

# **SETCCE**

## **Uporabniška navodila za namestitev in upravljanje komponente SETCCE proXSign® v2.2 za macOS**

**[Nova generacija komponent SETCCE proXSign® ]**

Identifikacijska oznaka dokumenta: n/a  
Različica dokumenta: 21  
Avtorji dokumenta: Helena Ostanek, Tina Zagmajster  
Status dokumenta: /  
Zadnja sprememba: dokumenta: 16.12.2024

## VSEBINA IN PRAVICE

Produkt **proXSign®** je razvila družba **SETCCE**. Posedovanje, uporaba ali distribucija produkta proXSign brez licence je nelegalna. Za pridobitev licence kontaktirajte ponudnika, ki v okviru svoje storitve uporablja podpisno komponento **proXSign®**. V primeru nakupa licence za integracijo v lastne rešitve pa kontaktirajte družbo SETCCE.

Dokument je v celoti v lasti SETCCE. Kopiranje dokumenta ali delov dokumenta brez soglasja SETCCE ni dovoljeno. Vse pravice pridržane. Ime SETCCE, grafični znak SETCCE in imena produktov SETCCE so registrirane znamke s strani SETCCE. Kopiranje in uporaba imen oziroma grafičnih znakov ni dovoljena.

### O SETCCE

SETCCE je vodilni ponudnik rešitev in storitev za zakonsko skladno elektronsko poslovanje ter varnost in zaupnost v informacijskih sistemih. Temeljna dejavnost družbe SETCCE je razvoj sodobnih produktov in rešitev elektronskega poslovanja za dematerializacijo poslovnih procesov ter s tem povezano svetovanje. Storitveno-produktni portfelj omogoča:

- uvedbo elektronskega podpisovanja v poslovnih procesih,
- elektronsko fakturiranje, distribucijo in arhiviranje e-računov,
- sklepanje pogodb v izključno elektronski obliki,
- zakonsko skladno elektronsko arhiviranje.

### Kontakti

SETCCE d.o.o.  
Tehnološki park 21  
1000 Ljubljana  
Slovenija  
Europe  
Web: [www.setcce.com](http://www.setcce.com)

## KAZALO

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| 1. Nova generacija komponent SETCCE proXSign® .....                           | 3  |
| 2. Podprta okolja .....                                                       | 4  |
| 2.1. Podprta okolja .....                                                     | 4  |
| 3. Pogoji za delovanje SETCCE proXSign® komponente .....                      | 5  |
| 3.1. Port za komunikacijo med brskalnikom in komponento .....                 | 5  |
| 3.2. Namestitev osebne digitalnega potrdila .....                             | 5  |
| 3.3. Zaupanje digitalnemu potrdilu »SETCCE proXSign« .....                    | 5  |
| 3.3.1. Postopek namestitve »SETCCE proXSign« digitalnega potrdila .....       | 5  |
| 3.3.2. Postopek samodejne obnove »SETCCE proXSign« digitalnega potrdila ..... | 7  |
| 3.3.3. Postopek preverbe »SETCCE proXSign« digitalnega potrdila .....         | 7  |
| 4. Namestitev SETCCE proXSign® komponente .....                               | 9  |
| 4.1. Postopek namestitve .....                                                | 9  |
| 5. Odnamestitev SETCCE proXSign® komponente .....                             | 11 |
| 6. Zagon SETCCE proXSign® komponente .....                                    | 12 |
| 6.1. Zagon .....                                                              | 12 |
| 6.2. Samodejni zagon .....                                                    | 12 |
| 7. Uporabniški vmesnik in nastavitve SETCCE proXSign® komponente .....        | 13 |
| 7.1. Osnovno pojavno okno Certificates/Certifikati .....                      | 13 |
| 7.2. Nastavitve/Settings .....                                                | 14 |
| 7.2.1. Samodejni zagon/Autostart .....                                        | 14 |
| 7.2.2. Prikaži pretečena digitalna potrdila/Show expired certificates .....   | 14 |
| 7.2.3. Dovolj podvojena digitalna potrdila/Allow duplicate certificates ..... | 15 |
| 7.2.4. Moduli/Modules .....                                                   | 15 |
| 8. Zaustavitev delovanja .....                                                | 16 |
| 9. Namestitev osebne digitalnega potrdila .....                               | 18 |
| 9.1. Ali imate nameščeno osebno digitalno potrdilo? .....                     | 18 |
| 9.1.1. Postopek namestitve .....                                              | 18 |
| 9.2. Ali imate nameščeno korensko in vmesno digitalno potrdilo? .....         | 19 |
| 9.2.1. Postopek namestitve .....                                              | 19 |
| 9.2.2. Zaupanja vredno korensko digitalno potrdilo .....                      | 20 |
| 9.3. Namestitev potrdila v Mozilla Firefox shrambo .....                      | 21 |
| 10. Uporaba pošta®CA digitalnega potrdila na zunanjem mediju .....            | 23 |

## 1. NOVA GENERACIJA KOMPONENT SETCCE PROXSIGN®

Komponente SETCCE proXSign® omogočajo digitalno podpisovanje dokumentov, šifriranje/dešifriranje in časovno žigosanje.

Nova generacija v2 je nastala kot odziv na omejitve večine spletnih brskalnikov pri podpori vtičnikom.

Nova generacija podpisne komponente SETCCE proXSign® je zasnovana na povsem novem konceptu in zaradi tehnološke neodvisnosti od sprememb brskalnikov omogoča delovanje v vseh priljubljenih brskalnikih.

Komponento se namesti kot namizno aplikacijo, ki teče v ozadju. Ponuja uporabniški vmesnik, kjer se lahko odločate glede samodejnega zagona in preverite delovanje komponente.

Prednosti nove generacije komponente SETCCE proXSign® za uporabnika:

- ena komponenta za vse funkcionalnosti (podpisovanje PDF in XML dokumentov, časovno žigosanje),

Če potrebujete pomoč pri namestitvi ali uporabi, se obrnite najprej na ponudnika storitve, kjer želite SETCCE proXSign® uporabiti (npr. spletna banka, storitve e-uprave itd.), nato na podporo SETCCE.

## 2. PODPRTA OKOLJA

### 2.1. Podprta okolja

| macOS                                                                                                                                 | Brskalnik                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Sonoma 14</li><li>• Sequoia 15</li></ul>                                                      | <ul style="list-style-type: none"><li>• Safari od v14.0.3</li><li>• Mozilla Firefox od v91</li><li>• Google Chrome; zadnja uradna različica</li></ul> |
| <b>Opomba:</b> Iz varnostnih razlogov priporočamo uporabo zadnjih razpoložljivih različic brskalnikov in operacijskega sistema macOS. |                                                                                                                                                       |

## 3. POGOJI ZA DELOVANJE SETCCE PROXSIGN® KOMPONENTE

### 3.1. Port za komunikacijo med brskalnikom in komponento

Komunikacija med brskalniki in SETCCE proXSign® komponento poteka preko enega izmed prostih portov:

- 14972
- 41472
- 57214
- 61427

Zato je potrebno za zagotovitev nemotenega delovanja komponente SETCCE proXSign®, v svojem okolju zagotoviti, da je vsaj en od zgoraj navedenih portov prost.

### 3.2. Namestitev osebne digitalnega potrdila

Vaše osebno digitalno potrdilo je lahko nameščeno v Login Keychain shrambi digitalnih potrdil, ali v Mozilla Firefox shrambi digitalnih potrdil. Obvezno namestite tudi korensko in vmesno digitalna potrdila izdajatelja vašega digitalnega potrdila. V primeru težav z nameščanjem digitalnih potrdil, se obrnite na izdajatelja vašega digitalnega potrdila. Glej poglavje 8.

