Описание функциональных характеристик программного обеспечения и информация, необходимая для установки и эксплуатации программного обеспечения «Программное обеспечение программных библиотек (SDK) ИС Клиента. Версия 1.0.»

Москва 2025

АННОТАЦИЯ

Настоящий документ определяет общие сведения о программных библиотеках (SDK) ИС Клиента, их структуре, функциональным характеристикам, информацию о порядке установки, настройки и проверки функционирования программных библиотек, а также дополнительную информацию, требующуюся в ходе эксплуатации программных библиотек.

Настоящий документ разработан с учетом рекомендаций ГОСТ 19.503-79 «Единая система программной документации. Руководство системного программиста».

Содержание

Термины и сокращения

Термин / сокращение	Определение
Адаптер программных библиотек (SDK)	Прикладное программное обеспечение, назначением которого является обеспечение взаимодействия программных библиотек (SDK) с участниками процесса аутентификации в рамках выполнения протоколов аутентификации, а также замкнутости среды функционирования СКЗИ
ЕСИА	Федеральная государственная информационная система «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме»
ИС Клиента	Внешняя относительно ПИА информационная система, для которой ПИА выполняет аутентификацию и авторизацию конечного пользователя
МР	Методические рекомендации
ОС	Операционная система
ПИА	Провайдер идентификации и аутентификации – поставщик идентификации и аутентификации, осуществляющий делегированную идентификацию, аутентификацию и авторизацию конечных пользователей по запросам от информационных систем клиентов ПИА (ИС Клиентов), зарегистрированных в ПИА
ПО	Программное обеспечение
ППО	Прикладное программное обеспечение
Программные библиотеки (SDK) ИС Клиента	Набор программных библиотек для поддержки протокола криптографической аутентификации и авторизации или протокола аутентификации МР ЕСИА и взаимодействия с СКЗИ
Протокол аутентификации МР ЕСИА	Протокол аутентификации на базе OpenID Connect 1.0 в соответствии с документом «Методические рекомендации по использованию ЕСИА»

Термин / сокращение	Определение
СКЗИ	Средство криптографической защиты информации
API (Applcation Programming Interface, программный интерфейс приложения, интерфейс прикладного программирования)	Набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) или операционной системой для использования во внешних программных продуктах
CMS	Стандарт, описывающий структуру криптографических сообщений, включающих в себя защищенные данные вместе со сведениями, необходимыми для их корректного открытия или использования
JSON (JavaScript Object Notation)	Текстовый формат обмена данными, основанный на JavaScript
JWE (JSON Web Encryption)	Структура данных в формате JSON, представляющая собой зашифрованное и защищенное от модификации сообщение. Используется для передачи зашифрованных данных (например, зашифрованного JWT токена)
JWT (JSON Web Token)	Токен доступа в формате JSON, определенном с учетом RFC 7519
REST API	Архитектурный стиль, который определяет правила обмена данными между приложениями, применяемый к API
SDK	Сокращенное название программных библиотек, используемое на схемах и рисунках

1.1 Функции программы

1.1.1 Функции программных библиотек (SDK) ИС Клиента и Адаптера в части выполнения протокола криптографической аутентификации и авторизации

Программные библиотеки (SDK) ИС Клиента в рамках выполнения протокола криптографической аутентификации и авторизации реализуют следующие функции:

- формирование токена запроса аутентификации и/или авторизации, отправляемого из ИС Клиента в ПИА;
- расшифрование JWE-структуры объекта ответа на запрос аутентификации и/или авторизации, полученного в ИС Клиента из ПИА:
- обработка токена ответа на запрос аутентификации и/или авторизации;
- обработка токена идентификации №1, содержащего информацию об успешной аутентификации (и авторизации) конечного пользователя в ПИА, а также значение хэш-функции, вычисленного в ПИА от кода авторизации;
- сравнение полученного значения хэш-функции с вычисленным в ИС Клиента от кода авторизации;
- обработка токена с уведомлением об ошибке аутентификации и/или авторизации;
- формирование токена запроса токена доступа, отправляемого из ИС Клиента в ПИА;
- формирование токена доказательства владения ключом;
- обработка токена ответа на запрос токена доступа, полученного в ИС Клиента из ПИА;
- обработка токена идентификации №2, содержащего информацию об успешной аутентификации и авторизации конечного пользователя в ПИА, а также значение хэш-функции, вычисленного в ПИА от токена доступа;
- сравнение полученного значения хэш-функции с вычисленным в ИС Клиента от токена доступа;
- обработка токена завершения сессии аутентификации в ПИА, полученного в ИС Клиента из ПИА;
- формирование зашифрованного токена идентификации для передачи в уведомлении о завершении сессии аутентификации пользователя в ИС Клиента;
- верификация токена доступа:
- верификация токена доступа протокола криптографической аутентификации и авторизации;
- верификация токена доступа протокола аутентификации МР ЕСИА

