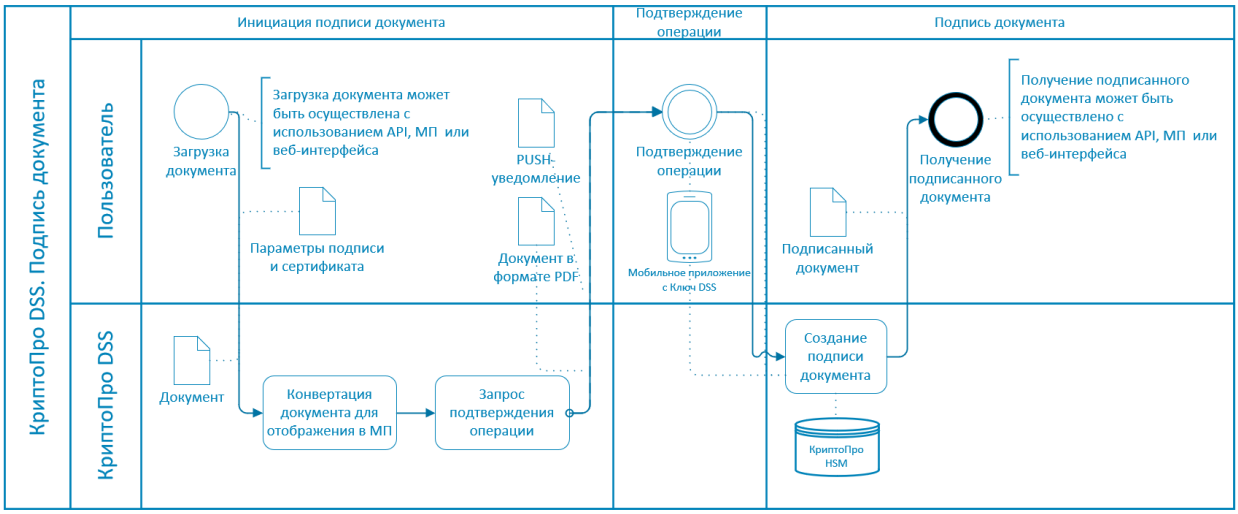

Рис. 9 — Подпись документа

Процесс создания электронной подписи документа при использовании DSS Lite выглядит следующим образом. Пользователь, используя браузер или иное клиентское приложение, осуществляющее взаимодействие с DSS Lite, отправляет в DSS Lite документ, сведения о выбранном им формате ЭП и свой сертификат. DSS Lite подготавливает документ к подписи, вычисляет от него хэш-значение и отправляет пользователю. На стороне пользователя происходит формирование электронной подписи полученного хэш-значения (средством ЭП пользователя), после чего хэш-значение, его ЭП и сведения о ней передаются в DSS Lite для завершения процедуры подписания. DSS Lite формирует подписанный документ согласно выбранному формату подписи и возвращает его пользователю.

7.6.3. 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. 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.

