ИНФОРМАЦИОННО ОБСЛУЖВАНЕ

1504 София, ул. Панайот Волов № 2
Тел.: 02/ 9420 340, факс: 02/ 943 66 07
office@is-bg.net www.is-bg.net
ЕИК: 831641791

Практическо ръководство за конфигуриране и работа с Удостоверение за електронен подпис с клиента за електронна поща Mozilla Thunderbird

РЪКОВОДСТВО НА ПОТРЕБИТЕЛЯ – версия 3.0.0

Това ръководство е предназначено за потребители, притежаващи следния тип смарт карти:

- **Setec** - управляват се от софтуера **SetWeb.** Картите от този тип имат индексен номер **XXXXXXXXs**;
- **Charismathics** - управляват се от софтуера **Charismathics**. Всички карти от този тип имат индексен номер **CHxxxxx-xxxxxxxxx.**

В момента на изготвяне на ръководството, настоящата версия на клиента е Mozilla Thunderbird 17.0.6.

Съдържание:

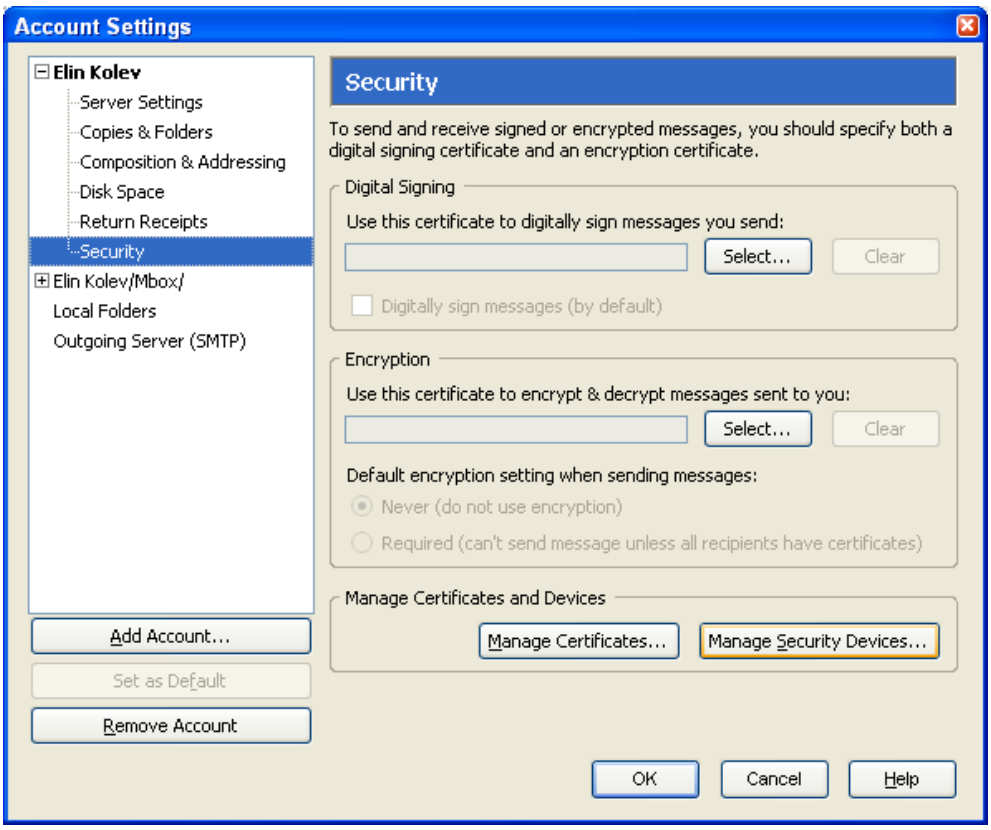
1. Инсталиране и настройка

1.1 Инсталиране на модул за управление на смарт картата/защитено устройство/

Забележка: За да подписвате със Вашия сертификат, e-mail адресът записан в съдържанието на сертификата трябва да е идентичен с този, който е настроен в пощенския акаунт.

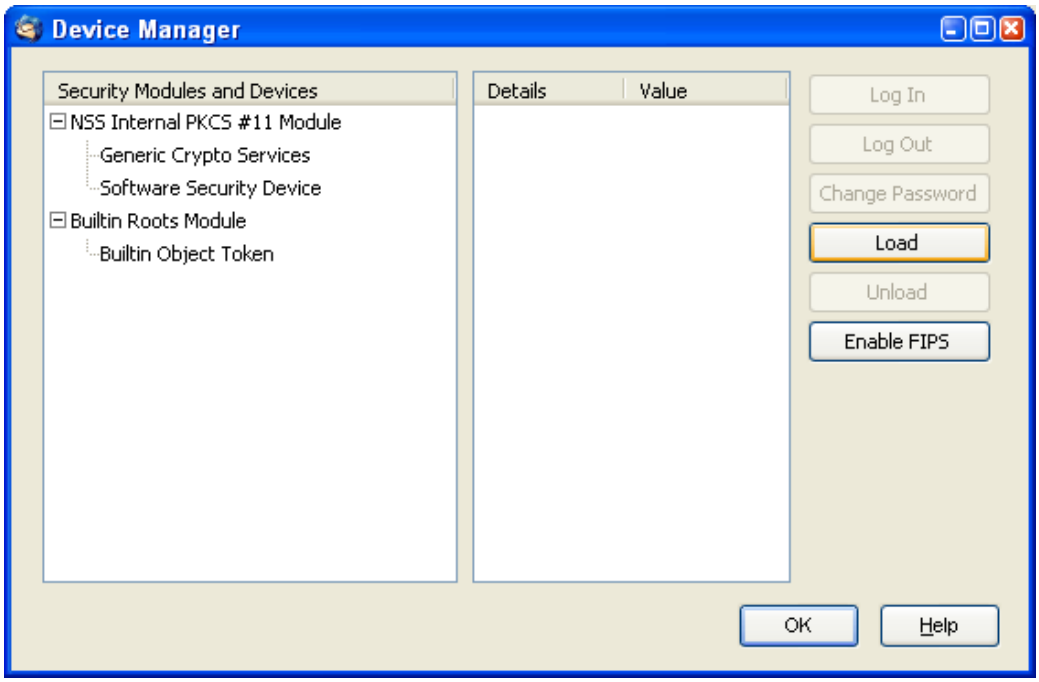
След като сте добавили вашия пощенски акаунт със съответните настройки за "**Pop3**" и „**SMTP**" сървъри следва да инсталирате сертификатите, като следвате последователността от действия:

- Изберете последователно „**Tools**", "**Accounts Settings**" и изберете вашия акаунт. Изберете секцията „**Security". /фиг. 1.1.1**/.



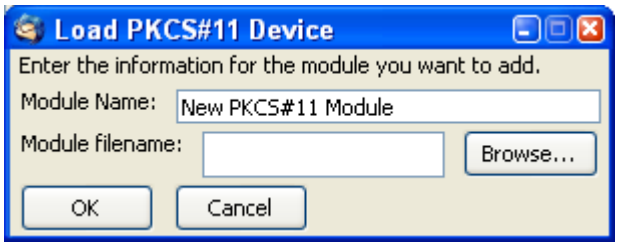
(фиг. 1.1.1)

- натиснете върху бутона „**Manage Security Devices…**”. Ще ви се отвори прозорец подобен на този от **фиг. 1.1.2**



фиг. 1.1.2

- за да добавите ново защитено устройство, натиснете бутона „**Load**” и следвайте последователността, посочена по-долу.



