Программа для работы с электронной подписью

«КриптоДокумент 2.0»

Описание программы

RU.04442686.62.01.29-01 13 01

Листов **7**

г. Москва
2020 г.

КриптоДок 2.0: Описание программы.

Оглавление

Определения, обозначения и сокращения

Термин	Определение
Криптопровайдер	Независимый модуль, позволяющий осуществлять криптографические операции в операционных системах пользователя.
Демон	Фоновый процесс, выполняемый на компьютере пользователя
Сертификат	Сертификат ключа проверки электронной подписи, или просто сертификат – 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.
Контейнер (сертификата)	Хранилище на компьютере пользователя, которое содержит открытую и закрытую часть ключа
PKCS11	Один из стандартов семейства Public-Key Cryptography Standards (PKCS). Он определяет платформонезависимый программный интерфейс доступа к криптографическим устройствам (смарткартам, токенам, серверам ключей и другим средствам криптографической защиты информации).
JSON	Текстовый формат обмена данными, основанный на JavaScript
WSS	URI-схема шифрованного соединения WebSocket
BASE64	Стандарт кодирования двоичных данных при помощи только 64 символов ASCII

Общие сведения

Полное наименование программы — программа для работы с электронной подписью «КриптоДокумент 2.0».

Условное обозначение программы — «КриптоДокумент»

Программа написана на языке Java и предназначена для работы под управлением операционной системы MS Windows.

Программа не выполняет криптографические операции самостоятельно. Для реализации функций работы с электронной подписью необходимо:
- функции работы контейнером электронной подписи: установка на компьютере пользователя локально установленного крипто провайдера из списка поддерживаемых.
- функции выполнения операций подписания, шифрования и дешифрования данных: доступ к веб-порталу удостоверяющего центра.

Функциональное назначение

Приложение позволяет получить простой и быстрый способ выпуска и применения электронных подписей (подписание документа ЭП, шифрование/дешифрование с применением сертификата ЭП).

Приложение самостоятельно не выполняет никаких криптографические операции и служит проводником между пользователем и локально установленными на компьютер пользователя крипто провайдерами. При взаимодействии с крипто провайдерами используется их программный интерфейс приложения (API), предусмотренный производителем средств криптографии.

Функции программы:

1. сопровождение процесса выпуска электронной подписи
2. сопровождение процесса подписания, шифрования и дешифрования документов/файлов

Сопровождение процесса выпуска электронной подписи представляет собой автоматизацию комплекса операций в составе:

- передача команд в локально установленный крипто провайдер для генерации закрытой части ключа,

- передача команд локально установленному крипто провайдеру по формированию запроса на сертификат ключа проверки ЭП,

- передачи запроса на сертификат на специализированный портал удостоверяющего центра для приема заявок на выпуск

- получение со специализированного портала УЦ готового сертификата

- передача команды локальному крипто провайдеру на запись сертификата ключа проверки ЭП с предварительной проверкой соответствия сертификата закрытой части ключа.

Сопровождение процесса подписания, шифрования/дешифрования документов/файлов представляет собой автоматизацию операций:

- передача на веб-портал удостоверяющего центра документа для подписания/шифрования/дешифрования,

- передача команд между веб-порталом удостоверяющего центра и локальным крипто провайдером в процессе выполнения криптографических операций

Описание работы программы

При запуске приложение разворачивает на ПК пользователя WebSocket-сервер и принимает WebSocket-подключения по адресу wss://localhost:90. Приложение работает как фоновый процесс в системе пользователя и управляет операциями с помощью команд, получаемых на указанный адрес.

Приложение имеет два интерфейса работы:

- программный интерфейс (REST API): основной режим работы приложения. Вызов функций приложения производится обращением на WebSocket. Взаимодействие с пользователем осуществляется с помощью всплывающих окон для подтверждения определенных действий.

- графический пользовательский интерфейс: дополнительный режим работы, позволяющий пользователю интерактивно вызывать функции:

- вызвать сервис подписания документов

- вызвать сервис шифрования документов

- вызвать сервис расшифровки документов

- зарегистрировать приложение

- проверить наличие обновления программы.

Функция вызова сервиса подписания документов встраивается в контекстное меню работы с файлами операционной системы.

Приложение имеет мастер установки. В процессе установки приложения добавляются необходимые корневые и промежуточные сертификаты в хранилища пользователя, чтобы обеспечить доверенное wss-соединение.

