

Практическо ръководство за конфигуриране и работа с квалифицирано удостоверение за  
квалифициран електронен подпис /КУКЕП/ с клиента за електронна поща  
Mozilla Thunderbird  
**РЪКОВОДСТВО НА ПОТРЕБИТЕЛЯ – версия 4.0.0**

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

- **Charismathics** - управляват се от софтуера **Charismathics Smart Security Interface**. Всички карти от този тип имат индексен номер **СНxxxxx-xxxxxxxxx** или **StampIT-xxxxxxx**.

В момента на изготвяне на ръководството, настоящата версия на клиента е Mozilla Thunderbird 60.7.1.

**Съдържание:**

1. **Инсталиране и настройка**
2. **Подписване на електронни писма**
3. **Криптиране на електронни писма**

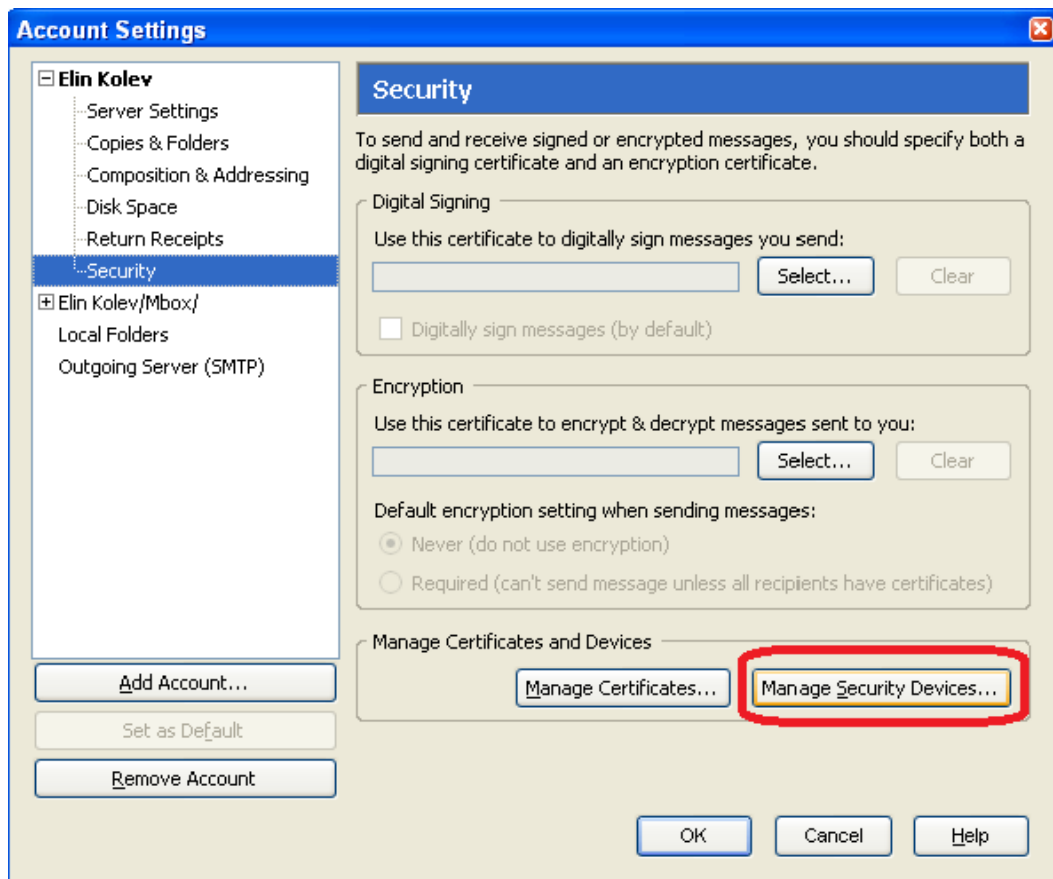
**1. Инсталиране и настройка**

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 този, който е настроен в пощенския акаунт.

