



# ИНСТРУКЦИЯ ЗА РАБОТА С SAFENET AUTHENTICATION CLIENT

Операционна система OS X

Версия 10.14 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 за OS X .....	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 за OS X.	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 Mac OS X от v.10.14.x до v.11.x**

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

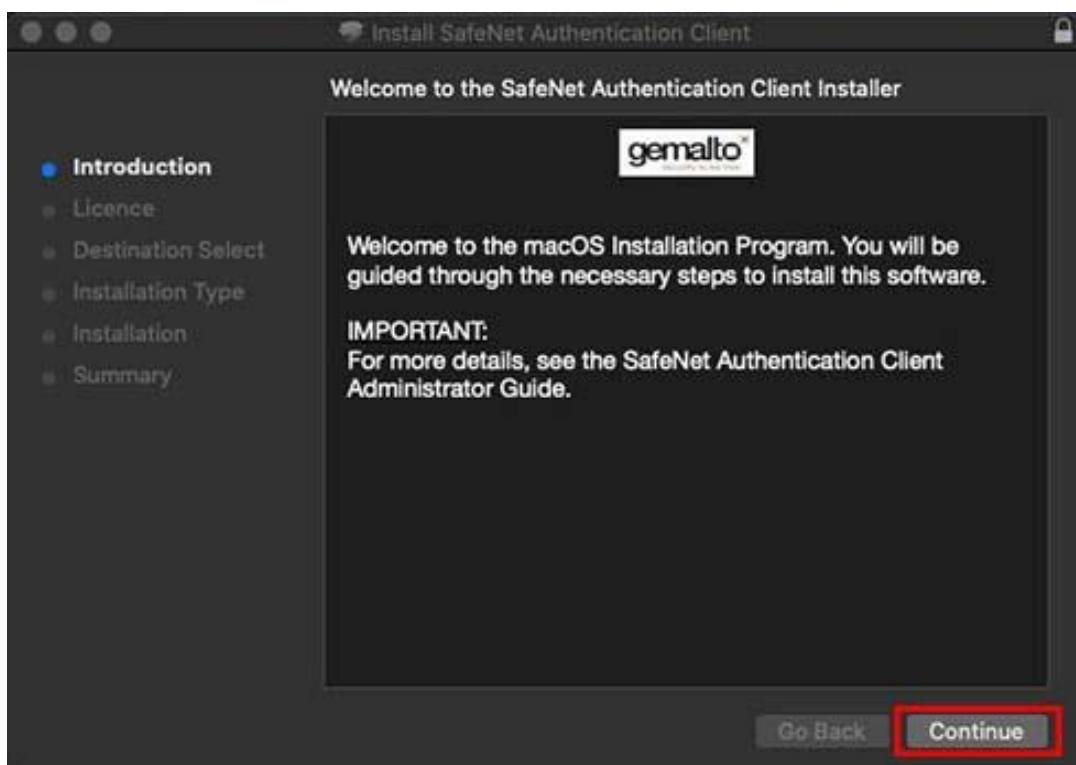
## 2. Инсталиране на софтуер за работа с SafeNet Authentication Client за OS X