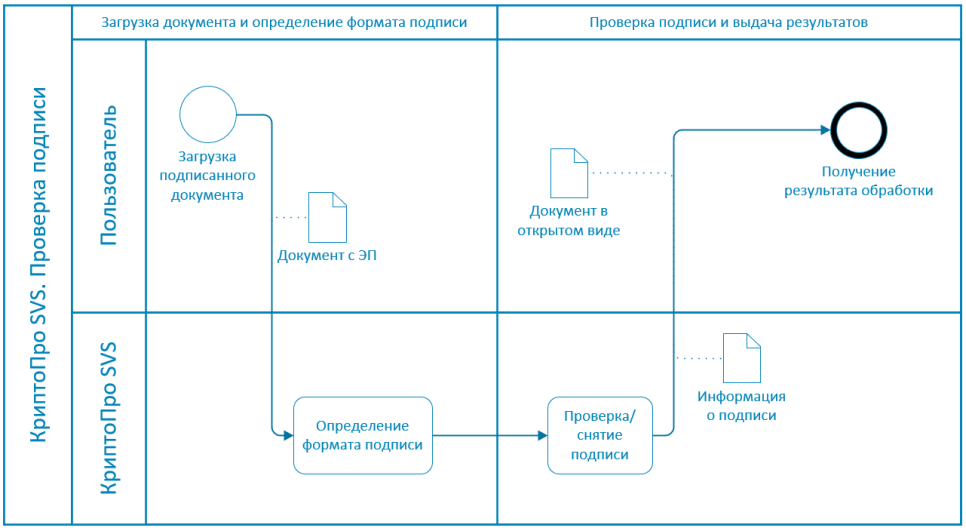

Рис. 10 — Проверка электронной подписи

7.6.4. 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.

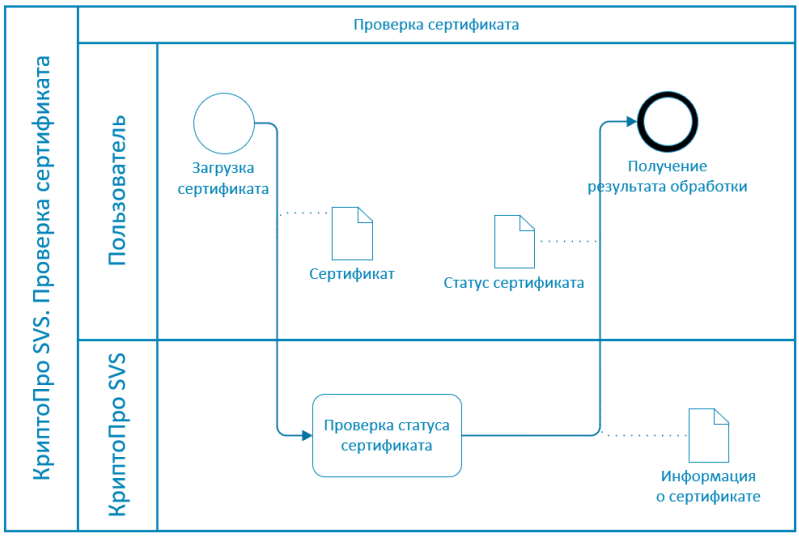

Рис. 11 — Проверка сертификата

7.6.5. Шифрование документа

Шифрование документов является одним из основных процессов, обеспечиваемых 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 REST API (в этом случае используется программный интерфейс КриптоПро DSS).

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.

