

Instructiuni de instalare a semnaturii digitale DIGISIGN pe Mac OS X 10.10 (Yosemite). Aceleasi instructiuni se pot folosi si pentru MAC OS X 10.11 (El Capitan).

Important: nu conectati tokenul inainte de instalare!

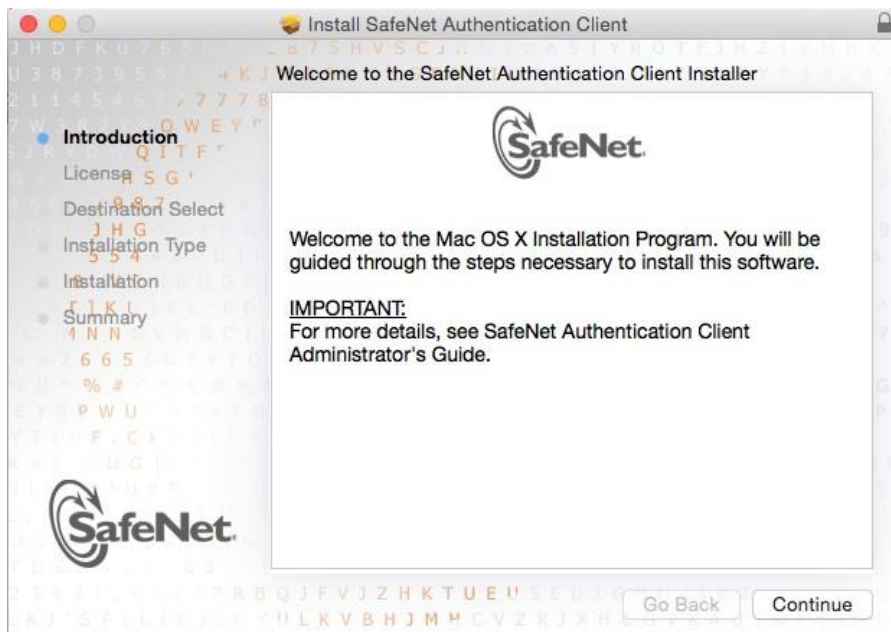
Pasul 1 – se descarca driverul token-ului. Ultima versiune de driver la momentul conceperii acestui ghid se afla la adresa:

ftp://ftp.ines.ro/test/DigiSign/Driver_eToken/macintosh/SafeNetAuthenticationClient.9.1.2.0.dmg

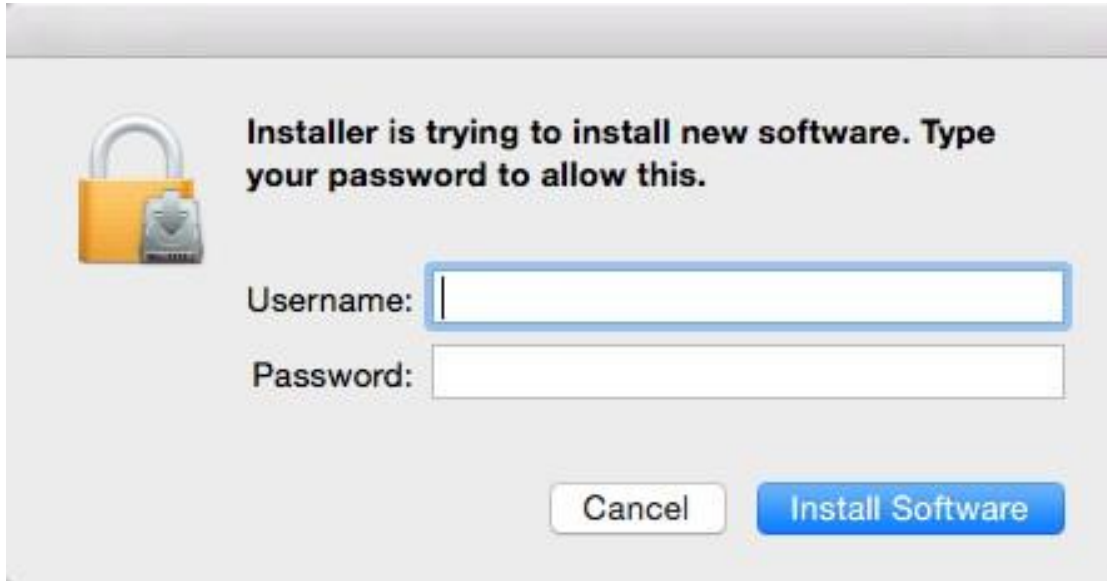
Pasul 2 – Se deschide fisierul DMG descarcat mai sus si se lanseaza “SafeNet Authentication Client 9.1 .pkg”:



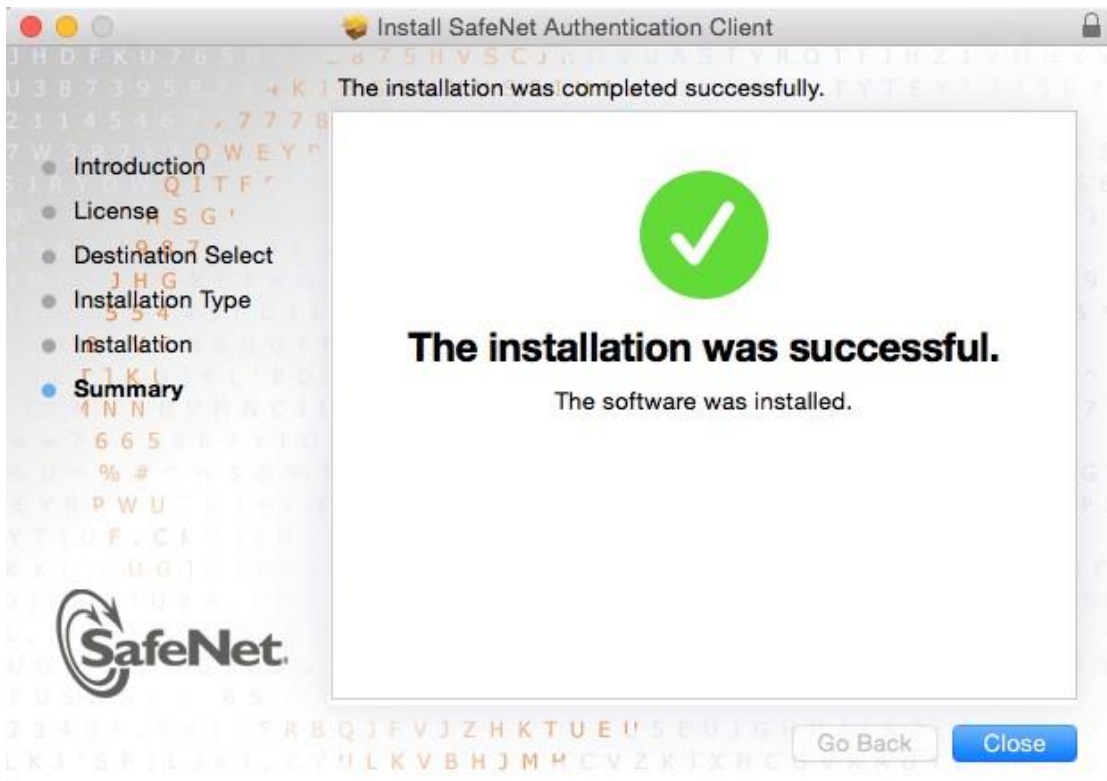
Se urmeaza pasii de instalare pana la finalizare:



La un moment dat se va cere parola pentru a continua:



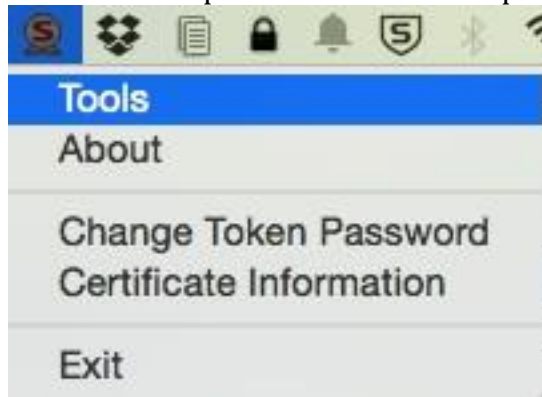
Se introduce userul si parola, apoi click pe "Install Software". In curand instalarea va fi finalizata:



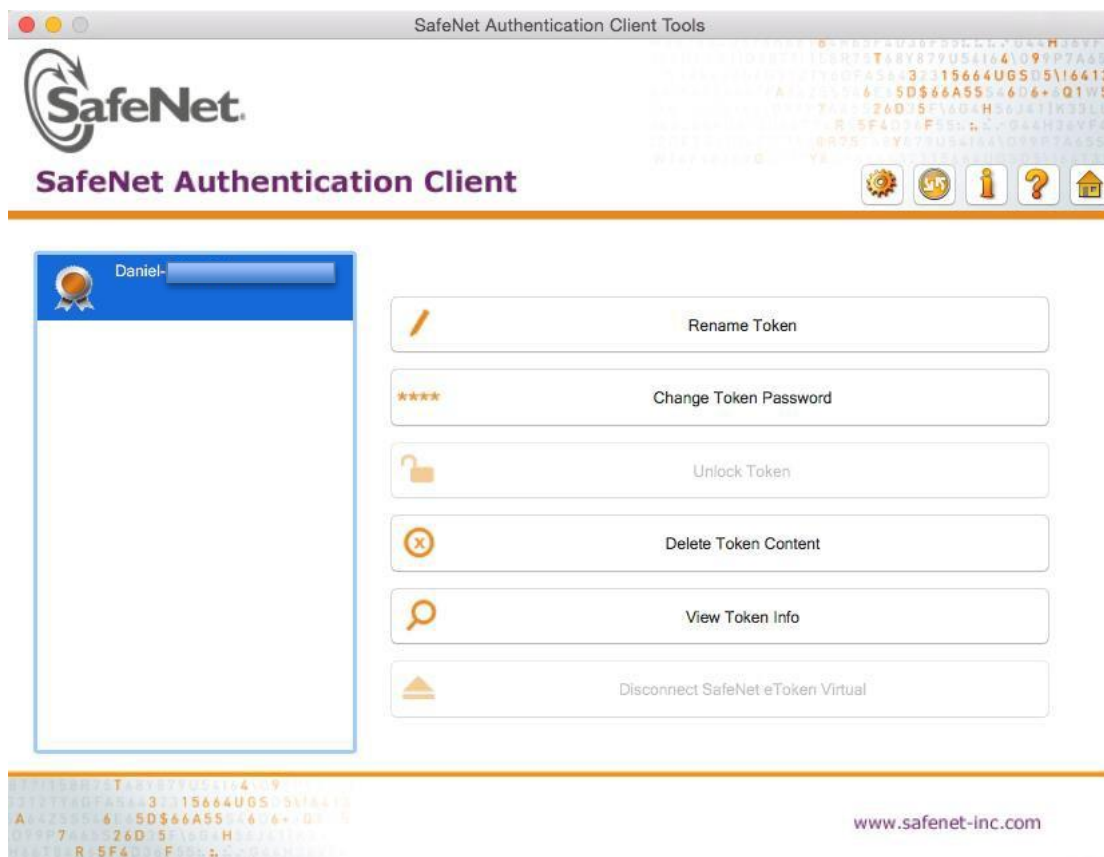
In bara de instrumente apare iconita specifica software-ului pentru token:



Pasul 3 – se conectează tokenul la unul dintre porturile USB, apoi click pe iconița menționată la pasul anterior și click pe “Tools”:



Ar trebui să apară informațiile despre certificat:

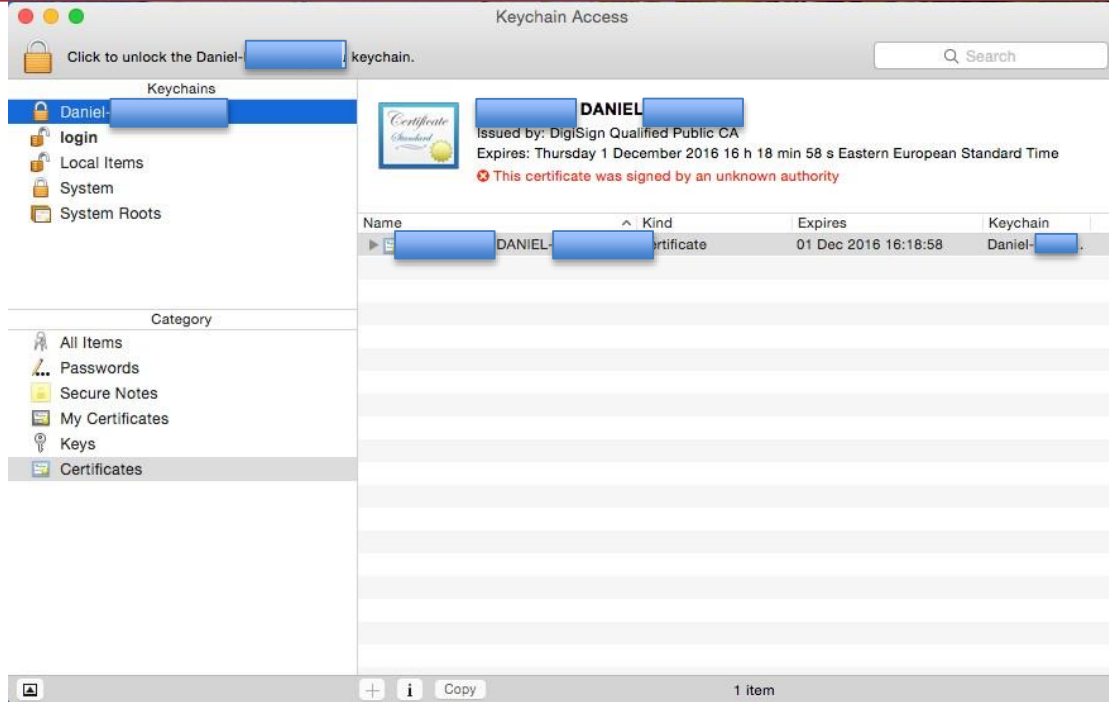


Pasul 4 – Se restartează computerul (fără restart nu se va putea folosi certificatul!!)

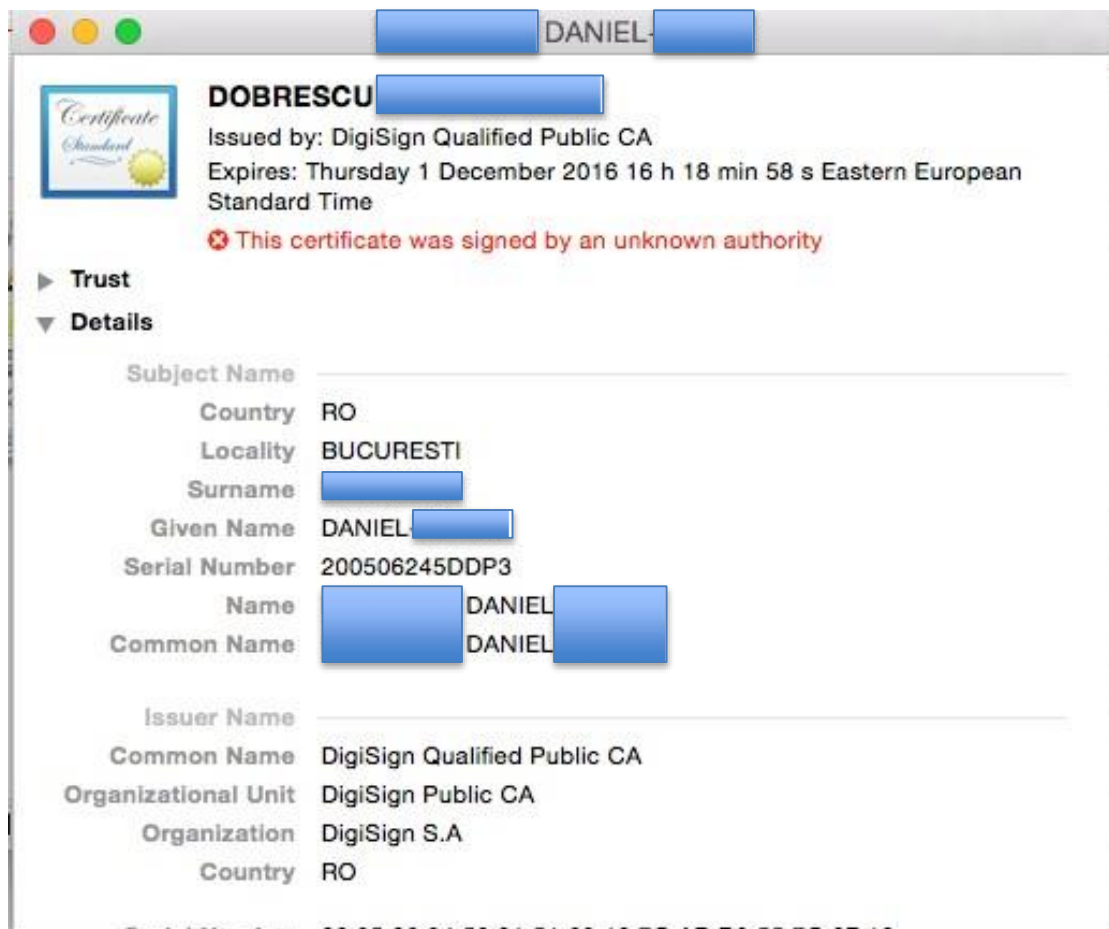
Pasul 5 – După restart se deschide aplicația “Keychain Access”, care se găsește în Applications -> Utilities -> Keychain Access. În lista din stânga sus ar trebui să apară certificatul cu numele pe care este emis (primul de sus).

Atentie! În cazul în care nu apare numele deasupra opțiunii “login” e nevoie de un restart pentru finalizarea instalării certificatului!