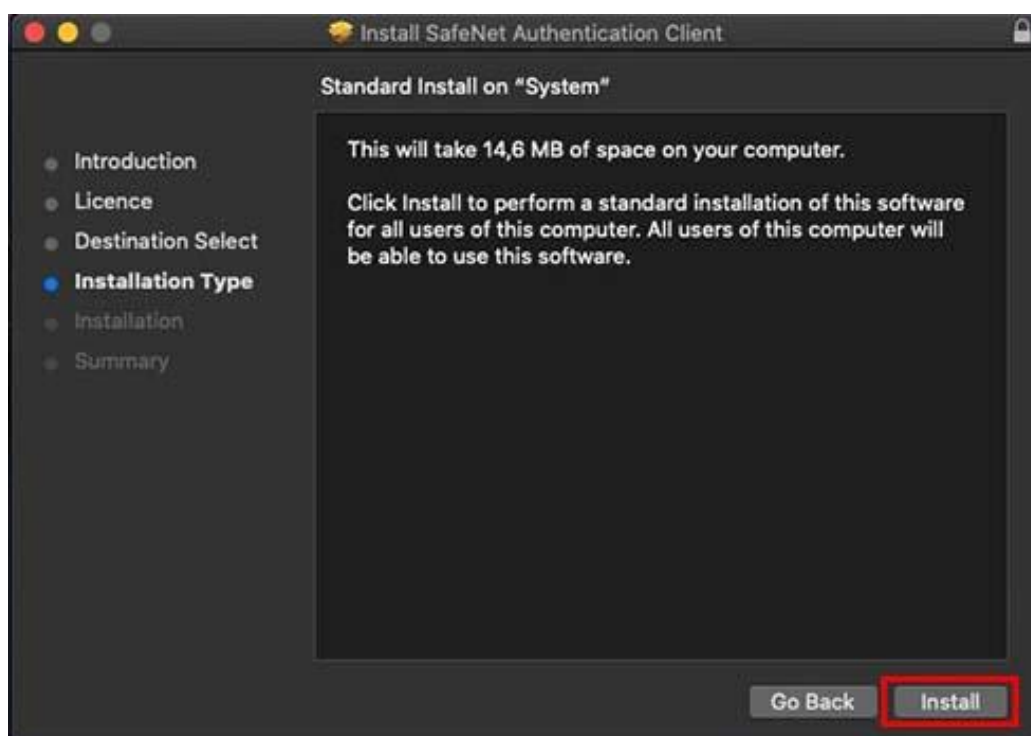
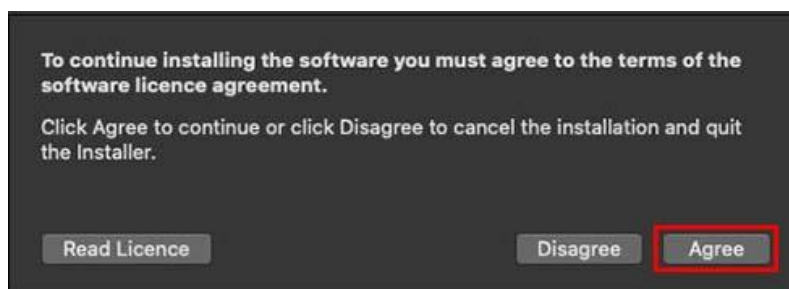
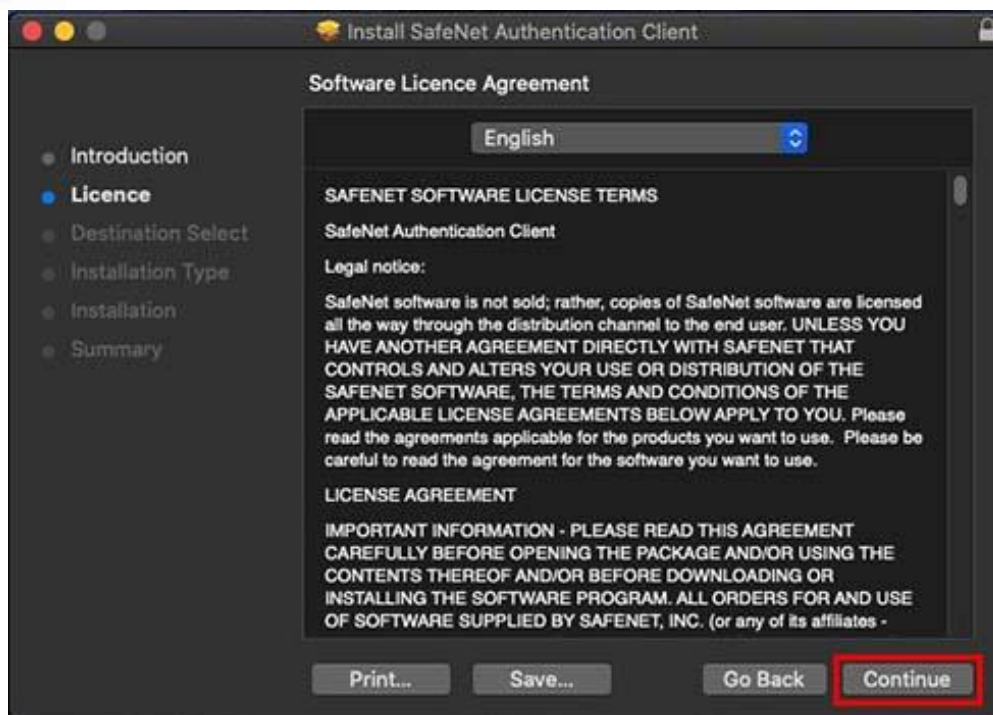
### 2.1 Инсталиране на софтуер за четец на смарт карти

В разархивираната в т. 1.1 папка, от директория **Circle\_Mac\_Installer\_v2.1.0** стартирайте файла „**abccid\_installer-2.1.0.dmg**“ и от монтираният имидж стартирайте файла „**abccid\_installer.pkg**“ и следвайте „стъпките“ по подразбиране на инсталатора.

