keyon

keyon / PKCS#11 to MS-CAPI Bridge User Guide

V3.0.0

March 2018

Table of contents

Overview

What it is the keyon / PKCS#11 to MS-CAPI Bridge?

keyon / PKCS#11 to MS-CAPI Bridge is a DLL, which provides access to the credentials in the Microsoft Certificate Store over virtual tokens using the PKCS#11 (Cryptoki) API.

Applications such as Microsoft Firefox can thus use certificates and keys available in the Microsoft Certificate Store and the Microsoft CryptoAPI.

Please note that beginning with version 2.4, the product was renamed from *keyon / MS-CAPI Bridge for Mozilla NSS* to *keyon / PKCS#11 to MS-CAPI Bridge* in order to comply with Mozilla trademark policies.

Key Features

- Provides access to keys and certificates in the user's certificate store (MY) for client authentication and secure mail.
- Support RSA keys managed by the standard Crypto API (CAPI) and the Crypto API Next Generation (CNG).
- Supports both soft tokens and Smart Cards. As long as the key is available over the Microsoft CryptoAPI, it can be used from Mozilla NSS based applications. To support a Smart Card, only a cryptographic service provider for Windows is necessary.
- If a PIN is required to use a credential, the PIN entry dialog from the Microsoft CryptoAPI is used.
- Supports SSO if the underlying Smart Card in the CryptoAPI supports it.
- Certificates are added and removed from the virtual token as soon as they are added or removed in the Microsoft Certificate Store. There is no need to restart the application if new certificates become available.
- Access to credentials in the Microsoft Certificate Store is read only, i.e. it is not possible to accidentally delete certificates or keys e.g. in Mozilla Firefox.
- Provides access to certificates in the user's trust store (Root, CA, TrustedPublishers and MY) allowing easy deployment of trusted CAs using the group policy.

Changelog

Version 2.4.4

- Renamed the extension to keyon / PKCS#11 to MS-CAPI Bridge to comply with Mozilla trademark policy
- CA certificates in the user's MY store are now added to the trusted certificates
- Some minor bug fixes in the PKCS#11 implementation
- Flag the extension as compatible with multiprocess Firefox
- Fixes problem with PKCS#11 module not unloaded when updating the extension

Version 3.0.0

- Converted the extension to a web extension as legacy extensions are no longer supported beginning with Firefox 57
- The extension now only registers the PKCS#11 DLLs that must be deployed separately
- Removed the update URL from the extension as it is only used to register the PKCS#11 modules and changes are only expected in the DLLs
- Since the PKCS#11 management API for web extensions was introduced beginning with Firefox 58, the new web extension is only supported on Firefox 58 or higher
- Changed the slot name of the MY trust store to MY (Trust only)
- Changed the serial number of all slots from 00 to an eight character number generated based on the slot name and the name of the logged on user

Installation

The PKCS#11 to MS-CAPI Bridge can be installed as a web extension in XPI form (for download). The PKCS#11 DLLs can also be installed manually by registering them as security modules over the GUI or in the security modules database.

Compatibility

The following types of installation are supported:

Type	Compatibility	Features
Web extension	▪ Firefox 58 or higher	The Add-On can be installed and removed without restarting the application, however **the PKCS#11 DLLs must be installed and registered on the system independently of the web extension** as they cannot be a part of the extension anymore.
Restartless extension	▪ Firefox 4.0 up to 56 ▪ Thunderbird 3.3 or higher ▪ Seamonkey 2.1 or higher	The Add-On can be installed and removed without restarting the application. It is also possible to disable and enable the plugin during runtime.
Manual installation (GUI)	▪ Any Firefox version ▪ Any Thunderbird version ▪ Any Seamonkey version	Needs manual registration of the PKCS#11 ("cryptoki") DLLs in the application or the modules database.
Manual installation (e.g. modutil)	▪ Firefox 4.0 or higher ▪ Any Thunderbird version ▪ Any Seamonkey version	Needs manual registration of the PKCS#11 ("cryptoki") DLLs in the modules database (or the pkcs11.txt in later versions). Can also be used for manual registration in the NSS3 module database and for some other applications that use PKCS#11.

Please make sure you do not install different installation types concurrently in the same application.

Web Extension

Beginning with Firefox version 57, the allowed kind of extensions were have been reduced to web extensions only.

Access to the PKCS#11 management API present in Firefox versions before 57 was removed in version 57 and only a limited, new PKCS#11 management API for use by web extensions was added beginning with Firefox 58.

The following table lists the extension versions supported for the different Firefox versions:

Firefox version	PKCS#11 to MS-CAPI Bridge Extension	Manual installation
≤ 56	≤ 2.4.4	Supported
57	not supported	Supported
≥ 58	≥ 3.0.0	Supported

The PKCS#11 native DLLs along with a JSON manifest and some registry settings are required for the web extension to work. The MSI packages will install the files and configuration settings on the workstation.

The web extension only performs the registration of the PKCS#11 modules in Firefox thus automating the manual installation steps.

Restartless Extension

Beginning with version 3.0.0, the PKCS#11 to MS-CAPI Bridge is no longer provided as a restartless extension.

If you need support for Firefox versions older than 57, please use version 2.4.4 of the PKCS#11 to MS-CAPI Bridge available via keyon support.

Windows Installer packages with the PKCS#11 DLLs

Since web extensions do not allow integrating native code, the PKCS#11 DLLs and the newly required native manifests need to be installed independently of the web extension on the workstation.

Different installer files are provided for 32-Bit and 64-Bit operating systems which include different features. The naming of the installer files is as follows:

`keyon_PKCS#11_to_MS-CAPI_Bridge[_<features>]_<version>_<arch>.msi`

Architecture

Architecture is either `x64` or `x86`. The `x64` package includes the DLLs for both 32-bit and 64-Bit Firefox versions. If you use a 32-Bit Firefox on a 64-Bit Windows system, you can also install the `x86` version though the `x64` package is preferred for 64-Bit operating systems:

	32-Bit		64-Bit	
Arch	Windows	Firefox	Windows	Firefox
x86	●	●	●	
x64		●	●	●

Features

The following features are available:

Feature	Description
empty	Installs the PKCS#11 DLLs, the native manifests and the web extension and registers the extension automatically for use with Firefox as a side-loaded extension.
`no_reg`	Installs the PKCS#11 DLLs, the native manifests and the web extension but does not register the extension in Firefox. The extension must be registered manually or using side-loading.
`P11_only`	Installs the PKCS#11 DLLs only. The web extension will not work with this installation; the DLLs however can be manually configured in Firefox.

The following table summarized the elements installed with each feature:

Feature	DLL	JSON	JSON Reg	XPI	XPI Reg
empty	●	●	●	●	●
`no_reg`	●	●	●	●	
`P11_only`	●				

With the following elements:

Element	Description

DLL	The PKCS#11 DLLs. The DLLs are installed under
	`%ProgramFiles%\keyon\p11capi`
	`%ProgramFiles(x86)%\keyon\p11capi`
	depending on the architecture.

JSON	The native manifest required for a web extension to manage the PKCS#11 module. https://developer.mozilla.org/en-US/Add-ons/WebExtensions/Native_manifests#PKCS_11_manifests
JSON Reg	The registry settings to make the module available for a web extension to manage the PKCS#11 module. https://developer.mozilla.org/en-US/Add-ons/WebExtensions/Native_manifests#Manifest_location
XPI	The web extension file
XPI Reg	The registry settings to automatically register the web extension in Firefox. https://developer.mozilla.org/en-US/Add-ons/WebExtensions/Alternative_distribution_options/Add-ons_in_the_enterprise#Installation_using_the_Windows_registry

It is also possible to use `ADDLOCAL` with `msiexec` to install only a subset of elements with the default package. Please contact keyon for the internal MSI feature names if you want to perform such a custom installation.