Обращения к wss-порту предполагаются только из браузера, с домена crm.uc-itcom.ru, вследствие чего приложение ограничивает входящие подключения, не имеющие соответствующего заголовка Host.

Для безопасности пользователя отправка команд приложению происходит в рамках сессии, согласие на открытие которой дает пользователь. Это реализовано в виде всплывающего GUI-окна с предупреждением о том, что открывается сессия работы с локальным криптопровайдером. В тексте предупреждения указано, что в текущий момент должен быть открыт браузер на странице, адрес которой начинается на https://crm.uc-itcom.ru. В случае отказа пользователя, дальнейшие запросы не выполняются. В случае согласия, последующие запросы, до момента закрытия сессии, обрабатываются без дополнительных предупреждений.

Запрос формируется в виде JSON-объекта. В объекте есть атрибут action, в котором содержится команда, и content, который содержит дополнительную информацию, необходимую для выполнения команды, зависящую от конкретной команды

Перечень команд, которые выполняются Приложением:

Команда	Параметры	Описание
IS_CP_INSTALLED	Нет	Возвращает информацию о том,

		установлен ли на компьютере криптопровайдер
GET_CP_VERSION	Нет	Возвращает версию криптопровайдера
GET_VERSION	Нет	Возвращает текущую версию приложения. Единственная команда, которую можно вызывать вне сессии
SESSION_START	Нет	Начать сессию команд
SESSION_END	Нет	Завершить сессию команд
WRITE_CERTIFICATE	**containerName** – имя контейнера, в который нужно записать сертификат **certificate** – BASE64-содержимое сертификата	Записать выпущенный PKCS-сертификат в контейнер, содержащий закрытую часть
GENERATE_REQUEST	content – содержимое сертификата	Сгенерировать PKCS-запрос на сертификат в формате *.req-файла
GET_CONTAINERS	Нет	Получить список контейнеров, доступных на компьютере пользователя
GET_CONTAINERS_CERTIFICATES_INFO	Нет	Получить список контейнеров, доступных на компьютере пользователя, с расширенной информацией о сертификатах
SIGN_DATA_BY_CONTAINER	**containerName** – имя контейнера используемого сертификата **detached** – признак, указывающий, генерировать ли открепленную подпись	Подписать данные сертификатом из указанного контейнера

	dataToSign - BASE64-содержимое для подписи **checkReject** – признак, указывающий, проводить ли проверку на отозванность сертификата	
SIGN_DATA	**message** – сообщение, которое будет показано пользователю в окне выбора сертификата **detached** – признак, указывающий, генерировать ли открепленную подпись **dataToSign** - BASE64-содержимое для подписи **checkReject** – признак, указывающий, проводить ли проверку на отозванность сертификата	Подписать данные сертификатом, выбранным пользователем
GET_CERTIFICATE_INFO	**content** – имя контейнера	Получить информацию о сертификате в контейнере

Используемые технические средства

В процессе работы программа использует следующие сторонние технические средства:

- операционная система пользователя

- локально установленные криптопровайдеры

- локально установленный веб-браузер (программа просмотра веб-страниц)

- веб-портал удостоверяющего центра

Программа работает в среде операционных систем Microsoft Windows версии не ниже Window 7.

Список поддерживаемых криптопровайдеров:

- КриптоПро
- КриптоПро с использованием ГОСТ Р 34.10-2012
- JaCarta

- Рутокен ГОСТ
- Vipnet
- Esmart ГОСТ

Ресурсы веб-портала удостоверяющего центра:

- Сервис подписания документов электронной подписью по алгоритму ГОСТ Р 34.10-2012
- Сервис шифрования документов на сертификат электронной подписи по алгоритму ГОСТ Р 34.10-2012
- Сервис расшифровки документа по алгоритму ГОСТ Р 34.10-2012

Установка и запуск программы

Программа имеет пакет установки.

При установке приложения выполняются операции:

- копирование исполняемого файла приложения
- копирование файлов среды выполнения Java
- установка в локальное хранилище сертификатов необходимых для работы программы сертификаты корневых и промежуточных удостоверяющих центров
- настройка автоматического запуска приложения при старте операционной системы (копирование ярлыка в папку автозагрузки пользователя)

Загрузка/запуск программы осуществляется запуском исполняемого файла вручную или автоматически при старте операционной системы.