

АО «СИГНАЛ-КОМ»

УТВЕРЖДЕНО
ШКНР.00051-01 31 01-ЛУ

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС
SIGNAL-COM CLOUD DSS
Версия 1.0

Описание применения

ШКНР.00051-01 31 01
Листов 22

АННОТАЦИЯ

Настоящий документ содержит описание применения программно-аппаратного комплекса Signal-COM Cloud DSS, предназначенного для централизованного дистанционного создания, обслуживания и применения ключей электронной подписи.

СОДЕРЖАНИЕ

Аннотация	2
Содержание	3
1. Назначение программы	4
1.1. Список сокращений	4
1.2. Термины и определения	4
1.3. Основные характеристики	5
2. Условия применения	6
2.1. Архитектура ПАК	6
2.2. Состав ПАК	6
2.3. Аппаратные требования	7
2.4. Требования к программному окружению	9
2.5. Описание компонентов ПАК Cloud DSS	9
2.5.1. ПАКМ «Сигнал-КОМ HSM»	9
2.5.2. Сервер электронной подписи	9
2.5.3. Сервер управления ключевой информацией	9
2.5.4. Веб-сервер идентификации	10
2.5.5. Веб-приложение идентификации	10
2.5.6. Веб-сервис администратора	10
2.5.7. Веб-сервис оператора	10
2.5.8. Веб-сервис пользователя	11
2.5.9. База данных	11
2.5.10. Веб-приложение администратора	11
2.5.11. Веб-приложение оператора	11
2.5.12. Веб-приложение пользователя	11
2.5.13. Сервер оповещения пользователей	12
2.5.14. Сервер аудита событий	12
3. Описание задачи	13
3.1. Роли участников ПАК Cloud DSS	13
3.1.1. Администратор	13
3.1.2. Оператор	13
3.1.3. Пользователь	13
3.2. Аутентификация пользователей	14
3.3. Контроль доступа	14
3.4. Подтверждение операций	14
3.5. Генерация ключей и запросов на создание сертификатов	14
3.6. Взаимодействие с доверенными УЦ	15
3.7. Взаимодействие с внешними УЦ	15
3.8. Создание ЭП	15
3.9. Проверка ЭП	15
3.10. Зашифрование данных	15
3.11. Расшифрование данных	16
3.12. Аннулирование сертификатов	16
3.13. Оповещение пользователей о событиях	16
3.14. Аудит событий системы	16
4. Входные и выходные данные	17
Приложение	18
Литература	21

1. НАЗНАЧЕНИЕ ПРОГРАММЫ

Программно-аппаратный комплекс Signal-COM Cloud DSS (далее ПАК Cloud DSS) предназначен для централизованного дистанционного создания, хранения, обслуживания и применения ключей электронной подписи и сертификатов ключей проверки электронной подписи.

Хранение ключей электронной подписи и реализация криптографических операций в ПАК Cloud DSS осуществляются централизованно и не требуют установки средств криптографической защиты информации на рабочих местах пользователей.

ПАК Cloud DSS позволяет выполнять операции создания и проверки электронных подписей в форматах CMS, CAdES, PAdES, XMLDSig, Office OpenXML. Дополнительно реализована возможность зашифрования и расшифрования данных в формате CMS.

В ПАК Cloud DSS реализован интерфейс взаимодействия с Удостоверяющими центрами, облегчающий пользователям получение сертификатов ключей проверки электронной подписи.

ПАК Cloud DSS реализован в виде веб-сервисов и предоставляет программный интерфейс по протоколам REST и SOAP [1].

1.1. Список сокращений

В настоящем руководстве используются следующие сокращения:

- БД – база данных;
- ИС – информационная система;
- ПАК - программно-аппаратный комплекс;
- ПАКМ – программно-аппаратный криптографический модуль;
- ПИН – персональный идентификационный номер;
- СУБД – система управления базами данных;
- ТК – технический комитет;
- УЦ – удостоверяющий центр;
- ЭП – электронная подпись;
- ASN.1 - Abstract Syntax Notation One;.
- CMC - Certificate Management over CMS;
- CMS – Cryptographic Message Syntax;
- CRL – Certificate Revocation List;
- HOTP - HMAC-Based One-Time Password Algorithm.
- HSM – Hardware Security Module;
- ITU-T – International Telecommunication Union - Telecommunication sector;
- OTP - One-Time Password;
- PIN – Personal Identification Number;
- REST - Representational State Transfer;
- RFC – Request for Comments;
- SMS - Short Message Service;
- SOAP – Simple Object Access Protocol;
- TOTP - Time-Based One-Time Password Algorithm;
- TSA – Time Stamp Authority;
- XML – eXtensible Markup Language.

1.2. Термины и определения

В настоящем руководстве используются следующие термины:

- веб-сервис – реализация интерфейса взаимодействия между различными приложениями по протоколам REST и SOAP;
- ключ электронной подписи – уникальная последовательность символов, предназначенная для создания электронной подписи;
- удостоверяющий центр – юридическое лицо, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей;

- сертификат ключа проверки электронной подписи – документ в электронном виде 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;
- 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.

1.3. Основные характеристики

ПАК Cloud DSS реализован в виде веб-сервисов и предоставляет программный интерфейс по протоколам REST и SOAP.

В ПАК Cloud DSS поддерживаются следующие криптографические алгоритмы:

- алгоритм создания ключей электронной подписи ГОСТ Р 34.10-2012 [16];
- алгоритм электронной подписи ГОСТ Р 34.10-2012 [16];
- алгоритм шифрования ГОСТ 28147-89 [22].

