

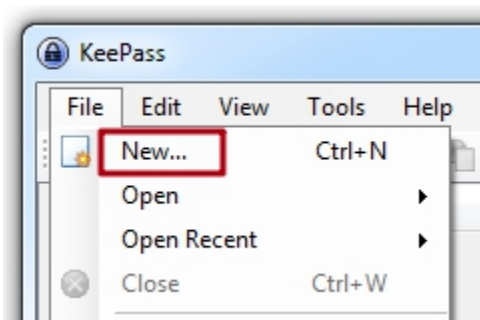
Интеграция Рутокен и KeePass

- [Вариант 1: Использование защищенного PIN-кодом пароля с ключевого носителя.](#)
- [Вариант 2: Использование RSA сертификата с ключевого носителя.](#)
- [Вариант 3: Шифрование локального ключевого контейнера сертификатом с ключевого носителя.](#)
- [Работа с базой KeePass из браузера Google Chrome](#)
- [Работа с базой KeePass из браузера Mozilla Firefox](#)

Вариант 1: Использование защищенного PIN-кодом пароля с ключевого носителя.

Возможно использование электронных идентификаторов Рутокен Lite, Рутокен ЕСР.

1. Скачать и установить KeePass версии старше 2.09:
<http://keepass.info/download.html>
2. Скачать и переместить в папку <KeePassInstallDir>/Plugins/ официальный плагин CryptokiKeyProvider.plgx:
<https://implygy.de/CryptokiKeyProvider/#download>
3. Скачать библиотеку PKCS#11:
<https://www.rutoken.ru/support/download/pkcs/>
4. Подключить устройство Рутокен.
 - а. Открыть KeePass и создать новую базу ключей. В открывшееся окно ввести имя файла, выбрать место для хранения и нажать Сохранить.



5. В следующем окне выбрать плагин CryptokiKeyProvider в качестве криптопровайдера, отключить галку **Master password** и нажать **OK**.

Create Composite Master Key

 **Create Composite Master Key**
C:\Users\Iazarev\Desktop\testdb.kdbx

Specify the composite master key, which will be used to encrypt the database.

A composite master key consists of one or more of the following key sources. All sources you specify will be required to open the database. If you lose one source, you will not be able to open the database anymore.

☐ **Master password:** 

Repeat password:

Estimated quality: 0 ch.

☒ Show expert options:

☒ **Key file / provider:**

 Create...  Browse...

A key file can be used as part of the master key; it does not store any database data. If an attacker has access to the key file, it does not provide any protection.

 If the key file is lost or its contents are changed, the database cannot be opened anymore. You should create a backup of the key file.

[More information about key files.](#)

