



ул. "Иван Вазов" №16, ет.6, София 1000, България, тел/факс: (+3592)9210890, e-mail: support@infonotary.com

Инструкции за инсталация и използване на удостоверения за електронен подпис

Версия 1.1



ИНСТАЛАЦИЯ И ИЗПОЛЗВАНЕ С ПРОДУКТИ НА MICROSOFT	3
1. ИНСТАЛАЦИЯ НА УДОСТОВЕРИТЕЛНАТА ВЕРИГА НА ИНФОНОТАРИ.....	3
1.1. <i>Microsoft Internet Explorer</i>	3
1.2. <i>Microsoft Outlook и Outlook Express</i>	7
2. НАСТРОЙКА НА ПОТРЕБИТЕЛСКИЯ ПРОФИЛ В MICROSOFT OUTLOOK	7
ИНСТАЛАЦИЯ И ИЗПОЛЗВАНЕ С ПРОДУКТИ НА MOZILLA	14
1. ИНСТАЛАЦИЯ НА УДОСТОВЕРИТЕЛНАТА ВЕРИГА НА ИНФОНОТАРИ.....	14
1.1. <i>Инсталация в Mozilla Firefox</i>	14
1.2. <i>Инсталация в Mozilla Thunderbird</i>	18
2. ИНСТАЛАЦИЯ НА ХАРДУЕРЕН КРИПТОГРАФСКИ МОДУЛ	18
2.1. <i>Инсталация в Mozilla Firefox</i>	19
2.2. <i>Инсталация в Mozilla Thunderbird</i>	22
3. НАСТРОЙКА НА ПОТРЕБИТЕЛСКИЯ ПРОФИЛ В MOZILLA THUNDERBIRD.....	23

Инсталация и използване с продукти на Microsoft

1. Инсталация на удостоверителната верига на Инфонотари

Преди да започнете работа с вашето удостоверение за електронен подпис е необходимо да инсталирате базовите удостоверения на Инфонотари. Удостоверителната верига можете да намерите в директория "certificates" на инсталационния диск или в Интернет на адрес:

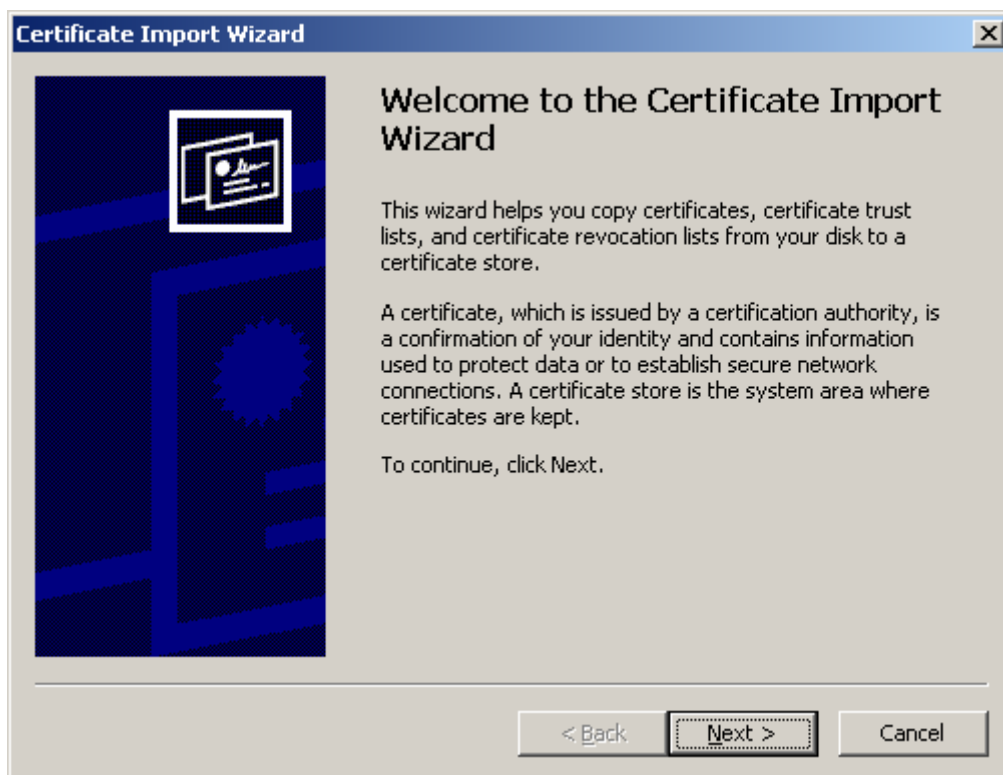
<http://www.infonotary.com/site/files/INotaryCertChain.p12>

1.1. Microsoft Internet Explorer

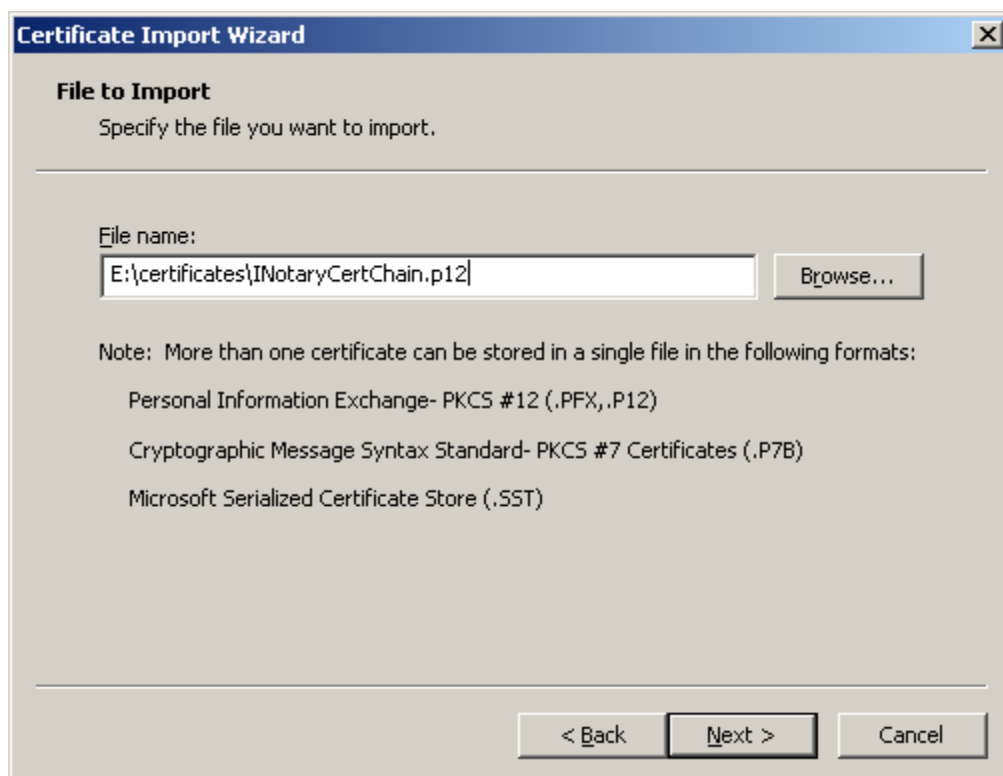
Операционната система Microsoft Windows използва централизирано хранилище за съхранение на удостоверения за електронен подпис (цифрови сертификати). Всички програми, използващи криптография имат достъп до това хранилище. Инсталацията на удостоверения се прави за текущия потребител на Windows. Ако повече от един потребители използват една система, то инсталацията трябва да се извърши поотделно за всеки един от тях.

За да инсталирате базовите удостоверения на Инфонотари за активния потребител на MS Windows направете следното:

Отворете файл "INotaryCertChain.p12" от инсталационния диск или от сайта на Инфонотари. Стартира се програма за инсталация на удостоверения, с екран, подобен на показания на следващата страница.



Изберете бутон Next > за да продължите.