### 3.3. Zaupanje digitalnemu potrdilu »SETCCE proXSign«

SETCCE proXSign® komponenta svojim **uporabnikom zagotavlja višjo stopnjo varnosti** tako, da šifrira podatke, ki si jih izmenjujeta brskalnik in komponenta.

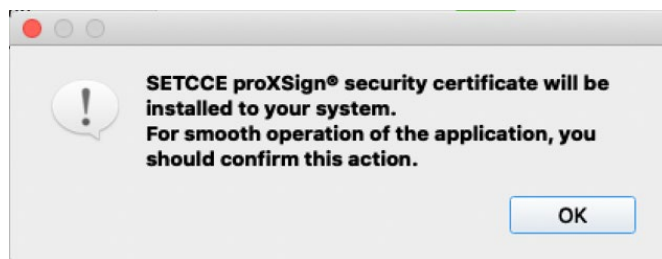
V ta namen se uporablja digitalno potrdilo »SETCCE proXSign«, ki se zgradi dinamično, ob prvem zagonu komponente. Namesti se v Keychain in v Mozilla Firefox shrambo digitalnih potrdil trenutnega uporabnika (»Current User«).

To digitalno potrdilo ima časovno veljavnost dve leti.

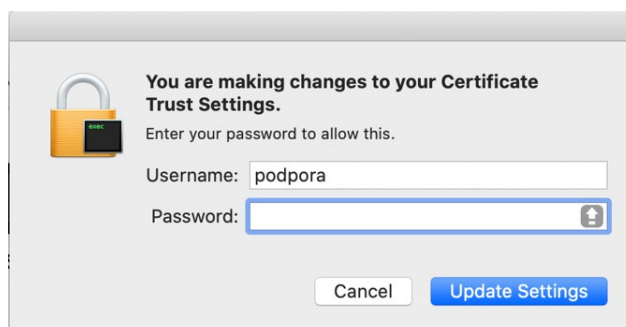
#### 3.3.1. Postopek namestitve »SETCCE proXSign« digitalnega potrdila

Po uspešni namestitvi SETCCE proXSign® komponente, se ob prvem zagonu le-te pojavi obvestilo (slika 1), ki ga je potrebno potrditi, dovoliti vpis digitalnega potrdila v Keychain in potrditi Zaupanje (slika 2). S tem zagotovite, da se digitalno potrdilo uspešno namesti in posledično zagotovite tudi delovanje komponente.

Potrditev je ob prvem zagonu komponente potrebna v vseh uporabniških profilih na sistemu.

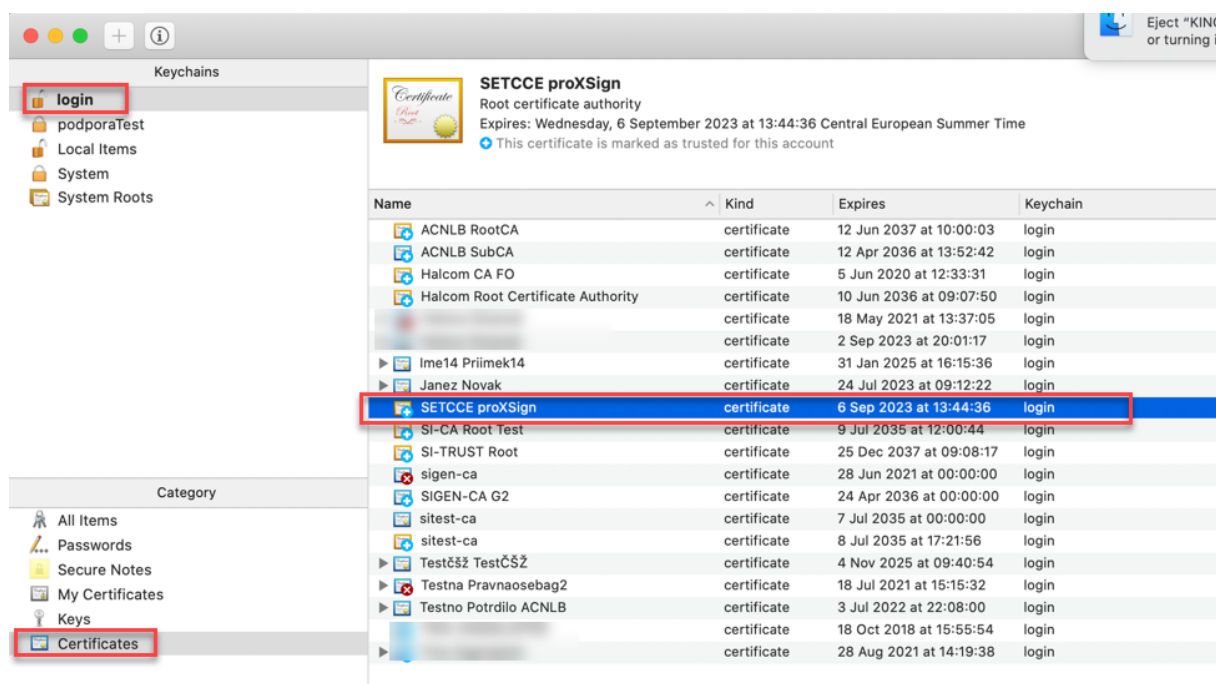


Slika 1: »SETCCE proXSign« opozorilo ob namestitvi SETCCE proXSign® digitalnega potrdila



Slika 2: Mac OS dialoško okno za nastavitve zaupanja

»SETCCE proXSign« digitalno potrdilo se namesti v shrambo digitalnih potrdil, pod **Keychains/Login** in **Category/Certificates**, kot je prikazano na sliki 3.

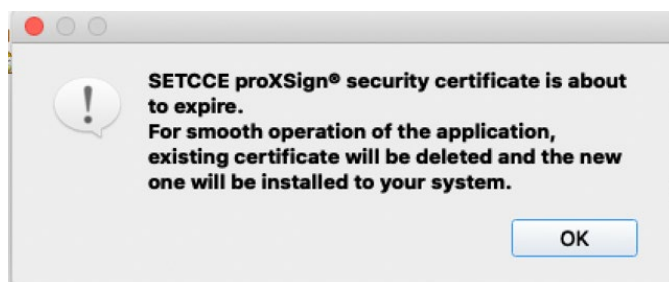


Slika 3: Prikaz namestitve »SETCCE proXSign« digitalnega potrdila v shrambi (Login Keychain)

### 3.3.2. Postopek samodejne obnove »SETCCE proXSign« digitalnega potrdila

Komponenta ob zagonu preverja ali je »SETCCE proXSign« digitalno potrdilo še časovno veljavno. V kolikor je že pretečeno, ali pa bo preteklo v naslednjih desetih dneh, komponenta samodejno zgradi novega in vam ga ponudi v namestitev.

Odnamestitev starega in namestitev novega digitalnega potrdila morate potrditi in dovoliti njegov vpis v Keychain. V Mozilla Firefox shrambo se digitalno potrdilo nadomesti brez vašega potrjevanja.