Manual installation (GUI)

Compatibility

Application	Version requirements
Firefox	1.0 or higher
Thunderbird	1.0 or higher
Seamonkey	1.0 or higher
Other	Applications based on NSS should be able to use the PKCS#11 library. Other applications capable of using a 32-Bit DLL implementing the PKCS#11 API v2.20 may work as well.

Installing the PKCS#11 libraries in Mozilla Firefox

Depending on the Firefox version, the security devices configuration where PKCS#11 modules are registered may be locates under a different settings page.

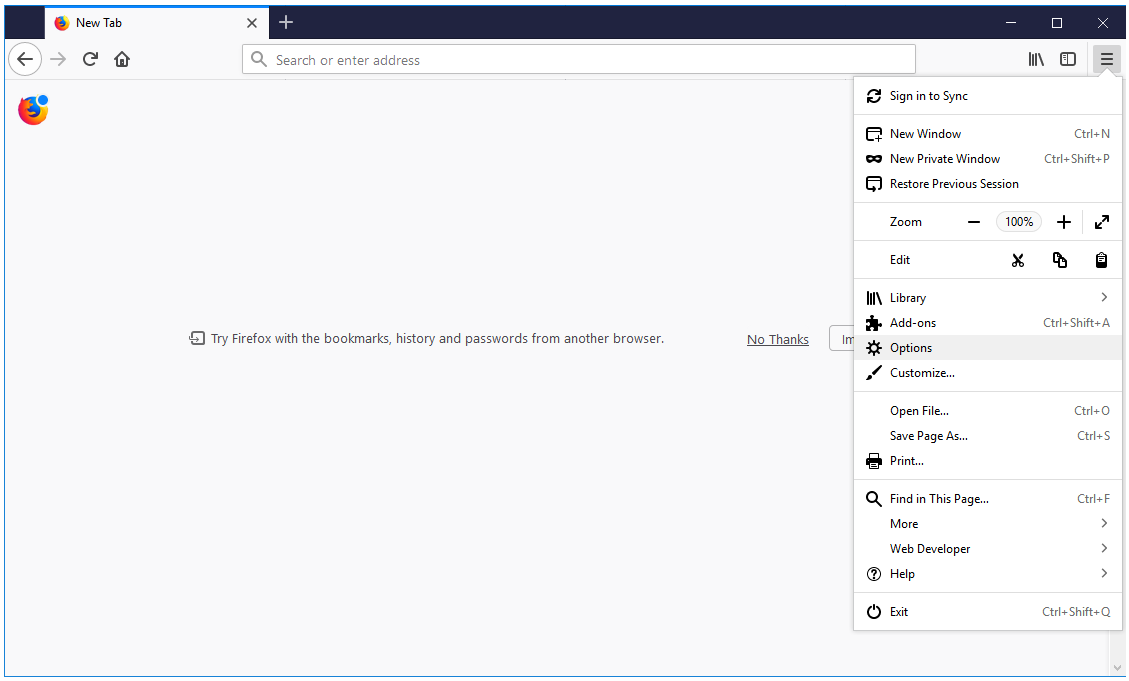
1. The MSI installers install the DLLs under

   `%ProgramFiles%\keyon\p11capi`

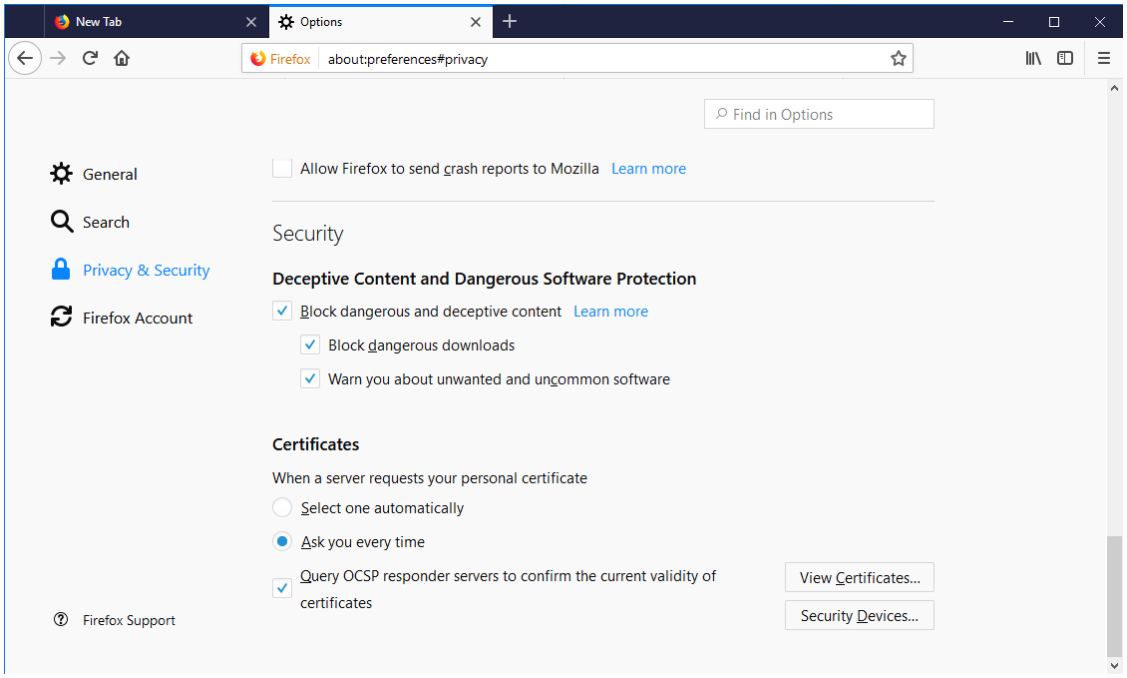
   `%ProgramFiles(x86)%\keyon\p11capi`

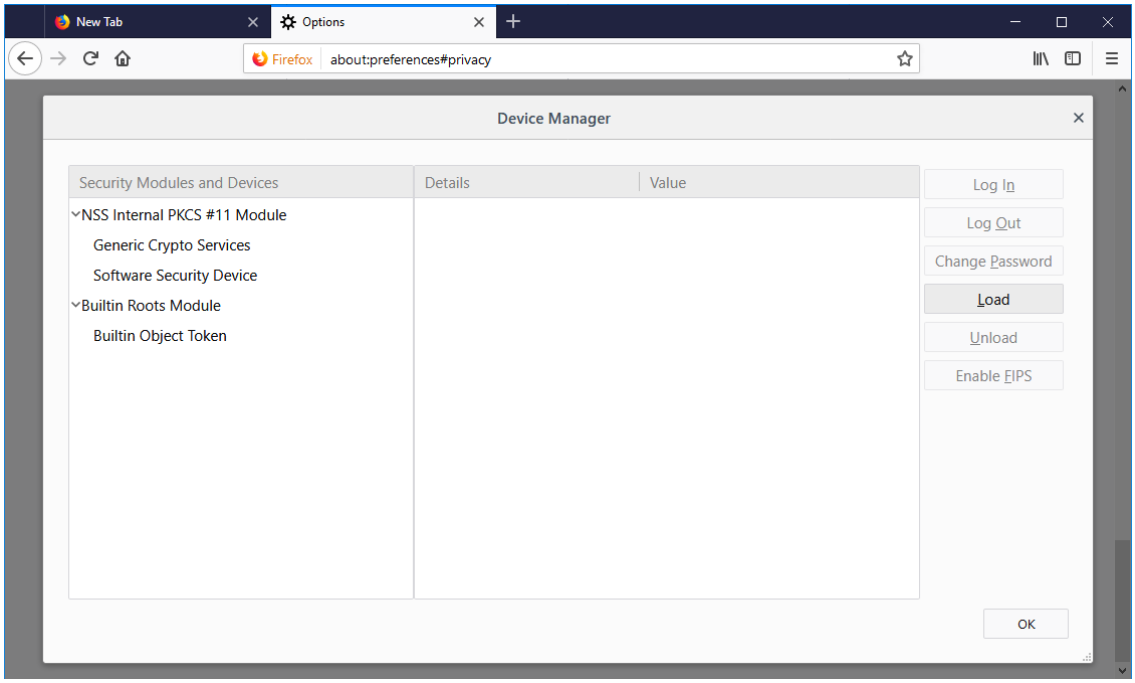
   However you can also store the `p11capi.dll` (user certificates) and `roots.dll` (CA certificates) files in an appropriate location on the file system.