Отново изберете Next >.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

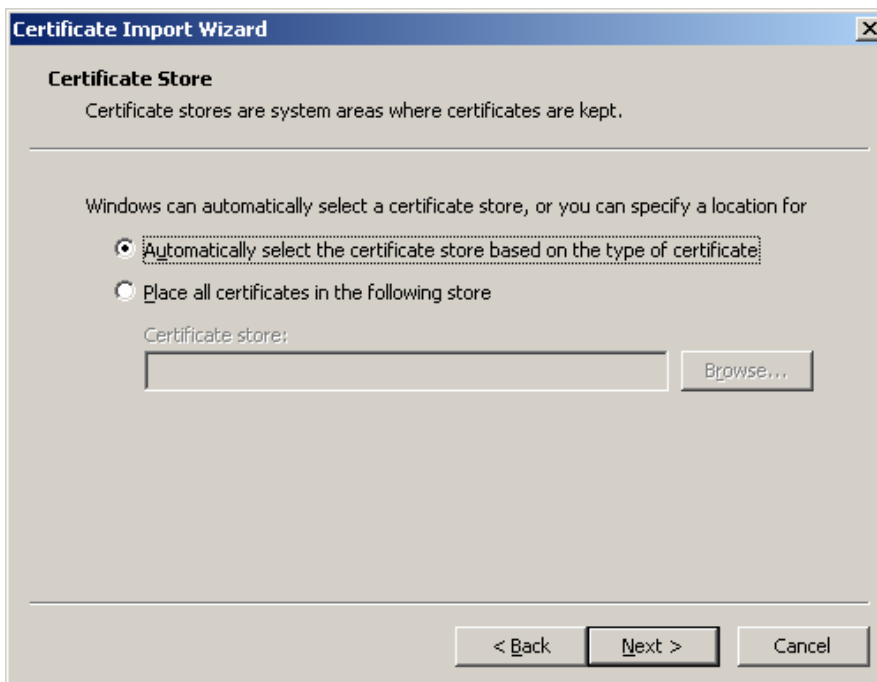
Password:

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back Next > Cancel

Оставете полето Password празно и изберете Next >.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

Automatically select the certificate store based on the type of certificate

Place all certificates in the following store

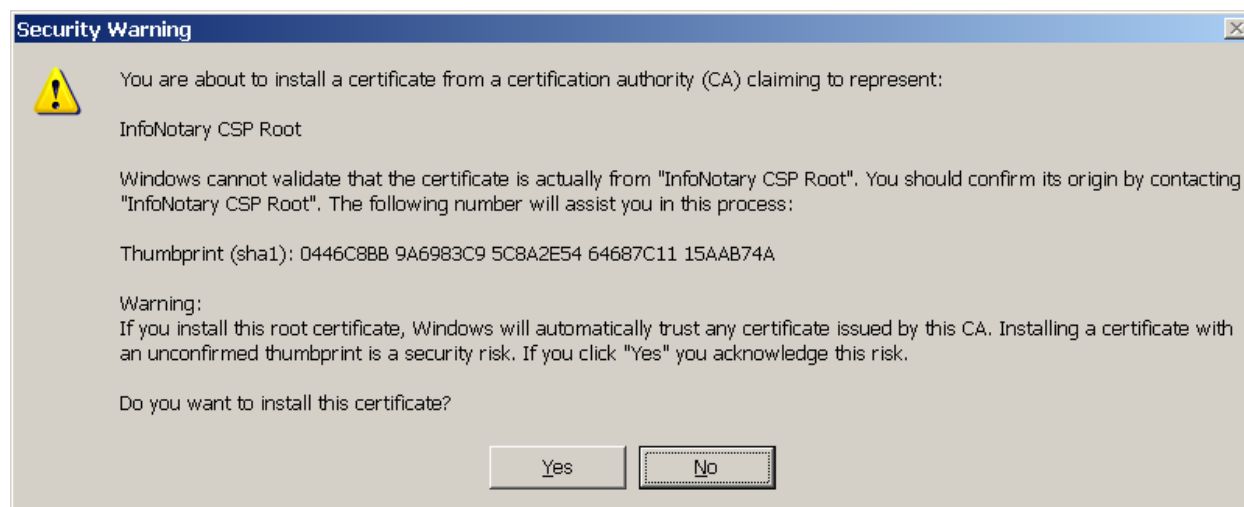
Certificate store:

 Browse...

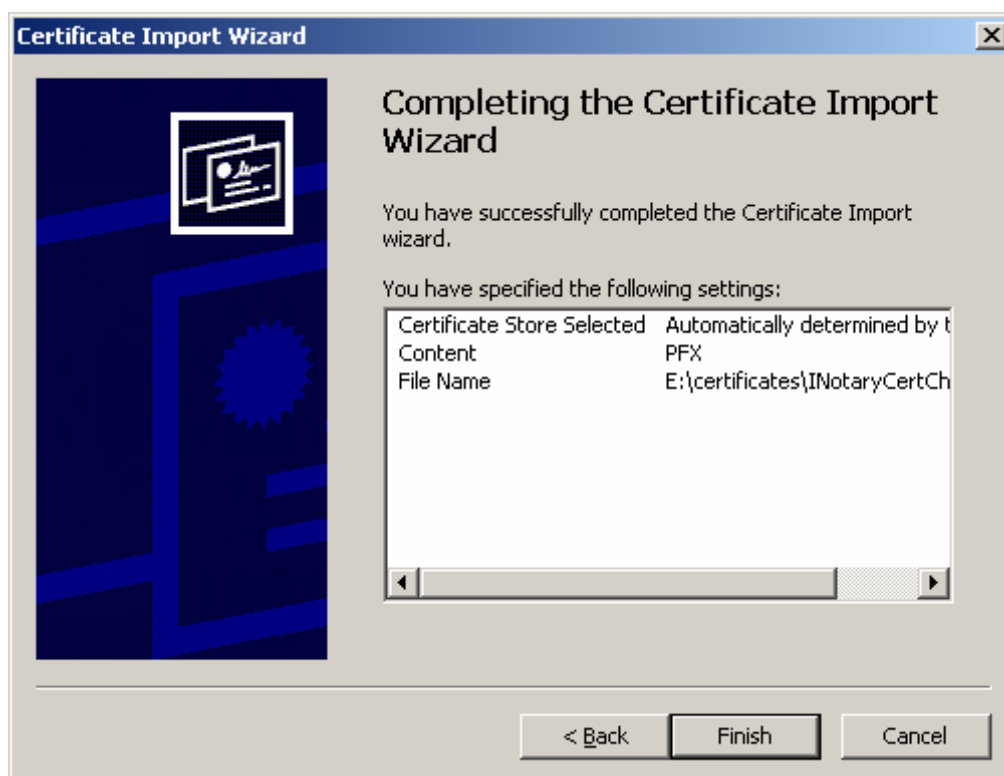
< Back Next > Cancel

Оставете маркираната по подразбиране опция за автоматичен избор на хранилище за удостоверения, в зависимост от техния тип и изберете Next >.

Програмата за инсталация ще инсталира всички удостоверения от веригата като ще поиска от вас потвърждение само за базовите (root) удостоверения:



Криптографските контролни суми (thumbprint) показани в тези диалози, можете да сравните с тези, публикувани на сайта на Инфонотари:



Изберете Finish за да финализирате процеса на инсталацията.

Забележка: Инсталацията на вашето удостоверение в хранилището на Microsoft Windows става автоматично при поставяне на смарт картата в четеца и не е необходимо да го инсталирате ръчно.

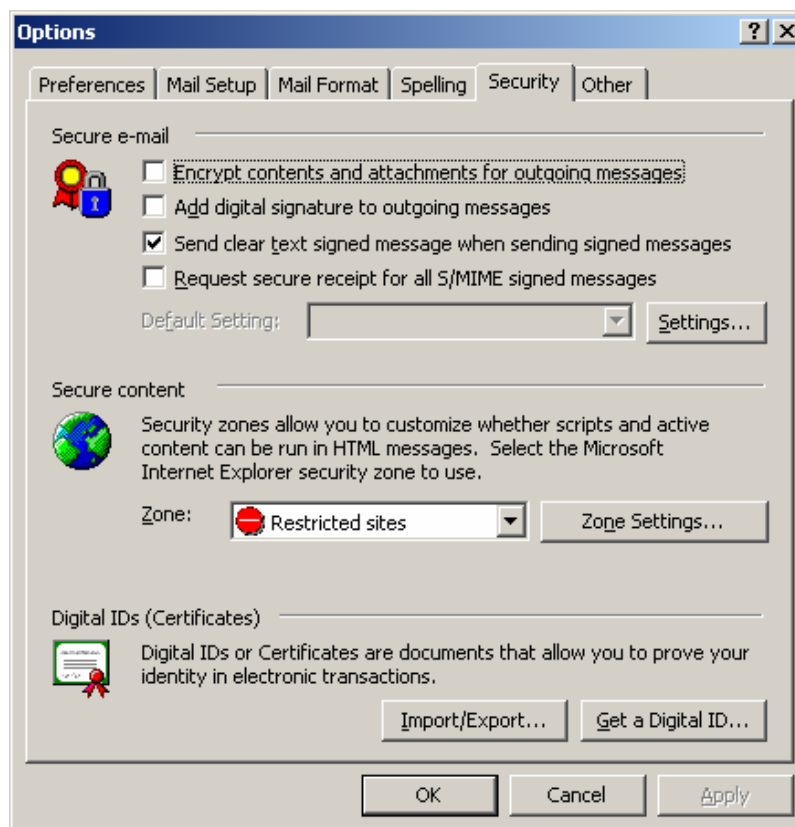
1.2. Microsoft Outlook и Outlook Express

Microsoft Outlook използва стандартното хранилище за удостоверения на операционната система Microsoft Windows. Ако сте изпълнили операциите описани в точка "1. Microsoft Internet Explorer", то не е необходимо да правите нищо повече, в противен случай сега е момента да ги изпълните.