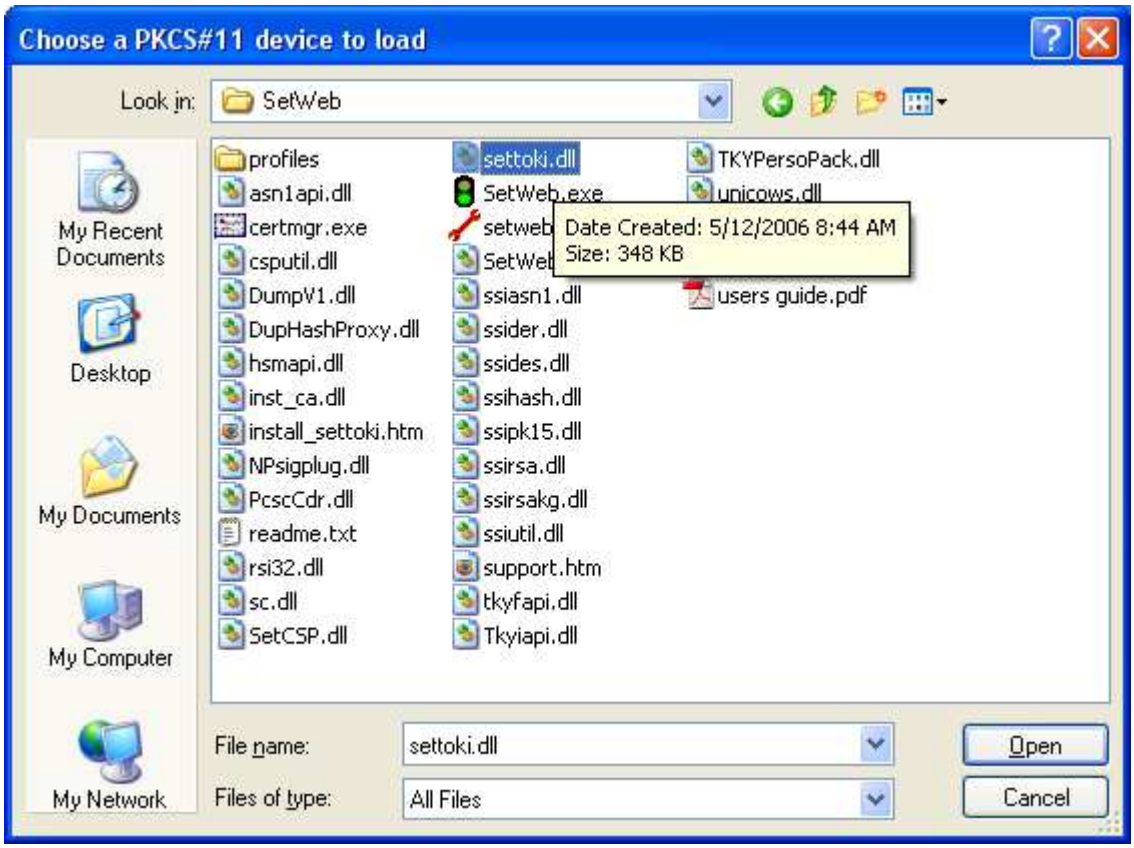
/фиг. 1.1.3/

- по желание можете да зададете име на защитеното устройство в полето **<Module Name>** и натиснете бутона <**Browse… фиг. 1.1.3**>

Забележка:

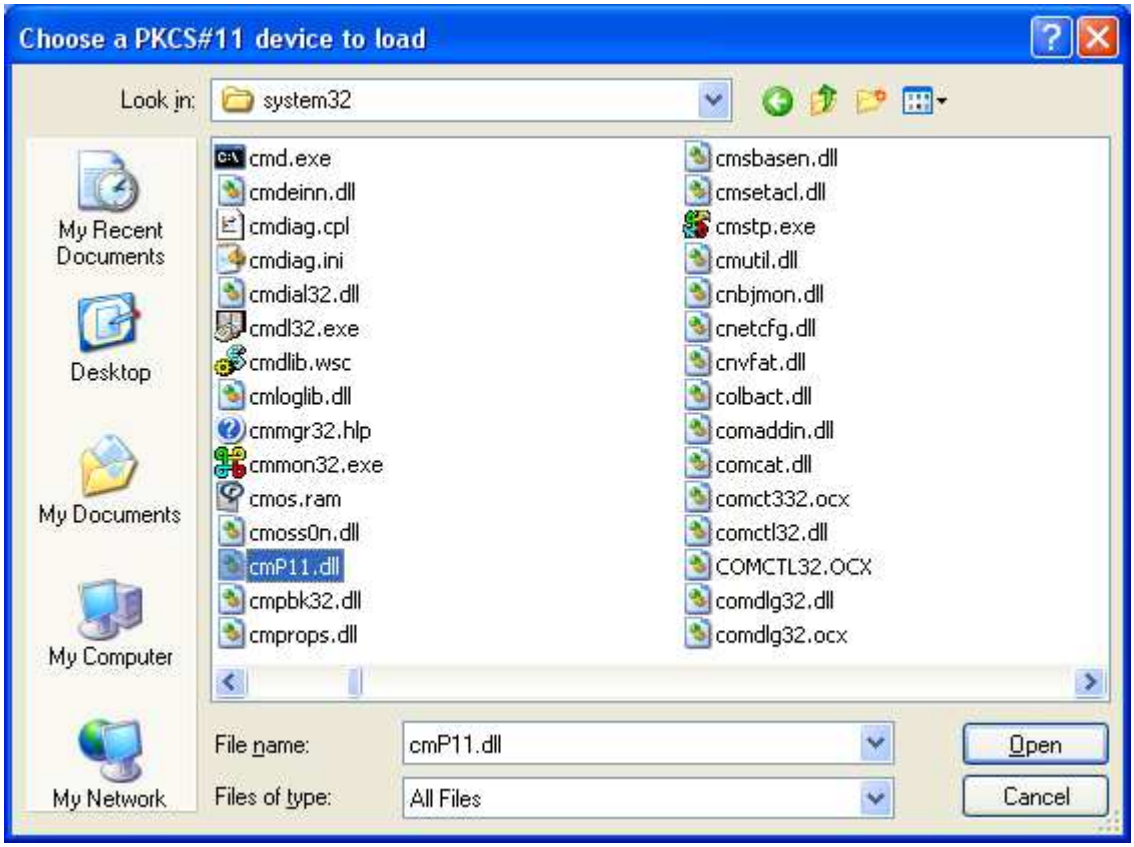
- Ако работите със смарт карта Setec, намерете и изберете файл **<settoki.dll>**, който се намира по подразбиране в папка **C:\Program Files\SetWeb** (**или където е инсталиран софтуера SetWeb**) - **фиг. 1.1.4**
- Ако вашата смарт карта се управлява от софтуера **Charismathics /**проверете дали индексния номер е **CHSI43BP15-xxxxxxxxx/**, намерете и изберете файла **<cmP11.dll>**, който се намира в папка **..\WINDOWS\system32** - **фиг. 1.1.5.**

Ако работите и с двата типа смарт карти, последователно добавете и двете устройства.



