SETCCE

Uporabniška navodila za namestitev in upravljanje komponente SETCCE proXSign® v2.1 za macOS

[Nova generacija komponent SETCCE proXSign®]

Identifikacijska oznaka dokumenta:	**n/a**
Različica dokumenta:	16
Avtorji dokumenta:	Helena Ostanek, Tina Zagmajster
Status dokumenta:	/
Zadnja sprememba: dokumenta:	20.10.2020

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.

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

KAZALO

1. NOVA GENERACIJA KOMPONENT SETCCE PROXSIGN®

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

Nova generacija v2.1 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

Operacijski sistem	Brskalnik
macOS • Mojave 10.14 • Catalina 10.15	Safari od v10.0.1 Mozilla Firefox od v60 Google Chrome; zadnja uradna različica
Opomba: 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.

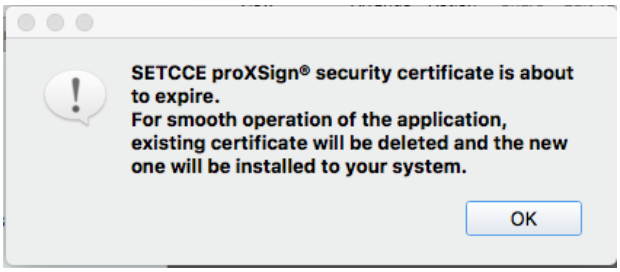
3.2. Namestitev osebnega digitalnega potrdila

Vaše osebno digitalno potrdilo mora biti nameščeno med osebna digitalna potrdila v shrambo digitalnih potrdil (login keychain). Glej poglavje 7.

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.

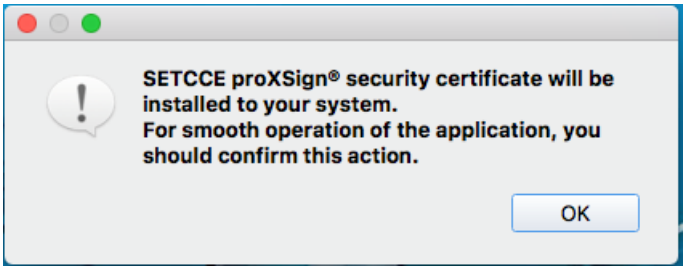
V ta namen se uporablja digitalno potrdilo **»SETCCE proXSign«**, ki se zgradi dinamično, ob prvem zagonu komponente. Namesti se v Keychain in v Mozilla Firefox shrambo digitalnih potrdil trenutnega uporabnika (»Current User«). To digitalno potrdilo ima veljavnost dve leti. Komponenta samodejno pravočasno zazna, da bo le-to preteklo, zato ga ob ponovnem zagonu komponente ponovno zgradi in ga uporabniku ponudi v namestitev. V tem primeru uporabnik potrdi namestitev novega digitalnega potrdila. Slednje velja za Keychain shrambo digitalnih potrdil. V Mozilla Firefox shrambi se-le to nadomesti brez potrjevanja uporabnika.



Slika 1: Prikaz opozorilnega okna

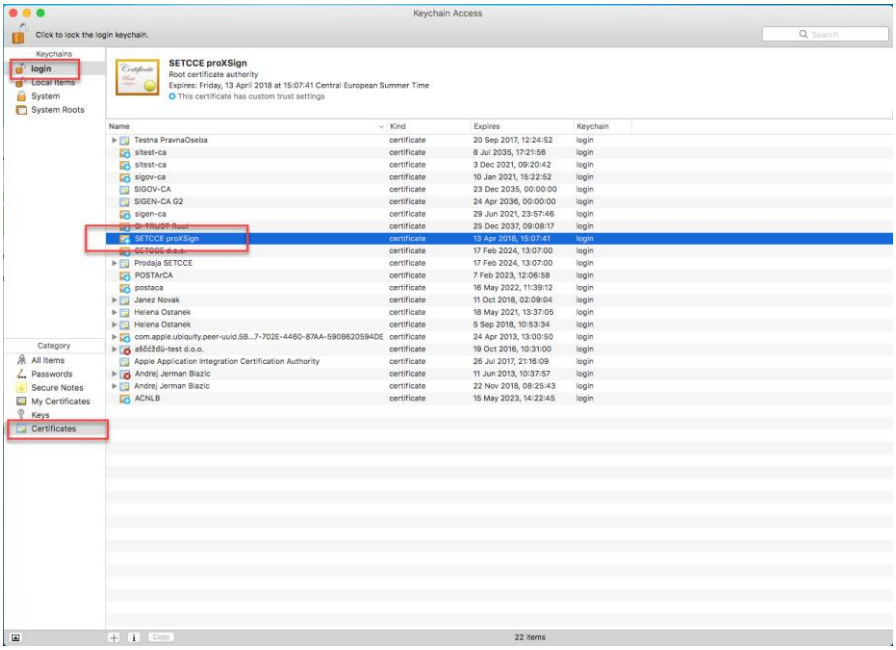
3.3.1. Postopek namestitve »SETCCE proXSign« digitalnega potrdila

Po uspešni namestitvi komponente, se ob prvem zagonu le-te pojavi spodnje opozorilo, ki ga je potrebno potrditi. 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.



