

# SafeNet Authentication Client

---

NAVODILA ZA UPORABO v1.0

CREAplus

## Navodila - SafeNet Authentication Client Pametna kartica/ključ USB Gemalto

CREAplus  
CREA plus d.o.o.  
[www.creaplus.si](http://www.creaplus.si)  
[info@creaplus.si](mailto:info@creaplus.si)

Morebitna novejša različica tega dokumenta je dostopna na spletnih straneh [www.creaplus.si](http://www.creaplus.si).

Windows je registrirana blagovna znamka podjetja Microsoft.

Mac je registrirana blagovna znamka podjetja Apple.

Ostale uporabljene blagovne znamke, logotipi, imena, slike in druge avtorske pravice so last njihovih lastnikov.

Distribucija tega dokumenta v bistveno spremenjeni različici ali v kakršnikoli papirni obliki za prodajne namene brez predhodnega dovoljenja imetnika avtorskih pravic ni dovoljena.

### Izjava o omejitvi odgovornosti

Proizvajalec in avtorji si pridržujejo pravice do kakršnekoli spremembe ali izboljšave tako pri izdelku kot tudi v navodilih, kadarkoli in brez predhodne najave. Proizvajalec in avtorji ne sprejemajo nobene odgovornosti v primeru težav, ki posredno ali neposredno izhajajo iz napak ali nepopolnosti izdelka ali navodil. Informacije v teh navodilih so veljavne od datuma izdaje navodil.

## Contents

1	SafeNet Authentication Client .....	4
2	Potek namestitve SafeNet Authentication Client .....	4
2.1	Windows .....	4
2.1.1	Odstranitev komponent IDGo800 .....	4
2.1.2	Namestitev SafeNet Authentication Client .....	5
2.1.3	Namestitev knjižnjice PKCS#11 za brskalnik Mozilla Firefox .....	6
2.2	MacOS.....	8
2.2.1	Odstranitev komponent IDGo800 .....	8
2.2.2	Namestitev SafeNet Authentication Client .....	9
2.2.3	Namestitev knjižnjice PKCS#11 za brskalnik Mozilla Firefox .....	11
2.3	Linux - Ubuntu .....	13
2.3.1	Namestitev SafeNet Authentication Client .....	13
2.3.2	Namestitev knjižnjice PKCS#11 za brskalnik Mozilla Firefox .....	14
3	Spreminjanje kode PIN .....	15
4	Odklepanje kode PIN .....	17
5	Upravljanje z digitalnimi potrdili .....	18
5.1	Uvoz digitalnega potrdila na pametno kartico/ključ.....	18
5.2	Izbris digitalnega potrdila .....	21

## 1 SafeNet Authentication Client

Programska oprema SafeNet Authentication Client je namenjena upravljanju in uporabi pametne kartice ali pametnega ključa Gemalto.

Pametne kartice Gemalto in pametni ključi USB Gemalto (K30, K50,..) so naprave z zmogljivim kriptografskim procesorjem za varno shranjevanje digitalnih potrdil. Zasebnega ključ digitalnega potrdila s pametne kartice/ ključa USB ni možno prenesti oziroma izvoziti na lokacijo, kjer bi lahko bil zlorabljen.

Orodja programske opreme SafeNet Authentication Client omogočajo:

- Pregled digitalnih potrdil na pametni kartici/ključu Gemalto,
- uvoz digitalnega potrdila iz varnostne kopije (.pfx, .p12) na pametno kartico/ključ USB Gemalto,
- spreminjanje kode PIN na pametni kartici/ključu USB Gemalto,
- odklepanje kode PIN s pomočjo kode PUK (odklepanje zaklenjene pametne kartice/ključa USB),
- uporaba pametne kartice v spletnem brskalniku Mozilla Firefox (z uvozom knjižnice PKCS#11).

## 2 Potek namestitve SafeNet Authentication Client

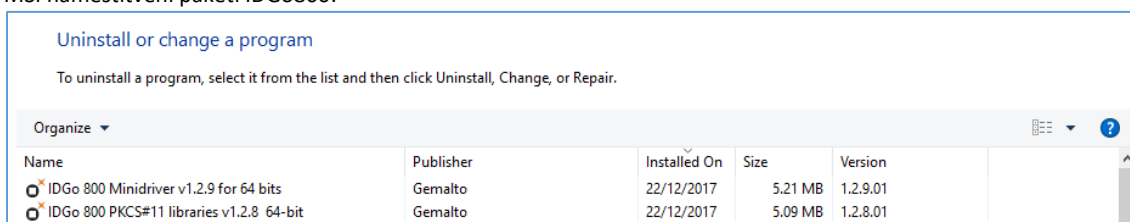
### 2.1 Windows

#### 2.1.1 Odstranitev komponent IDGo800

V kolikor smo na računalniku že uporabljali pametno kartico/ključ Gemalto s programsko opremo IDGo 800, je to potrebno odstraniti pred namestitvijo medprogramja Safenet Authentication Client.

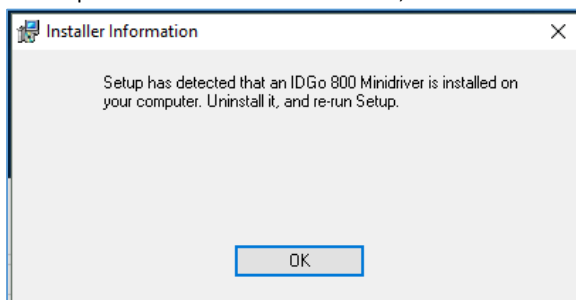
Pakete MSI odstranimo po klasičnem postopku za odstranitev programov v operacijskem sistemu Windows (**Programs and Features**).

MSI namestitveni paketi IDGo800:



Trenutna namestitev:	Potek namestitve SAC:
IDGo 800 Minidriver »Plug nad Play«	- namestitev medprogramja SAC
IDGo 800 Minidriver »Plug and Play«	- Odstranitev MSI paketa IDGo 800 PKCS11
IDGo 800 PKCS11 (MSI namestitveni paket)	- Namestitev medprogramja SAC
IDGo 800 Minidriver (MSI namestitveni paket)	- Odstranitev MSI paketa IDGo 800 minidriver
IDGo 800 PKCS11 (MSI namestitveni paket)	- Odstranitev MSI paketa IDGo 800 PKCS11
	- Namestitev medprogramja SAC

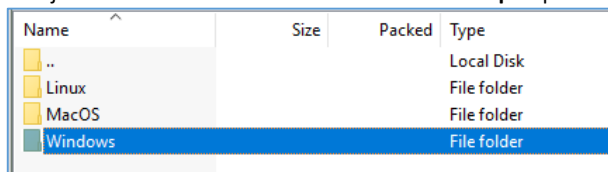
Če MSI paketov IDGo 800 ne odstranimo, namestitev SafeNet Authentication Client-a ni mogoča.



## 2.1.2 Namestitev SafeNet Authentication Client

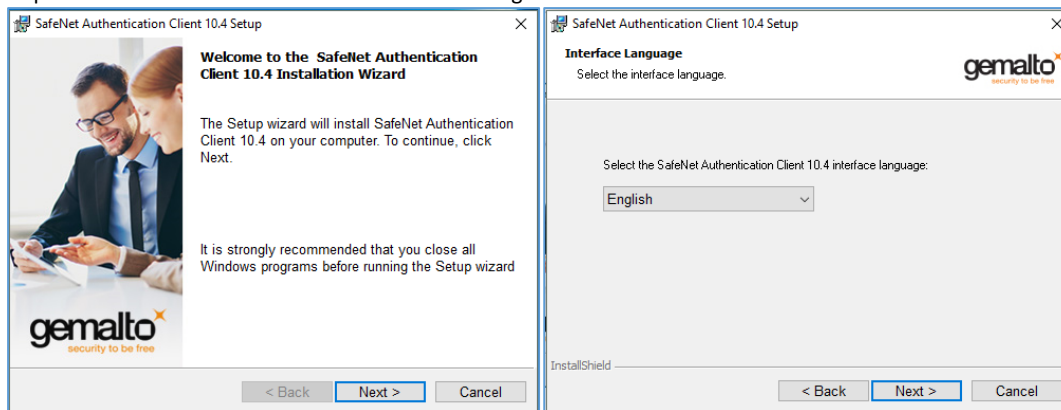
Sledimo postopku za namestitev medprogramja SAC:

