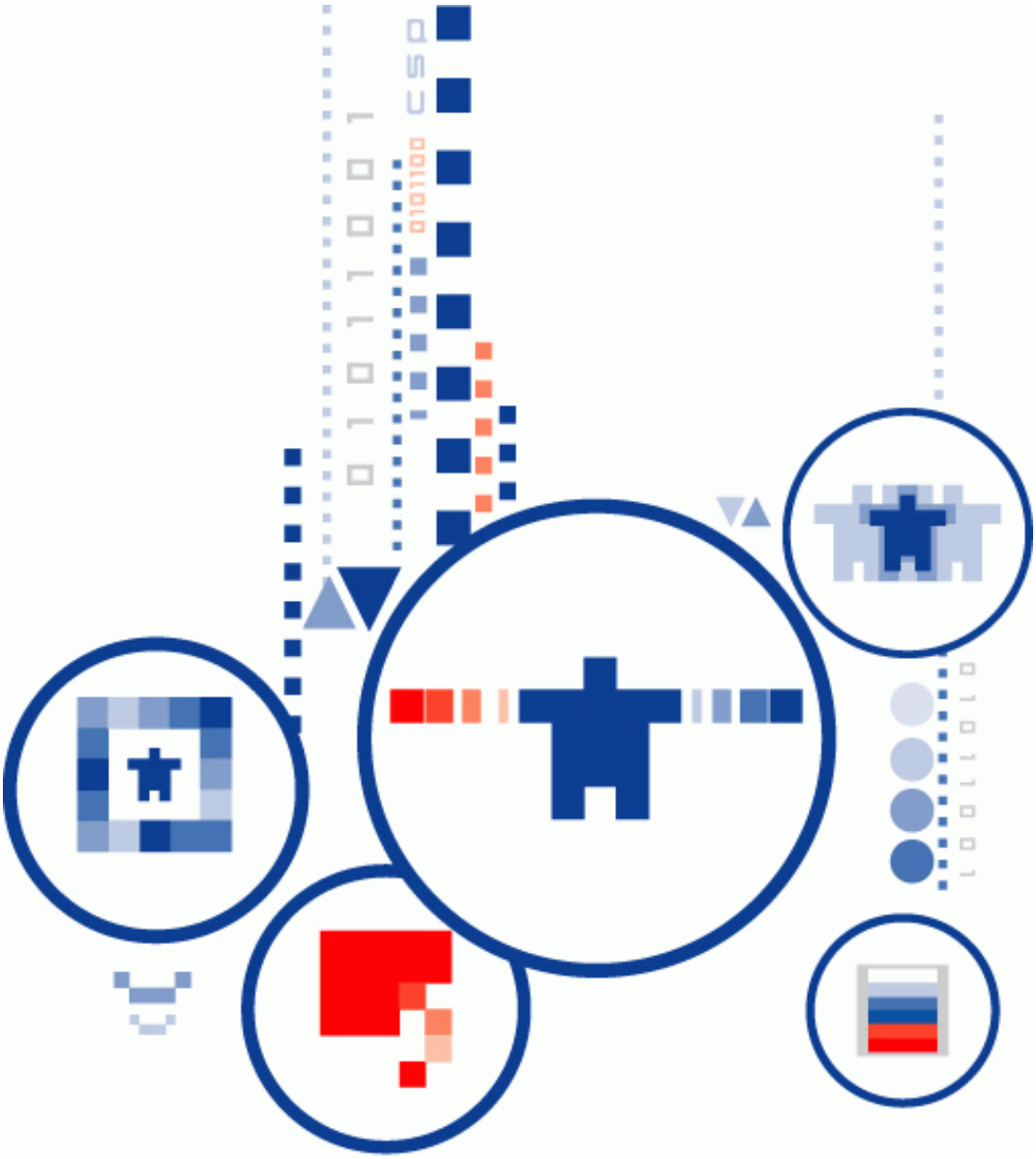

Программно-аппаратный комплекс

«КриптоПро DSS»

С ПОДДЕРЖКОЙ ASTRA LINUX (МОДИФИКАЦИЯ CLOUD)

Общее описание

СОДЕРЖАНИЕ

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

CAdES	—	Расширенная версия стандарта электронной подписи CMS (CMS Advanced Electronic Signatures)
CRL	—	Список отозванных 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)
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
ПК	—	Программный 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
ФКН	—	Функциональный ключевой носитель
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 ключа проверки электронной подписи.
Ключ электронной подписи	—	уникальная последовательность символов, предназначенная для создания электронной подписи
Закрытый ключ	—	ключ из ключевой пары субъекта, известный только данному субъекту.
Ключ проверки электронной подписи	—	уникальная последовательность символов, однозначно связанная с ключом электронной подписи и предназначенная для проверки (подлинности) электронной подписи.
Открытый ключ	—	общеизвестный ключ из ключевой пары субъекта.
Сертификат ключа проверки электронной подписи	—	электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи.
Квалифицированный сертификат ключа проверки электронной подписи	—	сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом (№63-ФЗ от 06.04.2011 г. «Об электронной подписи») и иными принимаемыми в соответствии с ним нормативными правовыми актами, созданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.
Сертификат открытого ключа	—	документ, выданный и подписанный удостоверяющим центром и содержащий открытый ключ и информацию, идентифицирующую субъекта, владеющего соответствующим закрытым ключом.
Мобильное устройство	—	смартфон или планшет, являющийся собственностью Пользователя ПАК «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.
Список отозванных сертификатов	—	перечень досрочно прекративших действие сертификатов открытых ключей, формирование и доступ к которому обеспечивает удостоверяющий центр.
Удостоверяющий центр	—	юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные

		Федеральным законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи».
Учетная запись	—	набор сведений о Пользователе ПАК «КриптоПро DSS», содержащий необходимую для работы с сервисом информацию.
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» (далее — КриптоПро DSS). КриптоПро DSS позволяет создавать электронную подпись и выполнять зашифрование и расшифрование документов различных форматов, что обеспечивает их конфиденциальность, целостность и аутентичность (подлинность и защиту от подделки). Выполнение криптографических операций реализуется при участии ПАКМ «КриптоПро HSM» и СКЗИ «КриптоПро CSP». Проверка электронной подписи и сертификатов возможна при участии КриптоПро SVS.

