ИНСТРУКЦИЯ ЗА РАБОТА С SAFENET AUTHENTICATION CLIENT

Операционна система macOS

Версия 10.15 и по висока

Съдържание

1. Преди инсталация на софтуер за работа с SafeNet Authentication Client 3
1.1 Преди инсталацията проверете версията на операционната система 3

2. Инсталиране на софтуер за работа с SafeNet Authentication Client 3
2.1 Инсталиране на софтуер за четец на смарт карти 3

2.2 Инсталиране на софтуер за работа със смарт карти - SafeNet Authentication Client 3

3. Смяна на PIN код 5

4. Отблокиране на PIN кода 5

5. Смяна на Администраторски ПУК / Administrator Password (PUK) 7

6. Изтриване токен / Delete Token Content 7

7. Допълнителни функционалности 7

8. Настройка на Mozilla Firefox за работа с SafeNet Authentication Client 7

9. Настройки за работа с Chrome и Safari 9
9.1 Изтеглете базов и оперативен сертификат 9

9.2 Инсталиране на базов и оперативен сертификат 9

10. Контакти 12

1. Преди инсталация на софтуер за работа с SafeNet Authentication Client

1.1 Преди инсталацията проверете версията на операционната система

Изтеглете и запазете на Вашия компютър архива с файла за инсталация като изберете линка **SafeNet Authentication Client инсталационен пакет v.10.8.x за macOS от v.10.14.x до v.12.x**

Разархивирайте съдържанието на файла. В пакета се съдържат необходимия потребителски софтуер за управление на устройството и смарт картата.

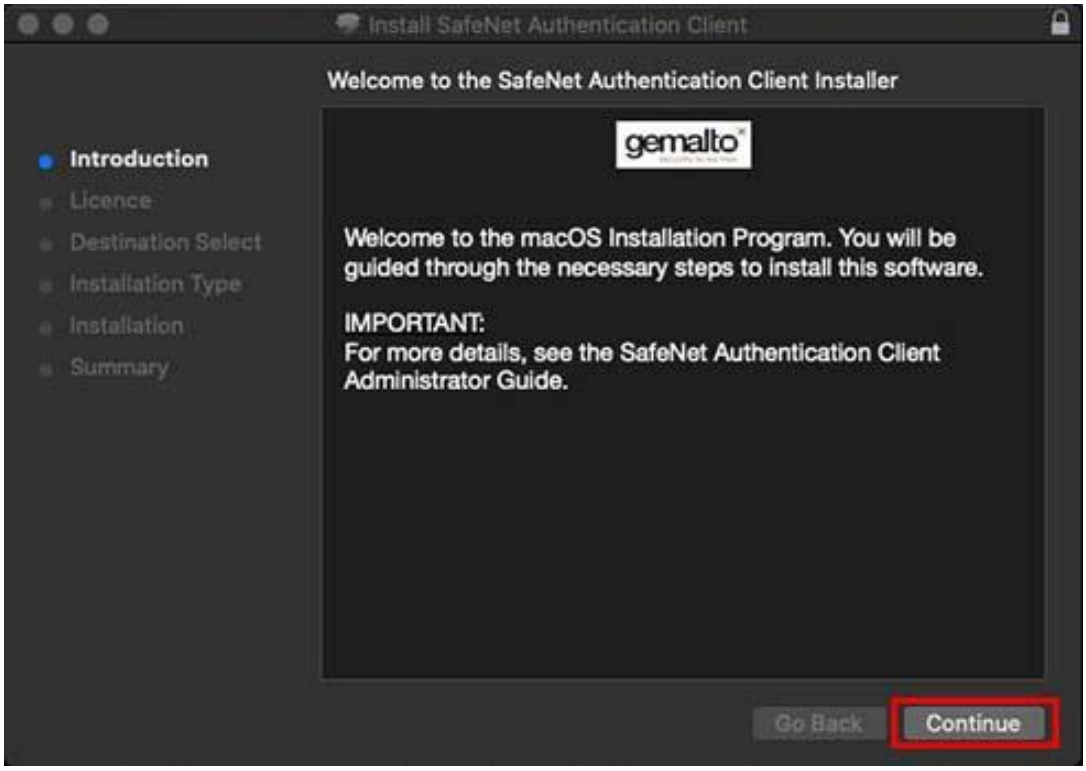
2. Инсталиране на софтуер за работа с SafeNet Authentication Client

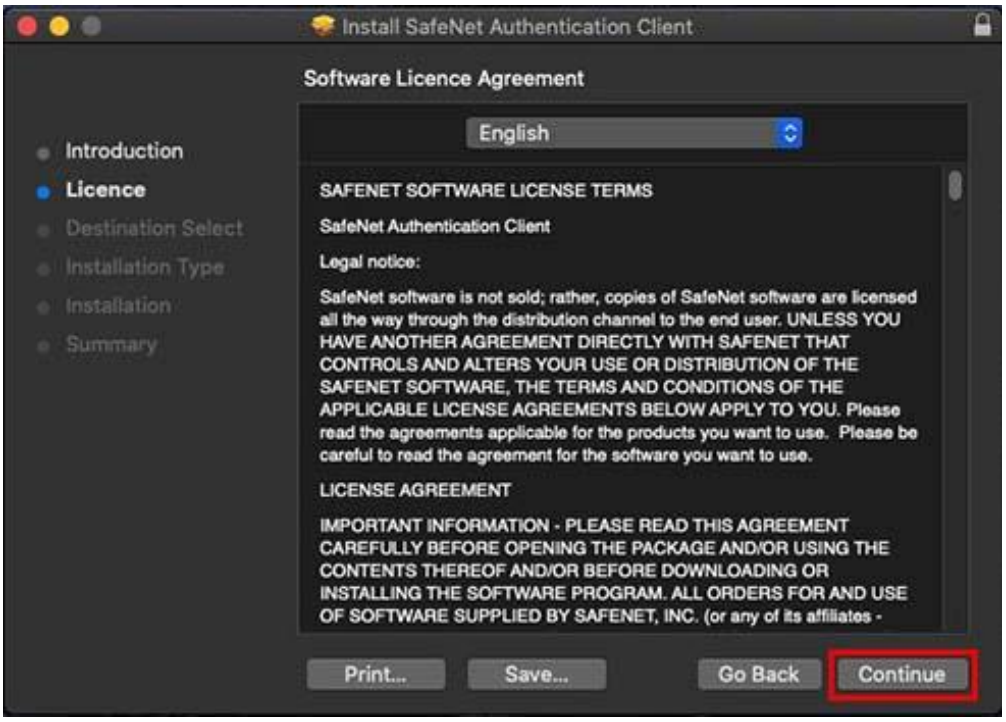
2.1 Инсталиране на софтуер за четец на смарт карти

