

Návod na inštaláciu aplikačného rozhrania SafeNet Authentication Client ver. 10.2.x pre macOS

Nevyhnutným predpokladom pre prácu so SmartCard čipovou kartou Gemalto je inštalácia aplikačného rozhrania pod názvom SafeNet Authentication Client (ďalej SAC) a ovládača pre prístup k zariadeniam typu PC/SC čítačky, vo forme mini SmartCard „USB Shell Token” čítačky alebo plno-formátovej SmartCard „GemPC Twin USB čítačka“.

Ovládač PCSC-Lite pre uvedené čítačky PC/SC zariadení je súčasťou operačného systému macOS.

V prípade ak Vaša čítačka nie je podporovaná ovládačmi operačného systému, prosím kontaktujte výrobcu zariadenia.

1. Inštalácia SafeNet Authentication Client (SAC) v macOS

- V internetovom prehliadači otvorte URL:
<https://eidas.disig.sk/sk/kvalifikovane-certifikaty/podpora/qscd-zariadenia/gemalto/>
- Vyhľadajte kategóriu pre macOS
Kliknite na odkaz „SAC pre macOS“, resp.
URL: https://dsrv.disig.sk/download/gemalto/SAC_10_2_OSX.ZIP
- Iniciujete stiahnutie súboru aplikačného vybavenia SAC komprimovaného ako ZIP archív.

Podľa použitého internetového prehliadača a jeho nastavení môžu nastať tieto situácie:

- A. Súbor archívu ZIP sa automaticky stiahne bez rozbalenia.
Pokračujte podľa:
„Postup A - Dekomprimácia inštalačného ZIP archívu“
- B. Súbor archívu ZIP sa automaticky stiahne a dekomprimuje.
Pokračujte podľa:
„Postup B - Automatická dekompresia inštalačného ZIP archívu“

Postup A - Dekomprimácia inštalačného ZIP archívu

1. Na obrazovke sa zobrazí okno „Stahovanie súborov/File Download“. V okne kliknite na „Uložiť/Save“ a následne prosím vyberte cieľový adresár pre uloženie súboru ZIP archívu.
2. Po skončení stahovania prejdite do adresára, ktorý ste si zvolili pre uloženie súboru ZIP archívu.
3. Súbor ZIP archívu otvorte v programe určenom pre dekomprimáciu a jeho obsah extrahujte do Vami zvoleného adresára.

Krok extrakcie súborov ZIP archívu si vyžaduje zadanie hesla.

Zadajte heslo, ktoré ste dostali spolu so zakúpenou čipovou kartou. V prípade, ak heslom nedisponujete, kontaktujte prosím našu spoločnosť prostredníctvom emailu na adrese „radisig@disig.sk“.

4. V ďalšom kroku pokračujte podľa časti „Inštalácia SAC“.

Postup B - Automatická dekompresia inštalačného ZIP archívu

1. Po dokončení stahovania sa súbor ZIP archívu automaticky otvorí v programe určenom pre dekomprimáciu a jeho obsah bude možné extrahovať do Vami zvoleného adresára.

Krok extrakcie súborov ZIP archívu si vyžaduje zadanie hesla.

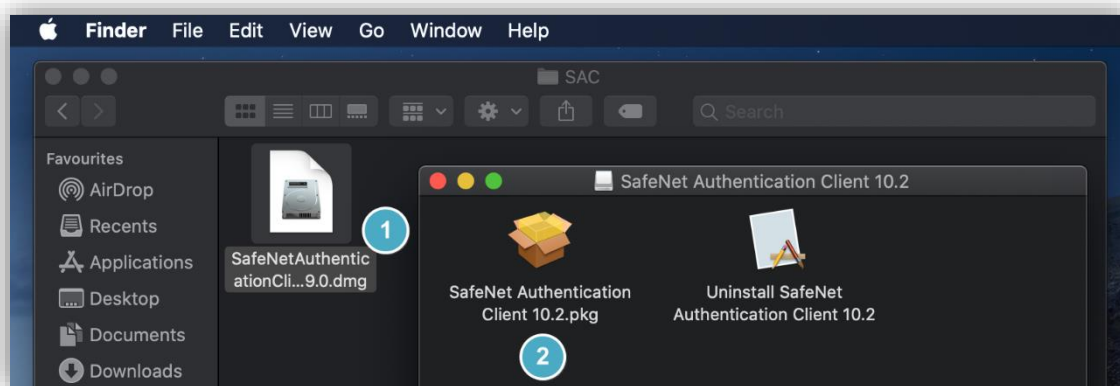
Zadajte heslo, ktoré ste dostali spolu so zakúpenou čipovou kartou. V prípade, ak heslom nedisponujete, kontaktujte prosím našu spoločnosť prostredníctvom emailu na adrese „radisig@disig.sk“.