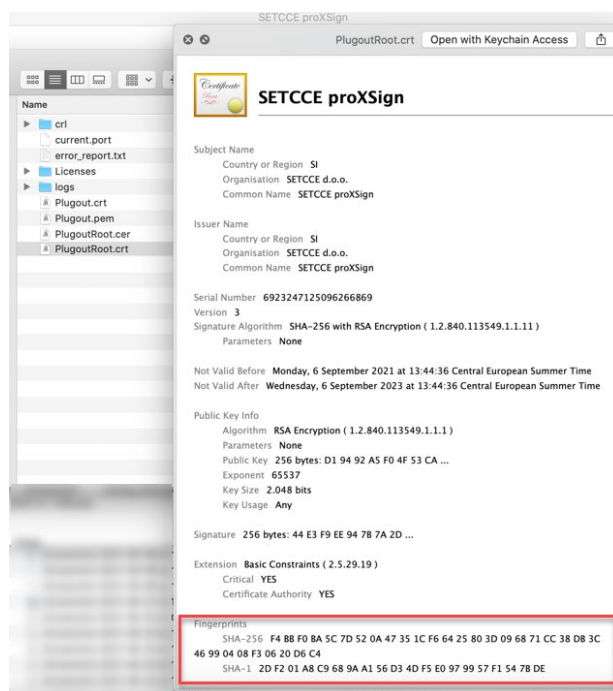


Slika 4: Opozorilo pri obnovi vašega SETCCE proXSign digitalnega potrdila

### 3.3.3. Postopek preverbe »SETCCE proXSign« digitalnega potrdila

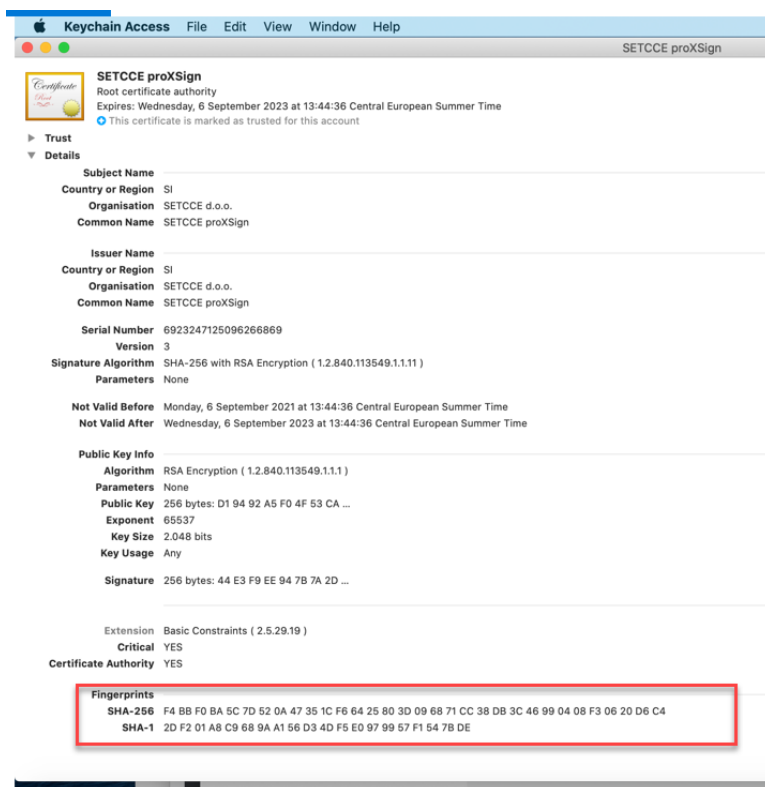
Če ste v dvomih, ali gre resnično za SETCCE proXSign digitalno potrdilo, lahko primerjate prstni odtis (Thumbprint) digitalnega potrdila, ki je nameščeno v Keychain ali Firefox Shrambo digitalnih potrdil s prstnim odtisom digitalnega potrdila, ki se nahaja na  
[User]\Library\Application Support\SETCCE\proXSign\PluginRoot.crt.

Na datotečnem sistemu označite PlugoutRoot.crt in pritisnite preslednico; odpre se vam okno z informacijami o digitalnem potrdilu.



Slika 5: Prikaz SETCCE proXSign digitalnega potrdila na datotečnem sistemu

In ga primerjajte s prstnim odtisom digitalnega potrdila »**SETCCE proXSign**« ki se namesti v digitalno shrambo potrdil na sliki ; morata se ujemati.



Slika 6: Prstni odtis digitalnega potrdila »SETCCE proXSign«

## 4. NAMESTITEV SETCCE PROXSIGN® KOMPONENTE

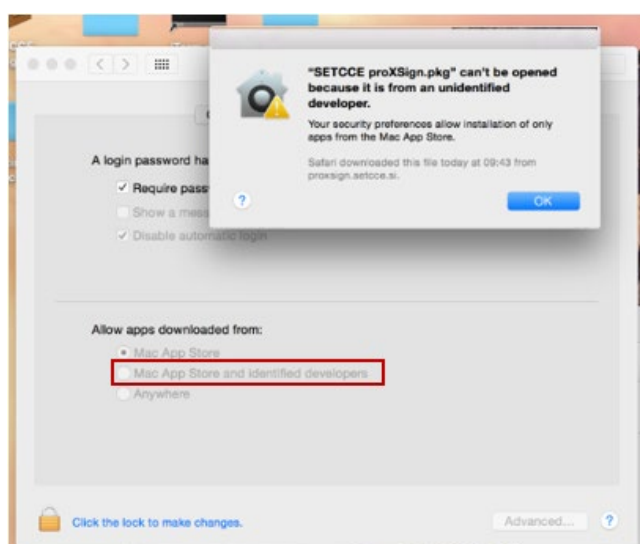
SETCCE proXSign® komponenta se namesti kot namizna aplikacija, ki teče v ozadju. Ponuja grafični uporabniški vmesnik, kjer se lahko odločate glede samodejnega zagona in preverite delovanje komponente.

Namestitveni paket se imenuje »**SETCCE\_proXSign\_<version>.pkg**«. Paket ni podpisan in ni prenešen iz »Mac App store«, zato je potrebno prenos in namestitev paketa dodatno omogočiti.

Namestitev SETCCE proXSign® komponente lahko izvedete le kot uporabnik z **administratorskimi pravicami**.

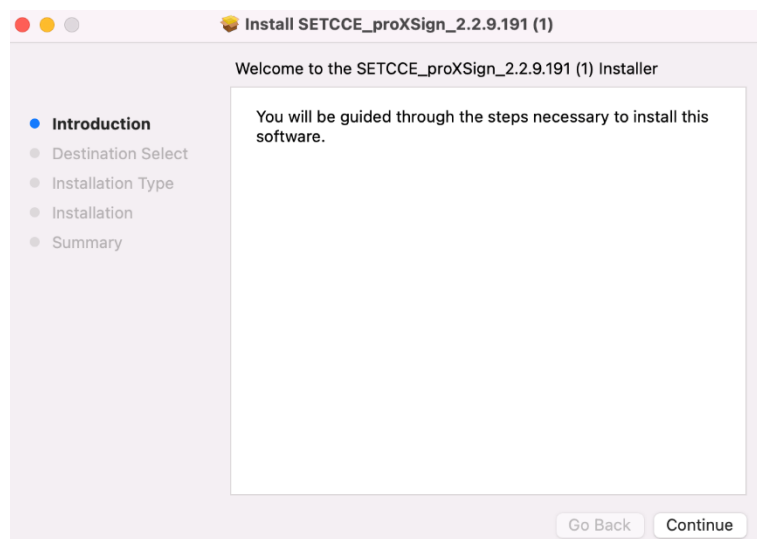
### 4.1. Postopek namestitve

1. Prijavite se kot uporabnik z administratorskimi pravicami.
2. Pod »**System Preferences**«/»**Security & Privacy**« izberite možnost »**Mac App Store and identified developers**«, kot je prikazano na sliki 7.



Slika 7: Prikaz nastavitev v »System Preferences« / »Security & Privacy«

3. Prenesete namestitveni paket »**SETCCE\_proXSign\_<version>.pkg**«.
4. Kliknete na namestitveni paket »**SETCCE\_proXSign\_<version>.pkg**« in sledite korakom namestitve. Komponenta proXSign.app se privzeto namesti v mapo »Applications«. Med postopkom namestitve lahko izberete poljubno mapo.