ПАК Cloud DSS позволяет формировать запросы на создание сертификатов в формате PKCS #10 [6] и CMC [7].

ПАК Cloud DSS реализует следующие протоколы электронной подписи:

- CMS;
- CAdES;
- PAdES;
- XMLDSig;
- OOXML.

ПАК Cloud DSS реализует следующие протоколы шифрования данных:

- CMS.

Протокол CMS реализован в соответствии с RFC 5652 [2] и рекомендациями ТК 26 [13].

Протокол CAdES реализован в соответствии с RFC 5126 [4].

Протокол PAdES реализован в соответствии с [23].

Протокол XMLDSig реализован в соответствии с [3] и рекомендациями ТК 26 [14].

Протокол подписи документов OOXML реализован в соответствии с [24].

В ПАК Cloud DSS реализована возможность добавления меток доверенного времени в подпись в соответствии с CAdES [4], PAdES [23] и RFC 3161 [15].

ПАК Cloud DSS использует сертификаты ключей проверки ЭП в формате ITU-T X.509 [8] и рекомендаций ТК 26 [11].

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Архитектура ПАК

Программно-аппаратный комплекс Cloud DSS состоит из следующих слоёв:

- веб-интерфейс – предназначен для обеспечения доступа участников к функциям ПАК через графическую оболочку;
- программный интерфейс – предназначен для доступа к функциям ПАК через API;
- набор внутренних сервисов – скрытые от пользователей ПАК функциональные компоненты;
- хранилище ключей (HSM) – также скрытый от пользователей ПАК компонент, в котором осуществляется хранение ключей ЭП и выполнение операций с их использованием (например, создание ЭП).

Рисунок 1 – Архитектура ПАК Cloud DSS



2.2. Состав ПАК

В состав программно-аппаратного комплекса Cloud DSS входят следующие обязательные компоненты:

- ПАКМ «Сигнал-КОМ HSM»;
- сервер электронной подписи DSS Server;
- сервер управления ключевой информацией DSS Key Manager;
- веб-сервер идентификации DSS Identity Server;
- веб-приложение идентификации DSS Identity Web;
- веб-сервис администратора DSS Administrator API;
- веб-сервис оператора DSS Operator API;
- веб-сервис пользователя DSS Customer API;
- сервер оповещений DSS Notification Server;
- сервер аудита событий DSS Audit Server;

- база данных ПАК Cloud DSS.

Дополнительно в состав ПАК Cloud DSS могут быть включены следующие компоненты:

- веб-приложение администратора DSS Administrator Web;
- веб-приложение оператора DSS Operator Web;
- веб-приложение пользователя DSS Customer Web.

2.3. Аппаратные требования

Минимальная аппаратная конфигурация ПАК Cloud DSS включает ПАКМ «Сигнал-КОМ HSM» и два сервера для программных компонентов (внутренних и внешних). Минимальные аппаратные требования к этим устройствам приведены ниже.

Таблица 1 – Требования к серверу для размещения внутренних компонентов

Оборудование	Минимальные требования
Процессор	64 бита, 4 ядра, 3 ГГц
Оперативная память	16 ГБ
Жесткий диск	2 ТБ
Сетевые адаптеры	Два сетевых адаптера

Таблица 2 – Требования к серверу для размещения внешних компонентов

Оборудование	Минимальные требования
Процессор	64 бита, 2 ядра, 3 ГГц
Оперативная память	8 ГБ
Жесткий диск	1 ТБ
Сетевые адаптеры	Два сетевых адаптера

База данных ПАК Cloud DSS в этой конфигурации устанавливается на сервер внутренних компонентов.