2. V ďalšom kroku pokračujte podľa časti „Inštalácia SAC“.

2. Inštalácia SAC

Extrakciou ZIP archívu získate adresár „SAC_10.2_OSX“. Inštalačný balík sa nachádza v podadresári: „SAC_10.2_OSX\Installation (Notarized)“.

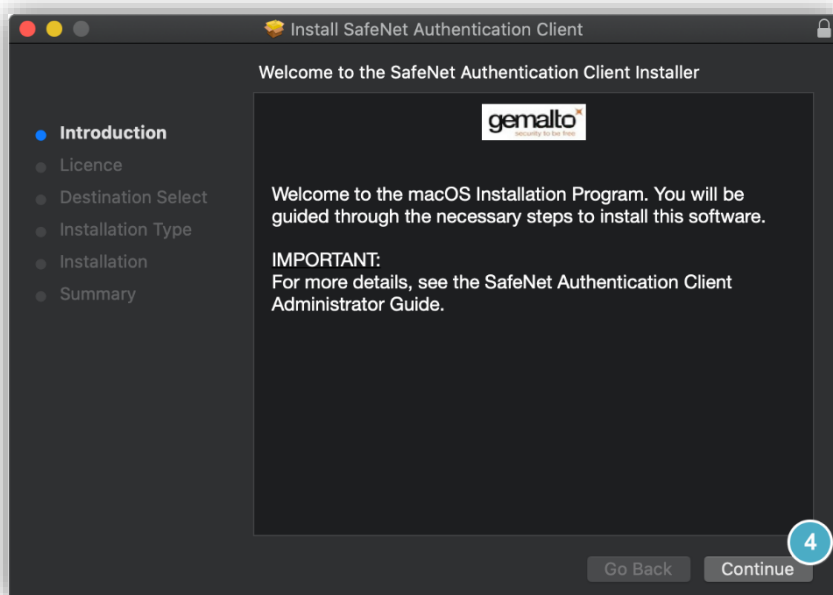
1. Otvorte súbor inštalačného balíka „SafeNetAuthenticationClient.10.2.x.dmg“
2. Spustíte inštalátor aplikácie „SafeNet Authentication Client.pkg“.



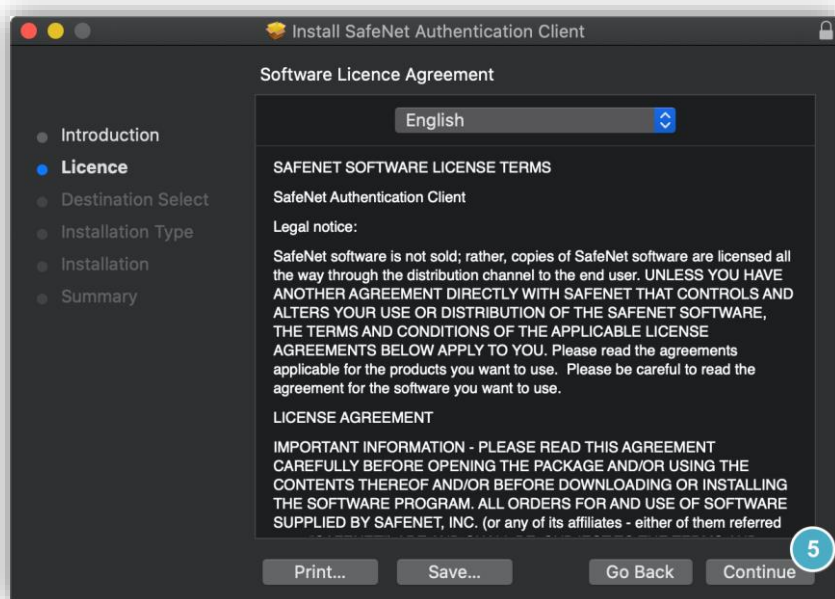
3. Vyjadrite súhlas s inštaláciou aplikácie.