2. Select *Options* from the menu:

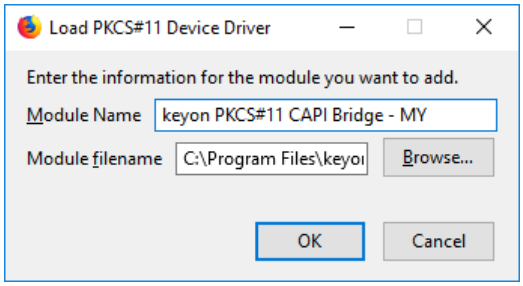


3. In the options dialog, select *Privacy & Security Certificates*, scroll down and click the *Security Devices* button:

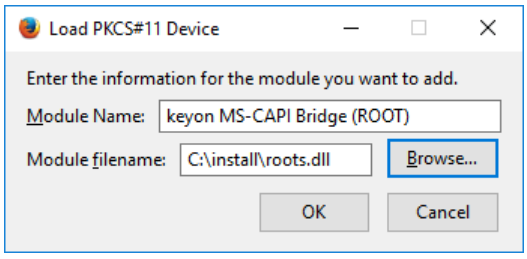




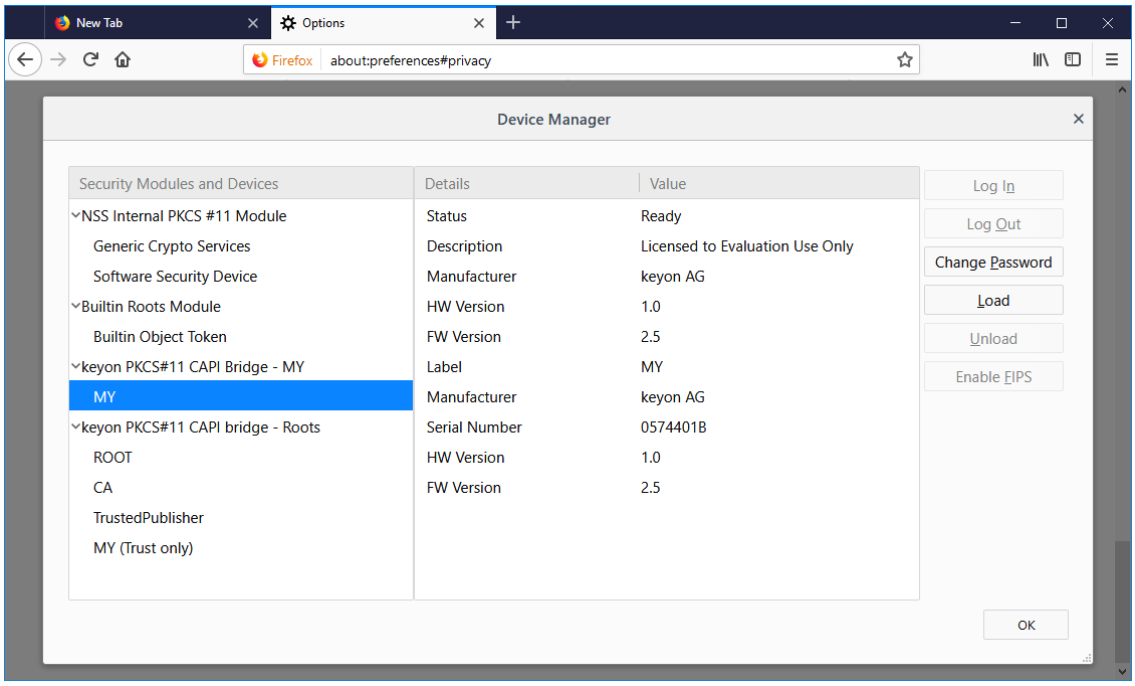
4. Click on Load, select the p11capi.dll along with the desired name and click *OK*:



5. Click on *Load*, select the roots.dll along with the desired name and click *OK*:



6. The laoded modules are now shown in the *Device Manager*:



Uninstalling the PKCS#11 libraries in Mozilla Firefox

To remove the modules, open the *Security Devices* configuration, select the module and click *Unload*.

Extension

Installation

Side-loading

Side-loading will add the extension in a disabled state by default, the users will have to enable it explicitly. This can be changed by altering the Firefox settings as described in

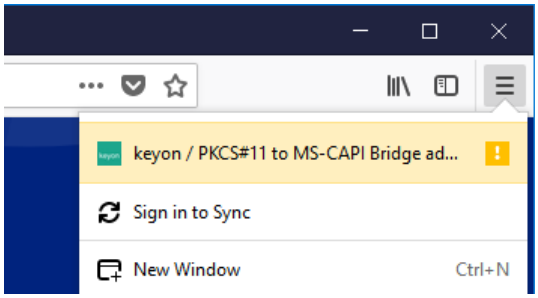
https://developer.mozilla.org/en-US/Add-ons/WebExtensions/Alternative_distribution_options/Add-ons_in_the_enterprise

Initial start of Firefox

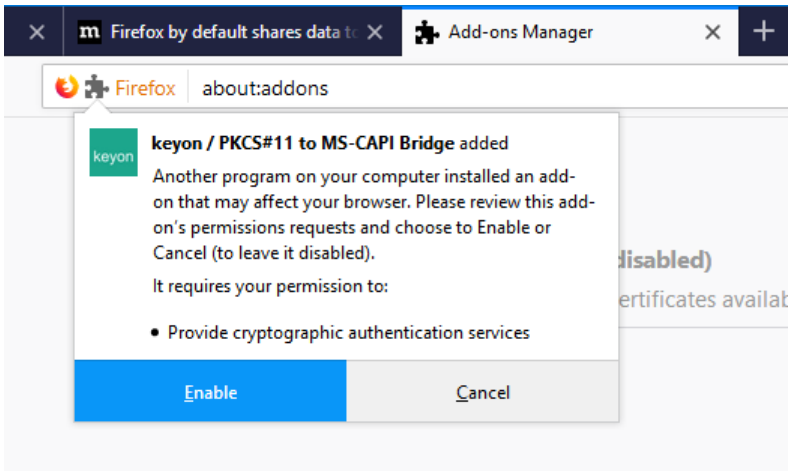
Depending on the Firefox version, this behavior may be different.

