

КриптоПро РКІ-Кластер

Описание функциональных характеристик

КриптоПро РКІ-Кластер – комплекс программного обеспечения для централизованного и унифицированного обмена сообщениями между различными компонентами РКІ-инфраструктуры организации, обеспечивающей управление жизненным циклом сертификатов ключей проверки электронной подписи и применение электронной подписи.

Назначение КриптоПро РКІ-Кластер:

- Автоматизация процесса создания, выдачи, аннулирования КСКПЭП заявителю на всех этапах оказания услуги (от момента получения заявления до записи КСКПЭП на ключевой носитель)
- Интеграция информационных систем РКІ-инфраструктуры в единый программный комплекс
- Предоставление единого API для доступа к РКІ-сервисам
- Предоставление веб-интерфейс для Операторов и Пользователей
- Аутентификация и авторизация вызывающих сторон
- Гарантированная передача данных/сообщений между РКІ-сервисами
- «Парсинг» входящих запросов и перенаправление их к целевым РКІ-сервисами
- Интеграция со СМЭВ для проверки сведений заявителей и отправки данных в ЕСИА
- Интеграция со средствами УЦ, построенными на базе ПАК «КриптоПро УЦ 2.0»
- Интеграция с корпоративными ИС для получения дополнительных данных (опционально)
- Обеспечение информационной безопасности на всех этапах информационного взаимодействия
- Обеспечение криптографической защиты информации при передаче данных между взаимодействующими ИС и РКІ-сервисами с использованием протокола TLS и обеспечение контроля целостности сообщений (формирование и проверка ЭП)
- Поддержка отечественных криптографических алгоритмов в части взаимодействия по протоколу TLS
- Сбор данных и статистический анализ
- Балансировка нагрузки
- Централизованный мониторинг РКІ-инфраструктуры

Компоненты РКІ-Кластера

- Шлюз прикладного уровня
- Сервис обеспечения работы Операторов УЦ
- Сервис проверок
- Сервис взаимодействия с УЦ
- Сервис взаимодействия с ЕЦП УЦ
- Центр Статистики

Ниже описаны функциональные характеристики каждого компонента в отдельности.

Шлюз прикладного уровня

Программный компонент «Шлюз прикладного уровня» представляет собой компонент из состава комплекса «КриптоПро РКІ-Кластер». Шлюз прикладного уровня

является центральным компонентом РКІ-Кластера и используется для управления процессами жизненного цикла сертификатов ключа проверки электронной подписи (далее — сертификатов), инициированными из интегрированных с РКІ-Кластером корпоративных и иных информационных систем (ИС), для управления учетными записями Операторов, подключающихся к РКІ-Кластеру, а также для координации взаимодействия других компонентов РКІ-Кластера.

Основные функции Шлюза прикладного уровня:

- обеспечение взаимодействия и обмена сообщениями между компонентами РКІ-Кластера
- управление учетными записями Операторов, взаимодействующих с РКІ-Кластером при помощи Сервиса обеспечения работы Операторов
- реализация модели обмена сообщениями «издатель-подписчик» по отдельным темам, в рамках которых происходит обмен сообщениями
- обеспечение гарантии доставки сообщений «как максимум один раз» и «как минимум один раз»
- обеспечение строгой проверки корректности запросов, аутентификации и авторизации вызывающих систем
- создание и проверка электронной подписи (ЭП) в соответствии с ГОСТ Р 34.10–2012 (и ГОСТ Р 34.11–2012), с использованием СКЗИ «КриптоПро CSP» версии 5.0 и ПАКМ «КриптоПро HSM» версии 2.0
- защита каналов связи с использованием протокола TLS в соответствии с Рекомендациями по стандартизации Р 1323565.1.020-2020 «Информационная технология. Криптографическая защита информации. Использование криптографических алгоритмов в протоколе безопасности транспортного уровня (TLS 1.2)» или с требованиями МР 26.2.001-2013 «Использование наборов алгоритмов шифрования на основе ГОСТ 28147-89 для протокола безопасности транспортного уровня (TLS)» с использованием СКЗИ «КриптоПро CSP» версии 5.0 и ПАКМ «КриптоПро HSM» версии 2.0
- проверка электронной подписи поступающих запросов
- хранение и предоставление статуса запросов от вызывающих систем
- поиск информации в реестре выданных и аннулированных сертификатов
- управление процессами жизненного цикла сертификатов, выданных УЦ, интегрированным с РКІ-Кластером
- координация взаимодействия между компонентами ЕЦП.