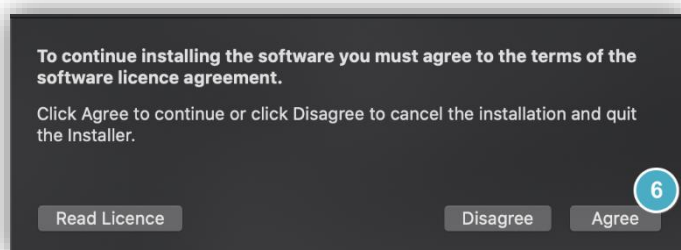
4. Pokračujte v sprievodcovi inštalácie.



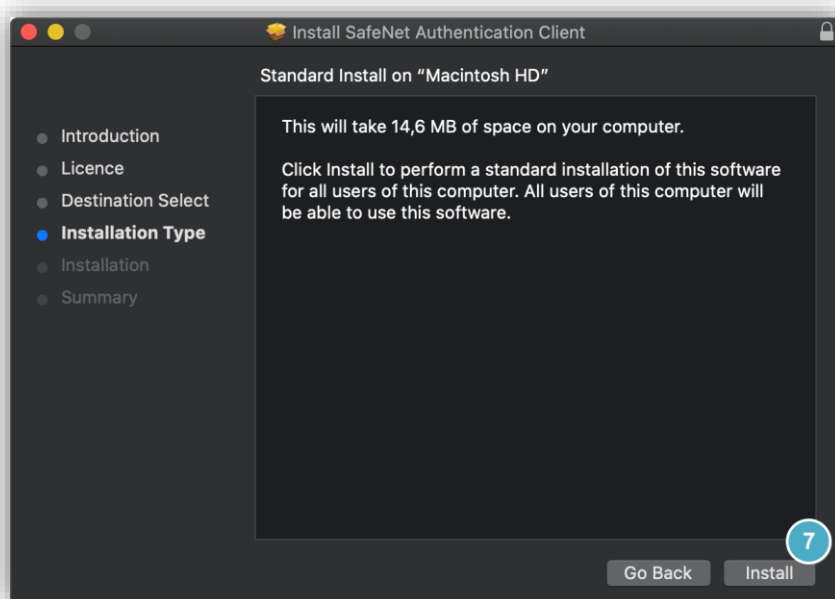
5. Zvoľte jazyk pre zobrazenie softvérovej licencie.



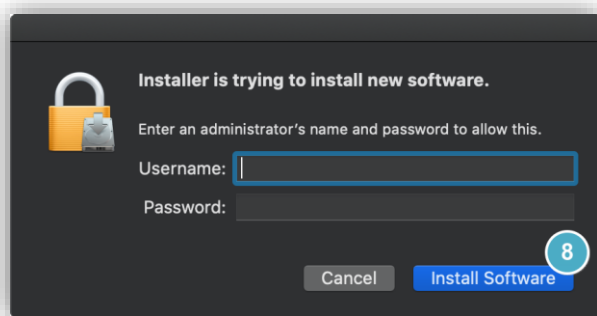
6. V prípade súhlasu vyjadrite súhlas s licenčnými podmienkami.



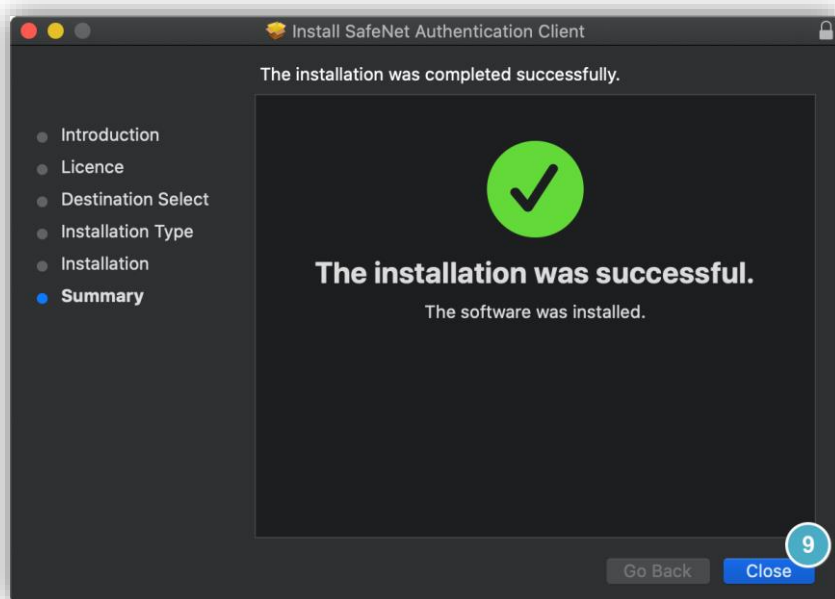
7. Spustíte inštalačný proces.