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

В разархивираната в т. 1.1 папка стартирайте имидж файла **SafeNetAuthenticationClient\_x.x.x.dmg** и след неговото отваряне, стартирайте **SafeNet Authentication Client 10.2.pkg** и следвайте стъпките по подразбиране. **След като инсталирате, рестартирайте OS X.**





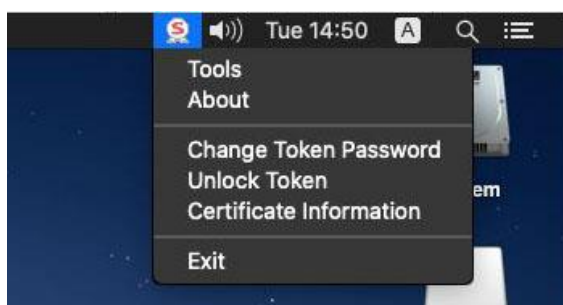
### 3. Смяна на PIN код

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**:

Change Password: Card #5C6FBF714B505E3F

SafeNet Authentication Client **gemalto**  
security to be free

Current Token Password:

New Token Password:

Confirm Password:

The new password must comply with the quality settings defined on the token.

A secure password has at least 8 characters, and contains upper-case letters, lower-case letters, numerals, and special characters (such as !, \$, #, %).

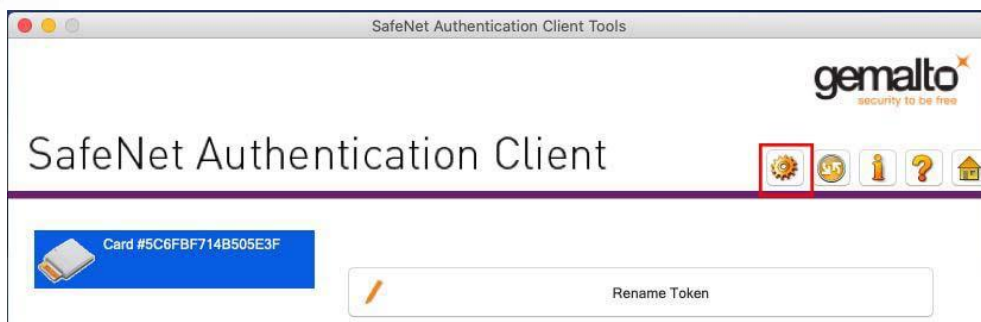
Current Language: EN

Enter your current password.

OK Cancel

### 4. Отблокиране на PIN кода

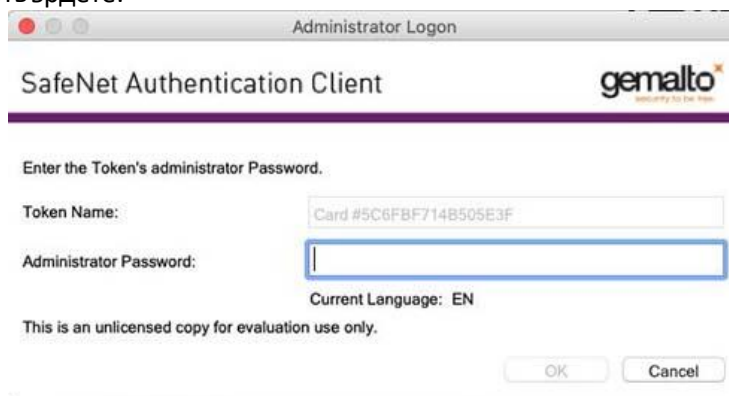
Отблокиране на PIN кода се извършва с помощта на Администраторски ПИН (PUK код), който сте получили от СЕП България. Имайте предвид, че **пет пъти грешно въвеждане на Администраторски ПИН** води до неговото блокиране. След блокирането му единственият изход за работа със смарт картата е предаване на „СЕП 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”**:



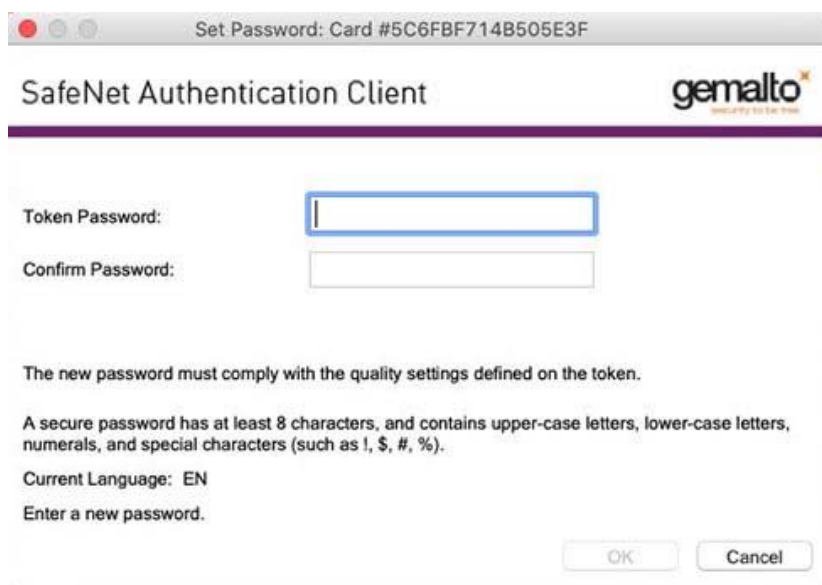
Изберете бутона **“Set Token Password”**:



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

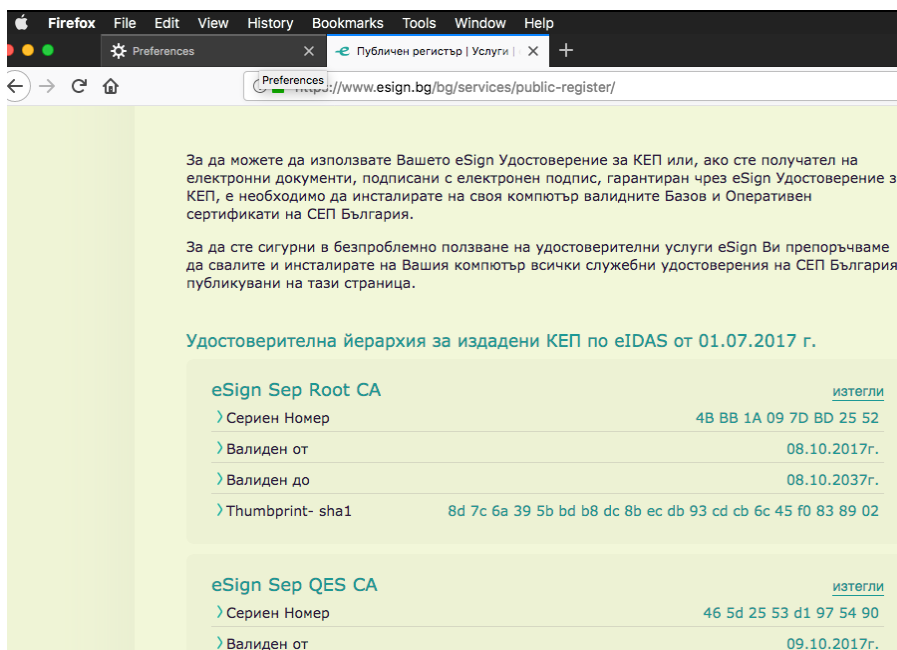
### ВНИМАНИЕ!!!

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 линковете [eSign Sep Root CA](#) и [eSign Sep QES CA](#).



The screenshot shows the Firefox browser interface with the address bar displaying <http://www.esign.bg/bg/services/public-register/>. The main content area displays information about two certificates:

За да можете да използвате Вашето eSign Удостоверение за КЕП или, ако сте получател на електронни документи, подписани с електронен подпис, гарантиран чрез eSign Удостоверение за КЕП, е необходимо да инсталирате на своя компютър валидните Базов и Оперативен сертификати на СЕП България.

За да сте сигурни в безпроблемно ползване на удостоверителни услуги eSign Ви препоръчваме да свалите и инсталирате на Вашия компютър всички служебни удостоверения на СЕП България, публикувани на тази страница.

