keyon

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

V2.4

April 2017

Table of contents

Overview **5**
What it is the keyon / PKCS#11 to MS-CAPI Bridge? 5
Key Features 5

Changelog **6**
Version 2.4.4 6

Installation **7**
Restartless extension 8
Compatibility 8
Extension Properties 8
Installing the XPI package 8
Installing the exploded package 11
Manual installation (GUI) 14
Compatibility 14
Installing the PKCS#11 libraries in Mozilla Firefox 14
Uninstalling the PKCS#11 libraries in Mozilla Firefox 16
Manual installation (modutil) 17
Compatibility 17

CAPI Credential Usage **18**
Soft Tokens 18
Smart Cards and other tokens 19
Behavior if the certificate and / or key is deleted 21
Behavior if the Workstation is locked 21

View available CAPI certificates **22**
User certificates from the Microsoft Certificate Store 22
Trusted CA certificates from the Microsoft Certificate Store 24

Licensing **25**
Evaluation nag screen 25
Entering the license string obtained from keyon 25
Checking the licensee and license type 26

Deploying the license in an enterprise environment 27
Deploy the license for specific users 27
Deploy the license for all users of a machine 27
License restrictions 28
License options 28
Reference 29
Links 29

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

Installation

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

The following types of installation are supported:

Type	Compatibility	Features
Restartless extension	▪ Firefox 4.0 and higher ▪ 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 (modutil)	▪ Any Firefox version ▪ Any Thunderbird version ▪ Any Seamonkey version	Needs manual registration of the PKCS#11 ("cryptoki") DLLs in the modules database. 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.

Restartless extension

Compatibility

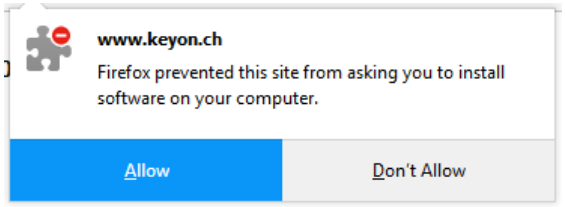
Application	Version requirements
Firefox	4.0 and higher
Thunderbird	3.3 or higher
Seamonkey	2.1 or higher

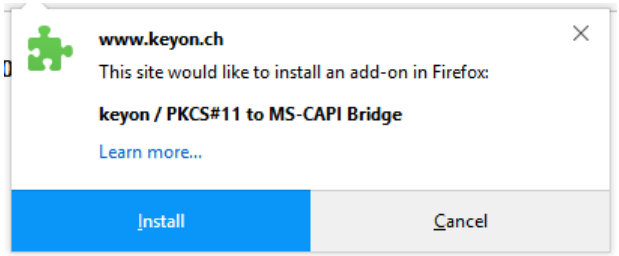
Extension Properties

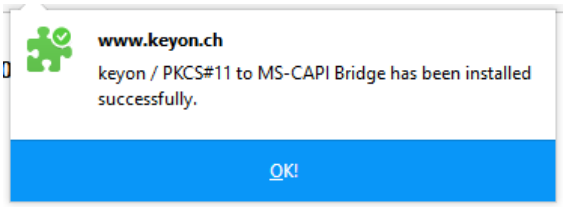
Property	Value
Extension ID	capi-bridge@keyon.ch
Supports disable / enable	Yes, without restart
Restart required after installation / removal	No

Installing the XPI package

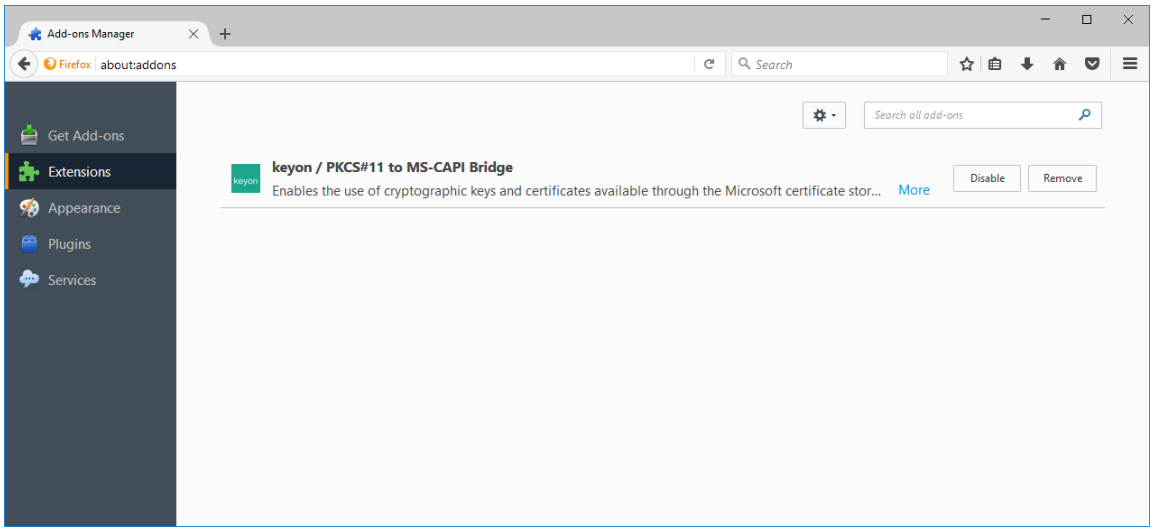
The XPI package can be installed by downloading the XPI or by drag and drop of the XPI file to Mozilla Firefox. The XPI is signed by Mozilla, however the XPI is not available over the addons.mozilla.org web site thus you will have to explicitly allow the download:



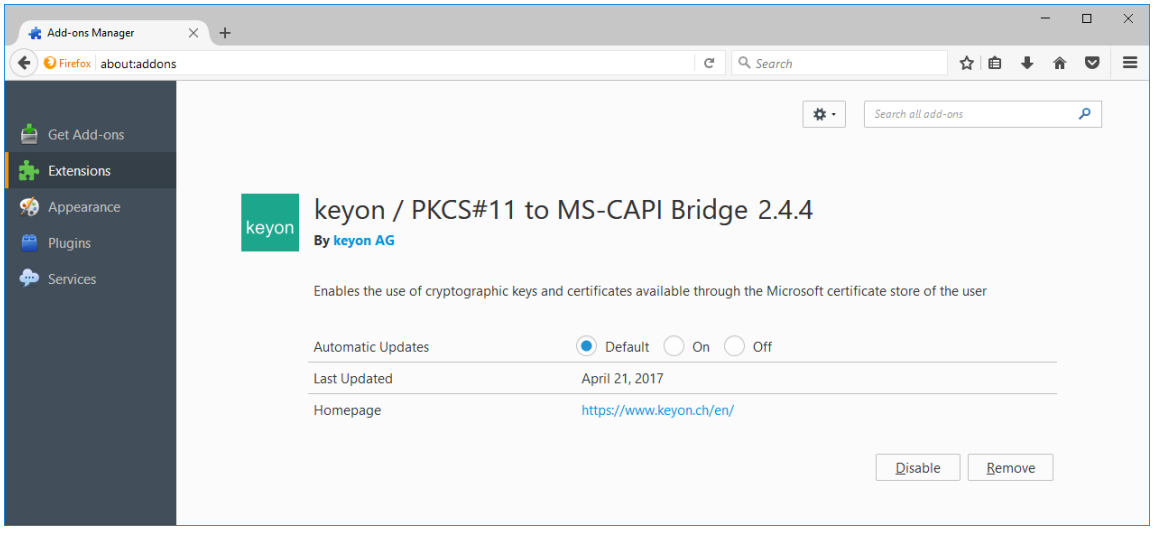




After confirming the installation, the functionalitiy is available immediately and the Add-on Manager shows the installed package:

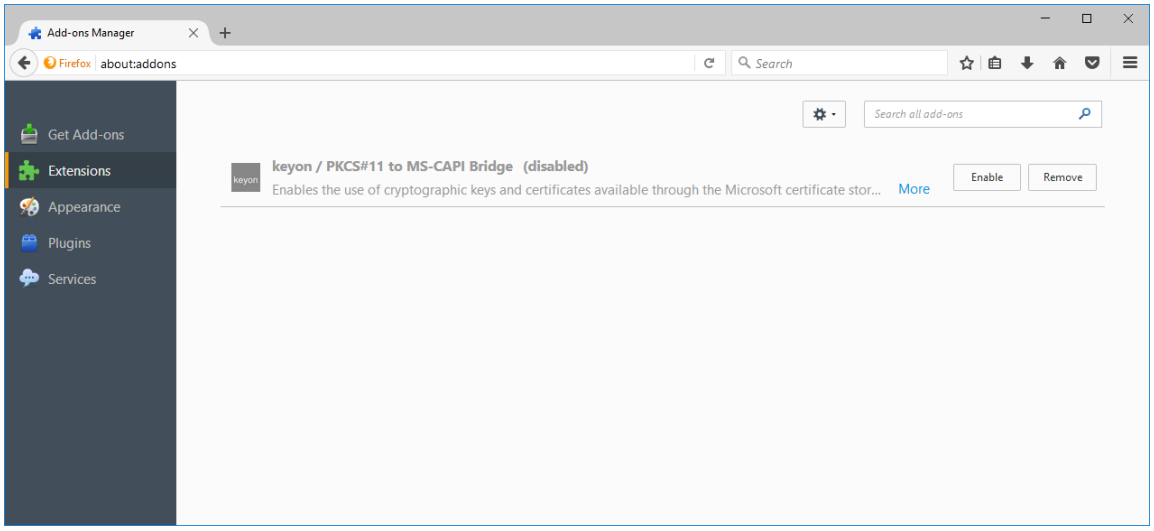


Clicking more will show some additional information:

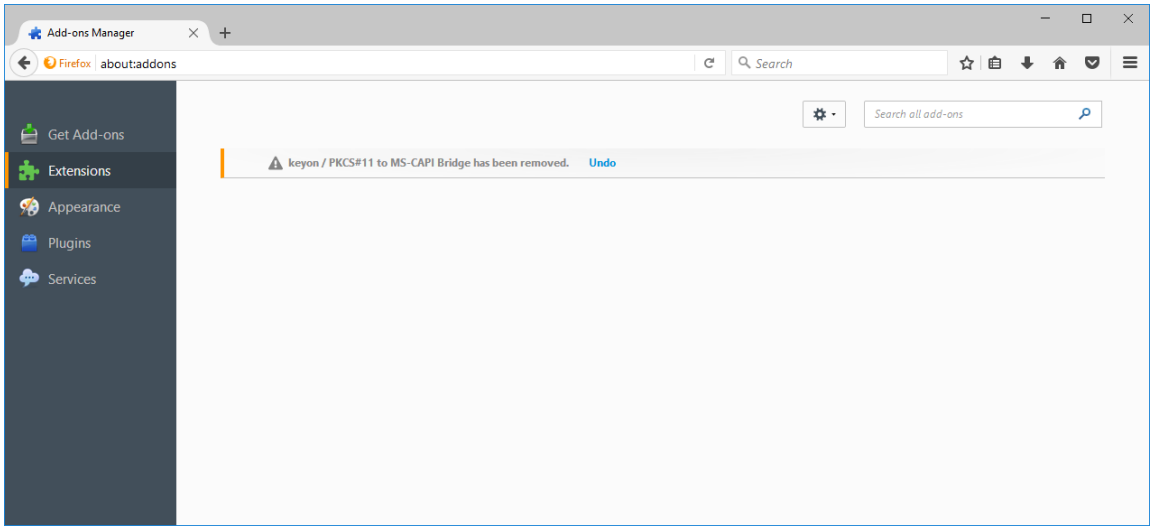


The extension supports automatic updates. The update site is located at https://www.keyon.ch/update/mozilla/capi-bridge/

The extension can be disabled in the Add-on Manager which immediately removes the PKCS#11 library. Certificates and keys in the Microsoft Certificate Store are no longer available when the extension is disabled:



The extension can be removed in the Add-on Manager which immediately removes the PKCS#11 library. Certificates and keys in the Microsoft Certificate Store are no longer available:

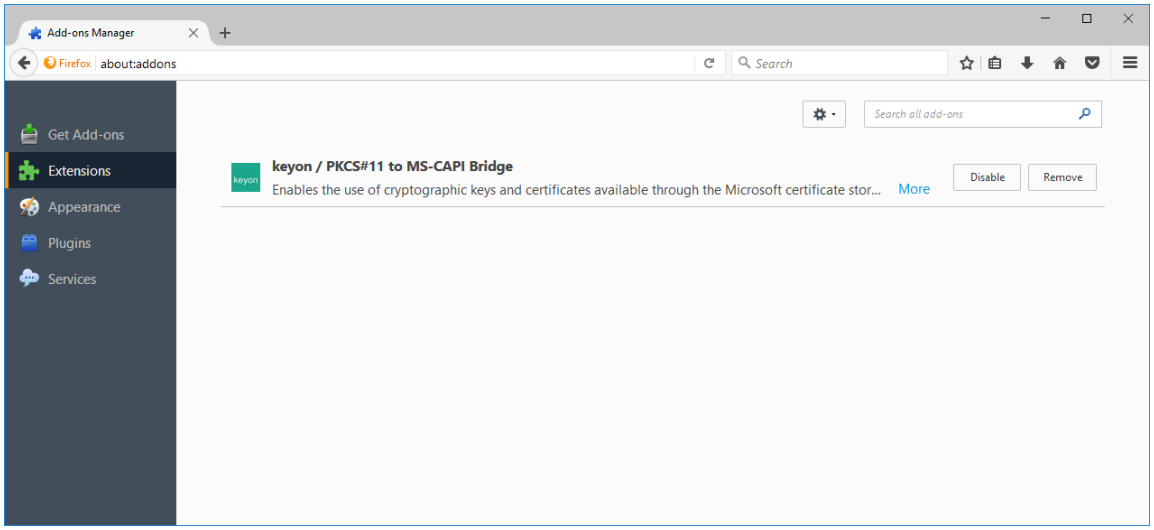


Installing the exploded package

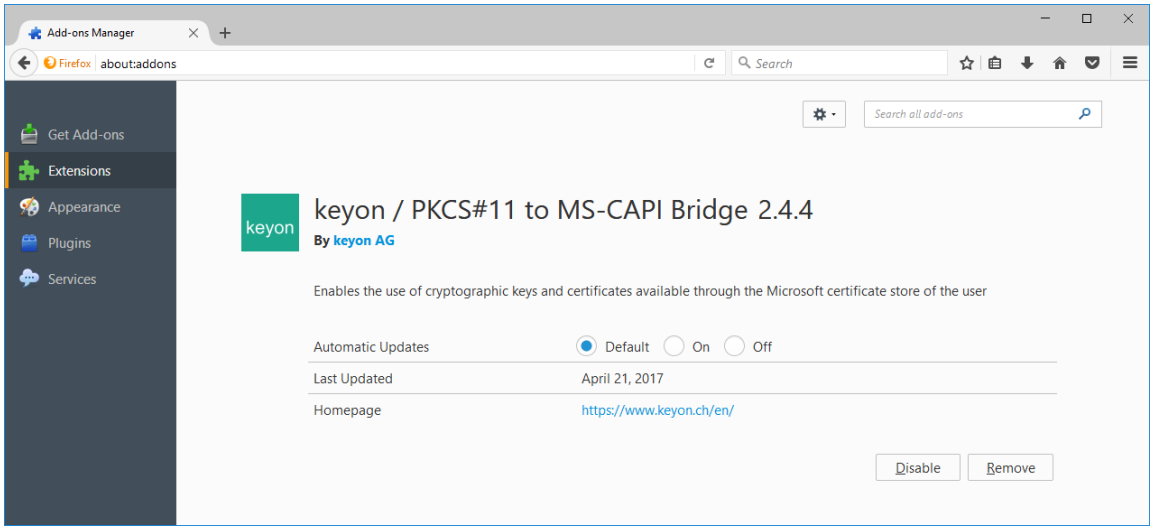
The exploded package can be installed directly in the file system. Please check the Mozilla documentation to learn in which locations to install the exploded plugin as they may differ depending on the version and deployment scenario (e.g. per user or for all users):

https://developer.mozilla.org/en/docs/Installing_extensions

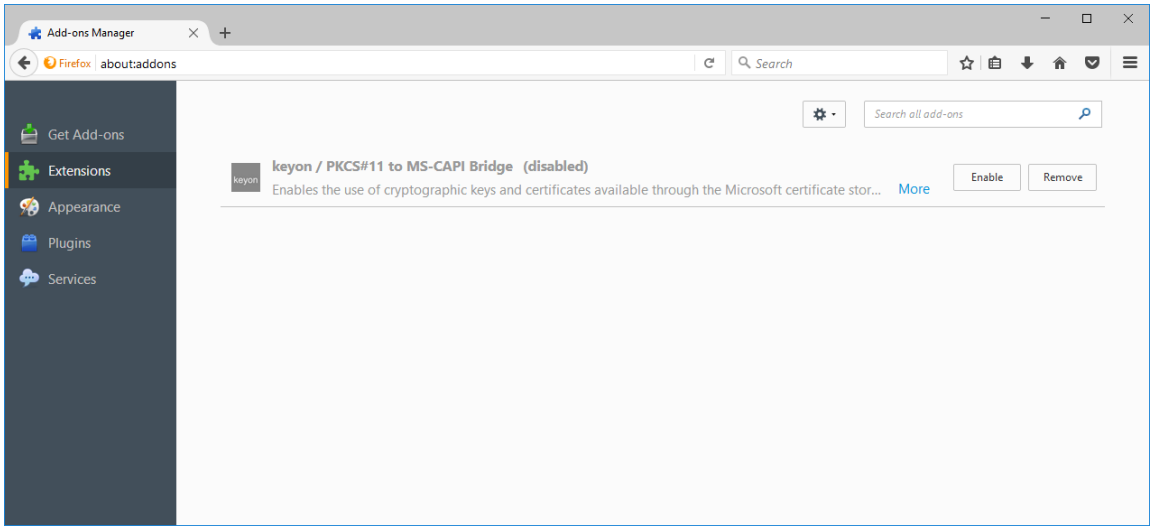
Unlike the installation using the XPI package, exploded extensions cannot be removed from within Mozilla Firefox by the user:



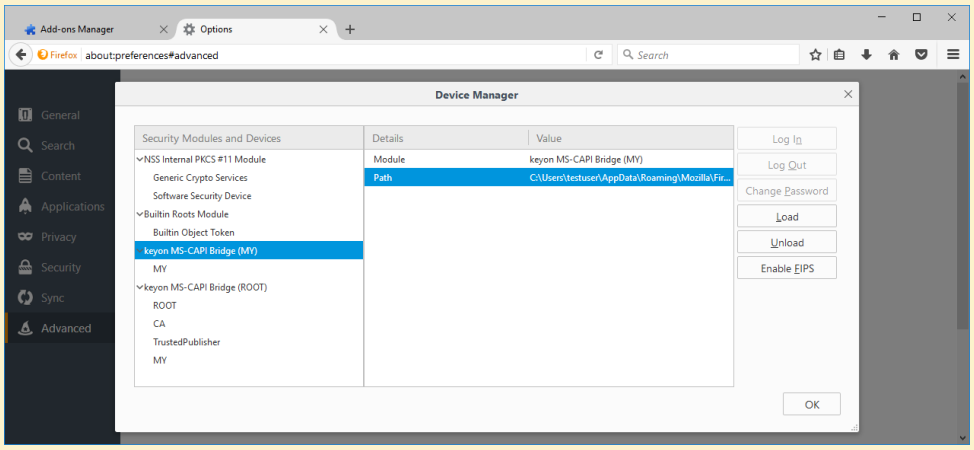
Clicking more will show some additional information:



However it is possible to disable the extension which immediately removes the PKCS#11 library. Certificates and keys in the Microsoft Certificate Store are no longer available:



Removing the extension in the file system does not properly uninstall the extension. If the exploded package directory is removed, the PKCS#11 library may still show up in the configuration, however it should not have any negative effects on the application itself:



Including the extension with your distribution of Firefox

Please consult the documentation of the Mozilla Developer Network to learn other deployment options:

https://developer.mozilla.org/en-US/docs/Developer_Guide/Customizing_Firefox

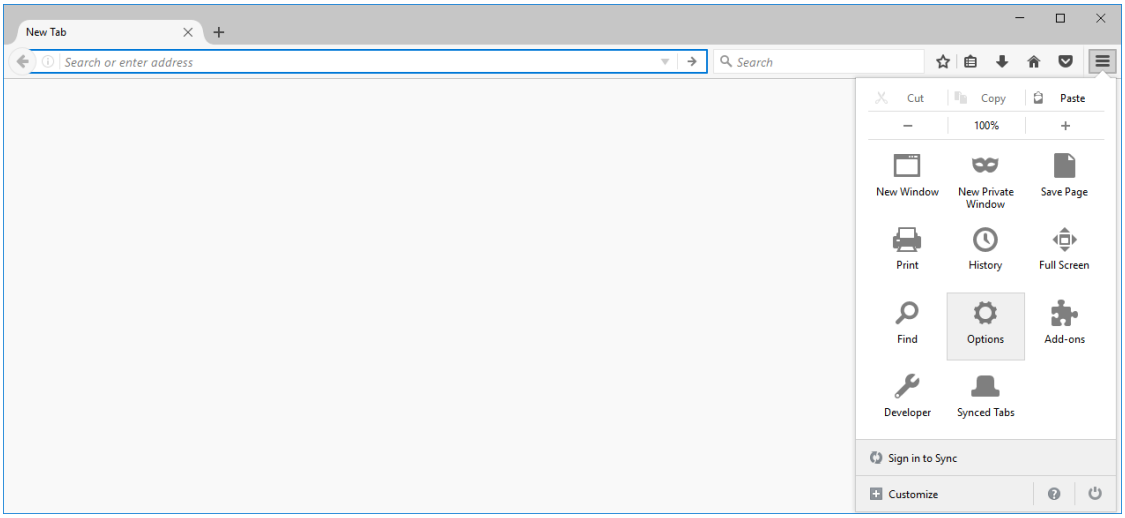
Manual installation (GUI)

Compatibility

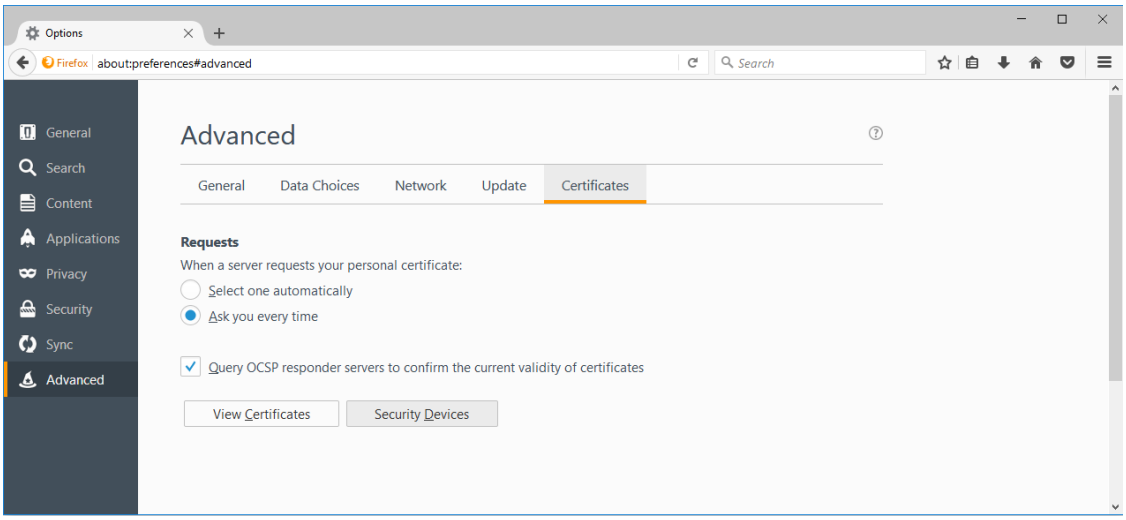
Application	Version requirements
Firefox	1.0 or higher
Thunderbird	1.0 or higher
Seamonkey	1.0 or higher
Other	Applications based on NSS should be able to use the PKCS#11 library. Other applications capable of using a 32-Bit DLL implementing the PKCS#11 API v2.20 may work as well.