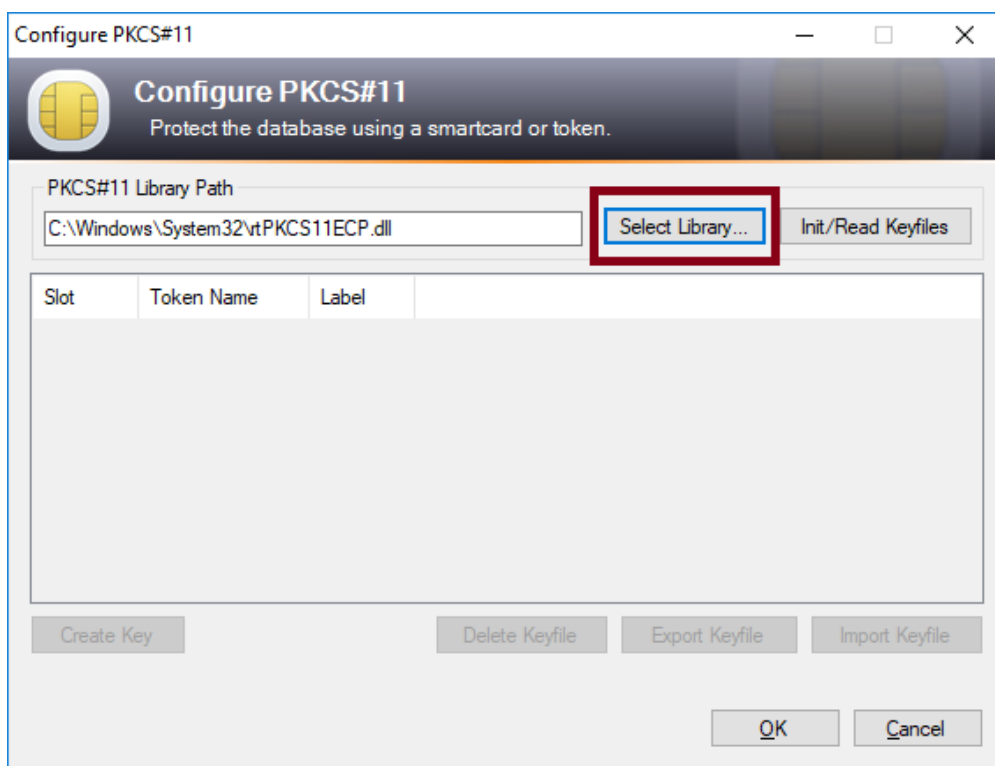
☐ **Windows user account**

This source uses data of the current Windows user account. This data does not change when the account password changes.

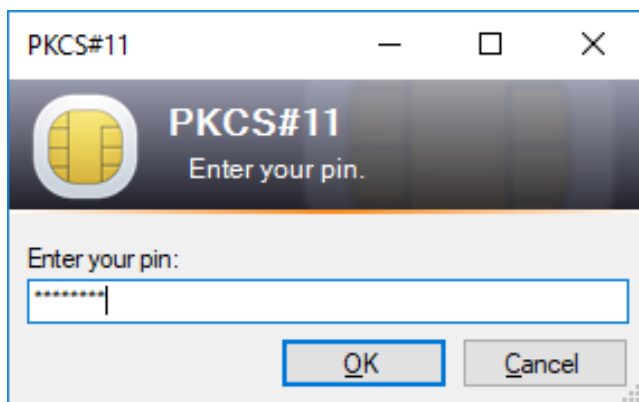
 If the Windows user account is lost, it will not be enough to create a new account with the same user name and password. A complete backup of the account is required. Creating and restoring such a backup is a very complicated task. If you don't know how to do this, don't enable this option.

[More information about Windows user accounts.](#)

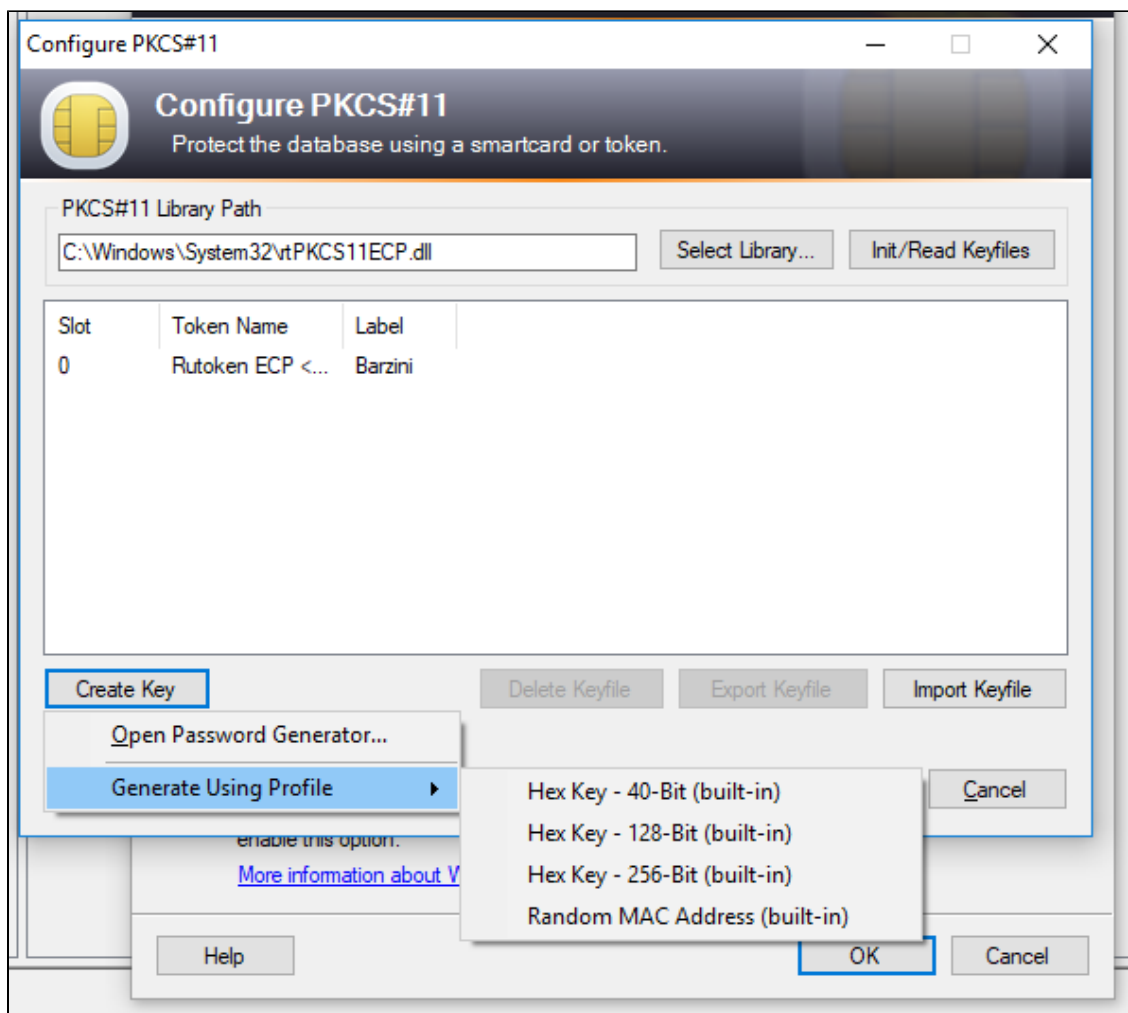
7. В следующем окне нажать **Select Library...** и выбрать месторасположение библиотеки **rtPKCS11ecp.dll**.