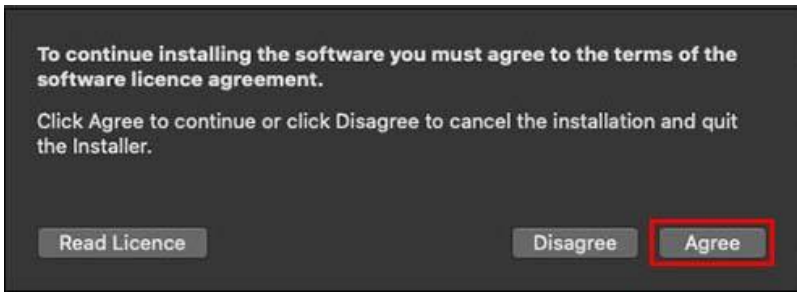
В разархивираната в т. 1.1 папка, от директория **Circle_Mac_Installer_v2.x.x** стартирайте файла „**abcccid_installer-2.x.x.dmg**“ и от монтираният имидж стартирайте файла „**abcccid_installer.pkg**“ и следвайте „стъпките“ по подразбиране на инсталатора.

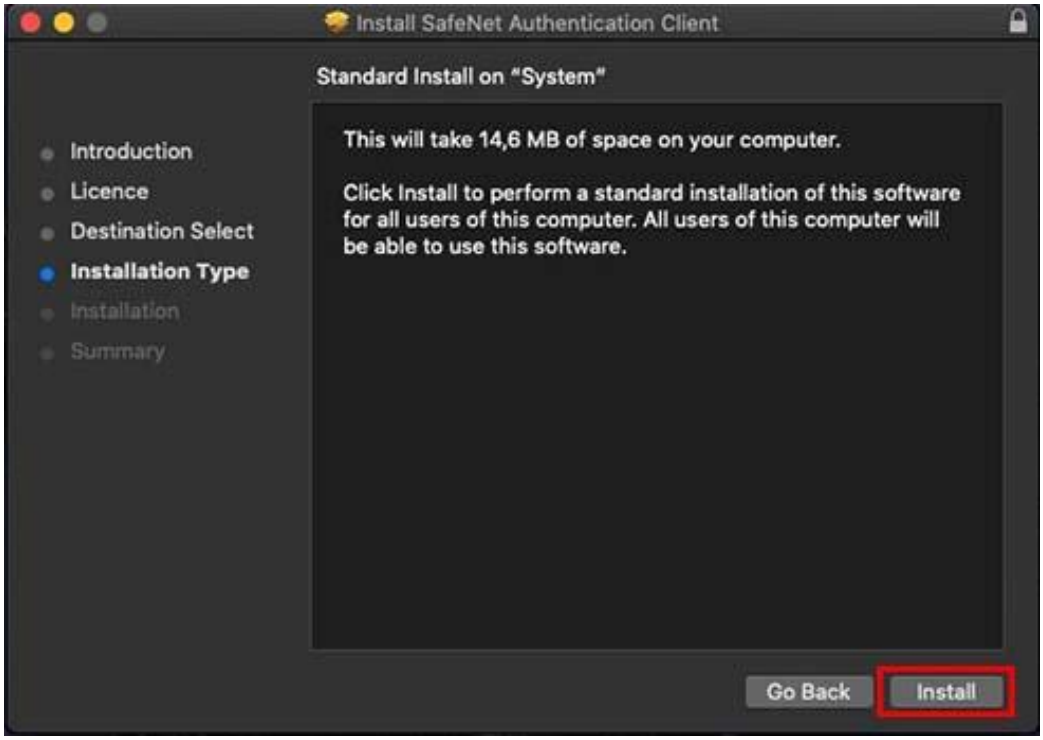
2.2 Инсталиране на софтуер за работа със смарт карти - SafeNet Authentication Client

В разархивираната в т. 1.1 папка стартирайте имидж файла **SafeNetAuthenticationClient_x.x.x.dmg** и след неговото отваряне, стартирайте **SafeNet Authentication Client 10.x.x.pkg** и **следвайте стъпките** по подразбиране**. След като инсталирате, рестартирайте macOS.**