1. Stisnjeno datoteko **SafeNetAuthenticationClient.zip** odpremo in jo razširimo na poljubno mesto.

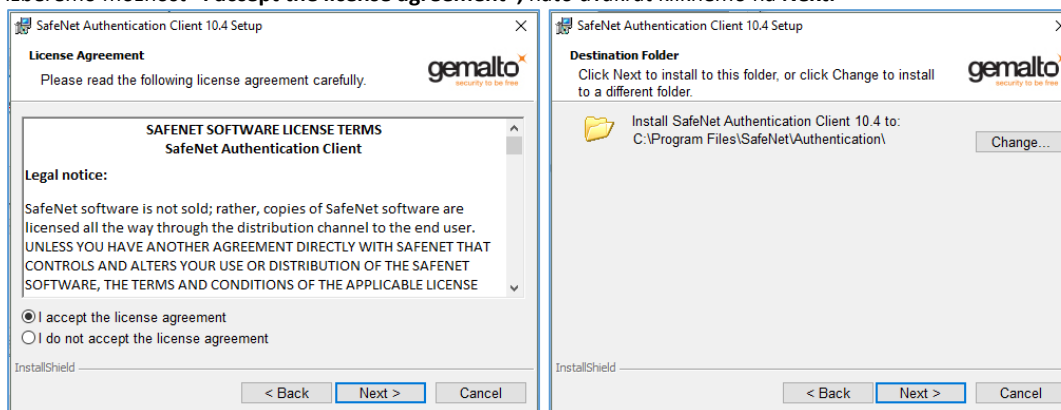


2. Za namestitev na operacijskem sistemu Windows, odpremo datoteko Windows.
3. Zaženemo ustrezen namestitveni paket, ki je primeren za naš operacijski sistem – 64-bitni ali 32-bitni.
  - SafeNetAuthenticationClient-x32-10.4.msi (32-bit)
  - SafeNetAuthenticationClient-x64-10.4.msi (64-bit)

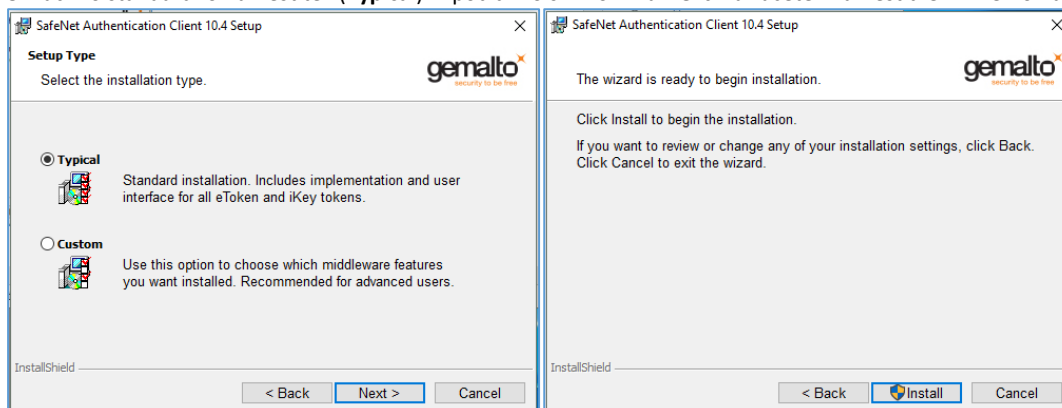
4. Odpre se čarovnik za namestitev. Dvakrat izberemo gumb **Next**.



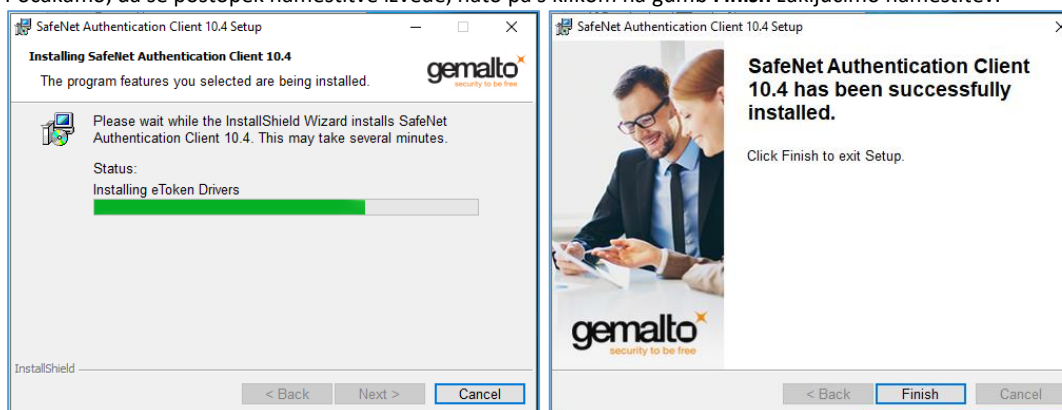
5. Izberemo možnost **“I accept the license agreement”**, nato dvakrat kliknemo na **Next**.



6. Označimo standardno namestitev (**Typical**) in potrdimo s klikom na **Next**. Za začetek namestitve kliknemo na **Install**.



7. Počakamo, da se postopek namestitve izvede, nato pa s klikom na gumb **Finish** zaključimo namestitev.

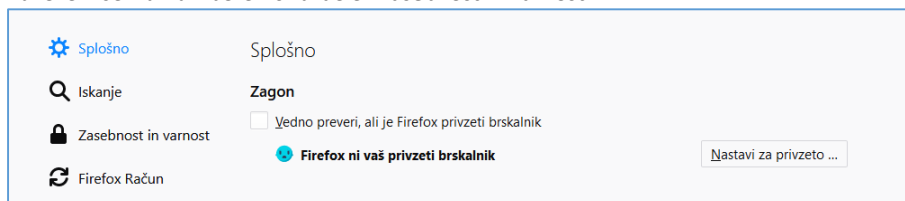


### 2.1.3 Namestitev knjižnice PKCS#11 za brskalnik Mozilla Firefox

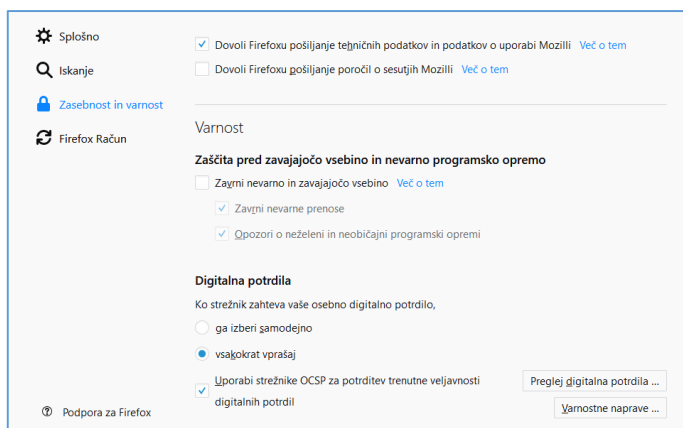
Za uporabo pametne kartice/ključa USB Gemalto v spletnem brskalniku Mozilla Firefox, je potrebno v Firefox uvoziti poseben modul PKCS#11.

Sledimo postopku:

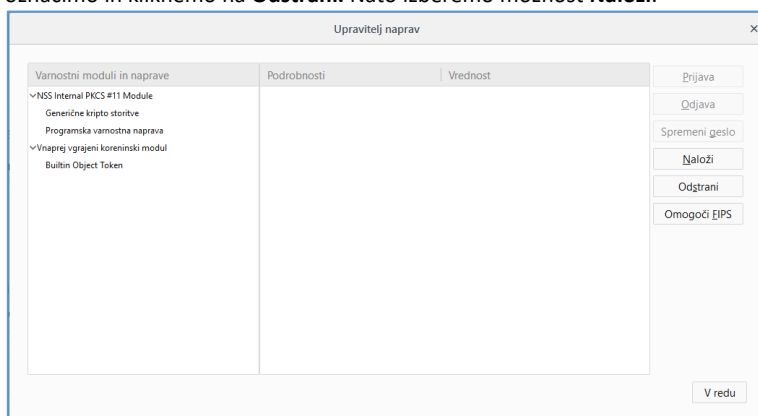
1. Zaženemo brskalnik Mozilla Firefox in v meniju ☰ izberemo **Možnosti**.
2. Na levem seznamu izberemo razdelek **Zasebnost in varnost**.