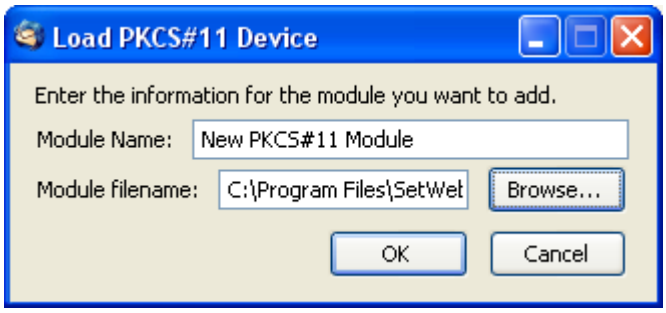
фиг. 1.1.4

- натиснете бутона <**Open**>



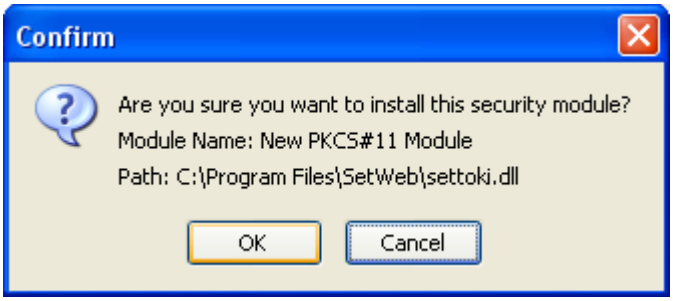
фиг. 1.1.5

- натиснете <**OK**>



фиг. 1.1.6

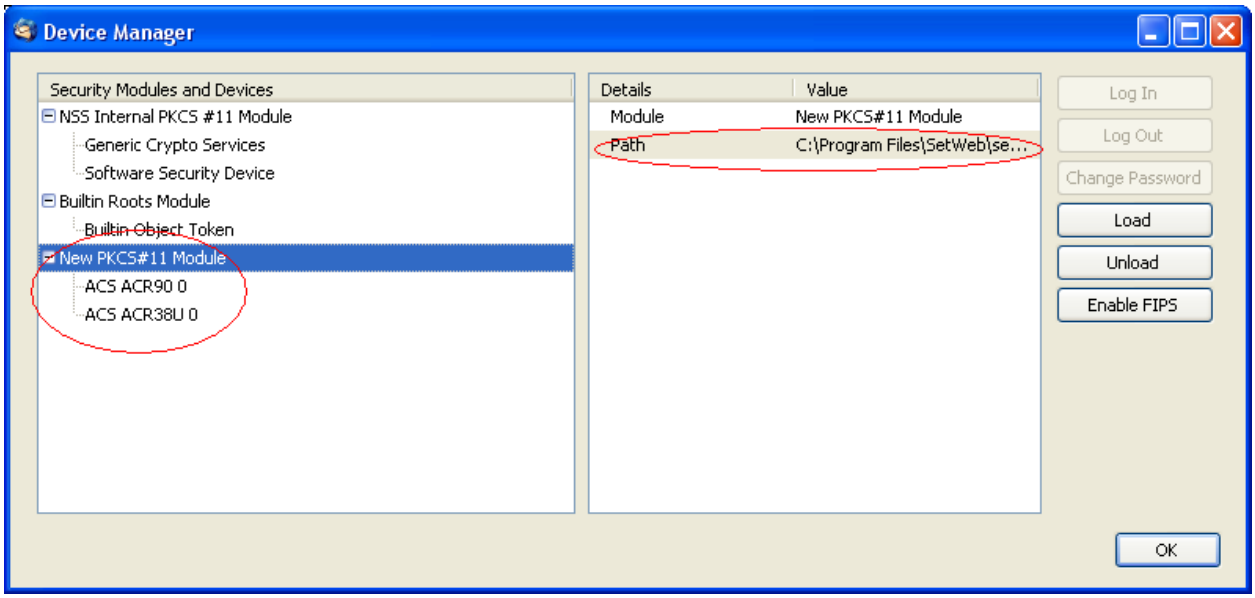
- потвърдете <**OK**>



фиг. 1.1.7

фиг. 1.1.8

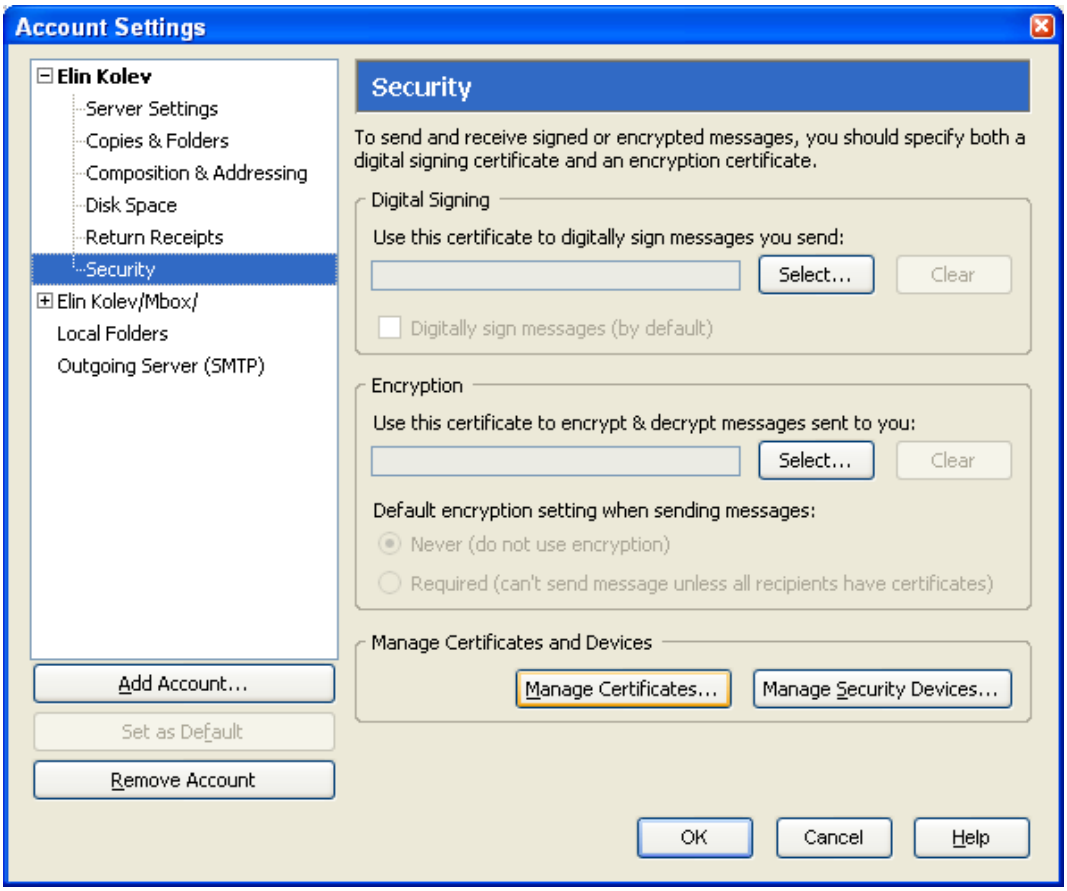
- След коректна инсталация трябва да видите екран подобен на този от **фиг. 1.1.8** и **фиг. 1.1.9**



фиг. 1.1.9

1.2. Инсталиране на сертификатите

Поставете смарт картата с Вашия сертификат в карточетящото устройство и натиснете бутона <**Manage Certificates…**> /**фиг. 1.2.1**/.

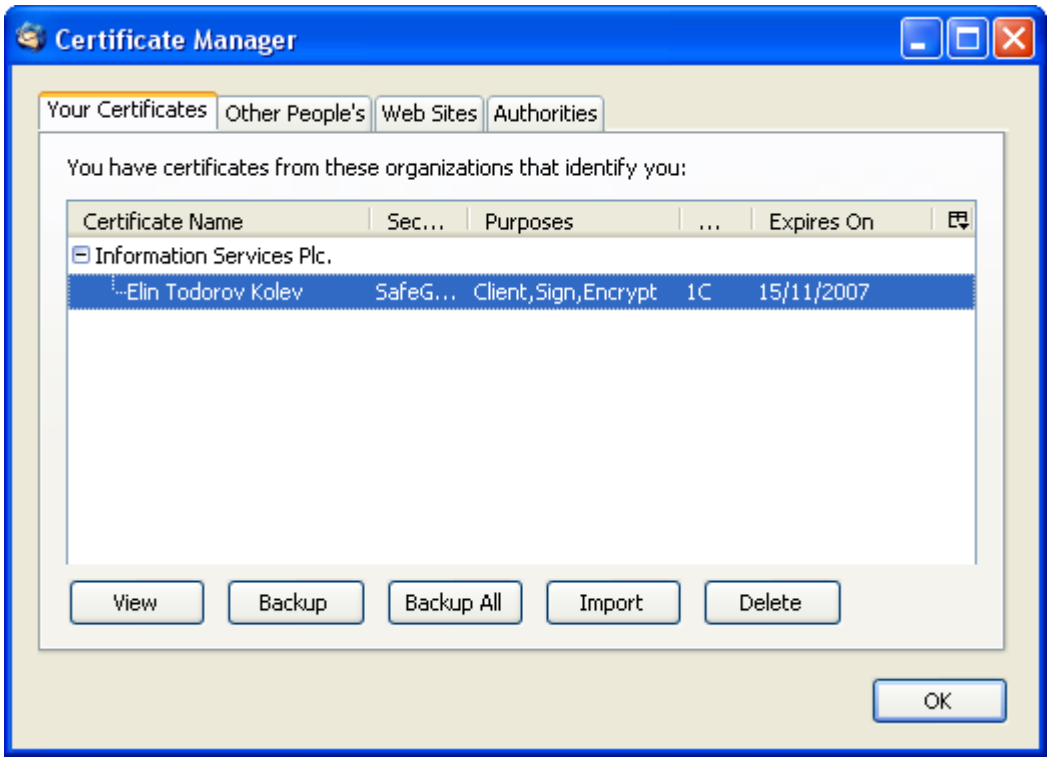


фиг. 1.2.1

- Въведете ПИН кода на смарт картата, който я защитава от неоторизиран достъп **/фиг. 1.2.2/**

фиг. 1.2.2

- Вашия сертификат е инсталиран успешно ако виждате прозорец подобен на този от **фиг. 1.2.3**

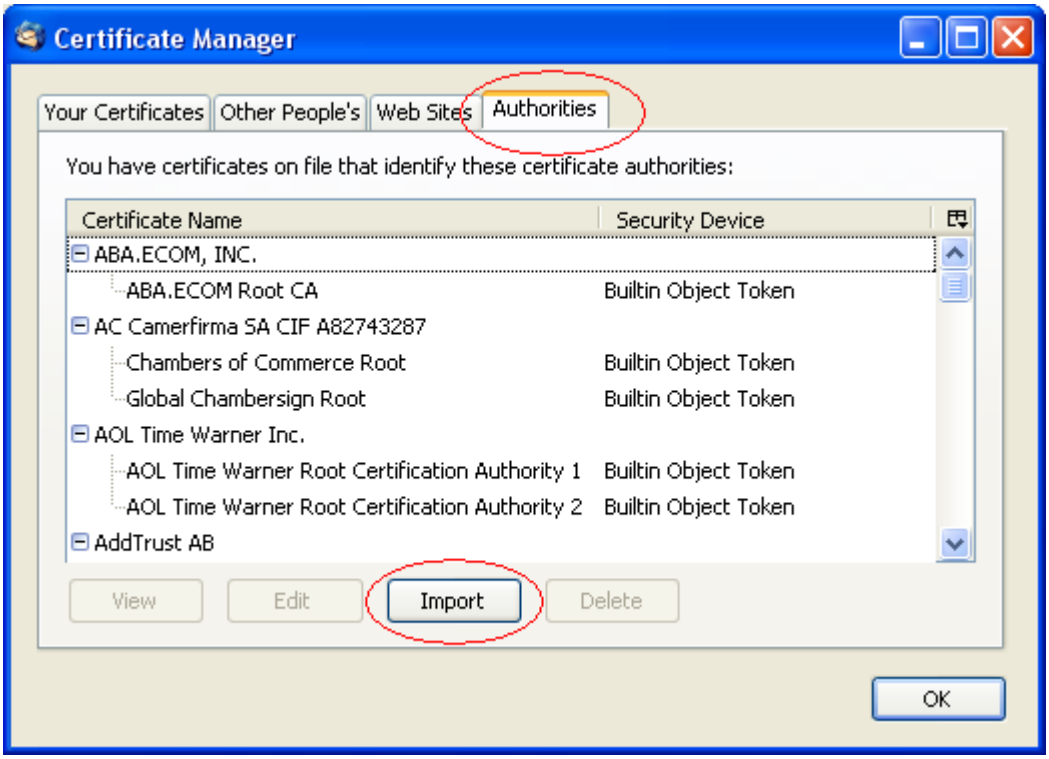


фиг. 1.2.3

!!!Забележка: Не използвайте бутона <Delete>. Това ще доведе до изтриване на вашия сертификат от смарт картата.