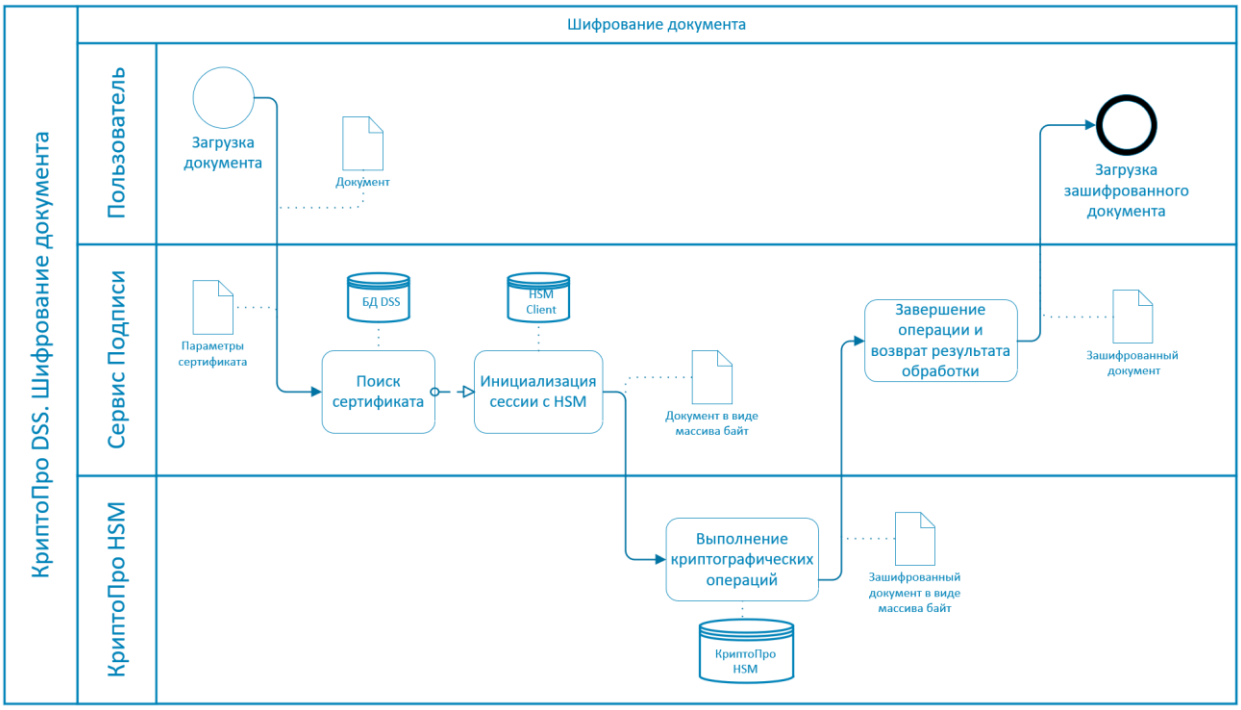

Рис. 12 — Шифрование документа

7.6.6. 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.