8. Autentifikujte sa ako užívateľ s právami pre inštaláciu aplikácii.



9. Inštalácia aplikácie SAC prebehla úspešne.



3. Spustenie SAC

Spustenie aplikácie SafeNet Authentication Client (ďalej SAC) prebehne pri nasledujúcom prihlásení užívateľa automatizovane. O behu aplikácie SAC je užívateľ informovaný ikonou s časti „Menu statov“.



Obrázok 1 - SAC detekoval vloženú Gemalto SmartCard

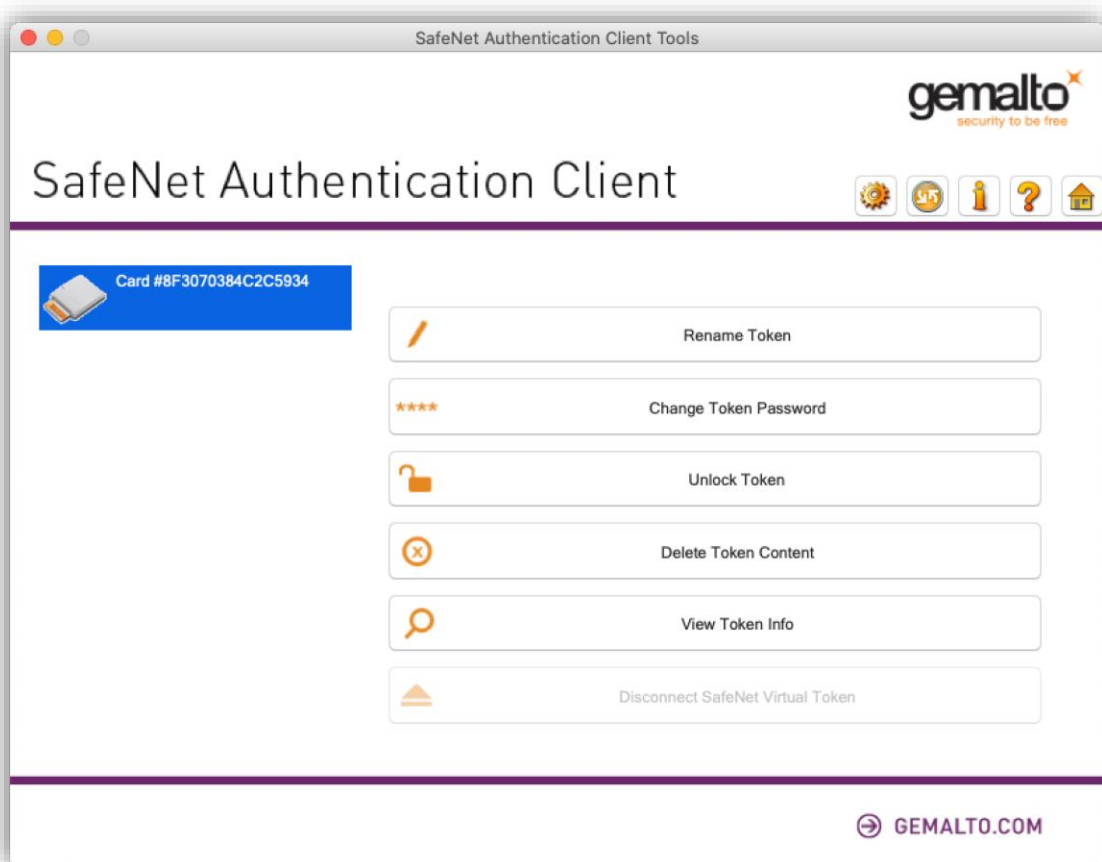


Obrázok 2 - SAC nedetekoval Gemalto SmartCard

Manuálne spustenie aplikácie je možné prostredníctvom zástupcu v zozname nainštalovaných aplikácii.

