

SETCCE

Uporabniška navodila za namestitev in upravljanje komponente SETCCE proXSign® v2.0.11 za MAC OS X

[Nova generacija komponent SETCCE proXSign®]



Identifikacijska oznaka dokumenta: **n/a**
Različica dokumenta: 9
Avtorji dokumenta: Helena Ostanek, Anja Rožac
Status dokumenta: Zaupen
Zadnja sprememba: dokumenta: 07.11.2016

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.si

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 osebnega digitalnega potrdila	5
3.3. Zaupanje digitalnim potrdilom »SETCCE services root CA« in »SETCCE proXSign intermediate CA«	5
3.3.1. Postopek namestitve SETCCE digitalnih potrdil	5
4. Namestitev in posodobitev	9
4.1. Postopek namestitve SETCCE proXSign® komponente	9
4.1.1. Postopek namestitve	9
4.2. Posodobitev SETCCE proXSign® komponente	10
4.3. Preverjanje različice SETCCE proXSign® komponente	10
5. Zaustavitev delovanja in ponovni zagon	11
5.1. Zagon SETCCE proXSign® komponente	11
5.2. Samodejni zagon	12
5.3. Zaustavitev delovanja	12
6. Odstranitev SETCCE proXSign® komponente	14
7. Namestitev digitalnega potrdila	15
7.1. Ali imate nameščeno osebno digitalno potrdilo?	15
7.1.1. Postopek namestitve	15
7.2. Ali imate nameščeno korensko digitalno potrdilo?	17
7.2.1. Postopek namestitve	17
7.2.2. Zaupanja vredno korensko digitalno potrdilo	18

1. NOVA GENERACIJA KOMPONENT SETCCE PROXSIGN®

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

Nova generacija v 2.0.0 je nastala kot odziv na omejitve večine spletnih brskalnikov pri podpori vtičnikom.

Nova generacija podpisne komponente 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 proXSign uporabiti (npr. spletna banka, storitve e-uprave itd.), nato na podporo SETCCE.

2. PODPRTA OKOLJA

2.1. Podprta okolja

Operacijski sistem	Brskalnik
MAC OS X: • Yosemite 10.10 • El Capitan 10.11	 Safari 9.0.1 in 9.0.3
macOS: • Sierra 10.12	 Safari 10.0.1

3. POGOJI ZA DELOVANJE SETCCE PROXSIGN® KOMPONENTE

3.1. Port za komunikacijo med brskalnikom in komponento

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

- 14972
- 41472
- 57214
- 61427

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

3.2. Namestitev osebne digitalnega potrdila

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

3.3. Zaupanje digitalnim potrdilom »SETCCE services root CA« in »SETCCE proXSign intermediate CA«

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

V ta namen se uporabljata dva digitalna potrdila, ki ju je izdala družba **SETCCE d.o.o.**:

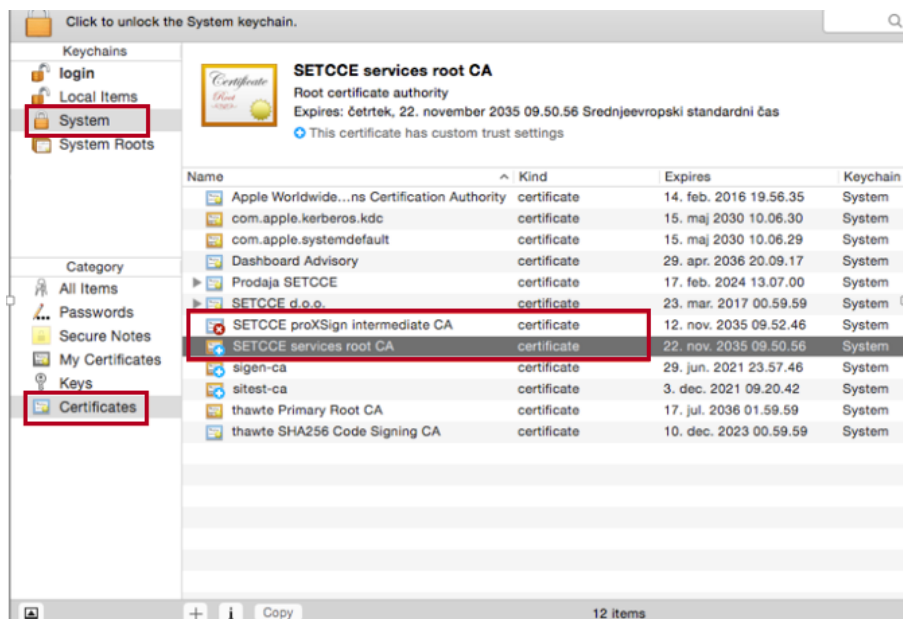
- **SETCCE services root CA** in
- **SETCCE proXSign intermediate CA**,

v nadaljevanju SETCCE digitalni potrdili.