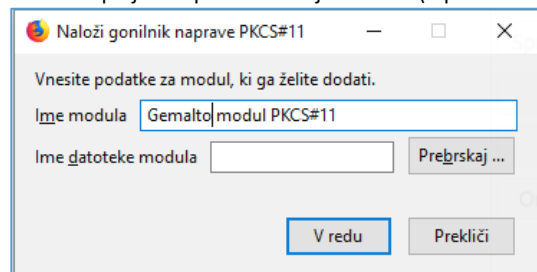
3. Pomaknemo se na dno okna in kliknemo na **Varnostne naprave...**



4. V kolikor je na seznamu **“Varnostni moduli in naprave”** že prisoten modul za uporabo pametne kartice Gemalto, tega označimo in kliknemo na **Odstrani**. Nato izberemo možnost **Naloži**.

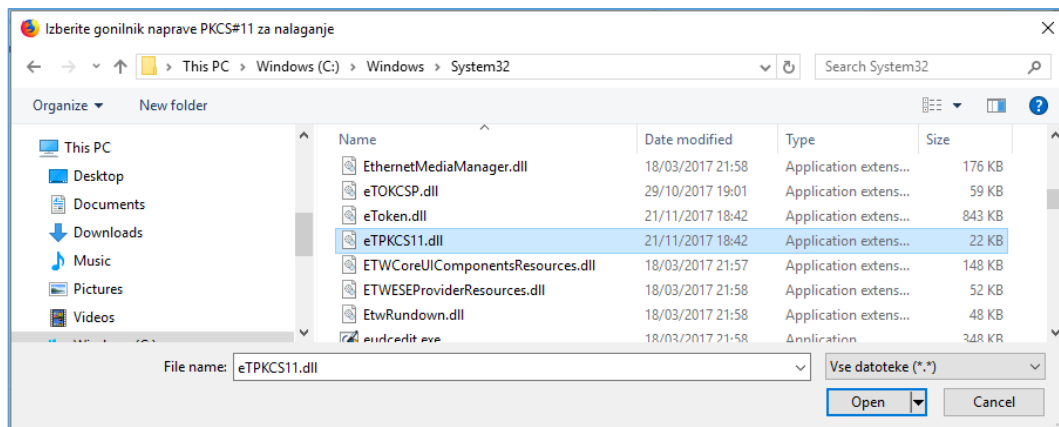


5. Vnesemo poljubno poimenovanje modula ( npr. Gemalto modul PKCS#11). Kliknemo na gumb **Prebrskaj...**

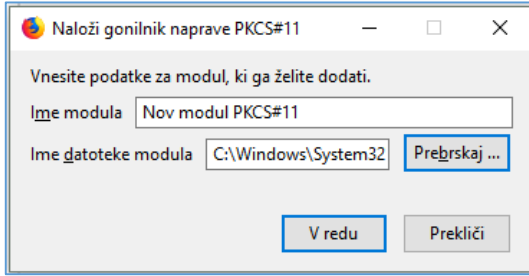


6. V file explorerju poiščemo in označimo ustezen modul , nato kliknemo **Open**.

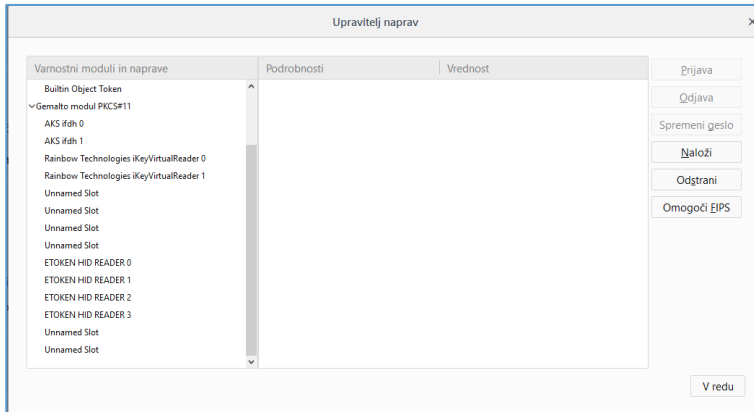
- C:\Windows\System32\eTPKCS11.dll (64-bitni brskalnik)
- C:\Windows\SysWOW64\eTPKCS11.dll (32-bitni brskalnik)



- S klikom na gumb **V redu** dodamo modul.



- Modul je nato prikazan na seznamu "**Varnostni moduli in naprave**". S tem je omogočena uporaba pametne kartice v spletnem brskalniku Mozilla Firefox.

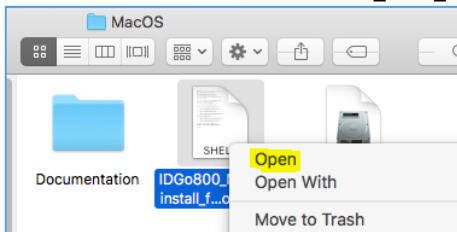


## 2.2 MacOS

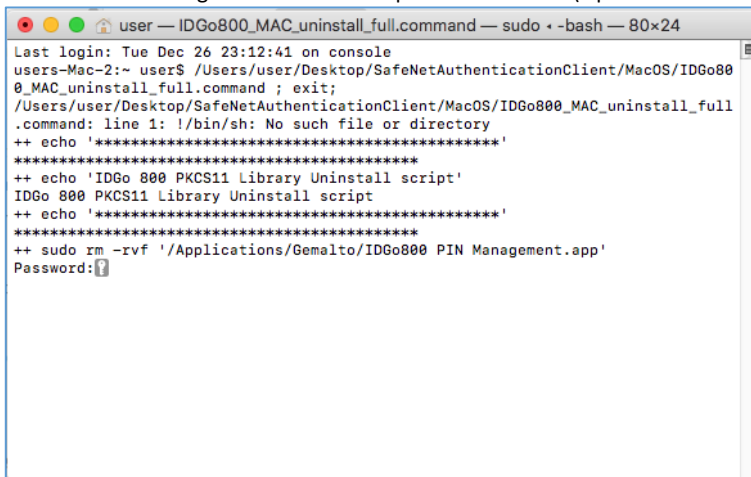
### 2.2.1 Odstranitev komponent IDGo800

V kolikor smo na računalniku že uporabljali pametno kartico/ključ Gemalto s programsko opremo IDGo 800, je to potrebno odstraniti pred namestitvijo medprogramja Safenet Authentication Client. Sledimo postopku:

- Desno kliknemo na datoteko **IDGo800\_MAC\_uninstall\_full.command** in izberemo **Open**.



- Vnesemo skrbniško geslo računalnika in potrdimo z **Enter**. (Opomba: Ob vnašanju gesla se znaki ne prikazujejo)





- Izvede se odstranitev paketa IDGo 800.

```

user — IDGo800_MAC_uninstall_full.command — 80x24
/usr/local/lib/PKCS11/libidprimepkcs11.dylib
++ '[' -f /usr/lib/pkcs11/libidprimepkcs11.dylib ']'
++ '[' -f /usr/lib/libidprimepkcs11.0.dylib ']'
++ '[' -f /Library/Documentation/Gemalto/Gemalto.PKCS11.ini ']'
++ '[' -d /usr/lib/IDPrimePKCS11 ']'
++ '[' -d /System/Library/Security/tokened/PKCS11.tokened ']'
++ '[' -d /Library/LaunchAgents/pinGuiForTokened ']'
++ sudo pkgutil --forget com.gemalto.idgo800Pkcs11.pkg
No receipt for 'com.gemalto.idgo800Pkcs11.pkg' found at '/'.
++ sudo pkgutil --forget com.gemalto.idgo800Pkcs11ElCapitan.pkg
Forgot package 'com.gemalto.idgo800Pkcs11ElCapitan.pkg' on '/'.
++ sudo pkgutil --forget com.gemalto.idgo800Pkcs11Yosemite.pkg
No receipt for 'com.gemalto.idgo800Pkcs11Yosemite.pkg' found at '/'.
++ echo Done.
Done.
logout
Saving session...
...copying shared history...
...saving history...truncating history files...
...completed.
Deleting expired sessions...4 completed.

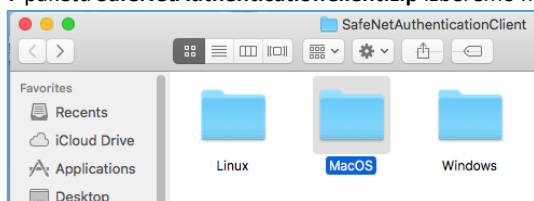
[Process completed]
    
```

- Terminalno okno zapremo in izvedemo ponovni zagon računalnika.

