

ViPNet PKI Client

Руководство разработчика

Версия продукта 2.1.1

О документе

Документ описывает SDK — комплект средств разработки на JavaScript, входящий в состав ViPNet PKI Client. SDK позволяет встраивать в веб-приложения вызовы криптографических операций, которые будут выполняться средствами ViPNet PKI Client. Подробное описание работы SDK см. в архиве `ViPNet PKI Client Web Unit SDK.zip (Windows)` или `ViPNet PKI Client Web Unit SDK.tar.gz (Linux)`.

Документ предназначен для разработчиков веб-приложений. Предполагается, что разработчики знакомы с JavaScript, имеют базовые представления о криптографии и инфраструктуре открытых ключей (PKI).

Назначение SDK

Стандартные браузеры не поддерживают выполнение в веб-приложениях криптографических операций по алгоритмам ГОСТ. SDK позволяет встраивать в веб-приложения вызовы следующих криптографических операций:

- создание запросов на сертификаты и установка сертификатов в хранилище;
- создание ЭП по ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012;
- проверка ЭП по ГОСТ Р 34.10-2001 с вычислением хэш-функции по ГОСТ Р 34.11-94 и ГОСТ Р 34.10-2012 с вычислением хэш-функции по ГОСТ Р 34.11-2012;
- шифрование файлов по ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) «Магма» и «Кузнечик».

Пользователи таких веб-приложений смогут выполнять данные криптографические операции на своих компьютерах, на которых установлен Web Unit из состава ViPNet PKI Client.

Выполнение криптоопераций с помощью Web Unit

Чтобы пользователи могли выполнять криптографические операции на своих компьютерах, на которых установлен Web Unit из состава ViPNet PKI Client:

- Создайте веб-приложение, которое обращается к Web Unit с помощью JavaScript-функций из SDK.
- Разместите веб-приложение на портале и предоставьте пользователям доступ к этому portalу.

Порядок работы пользователя с веб-приложением:

- 1 Пользователь в браузере переходит на страницу веб-приложения.
- 2 Пользователь в веб-приложении вызывает криптографическую операцию. При этом браузер обращается к Web Unit на компьютере пользователя.

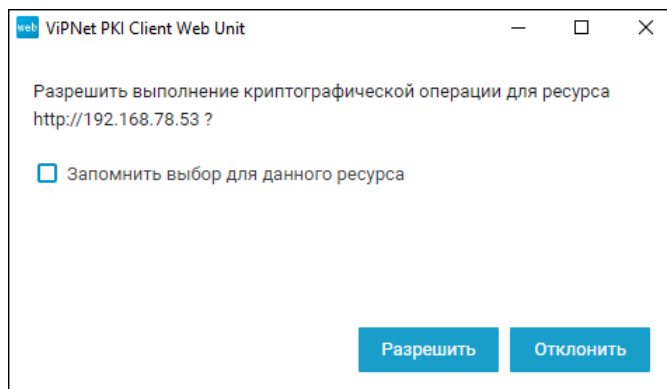
- 3 Web Unit запрашивает у пользователя параметры, необходимые для выполнения криптографической операции.
- 4 Web Unit передает полученный результат в браузер.
- 5 Браузер передает полученный результат на портал.

Автоматическое выполнение криптоопераций

С помощью SDK можно организовать выполнение криптографических операций в веб-приложении автоматически, без демонстрации графического интерфейса. Для этого предназначен режим «Без подтверждения» (`bypassMode`).

Особенности режима «Без подтверждения»:

- При первом вызове операции пользователю потребуется разрешить ее автоматическое выполнение. Чтобы далее операции выполнялись без демонстрации графического интерфейса, нужно выбрать **Запомнить выбор для данного ресурса**.



- Может открываться окно с запросом пароля к контейнеру ключей, соответствующему выбранному сертификату.
- Если веб-приложение при обращении к Web Unit не указывает свой IP-адрес, операция автоматически будет отклоняться.
- Операции создания запроса на сертификат (`generateCertificateRequest`) и установка сертификата в хранилище (`installCertificateIssuedByRequest`) не поддерживаются.
- Для ряда операций предварительно необходимо выбрать сертификат подписи (`selectCertificate` или `getCertificateList`), а именно: `sign`, `signFile`, `signAndEncrypt`, `signXml`, `specialSign01`, `specialSignFile`, `specialSignHash`.

Использование примеров и функций из SDK

Для работы с SDK установите ViPNet PKI Client — см. «Руководство пользователя» или «Руководство пользователя».

При установке ViPNet PKI Client на компьютер копируются примеры веб-приложений и JavaScript-функции, которые вы можете использовать при разработке своих веб-приложений:

- [Пример вызовов криптографических операций с бинарными данными на входе.](#)
- [Пример вызовов криптографических операций с файлами на входе.](#)

Пример вызовов криптоопераций с бинарными данными на входе

Пример представляет собой веб-приложение, в котором можно вызывать криптографические функции. В качестве входных параметров для функций используются бинарные данные в формате Base64. Для конвертации сертификата в формат Base64 можно воспользоваться [онлайн-конвертером](#).