3.3.1. Postopek namestitve SETCCE digitalnih potrdil

Ob **prvem zagonu** komponente se v sistemsko shrambo digitalnih potrdil, med zaupanja vredna potrdila, samodejno namestita korensko digitalno potrdilo »**SETCCE services root CA**« in vmesno digitalno potrdilo »**SETCCE proXSign intermediate CA**«, oba izdajatelja SETCCE d.o.o..

Obe SETCCE digitalni potrdili se namestita v sistemsko shrambo digitalnih potrdil, pod **Keychains/System** in **Category/Certificates** kot je prikazano na sliki 1.

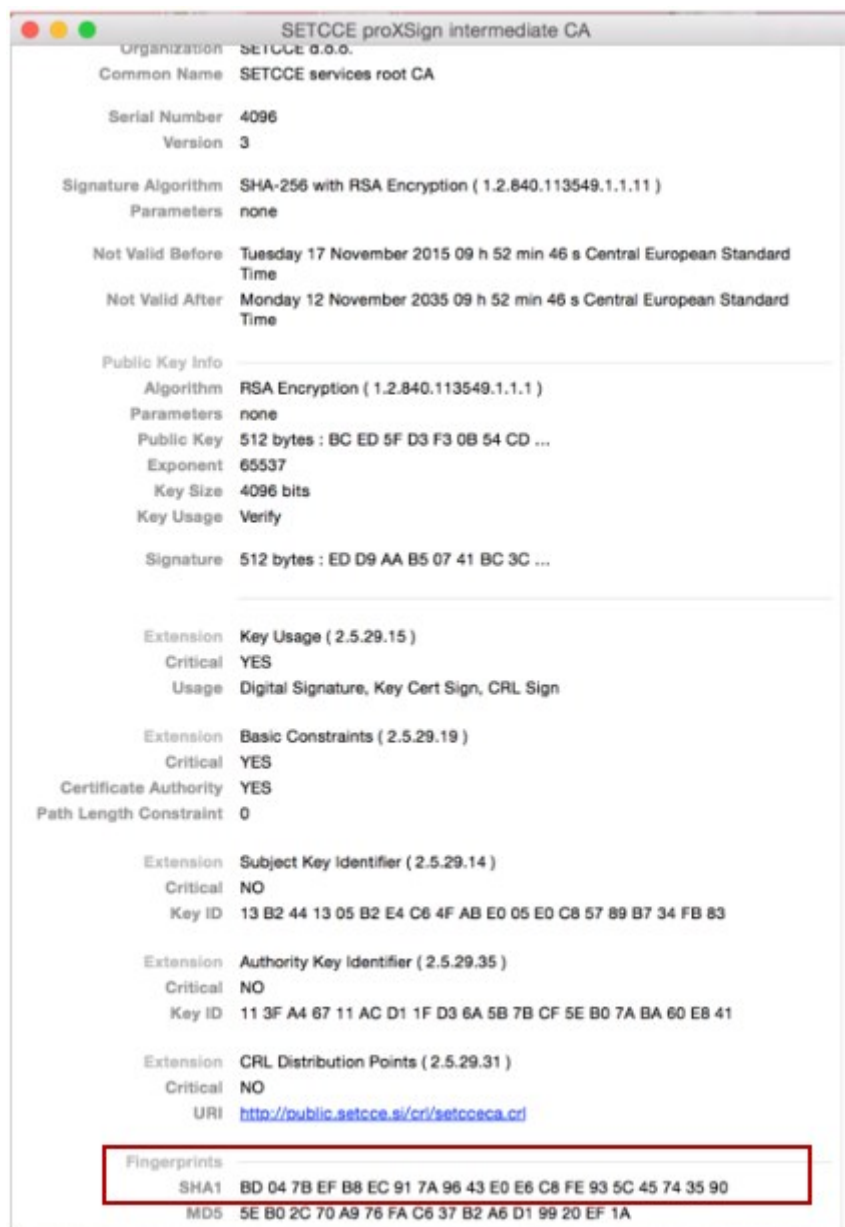


Slika 1: Prikaz namestitve SETCCE digitalnih potrdil v sistemske shrambi (System Keychain)