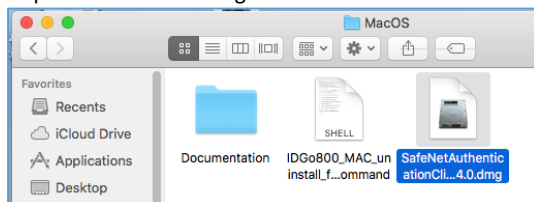
## 2.2.2 Namestitev SafeNet Authentication Client

Sledimo postopku za namestitev medprogramja SAC:

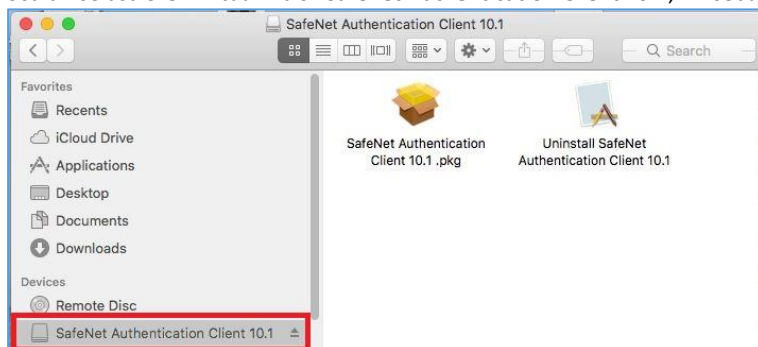
- V paketu **SafeNetAuthenticationClient.zip** izberemo mapo za namestitev na operacijski sistem MacOS.



- Odpremo datoteko .dmg.



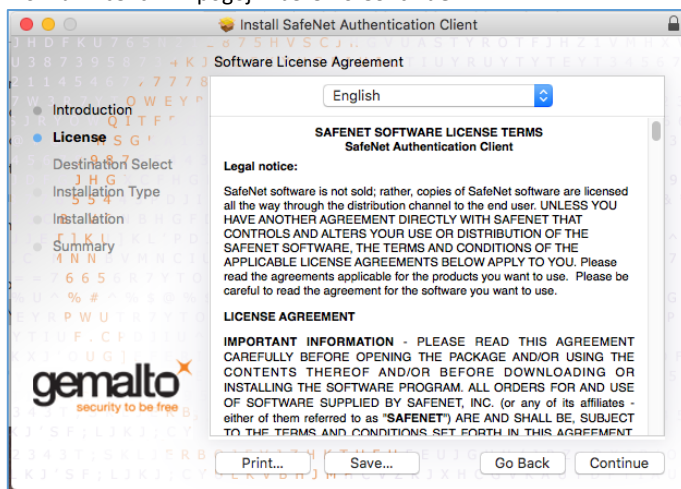
- Ustvari se ustrezen virtualni disk **SafeNet Authentication Client 10.1**, ki vsebuje namestitveni paket .pkg.



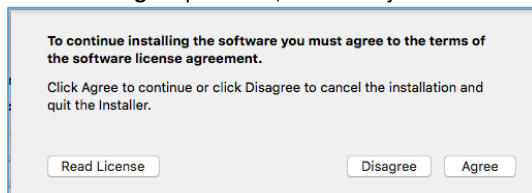
- Zaženemo paket **SafeNet Authentication Client 10.1.pkg** in dvakrat izberemo **Continue**.



5. V oknu z licenčnimi pogoji izberemo **Continue**.



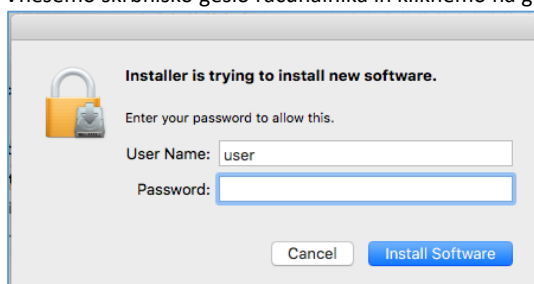
6. S klikom na **Agree** potrdimo, da se strinjamo z licenčnimi pogoji.



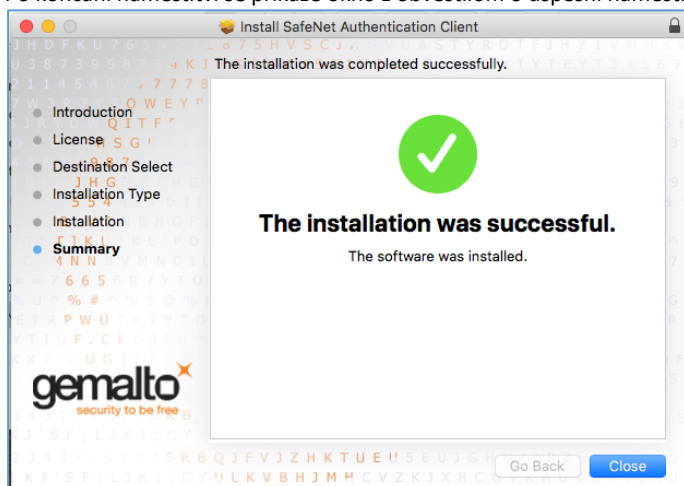
7. Kliknemo **Install**, s čimer pričnemo postopek namestitve.



- Vnesemo skrbniško geslo računalnika in kliknemo na gumb **Install Software**.



- Po končani namestitvi se prikaže okno z obvestilom o uspešni namestitvi.



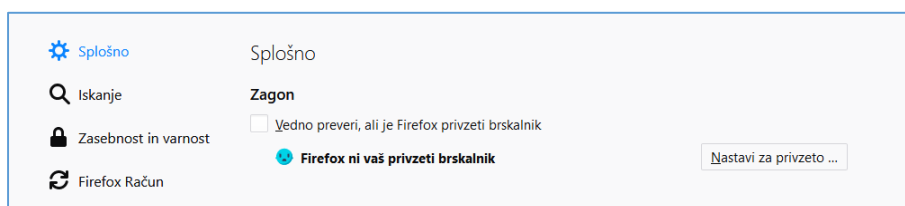
- Okno zapremo in izvedemo ponovni zagon računalnika.

### 2.2.3 Namestitev knjižnice PKCS#11 za brskalnik Mozilla Firefox

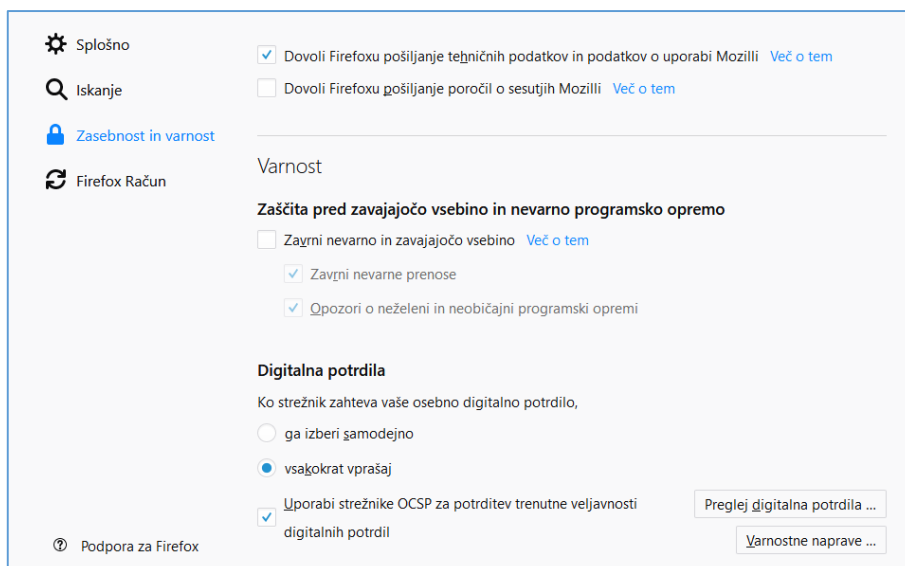
Za uporabo pametne kartice/ključca USB Gemalto v spletnem brskalniku Mozilla Firefox, je potrebno v Firefox uvoziti poseben modul PKCS#11.