В данном документе приведено назначение ПАК «КриптоПро DSS» 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».

2. Общие сведения

2.1. Назначение КриптоПро DSS

ПАК «КриптоПро DSS» предназначен для:

- Выполнения операций Пользователей по созданию электронной подписи;
- Выполнения операций Пользователей по шифрованию и расшифрованию документов;
- Выполнения криптографических операций при различных вариантах хранения и защиты ключей Пользователей (в соответствии с выбранным режимом хранения ключей, см. раздел 5).

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. 5);
- формирование запросов на сертификаты;
- создание и проверка ЭП;
- зашифрование и расшифрование документов.

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 6.2);
- получение и отправка документов, с которыми выполняются криптографические операции;
- визуализация (конвертация и отображение) документов для Пользователей перед выполнением операции с данными документами.

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 Пользователя (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);
- ПАКМ «КриптоПро HSM» (см. раздел 3.2.6);
- СКЗИ КриптоПро CSP (требуется установка на сервере для обеспечения работы компонентов).
- Клиентские компоненты (см. раздел 3.2.7):
  - КриптоПро CSP/JCP;
  - КриптоПро TSP Client (компонент из состава СКЗИ «КриптоПро CSP», используется опционально);
  - КриптоПро OCSP Client (компонент из состава СКЗИ «КриптоПро CSP», используется опционально).

Веб-интерфейс Пользователя может быть заменен другим графическим или программным интерфейсом, реализуемым с использованием СКЗИ «КриптоПро CSP»/СКЗИ «КриптоПро JCP» сторонней информационной системой, с которой интегрируется КриптоПро DSS. КриптоПро CSP (для сервера), TSP Client, OCSP Client и HSM Client входят в комплект поставки. ПАКМ «КриптоПро HSM» поставляется отдельно.

3.2. Описание компонентов КриптоПро DSS

3.2.1. Центр Идентификации

Компонент Центр Идентификации предназначен для регистрации, 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 (в том числе привилегированных — Операторов, см. подробнее раздел 8);
- ведение реестра зарегистрированных Пользователей
- удаление Пользователей;

- аутентификация Пользователей;
- 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 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).

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 Сервис Подписи предназначен для управления сертификатами Пользователей и выполнения криптографических операций.

К функциям Сервиса Подписи относятся:

- создание электронной подписи документов различных форматов (см. раздел 9);
- шифрование и расшифрование документов;
- 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 5);
- 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 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 инициируют вызовы REST API других компонентов КриптоПро DSS и обрабатываются их серверными программными модулями.

Для установки TLS-соединения при подключении Оператора или Пользователя со своего АРМ к Веб-интерфейсу Пользователя должен использоваться поддерживаемый СКЗИ «КриптоПро CSP» веб-браузер.

В своем личном кабинете на Веб-интерфейсе Пользователя Пользователь при наличии у него соответствующих прав доступа может изменять информацию профиля и настройки аутентификации. Пользователям и Операторам доступен просмотр журнала операций, совершенных ими 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 9, о форматах шифрования — раздел 10. 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 8.

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 получает события, подлежащие аудиту, с других компонентов КриптоПро DSS (в зависимости от настроек сбора событий) и записывает эти события в БД. С помощью Веб-интерфейса 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 Пользователю перед выполнением операции с ним;
- 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 11.

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 5).

ПАКМ «КриптоПро HSM» является необходимым элементом архитектуры КриптоПро DSS и должен устанавливаться в соответствии с процедурой, описанной в документе «ЖТЯИ.00096-03 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 (ГОСТ 34.10–2018).
- Проверка электронной подписи в соответствии с ГОСТ Р 34.10–2012 (ГОСТ 34.10–2018) и ГОСТ Р 34.10–2001.
- Вычисление значения хэш-функции в соответствии с ГОСТ Р 34.11–2012 (ГОСТ 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 5).
- Управление учетными записями Пользователей ПАКМ.

3.2.7. 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.

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».

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.

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.

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.

4.3. 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 4.1–4.2.

5. Управление ключами Пользователей

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

- в ПАКМ HSM;
- в БД Сервиса Подписи.

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.

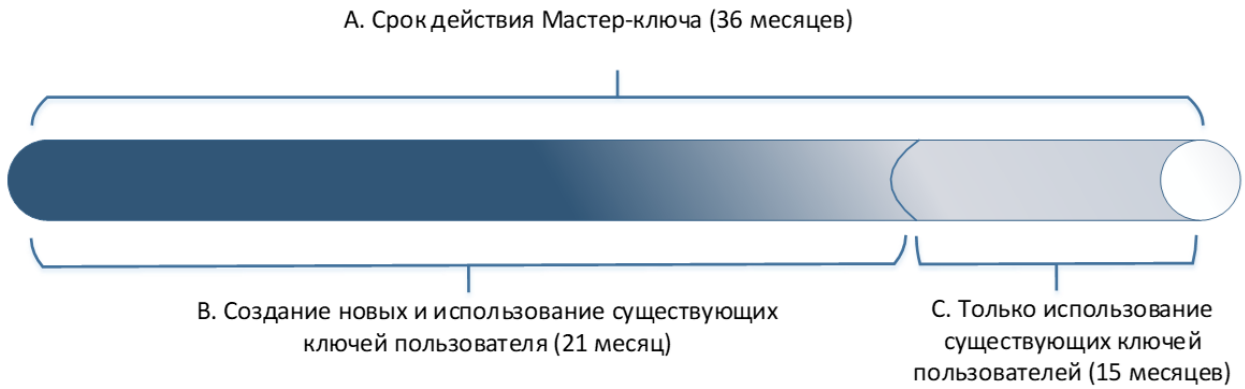

Рис. 1 — Сроки действия Мастер-ключа и ключей Пользователей

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
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.
Срок жизни ключа	36 месяцев.	**Мастер-ключ:** 36 месяцев, 21 месяц пригоден для создания новых ключей. **Ключи Пользователей:** 15 месяцев.