Slika 8: Prikaz namestitve

### Opozorilo:

po končani namestitvi in ob zagonu komponente, se namesti še SETCCE proXSign digitalno potrdilo, ki je ključno za delovanje komponente. Pri namestitvi potrdite vse korake. Glej poglavje 3.3.

Po končani namestitvi, se v Status meniju pojavi ikona **SETCCE proXSign®**. Z dvoklikom na le-to se odpre osnovno okno komponente »Certifikati/Certificates«, kjer so razvidna vsa digitalna potrdila, ki so nameščena v Keychain in/ali Mozilla Firefox osebni shrambi digitalnih potrdil.



Slika 9: Prikaz ikone SETCCE proXSign v status meniju

## 5. ODNAMESTITEV SETCCE PROXSIGN® KOMPONENTE

1. V sistem se prijavite kot uporabnik z administratorskimi pravicami in iz mape/lokacije, kamor ste predhodno namestili aplikacijo proXSign.app, le to brišite.

Privzeta lokacija proXSign.app je mapa Applications.

2. Iz shrambe digitalnih potrdil Keychain/Login in Mozilla Firefox shrambe, izbrišite »SETCCE proXSign« digitalno potrdilo.

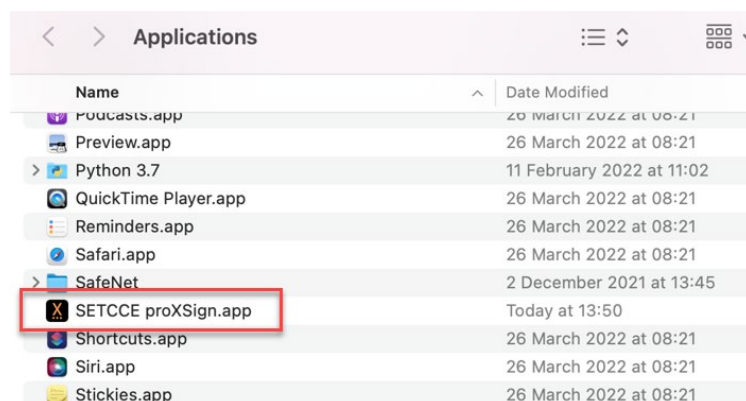
## 6. ZAGON SETCCE PROXSIGN® KOMPONENTE

### 6.1. Zagon

Komponento lahko zaženete na več načinov:

#### Zaženete SETCCE proXSign.app:

1. Komponento **SETCCE proXSign.app** poiščete v mapi »**Applications**« oz. na lokaciji, kamor ste jo predhodno namestili.

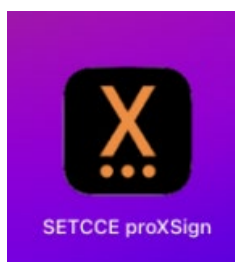


Slika 10: Prikaz zagona komponente SETCCE proXSign.app

2. Z dvojnim klikom na ikono **SETCCE proXSign.app**, SETCCE proXSign® komponento zaženete. Odpre se osnovno okno »**Certificates**« z vašimi osebnimi digitalnimi potrdili. Glej sliko 13.

#### Prek »Launchpad«:

1. Zaženete »**Launchpad**« in z dvojnim klikom na **SETCCE proXSign ikono** komponento zaženete.



Slika 11: Ikona SETCCE proXSign v »Launchpad«

Če je komponenta SETCCE proXSign® zagnana, se v **Status** meniju pokaže ikona proXSign®.



Slika 12: Prikaz ikone SETCCE proXSign v status meniju

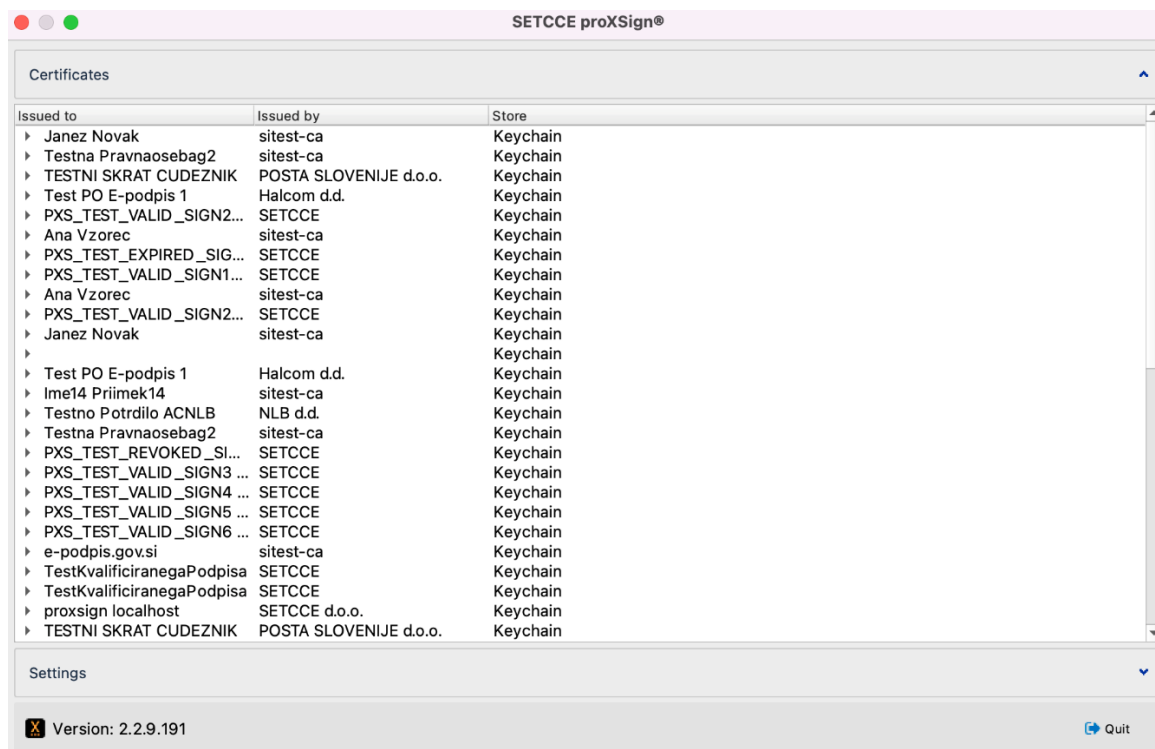
### 6.2. Samodejni zagon

Glej poglavje 7.2.1.

## 7. UPORABNIŠKI VMESNIK IN NASTAVITVE SETCCE PROXSIGN® KOMPONENTE

Z dvoklikom na SETCCE proXSign® ikono v **Status** meniju (slika 12), se vam odpre osnovno pojavno okno s seznamom vseh vaših osebnih digitalnih potrdil (slika 13).

### 7.1. Osnovno pojavno okno Certificates/Certifikati



Slika 13: Prikaz osnovnega pojavnega okna SETCCE proXSign® komponente

Pomen stolpcev na osnovnem pojavnem oknu:

- **Issued to/Izdano za:** ime digitalnega potrdila (CN)
- **Issued by/Izdajatelj:** izdajatelj digitalnega potrdila
- **Store/Shramba:** shramba digitalnih potrdil v kateri se nahaja (Keychain ali Firefox)

**Opcijsko:**

- **Chain Validity/Veljavnost verige:** Veljavnost verige digitalnega potrdila (ne preverja se preklicanost - CRL). Če je vrednost »Not OK«, podpis s takim digitalnim potrdilom ni mogoč. Razlog je lahko v pretečenem digitalnem potrdilu, če nimate nameščenih (ali pravilno nameščenih) korenskih ali vmesnih digitalnih potrdil, če korensko ali vmesno digitalno potrdilo ni zaupanja vredno (Trust v primeru Mozilla Firefox shrambe digitalnih potrdil) ... .