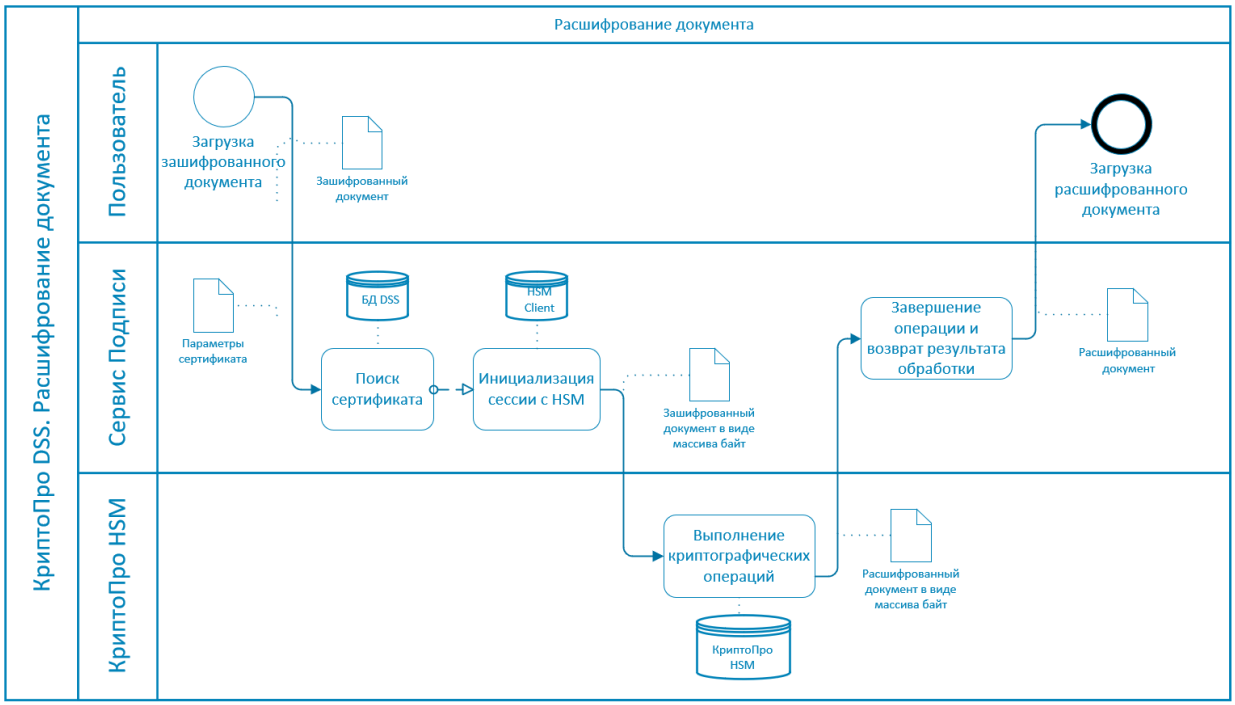

Рис. 13 — Расшифрование документа

7.6.7. 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 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. 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, поэтому ко всем его компонентам предъявляются одинаковые системные требования.

Для функционирования серверной части в *nix-системах:

- ОС Astra Linux Special Edition версии 1.7 Смоленск (РУСБ.10015-01);
- СУБД: PostgreSQL 11 и выше, Jatoba 4 Platform V или Pangolin SE 6;
- веб-сервер nginx 1.18.0 и выше.

Для функционирования серверной части в ОС Windows:

- Microsoft Windows Server 2016/2019/2022 (x64);
- SQL Server 2016/2017/2019/2022.

Для функционирования пользовательского АРМ:

- операционная система, поддерживаемая СКЗИ КриптоПро CSP/JCP;
- СКЗИ из состава компонентов выбранного исполнения;
- веб-браузер с установленным плагином КриптоПро Browser plug-in (Chromium Gost, Яндекс.Браузер, Opera, Firefox) (опционально).

Для функционирования пользовательского мобильного устройства (для групп исполнений 1 и 2, см. подраздел 2.4):

- мобильная ОС iOS версии не ниже 13 (при использовании DSS SDK) либо 15 (при использовании мобильных приложений), Android версии не ниже 8;
- мобильное приложение на базе SDK (DSS Client, myDSS 3.0, и другие приложения со встроенным SDK).

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

9. Интеграция с внешними ИС

КриптоПро DSS предоставляет программные интерфейсы автоматизации, которые позволяют выполнить интеграцию электронной подписи и шифрования в существующие бизнес-процессы и системы. На Рис. 14 представлена типовая схема использования КриптоПро DSS с интегрируемой ИС (например, ДБО).

В приведенных примерах иллюстрируется подпись документа в КриптоПро DSS, инициированная ИС, с подтверждением операции в мобильном приложении. О других способах аутентификации см. раздел 4.