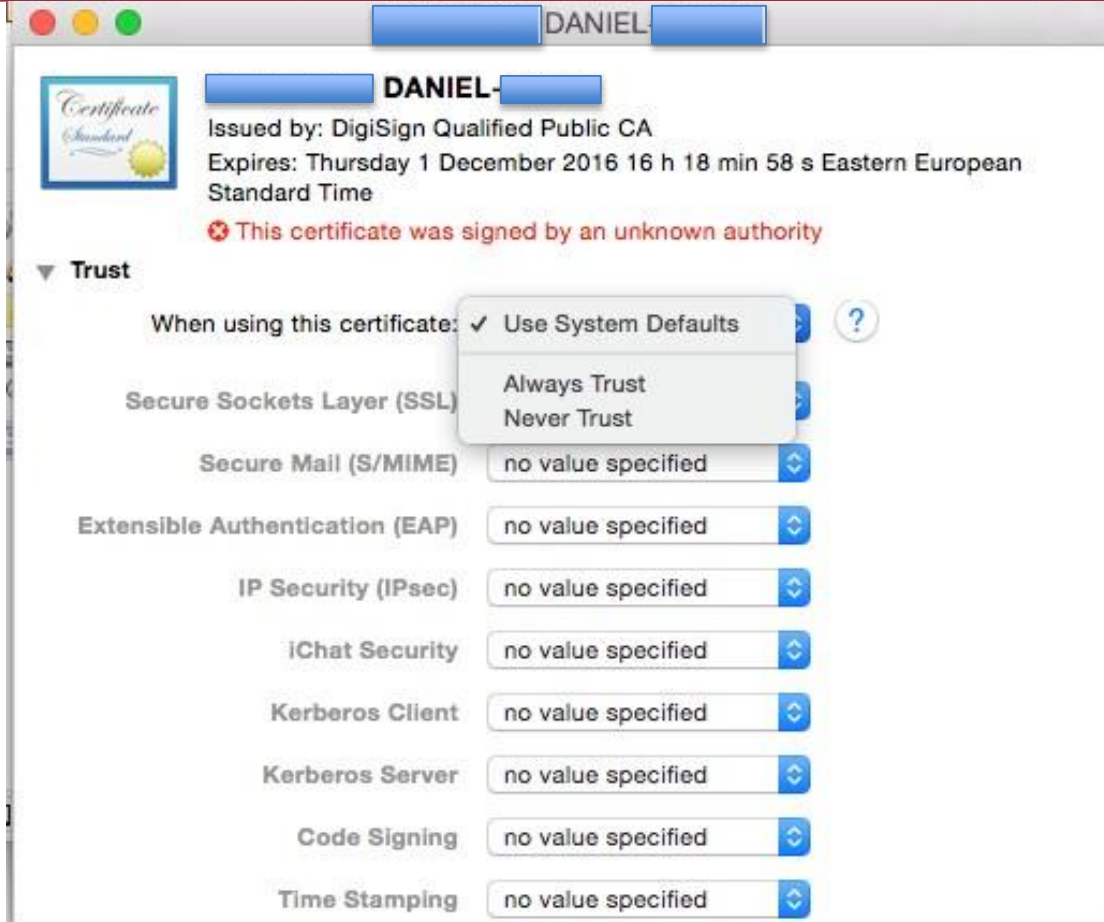


Se da dublu click pe certificat (in partea dreapta) si se deschide un ecran cu mai multe detalii.



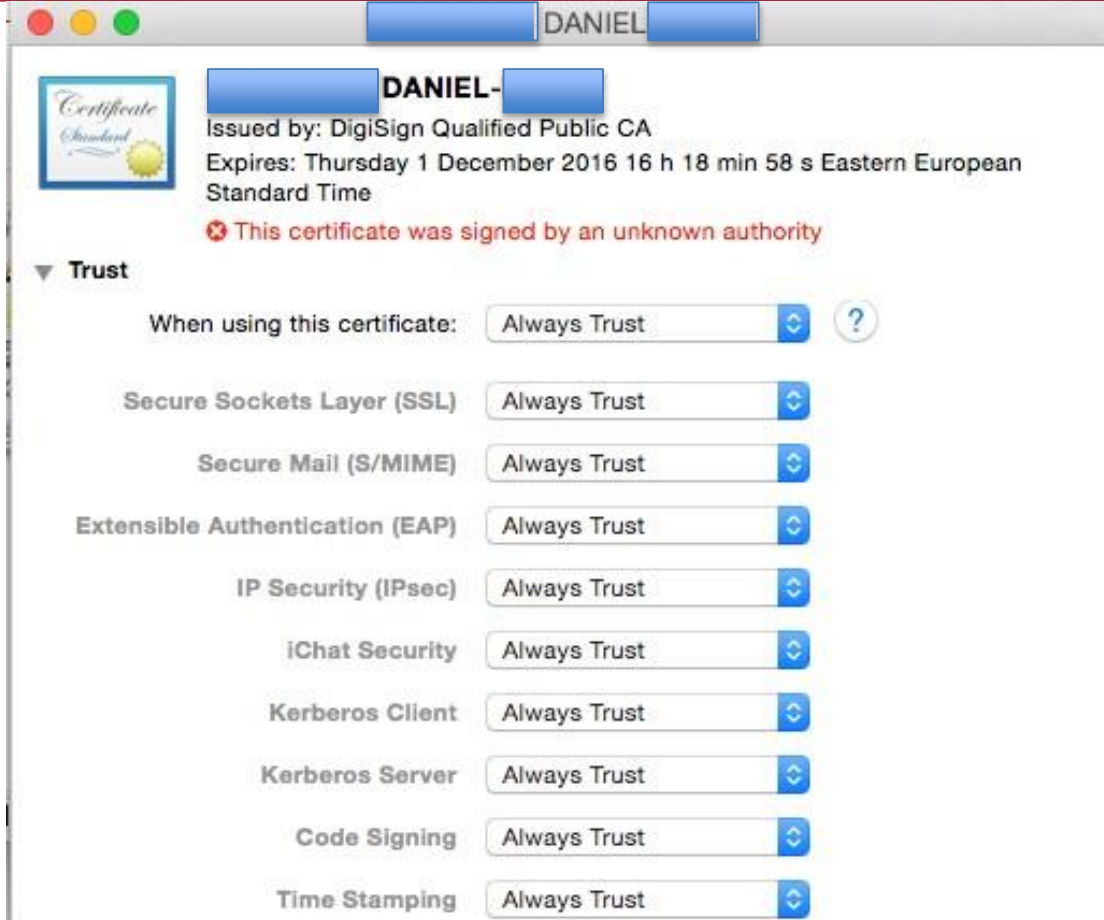
Se da click pe "Trust" si se va deschide un nou set de optiuni. De la prima optiune "When using this certificate" se alege: "Always trust":



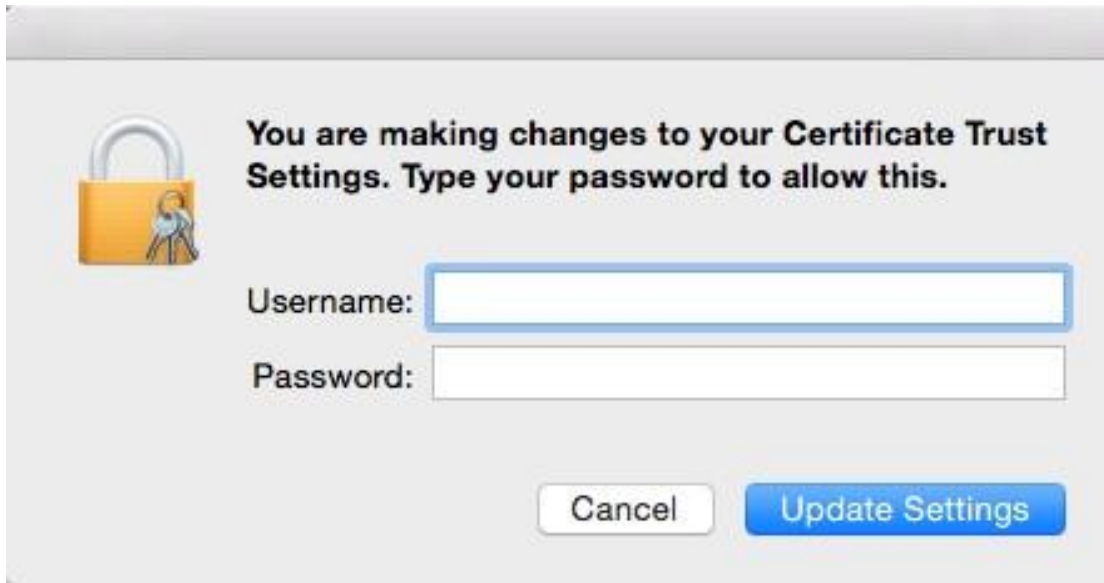


Toate optiunile se vor transforma in "Always trust":



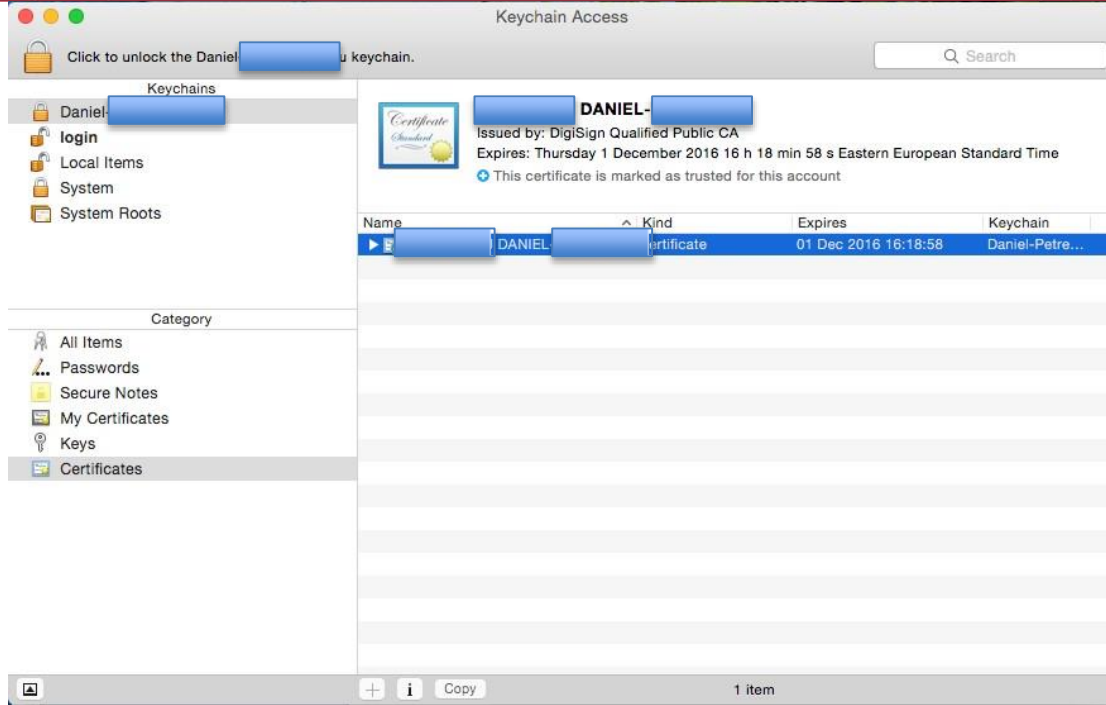


Se inchide fereastra de pe X din stanga sus, moment in care se cere parola:



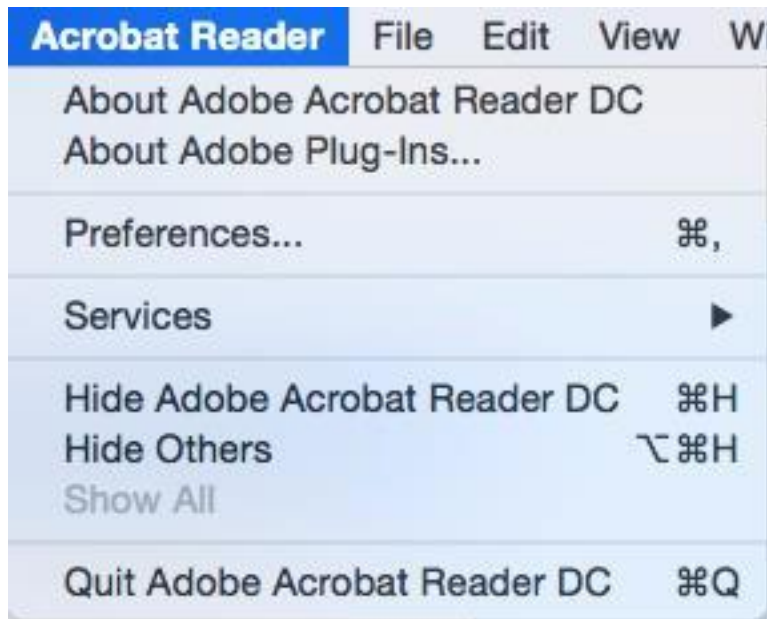
Se introduce user + parola, apoi click pe "Update Settings". Acum certificatul nu va mai avea un X rosu in dreptul lui, ci un + albastru:





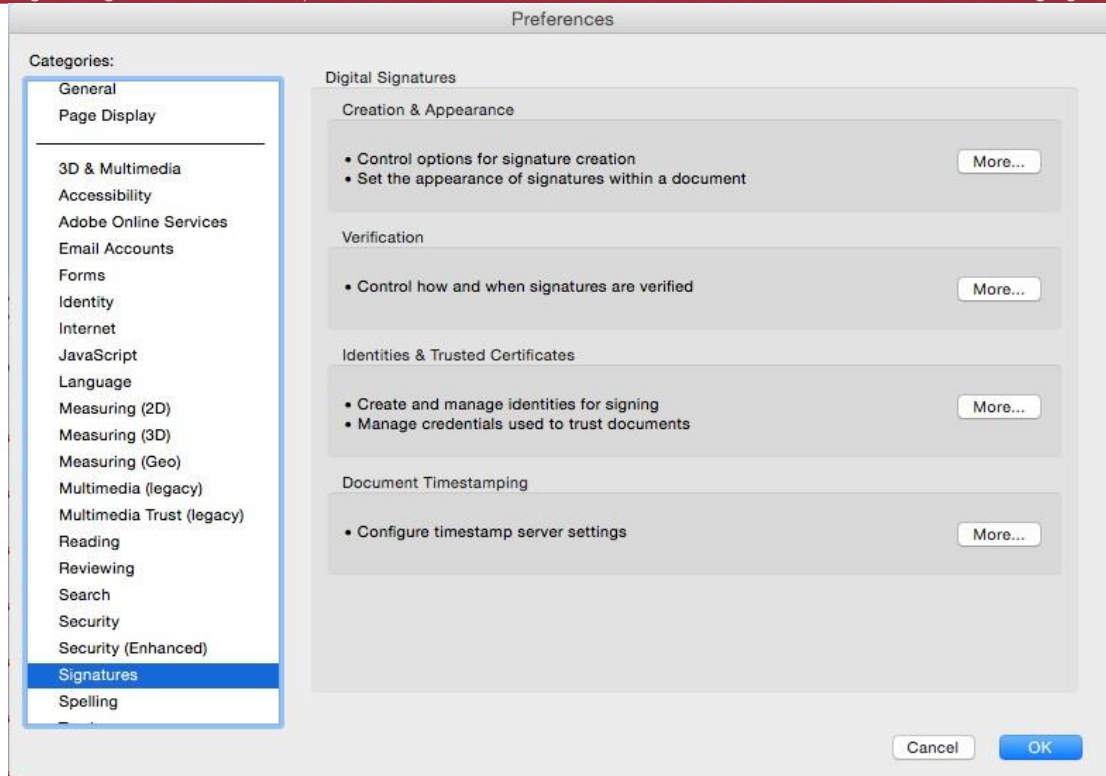
In acest moment poate fi folosit impreuna cu Adobe Reader.

Pasul 6 – Deschidem Adobe Acrobat Reader DC sau Adobe Reader si deschidem preferences:

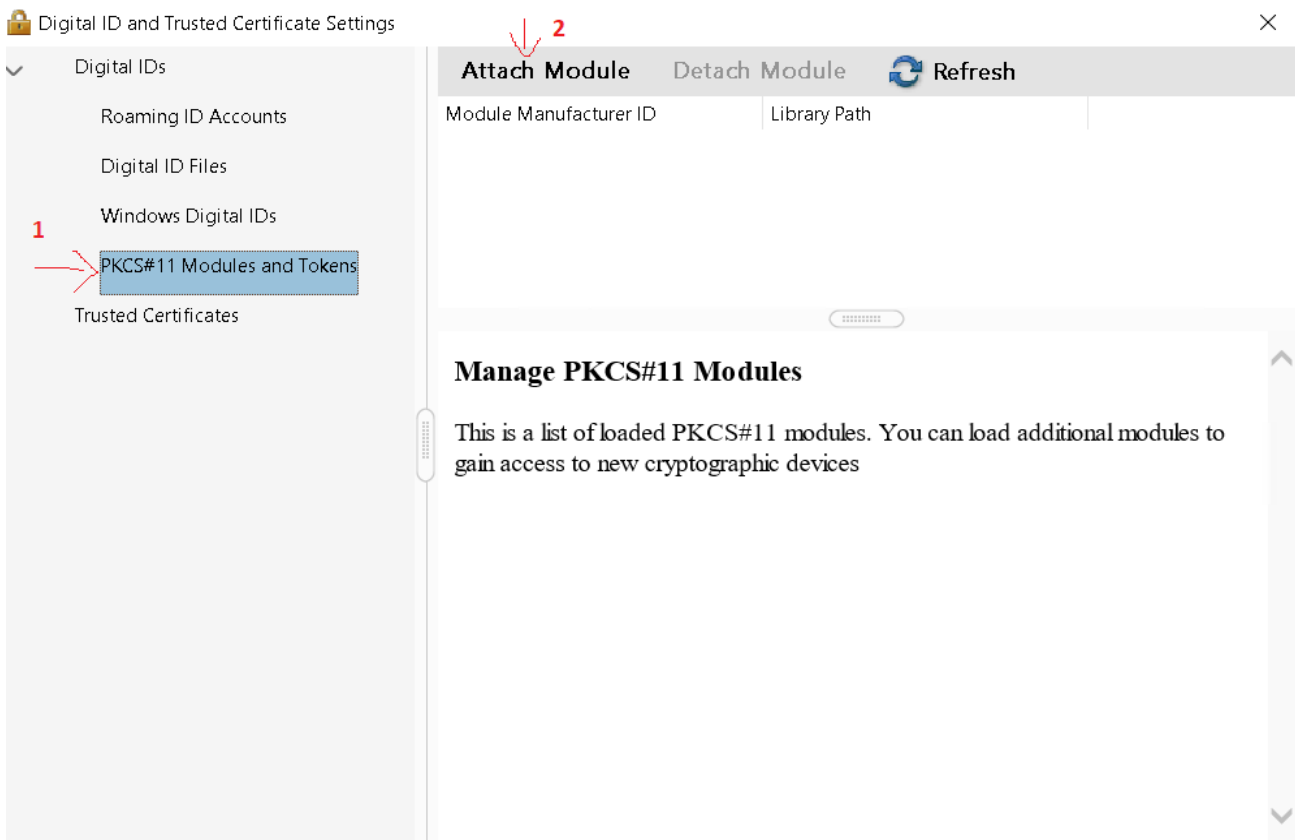


Se alege din meniul din stanga "Singatures", apoi in dreapta se da click pe butonul "More" din dreptul optiunii "Identity & Trusted Certificates":