Install SafeNet Authentication Client
Software Licence Agreement
English
Introduction
Licence
Destination Select
Installation Type
Installation
Summary
SAFENET SOFTWARE LICENSE TERMS
SafeNet Authentication Client
Legal notice:
SafeNet software is not sold; rather, copies of SafeNet software are licensed all the way through the distribution channel to the end user. UNLESS YOU HAVE ANOTHER AGREEMENT DIRECTLY WITH SAFENET THAT CONTROLS AND ALTERS YOUR USE OR DISTRIBUTION OF THE SAFENET SOFTWARE, THE TERMS AND CONDITIONS OF THE APPLICABLE LICENSE AGREEMENTS BELOW APPLY TO YOU. Please read the agreements applicable for the products you want to use. Please be careful to read the agreement for the software you want to use.
LICENSE AGREEMENT
IMPORTANT INFORMATION - PLEASE READ THIS AGREEMENT CAREFULLY BEFORE OPENING THE PACKAGE AND/OR USING THE CONTENTS THEREOF AND/OR BEFORE DOWNLOADING OR INSTALLING THE SOFTWARE PROGRAM. ALL ORDERS FOR AND USE OF SOFTWARE SUPPLIED BY SAFENET, INC. (or any of its affiliates -
Print...
Save...
Go Back
Continue


To continue installing the software you must agree to the terms of the software licence agreement.
Click Agree to continue or click Disagree to cancel the installation and quit the Installer.
Read Licence
Disagree
Agree

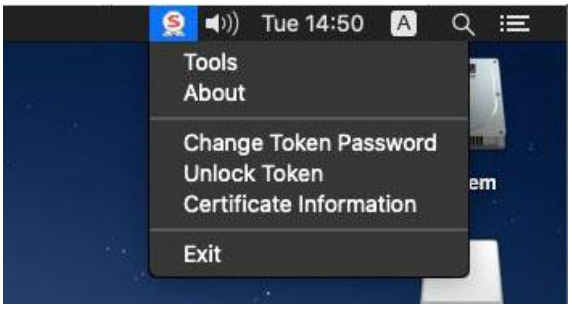

Install SafeNet Authentication Client
Standard Install on "System"
Introduction
Licence
Destination Select
Installation Type
Installation
Summary
This will take 14,6 MB of space on your computer.
Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.
Go Back
Install

3. Смяна на PIN код

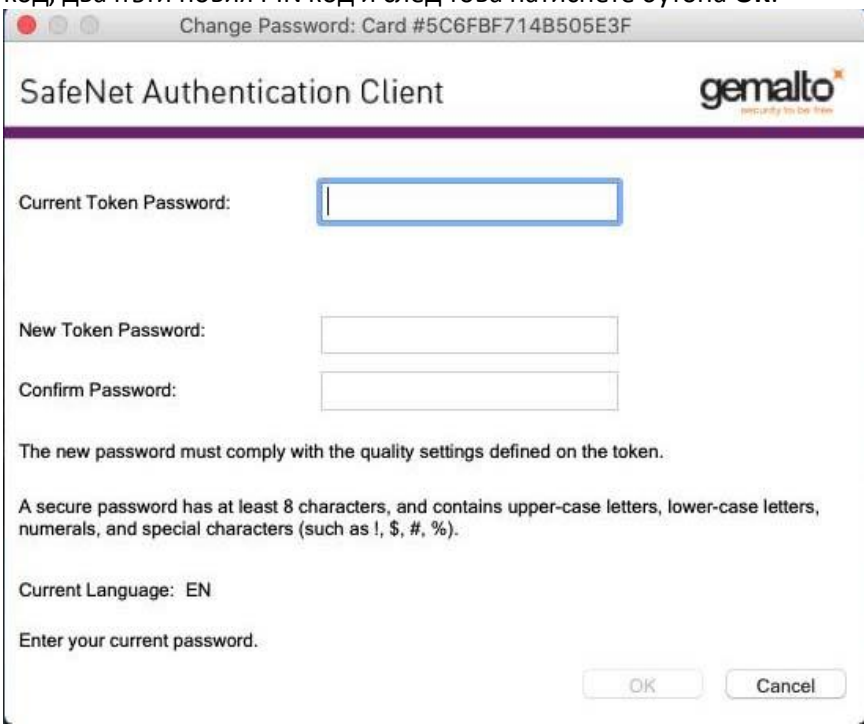
Съветваме Ви да промените предоставения Ви PIN код още при първото използване на **SafeNet Authentication Client**, както е посочено по-долу.

ВНИМАНИЕ!!!
Задължително Вашият PIN код трябва да се състои от четири цифри. Използването на повече от четири цифри или други символи може да доведе до блокиране на Вашият eSign SafeNet Authentication Client.
Смяната на ПИН кода може да се извърши по всяко време.

Стартирайте **SafeNet Authentication Client** и изберете **Change Token Password**

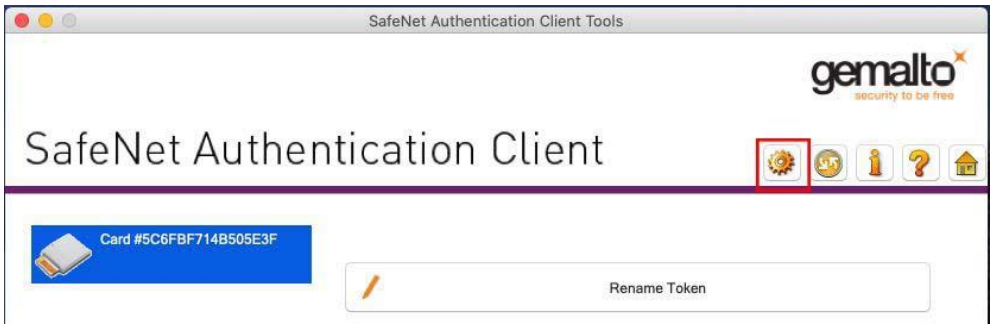


Въведете стария PIN код, два пъти новия PIN код и след това натиснете бутона **OK**:



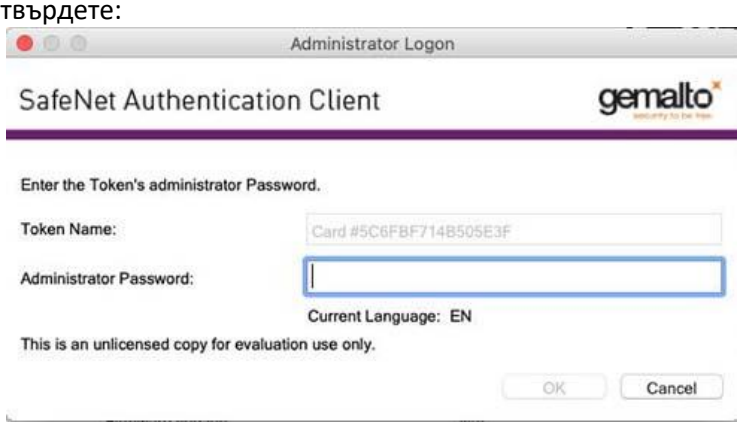
4. Отблокиране на PIN кода

Отблокиране на PIN кода се извършва с помощта на Администраторски ПИН (PUK код), който сте получили от СЕП България. Имайте предвид, че ***пет пъти грешно въвеждане на Администраторски ПИН*** води до неговото блокиране. След блокирането му единственият изход за работа със смарт картата е предаване на „СЕП България“ АД с цел нейното изтриване и генериране на нов КУКЕП. Използвайте програмата, SafeNet Authentication Client. Изберете командата **Tools** и от прозореца изберете бутона “**Advanced View**”:

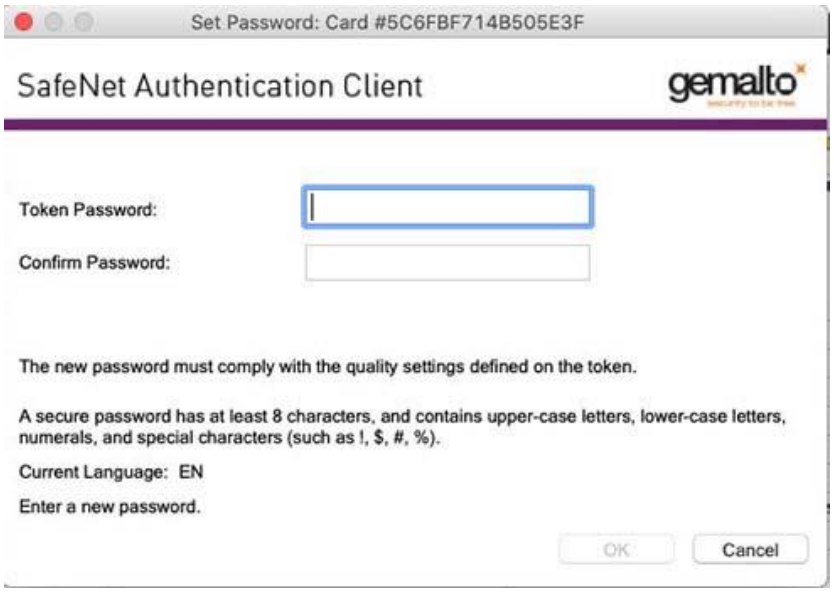


Изберете бутона “**Set Token Password**”:

Въведете Вашия PUK и потвърдете:



Въведете нов PIN код в полето “**Token Password**”, повторете го в “**Confirm Password**”и потвърдете:



5. Смяна на Администраторски ПУК / Administrator Password (PUK)

ВНИМАНИЕ!!!
Промяната на Администраторския ПИН / Administrator Password(PUK код) е на Ваша отговорност.
СЕП България не съхранява първоначалните Потребителски ПИН и Администраторски ПИН / Administrator Password (PUK код). Те са уникални за всяка карта.
СЕП България няма да може да Ви помогне в случай, че блокирате Администраторския ПИН / Administrator Password (PUK код).

6. Изтриване токен / Delete Token Content

ВНИМАНИЕ!!!
Използването на функционалността Изтриване токен / Delete Token Content изтрива безвъзвратно сертификатите от Вашата смарт карта и е на Ваша отговорност.