9.1. Использование REST

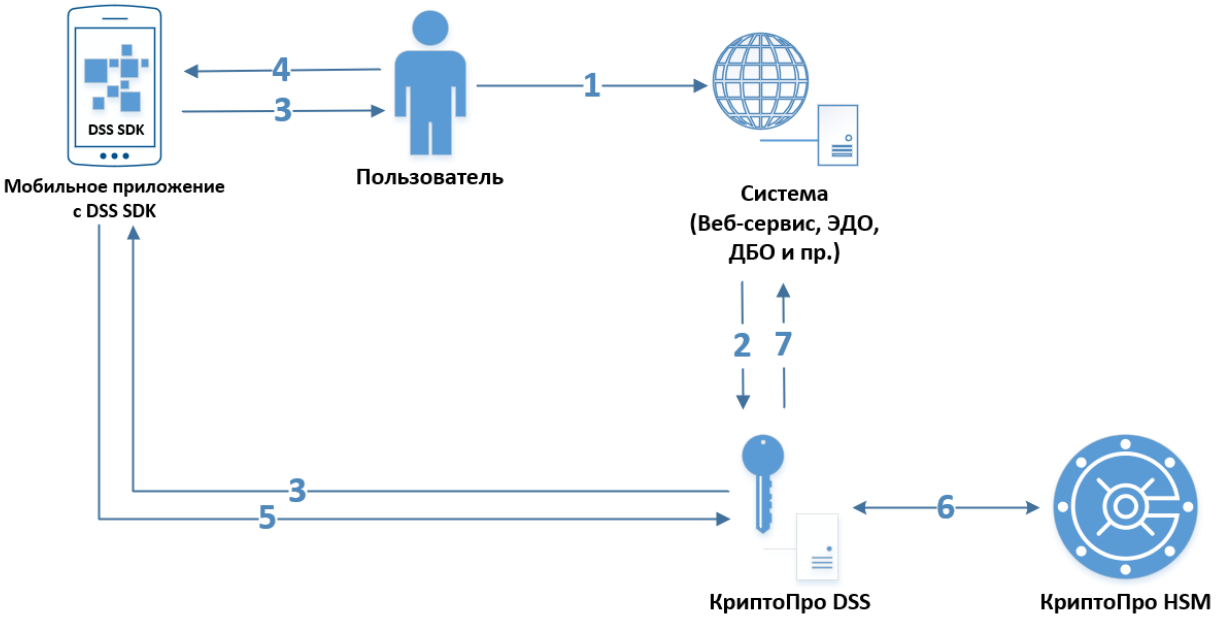

Рис. 14 — Взаимодействие с КриптоПро DSS с использованием REST

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 в мобильное приложение с DSS SDK на устройстве пользователя сведения об операции и подписываемый документ.
4. Пользователь просматривает документ, убеждается, что хочет выполнить операцию с данным документом, и подтверждает операцию.
5. Мобильное приложение передает информацию о волеизъявлении пользователя в КриптоПро DSS (см. подробнее подраздел 4.4).
6. КриптоПро DSS, используя документированные функции ПАКМ «КриптоПро HSM», отправляет запрос на подписание документа с

использованием закрытого ключа Пользователя и получает подписанный документ.

7. КриптоПро DSS 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-наблюдатель;
- Оператор Аудита;
- Администратор безопасности (организационная роль, далее — Администратор);
- Системный Администратор (организационная роль).