6. Архитектура решения КриптоПро DSS

6.1. 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 посредством вызова программных интерфейсов. Сторонние продукты расположены справа от границы, обозначенной пунктиром.

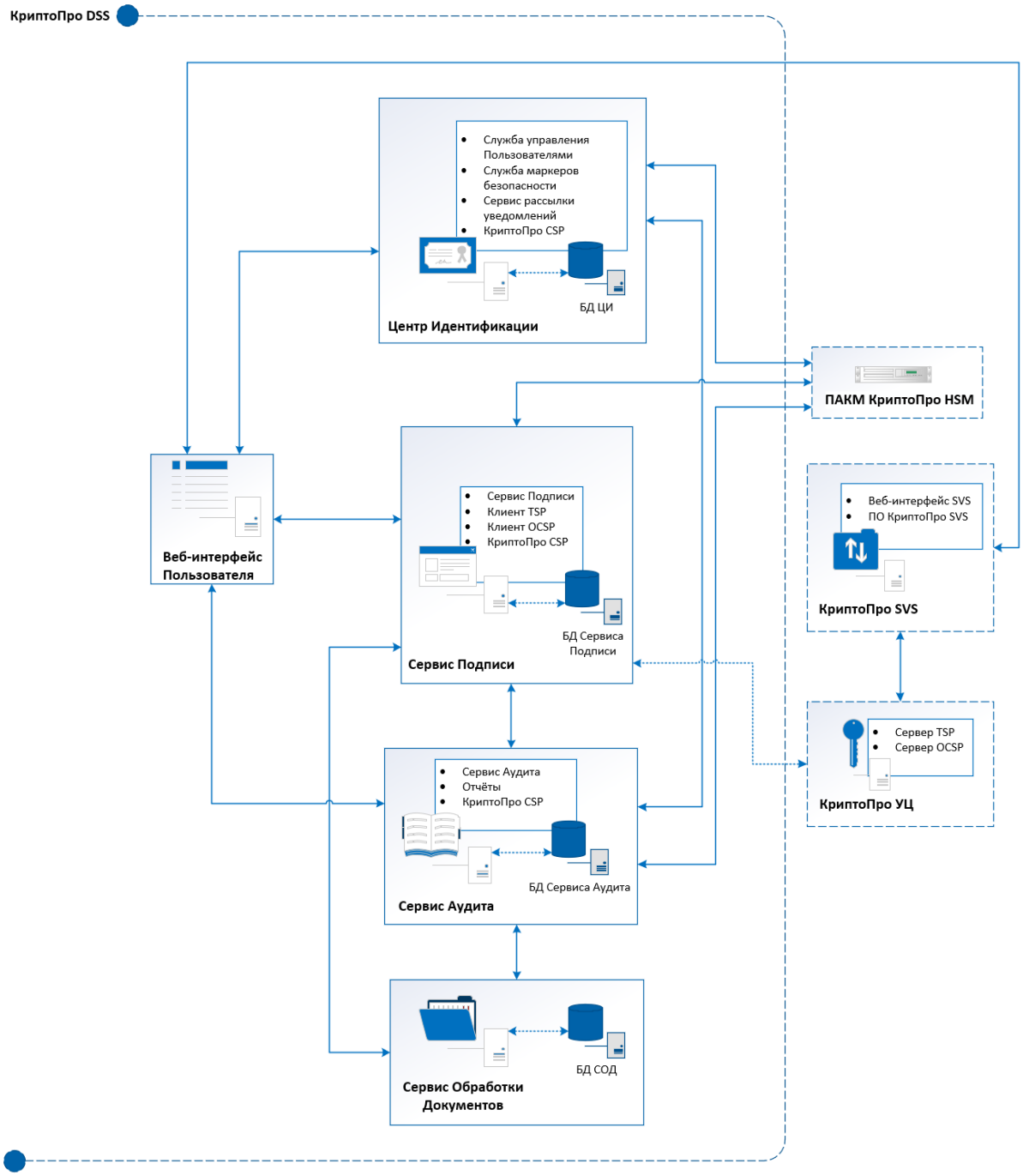

Рис. 2 — Схема взаимодействия компонентов КриптоПро DSS

6.2. Размещение компонентов КриптоПро DSS

Типовая схема размещения компонентов КриптоПро DSS представлена на Рис. 3. 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.

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.