- управление ключевыми контейнерами:
- формирование запроса на выпуск сертификата в формате PKCS#10 с учетом роли ИС Клиента (в роли ИС Клиента или в роли ресурсного сервера) с или без подписания PKCS#10 текущим ключом аутентификации;
- установка сертификата в ключевой контейнер;
- смена пароля ключевого контейнера;
- удаление ключевого контейнера;
- получение списка СКЗИ, подключенных к программным библиотекам (SDK) ИС Клиента;
- получение списка всех сертификатов из СКЗИ, подключенных к программным библиотекам (SDK) ИС Клиента;
- генерация псевдослучайной последовательности;
- разбор X.509 сертификата для его отображения в человекочитаемом виде;
- разбор PKCS#10 для его отображения в человекочитаемом виде.

Для выполнения программными библиотеками вышеперечисленных функций используется Адаптер, который обеспечивает взаимодействие:

- между ИС Клиента и программными библиотеками (SDK) ИС Клиента посредством предоставления REST API;
- программных библиотек (SDK) ИС Клиента с оперативным хранилищем данных;
- с программными библиотеками (SDK) ИС Клиента в части получения журналируемых событий и управления записями журналирования.

1.1.2 Функции программных библиотек (SDK) ИС Клиента и Адаптера в части выполнения протокола аутентификации МР ЕСИА

Программные библиотеки (SDK) ИС Клиента в рамках выполнения протокола аутентификации МР ЕСИА и Адаптер к ним реализуют следующие функции:

- выполнение протокола аутентификации МР ЕСИА: формирование запроса аутентификации, формирование запроса токена, обработку ответа на запрос токена, включая валидацию токена доступа и ID токена;
- поддержка модели состояний и контроля последовательности выполнения протокола аутентификации МР ЕСИА;

- поддержка взаимодействия с СКЗИ в соответствии с API, предоставляемым СКЗИ: генерация случайных чисел, создание подписи в формате PKCS#7 detached signature, создание подписи в формате 64 байтовой строки, вычисление значения хэш-функции по алгоритму ГОСТ Р 34.11-2012, верификация электронной подписи;
- реализация механизма журналирования работы для возможности отслеживания активности и выявления проблем.

Для выполнения программными библиотеками вышеперечисленных функций используется Адаптер, который обеспечивает взаимодействие:

- между ИС Клиента и программными библиотеками (SDK) ИС Клиента посредством предоставления REST API;
- программных библиотек (SDK) ИС Клиента с оперативным хранилищем данных;
- с программными библиотеками (SDK) ИС Клиента в части получения журналируемых событий и управления записями журналирования.

1.1.3 Функции программных библиотек (SDK) ИС Клиента и Адаптера в части реализации криптографических операций, необходимых для выполнения обеспечивающих процессов

Программные библиотеки (SDK) ИС Клиента в части реализации криптографических операций, необходимых для выполнения обеспечивающих процессов, предназначены для выполнения следующих функций:

- формирование электронной подписи от строки данных в виде CMS-контейнера;
- формирование электронной подписи от файла данных в виде CMS-контейнера;
- формирование электронной подписи от строки данных в виде байтовой строки;
- верификация электронной подписи JWT-токена;
- получение сертификата из ключевого контейнера;
- проверка состояния приложения.

Для выполнения программными библиотеками вышеперечисленных функций используется Адаптер, который обеспечивает взаимодействие:

- между ИС Клиента и программными библиотеками (SDK) ИС Клиента посредством предоставления REST API;
- с программными библиотеками (SDK) ИС Клиента в части получения журналируемых событий и управления записями журналирования.

1.2 Функциональные ограничения на применение

Программные библиотеки (SDK) ИС Клиента для взаимодействия с ИС Клиента должны применяться вместе с Адаптером программных библиотек (SDK) ИС Клиента, через которые обеспечивается взаимодействие непосредственно программных библиотек с ИС Клиента.

Программные библиотеки (SDK) ИС Клиента не реализуют взаимодействие с хранилищем данных напрямую – данное взаимодействие обеспечивается посредством Адаптера программных библиотек (SDK) ИС Клиента.

Программные библиотеки (SDK) ИС Клиента реализуют функции журналирования в части сбора записей событий и сообщений, а также их передачу в адрес ПИА через программный интерфейс, который реализован в ППО Адаптера программных библиотек (SDK) ИС Клиента.

Программные библиотеки (SDK) ИС Клиента не предоставляют внешние методы и не предусматривают вызов своих методов напрямую по сети.