Sledimo postopku:

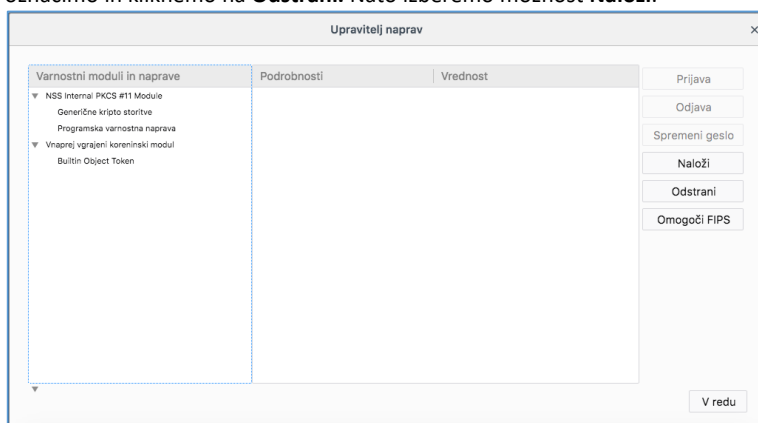
- Zažene brskalnik Mozilla Firefox in v meniju ☰ izberemo **Nastavitve**.
- Na levem seznamu izberemo razdelek **Zasebnost in varnost**.



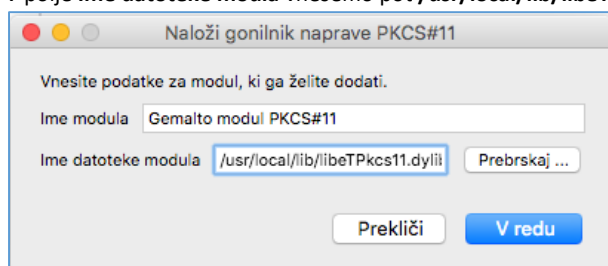
- Pomaknemo se na dno okna in kliknemo na **Varnostne naprave...**



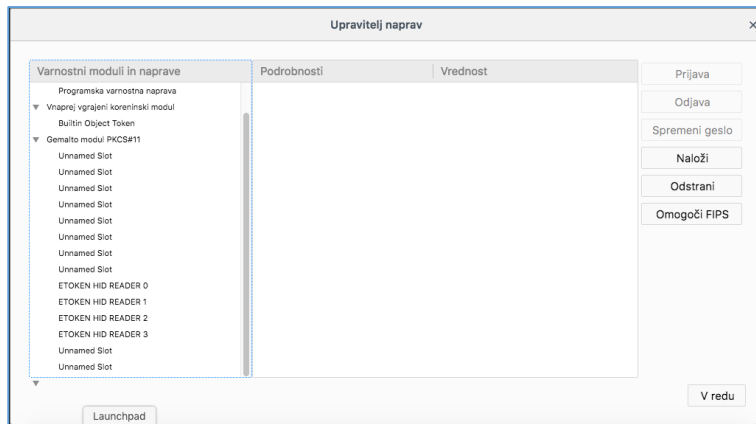
4. V kolikor je na seznamu “**Varnostni moduli in naprave**” že prisoten modul za uporabo pametne kartice Gemalto, tega označimo in kliknemo na **Odstrani**. Nato izberemo možnost **Naloži**.



5. V polje **Ime modula** vnesemo poljubno ime (npr. Gemalto modul PKCS#11). V polje **Ime datoteke modula** vnesemo pot **/usr/local/lib/libeTPkcs11.dylib** in potrdimo s klikom na **V redu**.



6. Modul je nato prikazan na seznamu “**Varnostni moduli in naprave**”. S tem je omogočena uporaba pamente kartice/ključa v spletnem brskalniku Mozilla Firefox.



## 2.3 Linux – Ubuntu 17.04

### 2.3.1 Namestitev SafeNet Authentication Client

1. Za namestitev medprogramja SafeNet Authentication Client na distribuciji Ubuntu, uporabimo Debian programski paket.
  - 32-bit: SafenetAuthenticationClient-core-10.0.xx-0\_i386.deb
  - 64-bit: SafenetAuthenticationClient-core-10.0.xx-0\_amd64.deb
2. Zaženemo terminal, odpremo mapo z namestitvenimi paketi .deb in izvedemo ukaz.

```

user@user-virtual-machine: ~/Desktop/DEB/Standard
user@user-virtual-machine:~/Desktop/DEB/Standard$ ls
SafenetAuthenticationClient-10.0.37-0_amd64.deb
SafenetAuthenticationClient-10.0.37-0_i386.deb
user@user-virtual-machine:~/Desktop/DEB/Standard$ sudo dpkg -i SafenetAuthentic
tionClient-10.0.37-0_amd64.deb

```

Vnesemo ukaz, ki mu prilagodimo ime namestitvenega paketa .deb:

- 32-bit OS: sudo dpkg -i SafenetAuthenticationClient-core-10.0.xx-0\_i386.deb
- 64-bit OS: sudo dpkg -i SafenetAuthenticationClient-core-10.0.xx-0\_amd64.deb

3. Vnesemo root geslo in potrdimo.

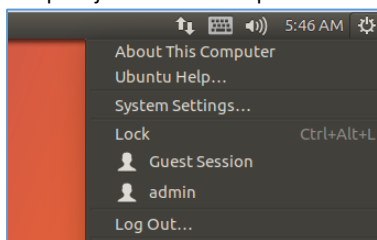
```

user@user-virtual-machine: ~/Desktop/DEB/Standard
user@user-virtual-machine:~/Desktop/DEB/Standard$ sudo dpkg -i SafenetAuthentic
tionClient-10.0.37-0_amd64.deb
[sudo] password for user:
(Reading database ... 169133 files and directories currently installed.)
Preparing to unpack SafenetAuthenticationClient-10.0.37-0_amd64.deb ...
Terminating eToken Service... done
[...] Stopping pcsd (via systemctl): pcsd.serviceWarning: Stopping pcsd.serv
ice, but it can still be activated by:
  pcsd.socket
. ok
Unpacking safenetauthenticationclient (10.0.37-0) over (10.0.37-0) ...
Setting up safenetauthenticationclient (10.0.37-0) ...
cat: /etc/xdg/menus/applications.menu: No such file or directory
warning: can't add eToken submenu
[...] Stopping pcsd (via systemctl): pcsd.serviceWarning: Stopping pcsd.serv
ice, but it can still be activated by:
  pcsd.socket
. ok
pcsd: no process found
[ ok ] Starting pcsd (via systemctl): pcsd.service.
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for systemd (232-21ubuntu2) ...
Processing triggers for libc-bin (2.24-9ubuntu2) ...
user@user-virtual-machine:~/Desktop/DEB/Standard$

```

Opomba: V kolikor pride do napake pri namestitvi zaradi odvisnosti od drugih programskih paketov, izvedemo ukaz `sudo apt-get install f`, nato pa ponovimo točko 2.

- Po opravljeni namestitvi uporabnika odjavimo in ponovno prijavimo v sistem.

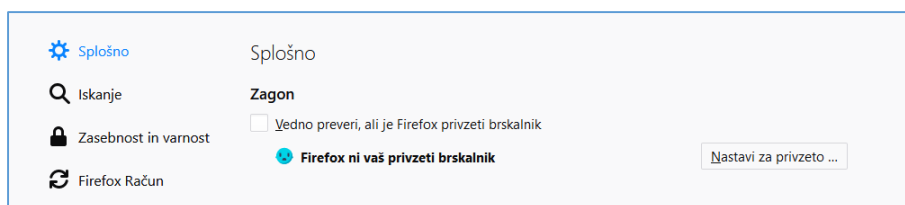


- Aplikacija SafeNet Authentication Client Tools je nato vidna v opravilni vrstici.