Рисунок 2 – Типовая схема размещения компонентов ПАК Cloud DSS

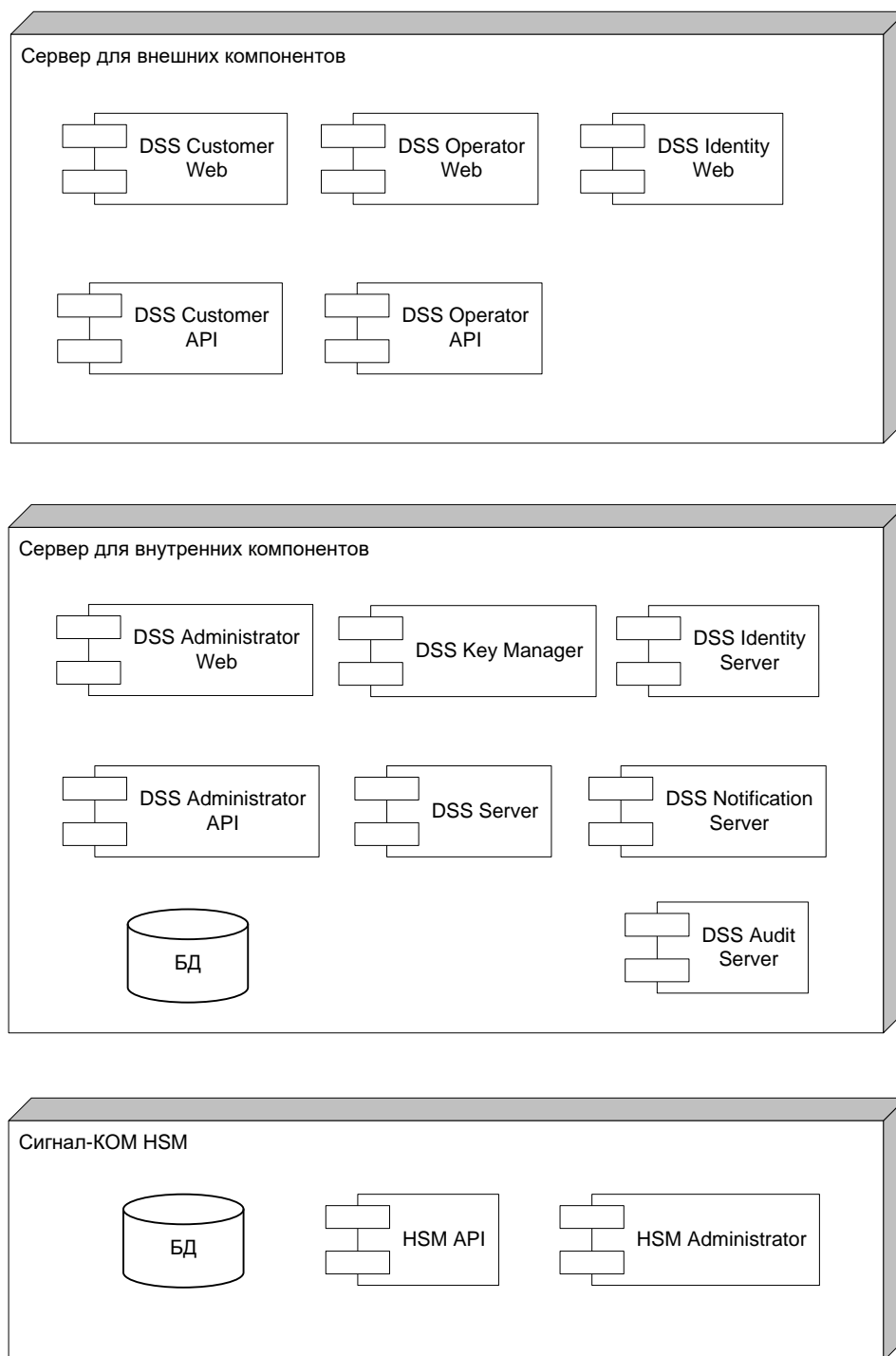


Схема размещения компонентов ПАК Cloud DSS при необходимости может быть изменена (при соблюдении принципа разделения компонентов типовой схемы) в следующих случаях:

- при размещении отдельных компонентов на выделенных серверах (например, БД);
- при увеличении количества (масштабировании) отдельных компонентов (например, DSS Server, ПАКМ «Сигнал-КОМ HSM»).

2.4. Требования к программному окружению

Все программные компоненты ПАК Cloud DSS реализованы для выполнения в виртуальной машине Java 8 (JRE 8). Рекомендуется использовать самую новую на момент установки версию Java 8.

Программные компоненты ПАК Cloud DSS могут быть установлены на любых серверных ОС, которые поддерживаются для Java 8 (<https://www.oracle.com/technetwork/java/javase/certconfig-2095354.html>). Рекомендуемая ОС – CentOS 7 и выше.

Программные компоненты ПАК Cloud DSS выполнены в виде Java EE приложений. Рекомендуемый сервер приложений – Apache Tomcat версии 8.5 и выше.

Рекомендуемая версия СУБД – MariaDB 10.4 и выше.

2.5. Описание компонентов ПАК Cloud DSS

2.5.1. ПАКМ «Сигнал-КОМ HSM»

ПАКМ «Сигнал-КОМ HSM» предназначен для надёжного хранения и обеспечения полного жизненного цикла ключей ЭП пользователей, а также для создания ЭП с использованием ключей ЭП пользователей.

ПАКМ «Сигнал-КОМ HSM» обеспечивает выполнение следующих функций:

- создание ключей ЭП и ключей проверки ЭП в соответствии с алгоритмом ГОСТ Р 34.10-2012;
- хранение ключей ЭП в защищённом хранилище, исключающее возможность их использования вне ПАКМ «Сигнал-КОМ HSM»;
- хранение сертификатов ключей проверки ЭП или (опционально) цепочек сертификатов;
- создание ЭП в соответствии с алгоритмом ГОСТ Р 34.10-2012;
- хранение и использование секретных значений для протоколов выработки ОТП;
- хранение доверенных сертификатов;
- согласование ключей на основе процедур открытого распределения ключей;
- выработка ключевого материала с использованием функций диверсификации (KDF);
- зашифрование и расшифрование областей памяти.

С ПАКМ «Сигнал-КОМ HSM» взаимодействуют как клиенты сервер электронной подписи и сервер управления ключевой информацией.

2.5.2. Сервер электронной подписи

Сервер электронной подписи DSS Server предназначен для выполнения операций создания и проверки электронных подписей, а также для зашифрования и расшифрования данных.

DSS Server представляет собой реализацию стандарта OASIS Digital Signature Service и позволяет выполнять операции создания и проверки электронных подписей в форматах CMS, CAdES, PAdES, XMLDSig, Office OpenXML. Дополнительно реализована возможность зашифрования и расшифрования данных в формате CMS.

Сервер электронной подписи реализован в виде веб-сервиса, предоставляющего программный интерфейс по протоколу SOAP.

DSS Server взаимодействует как клиент с ПАКМ «Сигнал-КОМ HSM». С сервером электронной подписи взаимодействует как клиент веб-сервис пользователя.

2.5.3. Сервер управления ключевой информацией

Сервер управления ключевой информацией DSS Key Manager предназначен для создания ключей ЭП и обслуживания ключей ЭП и сертификатов ключей проверки ЭП.

DSS Key Manager позволяет создавать ключи ЭП и запросы на создание сертификатов ключей проверки ЭП, помещать сертификаты ключей проверки ЭП в хранилище и удалять ключи ЭП.