8. Нажать на кнопку **Init/Read KeyFiles** и ввести PIN-код подключенного устройства Рутокен.



9. Если пароли не были сгенерированы ранее, в окне списка паролей нажать кнопку **CreateKey** и сгенерировать пароль через генератор паролей или, выбрав нужный профиль.



10. Выбрать пароль из списка и нажать **ОК**.
11. Ввести PIN-код подключенного устройства РутOKEN в окне ввода PIN-кода.
12. Указать настройки базы данных KeyPass и нажать **ОК**.

Вариант 2: Использование RSA сертификата с ключевого носителя.

Возможно использование электронных идентификаторов РутOKEN S и РутOKEN Lite.

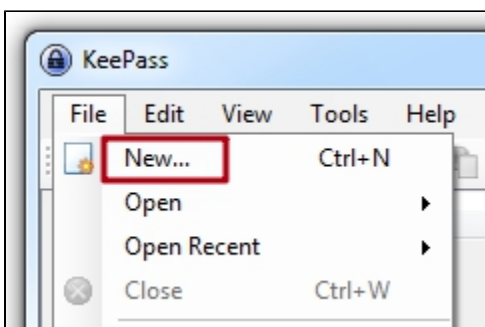
1. Скачать и установить KeePass версии старше 2.09:
<http://keepass.info/download.html>
2. Скачать и переместить в папку KeePass официальный плагин RSACertKeyProviderPlugin:
<http://www.creative-webdesign.de/en/software/keepass-plugins/rsa-cert-keyprovider.html>
3. Сгенерировать **экспортируемую** ключевую пару RSA на РутOKEN и выписать сертификат (можно самоподписанный).

Внимание!