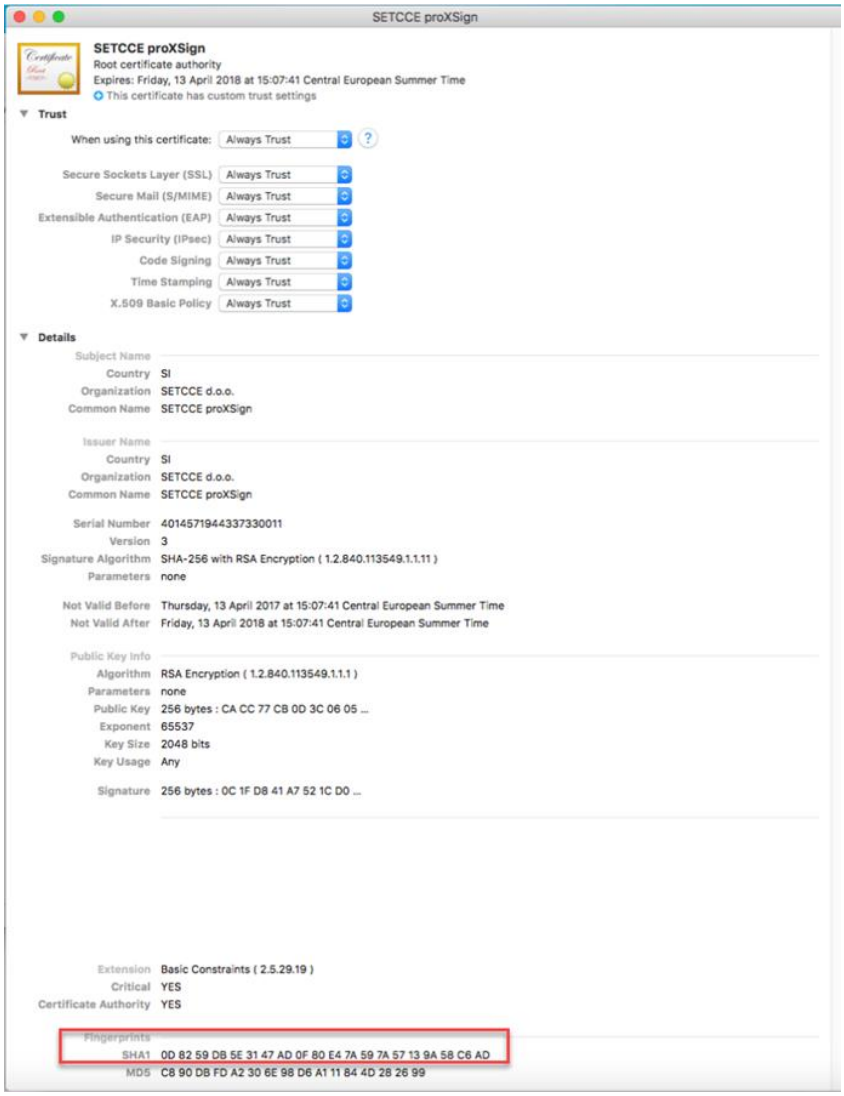
Slika 2: »SETCCE proXSign« security warning

»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)

Prstni odtis digitalnega potrdila **»SETCCE proXSign«** ki se namesti v digitalno shrambo potrdil se mora ujemati s prstnim odtisom na sliki 4.