4. Hlavné okno aplikácie SAC

Hlavné okno aplikácie SAC je možné vyvolať kliknutím na ikonu aplikácie v oblasti „Menu statov“ a výberom voľby „Tools“ v kontextovej ponuke.



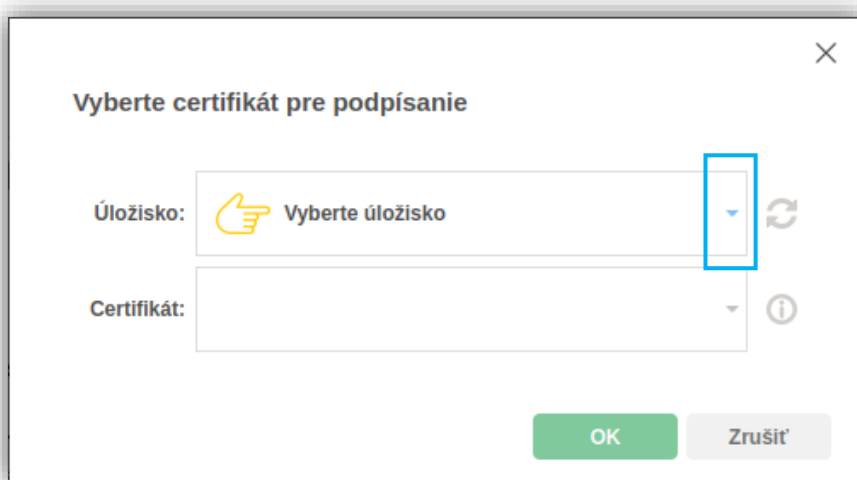
5. Výber podpisového certifikátu

Pri práci s podpisovou aplikáciou, napríklad s webovou aplikáciou Disig Web Signer na portály <https://www.zep.disig.sk> v kroku „Vyberte certifikát na podpísanie“ postupujte nasledovne.

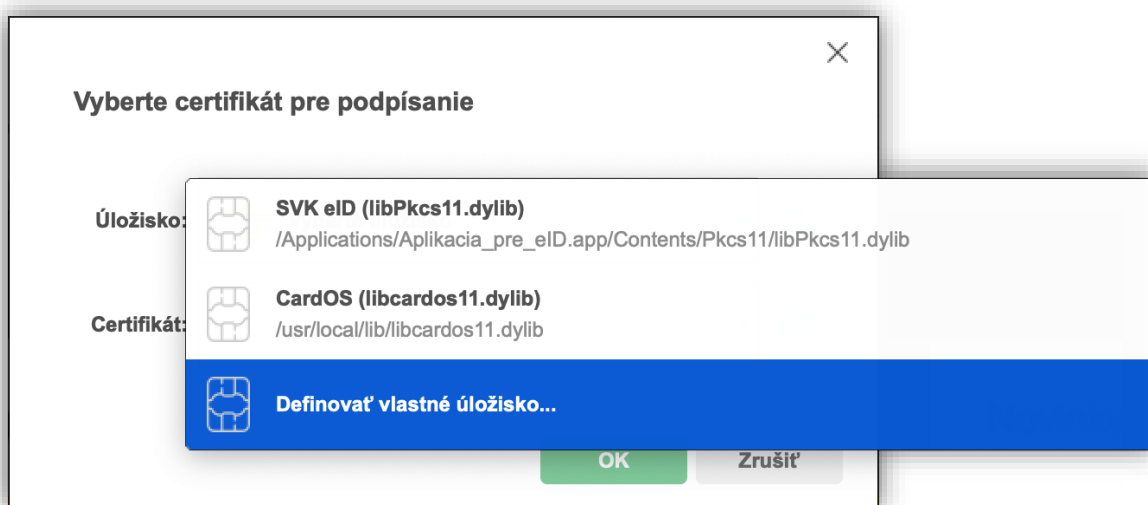
1. Zvoľte úložisko certifikátu.