Selectati PKCS#11 Modules and Tokens -> Attach Module

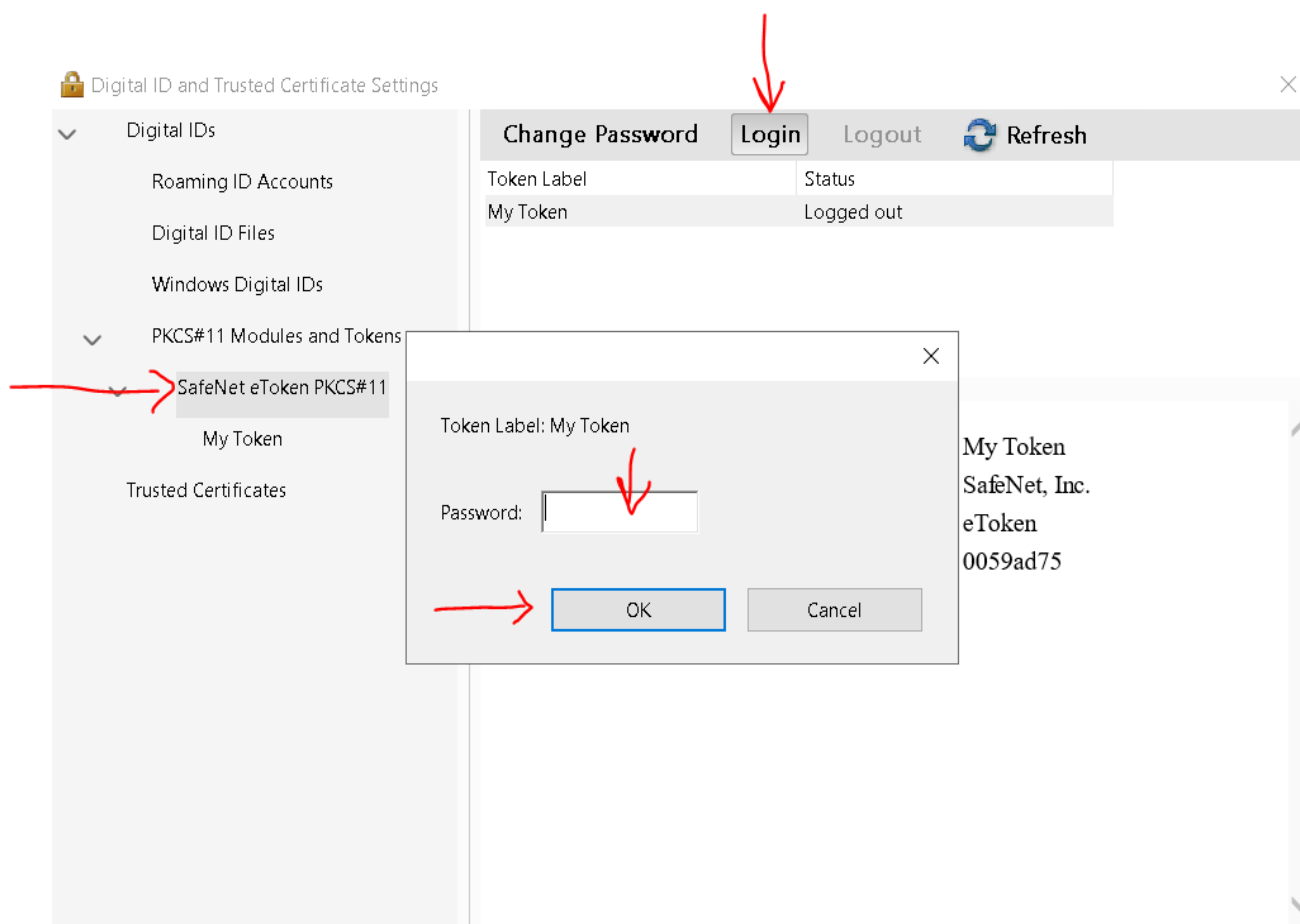


In casuta introduceti calea spre libraria pkcs11:

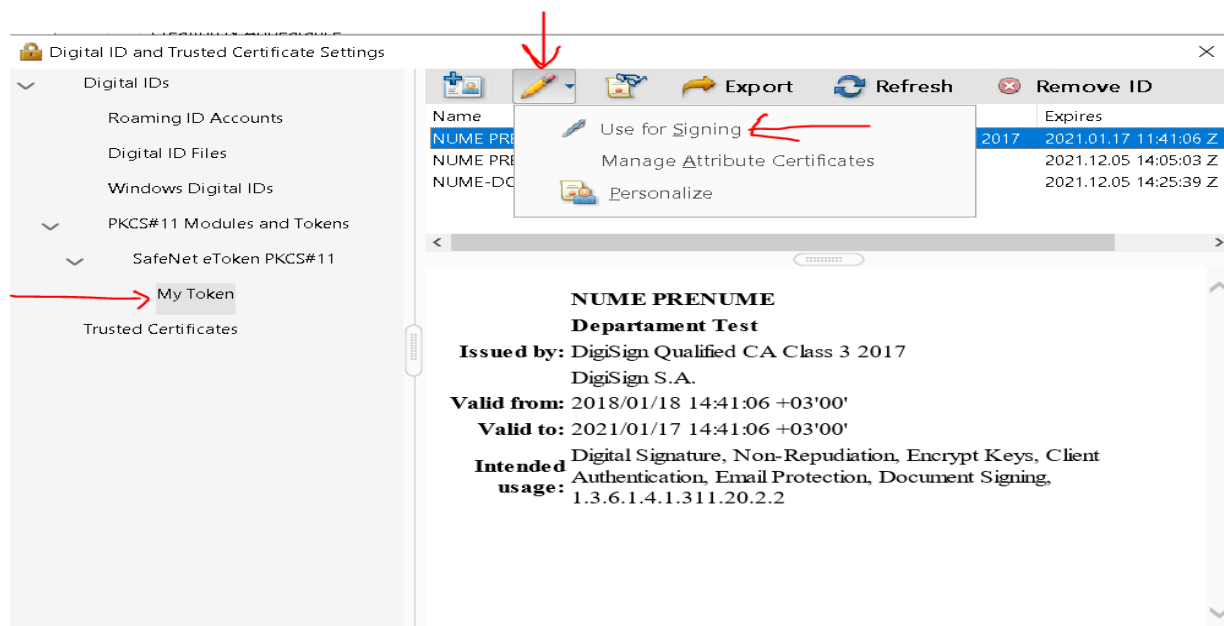
/Library/Frameworks/eToken.framework/Versions/A/libikeyTokenEngine.dylib si apasati OK.



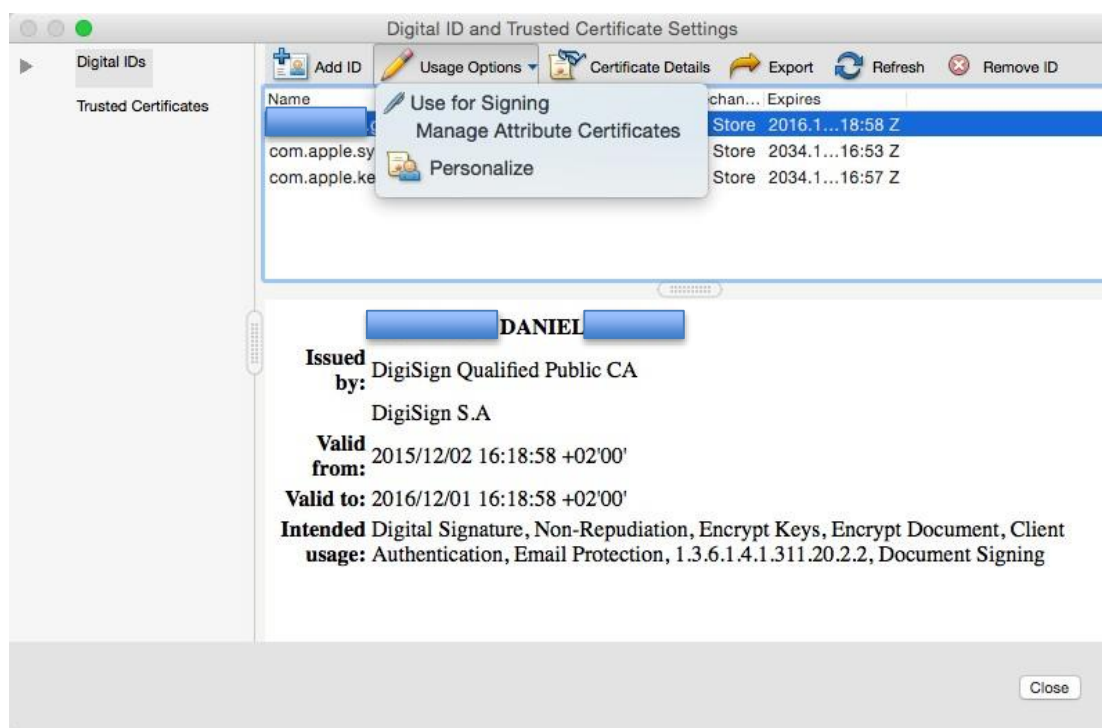
Selectati Safenet eToken PLKCS#11 -> Login. Introduceti parola eTokenului si apasati OK.



Dupa ce va logati pe eToken, selectati numele eTokenului din partea stanga, iar in partea din sus selectati optiunea de "Use for signing":



Pasul 7 – Deschidem un document PDF cu Adobe Acrobat Reader DC. Se da click pe “Tools” apoi pe “Certificates”:



Se selecteaza certificatul si din meniul “Usage Options” se alege “Use for Signing”. Apoi se da click pe “Certificate Details”:




Certificate Viewer

This dialog allows you to view the details of a certificate and its entire issuance chain. The details correspond to the selected entry.