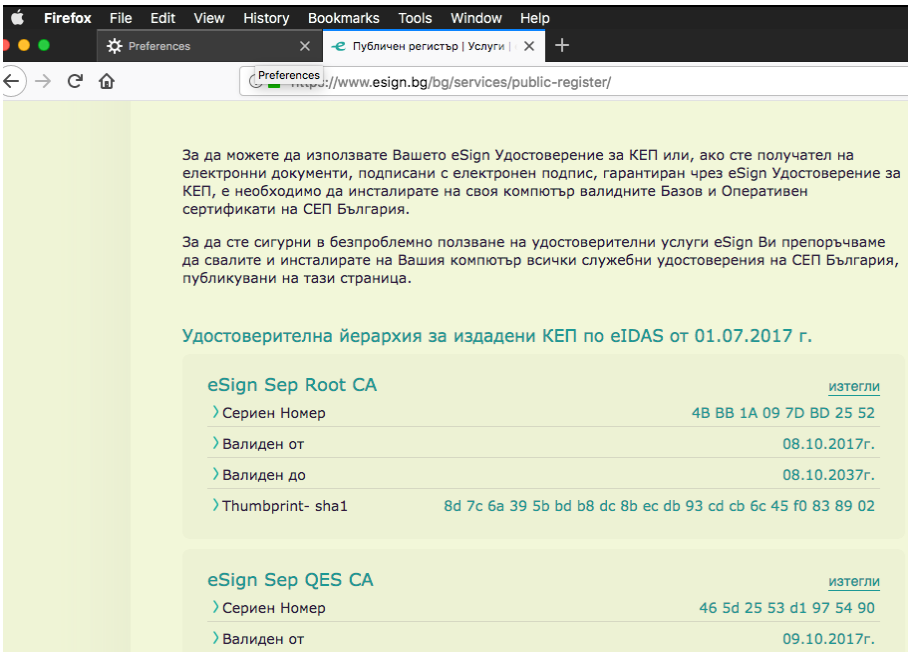
7. Допълнителни функционалности

ВНИМАНИЕ!!!
Функционалността „Изтриване на сертификат“ / “Deleting Certificate”, в раздел Advanced View изтрива безвъзвратно селектирания сертификат от Вашата смарт карта и използването му е на Ваша отговорност.

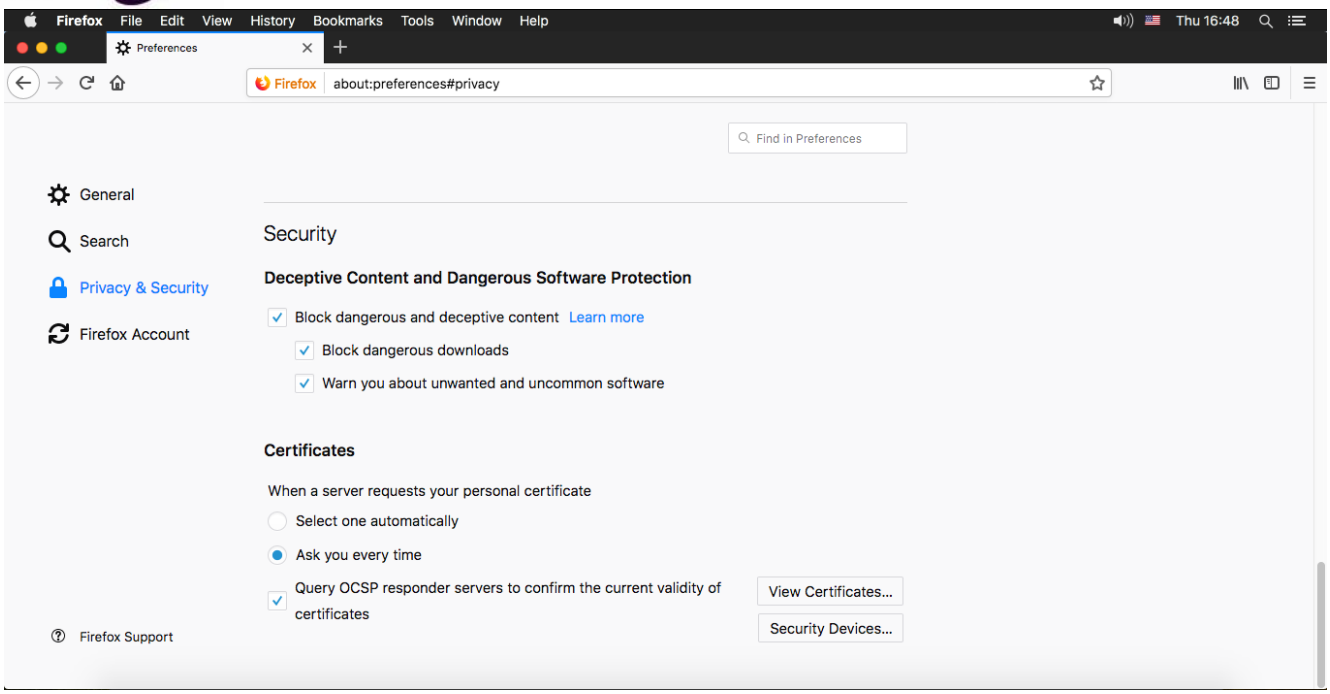
8. Настройка на Mozilla Firefox за работа с SafeNet Authentication Client

ВАЖНО! При използването на Charismatics с Firefox и Thunderbird се осъществява директен достъп до устройството. Когато успешно сте инсталирали удостоверенията си, НЕ ТРЯБВА да ги триете оттам, тъй като това ще доведе и до изтриване на удостоверението, заедно с частния и публичния ключ. След това удостоверението не може да се възстанови и трябва да се издаде ново.

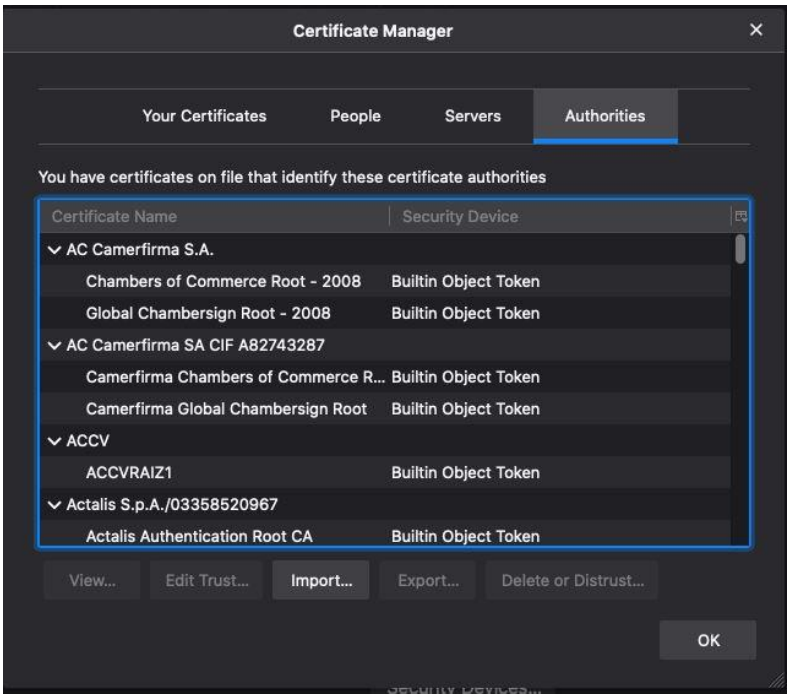
9.1 От интернет страницата на СЕП България: http://www.esign.bg **Услуги – Публичен регистър** изберете и запишете от линкковете **eSign Sep Root CA** и **eSign Sep QES CA**.



