

За инсталиране и работа с **Linux OS** на Вашия електронен подпис е необходимо да изпълните следните стъпки:

Зареждате <https://www.b-trust.bg/client-center/signature-installation>, където в полето изписвате email на сертификата и зареждате софтуер за карта от съответния модел.

Първо: От **ДРАЙВЕРИ ЗА КАРТОЧЕТЦИ** трябва да инсталирате драйвера за Вашия **четец**:
а) при модел **CCR7115**:



трябва да изтеглите **драйвер** от **COMITEX CCR LINUX** и да го инсталирате. След завършване на инсталацията, правите **задължителен рестарт** на компютъра или рестартирате **service pcsd**:

```
(U, R) sudo service pcsd restart или systemctl restart pcsd.service
```

Ако PC/SC не е инсталиран, което се среща при Debian базирани дистрибуции трябва задължително да го направите:

```
(U) sudo apt install pcsd
```

Проверка дали е активен може да направите, чрез командите:

```
(U, R) sudo service pcsd status или systemctl status pcsd.service
```

Резултатът трябва да показва, че е активен service:

```
● pcsd.service - PC/SC Smart Card Daemon
   Loaded: loaded (/lib/systemd/system/pcsd.service;
   Active: active (running) since Wed 2023-01-11 10:3
   TriggeredBy: ● pcsd.socket
```

Активиране може да се извърши, чрез:

```
(U, R) sudo service pcsd start или systemctl enable pcsd.service
```

б) друг модел четец например: **Gemalto**



или по стар е достатъчно да имате инсталиран **libccid**, който по-подразбиране трябва да го има:

```
(U) sudo apt install libccid
```

Важно: Някои дистрибуции на Linux не работят коректно с четци Omnikey!

Второ: Изтеглете софтуер за Вашата карта за **Linux** и го инсталирате: **LINUX INSTALLER**

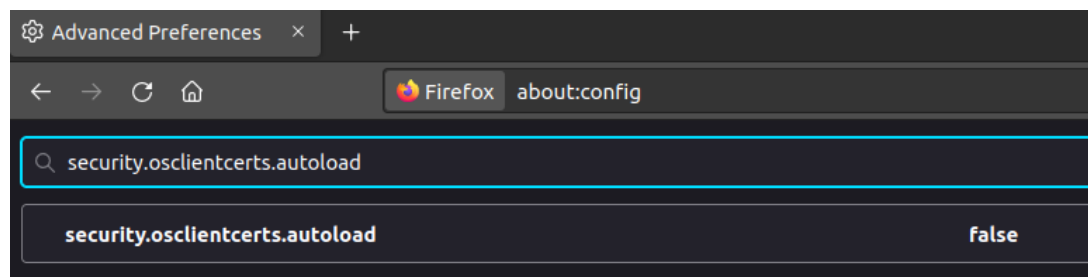
Трето: Настройки на Firefox Web Browser (**Firefox Snap** не може да зареди PKCS модул и съответно няма да могат да се изпълнят настройките по-долу):

- За версии на Firefox 90+ първо трябва да се изключи "OS Client Cert Module":

Details	Value
Module	OS Client Cert Module
Path	/usr/lib/firefox/libosclientcerts.so

За целта в адресната лента на браузъра се зарежда [about:config](#) натиска се "Accept the Risk and Continue" и в полето **Search preference name** се въвежда:

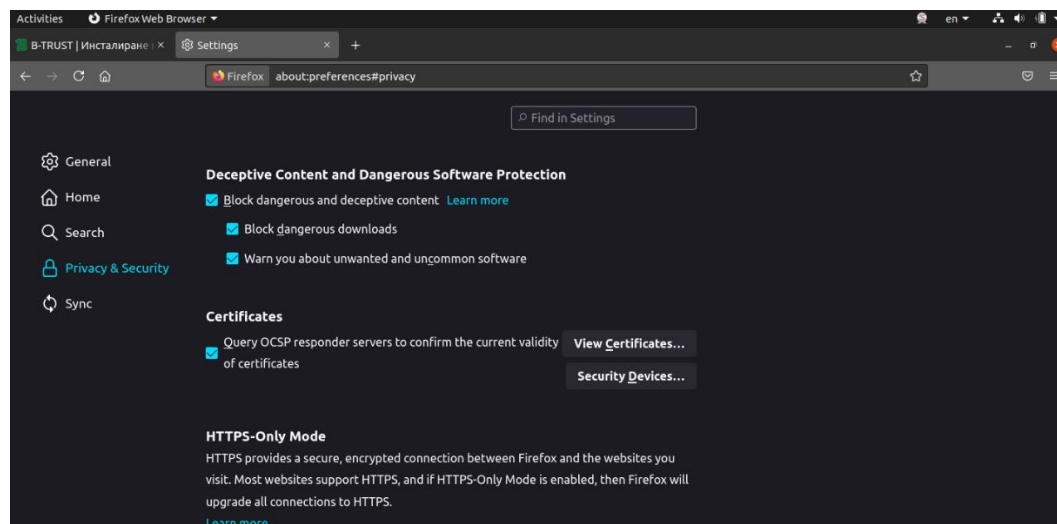
security.osclientcerts.autoload



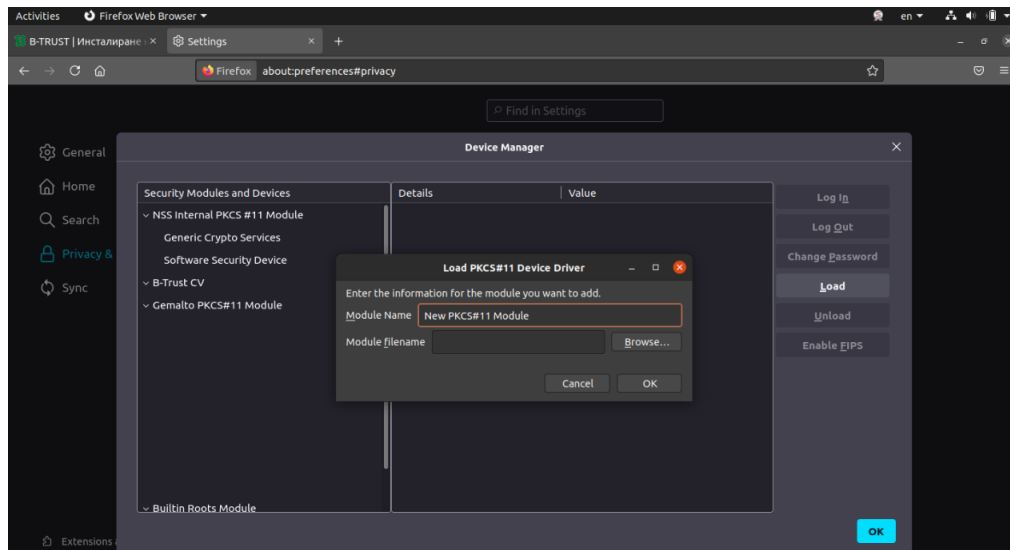
и се задава стойност "false" и се преминава към следващата стъпка.

- Необходимо е да заредите библиотеката на сертификата си във Firefox:

Preferences/Settings (Настройки) -> Privacy&Security (Поверителност и защита) -> Security Devices... (Устройства по безопасността)



Load (Зареждане) -> Задава се име на нов модул по желание -> Browse (Разглеждане)