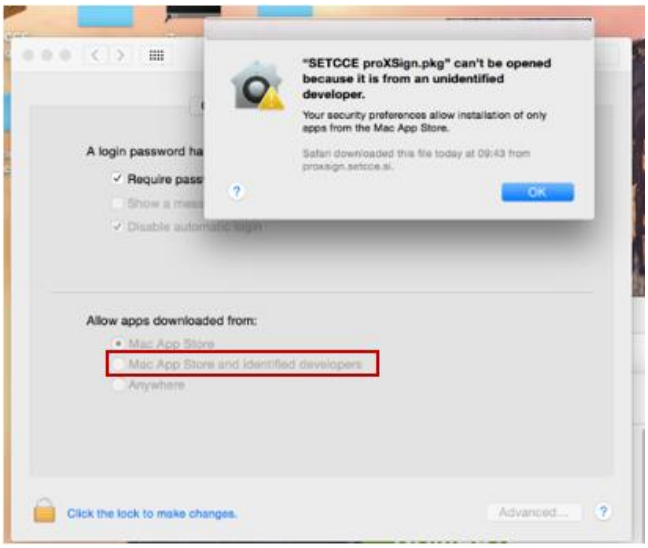
Slika 4: Prstni odtis digitalnega potrdila »SETCCE proXSign«

4. NAMESTITEV IN POSODOBITEV

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.

4.1. Postopek namestitve SETCCE proXSign® komponente

Namestitveni paket se imenuje »SETCCE_proXSign_<*version*>.pkg«. Paket ni podpisan in ni prenešen iz »Mac App store«, zato je potrebno prenos namestitvenega paketa dodatno omogočiti. Pod »System Preferences«/»Security & Privacy« izberite možnost »Mac App Store and identified developers«, kot je prikazano na sliki 5.



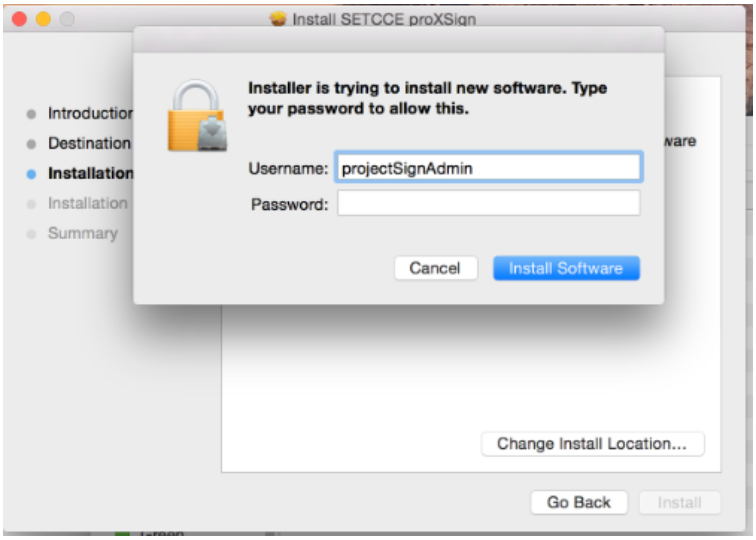
Slika 5: Prikaz nastavitev v »System Preferences« / »Security & Privacy«

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

4.1.1. Postopek namestitve

Za namestitev komponente sledite naslednjim korakom:

1. Prijavite se kot uporabnik z administratorskimi pravicami.
2. Prenesete namestitveni paket »SETCCE_proXSign_<version>.pkg«.
3. 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 6: Prikaz namestitve

4. Po končani namestitvi je potrebno SETCCE proXSign® komponento zagnati. Glej poglavje 5.1.

Pomembno:
Pred nadgradnjo komponente le-to ugasnite (»Quit/Izklopi«) in jo odstranite iz Application mape. Glej poglavje 5.3.

4.2. Posodobitev SETCCE proXSign® komponente

Posodobitev komponente (na zahtevo ali samodejno) v tej izdaji ni podprto.

4.3. Preverjanje različice SETCCE proXSign® komponente

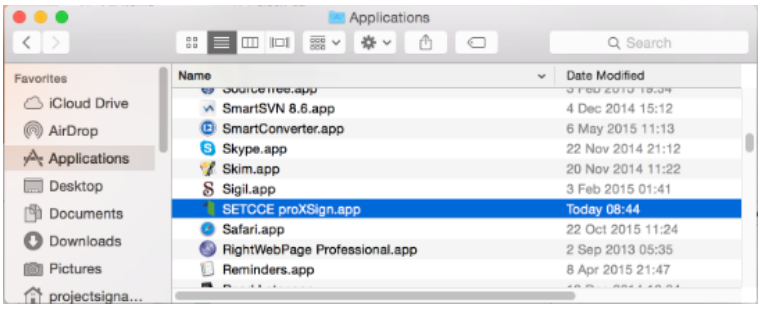
Preverjanje različice komponente v tej izdaji ni podprto.