Prstni odtis digitalnega potrdila »**SETCCE services root CA**«, ki se namesti v digitalno shrambo potrdil se mora ujemati s prstnim odtisom na sliki 2, prstni odtis digitalnega potrdila »**SETCCE proXSign intermediate CA**« pa s prstnim odtisom na sliki 3.

SETCCE services root CA	
Organization	SETCCE d.o.o.
Common Name	SETCCE services root CA
Issuer Name	
Country	SI
State/Province	Slovenia
Organization	SETCCE d.o.o.
Common Name	SETCCE services root CA
Serial Number	00 96 94 B6 D3 A3 54 3E 58
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Tuesday 17 November 2015 09 h 50 min 56 s Central European Standard Time
Not Valid After	Thursday 22 November 2035 09 h 50 min 56 s Central European Standard Time
Public Key Info	
Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	none
Public Key	512 bytes : EE 15 43 5B 7D 6F 9C D4 ...
Exponent	65537
Key Size	4096 bits
Key Usage	Verify
Signature	512 bytes : 61 F3 47 3A E5 1F 4D D1 ...
Extension Key Usage (2.5.29.15)	
Critical	YES
Usage	Digital Signature, Key Cert Sign, CRL Sign
Extension Basic Constraints (2.5.29.19)	
Critical	YES
Certificate Authority	YES
Extension Subject Key Identifier (2.5.29.14)	
Critical	NO
Key ID	11 3F A4 67 11 AC D1 1F D3 6A 5B 7B CF 5E B0 7A BA 60 E8 41
Extension Authority Key Identifier (2.5.29.35)	
Critical	NO
Key ID	11 3F A4 67 11 AC D1 1F D3 6A 5B 7B CF 5E B0 7A BA 60 E8 41
Fingerprints	
SHA1	D0 64 E2 3F 30 2C CE BD 50 39 FF 51 31 25 BB AC 85 39 B7 84
MD5	46 7D D1 BD E2 64 F9 8B 86 42 C1 C6 67 B7 AA 20

Slika 2: prstni odtis digitalnega potrdila »SETCCE services root CA«



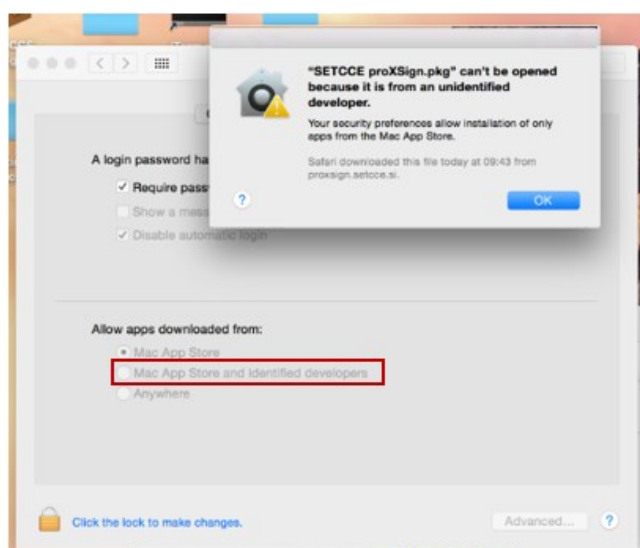
Slika 3: prstni odtis vmesnega digitalnega potrdila »SETCCE proXSign intermediate CA«

4. NAMESTITEV IN POSODOBITEV

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.pkg«. Ker ni podpisan in ni prenešen iz »Mac App store«, morate prenos namestitvenega paketa dodatno omogočiti. Pod »System Preferences«/»Security & Privacy« izberite možnost »Mac App Store and identified developers«, kot je prikazano na sliki 4.