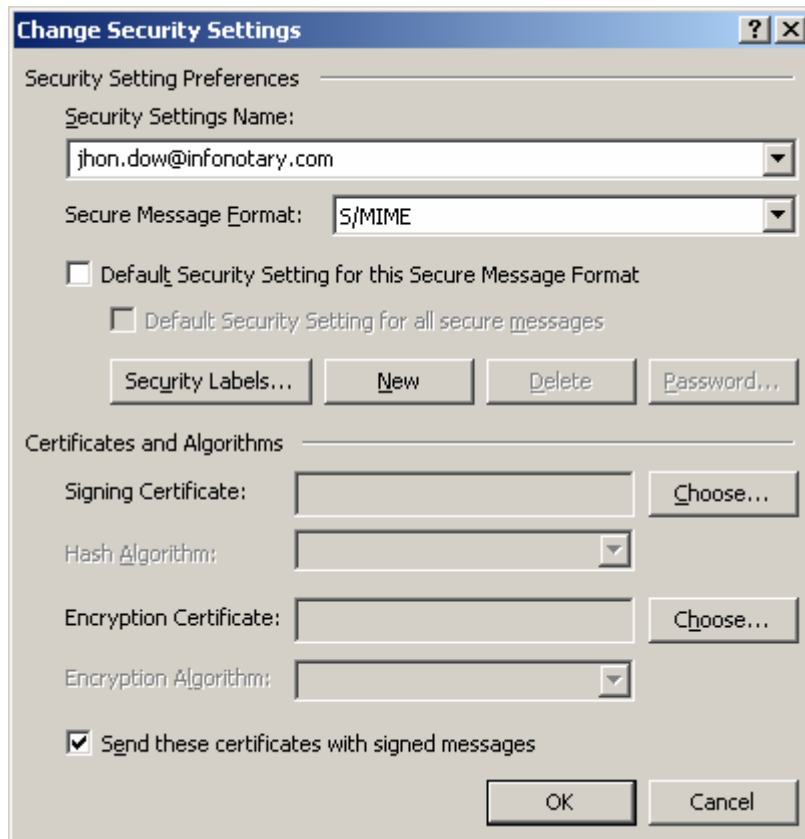
2. Настройка на потребителския профил в Microsoft Outlook

За да може да подписвате вашата изходяща електронна поща трябва да асоциирате потребителския си профил (account) с удостоверението за електронен подпис, записано на смарт-картата. Това става по следния начин:

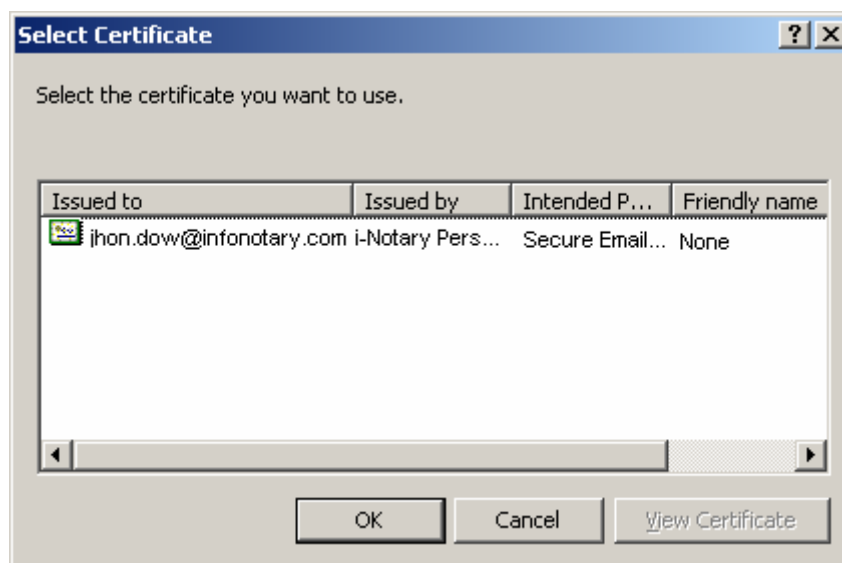
Стартирайте Microsoft Outlook. От меню Tools изберете Options. Изберете раздел Security и натиснете бутона Settings



В полето Security Settings Name изпишете e-mail адреса си



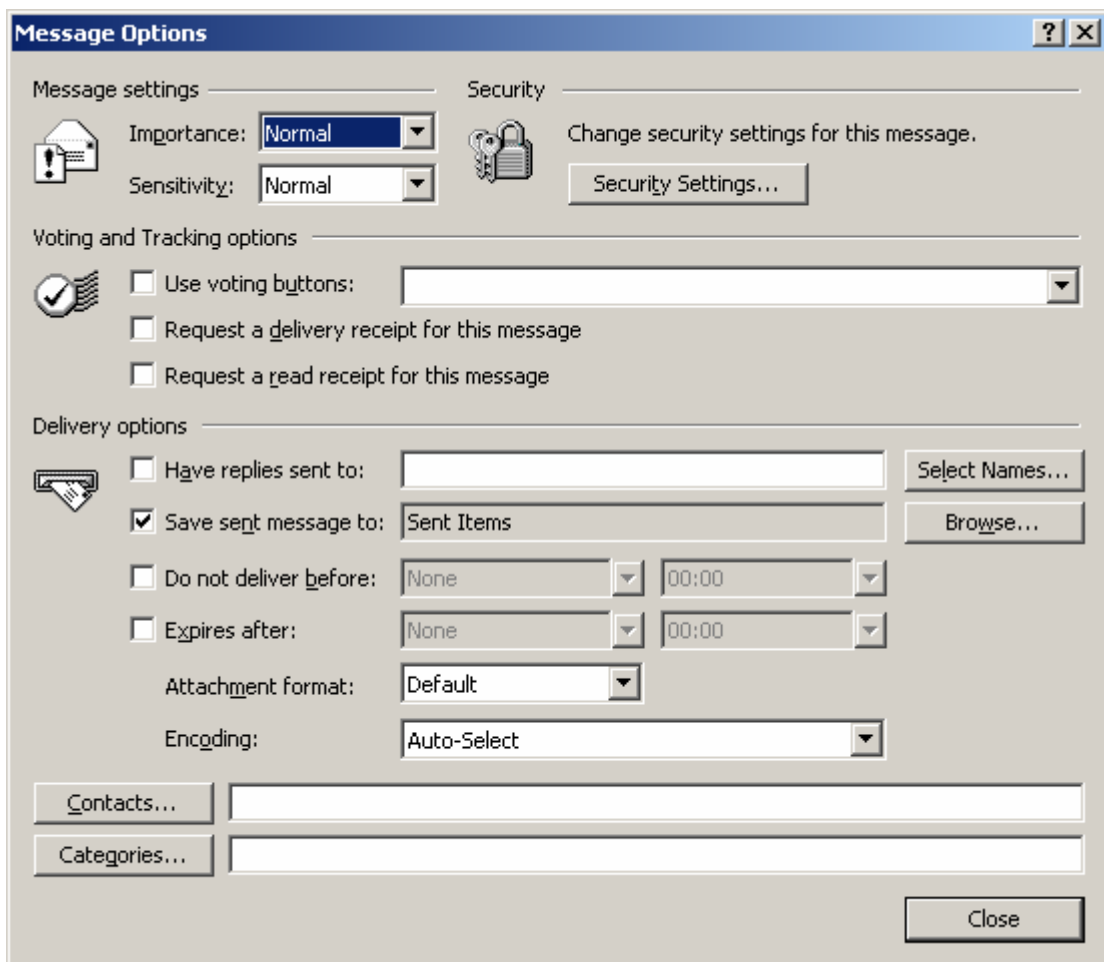
Натиснете бутон Choose и изберете желаното от вас удостоверение, с което ще подписвате кореспонденцията си. Потвърдете с OK.



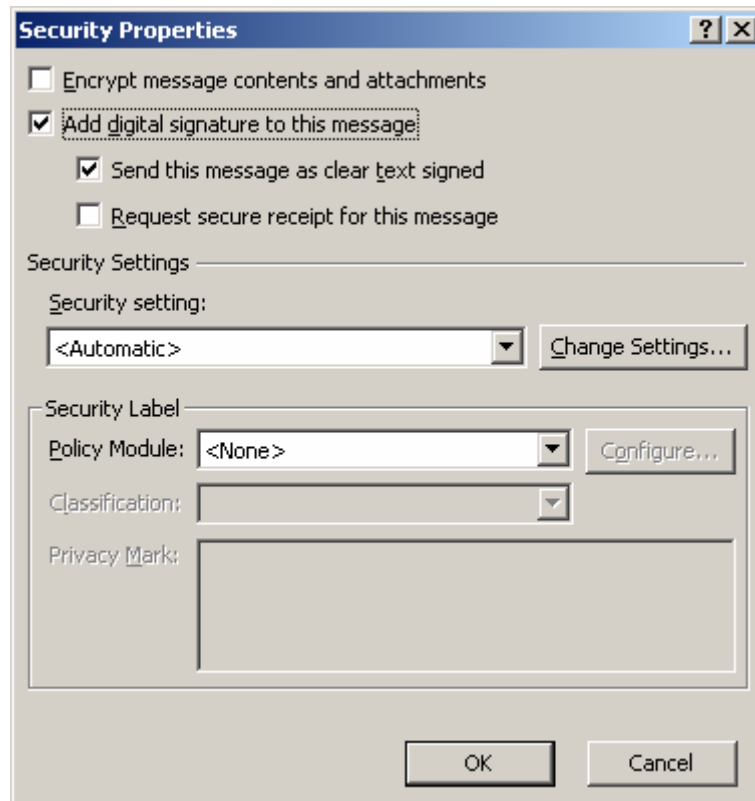
Ако е избрана опцията Add digital signature to outgoing messages, всяко изпратено съобщение ще бъде подписано с избраното удостоверение.