Сервер управления ключевой информацией реализован в виде веб-сервиса и предоставляет программный интерфейс по протоколу SOAP.

DSS Key Manager взаимодействует как клиент с ПАКМ «Сигнал-КОМ HSM». С сервером управления ключевой информацией взаимодействуют как клиенты веб-сервер идентификации, веб-сервисы администратора, оператора и пользователя.

2.5.4. Веб-сервер идентификации

Веб-сервер идентификации DSS Identity Server обеспечивает выполнение следующих функций:

- проверка учетных данных пользователей;
- формирование маркеров доступа;
- проверка маркеров доступа;
- предоставление информации о владельцах маркеров доступа;
- предоставление информации о транзакции (подтверждаемой операции);
- реализация протоколов вторичной аутентификации (OTP_VIA_SMS, TOTP, HOTP);
- подтверждение выполняемых операций.

DSS Identity Server взаимодействует как клиент с сервером управления ключевой информацией. С веб-сервером идентификации взаимодействуют как клиенты веб-приложение идентификации и веб-сервисы администратора, оператора и пользователя.

2.5.5. Веб-приложение идентификации

Веб-приложение идентификации DSS Identity Web осуществляет аутентификацию пользователей и выдачу маркеров доступа с помощью протокола OAuth 2.0 [22].

DSS Identity Web предоставляет графический (веб) интерфейс для ввода учетных данных пользователей, ввода ПИН-кода виртуального токена и отображения информации о подтверждаемой операции.

Веб-приложение идентификации позволяет осуществлять взаимодействие с внешними доверенными серверами идентификации с использованием различных протоколов аутентификации: OAuth 2.0, OpenId Connect 1.0, SAML и др.

DSS Identity Web взаимодействует как клиент с веб-сервером идентификации. С веб-приложением идентификации взаимодействуют все внешние веб-приложения, которым необходимо получить доступ к программному интерфейсу ПАК Cloud DSS (в частности, веб-приложение оператора и веб-приложение пользователя).

2.5.6. Веб-сервис администратора

Веб-сервис администратора DSS Administrator API предоставляет программный интерфейс для выполнения функций администратора (см. п. 3.1.1).

DSS Administrator API взаимодействует как клиент с веб-сервером идентификации и сервером управления ключевой информацией. С веб-сервисом администратора взаимодействует как клиент веб-приложение администратора.

2.5.7. Веб-сервис оператора

Веб-сервис оператора DSS Operator API предоставляет программный интерфейс для выполнения функций оператора (см. п. 3.1.2).

DSS Operator API взаимодействует как клиент с веб-сервером идентификации и сервером управления ключевой информацией. С веб-сервисом оператора взаимодействует как клиент веб-приложение оператора.

2.5.8. Веб-сервис пользователя

Веб-сервис пользователя DSS Customer API предоставляет программный интерфейс для выполнения функций пользователя (см. п. 3.1.3).

DSS Customer API взаимодействует как клиент с веб-сервером идентификации, сервером управления ключевой информацией и сервером электронной подписи. С веб-сервисом пользователя взаимодействует как клиент веб-приложение пользователя.

2.5.9. База данных

База данных ПАК Cloud DSS состоит из сервисной базы данных и базы данных аудита.

Сервисная БД осуществляет хранение, модификацию и удаление следующих объектов, необходимых для функционирования сервиса электронной подписи:

- внешние серверы идентификации;
- УЦ;
- TSA;
- группы пользователей;
- операторы;
- пользователи;
- запросы на создание сертификатов;
- сертификаты;
- запросы на аннулирование сертификатов;
- транспортные службы;
- службы оповещения;
- протоколы вторичной аутентификации;
- подтверждаемые операции;
- транзакции.

С сервисной БД взаимодействуют веб-сервер идентификации, веб-сервисы администратора, оператора и пользователя.

БД аудита осуществляет хранение определенных событий, получаемых сервером аудита от всех компонентов ПАК Cloud DSS.

2.5.10. Веб-приложение администратора

Веб-приложение администратора DSS Administrator Web предоставляет графический (веб) интерфейс для выполнения функций администратора (см. п. 3.1.1) с помощью веб-браузера.

DSS Administrator Web взаимодействует с веб-приложением идентификации и веб-сервисом администратора.

2.5.11. Веб-приложение оператора

Веб-приложение оператора DSS Operator Web предоставляет графический (веб) интерфейс для выполнения функций оператора (см. п. 3.1.2) с помощью веб-браузера.

DSS Operator Web взаимодействует с веб-приложением идентификации и веб-сервисом оператора.

2.5.12. Веб-приложение пользователя

Веб-приложение пользователя DSS Customer Web предоставляет графический (веб) интерфейс для выполнения функций пользователя (см. п. 3.1.3) с помощью веб-браузера.

DSS Customer Web взаимодействует с веб-приложением идентификации и веб-сервисом пользователя.

2.5.13. Сервер оповещения пользователей

Сервер оповещения пользователей DSS Notification Server предназначен для рассылки сообщений (с помощью SMS, email и т.д.) участникам системы об определенных событиях, получаемых от всех компонентов ПАК Cloud DSS, в том числе для подтверждения операций.

Параметры оповещения пользователей настраиваются администратором (см. п. 3.1.1).

2.5.14. Сервер аудита событий

Сервер аудита событий DSS Audit Server предназначен для сбора и сохранения в БД аудита определенных событий, получаемых от всех компонентов ПАК Cloud DSS.

Параметры аудита настраиваются администратором (см. п. 3.1.1).