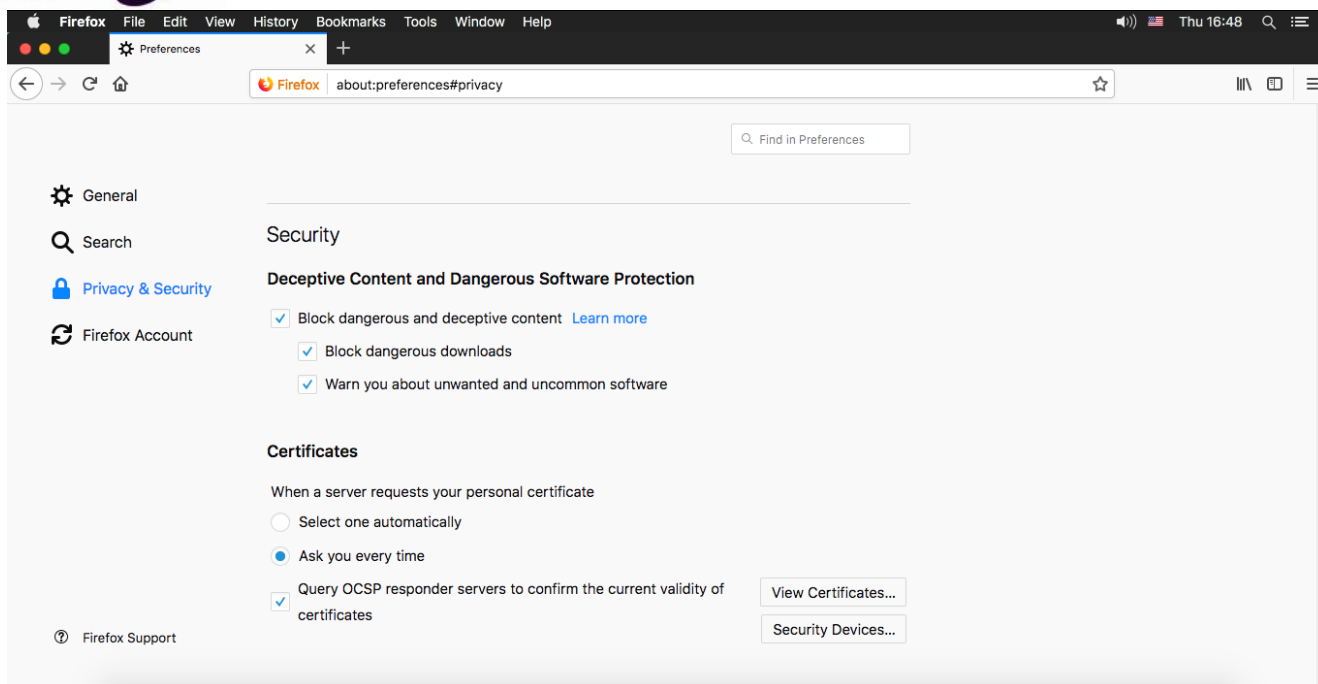
Удостоверителна йерархия за издадени КЕП по eIDAS от 01.07.2017 г.

eSign Sep Root CA		изтегли
Сериен Номер	4B BB 1A 09 7D BD 25 52	
Валиден от	08.10.2017г.	
Валиден до	08.10.2037г.	
Thumbprint- sha1	8d 7c 6a 39 5b bd b8 dc 8b ec db 93 cd cb 6c 45 f0 83 89 02	

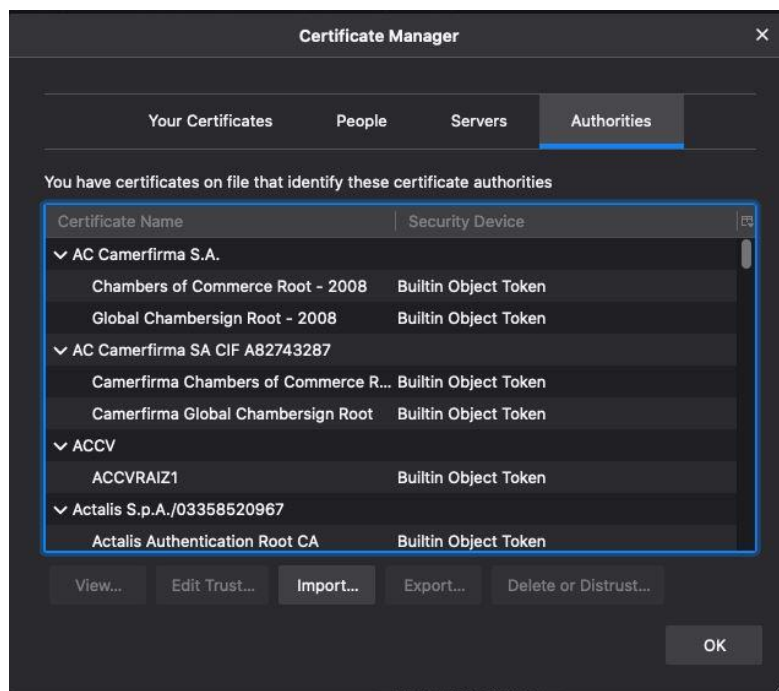
  

eSign Sep QES CA		изтегли
Сериен Номер	46 5d 25 53 d1 97 54 90	
Валиден от	09.10.2017г.	