Имате възможност да използвате същото удостоверение и за декриптиране на съобщения изпратени към вас. Имайте предвид, че не всички удостоверения могат да се използват за криптиране и декриптиране. Тези възможности зависят от типа на вашето удостоверение.

При създаване на ново съобщение, ако в предварителните настройки не е избрана опцията за изпращане на подписано съобщение (по подразбиране), ще трябва всеки път, когато желаете, да добавяте електронния си подпис към дадено съобщение. Това става по следния начин:



Необходимо е да сте в режим на създаване на ново съобщение (от бутон New). От лентата с бутони или от падащото меню View изберете Options. Натиснете бутон Security Settings.

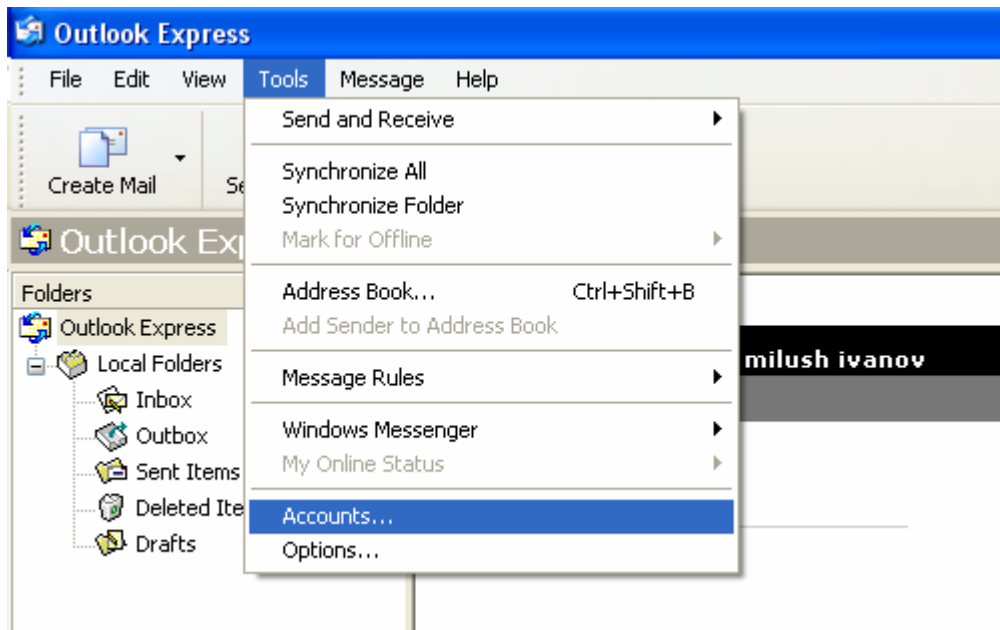


Изберете опцията Add digital signature to this message и потвърдете с ОК.

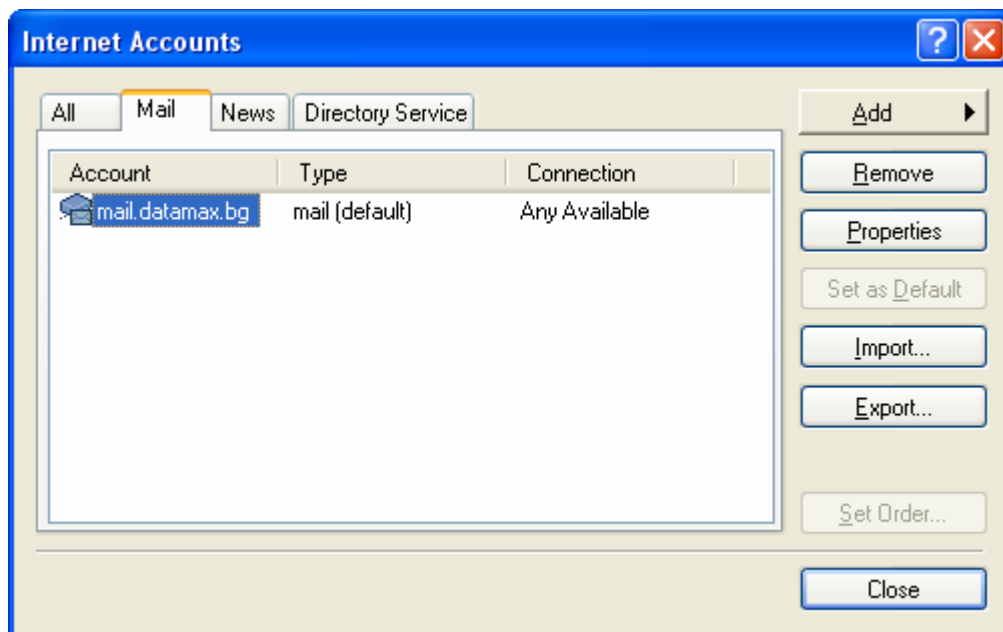
Всеки път, когато изпращате подписано съобщение смарт картата ви трябва да бъде поставена в четеца. В момента на изпращането системата ще ви поиска ПИН-код за достъп до картата.

3. Настройки за подписване при Outlook Express

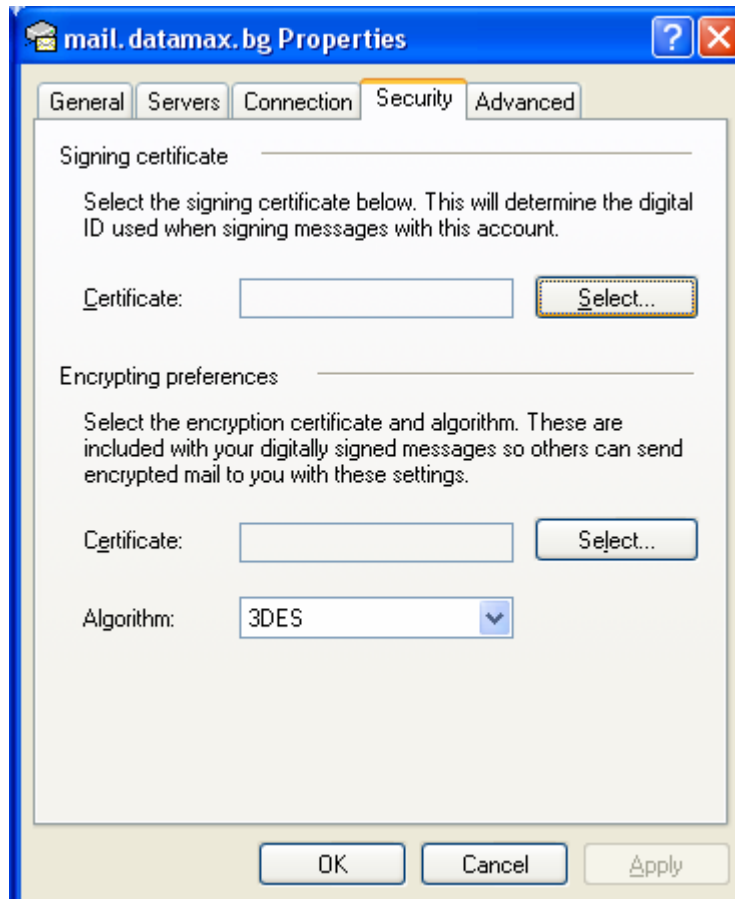
Стартирайте Microsoft Outlook Express. От меню **Tools** изберете **Accounts**



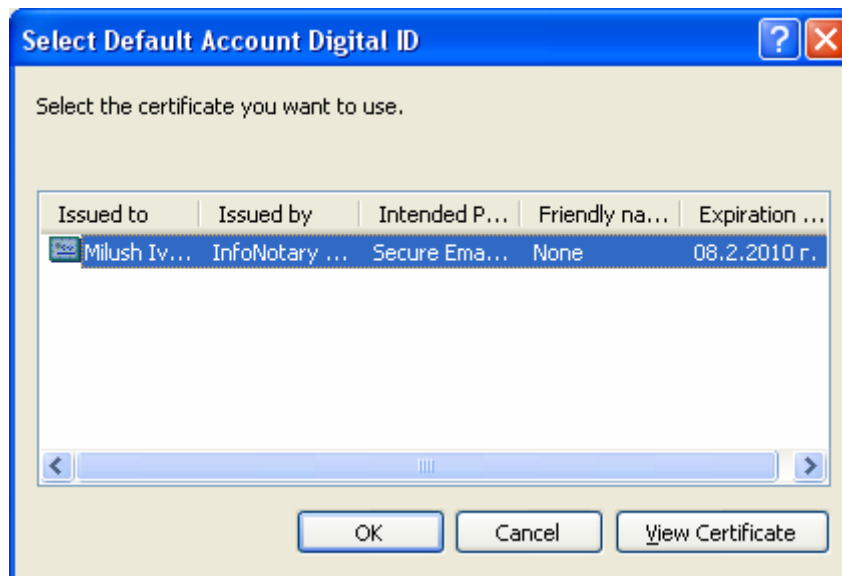
Изберете раздел **Mail** и натиснете бутон **Properties**.