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Роли участников ПAK Cloud DSS

В ПAK Cloud DSS используются следующие роли участников:

- администратор;
- оператор;
- пользователь.

3.1.1. Администратор

Администратор ПAK Cloud DSS является пользователем с максимальным набором прав и возможностей и выполняет следующие основные функции:

- ведение списка доверенных внешних серверов идентификации;
- ведение списка доверенных УЦ;
- ведение списка доверенных TSA;
- ведение списка групп пользователей;
- ведение списка операторов;
- настройка параметров протоколов вторичной аутентификации;
- настройка параметров подтверждения операций;
- настройка транспортных служб и служб оповещения;
- настройка параметров аудита.

Учётная запись администратора создается на этапе развертывания базы данных ПAK Cloud DSS.

3.1.2. Оператор

Оператор ПAK Cloud DSS управляет пользователями, которые входят в его группы. Администратор может назначить оператору одну и более групп пользователей. Каждой группе пользователей может быть назначен администратором один и более операторов.

Оператор ПAK Cloud DSS может одновременно являться оператором доверенного УЦ. Для этого он должен сгенерировать на ПАКМ «Сигнал-КОМ HSM» ключи ЭП и получить в доверенном УЦ сертификат ключа проверки ЭП оператора УЦ.

Оператор ПAK Cloud DSS выполняет следующие основные функции:

- ведение списка пользователей;
- генерация ключей ЭП и формирование запроса на создание сертификата ключа проверки ЭП оператора доверенного УЦ;
- формирование и отправка в доверенные УЦ сообщений в формате СМС, включающих запросы на создание сертификатов ключей проверки ЭП пользователей и подписанных ЭП оператора доверенного УЦ;
- аннулирование сертификатов ключей проверки ЭП.

Регистрация операторов осуществляется администратором ПAK Cloud DSS.

3.1.3. Пользователь

Пользователь использует ПAK Cloud DSS для создания и проверки электронных подписей, а также для зашифрования и расшифрования данных. Пользователи распределяются операторами по группам, один пользователь может принадлежать только одной группе.

Пользователь ПAK Cloud DSS выполняет следующие основные функции:

- генерация ключей ЭП и формирование запроса на создание сертификата ключа проверки ЭП;
- создание ЭП;
- проверка ЭП;
- зашифрование данных;
- расшифрование данных;
- аннулирование собственного сертификата ключа проверки ЭП.

Регистрация пользователей осуществляется операторами ПАК Cloud DSS.

3.2. Аутентификация пользователей

Аутентификация зарегистрированных пользователей ПАК Cloud DSS осуществляется в веб-приложении идентификации с помощью протокола OAuth 2.0 [22].

В случае использования двухфакторной аутентификации (определяется настройками ПАК Cloud DSS) для успешной аутентификации пользователь, кроме учетной информации, должен ввести одноразовый пароль, полученный в сообщении (например, в SMS) или сформированный специальной программой на мобильном устройстве (по протоколу HOTP [21] или TOTP [20]).

В результате процедуры аутентификации пользователь получает маркер доступа, который используется для получения доступа к функционалу ПАК Cloud DSS.

Веб-приложение идентификации ПАК Cloud DSS позволяет осуществлять взаимодействие с внешними доверенными серверами идентификации с использованием различных протоколов аутентификации: OAuth 2.0, OpenId Connect 1.0, SAML и др.

3.3. Контроль доступа

В ПАК Cloud DSS реализован контроль доступа пользователей к функционалу сервера и ключевой информации.

Каждому пользователю, за исключением администратора, предоставляется доступ к персональному виртуальному токenu, размещаемому на ПАКМ «Сигнал-КОМ HSM». Доступ к виртуальному токenu защищается ПИН-кодом, который известен только владельцу и не хранится в базе данных ПАК Cloud DSS. ПИН-код виртуального токена, также как и учетные данные пользователя, задается с помощью графического интерфейса веб-приложения идентификации.

Для доступа к программному интерфейсу ПАК Cloud DSS используется маркер доступа, который получается после завершения процедуры аутентификации в веб-приложении идентификации.

3.4. Подтверждение операций

Если для выполнения операции (например, создания ЭП) требуется подтверждение пользователя (определяется настройками ПАК Cloud DSS), операция выполняется в асинхронном режиме: при первом успешном вызове метода возвращается уникальный идентификатор транзакции, который необходимо использовать при взаимодействии пользователя с веб-приложением идентификации для подтверждения операции.

Для подтверждения операции пользователь должен ввести одноразовый пароль, полученный в сообщении (например, в SMS) или сформированный специальной программой на мобильном устройстве (по протоколу HOTP [21] или TOTP [20]).

После подтверждения операции пользователем, необходимо повторно вызвать тот же метод для завершения операции и получения результата, задав в соответствующем поле идентификатор транзакции. Остальные параметры (за исключением маркера доступа) задавать не требуется: для завершения операции будут использованы параметры, заданные при первом вызове метода и сохраненные во временном хранилище ПАК Cloud DSS.

3.5. Генерация ключей и запросов на создание сертификатов

Генерация ключей ЭП и запросов на создание сертификатов ключей проверки ЭП пользователей и операторов доверенных УЦ осуществляется с помощью программного интерфейса веб-сервиса пользователя или с помощью веб-приложения пользователя.

Ключи ЭП формируются в персональном виртуальном токене, размещенном на ПАКМ «Сигнал-КОМ HSM» и защищенном ПИН-кодом пользователя.

Запрос на создание сертификата ключа проверки ЭП сохраняется в базе данных ПАК Cloud DSS.