Vyberte úložisko certifikátov definované knižnicou: “libIDPrimePKCS11.dylib”

A prejdite na bod 3 - Výber certifikátu

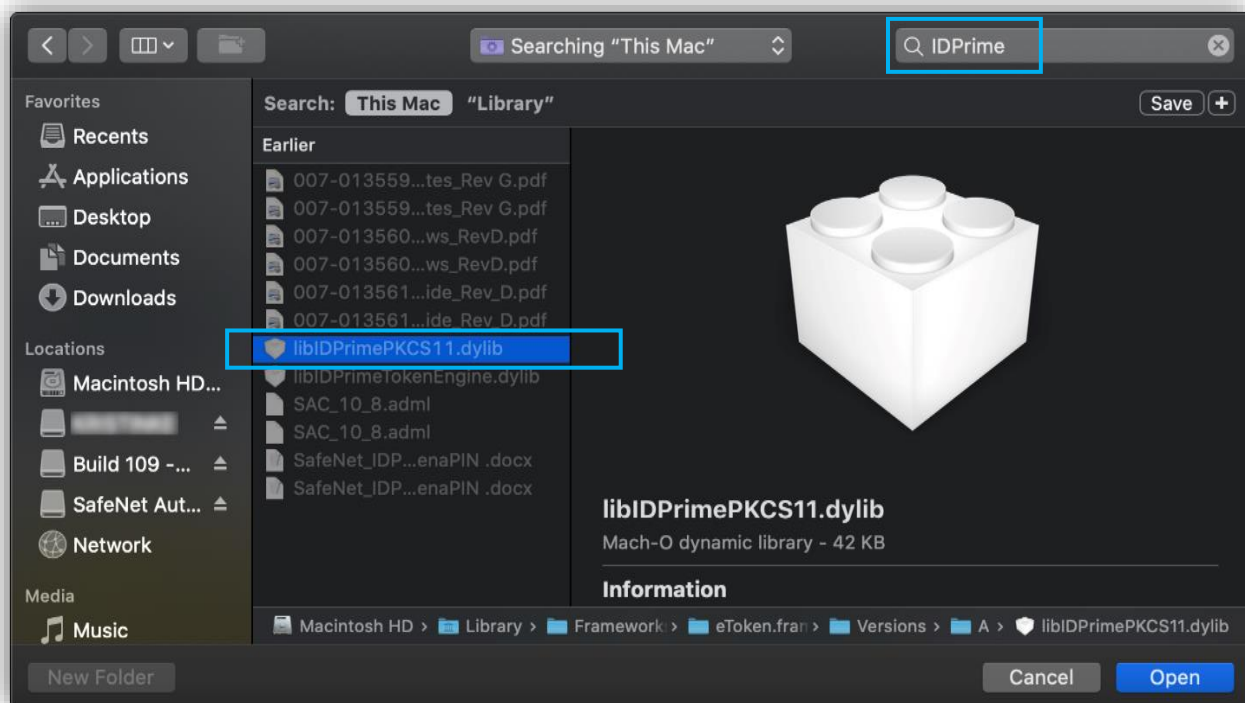


Ak sa v zozname toto úložisko nenachádza, vyberte možnosť: **Definovať vlastné úložisko** a prejdí na bod 2.



2. Definovať vlastné úložisko

Vyhľadajte na súborovom systéme knižnicu PKCS#11 s názvom:
“libIDPrimePKCS11.dylib”



Úplná cesta k súboru knižnice PKCS#11: `/usr/local/lib/libIDPrimePKCS11.dylib`

Resp. aj vo forme odkazu na hore uvedený súbor dostupný na ceste:
`/Library/Frameworks/eToken.framework/Versions/A/libIDPrimePKCS11.dylib`