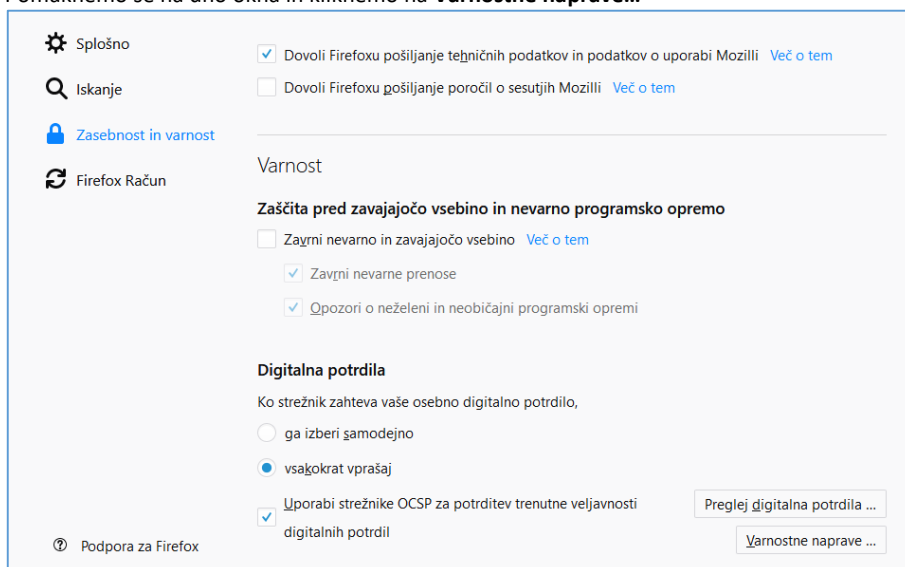


### 2.3.2 Namestitev knjižnice PKCS#11 za brskalnik Mozilla Firefox

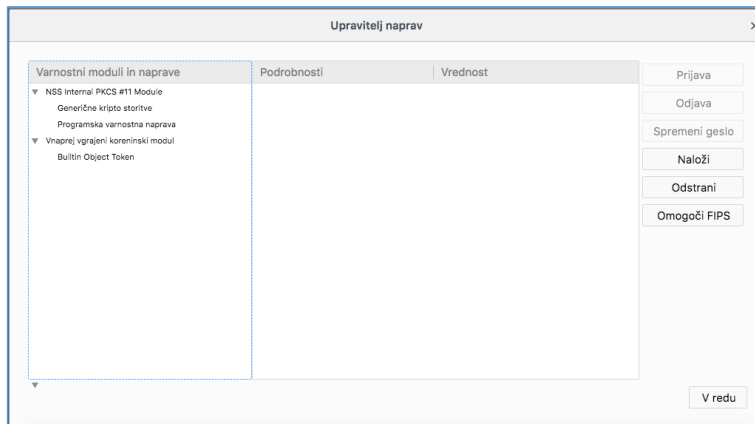
- Zaženemo brskalnik Mozilla Firefox in v meniju ☰ izberemo **Nastavitve**.
- Na levem seznamu izberemo razdelek **Zasebnost in varnost**.



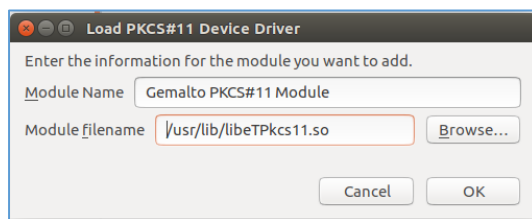
- Pomaknemo se na dno okna in kliknemo na **Varnostne naprave...**



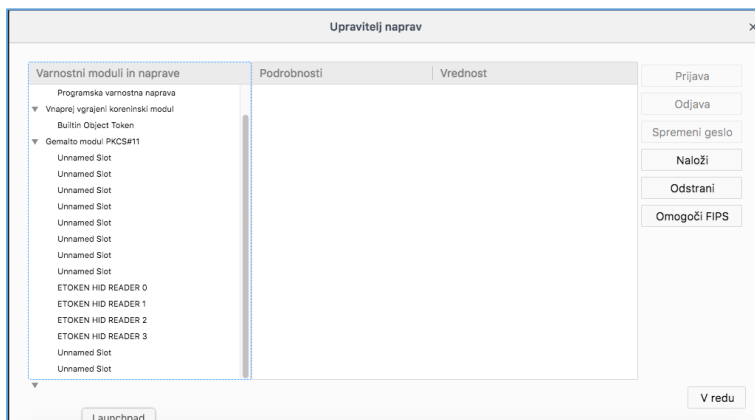
- V kolikor je na seznamu **“Varnostni moduli in naprave”** že prisoten modul za uporabo pametne kartice Gemalto, tega označimo in kliknemo na **Odstrani**. Nato izberemo možnost **Naloži**.



5. V polje **Module Name** vnesemo poljubno ime (npr. Gemalto module PKCS#11).  
V polje **Module filename** vnesemo pot `/usr/lib/libeTPkcs11.so` in potrdimo s klikom na **OK**.



6. Modul je nato prikazan na seznamu "**Varnostni moduli in naprave**". S tem je omogočena uporaba pamente kartice/ključa v spletnem brskalniku Mozilla Firefox.



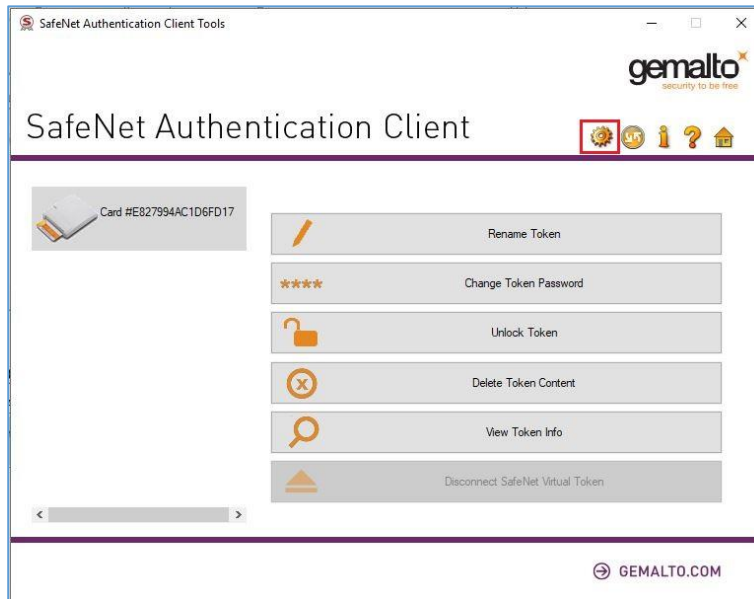
## 3 Spreminjanje kode PIN

Za izvedbo spremembe uporabniškega PINa sledimo postopku:

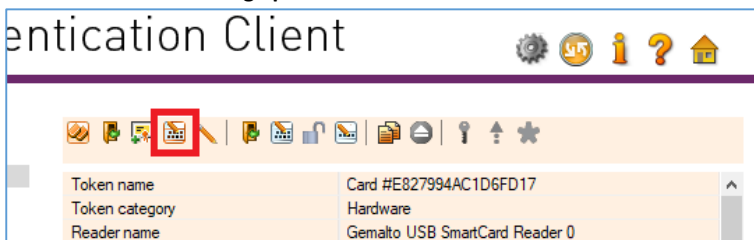
1. Zaženemo aplikacijo **SafeNet Authentication Client Tools**.

Windows	MacOS	Linux – Ubuntu 17.07

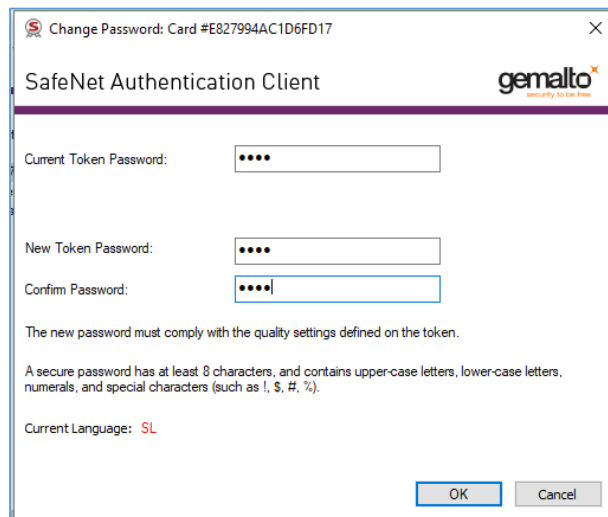
2. Izberemo ikono **Advanced View** (označeno na sliki)



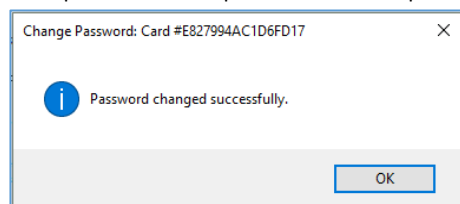
3. Kliknemo na ikono **Change password**.



4. V vnosno polje **Current Token Password** vnesemo trenutno PIN številko pametne kartice, v polji **New Token Password** in **Confirm Password** pa novo, željeno vrednost PIN številke. Spremembo potrdimo s klikom na **OK**.