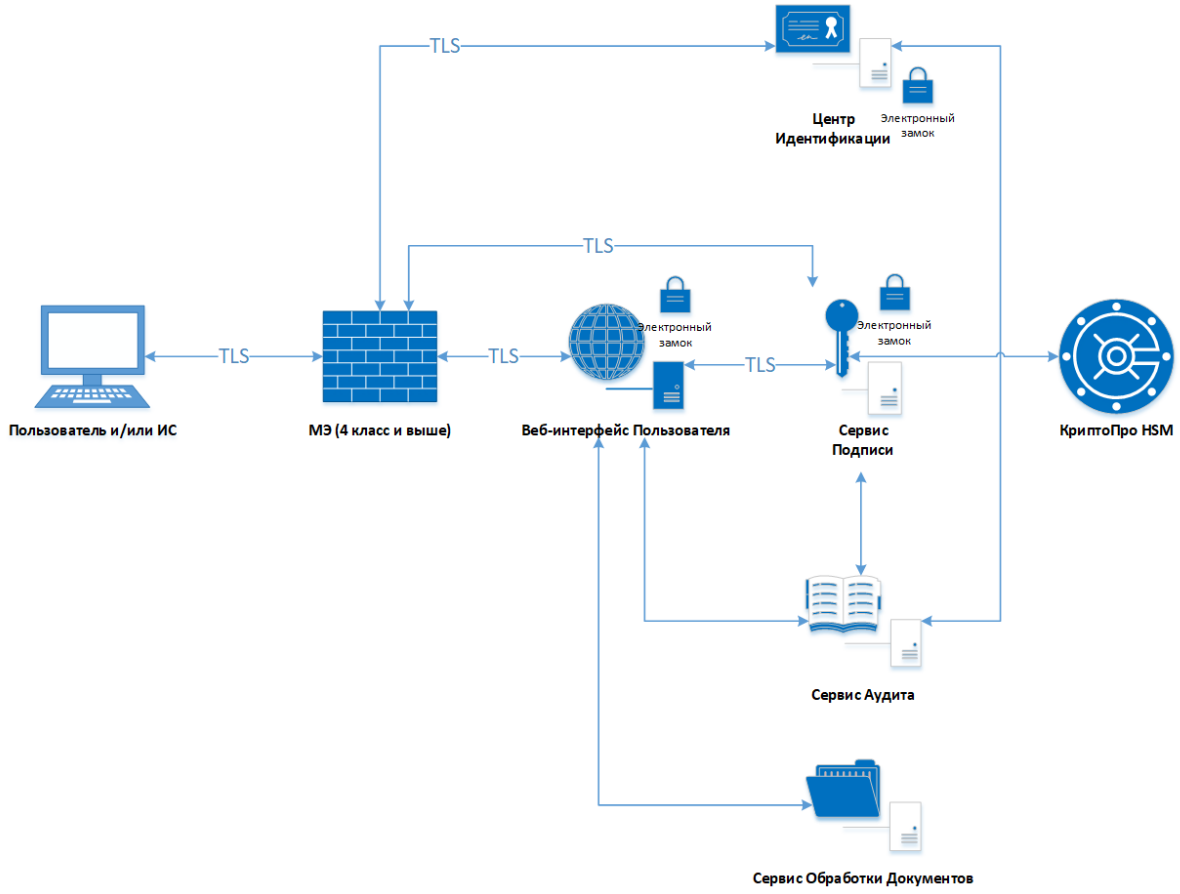

Рис. 3 — Схема размещения компонентов КриптоПро DSS

При использовании различных методов аутентификации (см. 4) требуется настроить взаимодействие КриптоПро DSS с внешними системами для доставки сообщений Пользователям. На Рис. 4 изображены компоненты КриптоПро DSS, взаимодействующие с такими системами. В зависимости от выбранного способа доставки возможна рассылка сообщений по электронной почте или посредством SMS-сообщений.

ЦИ КриптоПро DSS может быть подключен к почтовому серверу или SMS-шлюзу для доставки Пользователям одноразовых паролей, использующихся при вспомогательной аутентификации (см. подраздел 4.3) и/или для оповещения Пользователей о действиях, совершенных с их учетными записями и ключами аутентификации.

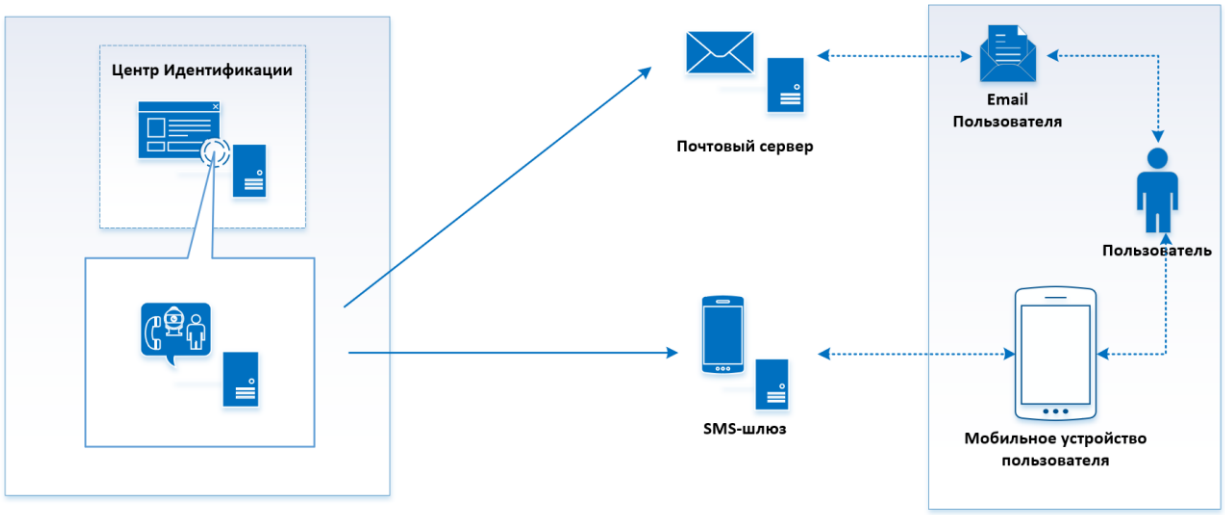

Рис. 4 — Доставка сообщений Пользователям

6.3. 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 6.3.1);
- Подпись документа (см. пункт 6.3.2);
- Проверка подписи (см. пункт 6.3.3);
- Проверка сертификата (см. пункт 6.3.4);
- Шифрование документа (см. пункт 6.3.5);
- Расшифрование документа (см. пункт 6.3.6);
- Аудит событий и формирование отчетов (см. пункт 6.3.7).

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».

6.3.1. 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 предоставляет Оператору необходимую для регистрации информацию, после чего Оператор регистрирует учетную запись Пользователя, заполняет его профиль и настраивает для Пользователя способ аутентификации. Пользователь получает учетные данные для входа от Оператора. По окончании регистрации сведения о профиле Пользователя и данные аутентификации заносятся в БД ЦИ КриптоПро DSS.