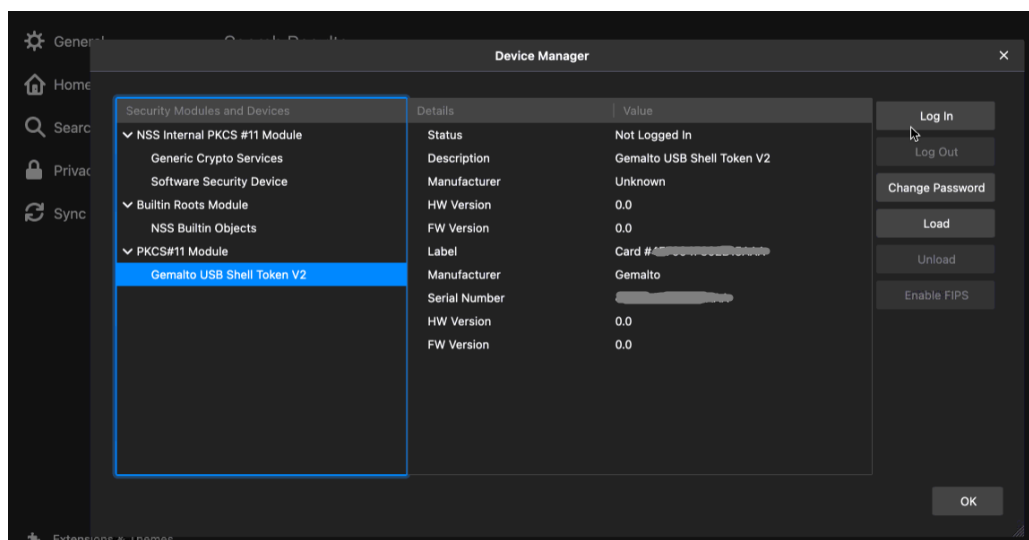


избира се път към библиотеката за карта Gemalto:

- (U) /usr/lib/pkcs11/libeTPkcs11.so
 - (R) /usr/lib64/pkcs11/libeTPkcs11.so
- или

- (U) /usr/local/lib64/libcvP11.so – за останалите видове карти.

Потвърждават се настройките. Под името на новосъздадения модул трябва да се зареди поставения четец. В полета „Details” и „Value” трябва да се заредят данни в **Label**, **Manufacturer** – ‘модел на картата’ и **Serial Number**.



- запишете локално на машината следните сертификати:

http://ca.b-trust.org/repository/B-TrustRootQA_DER.crt

http://ca.b-trust.org/repository/B-TrustRootACA_DER.crt

http://ca.b-trust.org/repository/ca5/RootCA5_DER.crt

http://ca.b-trust.org/repository/B-TrustOperationalQA_DER.crt

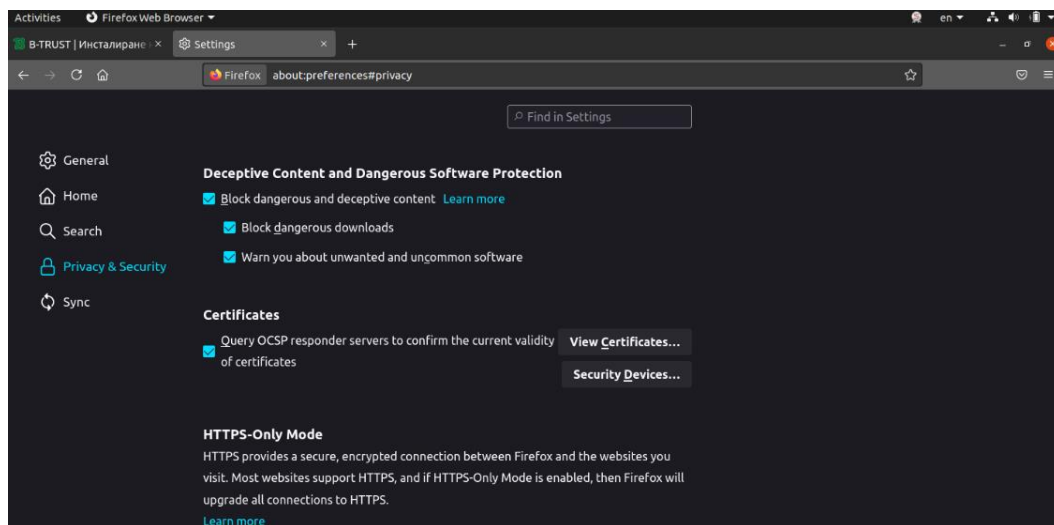
http://ca.b-trust.org/repository/B-TrustOperationalACA_DER.crt

http://ca.b-trust.org/repository/ca5/OperCA5QES_DER.cer

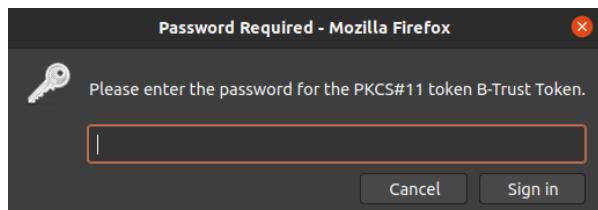
http://ca.b-trust.org/repository/ca5/OperCA5AES_DER.cer

Трябва да ги добавите във Firefox.