Installing the PKCS#11 libraries in Mozilla Firefox

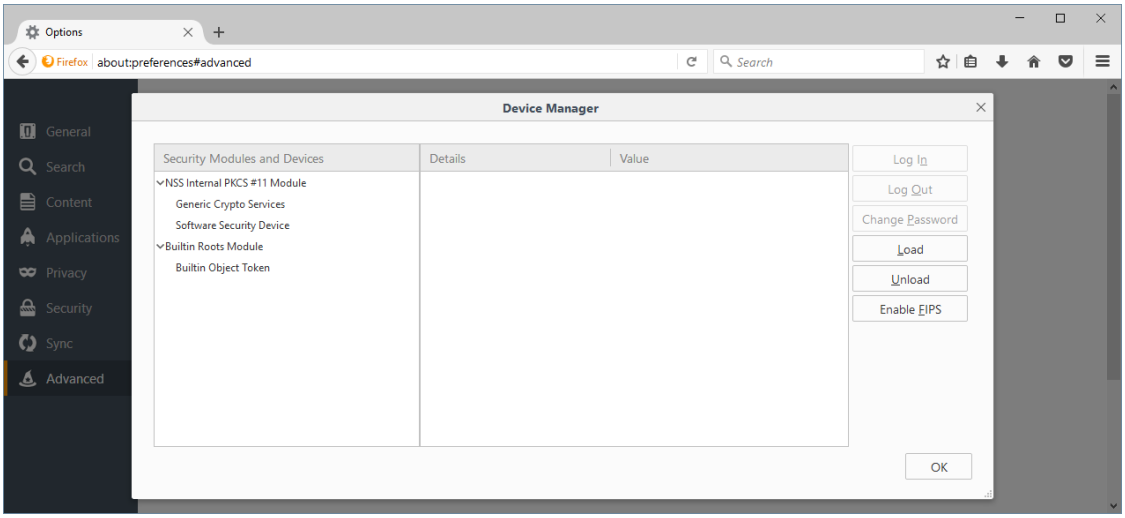
1. Store the `p11capi.dll` (user certificates) and `roots.dll` (CA certificates) files in an appropriate location on the file system.
2. Select *Options* from the menu:



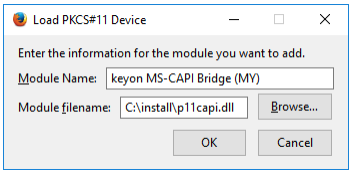
3. In the options dialog, select *Advanced* and the *Certificates* tab:



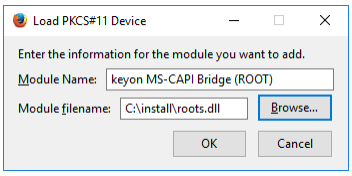
4. Click the *Security Devices* button:



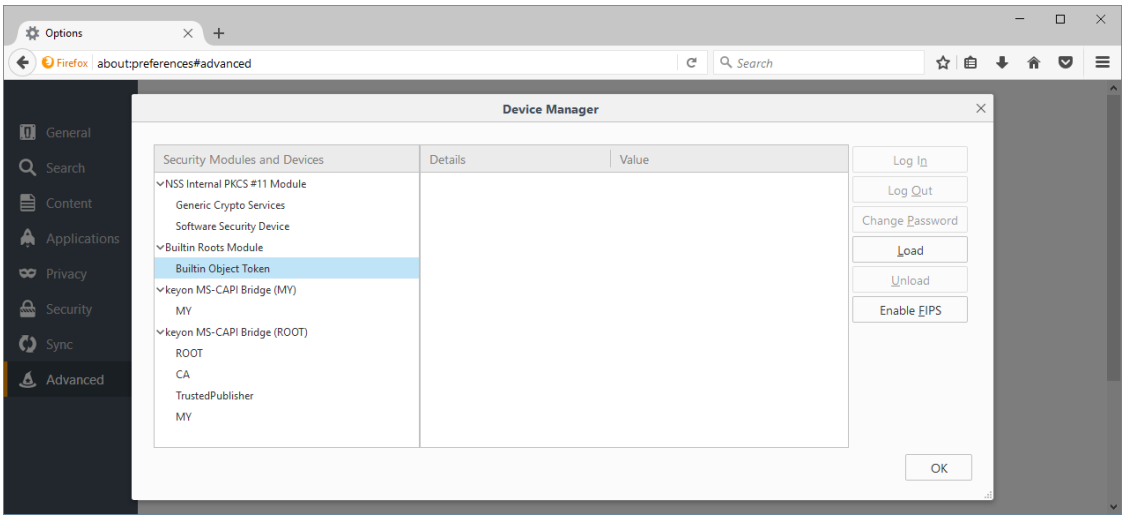
5. Click on Load, select the p11capi.dll along with the desired name and click *OK*:



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



7. Click on Load, select the roots.dll along with the desired name and click ok:



Uninstalling the PKCS#11 libraries in Mozilla Firefox

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

Manual installation (modutil)

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.

Please consult the Mozilla Developer Network to learn how to use the `modutil` command line utility to update the modules database to load the DLLs.

Using the Security Module Database (modutil):

https://developer.mozilla.org/en/docs/NSS/tools/NSS_Tools_modutil

CAPI Credential Usage

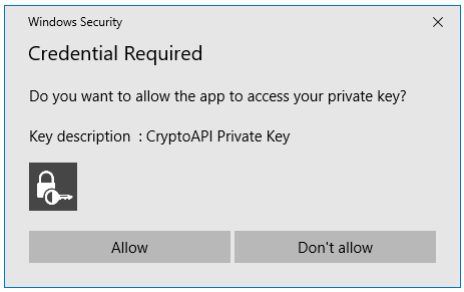
Depending on the type of CAPI credential, different dialogs may be shown when a key is used over the PKCS#11 to MS-CAPI Bridge.