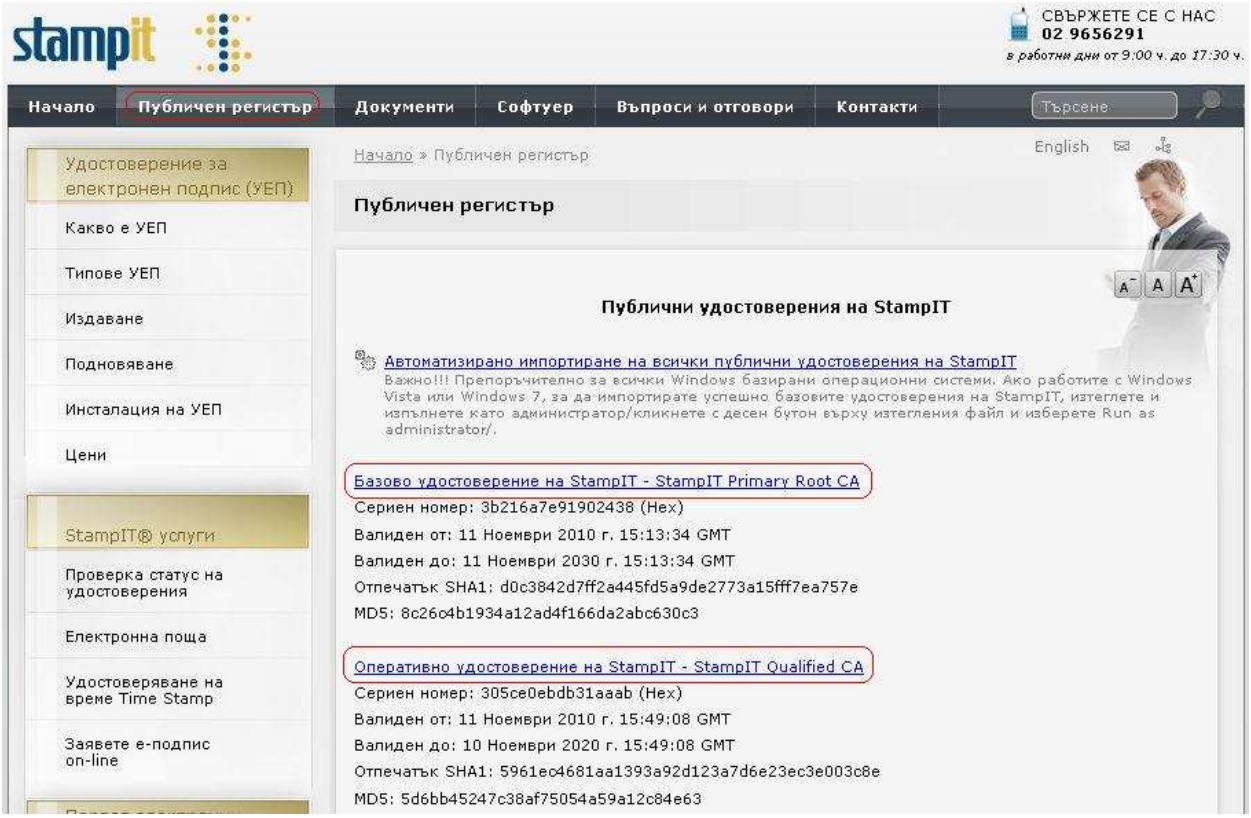
- Следващата стъпка е да инсталирате Удостоверенията на Доставчика на удостоверителни услуги. Изпълнете следните стъпки:

Натиснете <**Authorities**> **tab** и след това бутона <**Import**> **фиг. 1.2.3**



фиг. 1.2.3

- Изберете Базово удостоверение за електронен подпис на Доставчика на удостоверителни услуги **<StampIT Primary Root CA>**, което следва да изтеглите от www.stampit.org, секция **<Публичен регистър>** и го инсталирайте както е показано на фигурите.**/фиг. 1.2.4, фиг. 1.2.5/**