Show all certification paths found

DANIEL-P

Summary Details Revocation Trust Policies Legal Notice

 DANIEL [redacted]@gmail.com>


Issued by: DigiSign Qualified Public CA
DigiSign S.A

Valid from: 2015/12/02 16:18:58 +02'00'

Valid to: 2016/12/01 16:18:58 +02'00'

Intended usage: Digital Signature, Non-Repudiation, Encrypt Keys, Encrypt Document, Client Authentication, Email Protection, 1.3.6.1.4.1.311.20.2.2, Document Signing

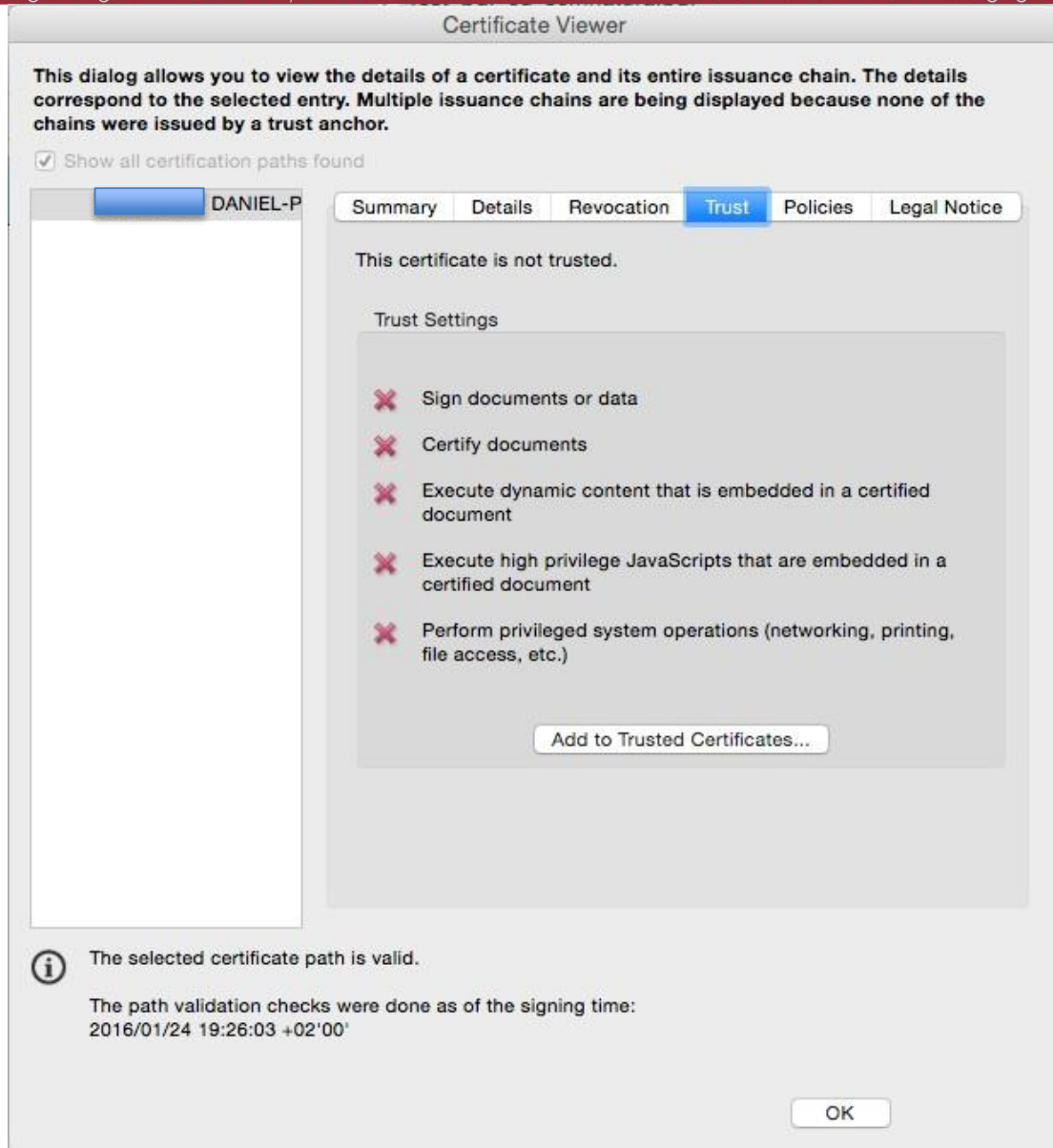
Export...

 The selected certificate path is valid.
The path validation checks were done as of 2016/01/24 20:16:52 +02'00'

OK

Se alege din meniul de sus "Trust":





Apoi click pe "Add to Trusted Certificates...":



Import Contact Settings

Certificate Details

Subject: [REDACTED] DANIEL [REDACTED]@gmail.com>
Issuer: DigiSign Qualified Public CA
Usage: Digital Signature, Non-Repudiation, Encrypt Keys, Encrypt Document
Expiration: 01/12/16 16:18:58

Trust

A certificate used to sign a document must either be designated as a trust anchor or chain up to a trust anchor in order for signature validation to succeed. Revocation checking is not performed on or above a trust anchor.

Use this certificate as a trusted root

If signature validation succeeds, trust this certificate for:

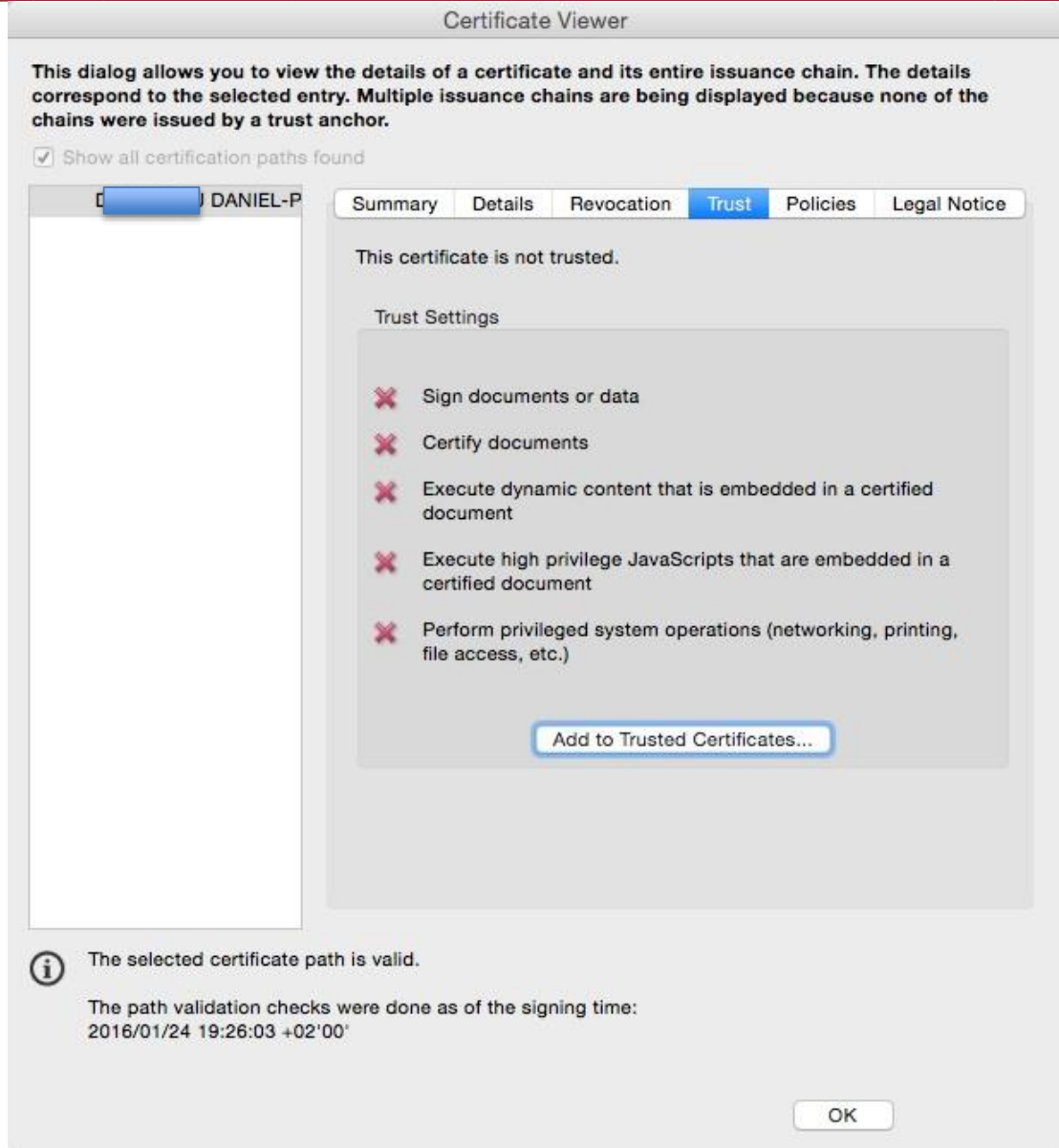
- Signed documents or data
- Certified documents
 - Dynamic content
 - Embedded high privilege JavaScript
 - Privileged system operations (networking, printing, file access)

Help **Cancel** **OK**

Se verifica sa fie bifat "Use this certificate as a trusted root" si "Signed documents or data", apoi click pe OK.