След това изберете раздел **Security** и натиснете бутон **Select**.




Изберете желаното от вас удостоверение, с което ще подписвате кореспонденцията си и потвърдете с **ОК**.



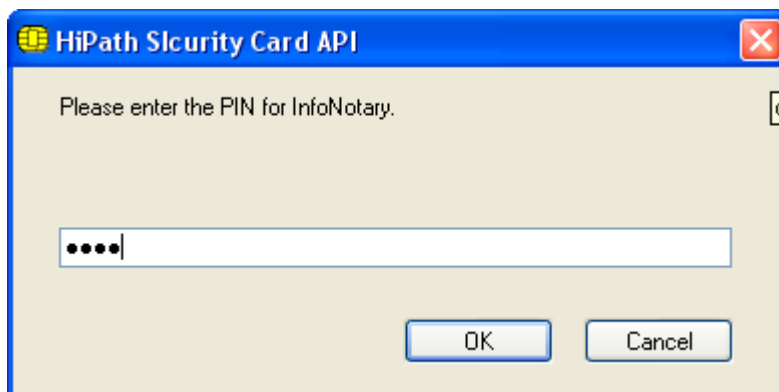
Забележка: Всички останали настройки за Microsoft Outlook Express са аналогични на гореописаните за Microsoft Outlook.

3.1. Как да подписваме e-mail съобщения:


Поставете картата с цифровия сертификат в карточетеца. Съставете нов e-mail както обикновено, евентуално прикачете и файлове.

Натиснете бутона **Sign**  (или изберете от **Tools->Digitally Sign**).

Натиснете бутона **Send**. Следва прозорец, в който трябва да се напише PIN-а на картата.



Инсталация и използване с продукти на Mozilla

	<p>При използването на продукти на Mozilla трябва да знаем, че се използва директен достъп до смарт картата, а не хранилище за удостоверенията. Когато успешно сме инсталирали удостоверенията си в Mozilla Firefox или Mozilla Thunderbird например, НЕ ТРЯБВА да ги трием от там, тъй като това ще доведе и до изтриване на удостоверението, заедно с частния и публичния ключ от смарт картата!</p>
---	--

Преди да започнете работа с вашето удостоверение за електронен подпис е необходимо да инсталирате базовите удостоверения на Инфонотари. Удостоверителната верига можете да намерите в директория "certificates" на инсталационния диск или в Интернет на адрес:

<http://www.infonotary.com/site/files/INotaryCertChain.p12>

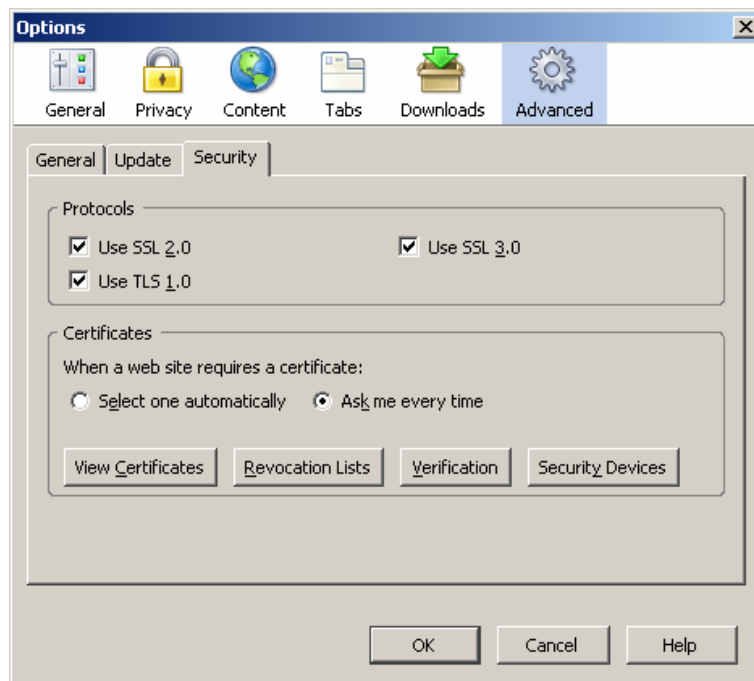
1. Инсталация на удостоверятелната верига на Инфонотари

Продуктите на Mozilla, работещи под Windows, не използват централизираното хранилище за удостоверения на операционната система. Всеки продукт използва собствено хранилище за удостоверения. Това налага отделна инсталация на удостоверятелната верига на Инфонотари за всяко приложение, което ползвате.

Снабдете се с копие на файл "INotaryCertChain.p12" от инсталационния диск или от сайта на Инфонотари.

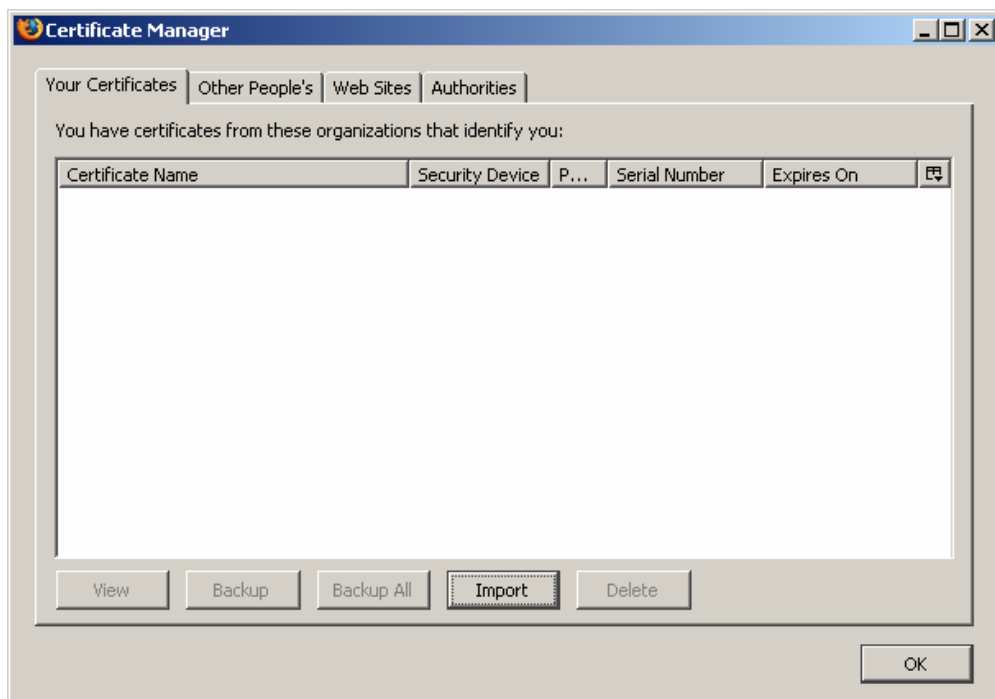
1.1. Инсталация в Mozilla Firefox

Стартирайте браузъра Mozilla Firefox. От меню Tools изберете Options.



Изберете раздел Advanced, подраздел Security, както е показано на картинката и натиснете бутона View Certificates.

От тази точка, процесът на инсталация на удостоверения е аналогичен и за Mozilla Thunderbird.

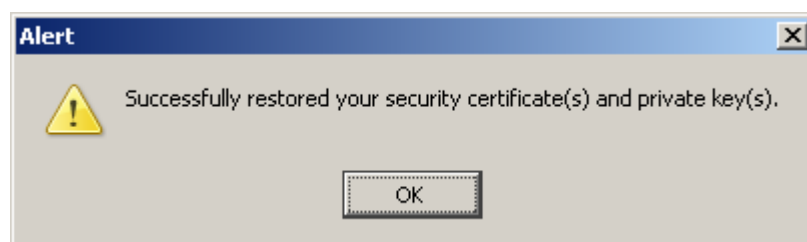


Натиснете бутон Import и посочете пътя до инсталационния файл на удостоверителната верига - INotaryCertChain.p12