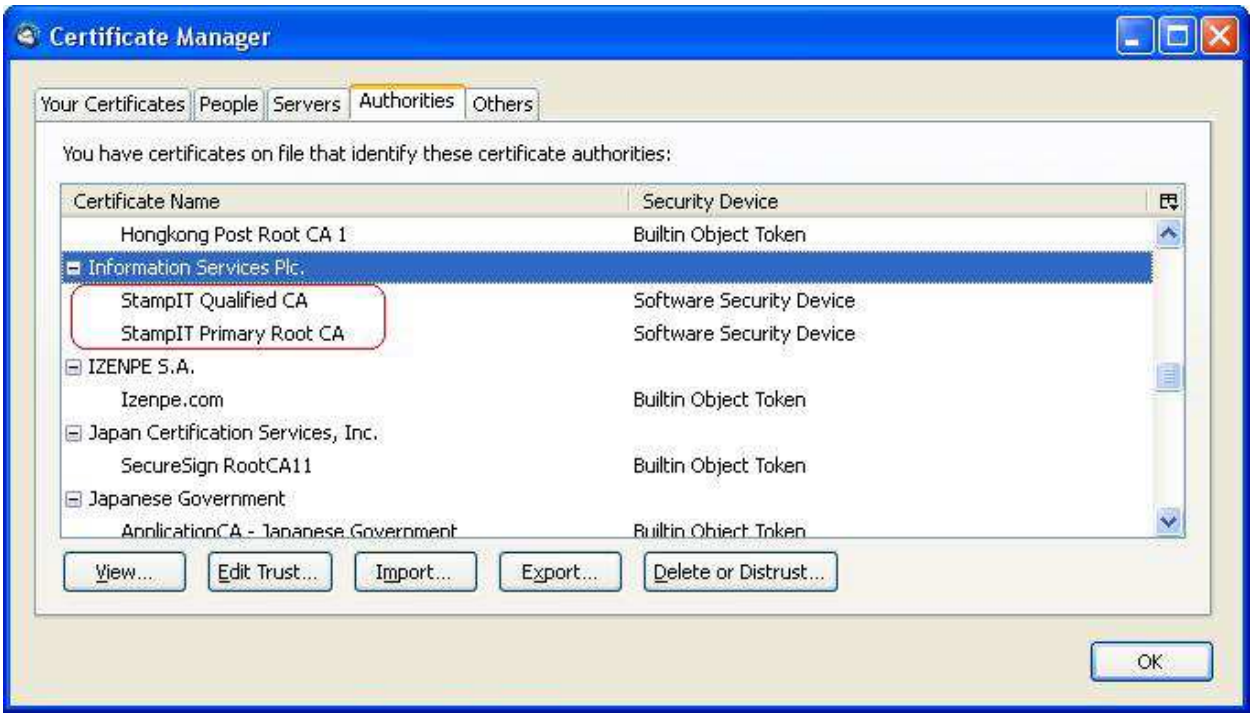


фиг. 1.2.4

фиг. 1.2.5

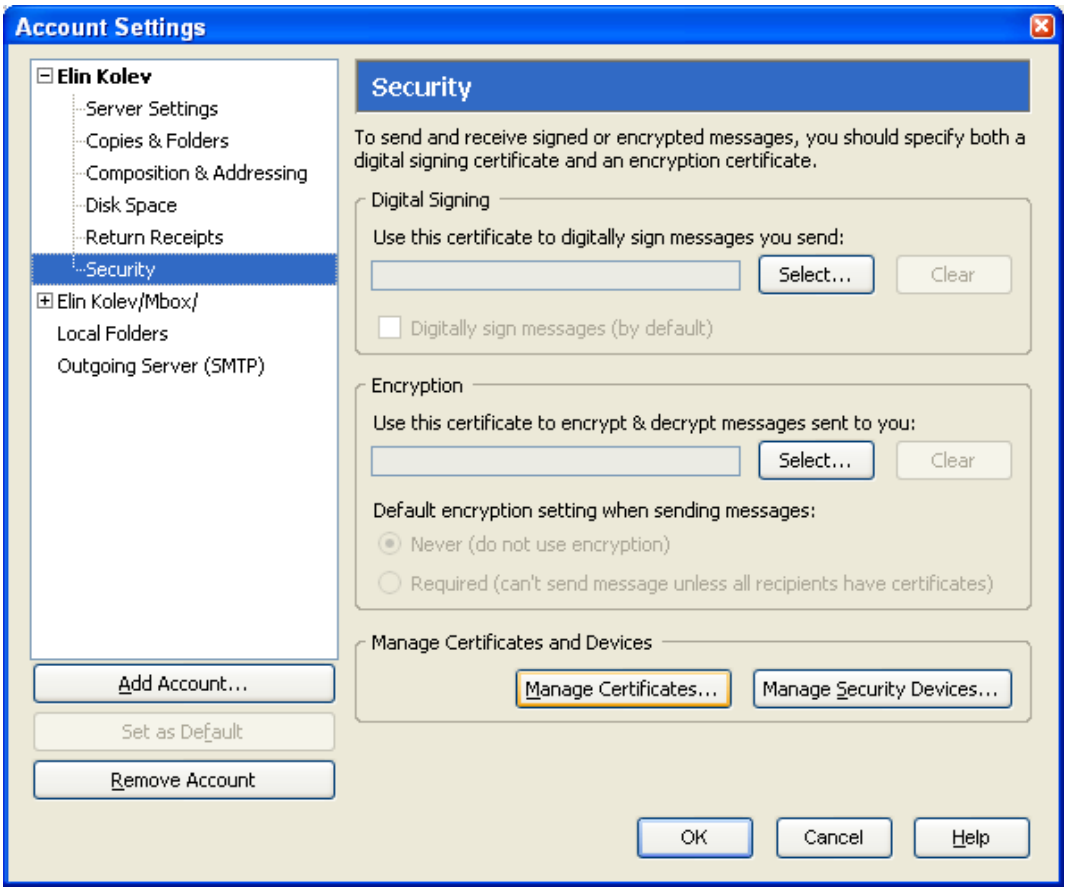
По аналогичен начин инсталирайте оперативното удостоверение **<StampIT Qualified CA>.**

След успешна инсталация в крайна сметка трябва да виждате прозорец подобен на този от фиг. 1.2.6



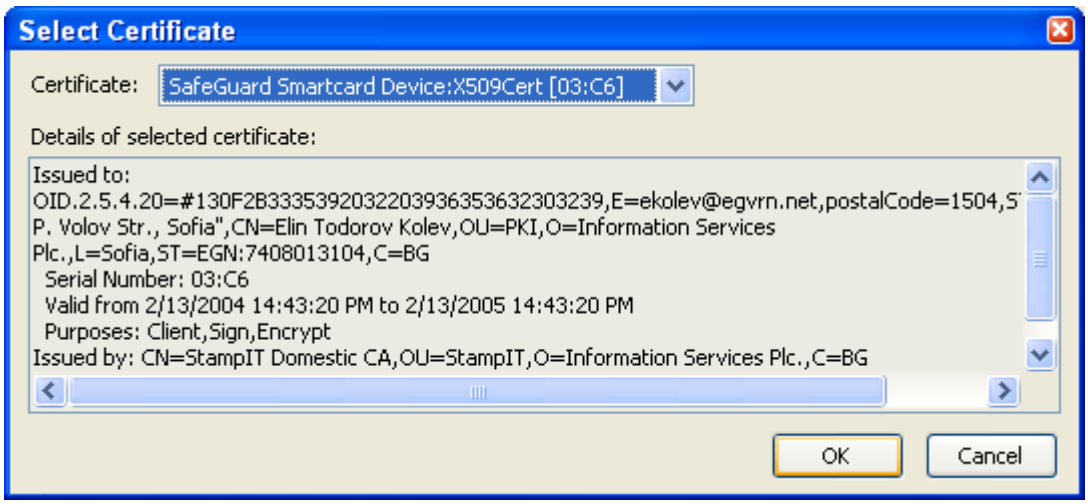
фиг. 1.2.6

- Сега потвърдете с <**ОК**> и ще видите първоначалния прозорец на секцията <**security**> **фиг. 1.2.7**
- Следващата стъпка е да изберете сертификат за подписване и криптиране. Картата трябва да бъде поставена в карточетящото устройство.



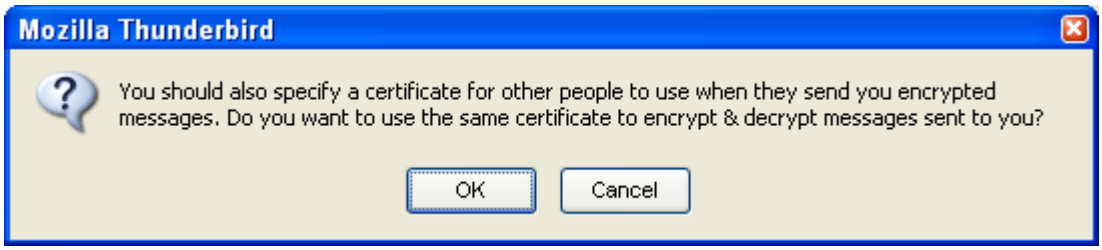
фиг. 1.2.7

- Изберете бутона <**Select....**> от секцията <**Digital Signing**> **фиг. 1.2.7** и следва да се появи прозорец, подобен на този от **фиг. 1.2.8.**



фиг. 1.2.8

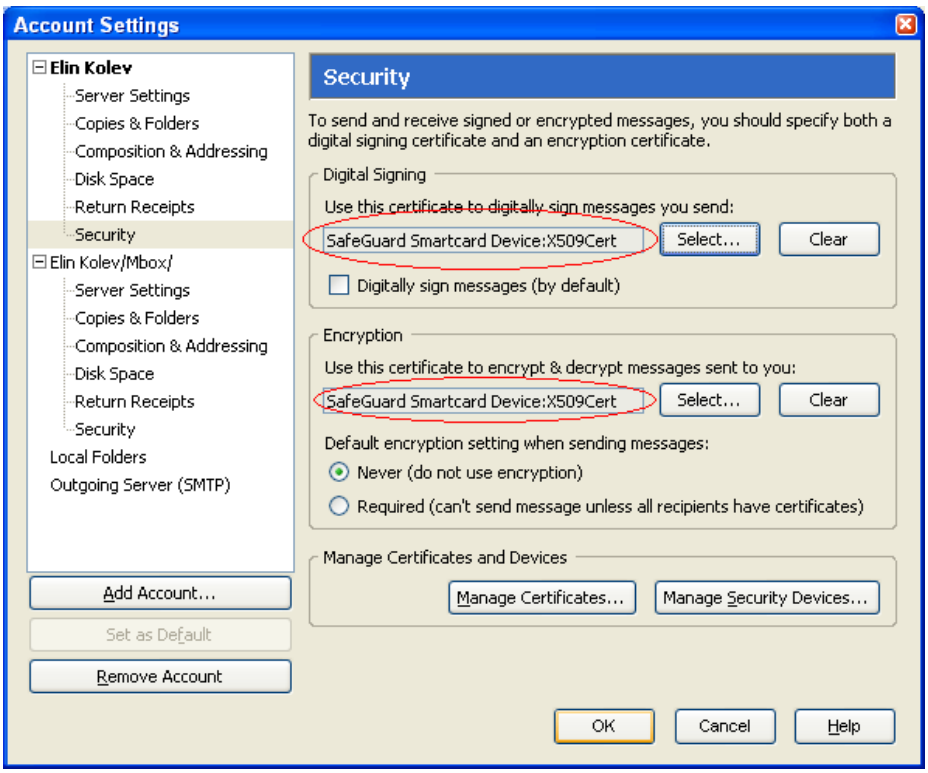
- Потвърдете с <**OK**>



фиг. 1.2.9

- Потвърдете отново с <**ОК**>

Ако инсталацията и селектирането на сертификатите е преминала успешно, трябва да виждате екран подобен на този от фиг. 1.2.10