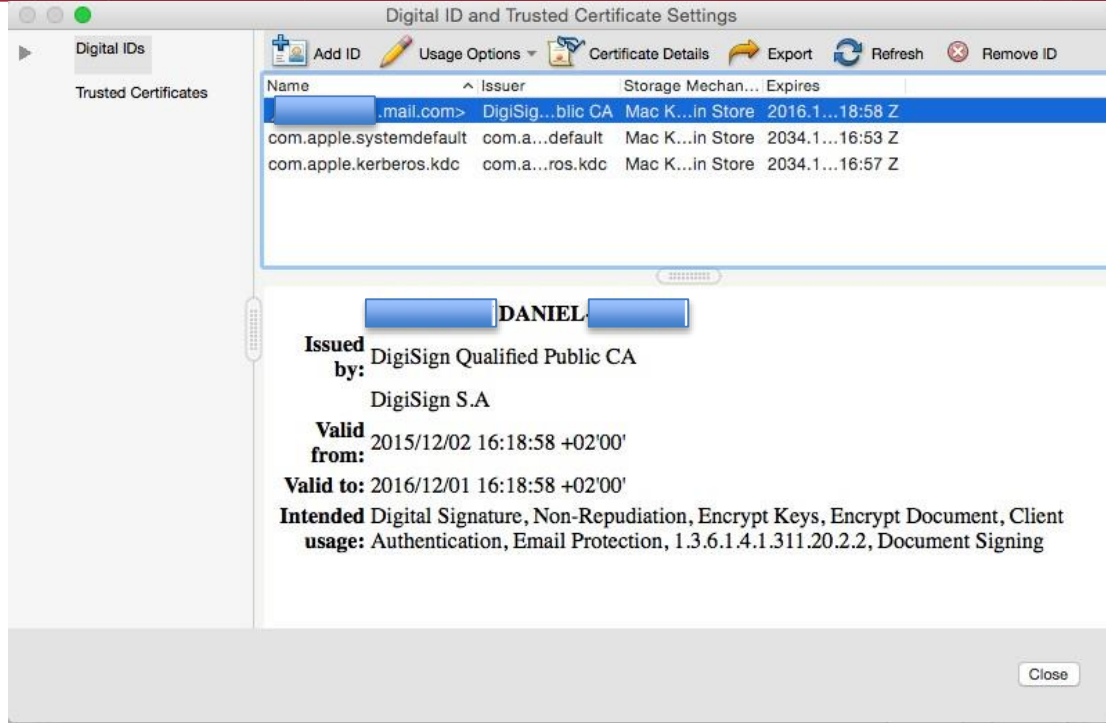
Click pe OK pe ecranul urmator:



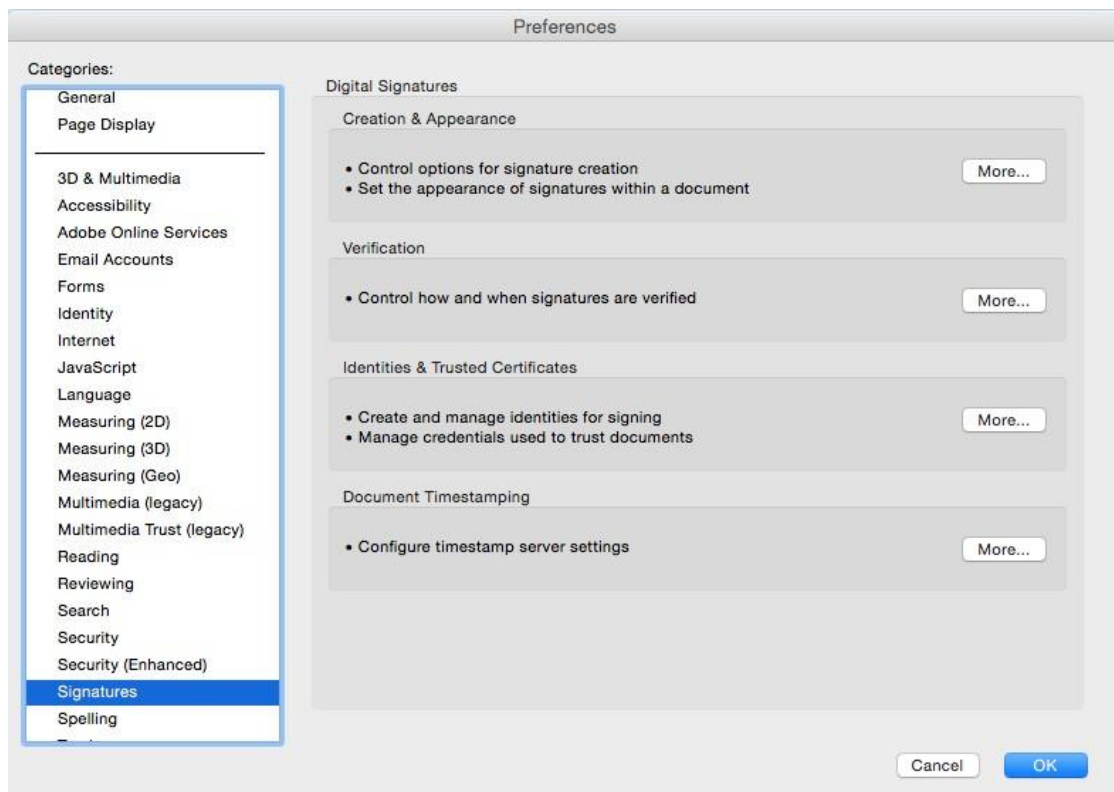


Din nou click pe OK, dupa care click pe Close in ecranul "Digital ID and Trusted Certificate Settings:



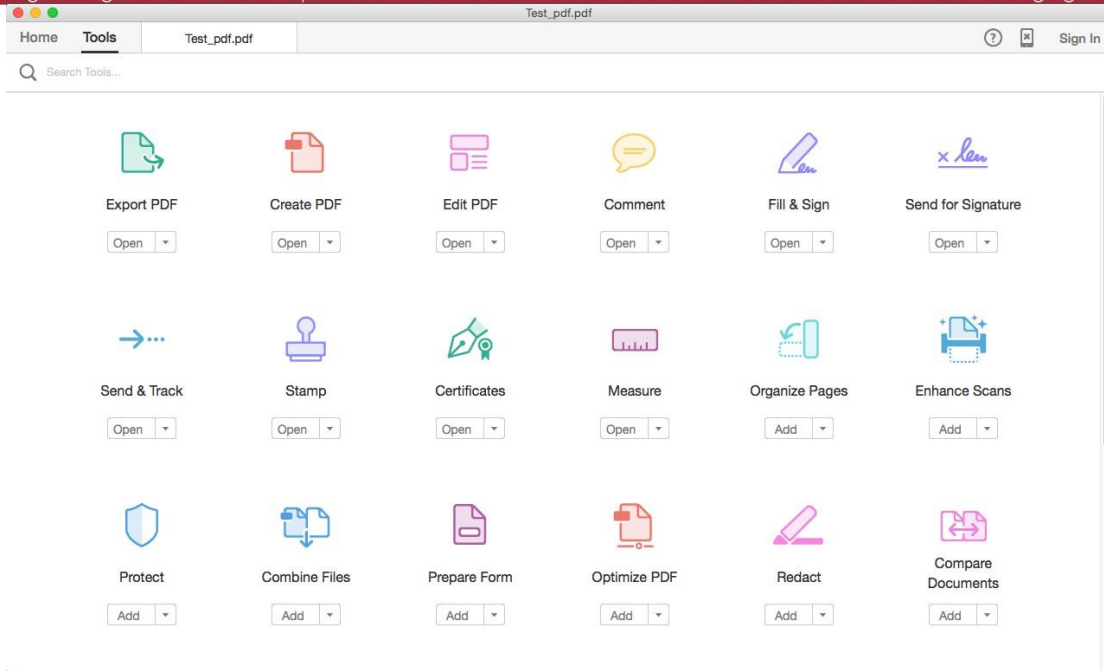


Apoi click pe OK pentru a inchide Adobe Preferences:

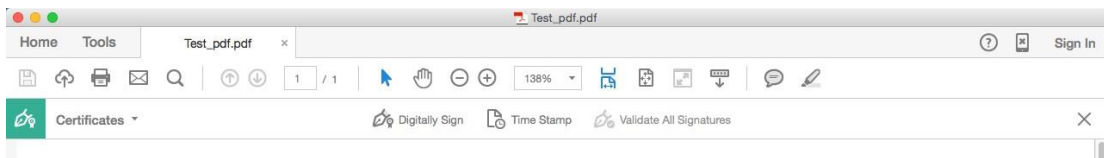


Acum se poate deschide un document PDF pentru a fi semnat. In Adobe Acrobat Reader DC se da click pe "Tools", apoi pe "Certificates":