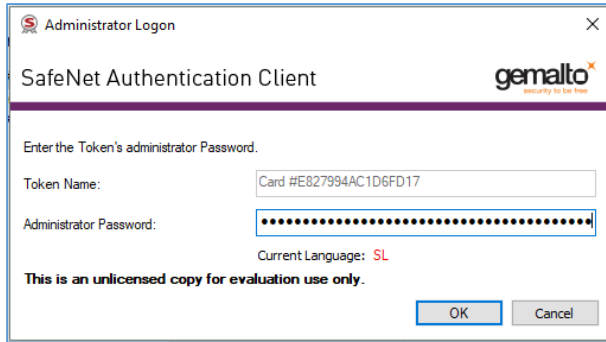


5. Ob uspešno izvedeni spremembi PINa se prikaže obvestilo na spodnji sliki.

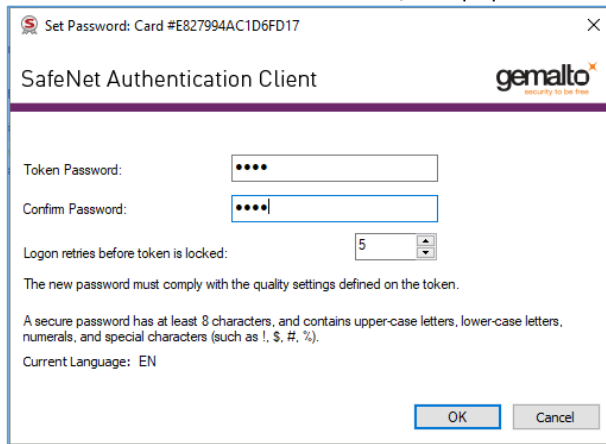




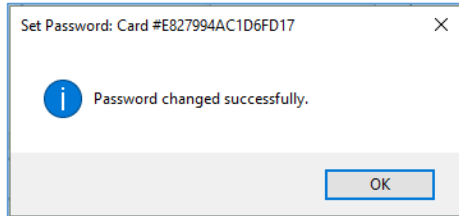




5. V vnosni okni **Token Password** in **Confirm Password** vnesemo (določimo) novo PIN kodo. Parameter **Logon retries before token is locked** nastavimo na vrednost **5**, nato pa potrdimo s klikom na **OK**.



6. Z določitvijo novega PINa smo izvedli tudi odklep pametne kartice.



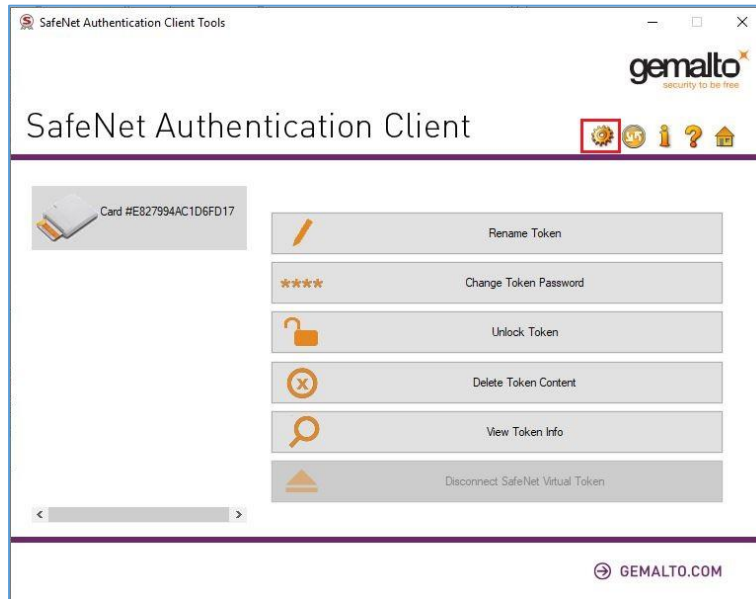
## 5 Upravljanje z digitalnimi potrdili

### 5.1 Uvoz digitalnega potrdila na pametno kartico/ključ

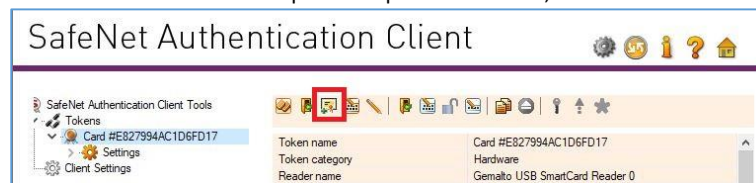
1. Zaženemo aplikacijo **SafeNet Authentication Client Tools**.

Windows	MacOS	Linux – Ubuntu 17.07

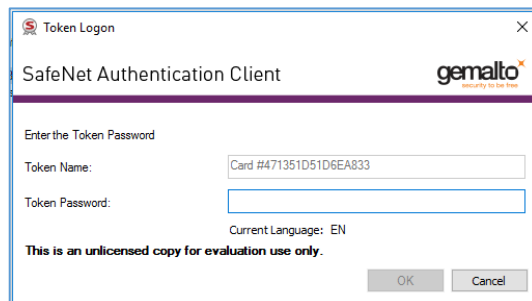
2. Izberemo ikono **Advanced View** (označeno na sliki)



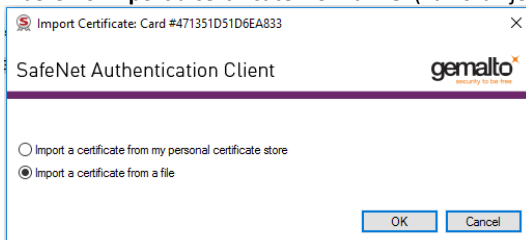
3. Na levem seznamu izberemo postavko pametne kartice, nato kliknemo na ikono **Import certificate**.



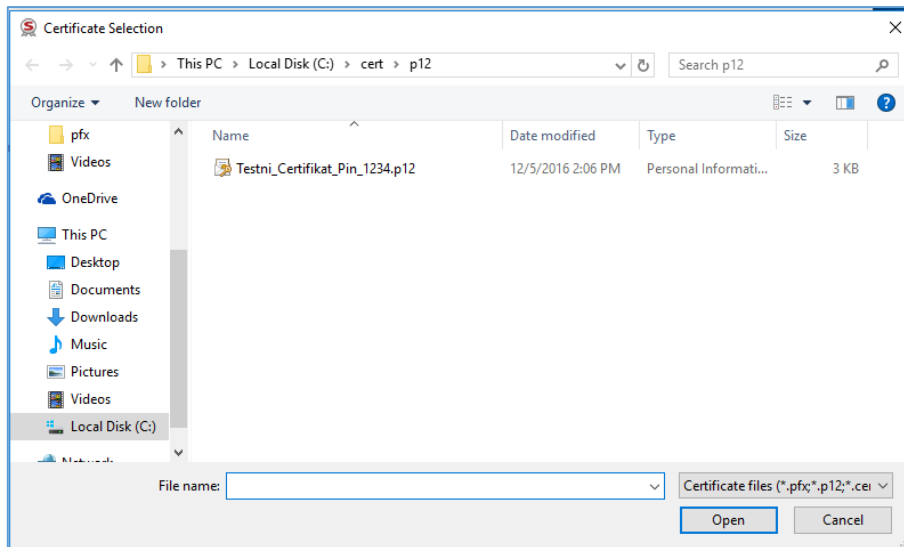
4. Vnesemo PIN kodo kartice (Token Password) in kliknemo na **OK**.



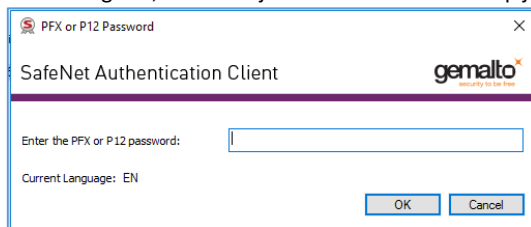
5. Izberemo **Import a certificate from a file**. (Ta korak je potreben sam na Windows napravah)



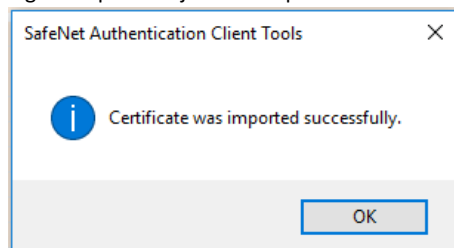
6. Poiščemo lokacijo varnostne kopije certifikata in kliknemo **Open**.