3.6. Взаимодействие с доверенными УЦ

Первый запрос на создание сертификата ключа проверки ЭП оператор доверенного УЦ должен передать в УЦ лично.

Первый запрос на создание сертификата ключа проверки ЭП пользователя подписывает оператор доверенного УЦ (запрос на создание сертификата в формате СМС) с помощью программного интерфейса веб-сервиса оператора или с помощью веб-приложения оператора. Подписанный запрос на создание сертификата автоматически отправляется в доверенный УЦ.

Если пользователь или оператор УЦ уже имеет действующий сертификат ключа проверки ЭП, выданный доверенным УЦ, запрос на создание сертификата нового ключа проверки ЭП может быть подписан действующим ключом ЭП (запрос на создание сертификата в формате СМС) с помощью программного интерфейса веб-сервиса пользователя или с помощью веб-приложения пользователя. Подписанный запрос на создание сертификата автоматически отправляется в доверенный УЦ.

Выпущенные сертификаты пользователей и операторов автоматически загружаются из доверенного УЦ и сохраняются в базе данных ПАК Cloud DSS.

3.7. Взаимодействие с внешними УЦ

Для взаимодействия пользователей с внешними УЦ в ПАК Cloud DSS предусмотрены следующие процедуры:

- выгрузка из базы данных ПАК Cloud DSS запроса на создание сертификата ключа проверки ЭП;
- загрузка сертификата ключа проверки ЭП в базу данных ПАК Cloud DSS .

Данные процедуры доступны с помощью программного интерфейса веб-сервиса пользователя или с помощью веб-приложения пользователя.

3.8. Создание ЭП

Создание ЭП осуществляется с помощью программного интерфейса веб-сервиса пользователя.

Для создания электронной подписи необходимо задать данные для подписи и идентификатор ключа ЭП пользователя.

В качестве данных для создания электронной подписи может быть задано хэш-значение.

Текущая реализация ПАК Cloud DSS позволяет создавать подписи в форматах CMS, CAdES, PAdES, XMLDSig и Office OpenXML.

В ПАК Cloud DSS реализована опциональная возможность добавления в подпись метки доверенного времени.

3.9. Проверка ЭП

Проверка ЭП осуществляется с помощью программного интерфейса веб-сервиса пользователя.

Возможно получение отчета проверки.

В случае успешной проверки возможно опциональное добавление в подпись метки доверенного времени.

3.10. Зашифрование данных

Зашифрование данных осуществляется с помощью программного интерфейса веб-сервиса пользователя.

Текущая реализация ПАК Cloud DSS позволяет зашифровывать данные в формате CMS.

Для выполнения операции необходимо задать данные, подлежащие зашифрованию, и сертификаты открытых ключей получателей зашифрованных данных.

3.11. Расшифрование данных

Расшифрование данных осуществляется с помощью программного интерфейса веб-сервиса пользователя.

Текущая реализация ПАК Cloud DSS позволяет расшифровывать данные в формате CMS.

Для выполнения операции необходимо задать данные, зашифрованные в формате CMS.

3.12. Аннулирование сертификатов

Пользовательский сертификат ключа проверки ЭП может быть аннулирован владельцем в веб-приложении пользователя или оператором УЦ-издателя в веб-приложении оператора.

Сертификат ключа проверки ЭП оператора может быть аннулирован владельцем в веб-приложении пользователя.

3.13. Оповещение пользователей о событиях

В ПАК Cloud DSS реализовано оповещение участников системы об определенных событиях, получаемых от всех компонентов ПАК Cloud DSS, в том числе для подтверждения операций.

Оповещение пользователей осуществляется сервером оповещения путем рассылки сообщений (SMS, email и т.д.).

Параметры оповещения пользователей настраиваются администратором (см. п. 3.1.1).

3.14. Аудит событий системы

В ПАК Cloud DSS реализован аудит определенных событий, получаемых от всех компонентов ПАК Cloud DSS. Сбор и сохранение событий в БД аудита осуществляет сервер аудита.

Параметры аудита настраиваются администратором (см. п. 3.1.1).