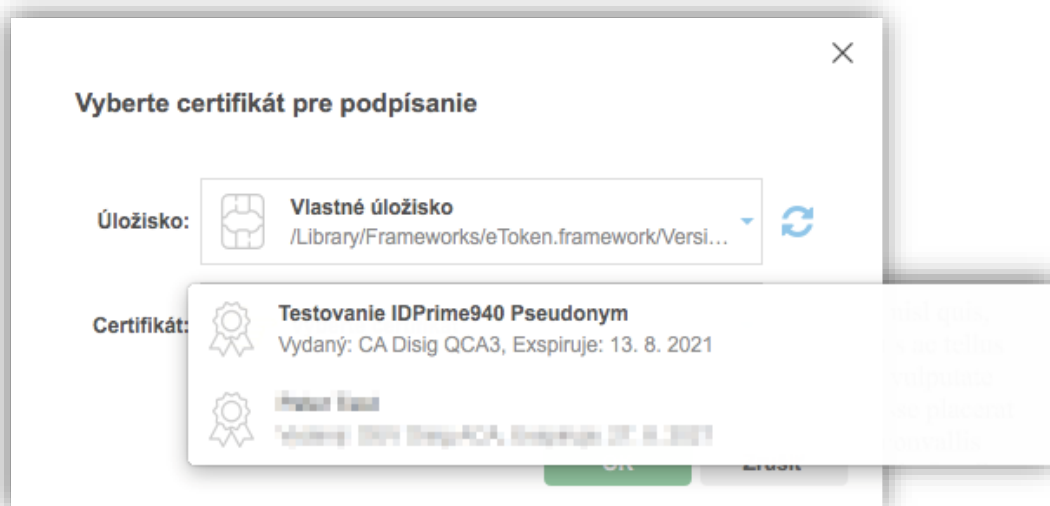
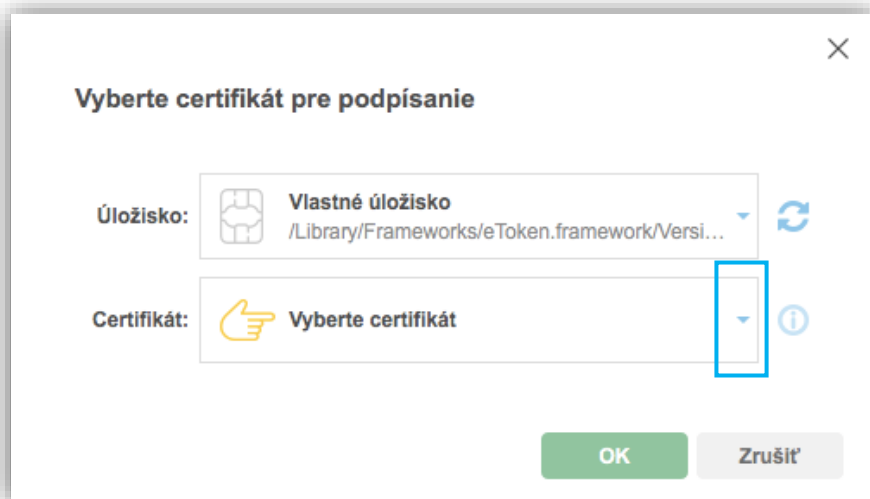
POZNÁMKA:

Operačný systém macOS neumožňuje svojim používateľom jednoducho vstúpiť do vnútra niektorých špeciálnych adresárov ako sú napríklad jednotlivé aplikácie nachádzajúce sa v adresári „/Applications“ alebo adresár „/usr“.

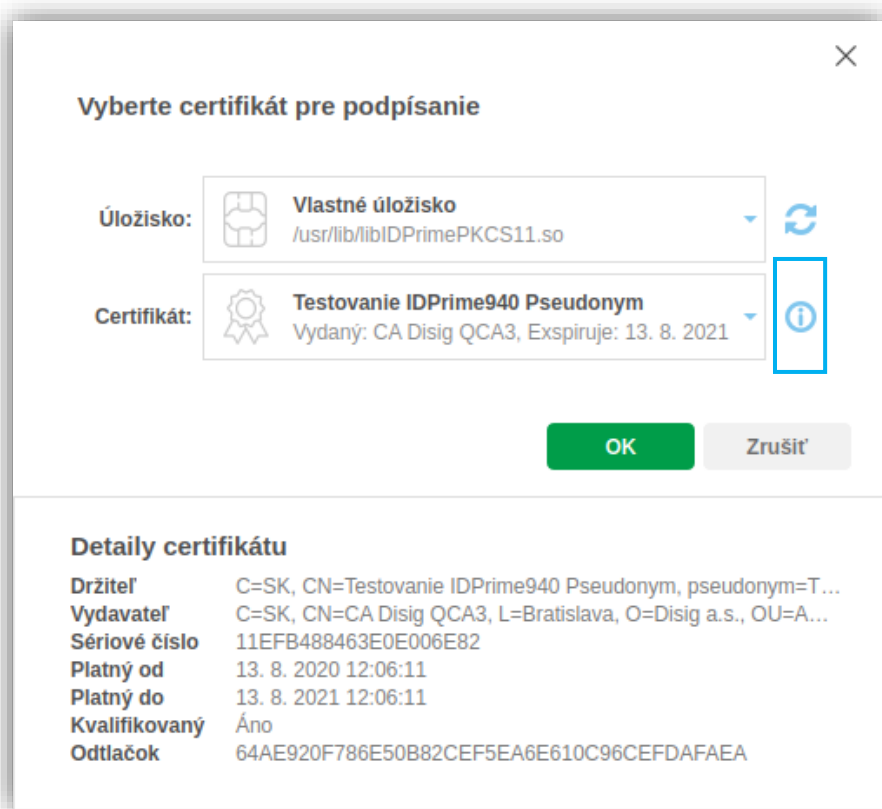
Pokiaľ je v dialógu zobrazenom aplikáciou Disig Web Signer pri výbere vlastnej PKCS#11 knižnice potrebné vstúpiť do takéhoto adresára, je možné uvedené obmedzenie operačného systému obísť použitím klávesovej skratky "Shift-Command-G" a následným priamym zadaním cesty k požadovanému adresáru.