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

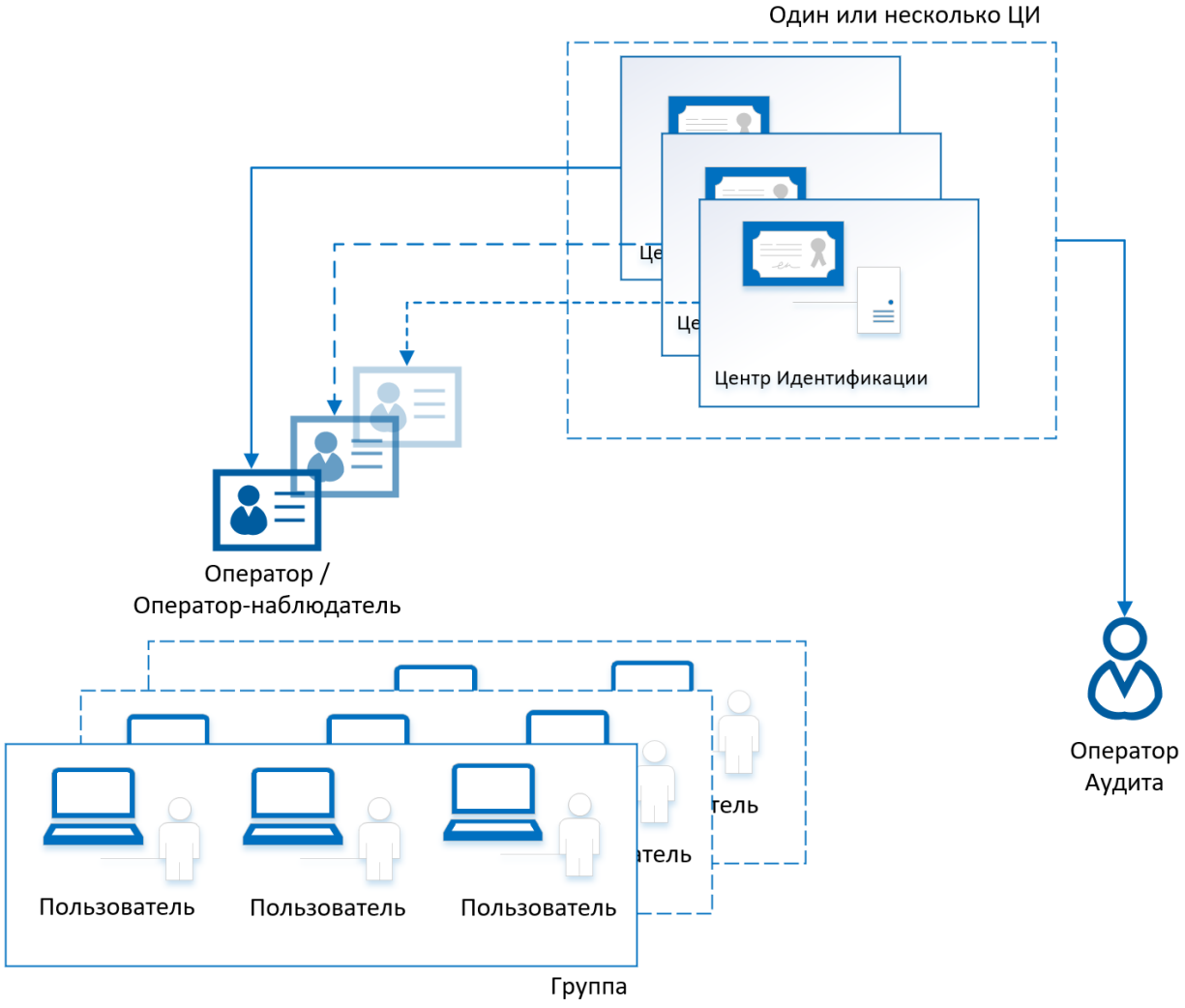

Рис. 15 — Логическая структура ролей в КриптоПро DSS

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

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. 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. 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.

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 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.

Роль **Оператора-наблюдателя** позволяет исключительно просматривать информацию о Пользователях, поступающую с Сервиса Подписи и Центра Идентификации.

Оператор-наблюдатель может просматривать следующее:

- Список Пользователей;

- Настройки аутентификации Пользователей;
- Просмотр средств аутентификации, зарегистрированных в ЦИ;
- Просмотр сертификатов и/или запросов на сертификаты Пользователей;
- Просмотр и печать событий аудита назначенных Оператору групп.

Роль Оператора-наблюдателя может использоваться также прикладными системами, которым необходим доступ к информации, указанной выше. Доступ возможен как через программный интерфейс, так и через Веб-интерфейс Пользователя — в этом случае у Оператора-наблюдателя будут отсутствовать некоторые элементы, отвечающие за изменение настроек аутентификации, сертификатов и проч.

В целях обеспечения безопасности Центр Идентификации не имеет предустановленных встроенных учетных записей Операторов всех типов. Поэтому создание учетной записи Оператора возможно только локально на сервере, где установлен Центр Идентификации КриптоПро DSS. Роль Оператора назначается Администратором путем выдачи Оператору соответствующего сертификата с клиентской аутентификацией.

Администратор (безопасности) 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 и организационно необходима 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 при использовании Группы исполнений 1 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 CAdES (CMS Advanced Electronic Signature)

КриптоПро DSS позволяет формировать различные форматы усовершенствованной подписи (CAdES), форматы которой основаны на стандартах ETSI TS 101 733 и ETSI EN 319 122-1.