A notification icon is shown in the menu button:

Clicking the menu shows the notification about the extension on top:



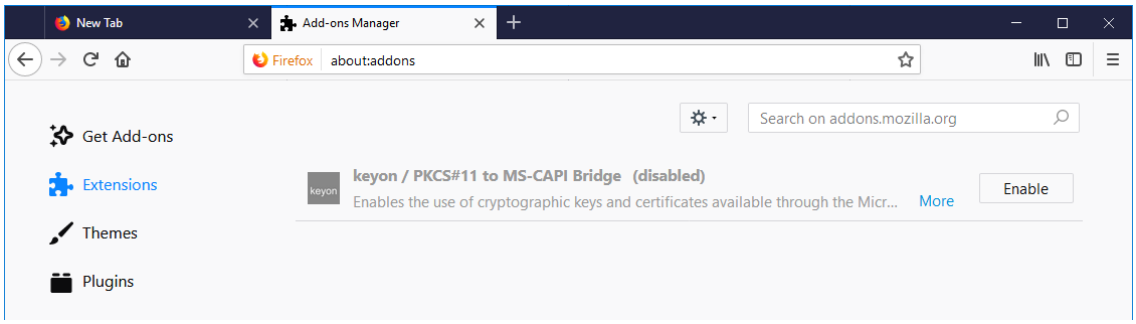
Clicking the highlighted entry will start adding the extension:



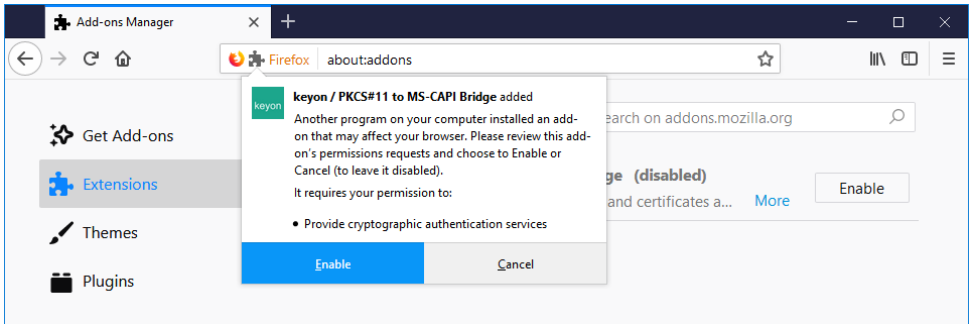
Note that if the user clicks Cancel or does not click the notification in the menu, the extension is still added due to side-loading but will be in a deactivated state. Unless the extension is activated, the PKCS#11 modules will not be registered.

Subsequent starts if not added initially

If the notification is not clicked by the user at the first start of Firefox, the extension is still added due to side-loading but will be in a deactivated state:



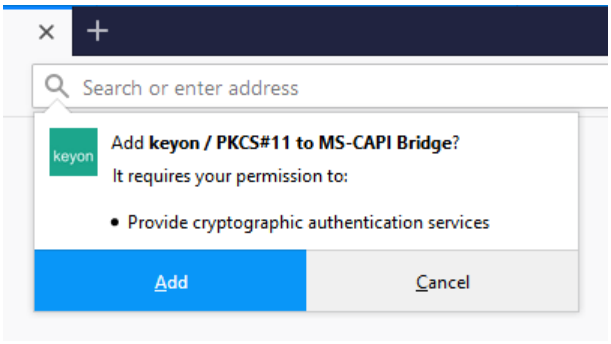
Clicking Enable will trigger adding the extension:



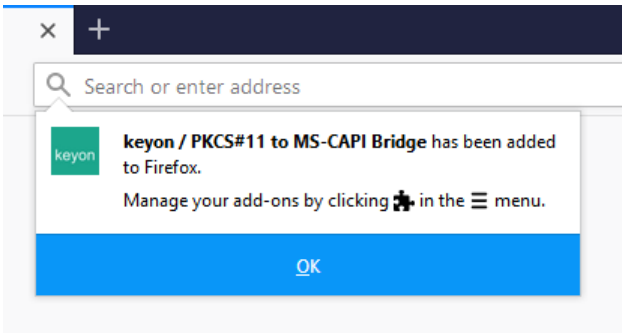
Standard installation

The extension XPI may be dropped from an Explorer Window to the Firefox window or the extension may be downloaded by clicking a link that provides the XPI for download.

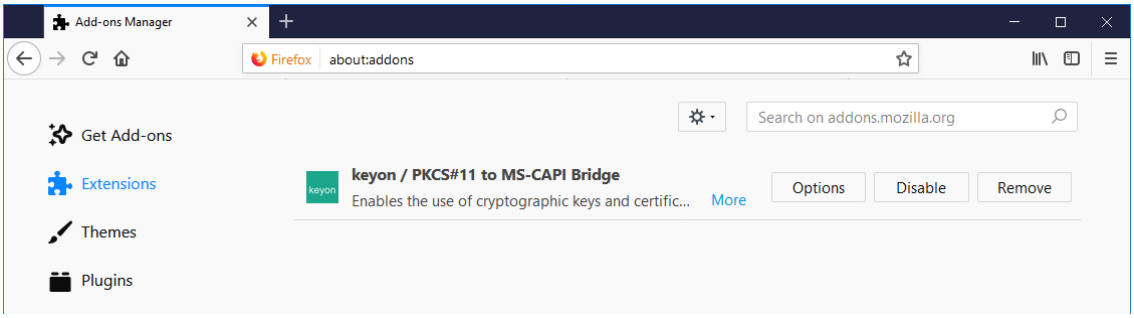
A notification will be shown asking the user to add the extension:



Is the user confirms adding the extension, a notification of the successful operation is shown:

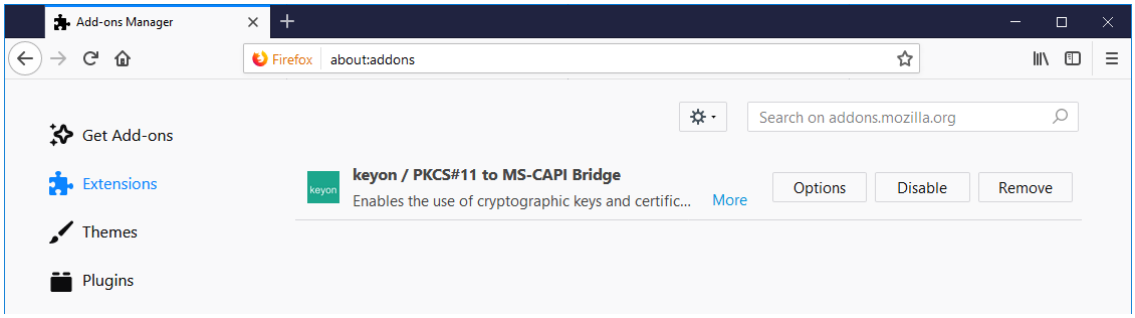


The extension is then available under Add-ons / Extensions:

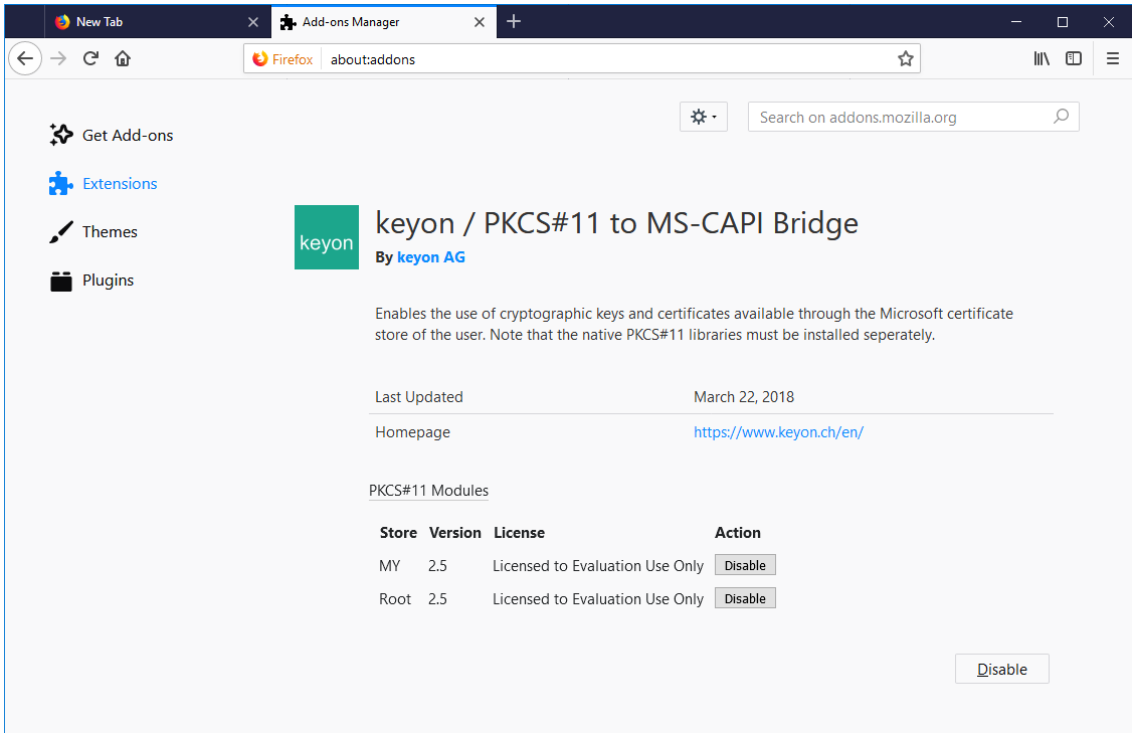


Options

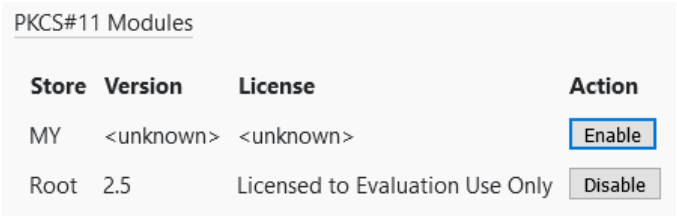
You can load or unload the PKCS#11 modules in the options of the extension under Add-ons / Extensions:



The settings page shown by clicking *Options* will also show the licensing status of the extension:



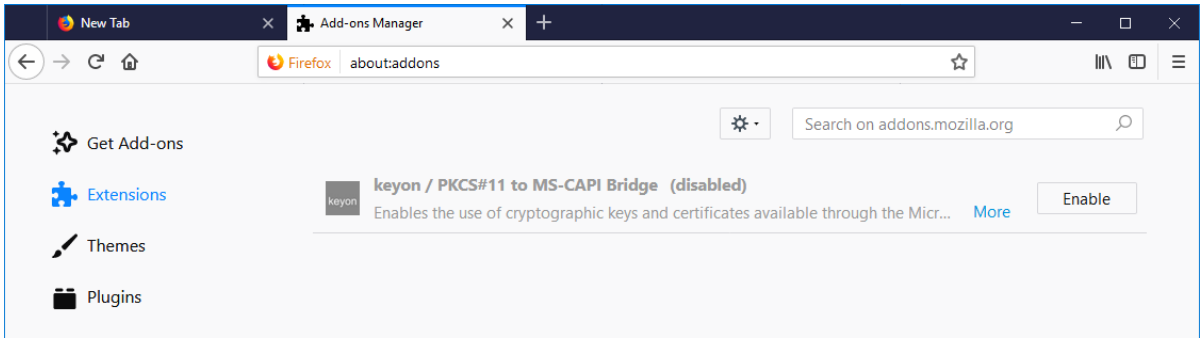
Click the *Disable* or *Enable* button next to the store to unload or load the PKCS#11 module. The effect will take place immediately and the enablement status is retained during restarts of Firefox:



Disabling the extension

PKCS#11 modules are not unloaded when the extension is disabled.

The web extension API does not provide the necessary events to detect the disabling or uninstallation of an extension. This is currently by design and the PKCS#11 to MS-CAPI Bridge web extension therefore cannot deregister the PKCS#11 modules itself.



Removing the extension

PKCS#11 modules are not unloaded when the extension is removed.

The web extension API does not provide the necessary events to detect the disabling or uninstallation of an extension. This is currently by design and the PKCS#11 to MS-CAPI Bridge web extension therefore cannot deregister the PKCS#11 modules itself.

If the PKCS#11 DLLs are no longer available, Firefox will not show any warnings and the registration in the Device Manager is still shown though no slots are present.

Side-loaded extension

If the extension is installed using side-loading, it cannot be removed, only disabled.

CAPI Credential Usage

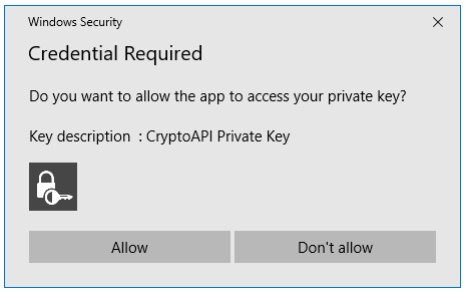
Depending on the type of CAPI credential, different dialogs may be shown when a key is used over the PKCS#11 to MS-CAPI Bridge.

No CAPI dialogs are shown unless a key is actually used for a cryptographic operation.

Soft Tokens

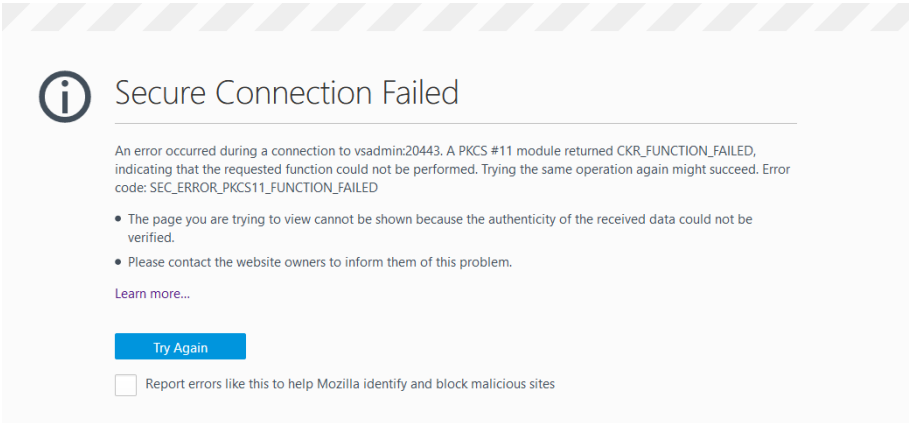
Soft tokens usually do not require the entry of a password or any other confirmation when used for cryptographic operations. However if strong protection was specified when the key was generated or imported, the following dialogs may show up once per process lifetime when such a key is used for a cryptographic operation:

Security level medium:



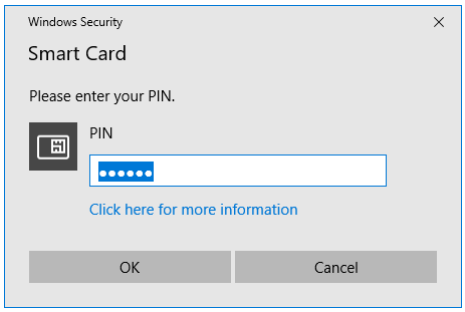
Security level high:

Selecting *Deny permission* or clicking *Cancel* will lead to a PKCS#11 error as the key cannot be used for cryptographic operations:

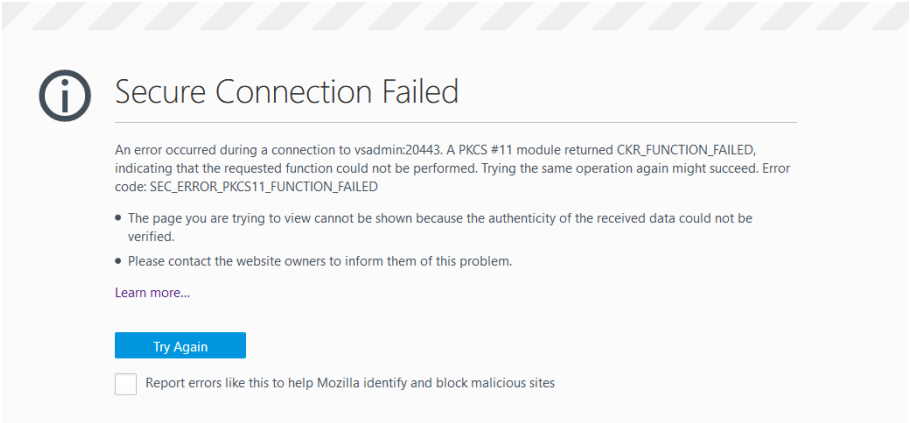


Smart Cards and other tokens

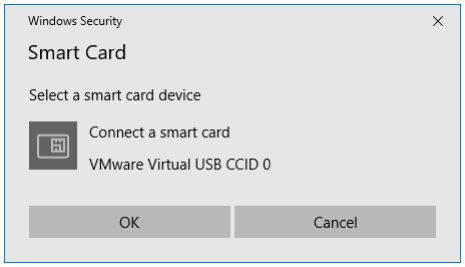
Smart Cards usually require the user to enter a PIN unless the middleware or Smart Card implements some sort of Single Sign On functionality. Unlike with strong protected soft tokens the Smart Card or middleware defines if a PIN must be entered only once per process lifetime or for each cryptographic operation:



Clicking *Cancel* will lead to a PKCS#11 error as the key cannot be used for cryptographic operations:



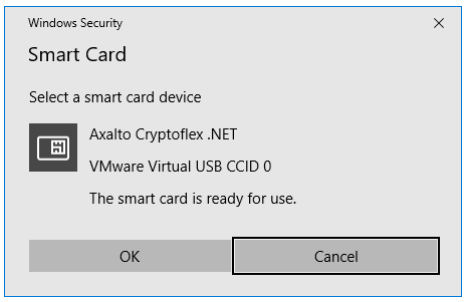
If the Smart Card for the slected certificate is not available, the following dialog may be shown:



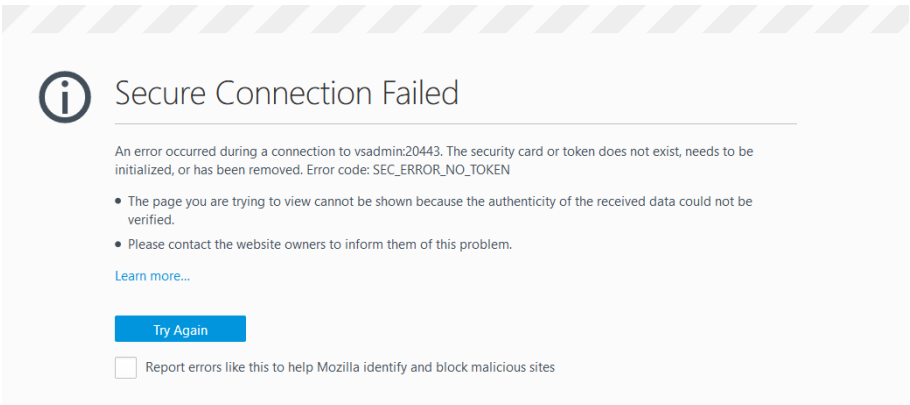
This dialog may not be tied to the application Window as a child Window. This is due to a bug in Windows, which does not set the Window handle for the Smart Card subsystem unlike for CAPI dialogs, which are tied to the application Window.

The Insert Smart Card dialog may pop-up behind the application window making the application look unresponsive while waiting for the dialog to be answered.

If the correct Smart Card is inserted, the *OK* button becomes active but must still be clicked by the user to continue:

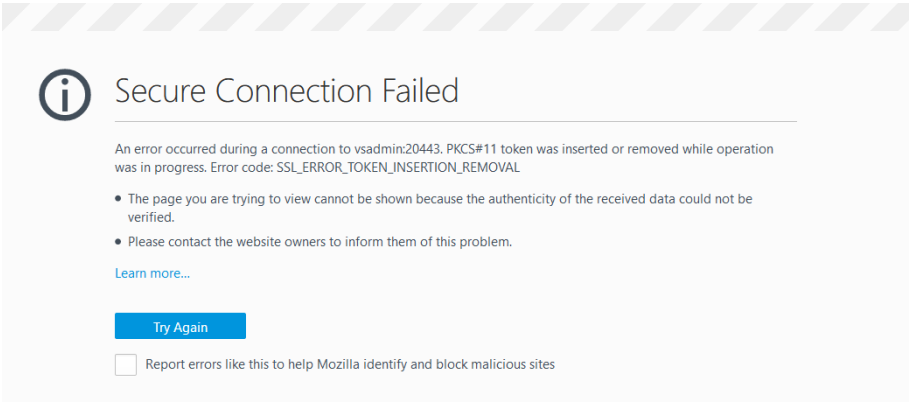


Cancelling this dialog will lead to the following PKCS#11 error:



Behavior if the certificate and / or key is deleted

If a certificate or key in use, e.g. for an open SSL connection, is not longer present in the Microsoft Certificate Store, e.g. because the Smart Card was removed and the certificate deleted from the store during this process, the following error is shown:



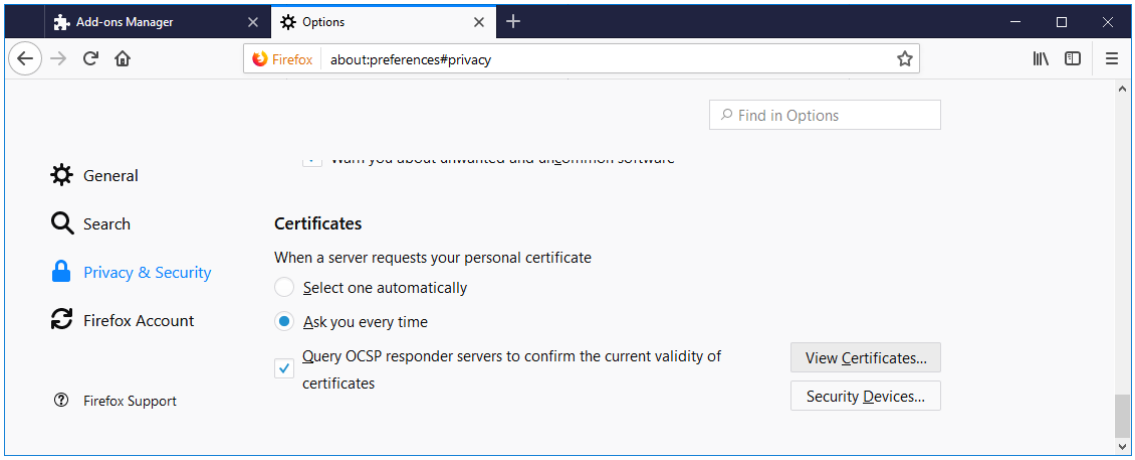
Behavior if the Workstation is locked

If the Workstation is locked, cryptographic operations are only performed „silent“, i.e. CAPI is not allowed to show dialogs.

This behavior is implemented to prevent PIN dialogs for Smart Cards beeing displayed while the screen is locked. Some middleware implementations do not allow concurrent logins while a PIN dialog is shown. Using a Smart Card to unlock the Workstation may not be possible in such a scenario thus effectively locking the user out.