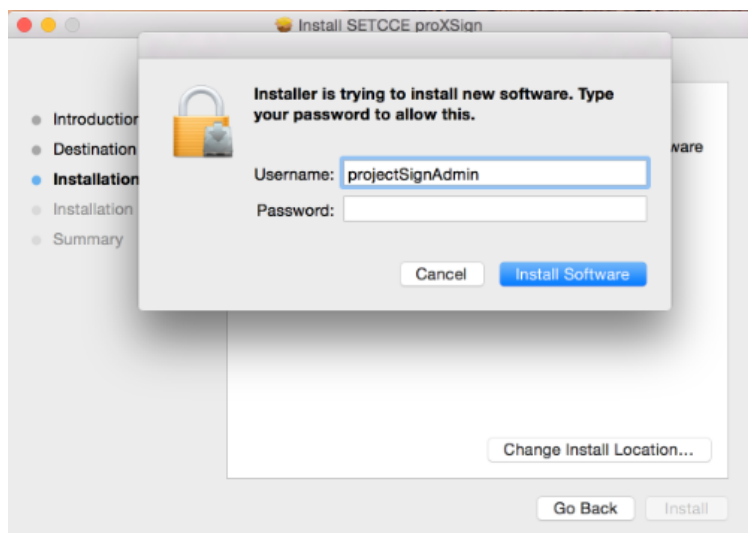
Slika 4: prikaz nastavitev v »System Preferences« / »Security & Privacy«

Namestitev 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.pkg«.
3. Kliknete na namestitveni paket in sledite korakom namestitve. Komponenta proXSign.app se privzeto namesti v mapo »**Applications**«.



Slika 5: prikaz namestitve

4. Po končani namestitvi morate komponento zagnati. Glej poglavje 5.1.

Pomembno:

Pred nadgradnjo komponente le-to ugasnite (»Quit/Izklopi«). 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

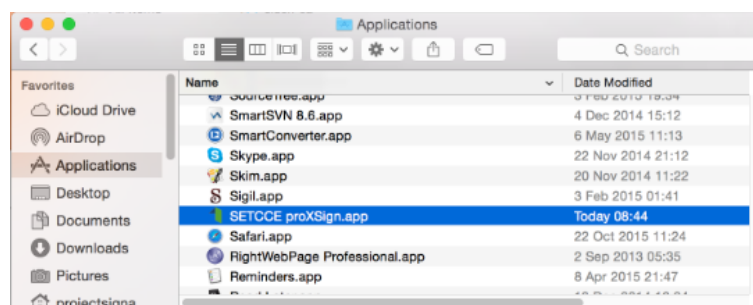
Preverjanje različice komponente v tej izdaji ni podprto.

5. ZAUSTAVITEV DELOVANJA IN PONOVI ZAGON

5.1. Zagon SETCCE proXSign® komponente

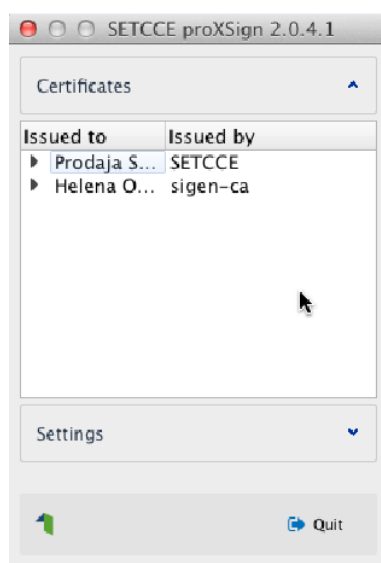
Komponento lahko zaženete na naslednji način:

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



Slika 6: Prikaz zagona komponente SETCCE proXSign.app

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



Slika 7: Prikaz osnovnega pojavnega okna komponente

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



Slika 8: Ikona SETCCE proXSign v »Launchpad«

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



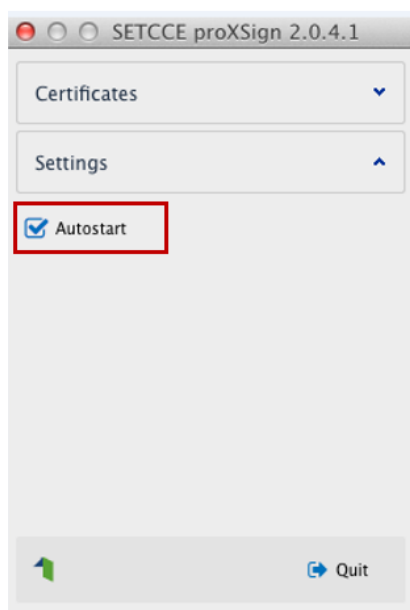
Slika 9: Prikaz ikone proXSign v Status meniju

5.2. Samodejni zagon

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

Samodejni zagon se lahko nastavi na dva načina:

1. Če je 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 10: Prikaz izbire možnosti »Autostart/Samodejni zagon«

Privzeto je možnost »Autostart/Samodejni zagon« onemogočena.