2 Установка и настройка программы

Перед установкой программы необходимо произвести настройку среды функционирования программы в соответствии с описанием, приведенным в п. 2.1.

2.1 Настройка среды функционирования

Для корректной работы программных библиотек (SDK) ИС Клиента должен быть предустановлен перечень компонентов среды функционирования на стороне инфраструктуры ИС Клиента, в программное обеспечение которой встраиваются Адаптеры и программные библиотеки (SDK) ИС Клиента:

- Операционная система Альт 8 СП;
- СКЗИ «КриптоПРО CSP» версия 5.0 R3 КС3 (исполнение 3-Base),
- Redis в кластерной конфигурации.

Команды для установки и запуска приложения, а также шаблоны конфигурационных файлов перечислены в скрипте install.sh. Скрипт запускается следующей командой: `./install.sh путь_к_папке_дистрибутива путь_к_папке_установки` из папки, в которой находится скрипт.

Для запуска программы, помимо запуска инсталляционного скрипта:

1) Должно быть установлено и настроено СКЗИ «КриптоПРО CSP» версии 5.0.
2) Должен быть настроен кластер Redis. Конкретные параметры конфигурации могут варьироваться в зависимости от настроек, принятых в используемой ИС Клиента.

3) Должны быть добавлены корневые сертификаты используемых УЦ.
4) Должны быть отредактированы файлы конфигурации `~/app/.env, client-old-static-config.yaml и secure-data.json`.
   a. Конфигурационные параметры, перечисленные в файле `.env`:
      – CLIENT_ID – мнемоника ИС Клиента, зарегистрированная в ПИА (ЕСИА);
      – SIGN_KEY, SIGN_KEY_PIN – имя ключа, сертификат которого привязан к ИС Клиента и используется для подписи запросов;
      – ESIA_CERTIFICATE_FILE_PATH – путь к файлу сертификата, которым ПИА (ЕСИА) подписывает токены;
      – ESIA_ISS – поле iss, которое ЕСИА записывает в токены;
      – CRYPTOPRO_THREADS – число потоков, из которых производится работа с СКЗИ «КриптоПРО».
   b. Конфигурационные параметры, перечисленные в файле secure-data.json:
      – redis_settings.redis1.password – пароль для подключения к кластеру Redis. При отсутствии защиты паролем поле остается пустым;
      – redis_settings.redis1.sentinels – адреса узлов кластера Redis;
      – redis_settings.redis1.shards – количество записей в массиве должно соответствовать количеству узлов кластера в вышеописанном параметре из-за ограничений userver.
   c. Конфигурационные параметры, перечисленные в файле `client-old-static-config.yaml`, настраиваются в соответствии с документацией на userver версии 2.6.
5) При работе скрипта должен быть доступен репозиторий ОС Альт 8 СП: либо посредством подключения сервера к сети интернет на момент проведения установки, либо посредством подключения локального репозитория с использованием отторгаемых носителей. Подключение репозитория к ОС Альт 8 СП должно быть осуществлено в соответствии с требованиями документации на ОС.

2.1.1 Требования к конфигурированию СКЗИ

1) Должны быть установлены все цепочки корневых сертификатов удостоверяющих центров, задействованных в выдаче сертификатов для ИС Клиента и ПИА.
2) Должны быть установлены актуальные списки отозванных сертификатов этих УЦ.

3) Должно быть обеспечено регулярное обновление списков отзыва, автоматически средствами СКЗИ, либо вручную путем регулярной загрузки актуальных списков отзыва, получаемых от УЦ.

3 Запуск программы

Запуск программы производится на серверной платформе. Приложение регистрирует сценарий запуска в подсистеме управления службами ОС systemd в пользовательской области применения и добавляется в автозапуск. Удаление из автозапуска выполняется при помощи команды `systemctl disable --user esia-client-adapter`

Запуск сценария в области применения пользователя осуществляется путем выполнения команды: `systemctl start --user esia-client-adapter`

Просмотр журналов осуществляется путем выполнения команды: `journalctl --user -u esia-client-adapter`

Уровни детализации журналов настраиваются в файле `config-vars.yaml`. Ротация журналов настраивается средствами ОС.

Рекомендуемые уровни детализации журналов для тестовой среды:

```
userver-logger-level: info
sdk-logger-level: trace
service-logger-level: trace
```

Рекомендуемые уровни детализации журналов для продуктивной среды:

```
userver-logger-level: info
sdk-logger-level: warning
service-logger-level: warning
```

4 Эксплуатация программы

ПО Адаптера SDK ИС Клиента должно функционировать на выделенном серверном оборудовании, соответствующем требованиям эксплуатационной документации на СКЗИ «КриптоПро CSP» 5.0 R3 (исполнение 3-Base), включая, в том числе, требования:

- к наличию аппаратно-программного модуля доверенной загрузки с аппаратным датчиком случайных чисел, находящемуся в списке совместимых в соответствии с эксплуатационной документацией на СКЗИ;
- установленной на сервере операционной системе и настроенной в соответствии с рекомендациями производителя, а также эксплуатационной документации на СКЗИ.