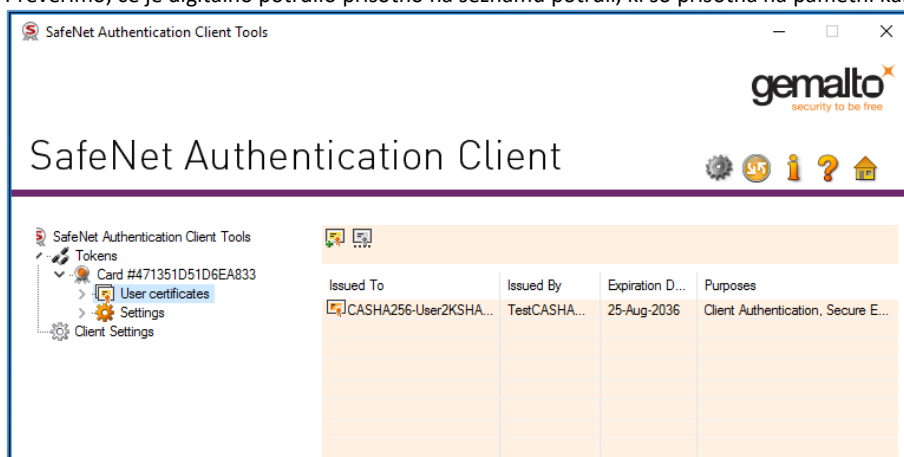
7. Vnesemo geslo, s katerim je zaščitena varnostna kopija digitalnega potrdila .pfx ali .p12. Potrdimo s klikom na **OK**.



8. Digitalno potrdilo je s tem uspešno nameščeno. Potrdimo s klikom na **OK**.

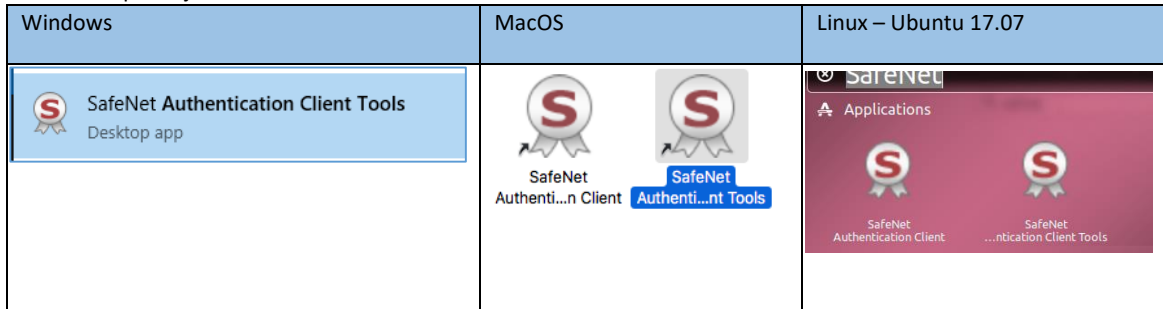


9. Preverimo, če je digitalno potrdilo prisotno na seznamu potrdil, ki so prisotna na pametni kartici/ključcu.

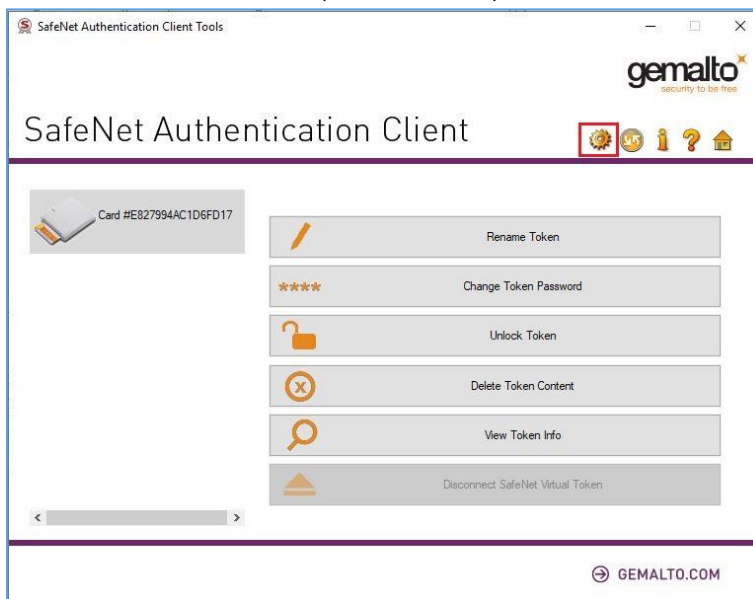


## 5.2 Izbris digitalnega potrdila iz pametne kartice/ključa

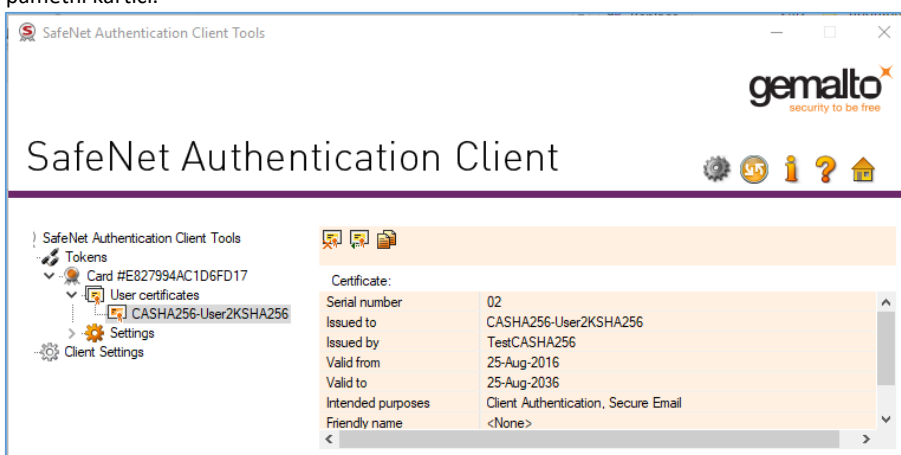
1. Zaženemo aplikacijo **SafeNet Authentication Client Tools**.



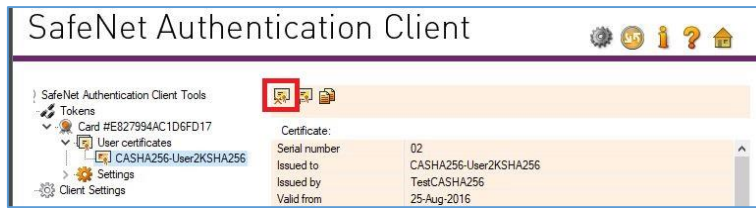
2. Izberemo ikono **Advanced View** (označeno na sliki)



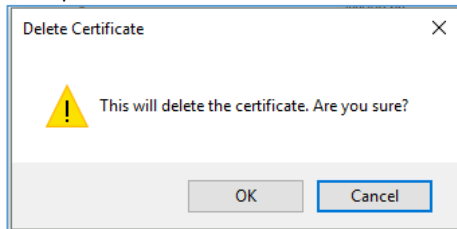
3. Na levem seznamu razširimo postavko **User certificates**, pod katero lahko vidimo vsa digitalna potrdila, ki so prisotna na pametni kartici.



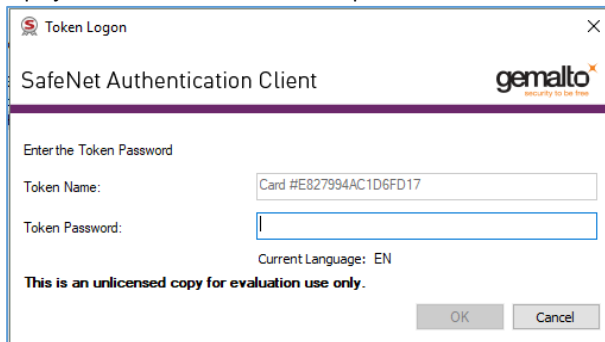
4. Označimo digitalno potrdilo, ki ga želimo odstraniti in izberemo ikono **Delete certificate**.



5. Izbris potrdimo s klikom na **OK**.



6. V polje **Token Password** vnesemo uporabniško PIN kodo in kliknemo na **OK**.



7. Digitalno potrdilo je s tem uspešno odstranjeno.