5.3. Zaustavitev delovanja

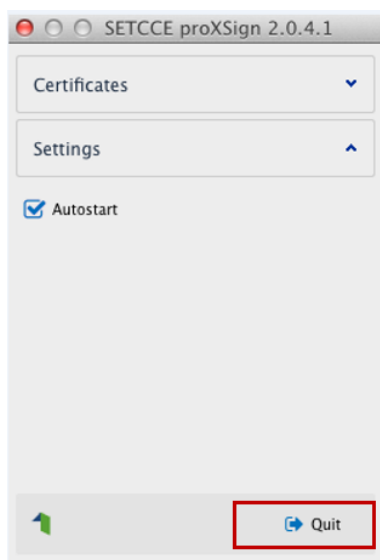
Predlagamo, da komponento proXSign pustite, da teče v ozadju. Komponenta v tem času ne izvaja aktivnosti.

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

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

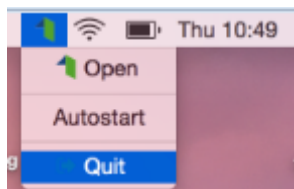
S klikom na gumb »**Quit/Izklopi**«  komponenta preneha delovati (proces se ubije).

Za ponovni zagon glej točko 5.1.



Slika 11: Prikaz izbire možnosti »Quit«/» Izklopi«

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



Slika 12: 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 skriva v območje Status menija. 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.pkg«, le te odstranite/brišite.

Prav tako iz shrambe digitalnih potrdil (Keychain Access) izbrišite obe digitalni potrdili:

- »SETCCE services root CA« in
- »SETCCE proXSign intermediate CA«.

7. NAMESTITEV DIGITALNEGA POTRDILA

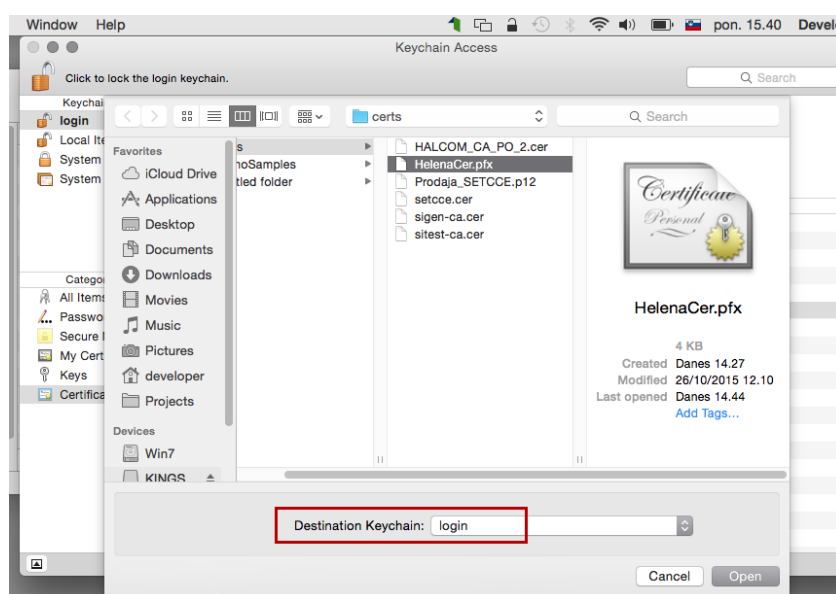
7.1. Ali imate nameščeno osebno digitalno potrdilo?

Pred podpisovanjem dokumentov s komponento SETCCE proXSign® morate imeti nameščeno osebno digitalno potrdilo v shrambi osebnih digitalnih potrdil ali na pametni kartici.