5. ZAUSTAVITEV DELOVANJA IN PONOVNI ZAGON

5.1. Zagon SETCCE proXSign® komponente

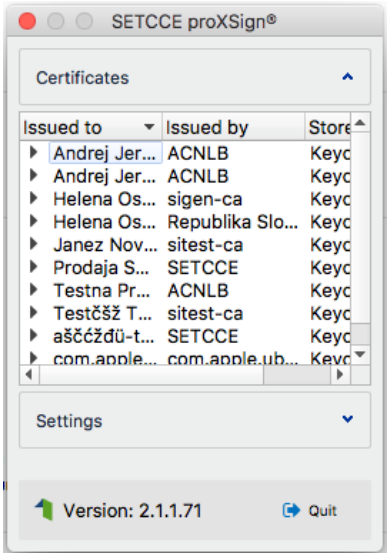
Komponento lahko zaženete na naslednji način:

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



Slika 7: 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.

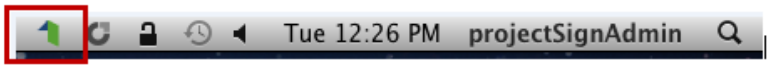


Slika 8: Prikaz osnovnega pojavnega okna SETCCE proXSign® komponente

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

Slika 9: Ikona SETCCE proXSign v »Launchpad«

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



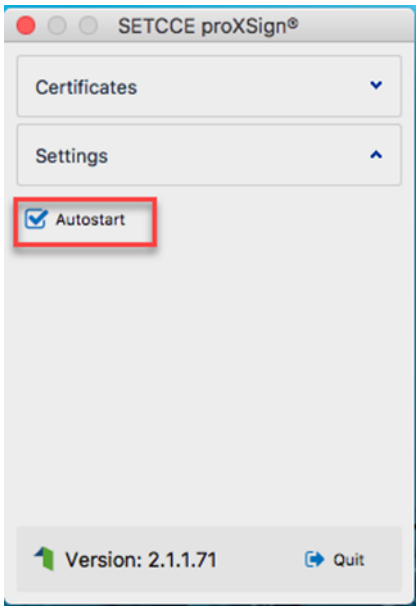
Slika 10: Prikaz ikone SETCCE proXSign v status meniju

5.2. Samodejni zagon

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

»**Autostart/Samodejni zagon«** se lahko nastavi na dva načina:

1. Če je SETCCE proXSign® komponenta že zagnana, v **Status** meniju kliknete na »**proXSign**« ikono in izberete možnost »**Autostart/Samodejni zagon«**.
2. V osnovnem pojavnem oknu komponente, s klikom na gumb »**Settings/Nastavitve**« odprete možnosti in izberete možnost »**Autostart/Samodejni zagon**«.



Slika 11: Prikaz izbire možnosti »Autostart/Samodejni zagon«

Privzeto je možnost »Autostart/Samodejni zagon« omogočena.

5.3. Zaustavitev delovanja

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

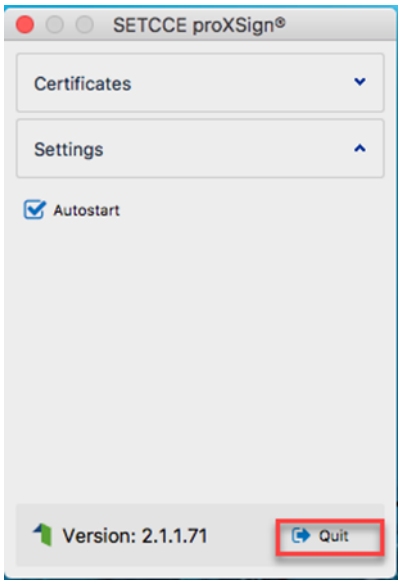
V kolikor želite, da se delovanje SETCCE proXSign® komponente povsem zaustavi (ugasne), lahko to storite na dva načina:

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

   S klikom na gumb »**Quit/Izklopi**« 

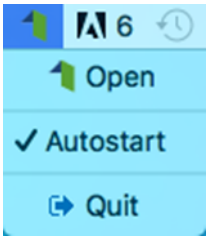
SETCCE proXSign® komponenta preneha delovati (proces se ubije).

   Za ponovni zagon glej točko 5.1.



Slika 12: Prikaz izbire možnosti »Quit«/» Izklopi«

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



Slika 13: 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.

6. ODSTRANITEV SETCCE PROXSIGN® KOMPONENTE

V sistem se prijavite kot uporabnik z administratorskimi pravicami in iz map/lokacij, kamor ste predhodno namestili pakete proXSign.app in »SETCCE_proXSign_<version>.pkg, le te odstranite/brišite.