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. 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 генерирует запрос на сертификат, который после его получения может быть установлен Оператором или Пользователем (при наличии соответствующих административных настроек).

Пример последовательности шагов процесса регистрации Пользователя и создания запроса на сертификат представлен на Рис. 5.

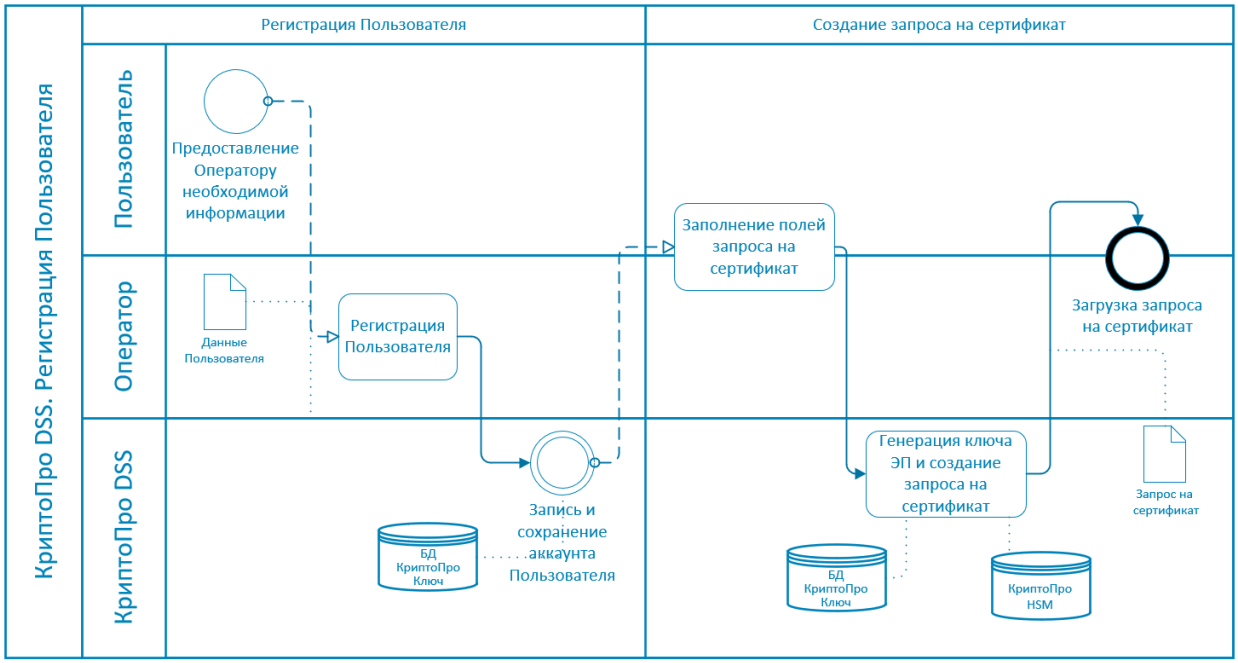

Рис. 5 — Регистрация Пользователя и создание запроса на сертификат

6.3.2. Подпись документа

Подпись документов является одним из основных процессов, обеспечиваемых КриптоПро DSS. Пользователь загружает подписываемый документ и указывает

сертификат и другие параметры подписи. КриптоПро DSS проверяет полученные данные, подготавливает документ для дальнейших действий и отображает его пользователю в Веб-интерфейсе или передает отображаемый документ интегрируемой системе. Пользователь убеждается, что хочет выполнить действия с нужным документом, после чего инициирует операцию подписи при помощи кнопки «Подписать» на Веб-интерфейсе Пользователя или при помощи программного интерфейса интегрируемой системы. КриптоПро DSS подписывает документ и возвращает его Пользователю. В общем виде шаги процесса подписи представлены на Рис. 6.

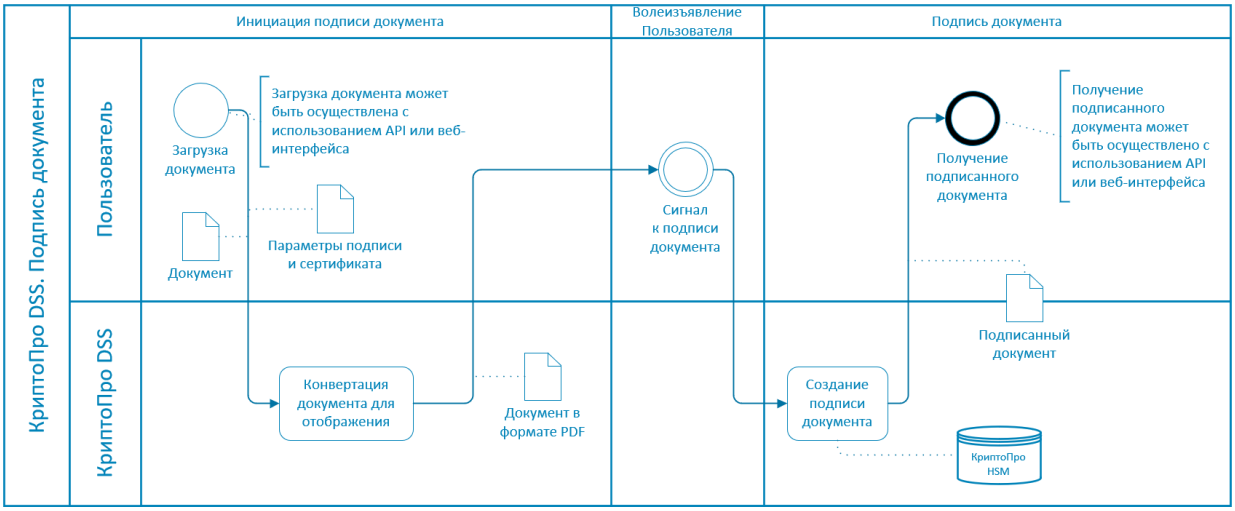

Рис. 6 — Подпись документа

6.3.3. 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). В данном разделе приведен пример описания процесса при использовании веб-интерфейса КриптоПро SVS 2.0, ссылка на который может быть добавлена на Веб-интерфейс Пользователя КриптоПро DSS. Аналогичные действия могут быть выполнены через программный интерфейс КриптоПро SVS 2.0.