7.1.1. Postopek namestitve

Za namestitev osebnega digitalnega potrdila sledite naslednjim korakom:

1. Svoje osebno digitalno potrdilo shranite na trdi disk.
2. Zaženeta **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**«. 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.



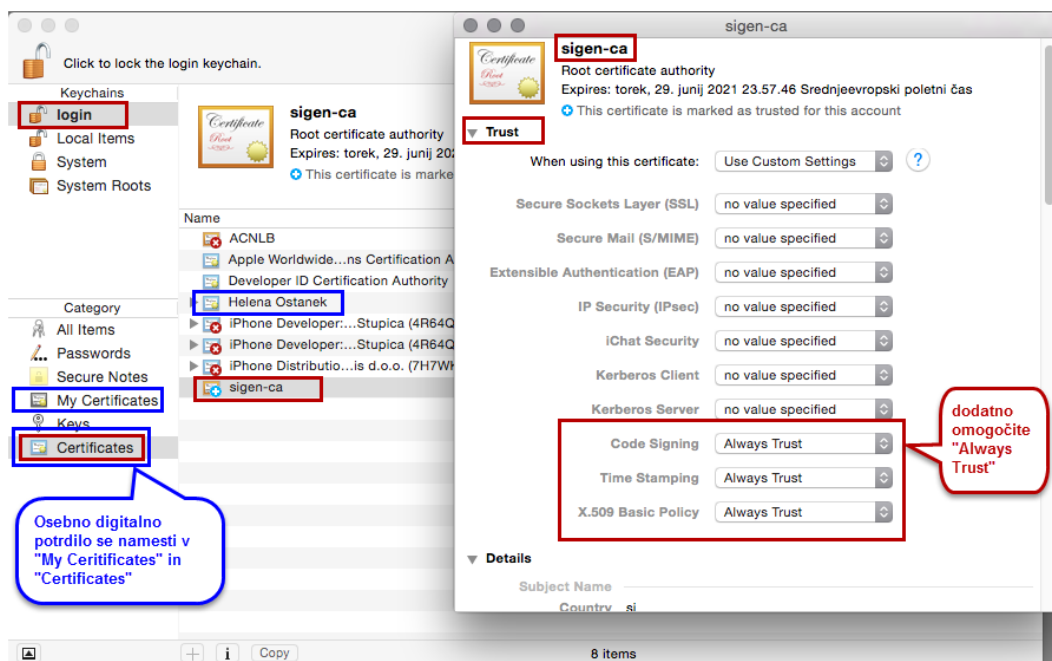
Slika 13: Prikaz namestitve osebnega digitalnega potrdila v Keychain Access

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 14.

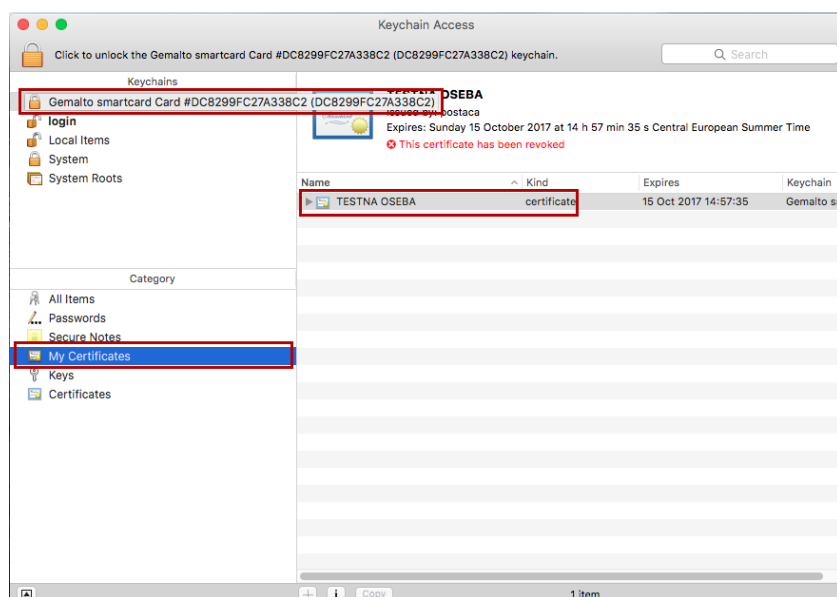
Pomembno:

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 15. Za podroben postopek nemestitve, se obrnite na izdajatelja vašega osebnega digitalnega potrdila.