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

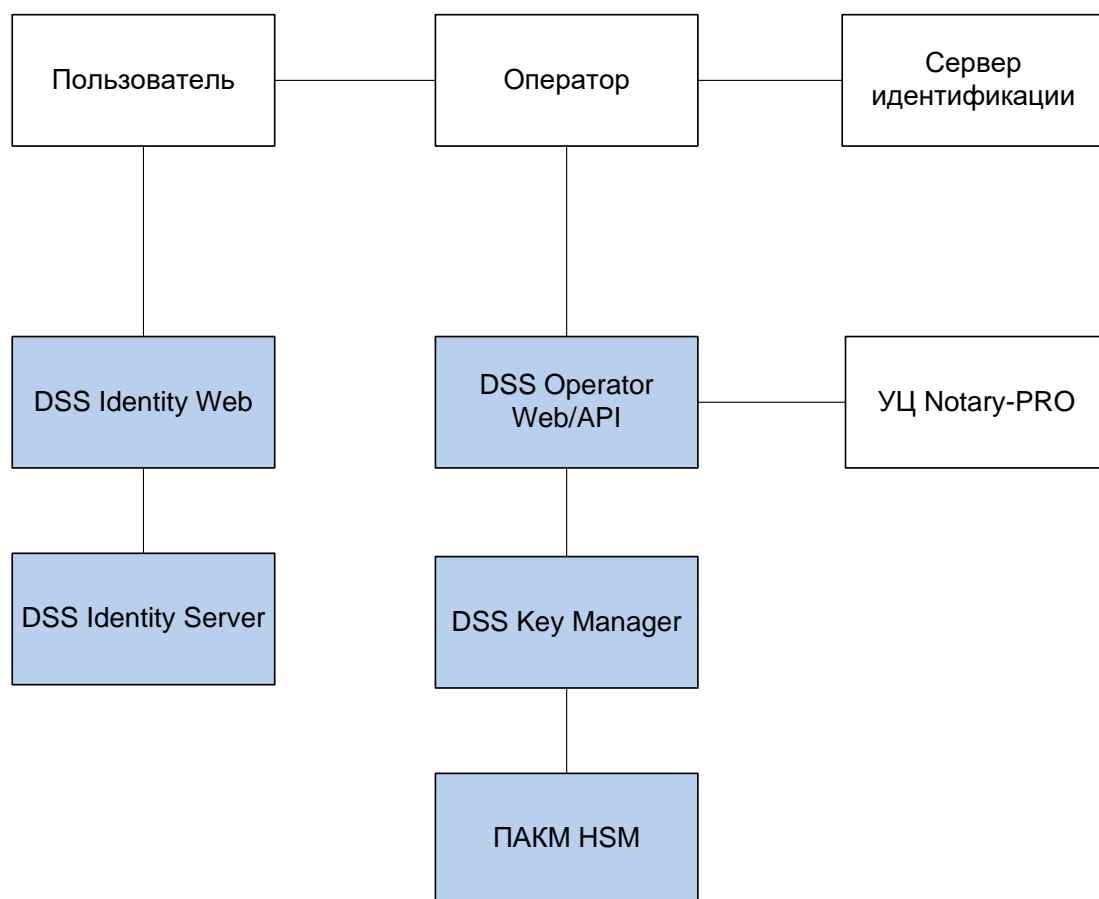
Входные и выходные данные, используемые в интерфейсах веб-сервисов ПАК Cloud DSS, задаются в виде структур (классов), описанных в Руководстве программиста.

Входные и выходные данные, задаваемые в интерфейсах веб-приложений, описаны в Руководстве Оператора и Руководстве Пользователя.

ПРИЛОЖЕНИЕ

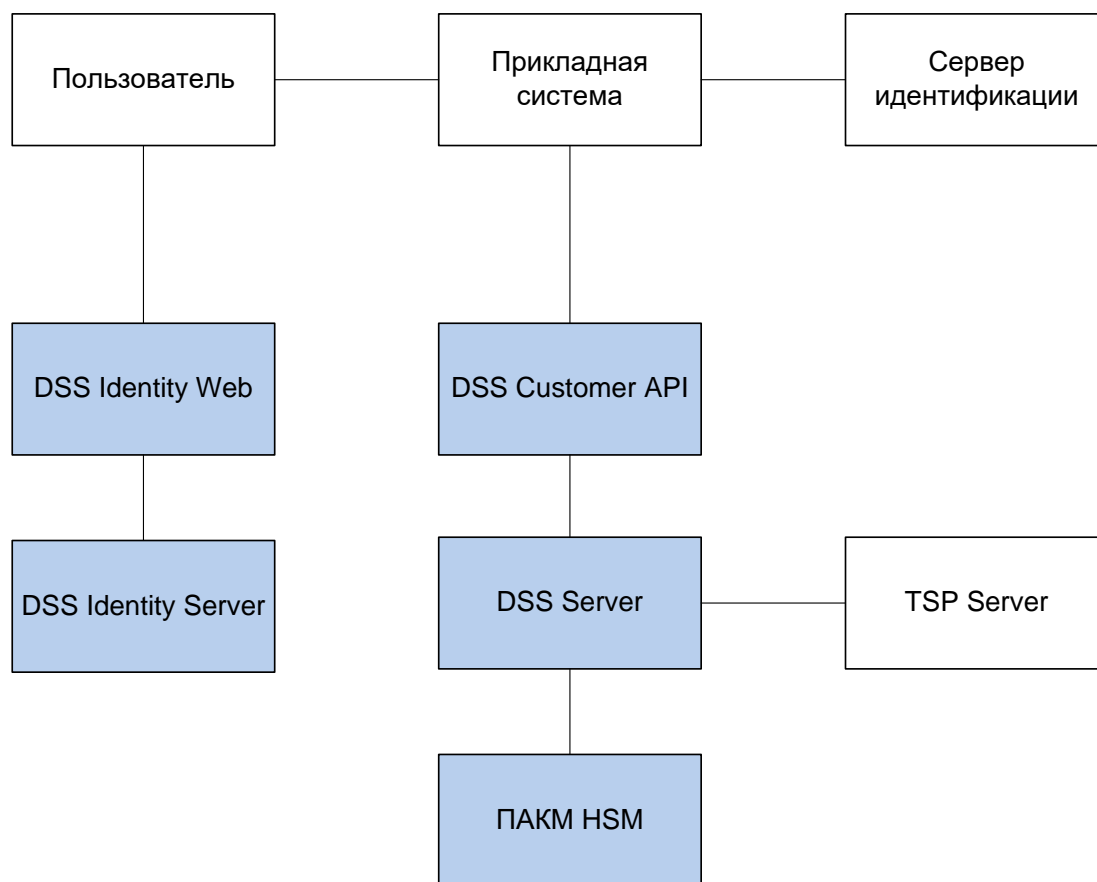
ПРИМЕРЫ

Рисунок 3 – Схема взаимодействия при регистрации пользователя и выпуске сертификата ключа проверки ЭП.