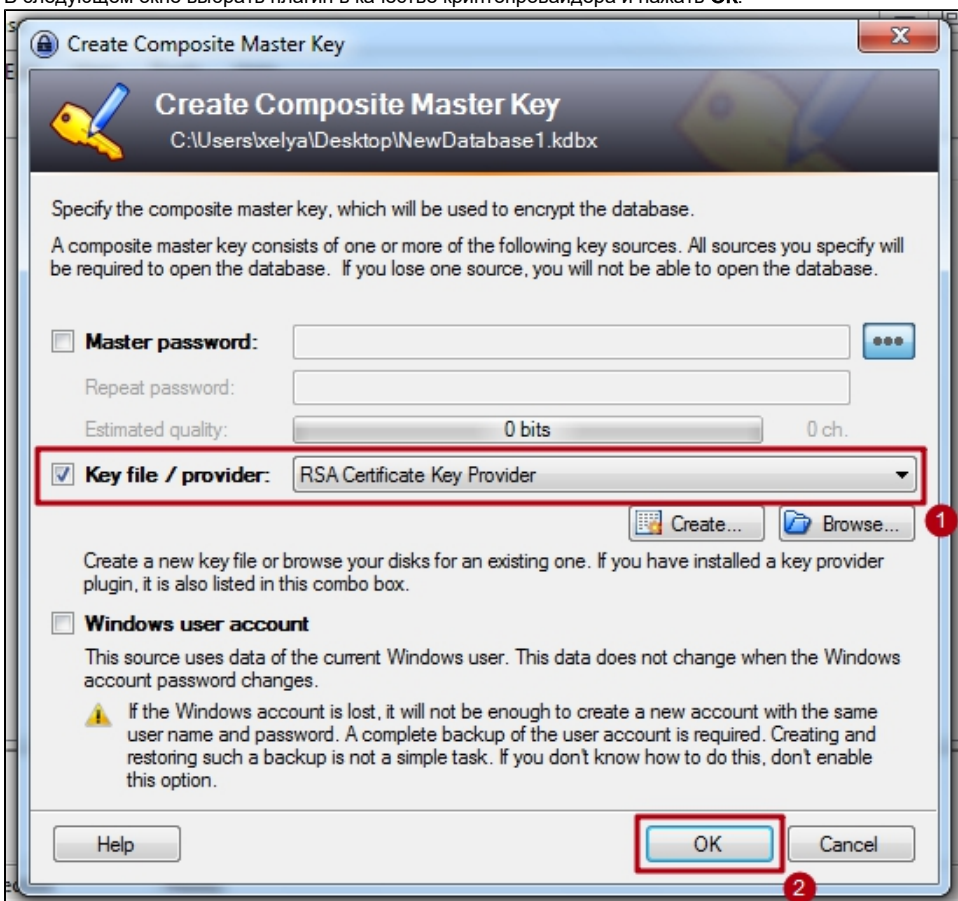


Из-за специфики работы данного плагина для KeePass неэкспортируемые ключевая пара и сертификат не могут быть использованы. Их использование вызовет ошибку, например "Key not valid for use in specified state".

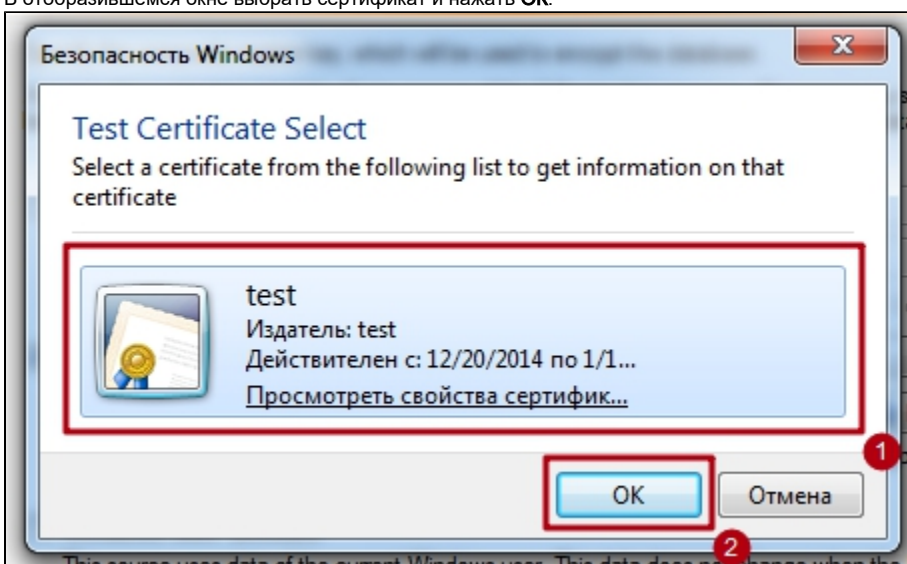
4. Открыть KeePass и создать новую базу ключей. В открывшееся окно ввести имя файла, выбрать место для хранения и нажать **Сохранить**.



5. В следующем окне выбрать плагин в качестве криптопровайдера и нажать **OK**.



6. В отобразившемся окне выбрать сертификат и нажать **ОК**.

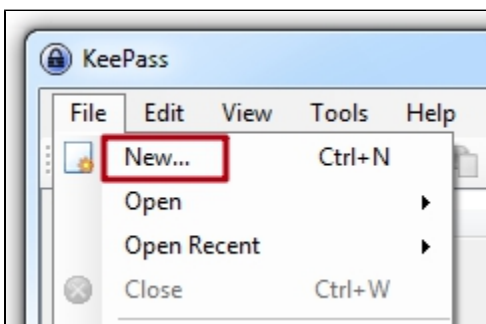


7. Указать настройки базы данных KeyPass и нажать **ОК**.