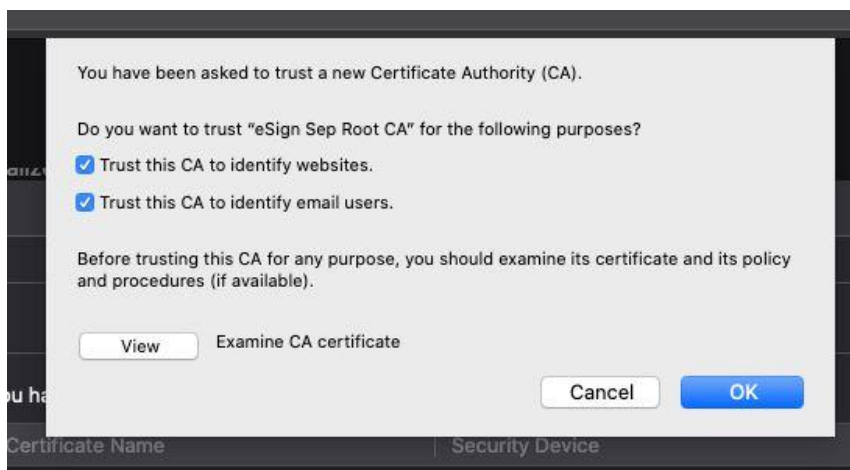
9.2 Отворете Firefox и изберете **Firefox-Preferences**, след това **Privacy & Security**. В секция **Certificates** изберете бутона **View Certificates...** за да се визуализира **Certificate Manager**.



### 9.3 Изберете Authorities и след това бутона Import

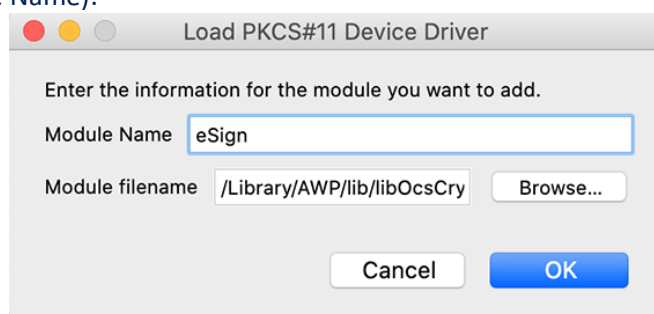


9.4 Изберете файла eSign\_Sep\_Root\_CA.crt и в диалоговия маркирайте бутоните за Trust.... И след това изберете бутона OK.



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 **Device 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

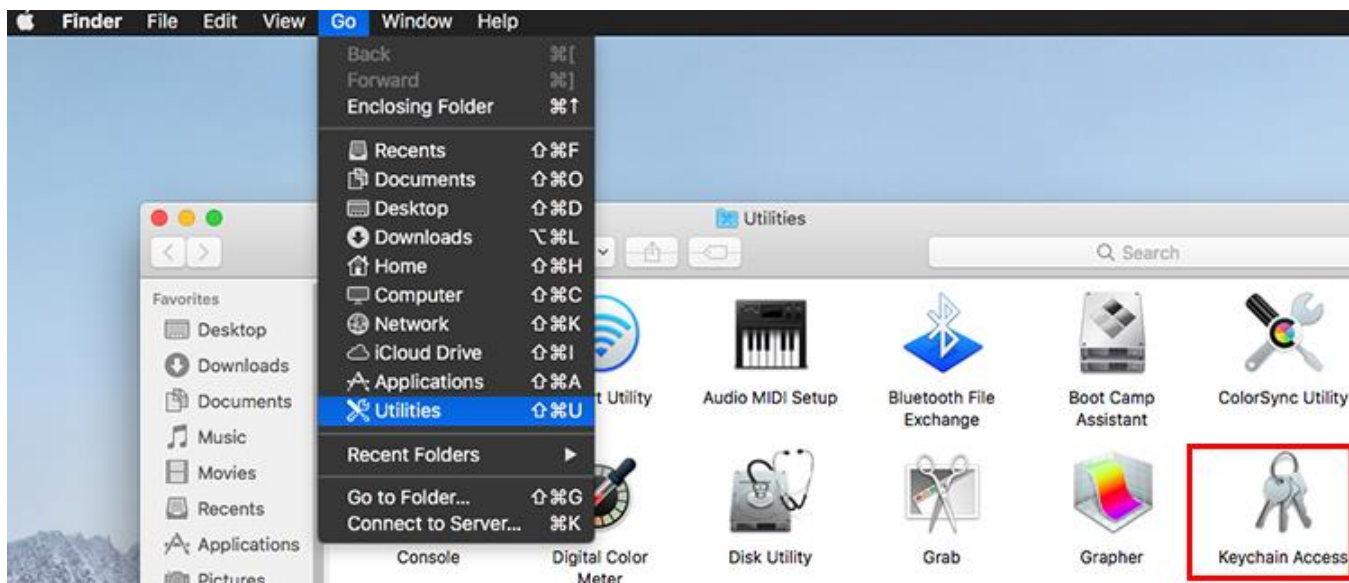
От интернат страницата на СЕП България, меню „Услуги“ – „Публичен регистър“, секция „Удостоверения на СЕП България“, за:

„Удостоверителна йерархия за издадени КЕП по eIDAS от 01.07.2017 г.“ изтеглете и запишете

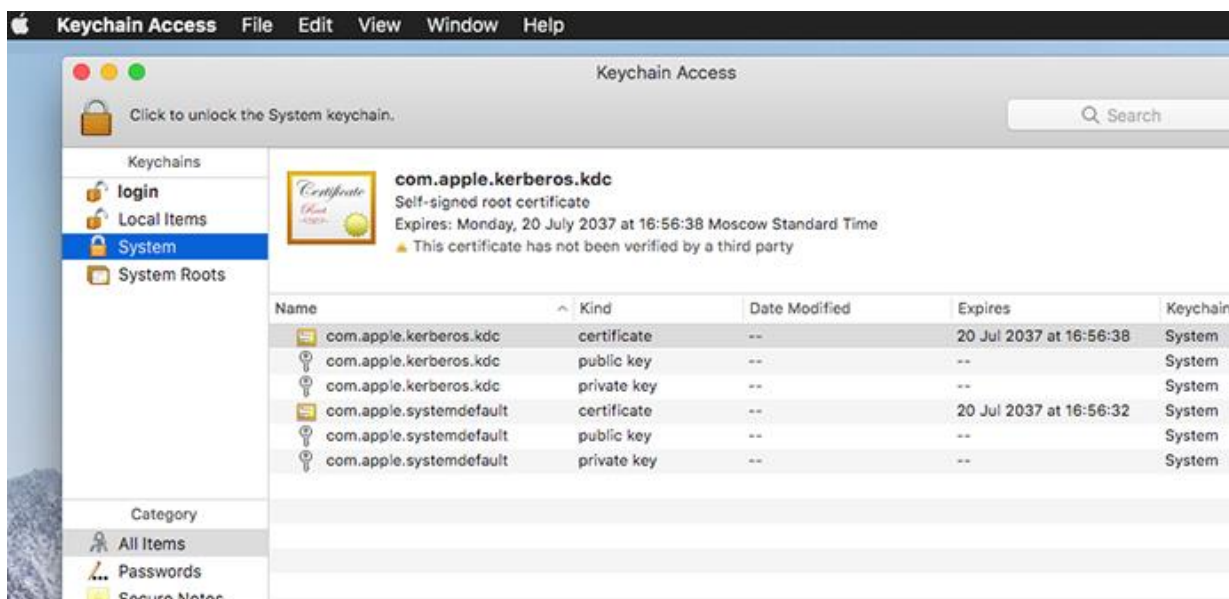
1. eSign Sep Root CA
2. eSign Sep QES CA

### 9.2 Инсталиране на базов и оперативен сертификат

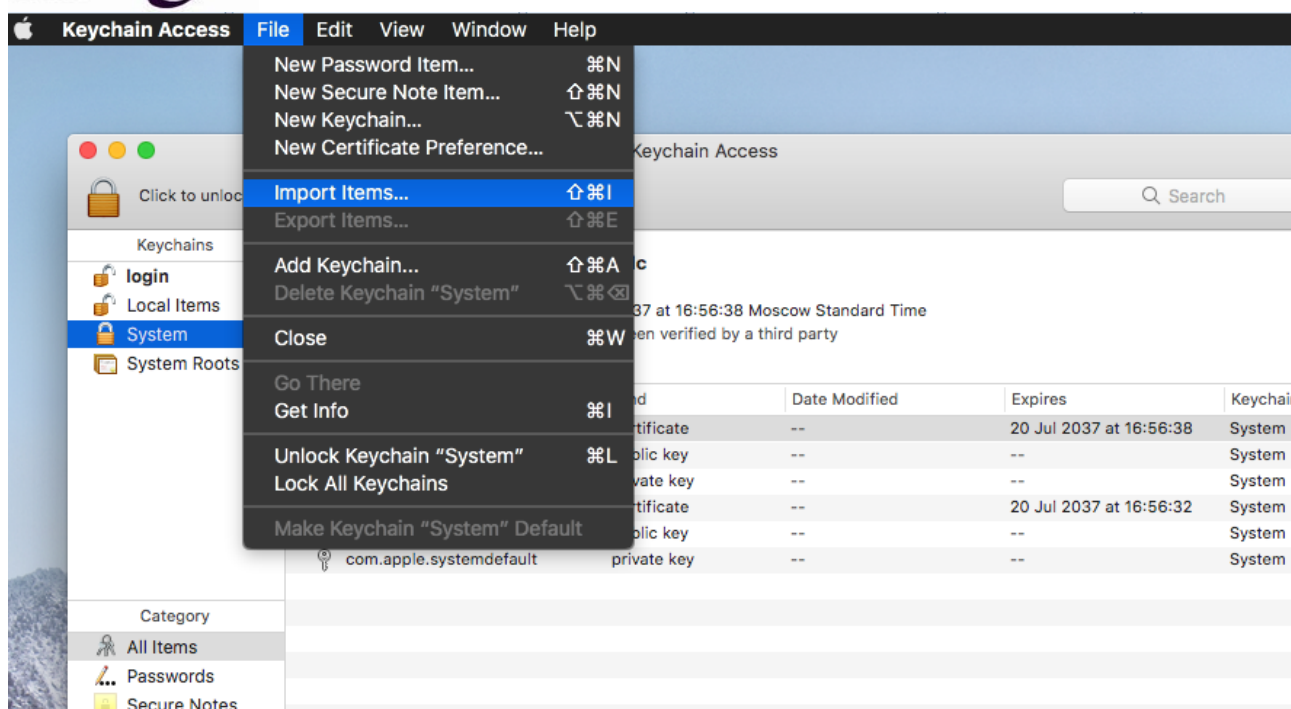
1. От меню “Go“ на Finder, се избира “Utilities“ и се стартира “Keychain Access“.