**Stolpec je viden, če je v proxsign.ini nastavljen ustrezen parameter.**

**Koraki:**

1. Ugasnite proXSign®

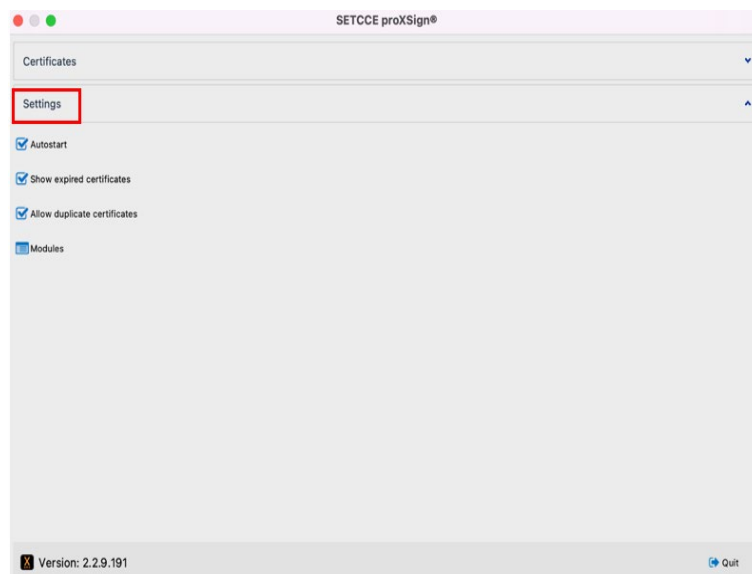
2. Odprite datoteko [C:\Program Files (x86)]\SETCCE\proXSign\etc\proxsign.ini
3. In spremenite vrednost  
    check\_all\_chains=false  
    na  
    check\_all\_chains=true
4. Shranite spremembe
5. Iz namizja ponovno zaženite proXSign®

Primer vklopa preverjanja veljavnosti verige v proxsign.ini datoteki:

```
[common]
update_url=http://public.setcce.si/proxsign/update/SETCCE_proXSign_update.exe
version_url=http://public.setcce.si/proxsign/update/version
check_all_chains=true
; use_CNG : no, yes, prefer, only
use_CNG = no
```

V kolikor se na vašem računalniku proXSign® zelo počasi zažene, preverjanje veljavnosti verige izklopite. Za vklop in izklop potrebujete Administratorske pravice.

## 7.2. Nastavitve/Settings



Slika 14: Prikaz okna Nastavitve/Settings v proXSign® komponenti

### 7.2.1. Samodejni zagon/Autostart

Komponenta SETCCE proXSign® podpira samodejni zagon ob prijavi v vaš uporabniški račun.

Privzeto je možnost »Samodejni zagon/Autostart« omogočena.

### 7.2.2. Prikaži pretečena digitalna potrdila/Show expired certificates

Privzeto je ta nastavek onemogočen.

V kolikor jo omogočite, so digitalna potrdila prikazana le v osnovnem proXSign vmesniku, privzeto pa digitalni podpis s pretečenimi digitalnimi potrdili ni omogočen.

### **7.2.3. Dovoli podvojena digitalna potrdila/Allow duplicate certificates**

V kolikor je vaše (isto) digitalno potrdilo nameščeno tako v Keychain shrambo digitalnih potrdil, kot v Mozilla Firefox brskalnik (NSS shramba), vam proXSign prikaže in omogoča podpis z obema.

Privzeto je ta nastavitev onemogočena.

### **7.2.4. Moduli/Modules**

Nastavitev služi podpisovanju z digitalnimi potrdili izdanimi na zunanjih kriptografskih napravah prek modula/knjižnice pkcs#11. Trenutno je podprto in testirano le digitalno potrdilo certifikatske agencije posta®CA. Glej poglavje 10.

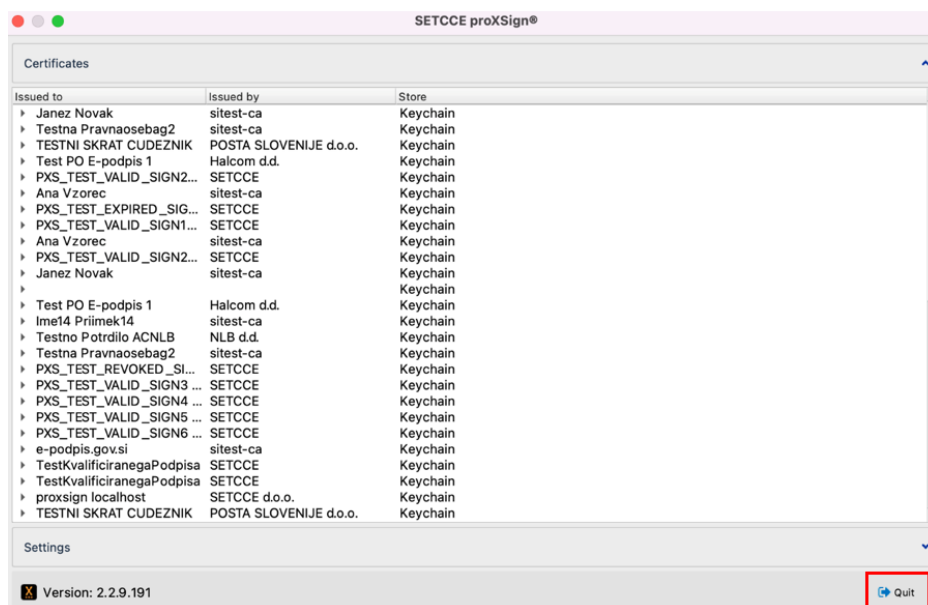
## 8. ZAUSTAVITEV DELOVANJA

Predlagamo, da SETCCE proXSign® komponento pustite, da teče v ozadju. SETCCE proXSign® komponenta v tem času ne izvaja aktivnosti.

V kolikor želite, da se delovanje SETCCE proXSign® komponente povsem zaustavi (ugasne), lahko to storite na dva načina:

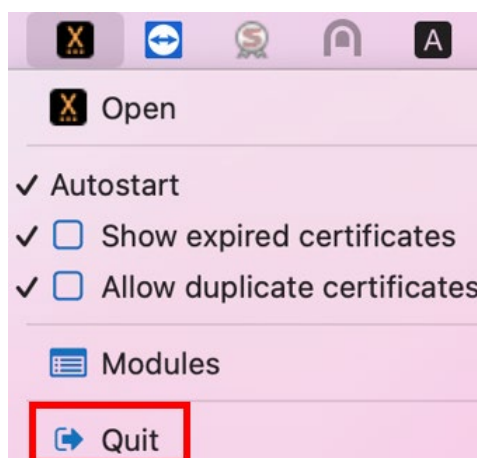
1. V grafičnem uporabniškem vmesniku izberite možnost »**Quit/Izklopi**«.

S klikom na gumb »**Quit/Izklopi**«  SETCCE proXSign® komponenta preneha delovati (proces se ubije).



Slika 15: Prikaz gumba Quit/Izklopi na osnovnem vmesniku proXSign® komponente

2. V **Status meniju** kliknete na ikono SETCCE proXSign in izberete opcijo »**Quit/Izklopi**«.



Slika 16: Prikaz izbire možnosti »Quit«/» Izklopi«

V kolikor želite, da se okno skrije oziroma zgolj pomanjša, potem v grafičnem uporabniškem vmesniku kliknete standardni rdeč krogec v levem zgornjem vogalu.

S klikom na gumb »**Close/Zapri**«  skrijete SETCCE proXSign pojavno okno, ki se skrije v območje status menija. SETCCE proXSign® komponenta nemoteno teče.