Для того чтобы проверить подпись документа, Пользователь в соответствующем разделе веб-интерфейса КриптоПро SVS 2.0 «Проверить подпись» выбирает нужный файл, после чего веб-форма пытается определить формат подписи (см. раздел 9). 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 КриптоПро SVS 2.0 возвращает Пользователю информацию о подписи и вывод об ее действительности/недействительности, информацию о сертификате, на котором она была создана, а также документ в открытом виде, если данная опция была выбрана в начале процесса.

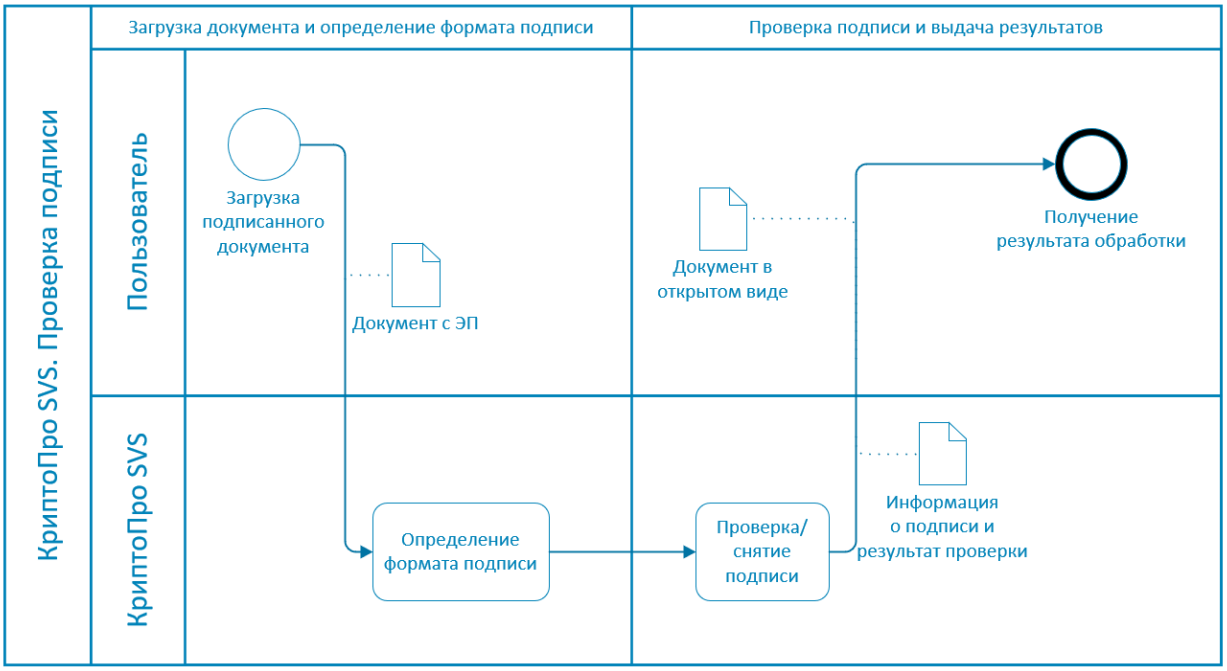

Рис. 7 — Проверка электронной подписи

6.3.4. 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). В данном разделе приведен пример описания процесса при использовании веб-интерфейса КриптоПро SVS 2.0, ссылка на который может быть добавлена на Веб-интерфейс Пользователя КриптоПро DSS. Аналогичные действия могут быть выполнены через программный интерфейс КриптоПро SVS 2.0.

Для того, чтобы проверить статус своего сертификата, Пользователь загружает его на веб-форму в соответствующем разделе «Проверить сертификат». Сертификат отправляется в КриптоПро SVS 2.0, 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.

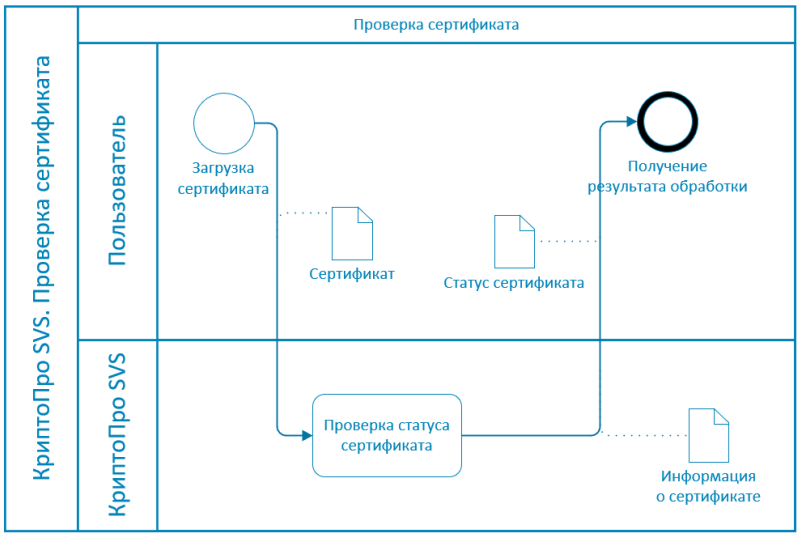

Рис. 8 — Проверка сертификата

6.3.5. 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 используются программные интерфейсы компонентов КриптоПро DSS).

Пользователь инициирует операцию шифрования при помощи кнопки «Зашифровать» на Веб-интерфейсе Пользователя или при помощи программного интерфейса интегрируемой системы, выбирает нужный сертификат ЭП, на открытом ключе которого необходимо произвести зашифрование, и документ, после чего происходит обращение к Сервису Подписи. Сервис Подписи находит выбранный 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.