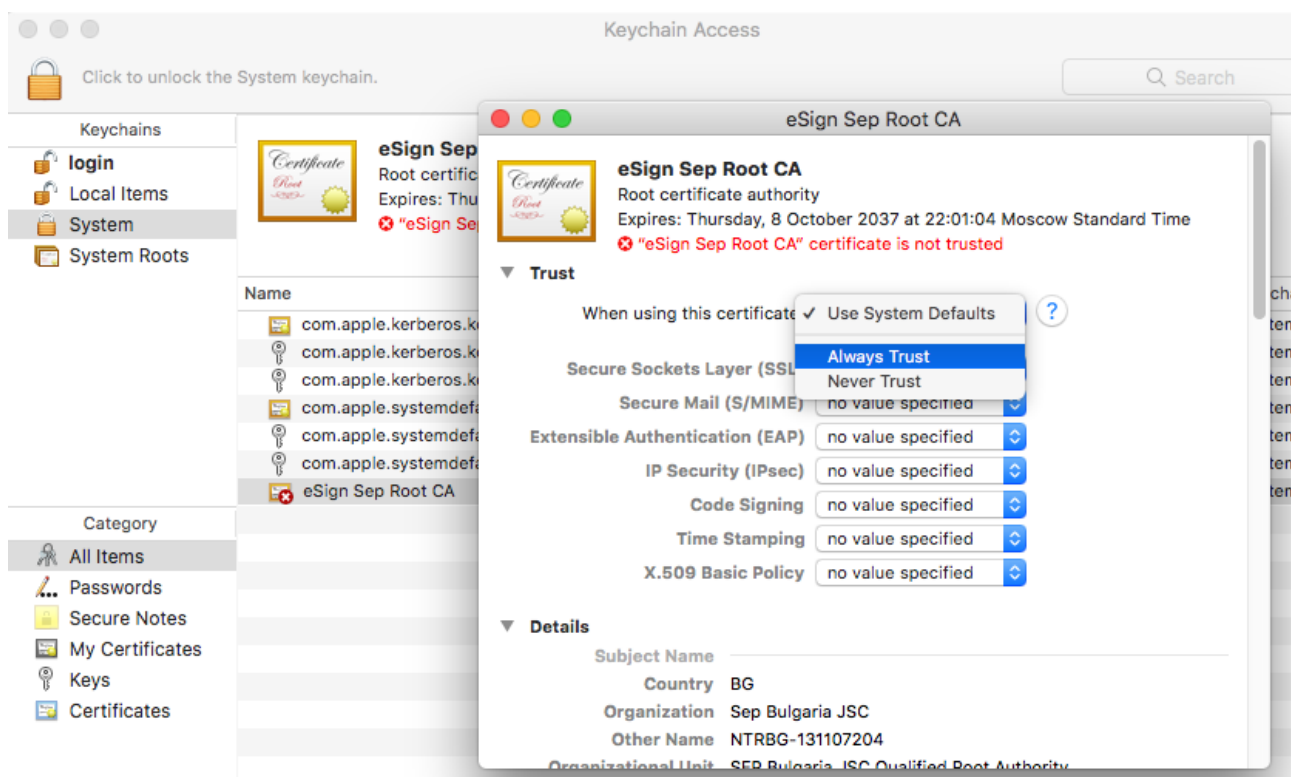
В Keychain Access изберете System.



- 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](http://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](mailto:esign@sep.bg).