Prav tako iz shrambe digitalnih potrdil Keychain/Login in Mozilla Firefox shrambe, izbrišite »SETCCE proXSign« digitalno potrdilo.

7. NAMESTITEV OSEBNEGA DIGITALNEGA POTRDILA

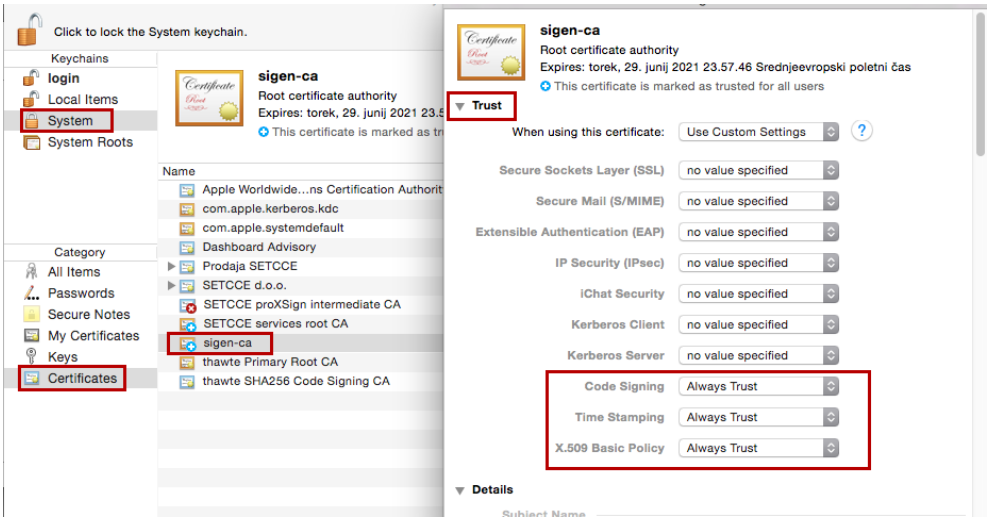
7.1. Ali imate nameščeno osebno digitalno potrdilo?

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.

7.1.1. 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.

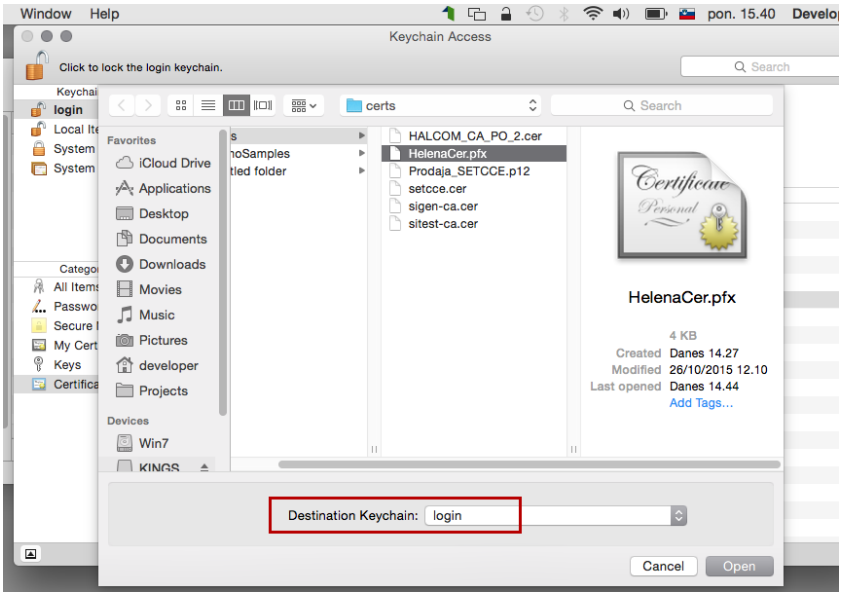


Slika 18: Prikaz namestitve korenskega digitalnega potrdila v »Keychain Access« in sprememba zaupanja

7.1.2. 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 14. 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 7.2.