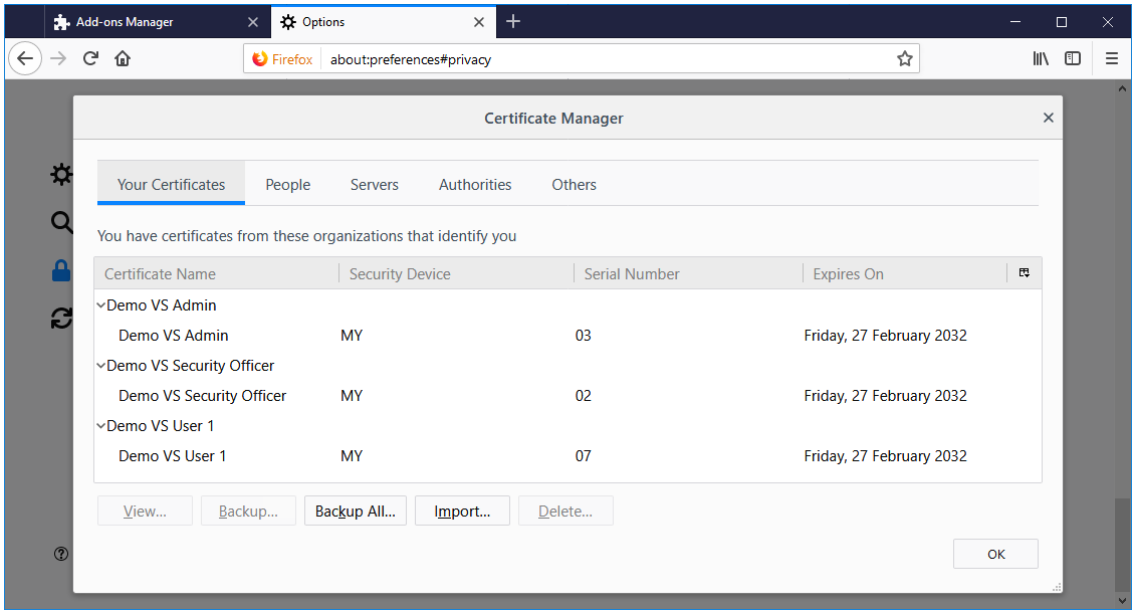
View available CAPI certificates

Start the Certificate Services Management console by selecting *Options* → *Privacy & Security* → *Certificates* → *View Certificates*:



User certificates from the Microsoft Certificate Store

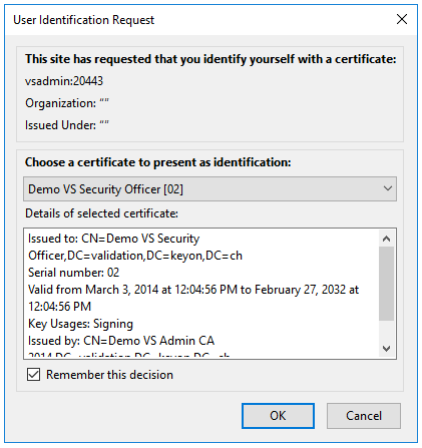
User certificates from the Microsoft Certificate Store (current user) show up using Security Device *MY* in the certificate manager:



You cannot delete certificates and keys that are stored in the Microsoft Certificate Store. This behavior is implemented this way to prevent unintentation deletion of credentials managed be the Microsoft CryptAPI.

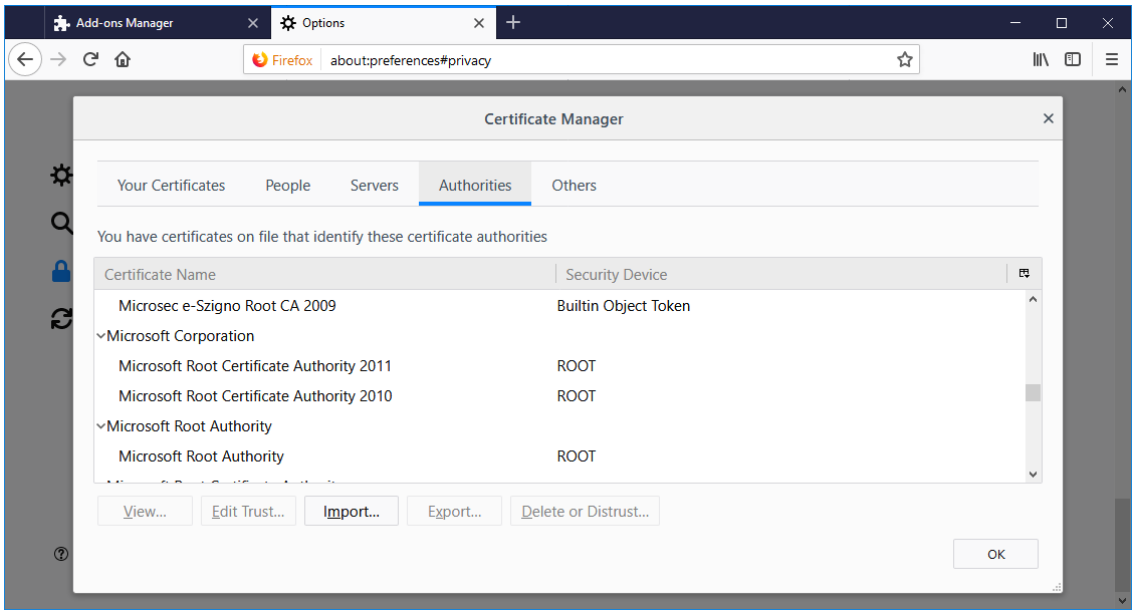
You cannot backup certificates and keys that are stored in the Microsoft Certificate Store. PKCS#11 to MS-CAPI Bridge only supports the use of keys over the CryptoAPI but not to export keys, which in case of Smart Card is impossible anyway.

User certificates from the Microsoft Certificate Store will always have *MY:* as a prefix in the selection dialog to distinguish them from non-CAPI certificates and keys:



Trusted CA certificates from the Microsoft Certificate Store

CA certificates from the Microsoft Certificate Store (current user) show up using Security Device *Root*, *CA* or *TrustedPublisher* (accoding to their Microsoft Certificate Store origin) in the certificate manager:



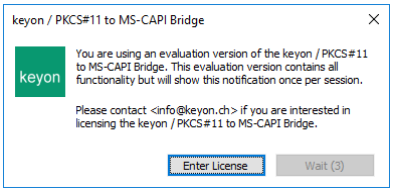
If the certificate is present in the Mozilla CA database it will always show up as *Builtin Object Token* regardless if it is also present in the Microsoft Certificate store.

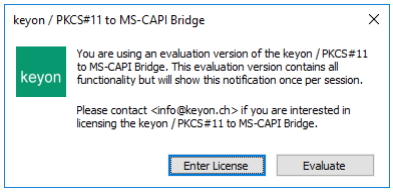
The allowed usage of the CA certificate (i.e. the trust settings) is set accordingly to the extended key usage of the certificate.

Licensing

Evaluation nag screen

Unless you purchase and install a license, the PKCS#11 to MS-CAPI Bridge will show a nag screen if a cryptographic operation with a certificate provided by the MS-CAPI Bridge is attempted:





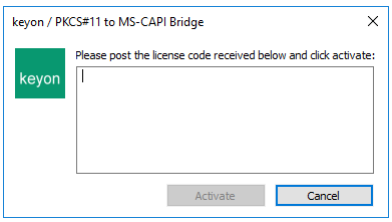
The nag screen will lock your browser window and can only be closed after some time has passed. The wait time increases over time to encourage you to purchase a license.

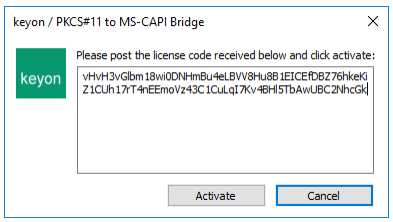
The nag-screen is only shown if you actually try to use the private key associated with a certificate provided over the MS-CAPI Bridge.