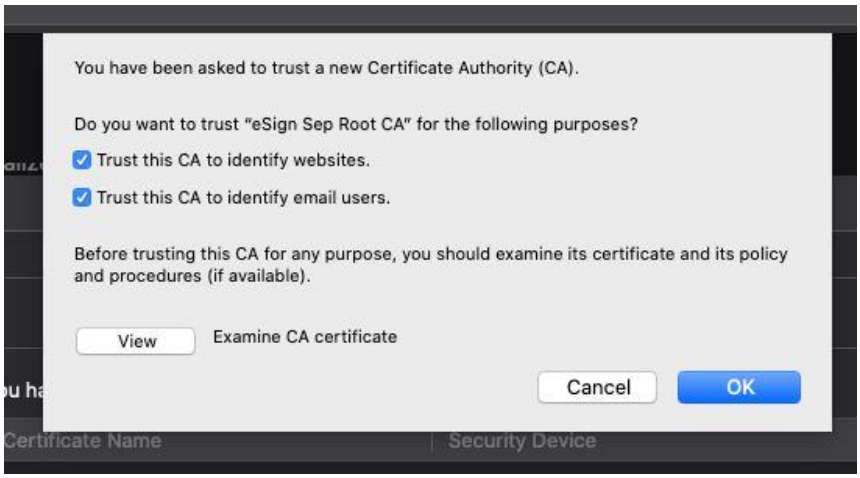
9.2 Отворете Firefox и изберете **Firefox-Preferences**, след това **Privacy & Security. В секция Certificates** изберете бутона **View Certificates… за да се визуализира Certificate Menager.**



9.3 Изберете **Authorities** и след това бутона **Import**

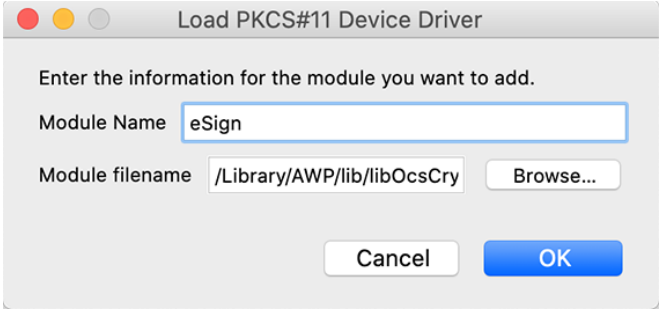


9.4 Изберете файла eSign_Sep_Root_CA.crt и в диалоговия маркирайте бутоните за Trust…. И след това изберете бутона OK.



Повторете стъпка 9.4 и с файла eSign_Sep_QES_CA.crt. Затворете диалоговия прозорец Certificate Manager

9.5 В **Privacy & Security, секция Certificates** изберете бутона **Security Devices** и в диалоговия прозорец **Devise Manager** изберете бутона **Load** за добавяне на Вашето устройство. Напишете **eSign** в полето за име на **PKCS#11** устройство (Module Name):



След това изберете бутона „Browse…" и въведете: /usr/local/lib/libeTPkcs11.dylib

Натиснете **Open** за потвърждение.

Firefox е настроен за работа с КУКЕП. Затворете прозореца за настройка.

След направените до сега инсталации и настройки, можете да ползвате Вашето eSign Удостоверение за КЕП за сайтове, изискващи съответното ниво на автентикация.

9. Настройки за работа с Chrome и Safari

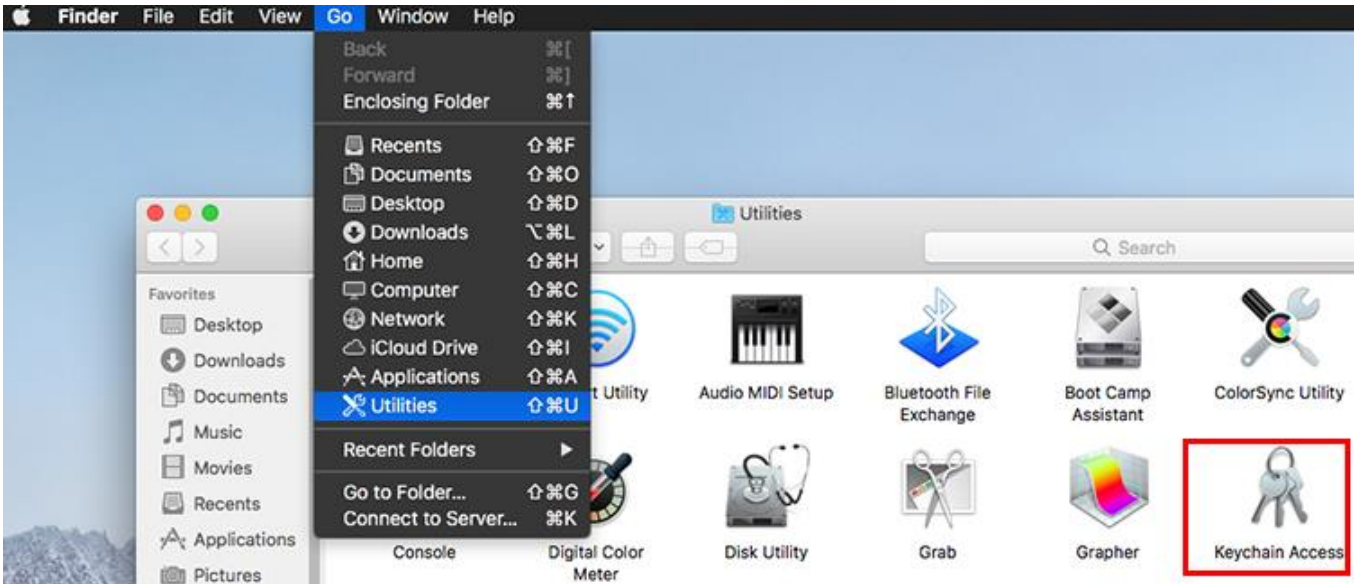
9.1 Изтеглете базов и оперативен сертификат