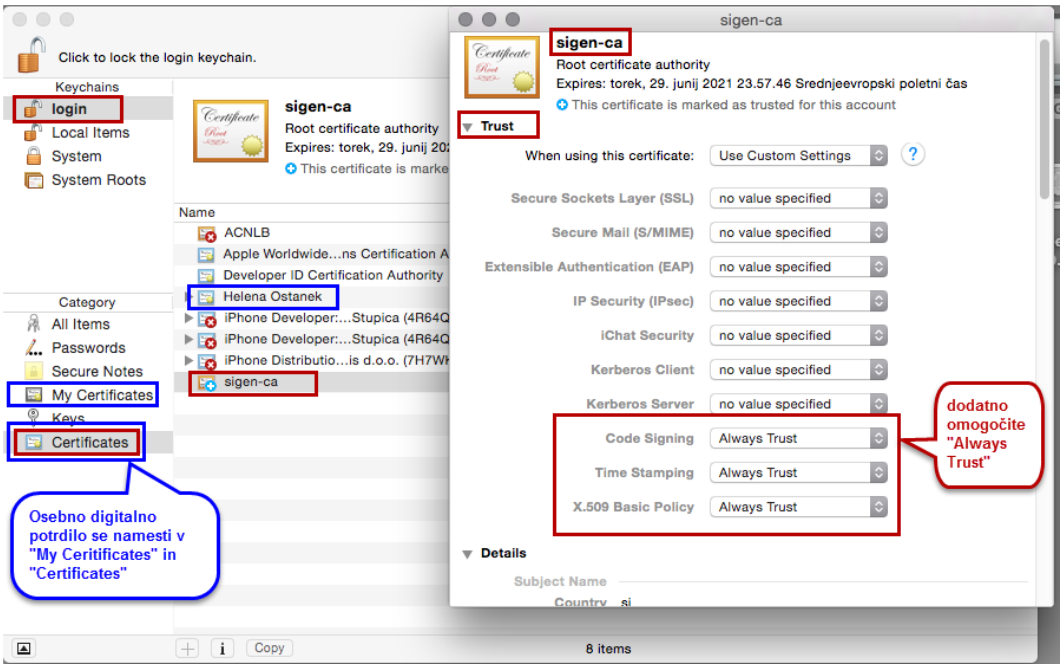


Slika 14: Prikaz namestitve osebnega digitalnega potrdila v Keychain Access

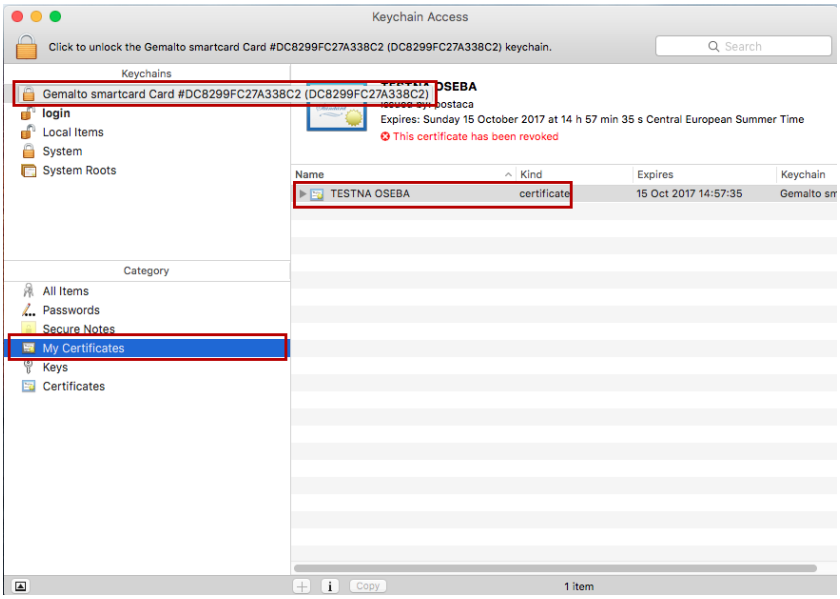
S tem postopkom namestitve se **obe digitalni potrdili** namestita v **Keychains/Login** in **Category/Certificates,** osebno pa je nameščeno tudi pod **Category/My Certificates** kot je prikazano na sliki 15.

Pomembno:

1. Privzeto se korensko digitalno potrdilo ne namesti kot zaupanja vredno, zato morate te lastnosti dodatno omogočiti (Glej 7.2.2).
2. Navedeni postopek namestitve velja za Yosemite in digitalna potrdila, ki se lahko shranijo na trdi disk.
3. Gemalto pametni USB ključ, na katerem je shranjeno osebno digitalno potrdilo, se v Keychain Access aplikaciji odraža kot svoja shramba (Keychain). Glej sliko 16. Za podroben postopek namestitve, se obrnite na izdajatelja vašega osebnega digitalnega potrdila.



