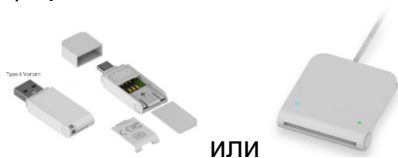


За инсталиране и работа с **Linux OS** на Вашия електронен подпис е необходимо да изпълните следните стъпки:

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:

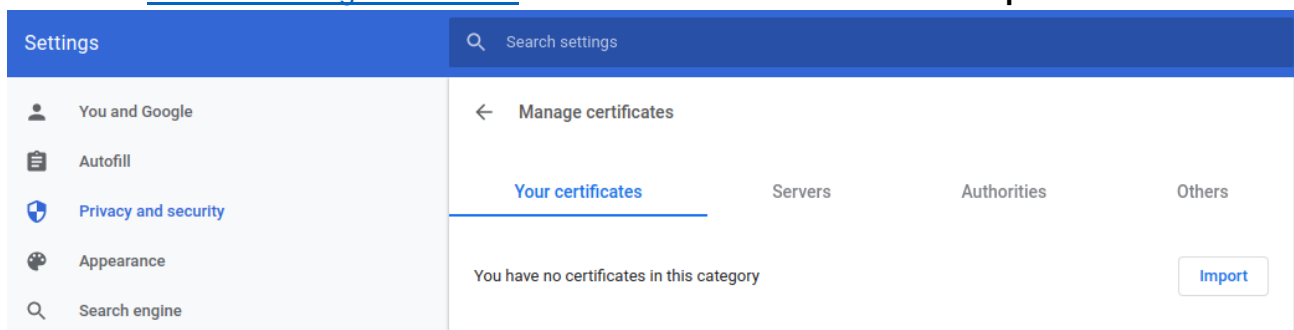
```
(U) sudo apt install libccid
```

**Важно:** Браузъра Google Chrome не работи коректно с четци Omnikey!

**Второ:** Изтегляте софтуер за Вашата карта за **Linux** и го инсталирайте: **LINUX INSTALLER**

**Трето:** Настройки на **Google Chrome**:

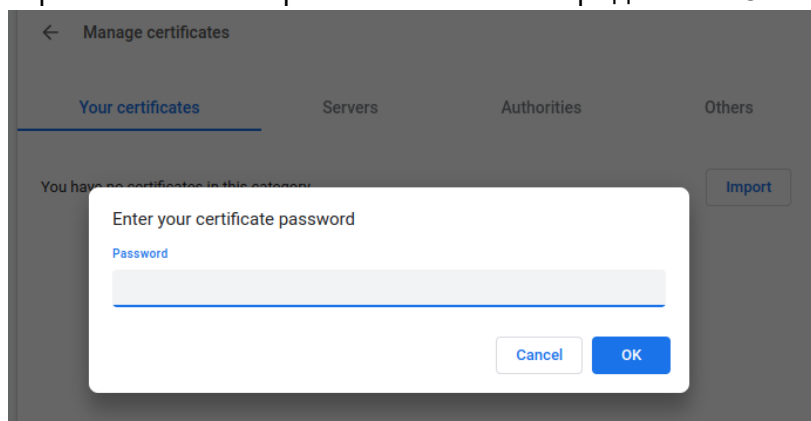
1. Изтегляте и записвате като файл от <https://www.b-trust.bg/queries/certification-chains-installation> автоматичния инсталатор за всички удостоверителни вериги на B-Trust – **СВАЛЕТЕ ФАЙЛ**
2. В Google Chrome от менюто изберате:
  - a. **Settings** → **Privacy and security** → **Security** → **Manage certificates** и от **Your certificates** и натискате **Import**
  - или
  - b. В адресната лента на Chrome зареждате: <chrome://settings/certificates> и от **Your certificates** натискате **Import**