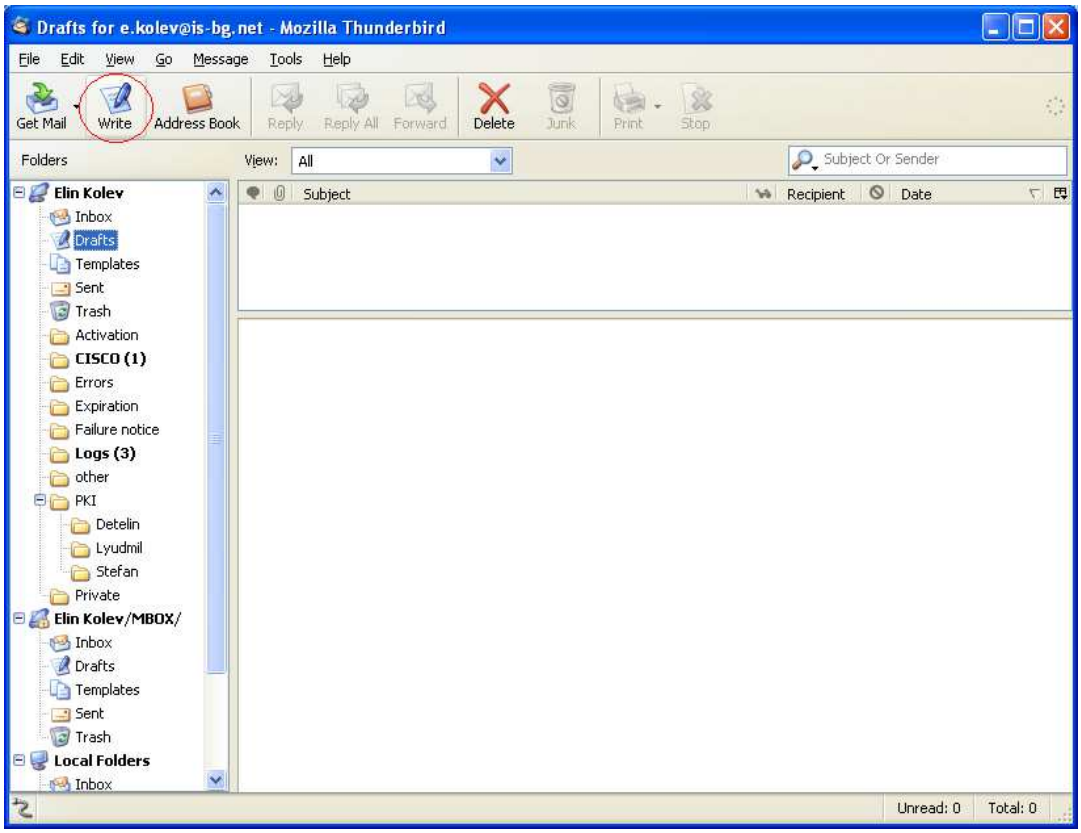


фиг. 1.2.10

2. Подписване на електронни съобщения

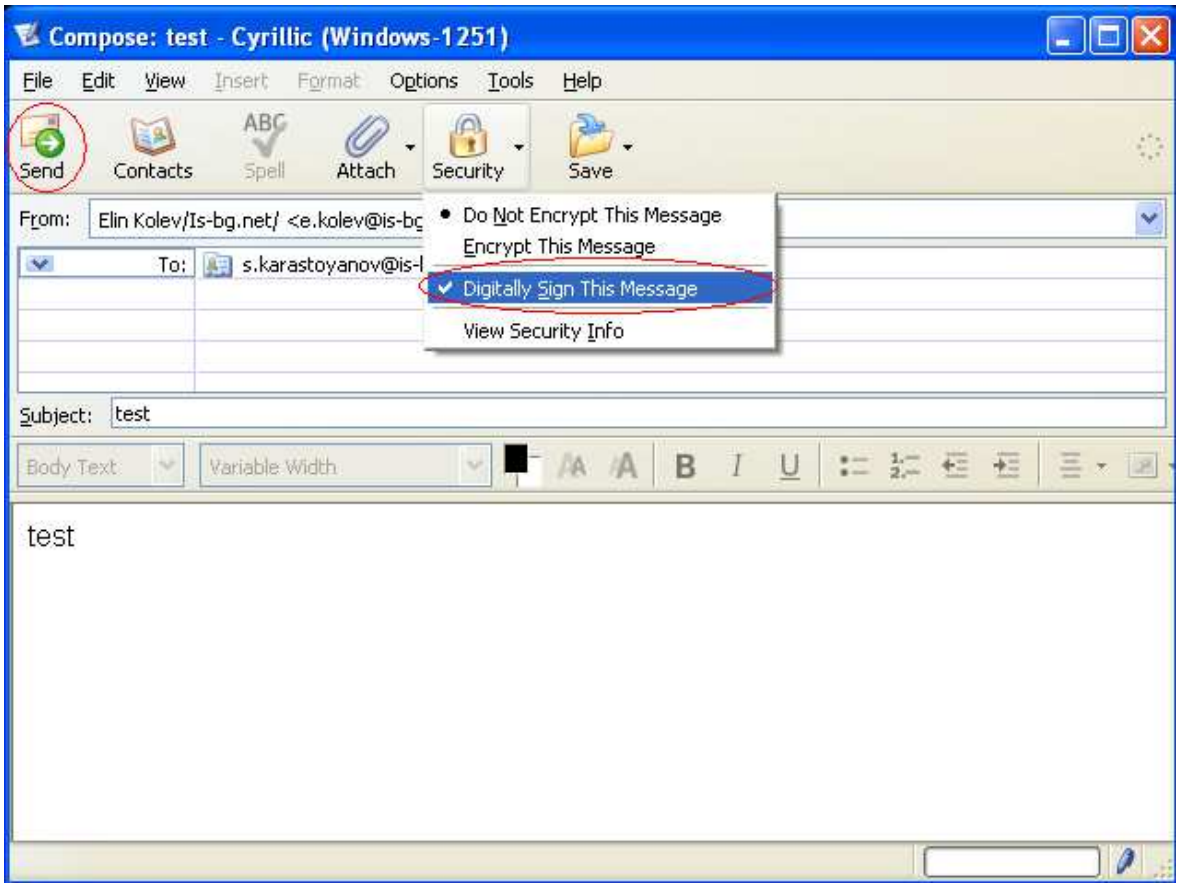
За да подпишете електронно съобщение изпълнете следните стъпки:

- Създайте ново електронно съобщение като натиснете бутона **<Write> фиг.2.1**



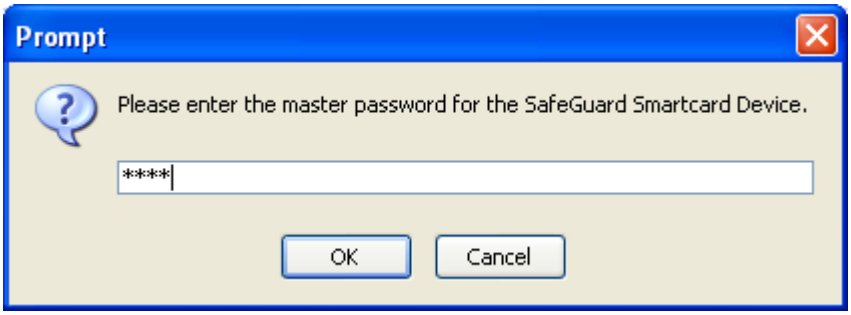
фиг. 2.1

- Въведете необходимите полета за **<To:>, <Subject:>**
- От падащото меню **<Security>** изберете **<Digitally Sign This Message>/ фиг.2.2**
- Поставете смарт картата в карточетящото устройство и натиснете бутона **"Send" фиг.2.2**