## 9. NAMESTITEV OSEBNEGA DIGITALNEGA POTRDILA

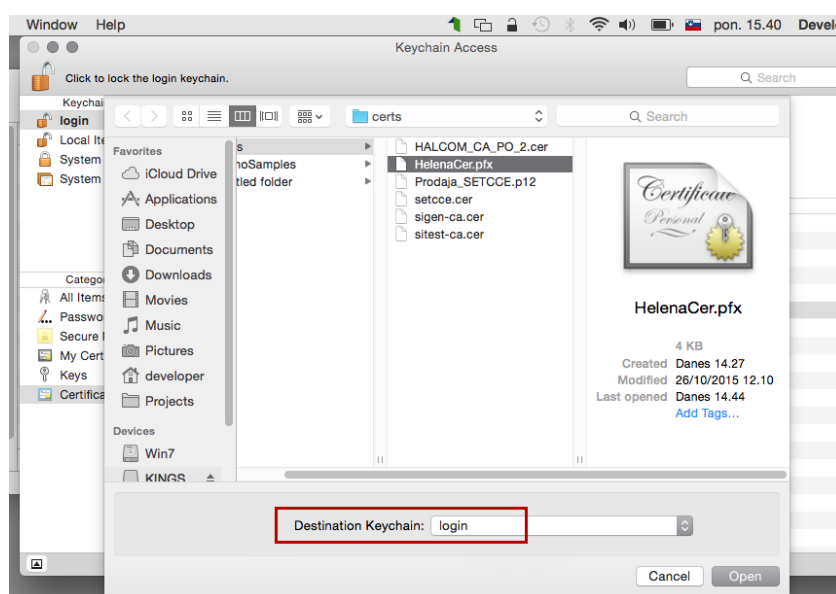
### 9.1. Ali imate nameščeno osebno digitalno potrdilo?

Pred podpisovanjem dokumentov s komponento SETCCE proXSign® je potrebno imeti nameščeno osebno digitalno potrdilo v shrambi osebnih digitalnih potrdil (Keychain Login oz. Mozilla Firefox shrambi) ali na pametni kartici/ključu.

#### 9.1.1. Postopek namestitve

Za namestitev osebnega digitalnega potrdila sledite naslednjim korakom:

1. Svoje osebno digitalno potrdilo shranite na trdi disk.
2. Zaženete **Keychain Access** aplikacijo (Spotlight->Keychain Access)
3. Izberete **File->Import Items** in izberete osebno digitalno potrdilo iz lokacije, kamor ste ga predhodno shranili ter pod »**Destination Keychain**« izberete možnost »**Login**« kot je prikazano na sliki 17. Osebno digitalno potrdilo se na ta način namesti **v vašo (User) shrambo digitalnih potrdil**. Hkrati z osebnim digitalnim potrdilom **se samodejno namesti tudi korensko digitalno potrdilo**, prav tako v vašo (User) shrambo digitalnih potrdil in je na voljo za uporabo le pod vašim uporabniškim računom. Več o korenskih digitalnih potrdilih je opisano v poglavju 9.2.



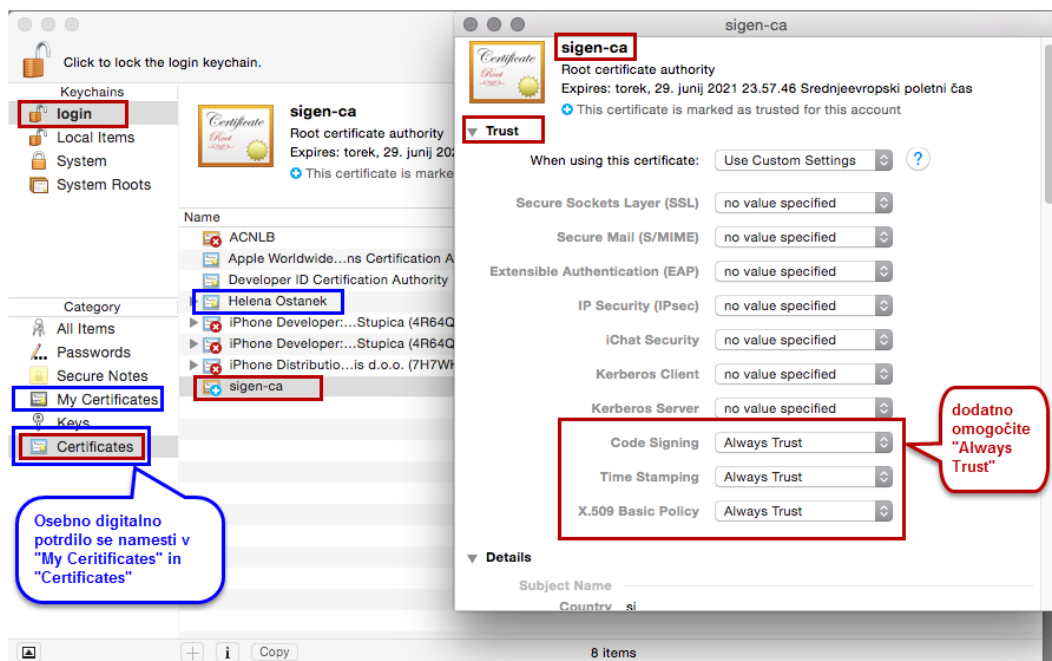
Slika 17: Prikaz namestitve osebnega digitalnega potrdila v Keychain Access

S tem postopkom namestitve se **obe digitalni potrdili** namestita v **Keychains/Login in Category/Certificates**, osebno pa je nameščeno tudi pod **Category/My Certificates**.

#### Pomembno:

1. Privzeto se korensko digitalno potrdilo ne namesti kot zaupanja vredno, zato morate te lastnosti dodatno omogočiti (Glej 9.2.2).
2. Navedeni postopek namestitve velja za Yosemite in digitalna potrdila, ki se lahko shranijo na trdi disk.
3. Od različice macOS Catalina lahko digitalno potrdilo posta®CA na Gemalto pametnem USB ključu/kartici uporabljate prek modula/knjižnice pkcs#11; Glej poglavje 9. Z

različico SETCCE proXSign® 2.2. pa lahko to direktno potrdilo na macOS Catalina in Big Sur ponovno uporabljate brez uporabe modula pkcs#11, a se digitalno potrdilo ne vidi v Keychain, kot je bilo to v preteklih različicah macOS-a.



Slika 18: Namestitev osebnega digitalnega potrdila v uporabniški (login) Keychain (skupaj s korenskim)

## 9.2. Ali imate nameščeno korensko in vmesno digitalno potrdilo?

Pred uporabo je potrebno namestiti korensko in vmesno digitalno potrdilo izdajatelja, ki vam je izdal osebno digitalno potrdilo.