От интернат страницата на СЕП България, меню „Услуги" – „Публичен регистър", секция „Удостоверения на СЕП България", за:
„Удостоверителна йерархия за издадени КЕП по eIDAS от 01.07.2017 г." изтеглете и запишете

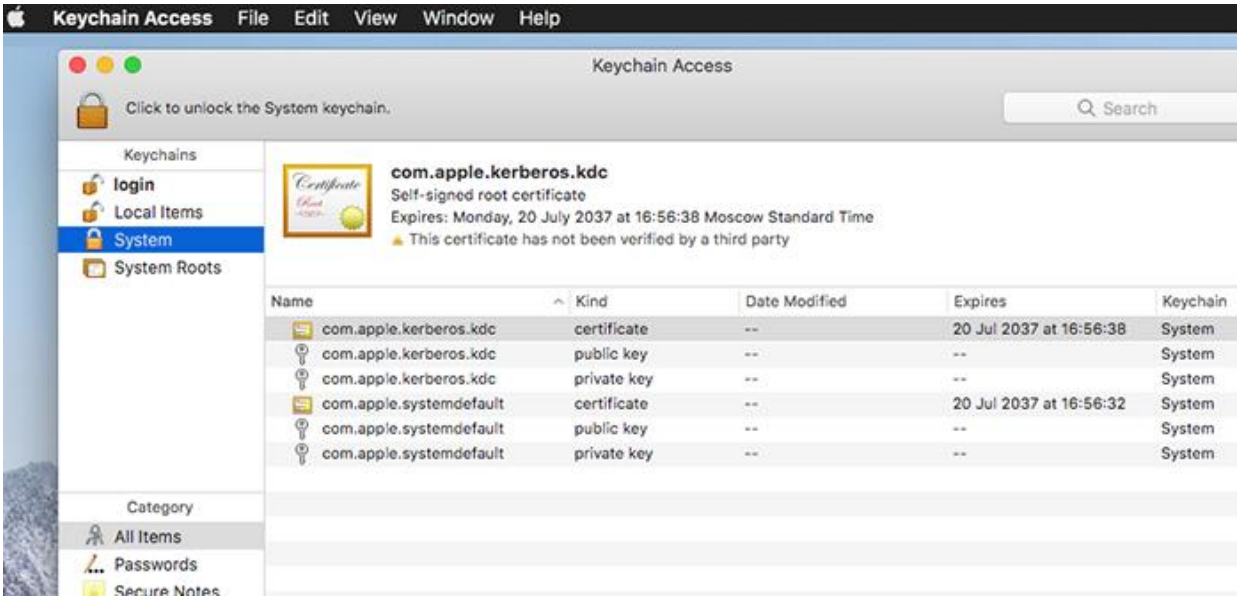
1. eSign Sep Root CA
2. eSign Sep QES CA

9.2 Инсталиране на базов и оперативен сертификат

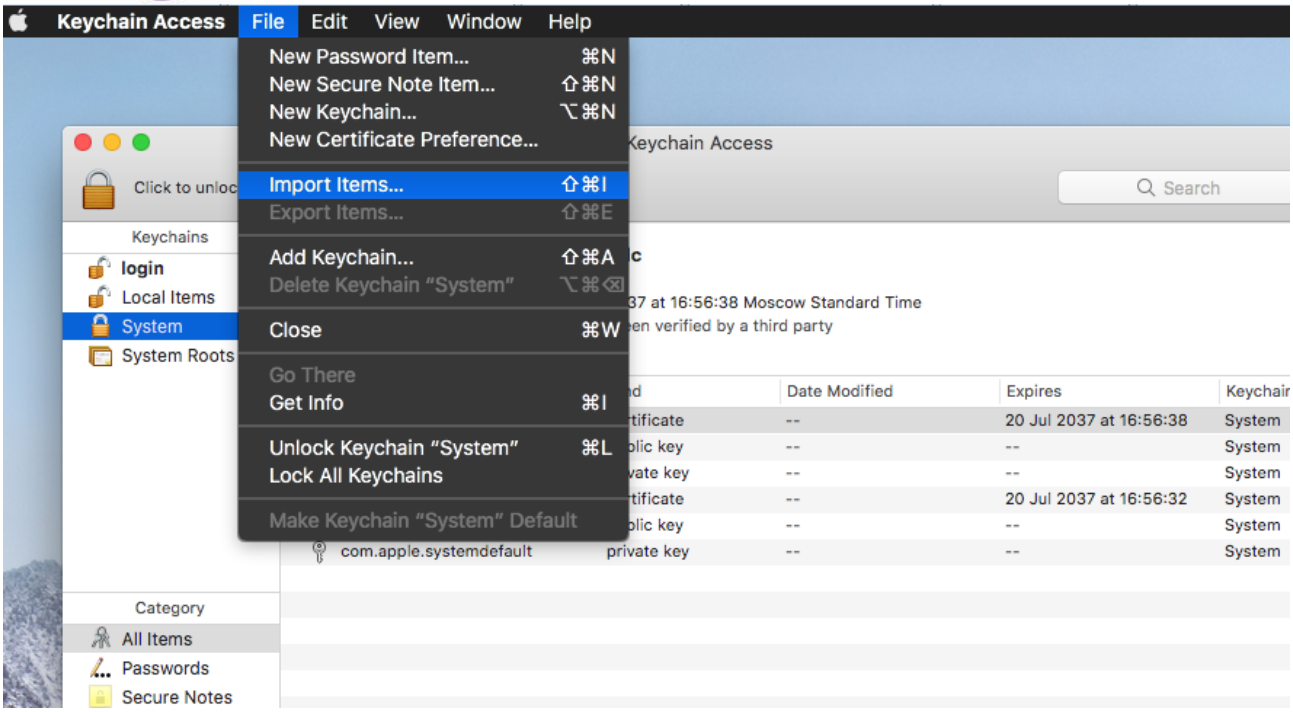
1. От меню "Go" на Finder, се избира "Utilities" и се стартира "Keychain Access".