Усовершенствованная подпись позволяет получить следующие преимущества:

- обеспечить доказательное подтверждение соответствия подписи тому сертификату, который используется для ее проверки;
- обеспечить доказательное подтверждение момента создания подписи;
- обеспечить доказательное подтверждение действительности соответствующих сертификатов на момент создания ЭП;
- обеспечить отсутствие необходимости сетевых обращений при проверке ЭП;
- обеспечить долговременное (архивное) хранение электронных документов.

Использование форматов подписи CAdES позволяет сформировать подписанное сообщение, являющееся полностью самодостаточным для выполнения проверки его подписи. С этой целью в сообщение в зависимости от выбранного формата подписи может быть помещена информация об исходном документе, алгоритмах хэширования и подписи, параметрах данных алгоритмов, времени подписи, сертификате подписи, а также цепочки сертификатов.

В зависимости от наличия исходного документа в самом сообщении, выделяют два типа 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.

КриптоПро DSS позволяет создавать усовершенствованную электронную подпись CAdES следующих форматов.

- **CAdES-BES/CAdES-B-B (Basic Signature).**

Электронная подпись формата CAdES-BES представляет собой расширенную версию CMS-сообщения типа «подписанные данные», описанного в документе Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами».

Формат подписи CAdES-BES требует наличия в подписанном сообщении подписанных и неподписанных атрибутов, некоторые из которых являются обязательными. Например, в подписанном сообщении обязательно должен присутствовать подписанный атрибут signing-certificate-v2. Данный атрибут идентифицирует сертификат подписывающего и позволяет дополнить подпись до других форматов.

Также в подписанное сообщение может быть добавлен подписанный атрибут signing-time, представляющий собой отметку о времени создания подписи.

Остальные типы электронной подписи формата CAdES, доступные в КриптоПро DSS, являются усовершенствованным вариантами CAdES-BES.

- **CAdES-T/CAdES-B-T (Signature with Time).**

Электронная подпись формата CAdES-T представляет собой усовершенствованную подпись с доверенным временем. Для этого к подписи формата CAdES-BES добавляется метка доверенного времени (см. ч. 19 ст. 2 закона «Об электронной подписи» от 06.04.2011 № 63-ФЗ), представляющая собой штамп времени, выданный службой штампов времени. Служба штампов времени ставит штампы времени на данные для гарантии того, что эти данные существовали до определенного момента времени.

Использование подписи формата CAdES-T подходит для случаев, когда требуется, например, проверить, что электронная подпись сообщения была создана до того момента, когда соответствующий сертификат был отозван, что позволяет использовать отозванный сертификат ключа проверки подписи для проверки подписей, созданных до момента отзыва.

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

Электронная подпись формата CAdES-X Long Type 1 представляет собой усовершенствованную подпись, позволяющую помимо подтверждения момента создания ЭП обеспечить доказательное подтверждение действительности сертификата ключа проверки подписи на момент создания ЭП. Подтверждение действительности сертификата ключа проверки подписи на момент создания ЭП может быть достигнуто при помощи протокола получения актуального статуса сертификата (OCSP).

Дополнительно могут быть собраны цепочки каждого из используемых сертификатов для создания полной доказательной базы, связанной с установлением момента подписи и статуса сертификата на момент подписи.

Перечисленные доказательства содержатся непосредственно внутри атрибутов ЭП, что позволяет минимизировать количество сетевых обращений для проверки подписи данного формата.

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

11.2.1. Подпись XMLDSig

Формат электронной подписи XMLDSig представляет собой подпись XML-документов, создаваемую в соответствии с Р 1323565.1.033–2020 «Информационная технология. Криптографическая защита информации. Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML».

Отличительной особенностью данного формата подписи является то, что электронная подпись представляет собой XML-элемент, помещаемый внутрь подписываемого документа или являющийся самостоятельным XML-документом, что позволяет обрабатывать XML-документы таким же образом, как и XML-документы без подписи.