Na spodnjih povezavah so na voljo korenska potrdila večine registriranih izdajateljev v Republiki Sloveniji:

- POŠTARCA: <https://postarca.posta.si/korensko-potrdilo/>
- AC NLB: <http://www.nlb.si/ac-nlb-identiteta-ac-nlb>
- HALCOM-CA: <http://www.halcom.si/si/pomoc/?action=showEntry&data=194&searchText=korensko>
- SIGEN-CA in SIGOV-CA: [http://www.si-ca.si/podpisna\\_komponenta/korenski\\_potrdili.php](http://www.si-ca.si/podpisna_komponenta/korenski_potrdili.php)

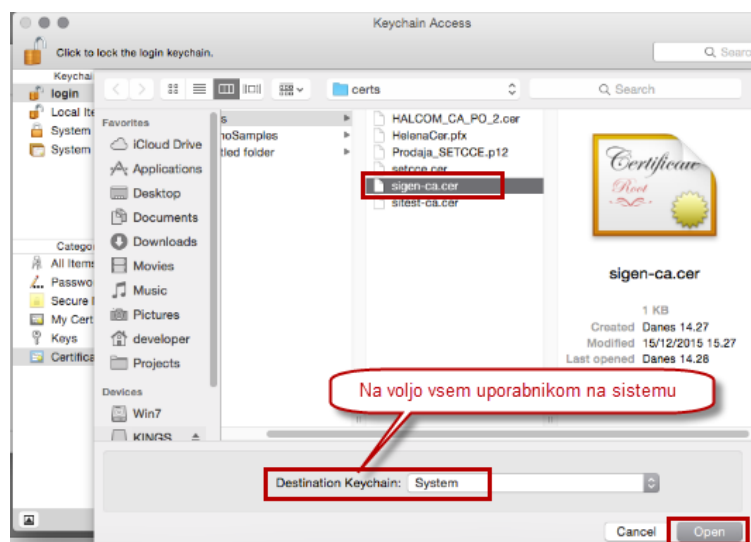
### 9.2.1. Postopek namestitve

Korensko digitalno potrdilo se lahko namesti (vsaj) na dva načina:

1. **Samodejno, ob prvi namestitvi vašega osebnega digitalnega potrdila** (Glej poglavje 9.1). V tem primeru se le-to namesti v **Keychains/Login** in **Category/Certificates** in velja **le za vaš uporabniški profil (User)**.
2. **Standardna namestitev z uporabo aplikacije Keychain Access**. V tem primeru priporočamo namestitev v sistemsko shrambo digitalnih potrdil, saj tako velja za vse uporabnike na vašem računalniku.

## Postopek standardne namestitve v sistemsko shrambo digitalnih potrdil (System Keychain):

1. Na računalnik se prijavite z uporabnikom, ki ima administratorske pravice.
2. Korensko digitalno potrdilo prenesete iz ene od zgornjih povezav in shranite na disk.
3. Zaženete **Keychain access** aplikacijo (Spotlight->Keychain Access).
4. Izberete **File->Import Items** in izberete korensko digitalno potrdilo iz lokacije, kamor ste ga predhodno shranili ter pod »**Destination Keychain**« izberete možnost »**System**«. Korensko digitalno potrdilo se na ta način namesti v sistemsko shrambo digitalnih potrdil in velja za **vse uporabnike** (User) na vašem računalniku.

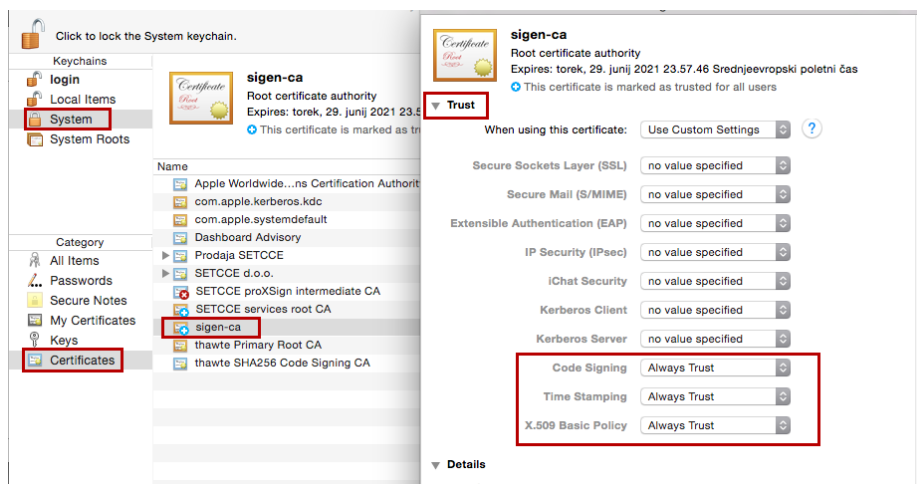


Slika 19: Namestitev korenskega digitalnega potrdila v sistemsko shrambo (System Keychain)

### 9.2.2. Zaupanja vredno korensko digitalno potrdilo

Korensko digitalno potrdilo privzeto **ni nameščeno kot zaupanja vredno**, zato morate te lastnosti dodatno nastaviti na naslednji način:

1. Z dvojnim klikom na digitalno potrdilo se odpre okno za urejanje zaupanja in pregled lastnosti digitalnega potrdila.
2. Izberete „**Trust**“ in vsaj za zadnje tri opcije izberete „**Always Trust**“.
3. S klikom na standardni x zaprete okno.
4. In z administratorskim geslom uveljavite spremembo.

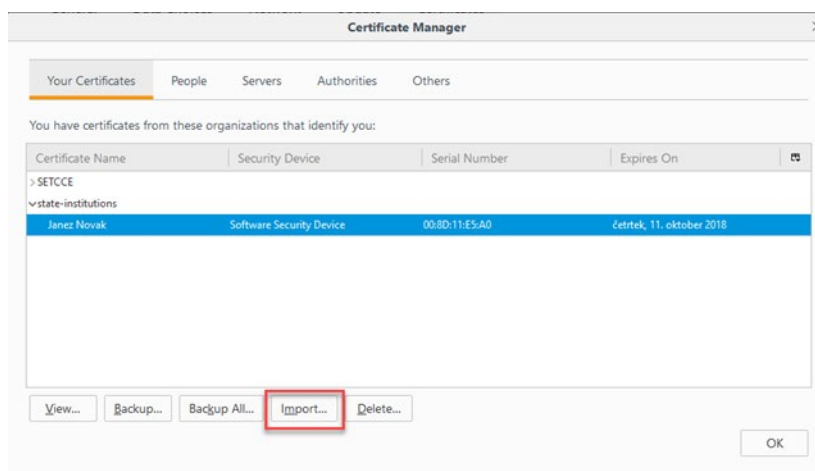


Slika 20: Prikaz namestitve korenskega digitalnega potrdila v »Keychain Access« in sprememba zaupanja

## 9.3. Namestitev potrdila v Mozilla Firefox shrambo

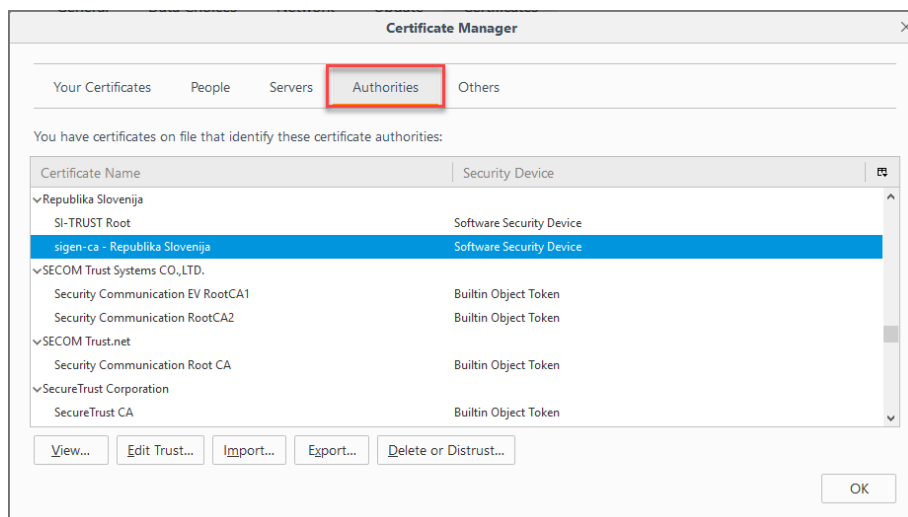
**Namestitev potrdila v Mozilla Firefox** shrambo preko brskalnika **Mozilla Firefox**:

1. Prenesite vaše digitalno potrdilo na osebni računalnik.
2. Odprite brskalnik Mozilla Firefox in se postavite na Možnosti/Napredno/Preglej digitalna potrdila/Vaša digitalna potrdila.
3. Nato kliknite na »**Uvozi/Import**« in izberite potrdilo. V pogovornem oknu vpišite geslo za namestitev potrdila in kliknite »**Naprej/Next**«, v naslednjem koraku pustite izbrano privzete možnosti nato sledite navodilom.
4. Vaše osebno digitalno potrdilo se namesti med **osebna digitalna potrdila v Mozilla Firefox shrambo digitalnih potrdil**, kot je prikazano na sliki 21.