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

Soft Tokens

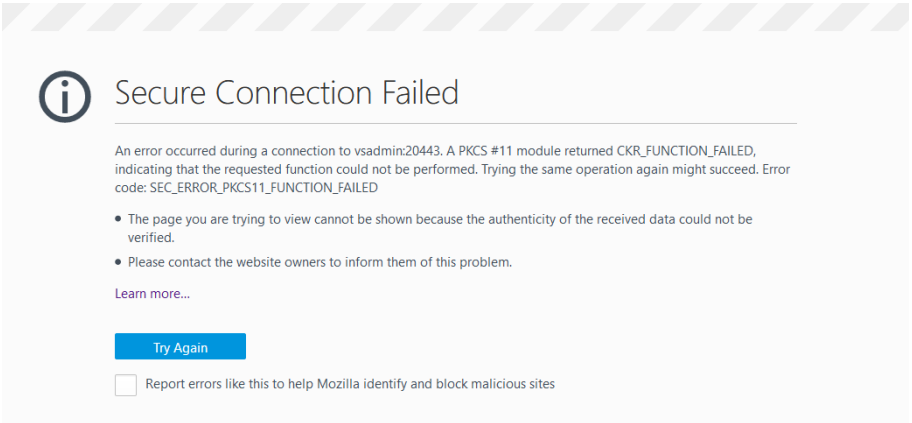
Soft tokens usually do not require the entry of a password or any other confirmation when used for cryptographic operations. However if strong protection was specified when the key was generated or imported, the following dialogs may show up once per process lifetime when such a key is used for a cryptographic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

Security level medium:



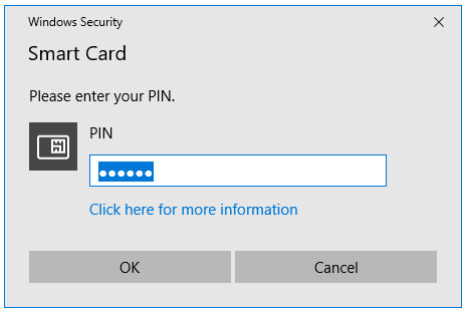
Security level high:

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

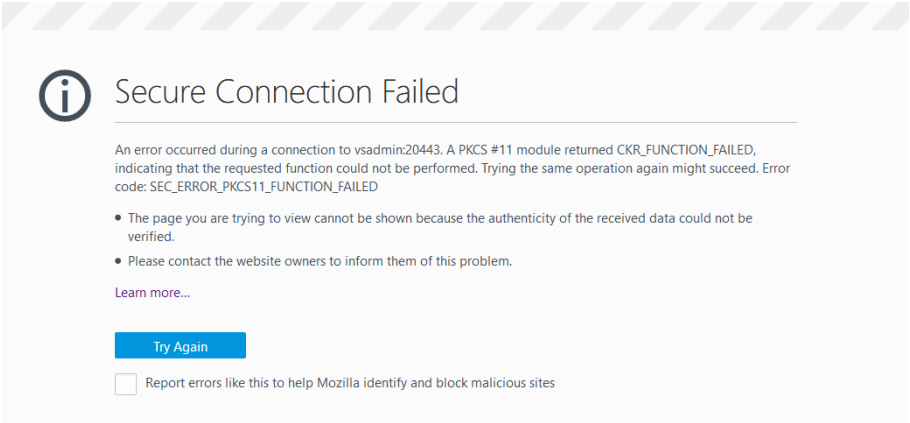


Smart Cards and other tokens

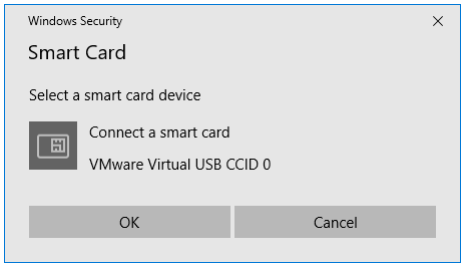
Smart Cards usually require the user to enter a PIN unless the middleware or Smart Card implements some sort of Single Sign On functionality. Unlike with strong protected soft tokens the Smart Card or middleware defines if a PIN must be entered only once per process lifetime or for each cryptographic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



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



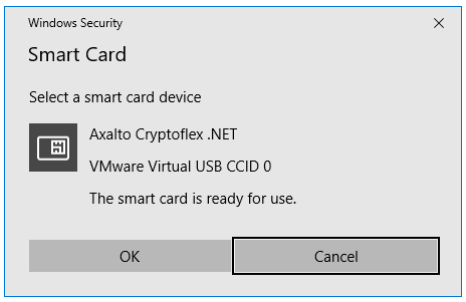
If the Smart Card for the slected certificate is not available, the following dialog may be shown:



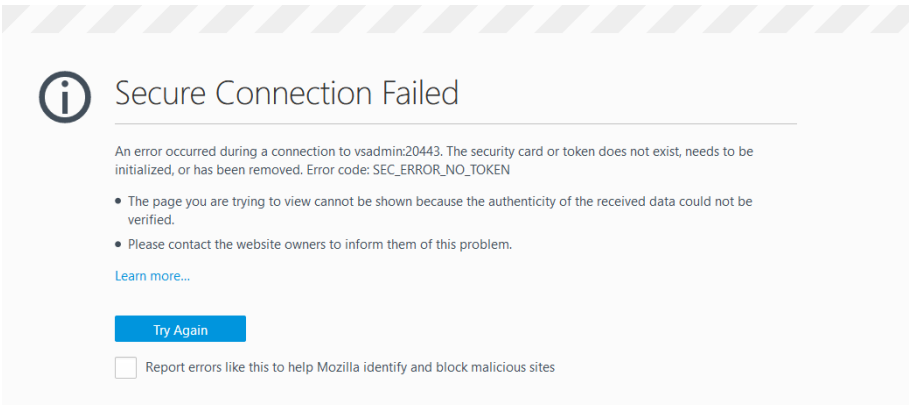
This dialog may not be tied to the application Window as a child Window. This is due to a bug in Windows, which does not set the Window handle for the Smart Card subsystem unlike for CAPI dialogs, which are tied to the application Window.