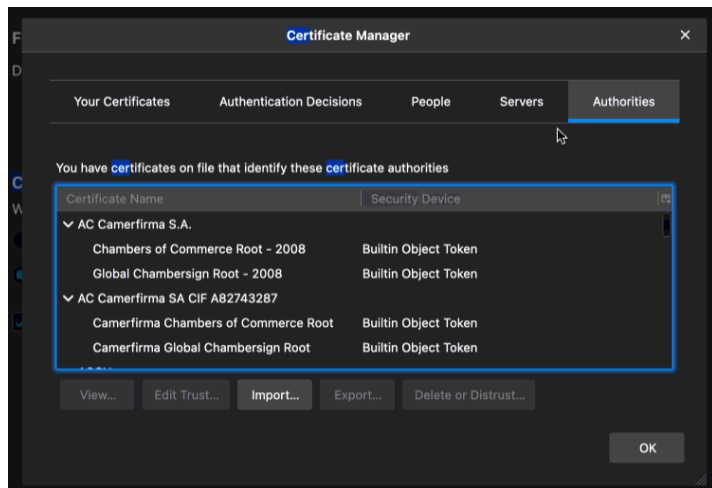
Preferences/Settings (Настройки) -> Privacy&Security (Поверителност и защита) -> View Certificates... (Преглед сертификати)



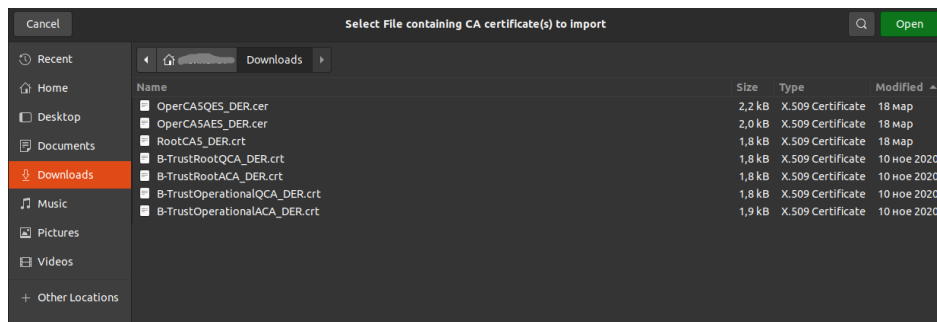
Ще излезе запитване на Вашия PIN:



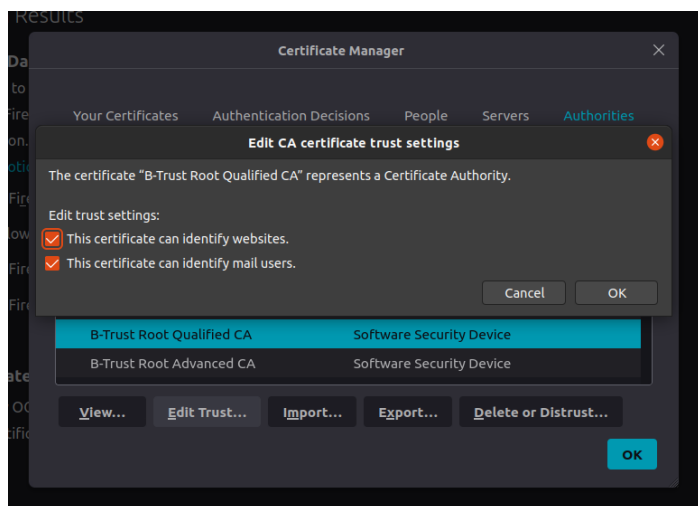
От **Certificate Manager** избирате **Authorities** (Удостоверители)



Import (Внасяне):



Всеки един сертификат се избира един по един. При импортирането е необходимо да разрешите всички права:



В „Your certificates” трябва да се появи Вашият сертификат.

ВНИМАНИЕ: Всички бутони в прозореца **Certificate Manager** работят директно върху смарт картата. Например „Delete“ ще изтрие физически от смарт картата електронния Ви подпис.

Настройките са завършени!
Опитайте да работите със сертификата в институциите, където желаете.

Ако все още имате затруднения, можете да се свържете с нас, чрез достъп с Teamviewer от следния линк: https://download.teamviewer.com/download/version_11x/teamviewer_gs.tar.gz (разархивирайте и стартирайте „teamviewer“ от същата папка)