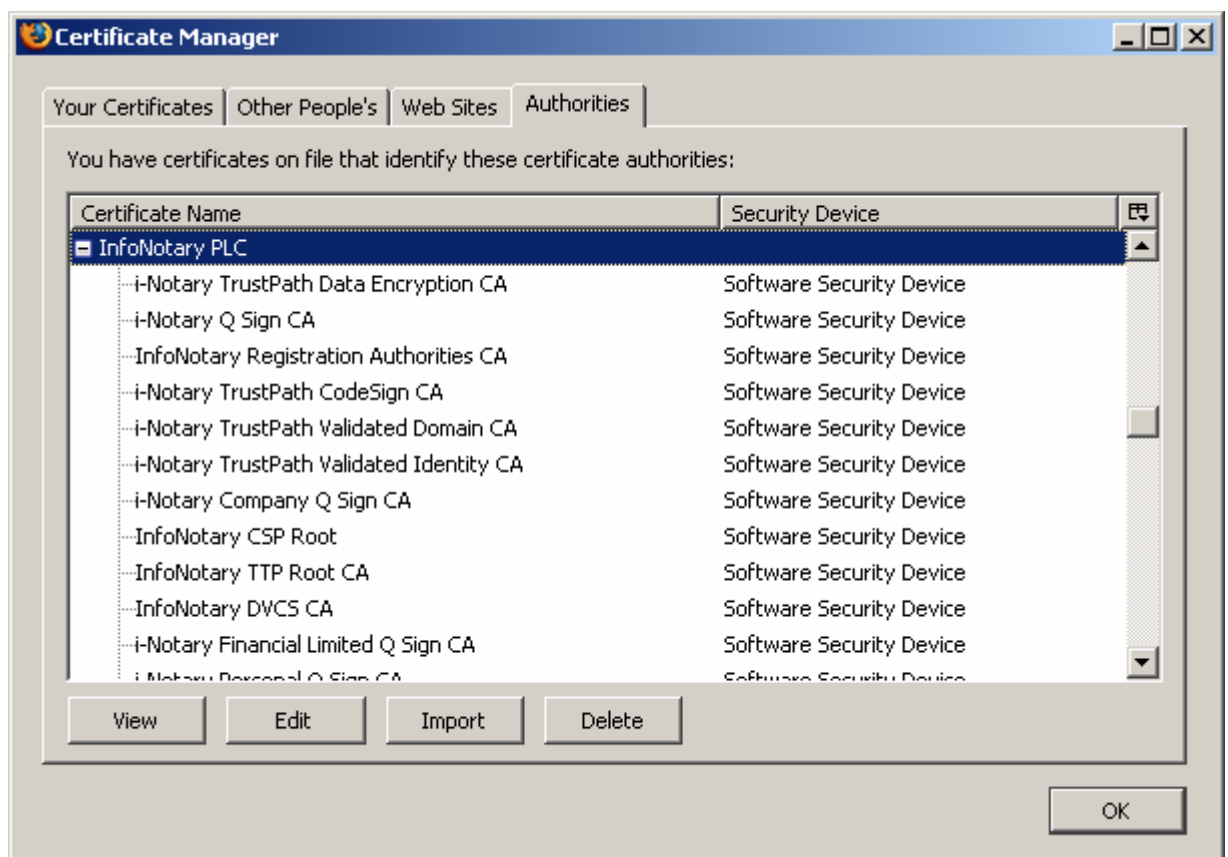
Оставете полето Password празно и натиснете бутон OK.



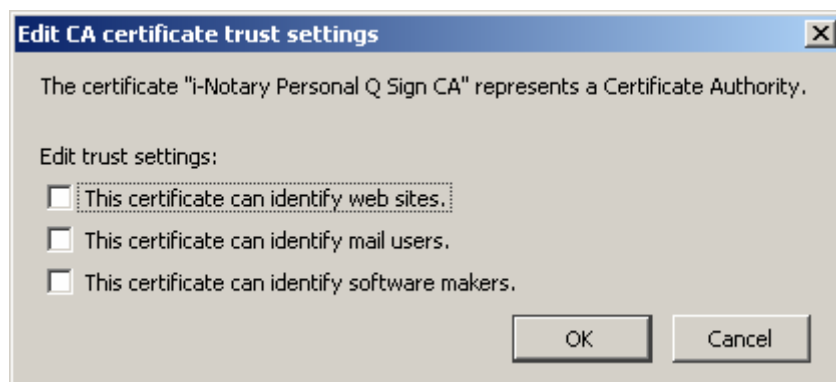
При успешна инсталация на удостоверителната верига излиза съобщение:



Новоинсталираните удостоверения можете да видите в раздел "Authorities":



В продуктите на Mozilla, за всяко удостоверение на удостоверяващ орган (CA), потребителят трябва да избере ниво на доверие. Това става чрез избор на удостоверение и натискане на бутона Edit.

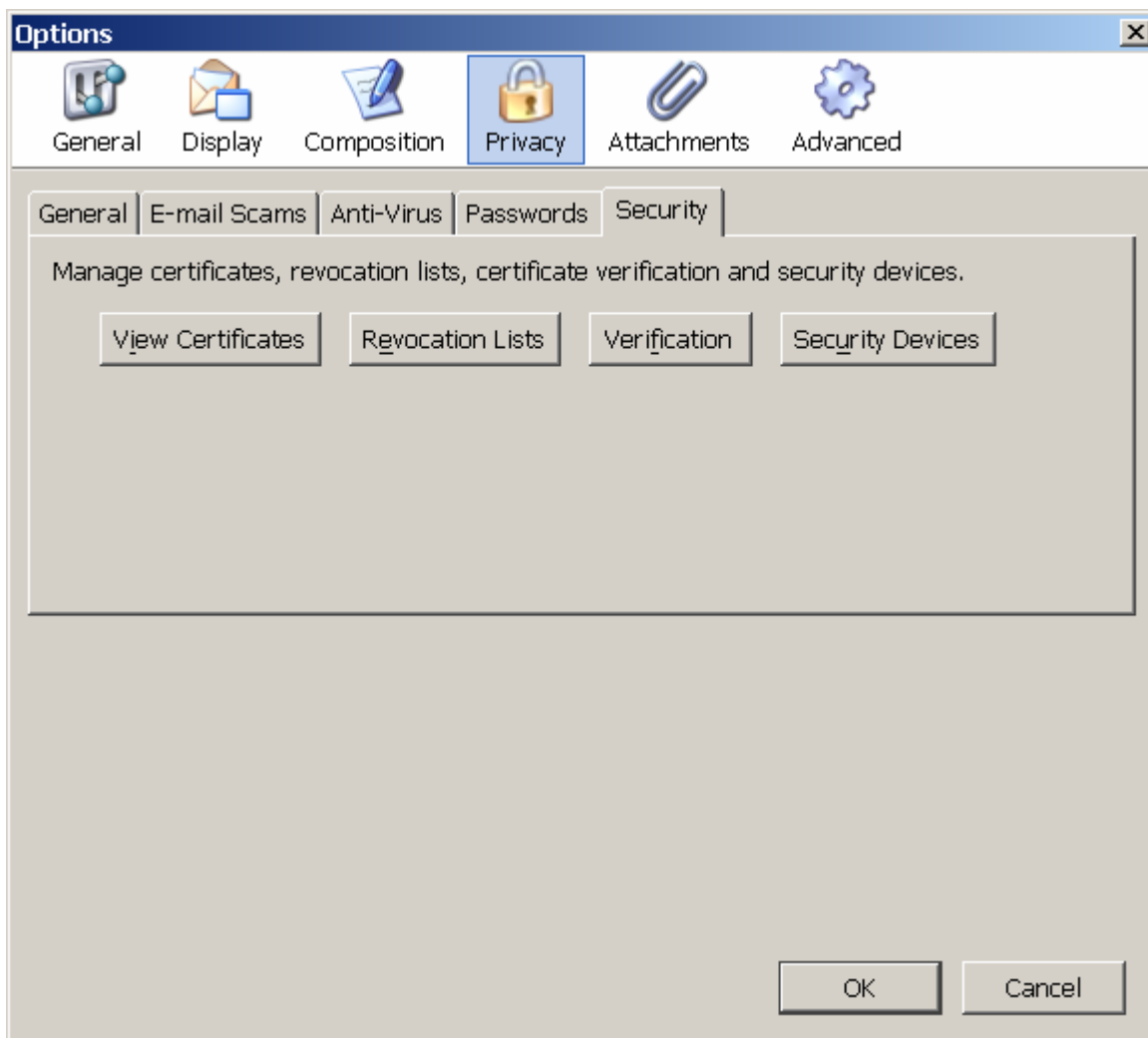


Трябва да направите следното:

- За удостоверението „i-Notary TrustPath Validated E-mail CA” изберете опцията „This certificate can identify mail users”.
- За удостоверението „i-Notary Personal Q Sign CA” изберете опцията „This certificate can identify mail users”.
- За удостоверението „i-Notary Company Q Sign CA” изберете опцията „This certificate can identify mail users”.
- За удостоверението „i-Notary TrustPath Validated Domain CA” изберете опцията „This certificate can identify web sites”.

1.2. Инсталация в Mozilla Thunderbird

Стартирайте пощенския клиент Mozilla Thunderbird. От меню Tools изберете Options.



Изберете раздел Privacy, подраздел Security, както е показано на картинката и натиснете бутона View Certificates.