Slika 15: Namestitev osebnega digitalnega potrdila v uporabniški (login) Keychain (skupaj s korenskim) po postopku v poglavju 7.1.1



Slika 16: Primer namestitve osebnega digitalnega potrdila v Keychain Access, ki se nahaja na Gemalto pametnem USB ključu

7.2. Ali imate nameščeno korensko digitalno potrdilo?

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

Nekatere aplikacije/storitve, ki delujejo v okviru Ministrstva za javno upravo RS, v podpis pošiljajo odtise (hash) dokumentov (eVEM, E-uprava, sodišče, ...). V ta namen zahtevajo

zaupanje v izdajatelja, s čigar potrdilom so ti odtisi podpisani. Trenutno je to vedno izdajatelj SIGOV-CA.

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

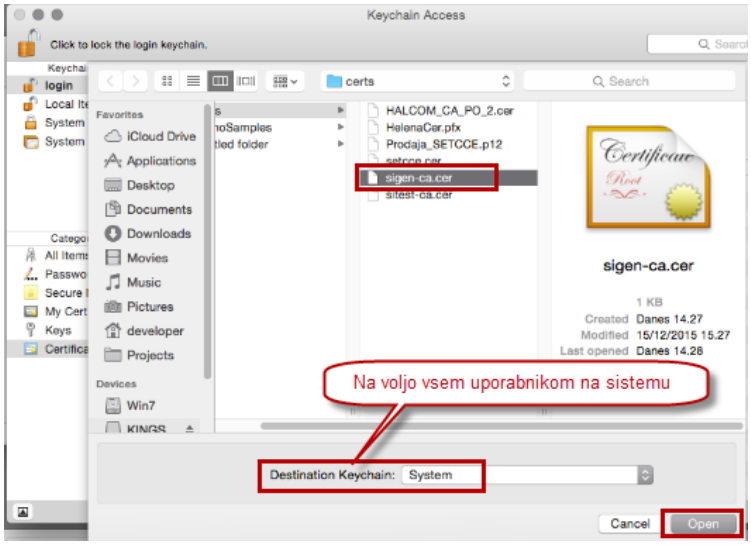
7.2.1. Postopek namestitve

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

1. **Samodejno**, **ob prvi namestitvi vašega osebnega digitalnega potrdila** (Glej 7.1.). 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.

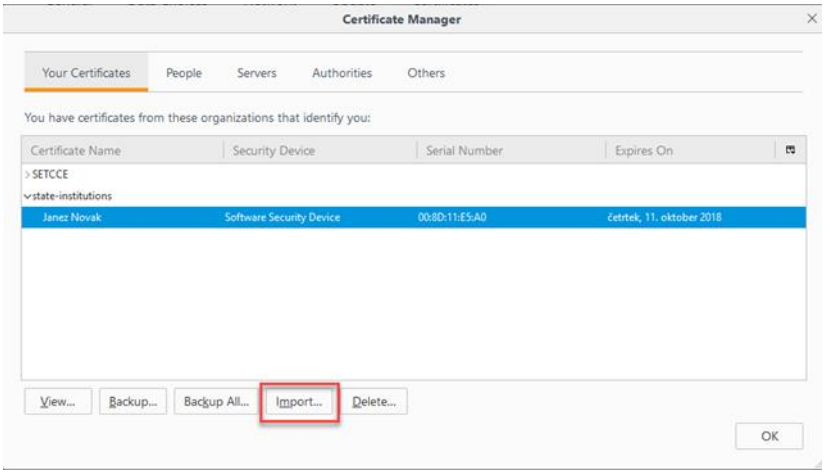


Slika 17: Namestitev korenskega digitalnega potrdila v sistemsko shrambo (System Keychain)

7.2.2. Namestitev potrdila v Mozilla Firefox shrambo

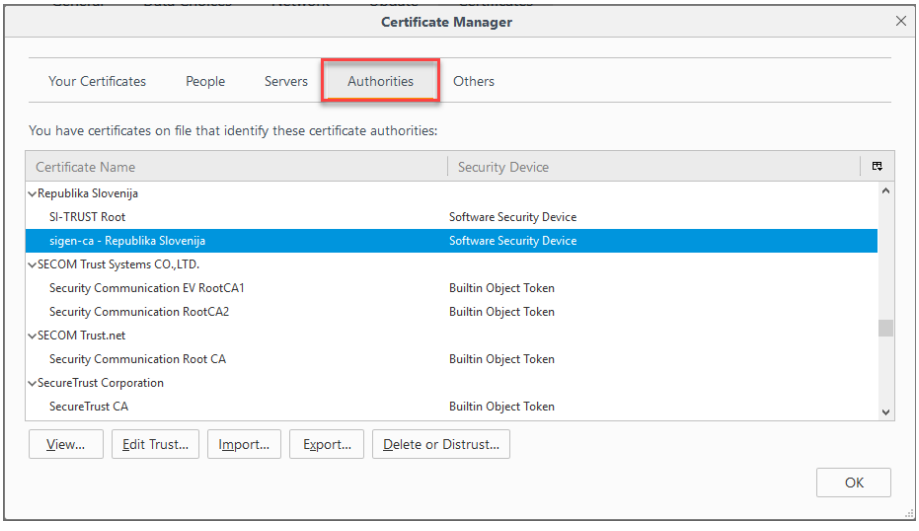
Namestitev potrdila v Mozilla Firefox shrambo preko brskalnika **Mozilla Firefox:**

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 19.