Расположение примера и JavaScript-функций по умолчанию

ОС	Путь к каталогу с примером
Windows 32-разрядная	C:\Program Files\InfoTeCS\ViPNet PKI Client\sdk\webunit\examples\Base64DataOnly
Windows 64-разрядная	C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\sdk\webunit\examples\Base64DataOnly
Linux	/opt/itcs/share/pki-client/pki-client-web-unit-sdk/examples/Base64DataOnly

Пример вызовов криптоопераций с файлами на входе

Пример представляет собой веб-приложение, в котором можно вызывать криптографические функции, требующие в качестве входных данных файлы.

Для Windows в демонстрационных целях работа с файлами реализована с помощью тестового файл-сервера. Программу тестового файл-сервера необходимо запустить на компьютере разработчика после установки ViPNet PKI Client. Она работает в фоновом режиме.



Примечание. При организации работы пользователей с файлами расположите файл-сервер на удаленном веб-сервере.

Порядок работы с файлами в примере:

- 1 Пользователь в тестовом веб-приложении указывает путь к файлу, для которого требуется выполнить криптографическую операцию, и вызывает эту операцию. При этом браузер передает в Web Unit на компьютере пользователя содержимое файла в формате Base64.
- 2 Web Unit передает полученный результат в виде данных в формате Base64 в браузер.
- 3 В Windows браузер передает полученные данные тестовому файл-серверу.
- 4 В Windows тестовый файл-сервер преобразует полученные данные в файл и передает ссылку на этот файл в браузер. Браузер автоматически скачивает файл.

Расположение примера, JavaScript-функций и тестового файла по умолчанию

ОС	Пути к каталогам с примером и тестовым файлом
Windows 32-разрядная	Пример для файлов размером до 100 МБайт — C:\Program Files\InfoTeCS\ViPNet PKI Client\sdk\webunit\examples\WithFiles Пример для файлов размером более 80 МБайт — C:\Program Files\InfoTeCS\ViPNet PKI Client\sdk\webunit\examples\BigFiles Тестовый файл-сервер — C:\Program Files\InfoTeCS\ViPNet PKI Client\sdk

ОС	Пути к каталогам с примером и тестовым файлом
Windows 64-разрядная	Пример для файлов размером до 100 МБайт — C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\sdk\webunit\examples\WithFiles Пример для файлов размером более 80 МБайт — C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\sdk\webunit\examples\BigFiles Тестовый файл-сервер — C:\Program Files (x86)\InfoTeCS\ViPNet PKI Client\sdk
Linux	Пример для файлов размером до 100 МБайт — /opt/itcs/share/pki-client/pki-client-web-unit-sdk/examples/WithFiles Пример для файлов размером более 80 МБайт — /opt/itcs/share/pki-client/pki-client-web-unit-sdk/examples/BigFiles

Возможные неполадки

Не удастся выбрать сертификат для подписи файла

Если при подписании файла список сертификатов пуст, убедитесь:

- что сертификат действителен;
- сертификат установлен в категорию **Личные сертификаты**;
- сертификат содержит расширение **Использование ключа** со значением **Цифровая подпись**.

Ошибка отправки файла при работе по HTTPS

Для выполнения криптографических операций при установленном HTTPS-соединении в Web Unit используется самоподписанный сертификат, который автоматически создается и устанавливается в хранилище при установке ViPNet PKI Client. Если срок действия этого сертификата истек, после установления HTTPS-соединения при попытке выполнения криптографической операции возникает ошибка **Не удалось отправить файл на файл-сервер**.

Переустановите ViPNet PKI Client.

Ошибка при подключении по HTTPS в Firefox

Если в Firefox при подключении по адресу `https://127.0.0.1:61112/` или `https://127.0.0.1:62223/` появляется предупреждение о вероятной угрозе безопасности:



Нажмите **Принять риск и продолжить** и продолжите работу.



АО «ИнфоТеКС», 125167, г. Москва, вн. тер. г. муниципальный округ Хорошевский, ул. Викторенко, д. 9, стр. 1, помещ. 47

Телефон: +7 (495) 737-6192, 8 (800) 250-0260 — бесплатный звонок из России (кроме Москвы)

Сайт: infotecs.ru

Служба поддержки: hotline@infotecs.ru, телеграм-канал поддержки: t.me/vhd21

ФРКЕ.00175-03 33 01, версия продукта 2.1.1

© АО «ИнфоТеКС», 2025. ViPNet[®] является зарегистрированным товарным знаком АО «ИнфоТеКС».

Все названия компаний и продуктов, являющиеся зарегистрированными товарными знаками, принадлежат соответствующим владельцам.