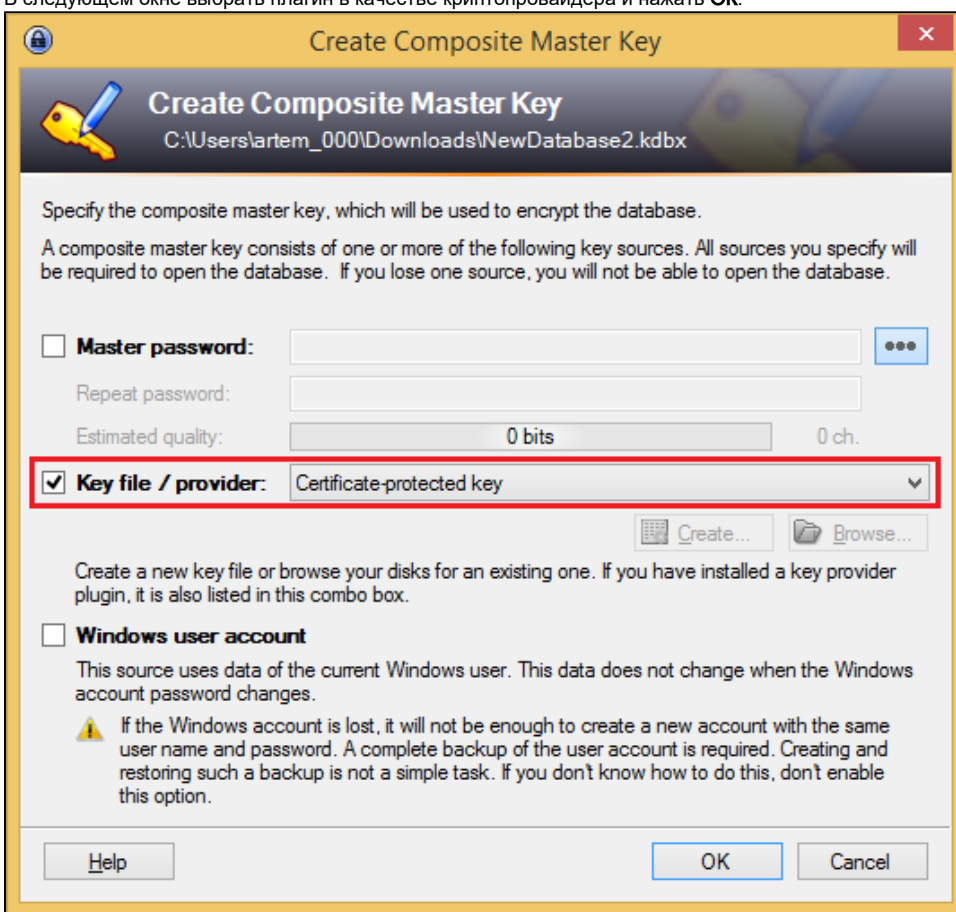
Вариант 3: Шифрование локального ключевого контейнера сертификатом с ключевого носителя.

Возможно использование любых электронных идентификаторов Рутокен.

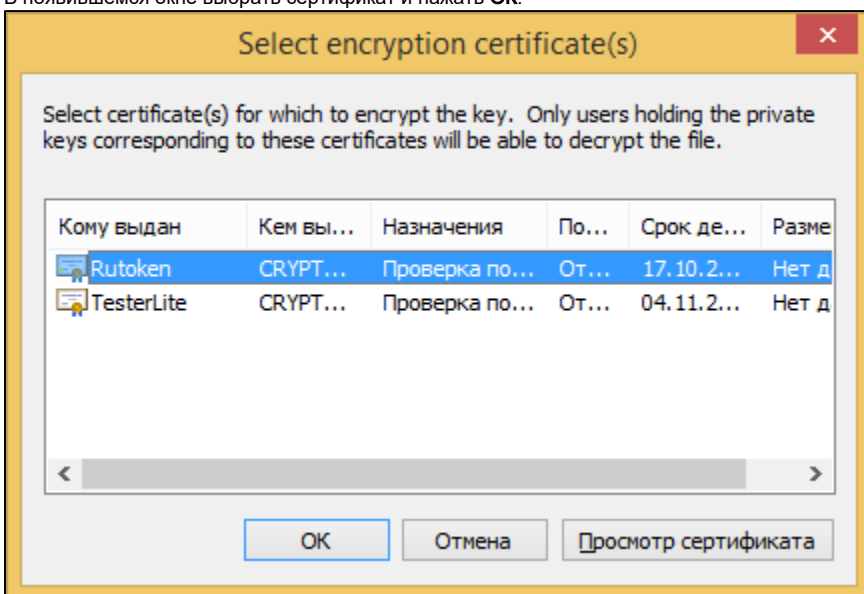
1. Скачать и установить KeePass версии старше 2.09:
<http://keepass.info/download.html>
2. Скачать и переместить в папку KeePass официальный плагин CertKeyProvider:
<https://www.dropbox.com/s/efaeqm88hycybiu/CertKeyProviderPlugin.plgx?dl=0>
3. Сгенерировать ключевую пару RSA на Рутокен и выписать сертификат (можно самоподписанный).
4. Открыть KeePass и создать новую базу ключей. В открывшемся окне ввести имя файла, выбрать место для хранения и нажать **Сохранить**.