В КриптоПро DSS реализована поддержка трех типов XML-подписи:

- Вложенная XML-подпись (enveloped). XML-подпись находится внутри подписываемого элемента.
- Присоединенная XML-подпись (enveloping). Подписываемый элемент находится внутри структуры XML-подписи.

- XML-подпись по шаблону. Создается подпись документа, содержащего шаблон подписи с незаполненными значениями подписи. В процессе подписи данные значения вычисляются и заносятся в структуру подписи.

11.2.2. Подпись XAdES

Формат электронной подписи XAdES представляет собой подпись XML-документов, создаваемую в соответствии со стандартами ETSI EN 319 132. КриптоПро DSS позволяет создавать усовершенствованную электронную подпись XAdES следующих форматов.

- базовая подпись XAdES-BES (XAdES-B-B);
- подпись с указанием времени создания XAdES-T (XAdES-B-T).

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

Данный формат предназначен для вычисления электронной подписи для некоторых данных, используя алгоритмы, определенные в ГОСТ Р 34.10–2012 и ГОСТ Р 34.11-2012. Для обеспечения возможности использования и долговременного (архивного) хранения подписанных документов КриптоПро DSS поддерживает дополнительно создание электронной подписи документов с использованием алгоритмов, определенных в ГОСТ Р 34.10–2001 и ГОСТ Р 34.11–94.

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, описанной в ГОСТ Р 34.11-2012 или ГОСТ Р 34.11-94.

11.4. Подпись PDF-документов

Данный формат подписи позволяет формировать электронную подпись для обеспечения юридической значимости электронных документов формата PDF.

В КриптоПро DSS реализованы следующие виды подписи данного формата:

- Подпись документа PDF с использованием формата CAdES-BES. В документ будет добавлена подпись в формате CAdES-BES. 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 формата CAdES-XLT1. 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.
- Подпись документа PDF в соответствии со стандартами ETSI EN 319 142 (PAdES). Поддерживаются форматы подписи PAdES-B-B, PAdES-B-T и PAdES с включением доказательств проверки.

12. Поддерживаемый формат шифрования документов

КриптоПро DSS поддерживает следующие форматы шифрования документов.

- CMS-сообщение типа «конверт данных», описанного в документе Р 1323565.1.025–2019 «Информационная технология. Криптографическая защита информации. Форматы сообщений, защищенных криптографическими методами».

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.

- Формат шифрования XML-документов XML Encrypted, описанный в Рекомендациях W3C XML Encryption Syntax and Processing Version 1.1.

В случае использования шифрования XML Encrypted доступна передача ключевой информации только при помощи X.509-сертификата, как это описано в Р 1323565.1.033–2020 и Рекомендациях W3C XML Encryption Syntax and Processing Version 1.1.

13. Поддерживаемые форматы документов для отображения при подтверждении операций

КриптоПро DSS предоставляет возможность отображения документов перед созданием подписи на Веб-интерфейсе Пользователя и при подтверждении операции подписи в мобильном приложении на базе DSS SDK.

Отображение документов перед подтверждением операции могут выполнять следующие компоненты КриптоПро DSS:

- Сервис Обработки Документов — отображение в мобильном приложении и на Веб-интерфейсе Пользователя;
- DSS SDK — отображение документа в мобильном приложении собственными средствами (в том числе встроенными средствами ОС). Использование данного способа отображения обязательно для группы исполнений 1.

КриптоПро DSS поддерживает отображение документов следующих форматов: PDF, XML, ODT, а также текстовых документов. Возможно также отображение документов форматов DOC, DOT, DOCM, DOTM, DOCX, DOTX, FlatOpc, FlatOpcMacroEnabled, FlatOpcTemplate, FlatOpcTemplateMacroEnabled, OTT, OOXML, WordML, RTF, HTML, XHTML, MHTML.

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