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:

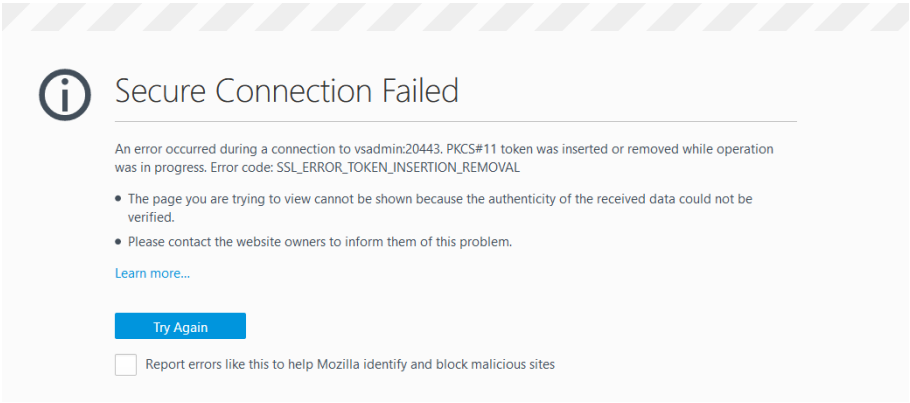


Cancelling this dialog will lead to the following PKCS#11 error:



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:



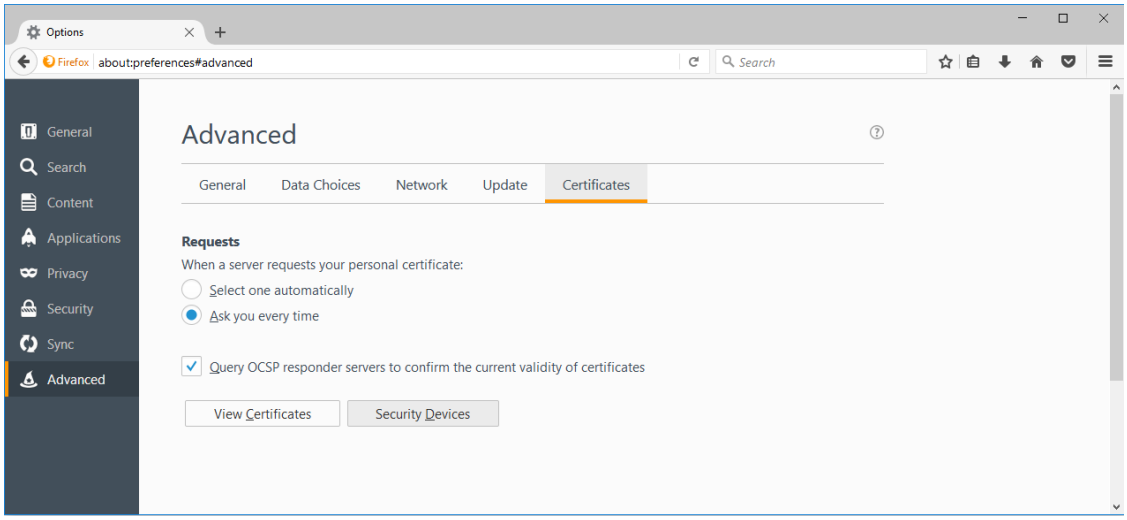
Behavior if the Workstation is locked

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.

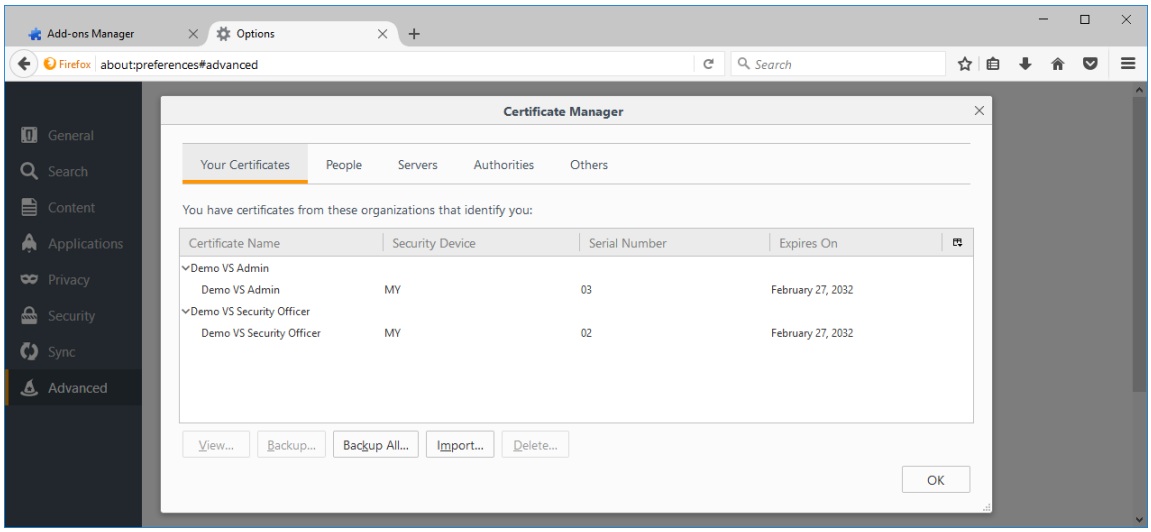
View available CAPI certificates

Start the Certificate Services Management console by selecting *Options* → *Advanced* → *Certificates* → *View Certificates*:



User certificates from the Microsoft Certificate Store

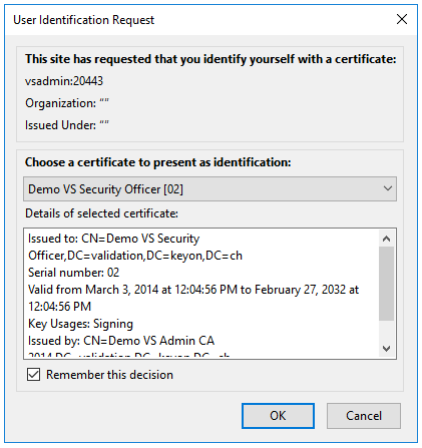
User certificates from the Microsoft Certificate Store (current user) show up using Security Device *MY* in the certificate manager:



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.