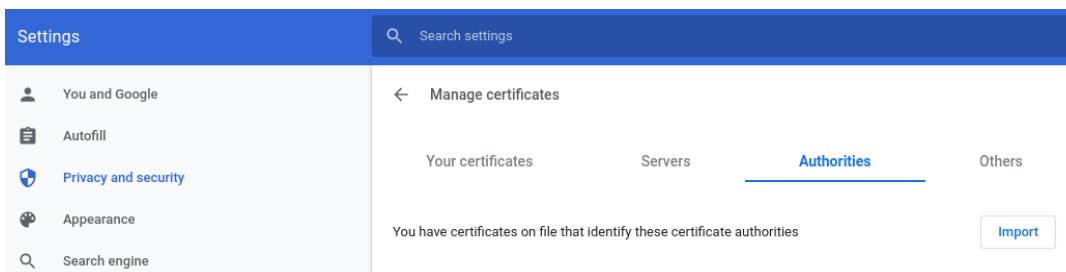
Изберате и зареждате файла **Btrust-Cas.p12**, който сте изтеглили от точка 1:



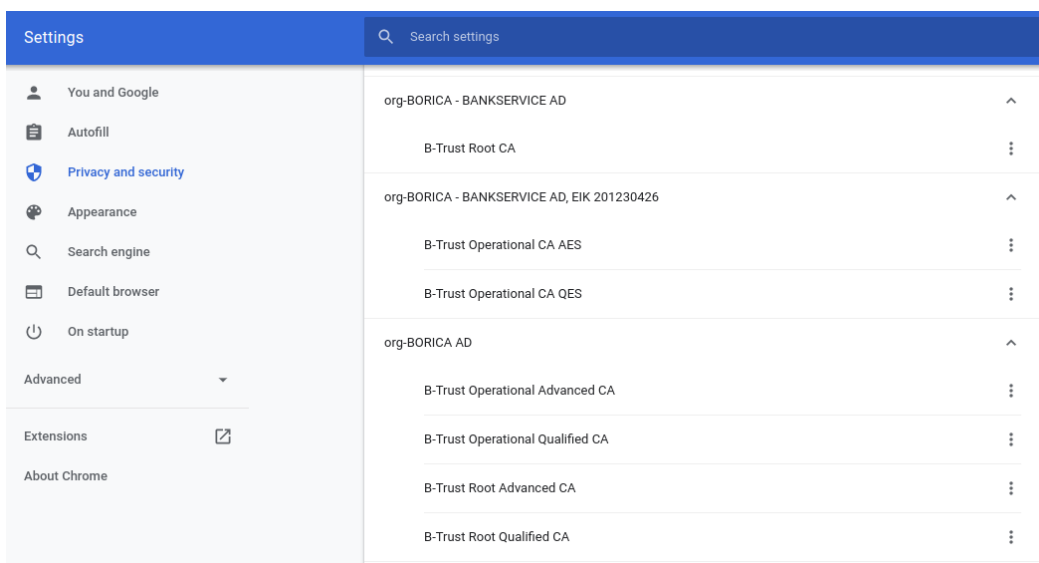
Ще Ви поиска парола – оставяте празно полето и потвърждавате с **OK**.