5. В следующем окне выбрать плагин в качестве криптопровайдера и нажать **ОК**.



6. В появившемся окне с описанием работы плагина нажать **ОК**.
7. Указать локальное место хранения защищенного ключевого контейнера.
8. В появившемся окне выбрать сертификат и нажать **ОК**.

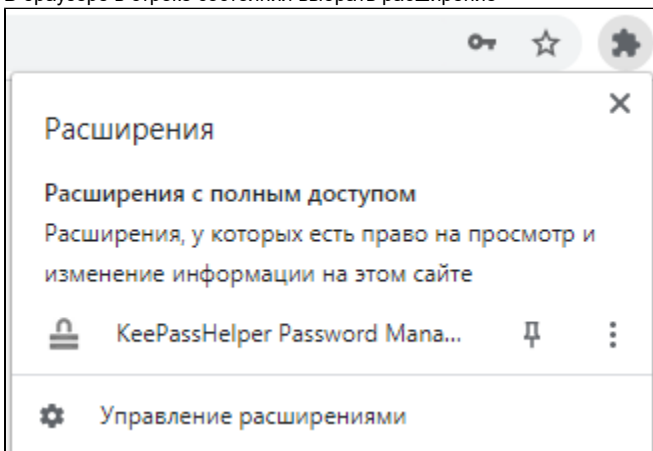


9. В случае отображения предупреждения "The following certificate didn't validate properly", подтвердить использование выбранного сертификата нажатием **ДА**.
10. Указать настройки базы данных KeyPass и нажать **ОК**.

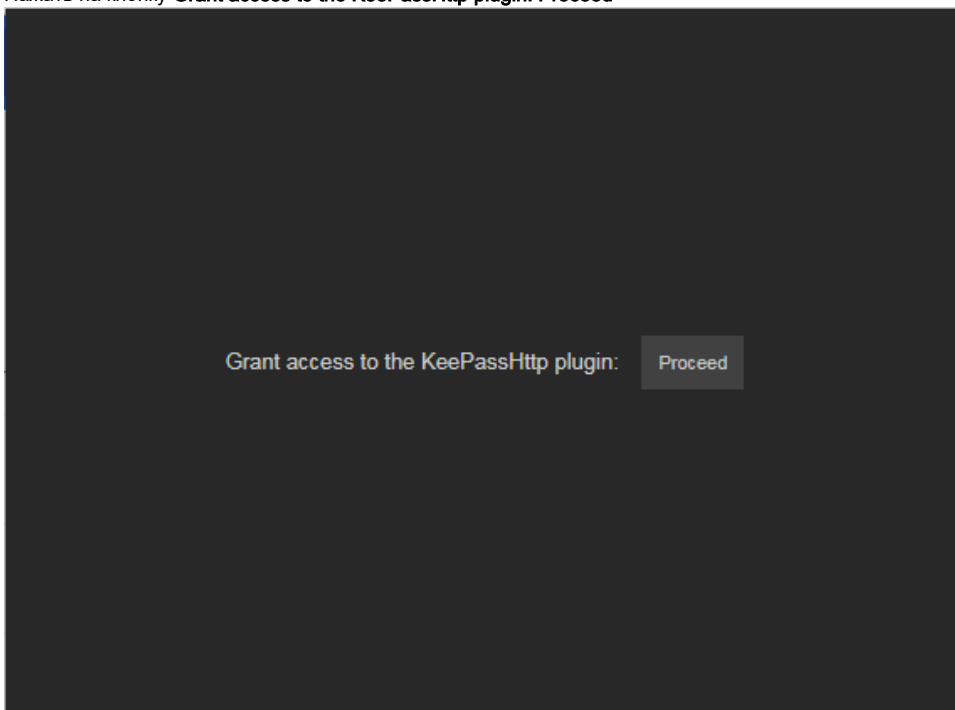
Работа с базой KeePass из браузера Google Chrome

Для работы из браузера Google Chrome необходимо выполнить следующие шаги:

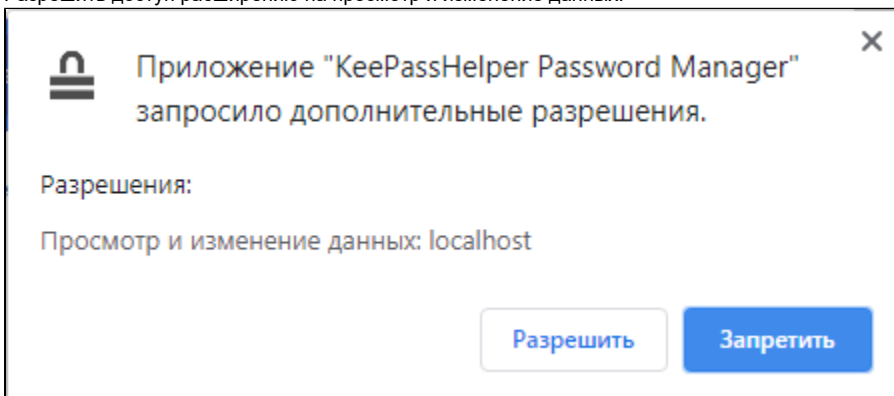
1. Установить расширение браузера:
[KeePassHelper Password Manager](#)
2. Скачать и установить плагин для программы Keypass:
[KeePassHttp](#)
3. В браузере в строке состояния выбрать расширение



4. Нажать на кнопку **Grant access to the KeePassHttp plugin: Proceed**

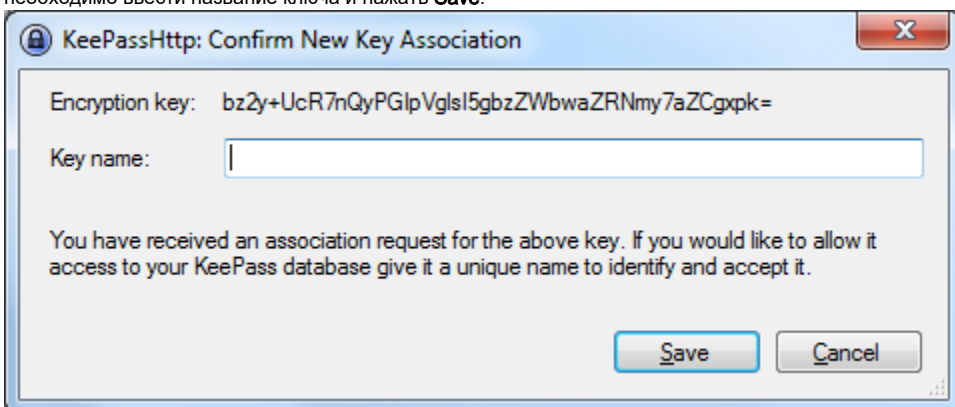


5. Разрешить доступ расширению на просмотр и изменение данных.

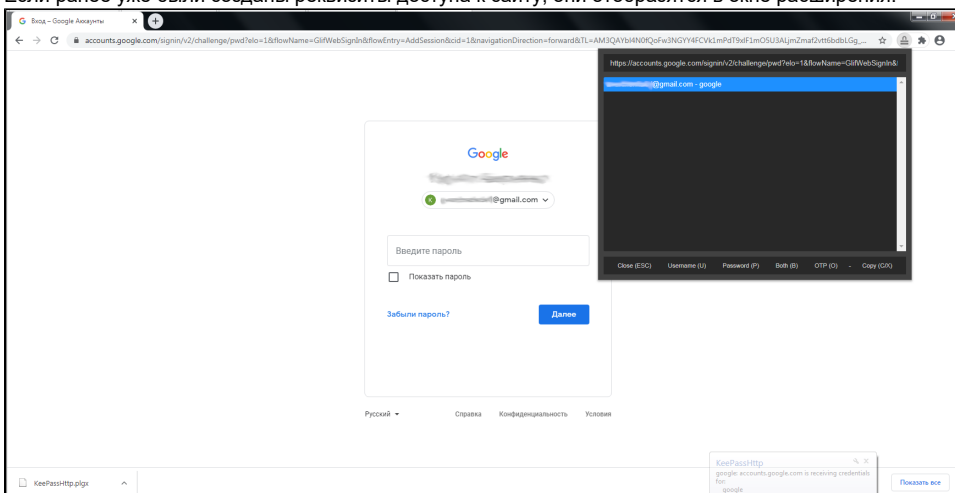


6. Запустить приложение KeePass.

7. При первой попытке синхронизации расширения браузера и локальной базы данных потребуется создать Ключ Ассоциации, для этого необходимо ввести название ключа и нажать **Save**.



8. Если ранее уже были созданы реквизиты доступа к сайту, они отобразятся в окне расширения.