The nag screen is shown only once for each browser session.

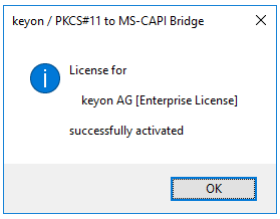
Entering the license string obtained from keyon

You can enter the license string directly in the nag screen by clicking *Enter License* and pasting the license string:



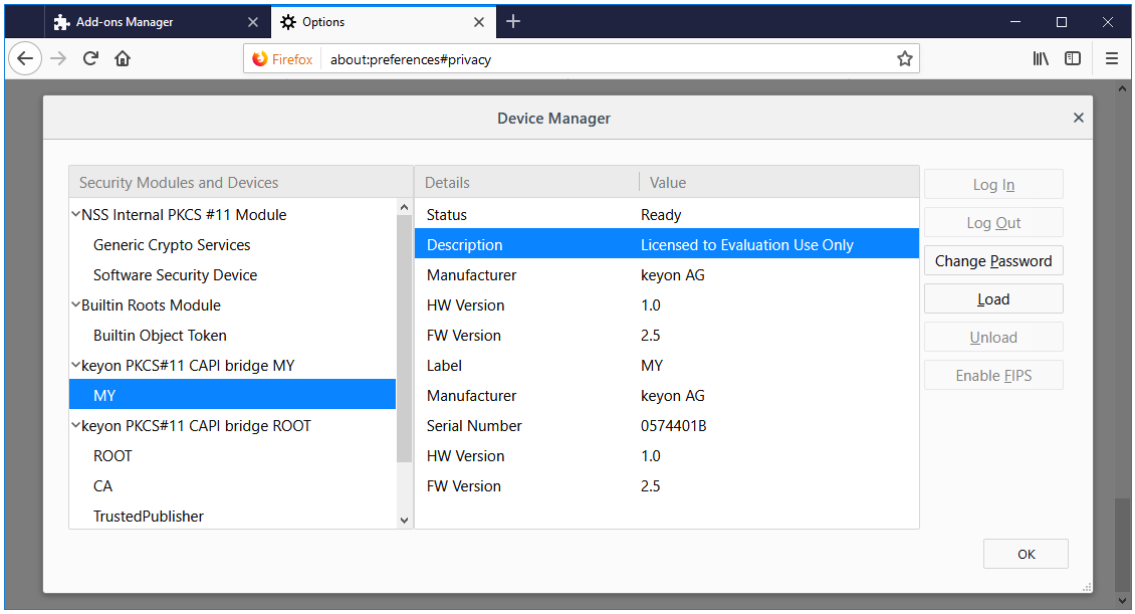


After clicking *Activate*, the licensee and license type is shown if the license is validated successfully

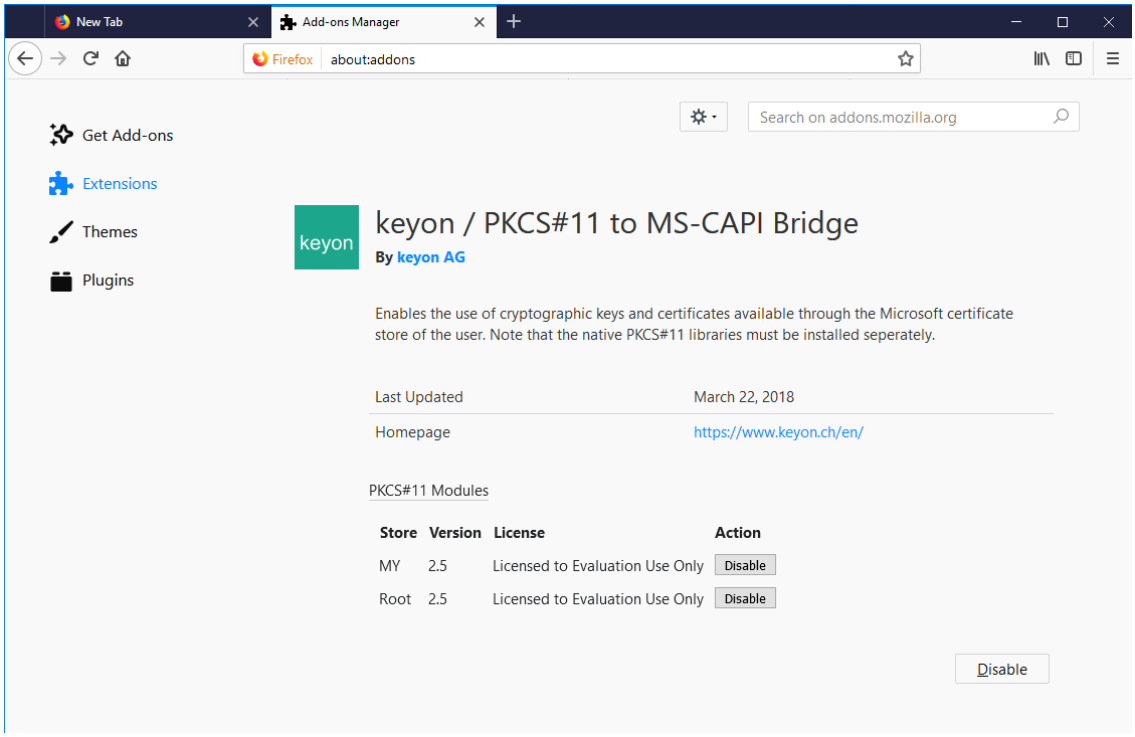


Checking the licensee and license type

The licensee and the license type is available in the description of the PKCS#11 token:



If the extension is used and enabled, the license information is also shown in the *Options* of the extension:



Deploying the license in an enterprise environment

If you need to deploy a license for multiple users or computers, you can simply create a registry entry with the license string using e.g. the Group Policy or your software deployment system.

Deploy the license for specific users

Store the license string in the following registry location:

```
[HKEY_CURRENT_USER\Software\keyon\capi-bridge]
"License"="vHvH3vGlbm18wi0DNHm...BggEB"
```

Deploy the license for all users of a machine

Store the license string in the following registry location:

```
[HKEY_LOCAL_MACHINE\Software\keyon\capi-bridge]
"License"="vHvH3vGlbm18wi0DNHm...BggEB"
```

License restrictions

Depending on the kind of license acquired, the license may be subject to one or more of the following restrictions:

Restriction	Description
Expiration date	If you want to evaluate the product without the evaluation nag screen, keyon can provide you with a time limited evaluation license. While the license is not yet expired, no nag screen will be shown.
User	The license may be restricted to one or more Windows user names. The nag screen will be shown if the current Windows user is not in the list of the allowed users.
Host	The license may be restricted to one or more Windows computers. The nag screen will be shown if the current computer is not in the list of the allowed computers.
Domain	The license may be restricted to one or more Windows Active Directory domains. The nag screen will be shown if the current computer is not a member of one of the allowed domains.

License options

Depending on the options requested when ordering the license, the license may restrict some of the features of the PKCS#11 to MS-CAPI Bridge:

Options	Description
Disable MY	Do not make the user's certificates available. With this option set, only the *ROOT*, *CA* and *TrustedPublisher* certificates are available over the PKCS#11 library. (Trust only)
Disable ROOT	Do not make the *ROOT*, *CA* and *TrustedPublisher* certificates available. With this option, only the user's certificate are available over the PKCS#11 library. (User certificates only)

Reference

Links

Mozilla PKCS#11	https://developer.mozilla.org/en-US/docs/PKCS11_Module_Installation
	https://developer.mozilla.org/en/docs/PKCS11_FAQ
	https://developer.mozilla.org/en-US/Add-ons/WebExtensions/API/pkcs11