Slika 19: Digitalno potrdilo »Janez Novak« med osebnimi 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 20.



Slika 20: Korensko digitalno potrdilo »Sigen-ca« med »Zaupanja vredni overitelji korenskih potrdil« v Mozilli 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.

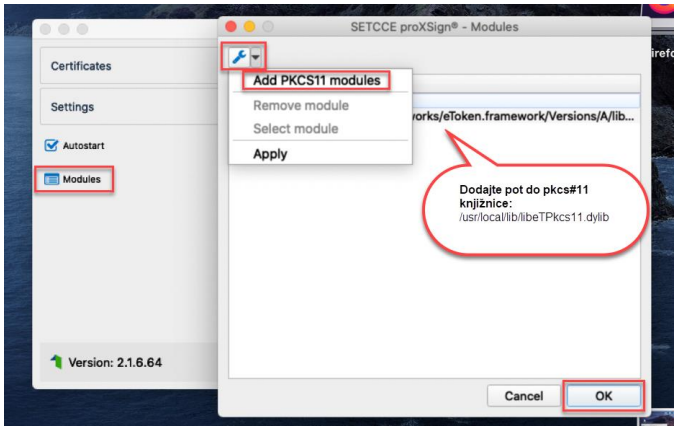
2. Če si SETCCE proXSign® komponento **namestite in zaženete** preko brskalnika **Mozilla Firefox**, morate po končani namestitvi brskalnik zapreti in ponovno zagnati. Tako Mozilla Firefox brskalnik osveži svoje podatke in »SETCCE proXSign« digitalno potrdilo obvelja.

8. UPORABA POŠTA®CA DIGITALNEGA POTRDILA NA ZUNANJEM MEDIJU

Digitalna potrdila slovenskega kvalificiranega izdajatelja pošta®CA na zunanjih medijih so z različico komponente SETCCE proXSign® 2.1.6.64 na macOS Catalina in novejših podprta z uporabo knjižnice pkcs#11 in ne več prek Keychain1.

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 »Moduli«.
4. Izberite »Tools« in iz padajočega menija izberite »Add PKCS11 modules«.



Slika 21: Primer nastavitev knjižnice pkcs#11 za delo z pošta®CA digitalnim potrdilom na zunanjem mediju.

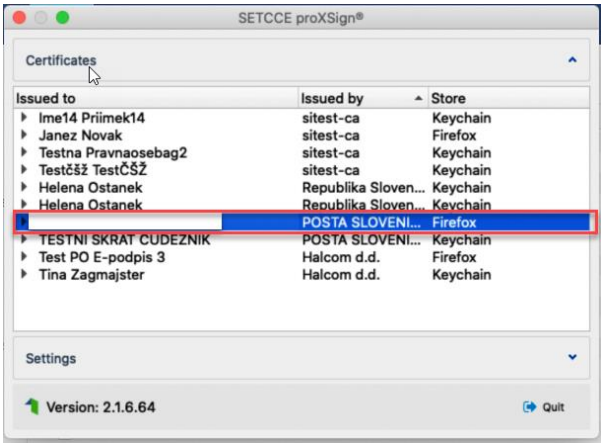
5. Odpre se vam dialoško okno. Na datotečnem sistemu poiščite in izberite knjižnico za pkcs#11, ki se na vaš računalnik namesti skupaj z SAC.
6. Za lokacijo knjižnice preverite navodila izdajatelja vašega digitalnega potrdila.

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

   `/usr/local/lib/`**`libeTPkcs11.dylib`**

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

[1] Testirano z Gemalto SafeNet Authentication Client (SAC), različica SAC 10.2.(10.2.97.0) na macOS Catalina 10.15. V primeru sprememb v delovanju Gemalto SAC pkcs#11 knjižnice libeTPkcs11.dylib, delovanja ne garantiramo.



Slika 22: Prikaz digitalnega potrdila pošta®CA na zunanjem mediju v komponenti proXSign®