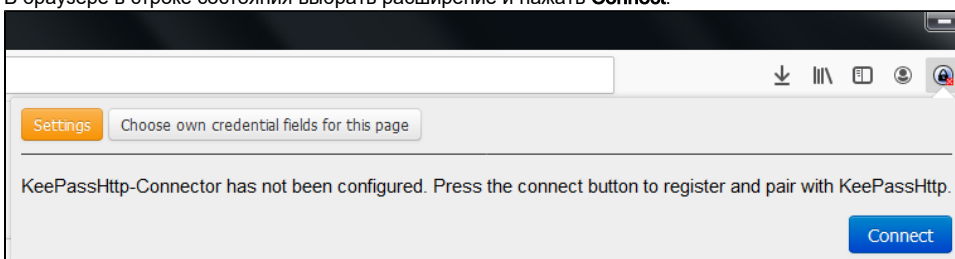


9. После выбора реквизитов доступа они автоматически вставятся в окно входа.

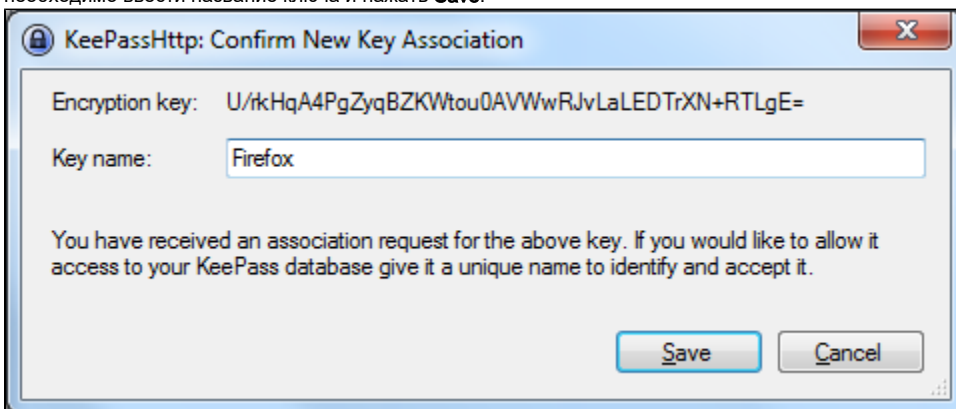
Работа с базой KeePass из браузера Mozilla Firefox

Для работы из браузера Mozilla Firefox необходимо выполнить следующие шаги:

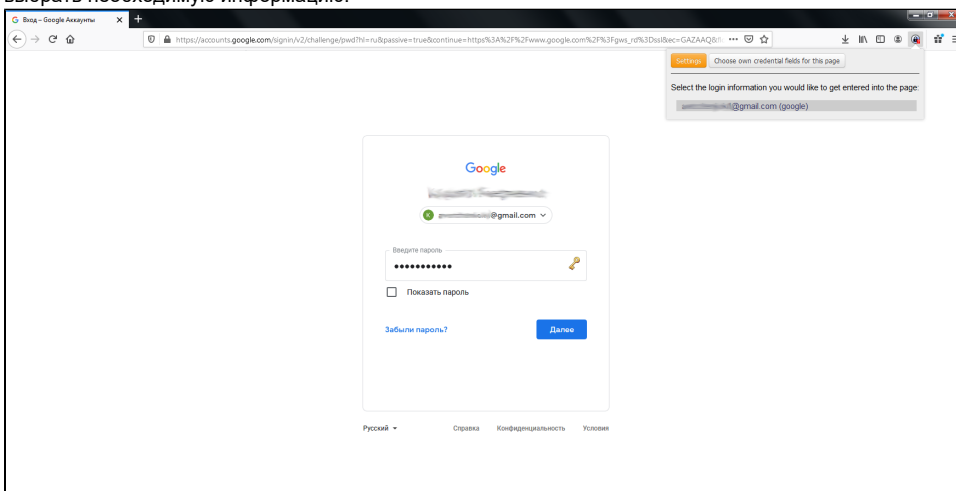
1. Установить расширение браузера:
[KeePassHelper Password Manager](#)
2. Скачать и установить плагин:
[KeePassHttp](#)
3. Запустить приложение KeePass.
4. В браузере в строке состояния выбрать расширение и нажать **Connect**.



5. При первой попытке синхронизации расширения браузера и локальной базы данных потребуется создать Ключ Ассоциации, для этого необходимо ввести название ключа и нажать **Save**.



6. При переходе на сайт, для которого необходимо ввести сохраненные в KeePass данные необходимо нажать на кнопку расширения и выбрать необходимую информацию.



7. После выбора реквизитов доступа они автоматически вставятся в окно входа.