Сервис обеспечения работы Операторов УЦ

Сервис обеспечения работы Операторов УЦ представляет собой компонент из состава ПК «КриптоПро РКІ-Кластер». Основной функцией Сервиса является предоставление интерфейсов взаимодействия для Операторов УЦ. Под Операторами УЦ понимаются потребители сервисов РКІ-Кластера, осуществляющие управление пользователями, проверку сведений о них и управлением их сертификатами. Операторы УЦ могут взаимодействовать с Сервисом обеспечения работы Операторов УЦ как напрямую, так по средствам интерфейса интегрированной с РКІ-Кластером ИС.

Сервис предоставляет веб- и программный интерфейсы для подключения Операторов. Веб-интерфейс предоставляется только для Операторов, которые напрямую

взаимодействуют с Сервисом, для информационных систем, интегрированных с РКІ-Кластером, доступен только программный интерфейс.

Сервис обеспечения работы Операторов УЦ фактически представляет собой точку входа для Операторов УЦ, предоставляющую возможность подавать запросы и управлять полученными данными для последующего обращения к нужным сервисам РКІ-Кластера.

Сервис обеспечения работы Операторов УЦ предоставляет функции, связанные с проверкой сведений заявителей и управлением жизненным циклом сертификата, а именно:

- направление в СМЭВ и другие внешние информационные системы (ИС) запросов на проверку сведений о заявителе и регистрацию в ЕСИА созданных сертификатов. Указанное взаимодействие осуществляется через компоненты «Шлюз прикладного уровня» и «Сервис проверок»
- направление в УЦ запросов на создание и аннулирование сертификатов. Указанное взаимодействие осуществляется через компоненты «Шлюз прикладного уровня» и «Сервис взаимодействия с УЦ».

Основные функции Сервиса обеспечения работы Операторов УЦ:

- ввод данных Заявителя (создание заявки) через веб-форму
- проверка наличия действующего сертификата в реестре сертификатов
- отзыв сертификата при наличии действующего сертификата
- отзыв сертификата по заявлению
- получение данных о Заявителе из интегрированной ИС (при наличии)
- проверка сведений о Заявителе в интегрированной ИС (при наличии)
- проверка сведения о Заявителе в СМЭВ (доступные для АУЦ виды сведений)
- получение выписки из ЕГРЮЛ или ЕГРИП через СМЭВ
- проверка сведений по выписке из ЕГРЮЛ или ЕГРИП через СМЭВ
- отправка информации о созданных сертификатах в ЕСИА
- контроль и ограничение подключаемых ключевых носителей
- интеграция со сканером паспортов, для получения образа паспорта и его проверки
- интеграция с камерой, для сохранения фотоизображения Заявителя
- прикрепление документов к заявке
- генерация ключа ЭП и формирование ключевого документа на ключевом носителе
- передача в УЦ запроса на сертификат
- получение сертификата/ статуса сертификата из УЦ
- печать заявлений на создание и отзыв сертификата, а также копии сертификата на бумажном носителе.
- запись сертификата на носитель
- создание предзаявки для последующей обработки
- получение данных Заявителя из ИС, которая подключается к РКІ-кластеру
- передача в ИС результатов проверки сведений о Заявителе
- поиск заявки/предзаявки Заявителя
- получение запроса на сертификат от ИС
- передача в ИС выпущенного сертификата или сведений об ошибке

Сервис проверок

Программный компонент Сервис проверок представляет собой компонент из состава комплекса ПК «КриптоПро РКІ-Кластер» и используется для выполнения проверок данных и сведений заявителей перед созданием сертификата.

Сервис проверок предоставляет возможность проведения различных проверок по запросам вызывающих систем, посредством обращения последних к программному интерфейсу РКІ-Кластера. В Сервисе реализованы следующие виды проверок:

- в ПФР для проверки соответствия фамильно-именной группы и СНИЛС
- в МВД России для проверки действительности паспорта гражданина РФ и проверки действительности паспорта по серии и номеру
- в ФНС России для запроса выписки из ЕГРЮЛ/ЕГРИП, запроса изменений в ЕГРЮЛ/ЕГРИП и проверки соответствия данным заявителя и полученным сведениям из выписок
- в ФНС России для проверки соответствия паспортных данных и ИНН
- (опционально) в смежных учетных ИС для проверки сведений о заявителе и его полномочий.