3. Certifikát

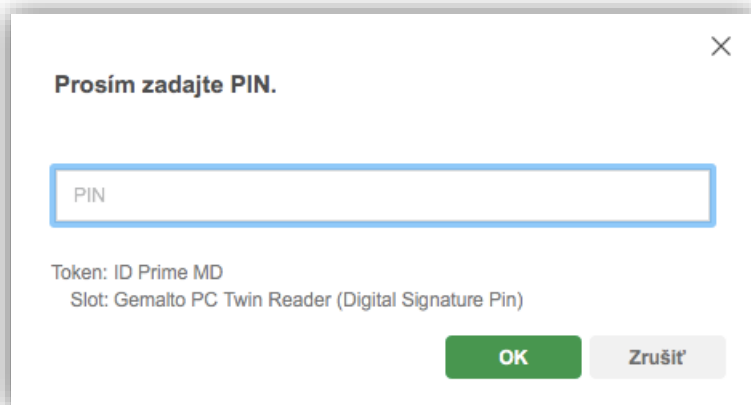
Zo zoznamu certifikátov uložených na kvalifikovanom zariadení vyberte certifikát pre vytvorenie kvalifikovaného elektronického podpisu.



4. Detailné informácie o zvolenom certifikáte získate po kliknutí na ikonu „i“. Výber zvoleného certifikátu potvrdíte stlačením OK.



5. Po výbere podpisového certifikátu pre vytvorenie kvalifikovaného elektronického podpisu zadajte ako hodnotu pre PIN kód Gemalto karty Vaše Heslo ku karte Gemalto.



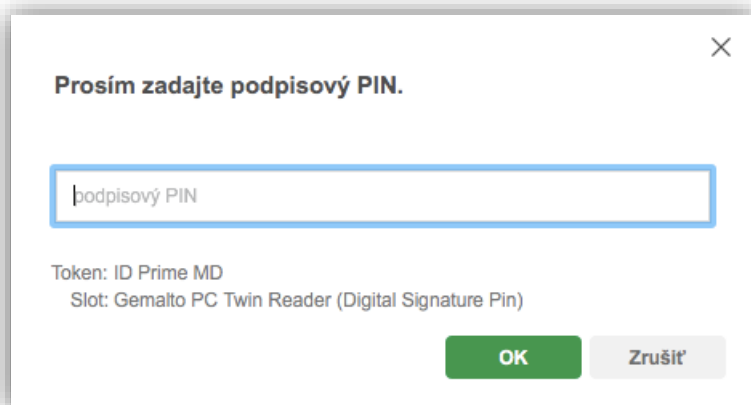
Prosím zadajte PIN.

PIN

Token: ID Prime MD
Slot: Gemalto PC Twin Reader (Digital Signature Pin)

OK Zrušiť

6. Pre použitie zvoleného certifikátu na úkon elektronického podpisu sa prosím identifikujte pomocou Podpisového PIN-u pre elektronický podpis Gemalto karty.



Prosím zadajte podpisový PIN.

podpisový PIN

Token: ID Prime MD
Slot: Gemalto PC Twin Reader (Digital Signature Pin)

OK Zrušiť

Po úspešnej autentifikácii zadaním podpisového PIN-u aplikácia Váš dokument elektronicky podpíše.



✓ Dokument bol úspešne podpísaný

OK