Slika 21: Digitalno potrdilo »Janez Novak« med osebni digitalnimi potrdili (mapa Osebna/Personal) v Mozilla Firefox shrambi.

Korensko digitalno potrdilo namestite v Mozilla Firefox shrambo digitalnih potrdil med »Zaupanja vredni overitelji korenskih potrdil/Authorities«, kot je prikazano na sliki 22.



Slika 22: Korensko digitalno potrdilo »Sigen-ca« med »Zaupanja vredni overitelji korenskih potrdil« v Mozilla Firefox shrambi.

**Pomembno:**

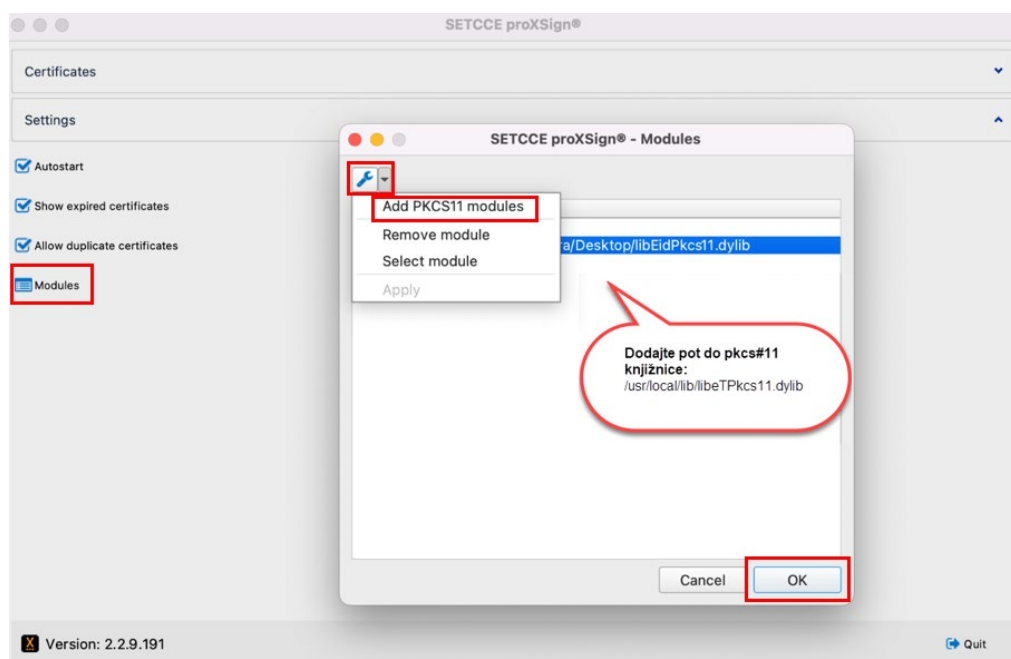
1. Če brskalnik **Mozilla Firefox** na vaš računalnik **namestite naknadno** (komponenta SETCCE proXSign® je že nameščena in zagnana), je potrebno **le-to ponovno zagnati**. Tako se »SETCCE proXSign« digitalno potrdilo namesti še v Mozilla Firefox shrambo digitalnih potrdil. Nato brskalnik zaprite ter ponovno zaženite, saj tako Mozilla Firefox brskalnik osveži svoje podatke in »SETCCE proXSign« digitalno potrdilo obvelja.
2. Če si SETCCE proXSign® komponento **namestite in zaženete** preko brskalnika **Mozilla Firefox**, morate po končani namestitvi brskalnik zapreti in ponovno zagnati. Tako Mozilla Firefox brskalnik osveži svoje podatke in »SETCCE proXSign« digitalno potrdilo obvelja.

## 10. UPORABA POŠTA®CA DIGITALNEGA POTRDILA NA ZUNANJEM MEDIJU

Digitalna potrdila slovenskega kvalificiranega izdajatelja pošta®CA na zunanjih medijih so z različico komponente **SETCCE proXSign® 2.2** na macOS Catalina in novejših podprta prek keychaina (se ne vidijo več v Keychainu, kot je bilo to običajno v starejših različicah macOS-a), kot z uporabo knjižnice pkcs#11.

### Nastavitev pkcs#11 knjižnice v komponenti SETCCE proXSign®:

1. Namestite gonilnike za vaše digitalno potrdilo, Gemalto Safenet Authentication Client (SAC). Navodila za namestitev SAC niso predmet teh navodil.
2. Zaženite SETCCE proXSign®.
3. Izberite »Nastavitve/Settings«
4. Izberite »Moduli/Modules«.
5. Izberite ikono »Orodja/Tools« in iz padajočega menija izberite »Add PKCS11 modules«.



Slika 23: Primer nastavitve knjižnice pkcs#11 za delo z pošta®CA digitalnim potrdilom na zunanjem mediju.

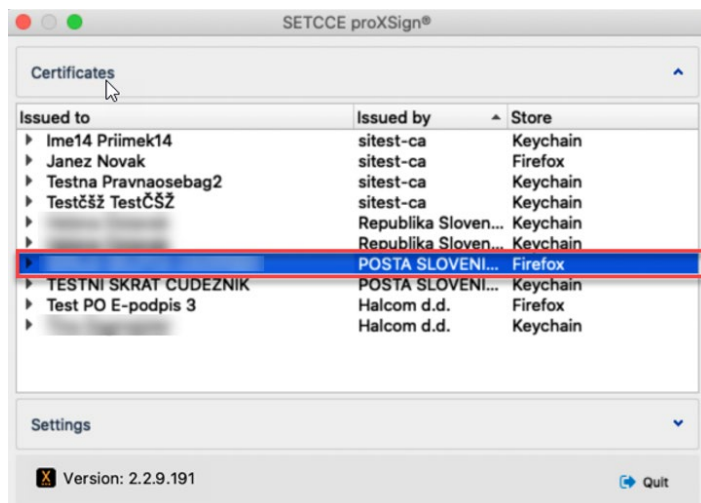
6. Odpre se vam dialoško okno. Na datotečnem sistemu poiščite in izberite knjižnico za pkcs#11, ki se na vaš računalnik namesti skupaj s SAC.
7. Za lokacijo knjižnice preverite navodila izdajatelja vašega osebnega digitalnega potrdila.

### Primer lokacije knjižnice pkcs#11 v SAC 10.2 (10.2.97.0):

`/usr/local/lib/libTPkcs11.dylib`

8. Izbiro potrdite z »OK«.
9. Ugasnite ter ponovno zaženite SETCCE proXSign®.
10. Vaše digitalno potrdilo je v osnovnem oknu proXSign® vidno v Firefox shrambi digitalnih potrdil. Glej sliko 24.

**Pomembno:** Korensko in vmesno digitalno potrdilo pošta®CA morate v tem primeru namestiti v Mozilla Firefox shrambo digitalnih potrdil (<https://postarca.posta.si/korensko-potrdilo/>).



Slika 24: Prikaz digitalnega potrdila pošta®CA na zunanjem mediju prek pkcs#11 modula