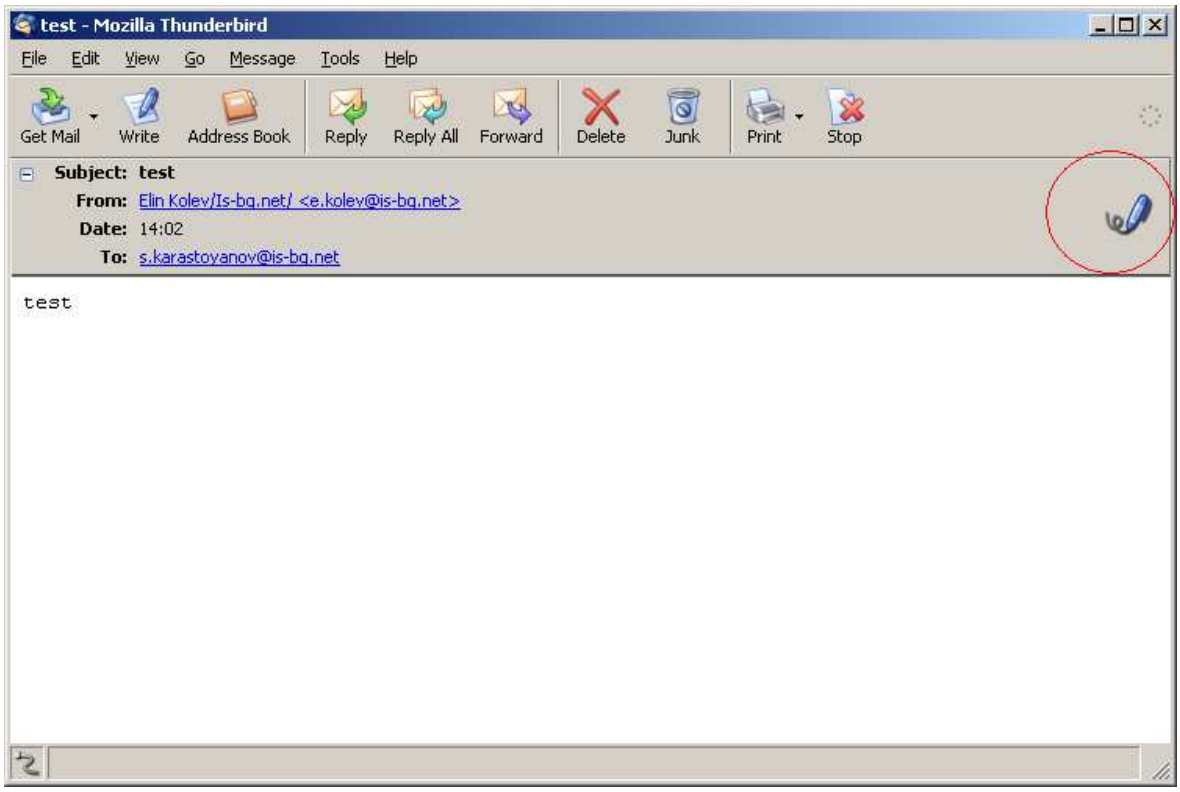
фиг.2.2

- Въведете вашия ПИН код за достъп до смарт картата.**фиг. 2.3**



фиг. 2.3

След въвеждане на ПИН кода и натискане на бутона **<OK>** вашето електронно съобщение би следвало да е успешно подписано и изпратено. Когато адресатът го получи и отвори, следва да види прозорец подобен на този от **фиг.2.3**



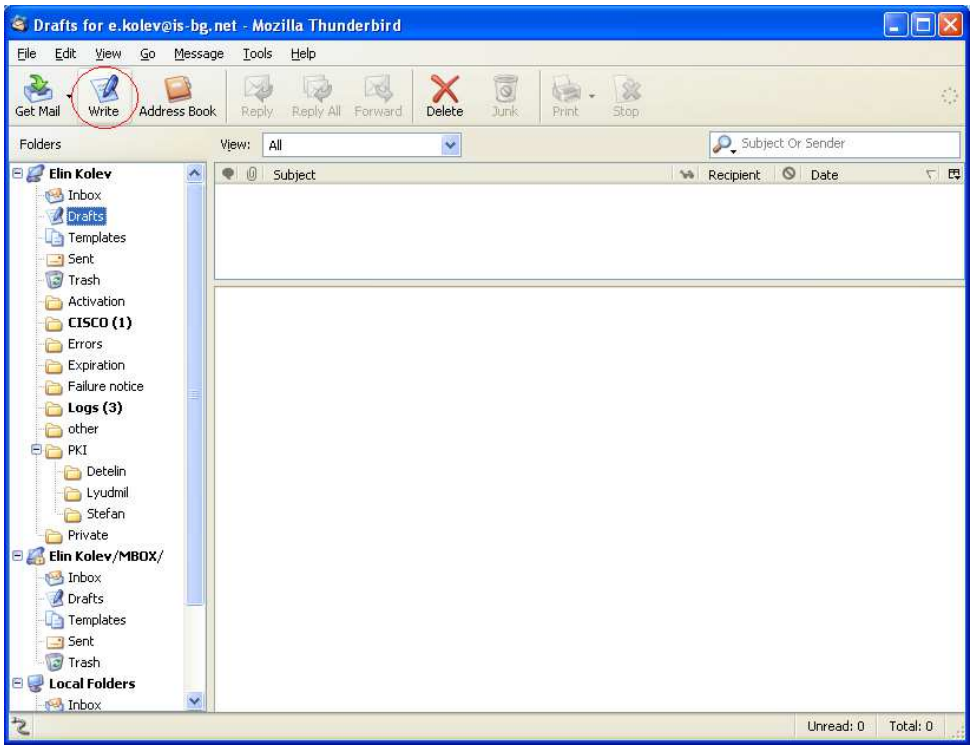
фиг.2.3

3. Криптиране на електронни съобщения

За да криптирате електронно съобщение трябва да имате съхранен публичния ключ на адресата, към който искате да криптирате./**Ако определен адресат Ви изпрати подписано електронно съобщение, "Mozilla Thunderbird" автоматично ще го съхрани/**

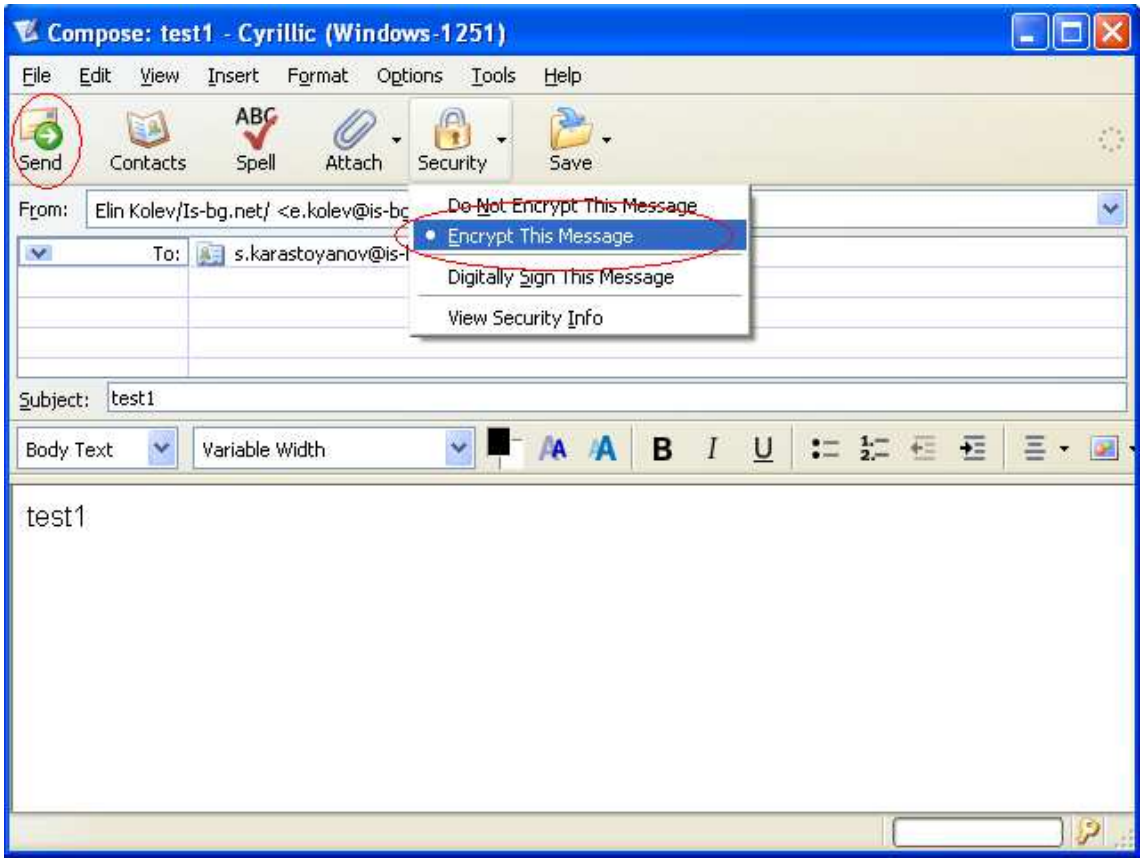
След като имате съхранен публичния ключ изпълнете следните стъпки:

1. Създайте ново електронно съобщение като натиснете бутона **<Write> фиг.3.1**



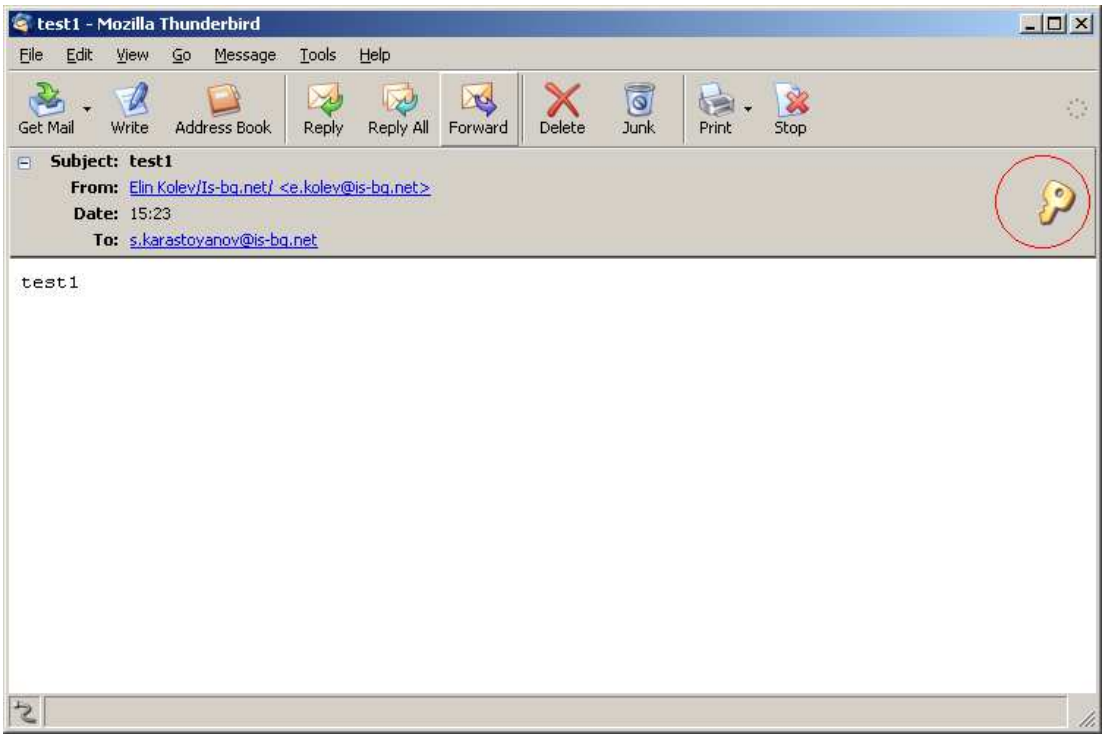
фиг. 3.1

1. Въведете необходимите полета за **<To:>, <Subject:>**
2. От падащото меню **<Security>** селектирайте **<Encrypt This Message>** натиснете бутона **<Send> /фиг. 3.2/**