Для серверного оборудования, на котором развернуто ПО Адаптера SDK ИС Клиента и программные библиотеки (SDK) ИС Клиента должны быть выполнены меры обеспечения ИБ, реализация которых должна производиться средствами ОС, под управлением которой работает Адаптер:

- идентификация и аутентификация пользователей, являющихся работниками оператора, обеспечение правил разграничения их доступа;
- управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, разграничение ролей;
- ограничение неуспешных попыток входа в ОС;
- блокирование сеанса доступа в ОС после установленного времени бездействия (неактивности) пользователя или по его запросу;
- фильтрация и контроль соединений информационных потоков между серверным оборудованием с развернутым ПО с использованием сертифицированных ФСТЭК России межсетевых экранов не ниже 5 класса;
- обеспечение доверенной загрузки серверного оборудования с развернутым ПО;
- мониторинг (просмотр, анализ) событий безопасности и реагирование на них (реализация допускается путем применения организационных мер);
- реализация антивирусной защиты (реализация (допускается путем применения организационных мер);
- контроль установки обновлений ОС, включая обновление программного обеспечения средств защиты информации;
- контроль работоспособности, параметров настройки и правильности функционирования ОС и средств защиты информации
- контроль целостности ОС.

Устанавливаемое на выделенное серверное оборудование совместно с Адаптером SDK ИС Клиента и СКЗИ дополнительное программное обеспечение не должно нарушать корректное функционирование ПО Адаптера SDK ИС Клиента и не должно влиять на инженерно-криптографические качества СКЗИ. Установка совместного ПО не должна противоречить требованиям со стороны документации на ОС и на СКЗИ, включая требования к замкнутости программной среды.

Необходимо обеспечить замкнутость программной среды СКЗИ. Установка программного обеспечения, не прошедшего исследования по оценке влияния на СКЗИ, включая программное обеспечение ИС Клиента, на выделенном серверном оборудовании совместно с Адаптером SDK ИС

Клиента, допускается в случае, если это допускается эксплуатационной документацией на операционную систему и эксплуатационной документацией на СКЗИ.

При эксплуатации ИС Клиента должны быть предусмотрены организационные и технические меры для ограничения доступа к выделенному серверному оборудованию, на котором устанавливается ПО Адаптера SDK ИС Клиента, и к функциям ПО Адаптера SDK ИС Клиента.

При эксплуатации программы должны применяться средства межсетевого экранирования (далее – межсетевой экран, МСЭ) для фильтрации и контроля соединений информационных потоков между устройствами, сегментами ИС, а также между ИС с использованием сертифицированных ФСБ России или ФСТЭК России межсетевых экранов не ниже 5 класса. МСЭ должен:

- разрешать сетевой доступ к ПО кэширования данных Redis применяемом в Адаптере SDK ИС Клиента только для Адаптера SDK ИС Клиента; доступ иного программного обеспечения к ПО кэширования данных Redis применяемом в Адаптере SDK ИС Клиента должен быть запрещен;
- разрешать сетевой доступ только для компонентов ИС Клиента, непосредственно интегрированных с Адаптером SDK ИС Клиента; доступ иного программного обеспечения к API Адаптера SDK ИС Клиента должен быть запрещен;
- запрещать доступ других серверов, кроме серверов с которых осуществляется взаимодействие сервисов ИС Клиента, непосредственно интегрированных с Адаптером SDK ИС Клиента;
- запрещать доступ в сети общего пользования любого ПО, функционирующего на серверном оборудовании с развернутым ПО Адаптера, за исключением доступа для получения списков отозванных сертификатов со стороны СЭП по протоколу CDP, если применяется механизм автоматического обновления списков отзыва.

Эксплуатация программы должна производиться под контролем лица – сотрудника эксплуатирующей организации, ответственного за обеспечение информационной безопасности, либо который назначен администратором информационной безопасности.

Эксплуатация СКЗИ должна производиться в соответствии с требованиями документации на СКЗИ, а также в соответствии с требованиями Приказа ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

В отношении ИС Клиента должны быть соблюдены требования Приложения Д «Требования по безопасности сервисов ЕСИА, основанных на протоколах Oauth2.0 и OpenId

Connect 1.0» (далее – требования по безопасности) Методических рекомендаций по использованию ЕСИА, а при эксплуатации Адаптера SDK ИС Клиента должны соблюдаться Требования к применению типового решения указанных требований по безопасности.