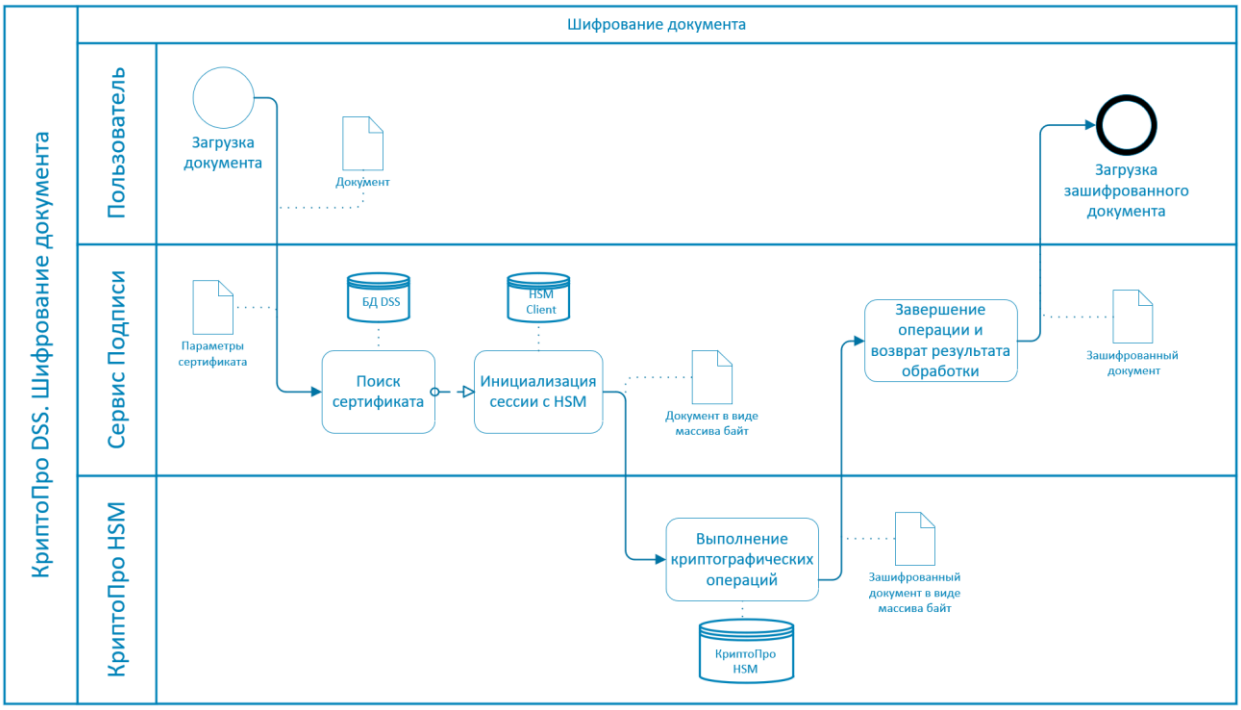

Рис. 9 — Шифрование документа

6.3.6. 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 соответствующих закрытых ключах которых документ можно расшифровать. После того, как Пользователь выбрал сертификат, 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.

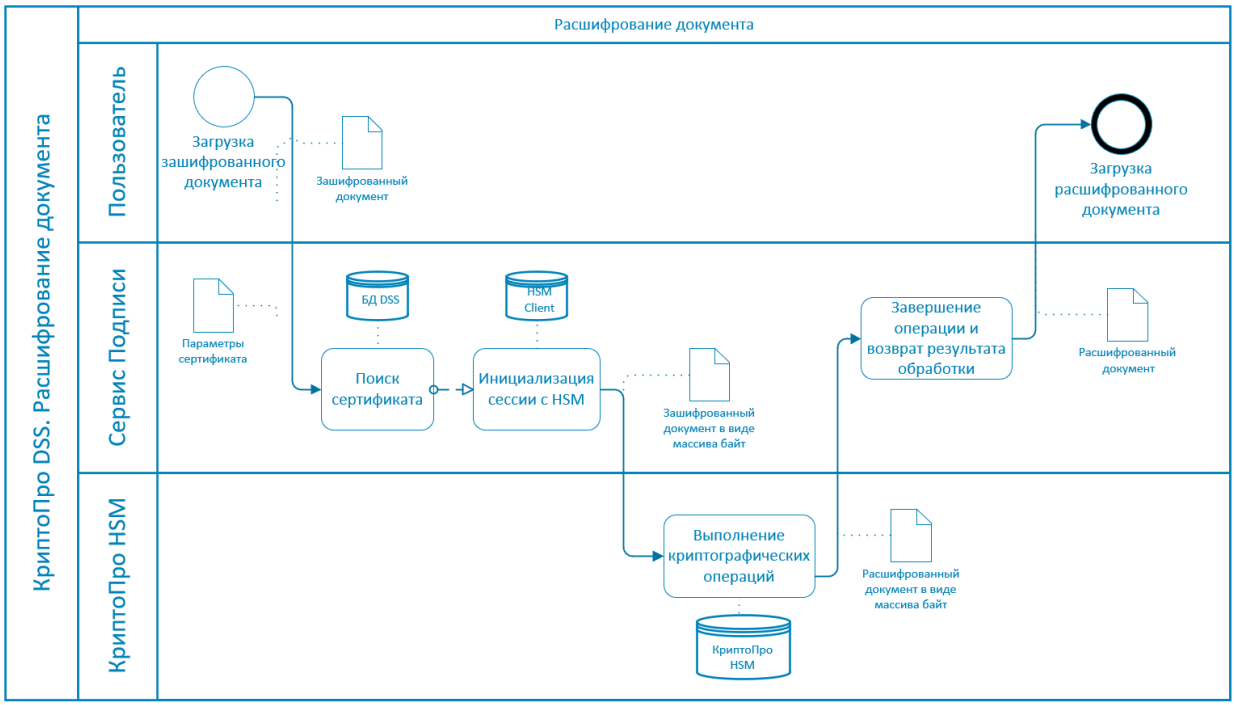

Рис. 10 — Расшифрование документа

6.3.7. 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. Подробнее о ролевой системе см. раздел 8.