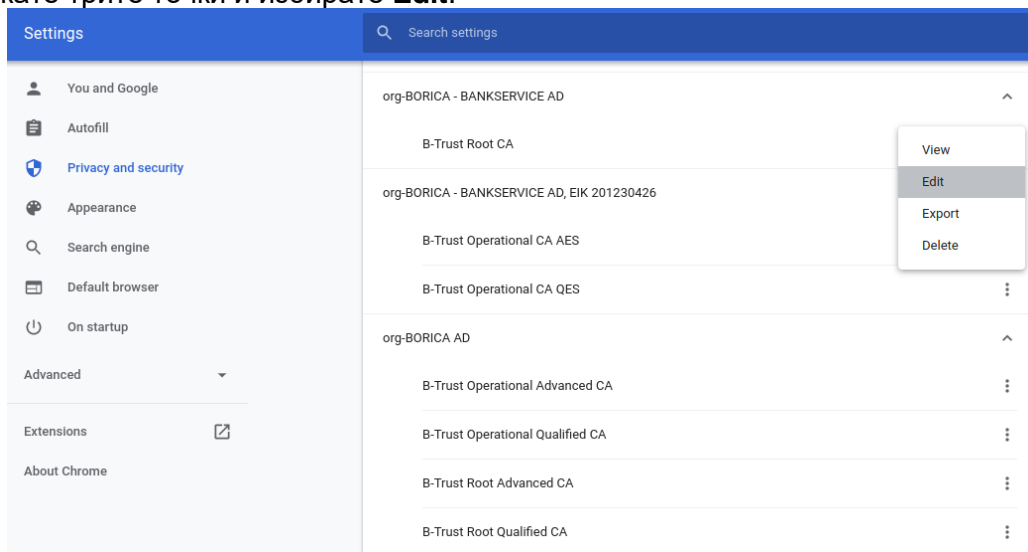
След това от горе избирате **Authorities**:



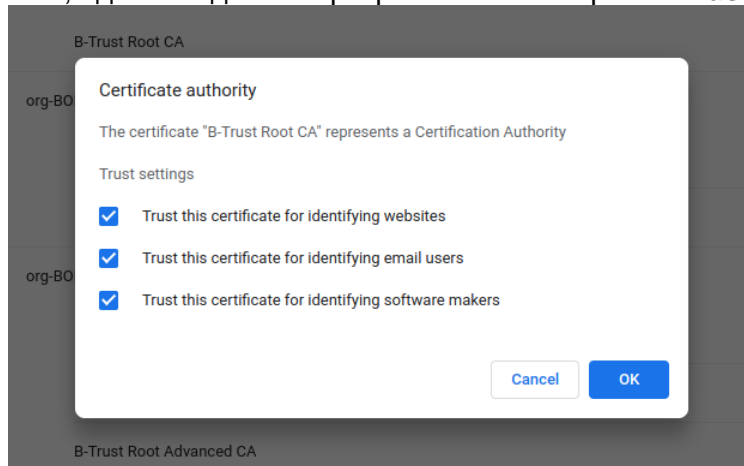
Намирате всички седем сертификата на **B-Trust**, както са показани:



Натискате трите точки и избирате **Edit**:



За всеки сертификат, един по един и маркирате всяка настройка **Trust this certificate...**



### 3. Отваряте **Terminal**

a. Инсталирате инструментите за работа с NSS:

(U) `sudo apt install libnss3-tools`

(R) `su -c "yum install nss-tools"`

b. Затваряте **Google Chrome** и изключвате подписа от компютъра.

c. Създавате директория за базата данни на NSS

(U, R) `mkdir -p $HOME/.pki/nssdb`

d. Изпълнявате следната команда:

- за карта тип Gemalto (U, R):

```
modutil -add "PKCS11_Gemalto" -libfile libeTPkcs11.so -dbdir sql:$HOME/.pki/nssdb -mechanisms FRIENDLY
```

- за карта тип Cryptovision - **само за Debian базирани дистрибуции** (U):

```
modutil -add "PKCS11_CV" -libfile /usr/local/lib64/libcvP11.so -dbdir sql:$HOME/.pki/nssdb -mechanisms FRIENDLY
```

Трябва да получите резултат:

*Module "PKCS11\_Gemalto" added to database* или съответно: *Module "PKCS11\_CV" added to database*

Можете да проверите добавените модули с команда:

(U, R) `modutil -dbdir sql:$HOME/.pki/nssdb -list`

Може да включите подписа в компютъра и да стартирате **Google Chrome**.

Настройките са завършени!

Ако все още имате затруднения, можете да се свържете с нас, и чрез достъп с Teamviewer от следния линк:

[https://download.teamviewer.com/download/version\\_11x/teamviewer\\_gs.tar.gz](https://download.teamviewer.com/download/version_11x/teamviewer_gs.tar.gz)

(разархивирайте и стартирайте „teamviewer“ от същата папка)