Рутокен Коннект. Пример встраивания клиентской части

Для успешного соединения требуется выполнение следующих условий:

№	условие	как выполнить
0	убедиться, что ОС и браузер подходят для работы Рутокен Коннекта	через USERAgent браузера
1	установить Рутокен Коннект	установка руками пользователя
2	убедиться, что Рутокен Коннект активирован	через функцию Рутокен Коннекта
3	установить Рутокен Плагин	установка руками пользователя
4	убедиться, что Рутокен Плагин активирован	через функцию Рутокен Плагина
5	проверить наличие подключенного устройства семейства Рутокена ЭЦП	через функцию Рутокен Плагина
6	ввести PIN-код пользователя Рутокена ЭЦП	через функцию Рутокен Плагина
7	проверить наличие корректного личного сертификата на Рутокене	через функцию Рутокен Плагина
8	перенаправить пользователя на защищенный ресурс	ссылкой или через redirect

0. Определяем окружение для корректной работы Рутокен Коннекта

Используем User-agent для поиска условий указанных в описании продукта.

Если условия не соответствуют следует показать пользователю сообщение с просьбой использовать подходящую для Рутокен Коннекта платформу и окружение.

1. Установка Рутокен Коннекта

По ссылке на сайте производителя либо на собственном сайте.

Если использовать ссылку на сайте производителя, то не нужно беспокоиться об обновлении версий, так как эту заботу берет на себя сам производитель.

Используя ссылку на собственном сайте, вы избегаете лишних переходов на сторонние сайты, но должны самостоятельно отслеживать обновления программного обеспечения.

2. Убеждаемся, что Рутокен Коннект активирован

Функции:

- isExtensionInstalled() -> Promise(bool)
- isPluginInstalled() -> Promise(bool)

Должны вернуть true.

Если одна из функций или обе вернули false - необходимо вернуться к пункту 1.

3. Установка Рутокен Плагин

По ссылке на сайте производителя либо на собственном сайте.

Если использовать ссылку на сайте производителя, то не нужно беспокоиться об обновлении версий, так как эту заботу берет на себя сам производитель.

Используя ссылку на собственном сайте, вы избегаете лишних переходов на сторонние сайты, но должны самостоятельно отслеживать обновления программного обеспечения

4. Убеждаемся что Рутокен Плагин активирован

Функции:

- isExtensionInstalled() -> Promise(bool)
- isPluginInstalled() -> Promise(bool)

Должны вернуть true.

Если одна из функций или обе вернули false - необходимо вернуться к пункту 3.

5. Проверяем наличие подключенного Рутокена ЭЦП

Устройства семейств Рутокен S, Lite и PKI не поддерживаются.

Рутокен Коннект работает только с устройствами семейства Рутокен ЭЦП с поддержкой аппаратной ГОСТ-криптографии, поэтому отсутствие подходящего устройства не даст возможности подключиться к защищенному серверу через Рутокен Коннект.

Функция enumerateDevices(options) → {number[]} возвращает список подключенных устройств.

Функция getDeviceInfo(deviceId, option) → {object} может вернуть модель устройства (option - TOKEN_INFO_MODEL).

Необходимо убедиться, что подключенное устройство не принадлежит к семейству Рутокен Lite, так как с ним работа Рутокен Коннекта невозможна.

Если ваш защищенный сервер работает по шифрсьютам основанным на алгоритмах электронной подписи 2012 года, то дополнительно нужно убедиться что подключенное устройство поддерживает работу по новым алгоритмам

Код:

```
var options = plugin.TOKEN_INFO_SUPPORTED_MECHANISMS;

function isRt20() {

	plugin.getDeviceInfo(deviceId, options).then(function(results) {

		return results.indexOf(plugin.PUBLIC_KEY_ALGORITHM_GOST3410_2012_256) !== -1 || results.indexOf(plugin.
PUBLIC_KEY_ALGORITHM_GOST3410_2012_512) !== -1;

	});

}
```

вернет 2, если подключенное устройство Рутокен поддерживает алгоритмы электронной подписи 2012 года.

Если подключенного устройства нет, или оно неподходящее, то пользователю следует показать предупреждение с просьбой подключить подходящее устройство и повторить пункт 6.

6. Вводим PIN-код от устройства Рутокен ЭЦП

Перед проверкой сертификатов хранящихся на Рутокене ЭЦП необходимо авторизоваться на устройстве. Без авторизации перечисление сертификатов и закрытых ключей невозможно.

Функция login(deviceId, pin) принимает PIN-код пользователя, который необходимо принять с помощью специального окна или поля ввода.

Если функция бросает исключение значит PIN-код неверный и следует сообщить об этом пользователю и повторить пункт 7.

Важно понимать, что пользователь может исчерпать попытки ввода неправильного PIN-кода и заблокировать этот PIN-код. В этом случае тоже нужно сообщить пользователю об этой ситуации.

Количество оставшихся попыток ввода PIN-кода возвращает функция getDeviceInfo(deviceId, option) → {object} с option TOKEN_INFO_PIN_RETRIES_LEFT.

Если их станет меньше 1 - значит PIN-код заблокирован и пользователю следует обратиться к администратору для разблокировки PIN-кода.

7. Проверяем наличие подходящего личного сертификата на Рутокене ЭЦП

Список сертификатов с соответствующими им закрытыми ключами возвращает функция enumerateCertificates(deviceId, category) → {string[]}

Тело сертификата (каждого по отдельности) можно получить функцией getCertificate(deviceId, certId) → {string}

Среди обнаруженных на Рутокене сертификатов необходимо найти соответствующий требованиям защищенного сервера вашей информационной системы.

Если среди обнаруженных сертификатов не оказалось подходящего, либо Рутокен пуст, следует сообщить пользователю, что необходимый для подключения сертификат не найден и ему необходимо его получить установленным для вашей информационной системы способом.

8. Перенаправляем пользователя на защищенный ресурс

Необходимо дать возможность пользователю нажать на кнопку или ссылку для перехода на защищенный ресурс вашей информационной системы либо автоматически его редиректить.