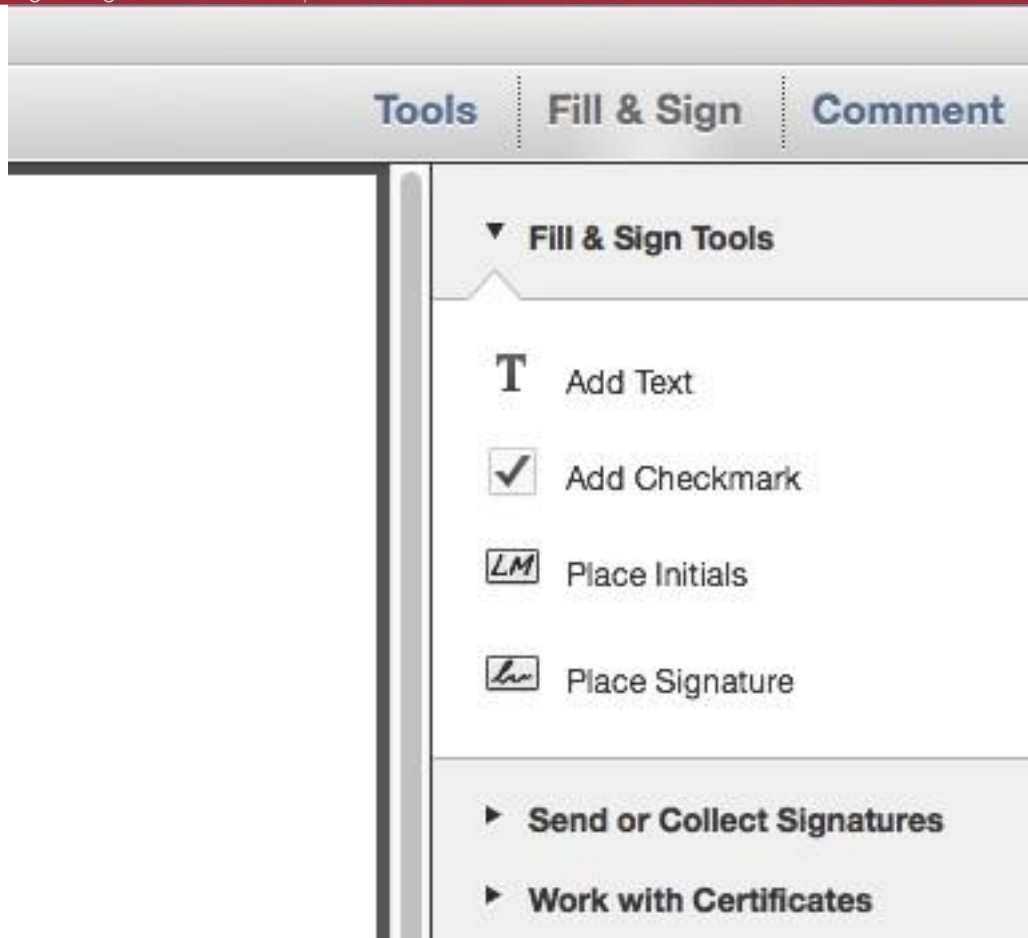


Din meniul care apare se da click pe “Digitally Sign”:



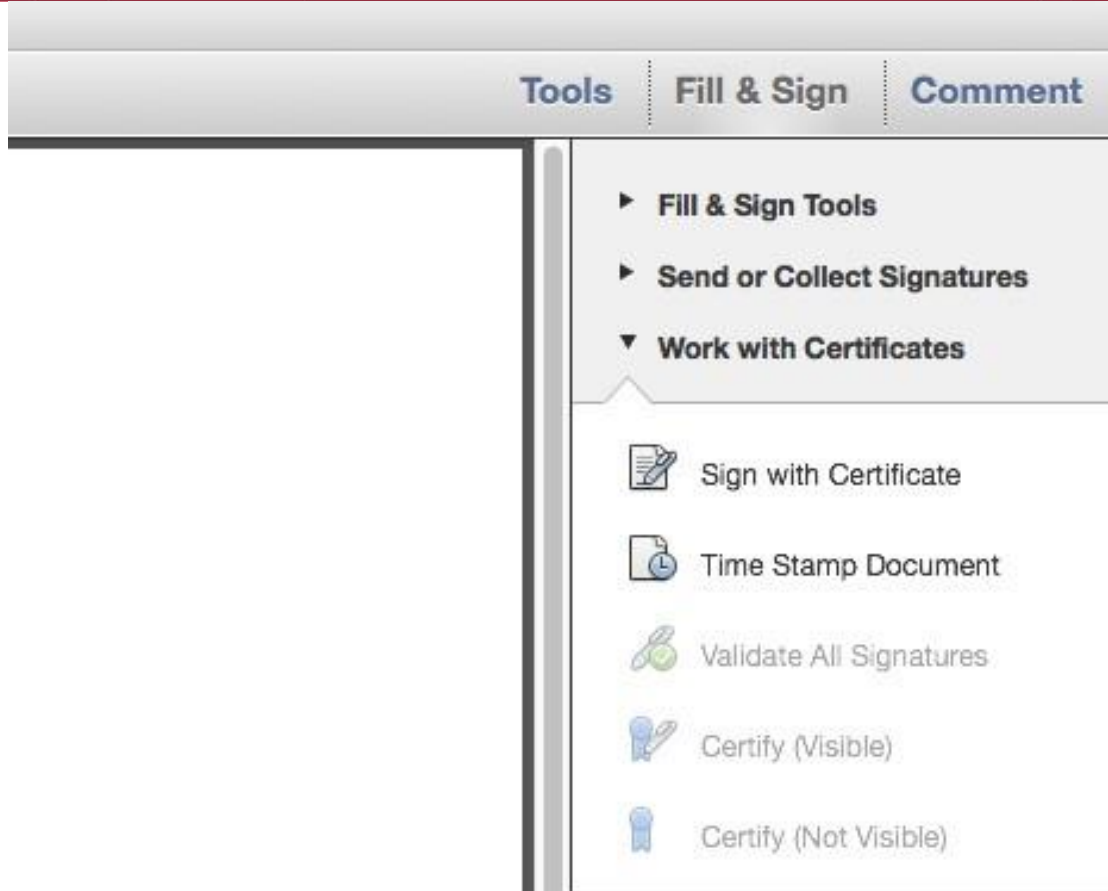
Pentru Adobe Reader se alege din meniul din dreapta sus “Fill & Sign”, apoi click pe “Work with Certificates”:



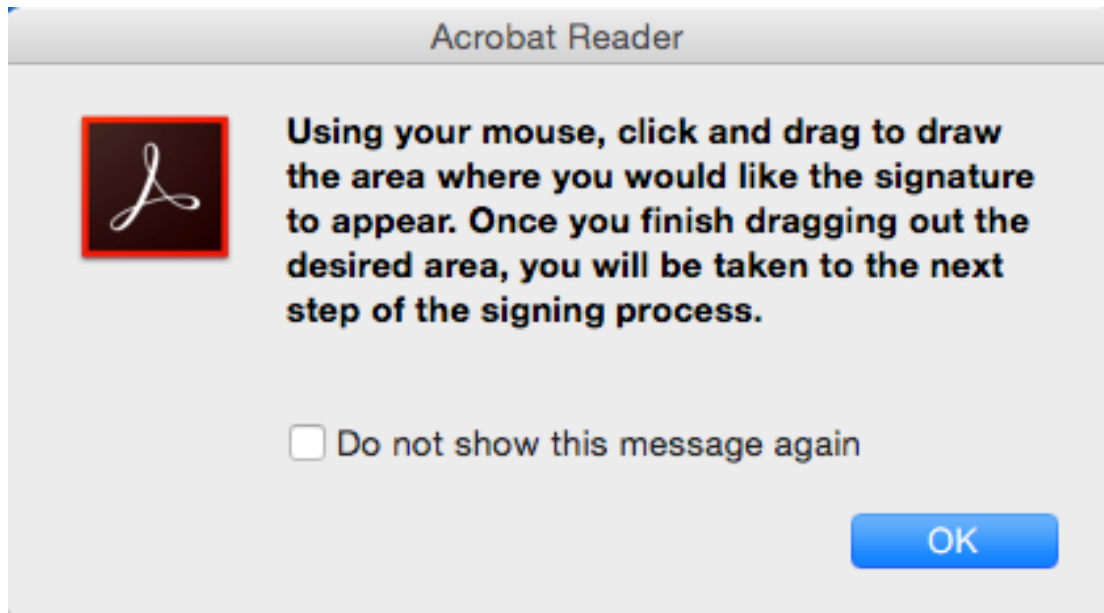


Apoi se da click pe "Sign with Certificate":





Apare un mesaj care solicita trasarea unui dreptunghi unde se va plasa semnatura electronica:



Dupa trasarea dreptunghiului apare confirmarea semnaturii:



Sign Document

Sign As: DANIEL- (DigiSign...)

Issued by: DigiSign Qualified Public CA [More Details](#)

Appearance: Standard Text


DANIEL- Digitally signed by DANIEL-
Date: 2016.01.24 19:05:41 +02'00'

Lock Document After Signing

Click Review to see if document content may affect signing [Review...](#)

[Help](#) [Cancel](#) [Sign](#)

Se da click pe "Sign" si se va solicita parola token-ului:

 **Adobe Acrobat Reader DC wants to use the "Daniel-" keychain.**

Please enter the keychain password.

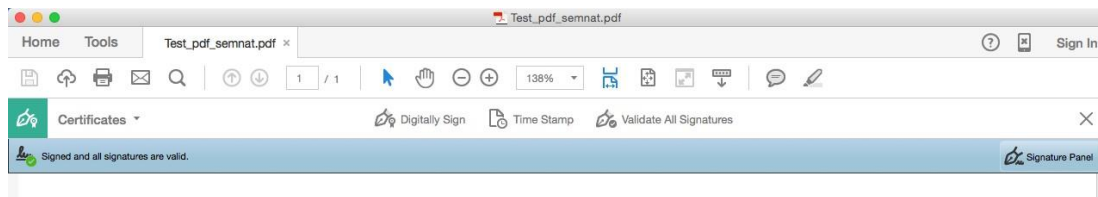
Password:

[?](#) [Cancel](#) [OK](#)

Se introduce parola primita impreuna cu token-ul si se da click pe "OK". Se va deschide o fereastră cu locatia in care sa se salveze documentul semnat digital.



Dupa ce salveaza documentul ar trebui sa apara in bara de sus mesajul "Signed and all signatures are valid":



IMPORTANT: pentru a putea mai multe documente este necesar urmatorul proces:

1. Se conecteaza token-ul
2. Se porneste Adobe Acrobat Reader DC si se semneaza documentul conform pasilor de mai sus
3. Se inchide Adobe Acrobat Reader DC (CMD+Q)
4. Se deconecteaza token-ul

Pasii 1-4 se repeta pentru fiecare document ce se doreste a fi semnat, altfel nu se va mai cere parola token-ului si nu se va putea completa procesul de semnare.

