Программа для работы с электронной подписью
«КриптоДокумент 2.0»

Руководство программиста

RU.04442686.62.01.29-01 33 01

Листов **3**

г. Москва
2020 г.

КриптоДок 2.0: Руководство программиста.

Оглавление

Функциональное назначение 2

Описание интерфейса HTTP API 2

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.

Описание интерфейса HTTP API

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 адресПодписание документа электронной подписью

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 доступных команд:

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	Записать выпущенный PKCS-сертификат в контейнер, содержащий закрытую часть

	certificate – BASE64-содержимое сертификата	
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 откреплённую подпись **dataToSign** - BASE64-содержимое для подписи **checkReject** – признак, указывающий, проводить ли проверку на отозванность сертификата	Подписать данные сертификатом из указанного контейнера
SIGN_DATA	**message** – сообщение, которое будет показано пользователю в окне выбора сертификата **detached** – признак, указывающий, генерировать ли откреплённую 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