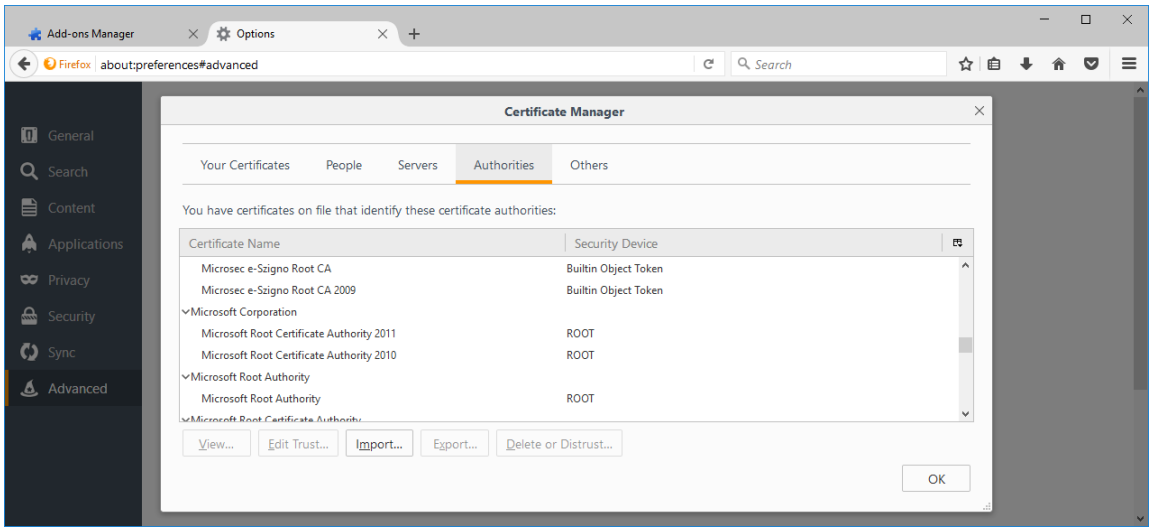
You cannot backup certificates and keys that are stored in the Microsoft Certificate Store. PKCS#11 to MS-CAPI Bridge only supports the use of keys over the CryptoAPI but not to export keys, which in case of Smart Card is impossible anyway.

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:



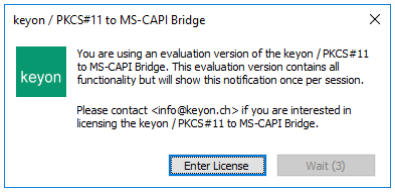
If the certificate is present in the Mozilla CA database it will always show up as *Builtin Object Token* regardless if it is also present in the Microsoft Certificate store.

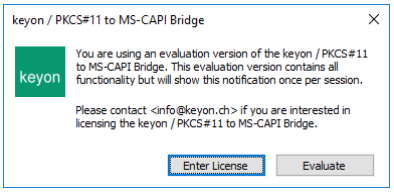
The allowed usage of the CA certificate (i.e. the trust settings) is set accordingly to the extended key usage of the certificate.

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:





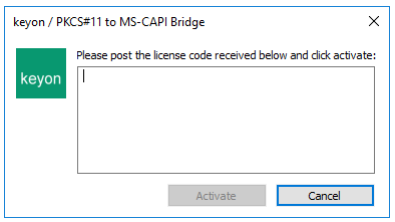
The nag screen will lock your browser window and can only be closed after some time has passed. The wait time increases over time to encourage you to purchase a license.

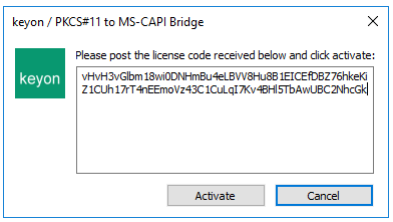
The nag-screen is only shown if you actually try to use the private key associated with a certificate provided over the MS-CAPI Bridge.

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

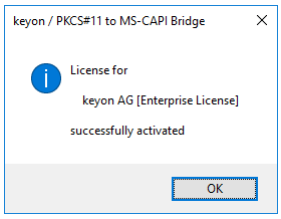
Entering the license string obtained from keyon

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



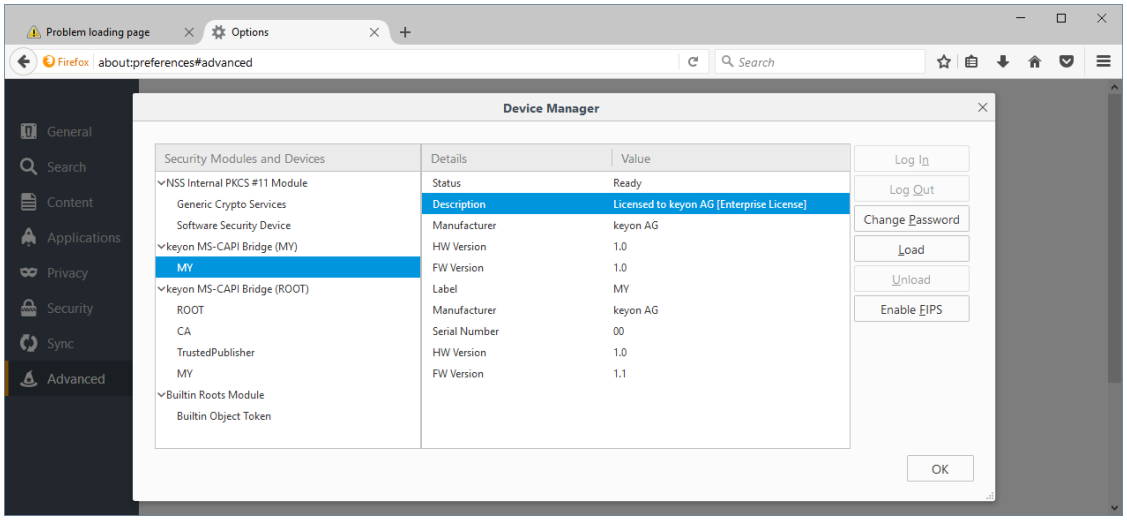


After clicking *Activate*, the licensee and license type is shown if the license is validated successfully



Checking the licensee and license type

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



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