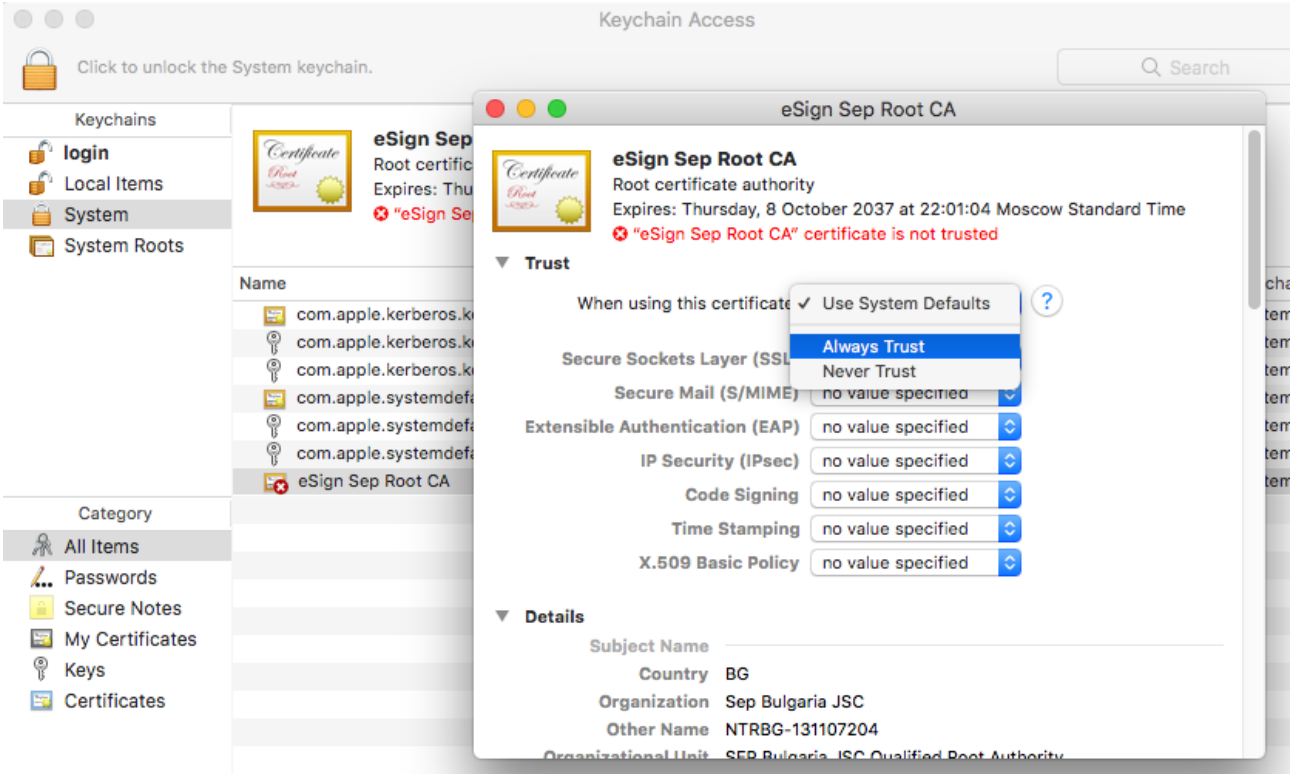
В Keychain Access изберете System.



2. От меню File, на Keychain Access изберете “Import Items”. В диалоговия прозорец за избор на файл, селектирайте записаният по рано файл eSign_Sep_Root_CA.crt.



След импорта, в System намерете и отворете (двоен клик на мишката) “eSign Sep Root CA”, отворете секция Trust и изберете “Always Trust”, както е показано по-долу.



3. Повторете горните стъпки за eSign Sep QES CA - файл eSign_Sep_QES_CA.crt

10. Контакти

За повече информация и за нови версии на ръководството и софтуера посетете Интернет сайта на СЕП България: www.eSign.bg

Ако имате нужда от допълнителна информация или съдействие при инсталацията, моля свържете се с информационния център на СЕП България, на телефон **0700 18283** или на имейл: esign@sep.bg.