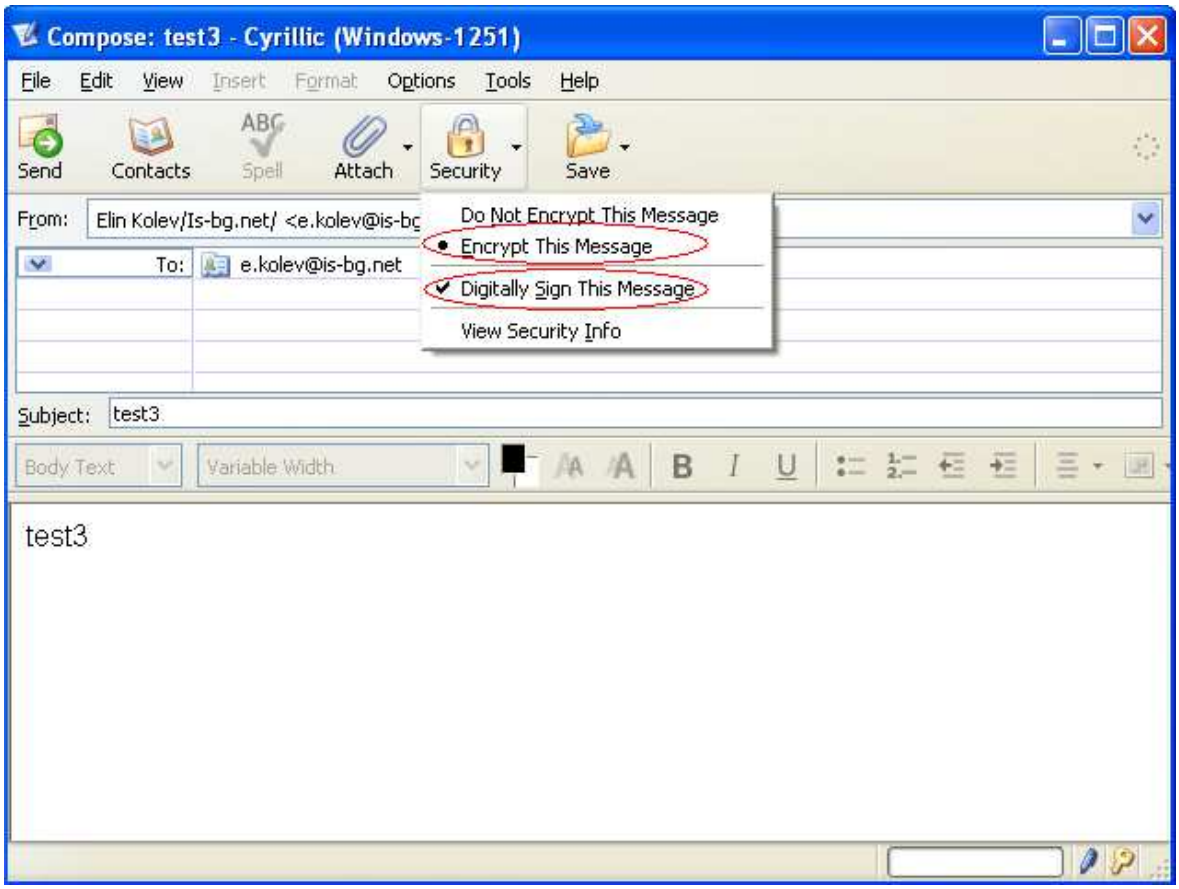
фиг. 3.2

Когато адресатът получи криптираното електронно съобщение, за да го декриптира, следва да въведе ПИН кода за достъп до своята смарт карта, след което, ако писмото е декриптирано успешно, ще се появи прозорец подобен на този от **фиг. 3.3**

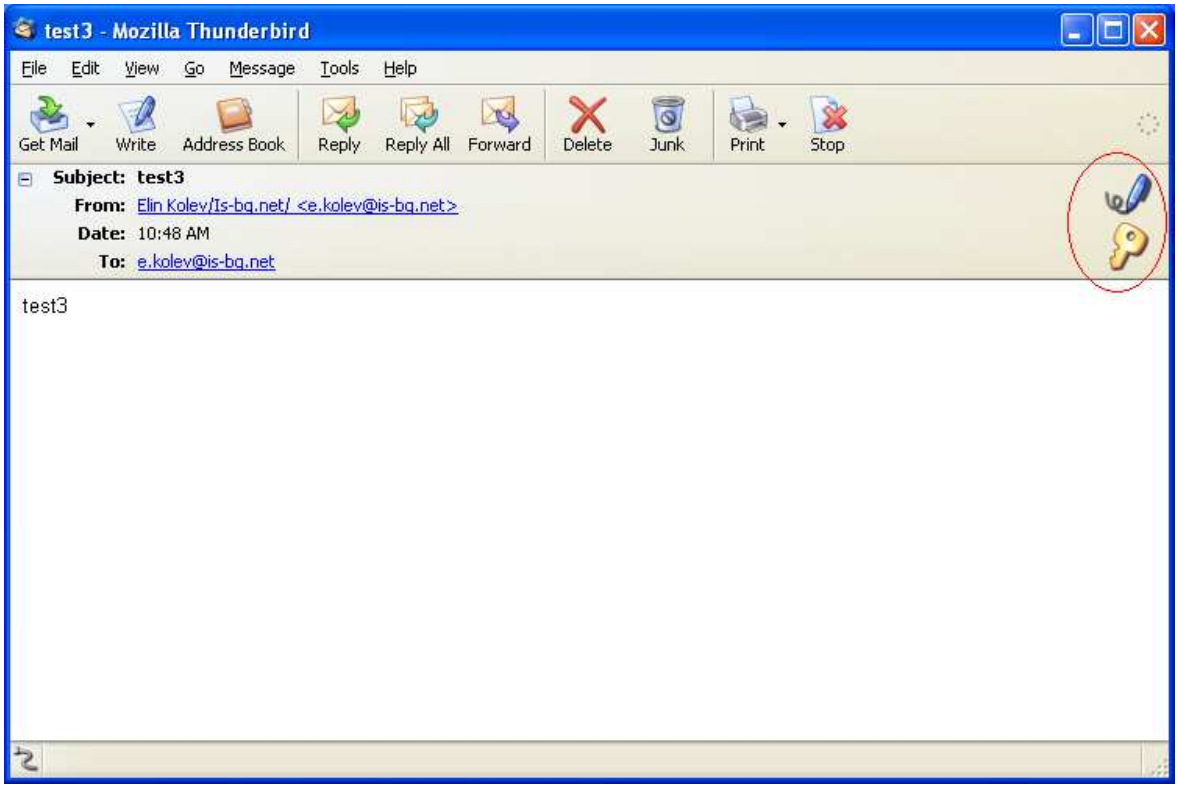


фиг. 3.3

Забележка: По аналогичен начин едно електронно съобщение може да бъде едновременно подписано и криптирано - **фиг. 3.4 и 3.5.**


Compose: test3 - Cyrillic (Windows-1251)
File Edit View Insert Format Options Tools Help
Send Contacts Spell Attach Security Save
From: Elin Kolev/Is-bg.net/ <e.kolev@is-bg
To: e.kolev@is-bg.net
Do Not Encrypt This Message
Encrypt This Message
Digitally Sign This Message
View Security Info
Subject: test3
Body Text Variable Width
test3

фиг. 3.4


test3 - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Mail Write Address Book Reply Reply All Forward Delete Junk Print Stop
Subject: test3
From: Elin Kolev/Is-bg.net/ <e.kolev@is-bg.net>
Date: 10:48 AM
To: e.kolev@is-bg.net
test3

фиг. 3.5