7. Системные требования

7.1. 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.

7.2. 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 (РУСБ.10015-01), Ubuntu 20.04 LTS и Ubuntu 22.04 LTS;
- СКЗИ: КриптоПро CSP версии 5.0 и выше или JCP версии 2.0 и выше;
- СУБД: PostgreSQL 11 и выше, Jatoba 4 Platform V или Pangolin SE 6;
- веб-сервер: nginx 1.18.0 и выше.

Для функционирования серверной части в ОС Windows:

- ОС: Microsoft Windows Server 2016/2019/2022/2025 (x64);
- СКЗИ: КриптоПро CSP версии 5.0 и выше или JCP версии 2.0 и выше;
- СУБД: SQL Server 2016/2017/2019/2022/2025;
- веб-сервер: IIS, соответствующий используемой ОС.

Для функционирования пользовательского АРМ:

- операционная система, поддерживаемая СКЗИ КриптоПро CSP/JCP;
- СКЗИ КриптоПро CSP версии 5.0 и выше или JCP версии 2.0 и выше.

8. 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. 11.

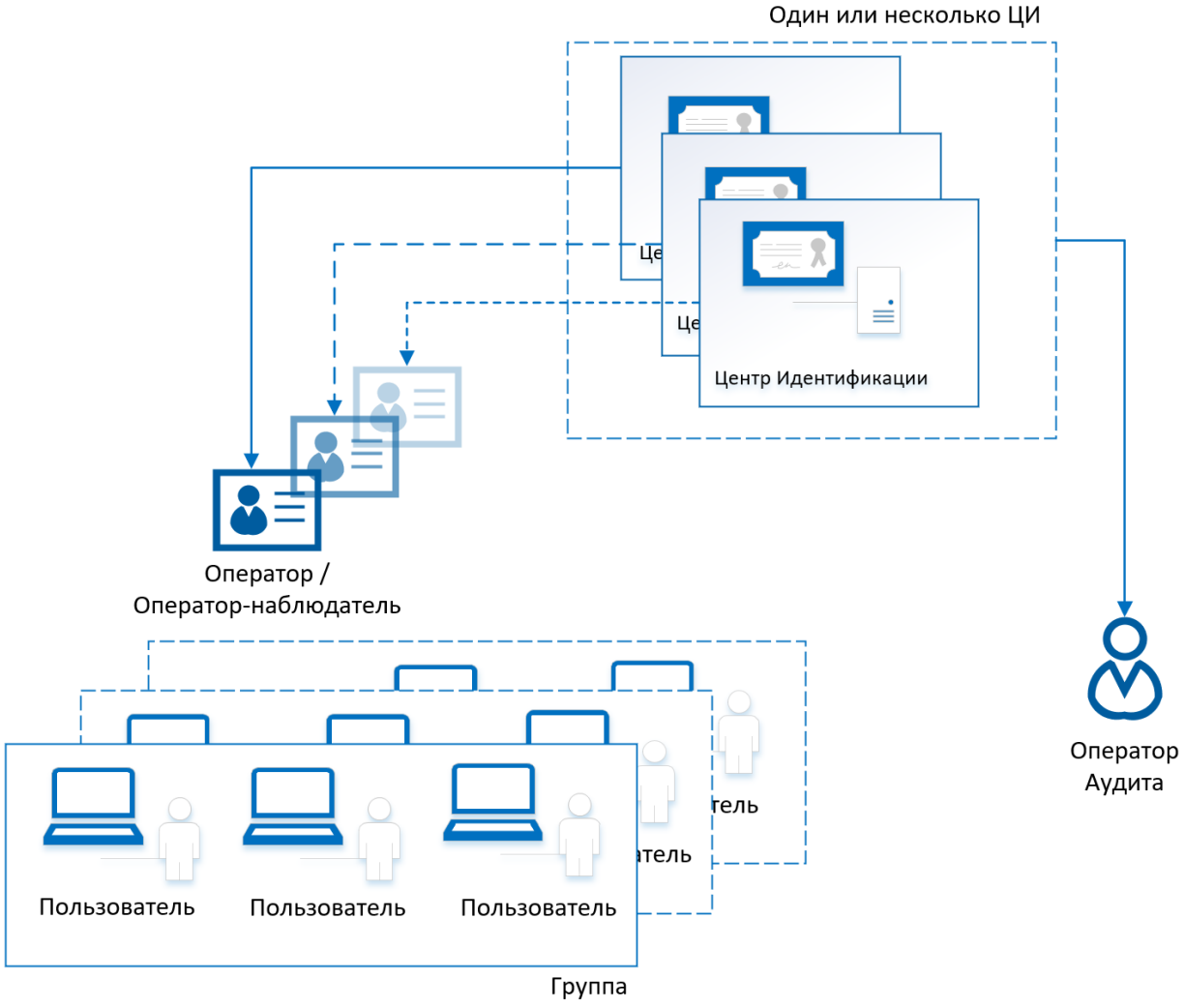

Рис. 11 — Логическая структура ролей в КриптоПро DSS

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 (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 разделе 4);
- Просмотр средств аутентификации, зарегистрированных в ЦИ КриптоПро DSS;
- Создание запросов на сертификаты Пользователей КриптоПро DSS;
- Выдача (установка) 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 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.

9. Поддерживаемые типы ЭП и форматы документов

9.1. 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.

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

9.2.1. 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.

9.2.2. 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).

9.3. 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.

9.4. 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.

10. 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.

11. Поддерживаемые форматы документов для отображения при подтверждении операций

КриптоПро DSS предоставляет возможность отображения документов перед созданием подписи на Веб-интерфейсе Пользователя.

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