Slika 14: Namestitev osebnega digitalnega potrdila v uporabniški (login) Keychain (skupaj s korenskim) po postopku v poglavju 7.1.1



Slika 15: 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/default.asp?vsebina=3&sub=6>
- AC NLB: <http://www.nlb.si/ac-nlb-identiteta-ac-nlb>
- HALCOM-CA: <http://xylon.halcom.si/cacert.html>
- SIGEN-CA in SIGOV-CA: http://www.si-ca.si/podpisna_komponenta/korenski_potrdili.php

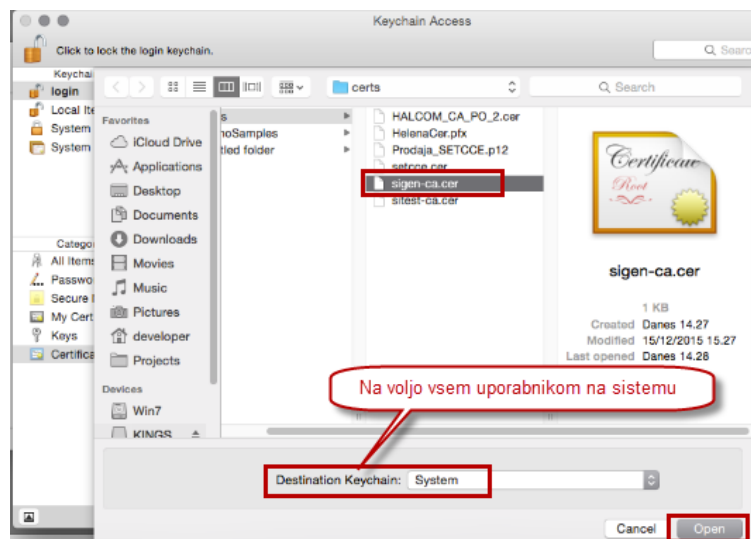
7.2.1. Postopek namestitve

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.

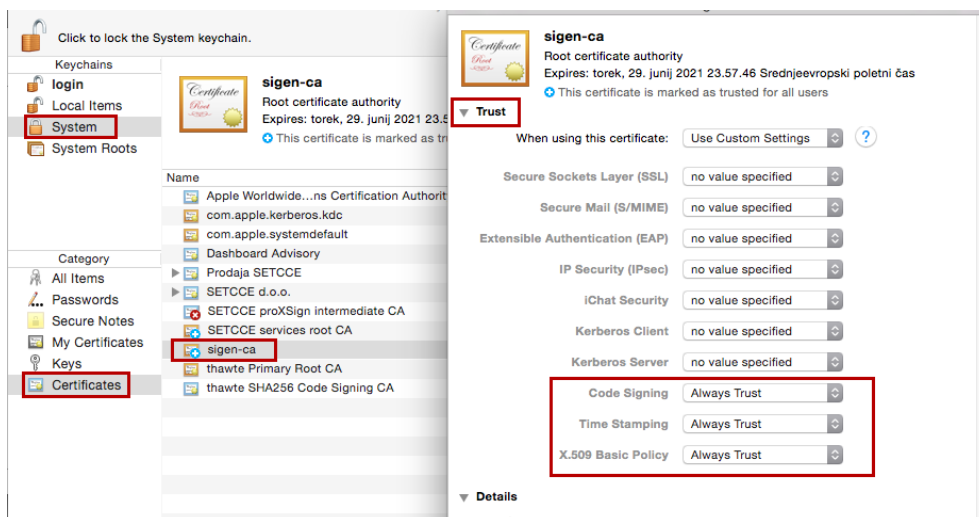


Slika 16: Namestitev korenskega digitalnega potrdila v sistemsko shrambo (System keychain)

7.2.2. 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 urejenje zaupanja in pregled lastnosti digitalnega potrdila.
2. Izbere „**Trust**“ in vsaj za zadnje tri opcije izbere „**Always Trust**“.
3. S klikom na standardni x zaprete okno.
4. In z administratorskim geslom uveljavite spremembo.



Slika 17: Prikaz namestitve korenskega digitalnega potrdila v »Keychain Access« in sprememba zaupanja