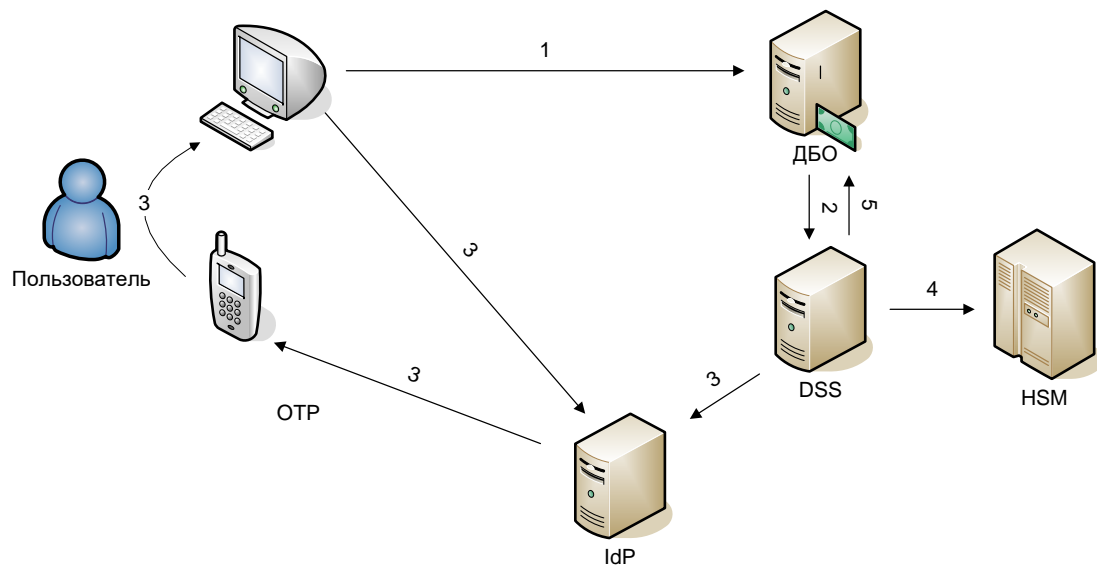
Примечание. Цветом на рисунке выделены компоненты ПАК Cloud DSS.

Рисунок 4 – Схема взаимодействия при создании ЭП.



Примечание. Цветом на рисунке выделены компоненты ПАК Cloud DSS.

Рисунок 5 – Пример использования ПАК Cloud DSS в системе дистанционного банковского обслуживания (ДБО).



ЛИТЕРАТУРА

1. SOAP Version 1.2, W3C Recommendation, 27 April 2007.
2. Housley, R., Cryptographic Message Syntax, RFC 5652, September 2009.
3. XML Signature Syntax and Processing (Second Edition). W3C Recommendation, 10 June 2008.
4. D. Pinkas, N. Pope, J. Ross, CMS Advanced Electronic Signatures (CAAdES). RFC 5126, February 2008.
5. XML Path Language (XPath) Version 1.0. W3C Recommendation, 16 November 1999.
6. PKCS #10 v1.7: Certification Request Syntax Standard. RSA Laboratories, May 26, 2000.
7. J. Schaad, M. Myers, Certificate Management over CMS (CMC), RFC 5272, June 2008.
8. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997.
9. Housley, R., Polk, W., Ford, W. and D. Solo, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, April 2002.
10. Additional Cryptographic Algorithms for Use with GOST 28147-89, GOST R 34.10-94, GOST R 34.10-2001, and GOST R 34.11-94 Algorithms. V.Popov, I.Kurepkin, S.Leontiev, RFC 4357, January 2006.
11. Р 1323565.1.023-2018. «Информационная технология. Криптографическая защита информации. Использование алгоритмов ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012 в сертификате, списке аннулированных сертификатов (CRL) и запросе на сертификат PKCS #10 инфраструктуры открытых ключей X.509». Федеральное агентство по техническому регулированию и метрологии, 2018.
12. Р 50.1.113-2016. Информационная технология. Криптографическая защита информации. Криптографические алгоритмы, сопутствующие применению алгоритмов электронной цифровой подписи и функции хэширования. Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии, 2016.
13. МР 26.2.002-213. Использование алгоритмов ГОСТ 28147-89, ГОСТ Р 34.11 и ГОСТ Р 34.10 в криптографических сообщениях формата CMS. Методические рекомендации. Технический комитет по стандартизации «Криптографическая защита информации», 2013.
14. Р 1323565.1.033-2020. Использование российских алгоритмов электронной подписи в протоколах и форматах сообщений на основе XML. Рекомендации по стандартизации. Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Технический комитет 26 «Криптографическая защита информации», 2020.
15. C. Adams, P. Cain, D. Pinkas, R. Zuccherato, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), RFC 3161, August 2001.
16. ГОСТ Р 34.10-2012. Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
17. Signal-COM Cloud DSS. Интерфейс пользователя. Руководство системного программиста. ШКНР.00051-01 32 01. ЗАО «Сигнал-КОМ», 2018.
18. Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0. OASIS, 11 April 2007.
19. D. Hardt, The OAuth 2.0 Authorization Framework, RFC 6749, October 2012.
20. D. M'Raihi, S. Machani, M. Pei, J. Rydell, TOTP: Time-Based One-Time Password Algorithm, RFC 6238, May 2011.

21. D. M'Raihi, M. Bellare, F. Hoornaert, D. Naccache, O. Ranen, HOTP: An HMAC-Based One-Time Password Algorithm, RFC 4226, December 2005.
22. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритмы криптографического преобразования.
23. ETSI EN 319 142-1 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures. European Telecommunications Standards Institute ETSI.
24. ECMA-376. Office Open XML file formats, 4th edition, December 2012. Ecma International.