Дополнительно Сервис проверок осуществляет направление в ЕСИА сведения о созданных сертификатах.

В ответ на запросы проверки сведений о заявителе Сервис возвращает статус каждой проверки – Пройдена/Не пройдена/В ожидании. Если проверка пройдена успешно, то ей назначается срок действия (настраиваемый параметр), в течение которого проверка считается действительной. В случае, если какая-либо из проверок завершается не успешно, Сервис возвращает описание ошибки, с указанием какие данные не прошли проверку.

В общем случае функции Сервиса проверок вызываются в процессе выполнения заявки на создание нового сертификата через веб-интерфейс Сервиса обеспечения работы Операторов либо посредством обращения к программному интерфейсу Шлюза прикладного уровня. Дополнительно Сервис проверок имеет свой программный интерфейс, который можно вызывать независимо от процесса создания.

Сервис взаимодействия с УЦ

Программный компонент Сервис взаимодействия с УЦ представляет собой компонент из состава ПК «КриптоПро РКІ-Кластер». Сервис взаимодействия с УЦ обеспечивает взаимодействие компонентов РКІ-Кластера с Удостоверяющим центром посредством обращения к программному интерфейсу Центра Регистрации (ЦР) ПАК «КриптоПро УЦ».

Основные функции Сервиса взаимодействия с УЦ:

- фильтрация и организация очереди запросов к ЦР УЦ
- передача в УЦ запросов на создание/аннулирование сертификата ключа проверки электронной подписи (далее — сертификата)
- получение статусов запросов на создание/аннулирование СКП ЭП в УЦ;

- поиск сертификата в УЦ и его получение
- подпись запросов, передаваемых в УЦ, технологической электронной подписью Сервиса взаимодействия с УЦ.

Сервис взаимодействия с ЕЦП УЦ

Программный компонент Сервис взаимодействия с ЕЦП УЦ представляет собой компонент из состава ПК «КриптоПро РКІ-Кластер», который обеспечивает взаимодействие с Единой цифровой платформой ФНС России (далее ЕЦП) в процессе жизненного цикла сертификатов. Сервис позволяет обеспечить безопасное подключение и взаимодействие с АРІ ЕЦП для доверенных лиц (далее – ДЛ) УЦ ФНС России. Сервис предоставляет собственное REST АРІ для ИС ДЛ.

Основные функции Сервиса взаимодействия с ЕЦП УЦ:

- Получение данных Заявителя из ИС ДЛ
- Проверка наличия действующего сертификата в реестре УЦ ФНС
- Отзыв сертификата при наличии действующего сертификата
- Отзыв сертификата по заявлению / запросу
- Проверка сведений о Заявителе в АИС Налог-3
- Проверка соответствия фамильно-именной группы и СНИЛС
- Проверка соответствия паспортных данных и ИНН физического лица
- Получение выписки из ЕГРЮЛ или ЕГРИП
- Проверка сведений по выписке из ЕГРЮЛ или ЕГРИП
- Передача в ИС ДЛ результатов проверки сведений о Заявителе
- Передача в ЕЦП документов заявителя
- Получение запроса на сертификат от ИС ДЛ
- Подписание запроса на сертификат ключом ДЛ
- Передача в УЦ ФНС запроса на сертификат
- Получение сертификата/ статуса сертификата из УЦ ФНС
- Передача в ИС ДЛ выпущенного сертификата.

Центр Статистики

Программный компонент «Центр статистики» представляет собой дополнительный компонент из состава программного комплекса ПК «КриптоПро РКІ-Кластер». Сервис статистики осуществляет сбор и обработку информации о действиях с сертификатами ключей проверки ЭП (далее — сертификатах), полученной в процессе работы ПК «КриптоПро РКІ-Кластер».

Основные функции Центра статистики

- отображение сводной информации о количестве созданных/аннулированных сертификатов и зарегистрированных в УЦ лиц
- фильтрация и сортировка данных по различным критериям - по дате, субъекту, типу владельца, точке выдачи, причине отзыва
- отображение информации на карте России с привязкой к точкам выдачи сертификатов.