От тази точка, процесът на инсталация в Thunderbird е аналогичен на процеса във Firefox. Моля вижте точка „1.1. Инсталация в Mozilla Firefox“

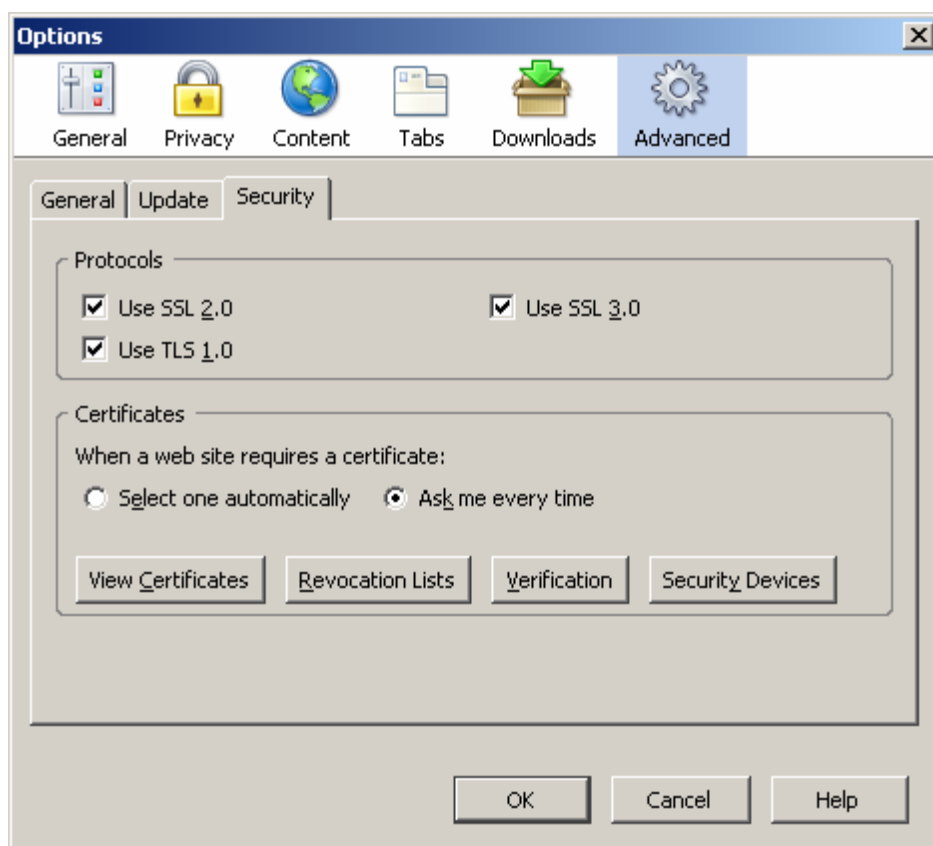
2. Инсталация на хардуерен криптографски модул

За да използвате вашето удостоверение за електронен подпис в базираните на Mozilla програми като Firefox, Thunderbird и др. трябва да регистрирате криптографски

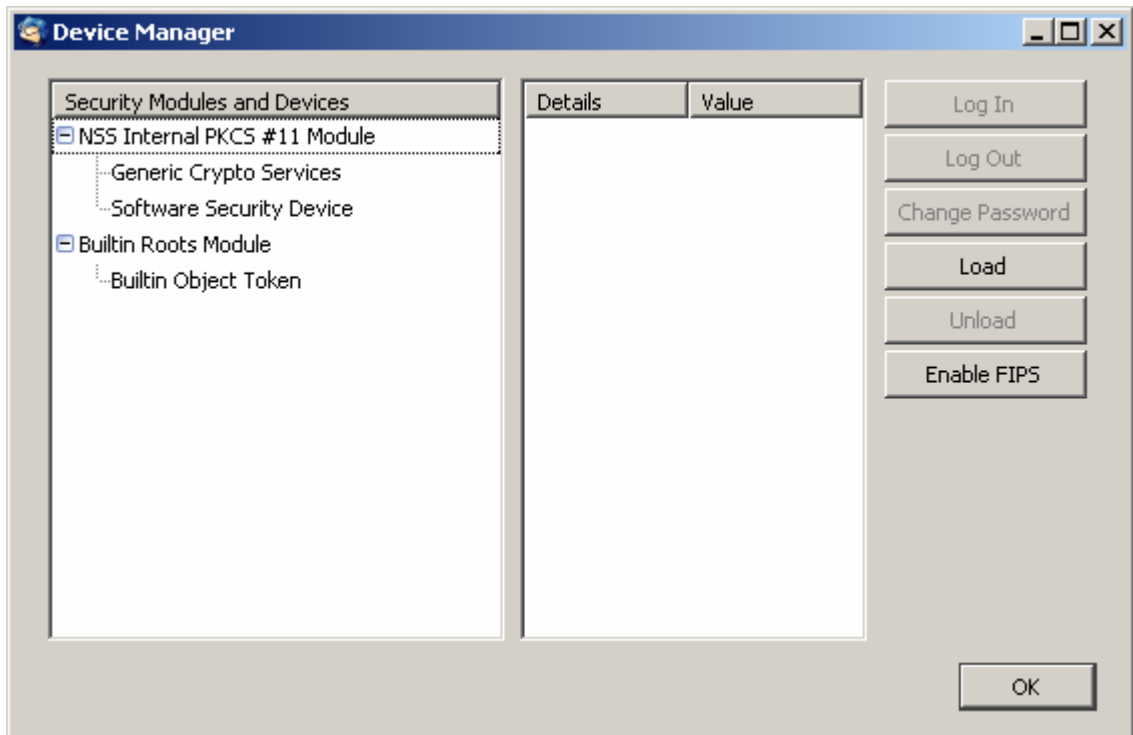
PKCS#11 модул съответстващ на използваната от вас смарт карта. Необходимо е предварително да сте инсталирали драйвера за картата за да пристъпите към регистрацията.

2.1. Инсталация в Mozilla Firefox

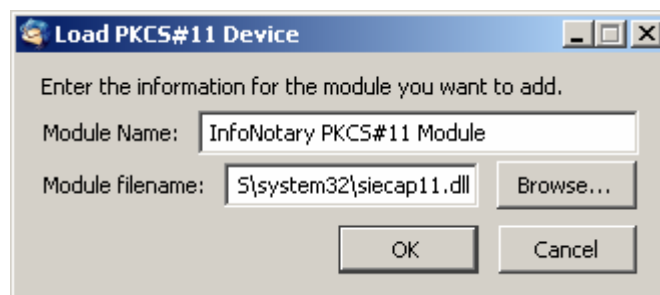
Стартирайте Mozilla Firefox. От меню Tools изберете Options.



Изберете раздел Advanced, подраздел Security, както е показано на картинката и натиснете бутона Security Devices.



За да добавите ново устройство изберете бутона Load

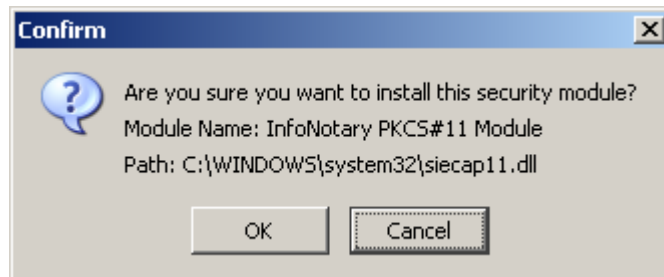


Променете името на модула (Module Name), както желаете.

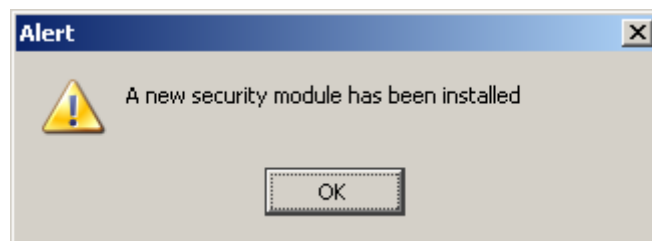
Изберете PKCS#11 библиотеката, съответстващата на вашата смарт карта.

За Siemens това е файл WINDOWS\system32\siecap11.dll

Ако сте избрали правилния модул, ще излезе диалог за потвърждаване, подобен на показания:



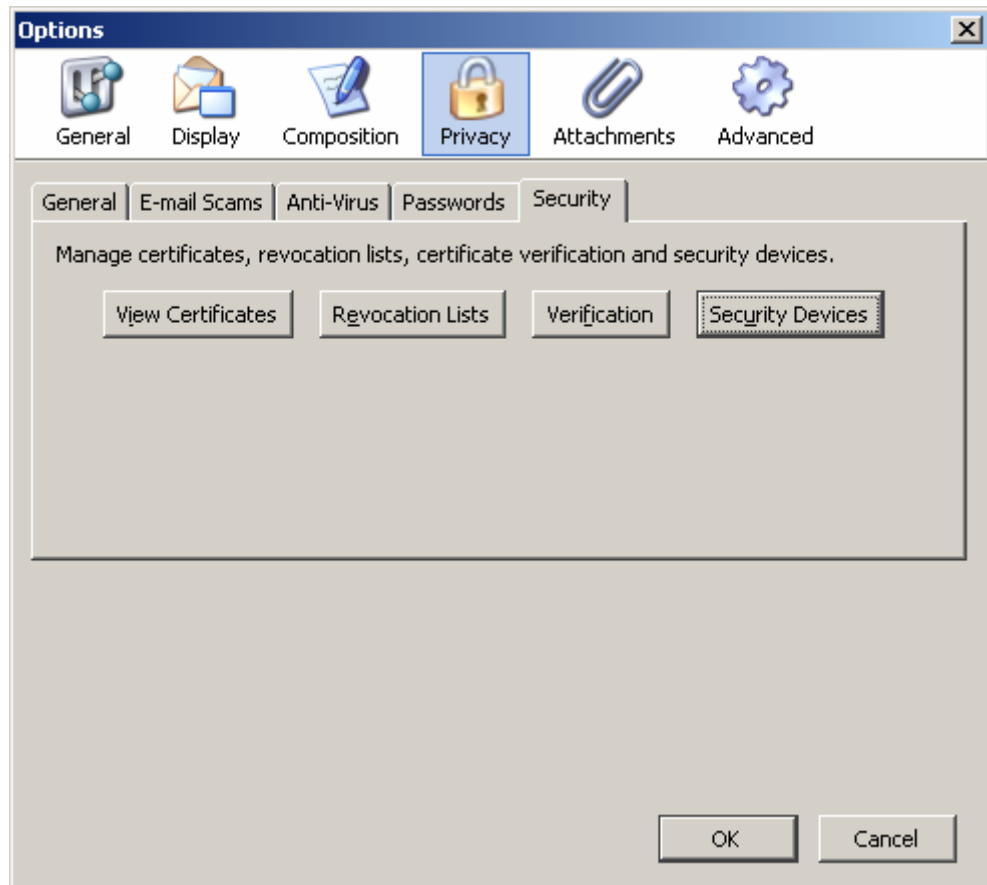
Изберете ОК за потвърждаване на операцията по добавяне на модула.



След като натиснете ОК вашата смарт карта ще се появи в списъка с достъпни устройства.

2.2. Инсталация в Mozilla Thunderbird

Стартирайте Thunderbird и от менюто Tools изберете Options.



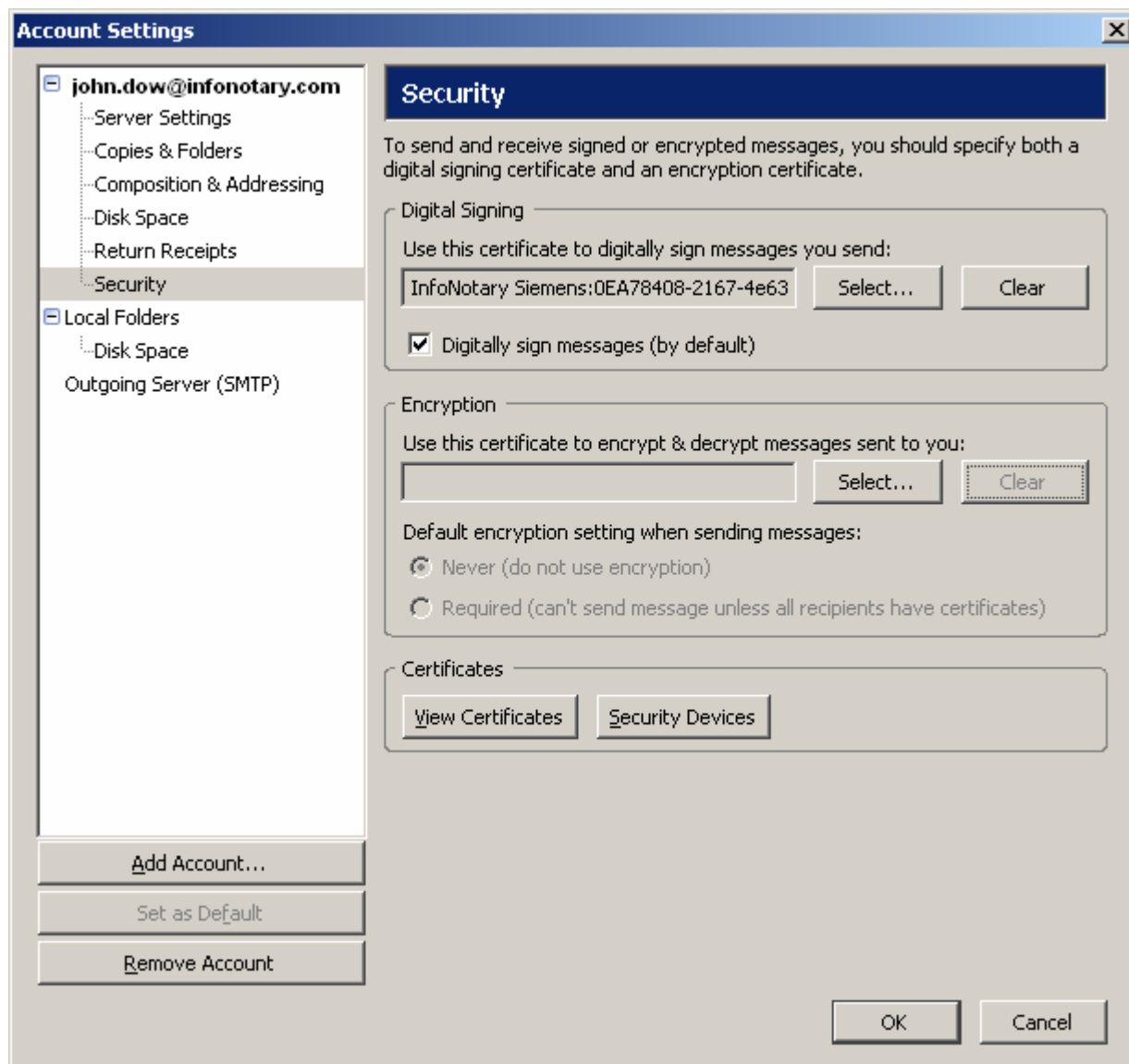
Изберете раздел Privacy, подраздел Security, както е показано на картинката и натиснете бутона Security Devices.

От тази точка, процесът на инсталация в Thunderbird е аналогичен на процеса във Firefox. Моля вижте точка „2.1. Инсталация в Mozilla Firefox“

3. Настройка на потребителския профил в Mozilla Thunderbird

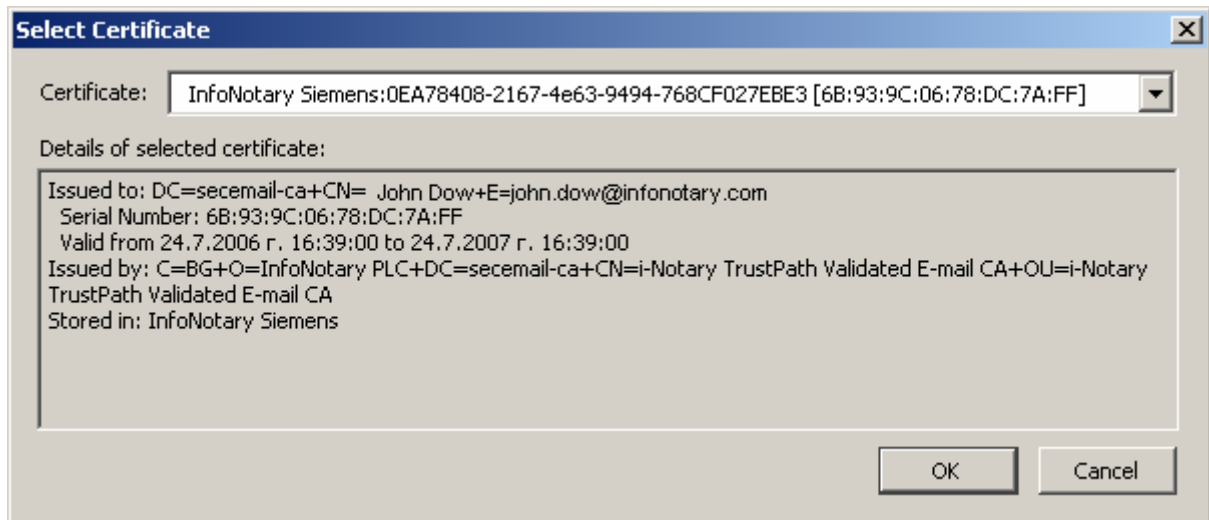
За да може да подписвате вашата изходяща електронна поща трябва да асоциирате потребителския си профил (account) с удостоверението за електронен подпис, записано на смарт-картата. Това става по следния начин:

Изберете меню Tools > Account Settings > Security, както е показано:



Изберете бутон Select... от графата Digital Signing.

Появява се прозорец за избор на удостоверение:



Изберете, желаното от вас удостоверение от смарт-картата и потвърдете с ОК.

Ако е избрана опцията Digitally sign messages (by default), всяко изпратено съобщение ще бъде подписано с избраното удостоверение.

Thunderbird ще ви предложи да използвате същото удостоверение и за декриптиране на съобщения изпратени към вас. Ако откажете може да зададете удостоверение за декриптиране на електронна поща от Select в графата Encryption. Имайте предвид, че не всички удостоверения могат да се използват за криптиране и декриптиране. Тези възможности зависят от типа на вашето удостоверение.