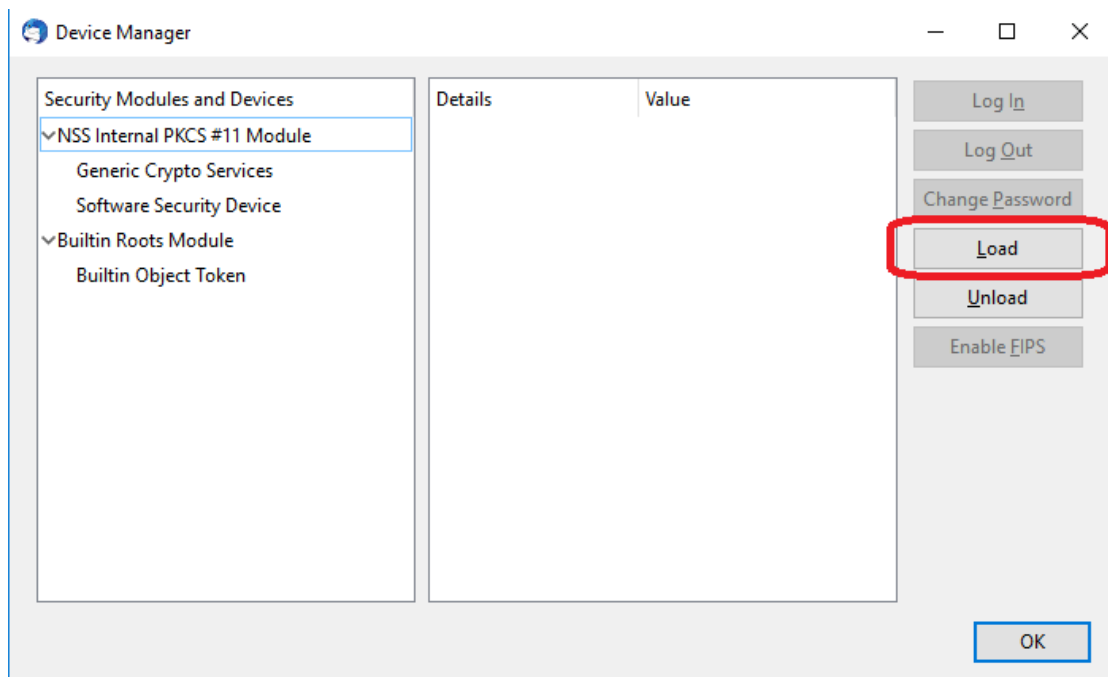
След като сте добавили вашия пощенски акаунт със съответните настройки за “Pop3” и „SMTP”, IMAP сървъри на Вашият доставчик на електронна поща е необходимо да инсталирате КУКЕП /сертификатите/, като изпълните последователността от действия:

- Изберете последователно „Tools”, “Accounts Settings” и изберете вашия акаунт. Изберете секцията „Security” и натиснете върху бутона „Manage Security Devices...” - **фиг. 1.1.1**



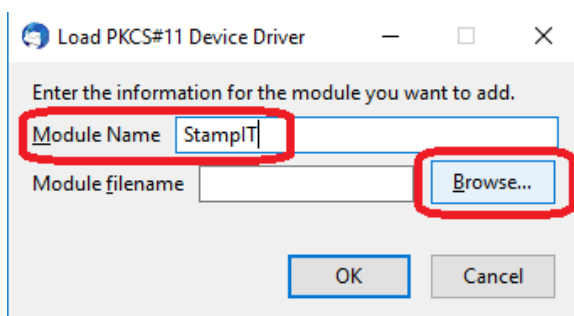
(фиг. 1.1.1)

- за да добавите ново защитено устройство, натиснете бутона „Load” и следвайте последователността, посочена по-долу. **фиг. 1.1.2**



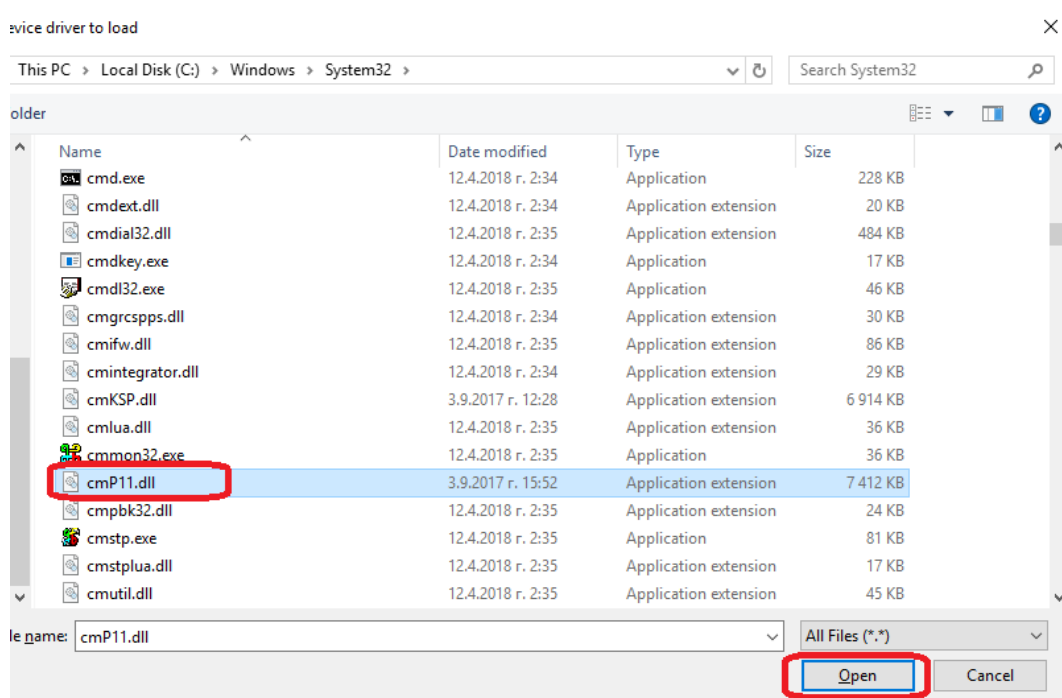
фиг. 1.1.2

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



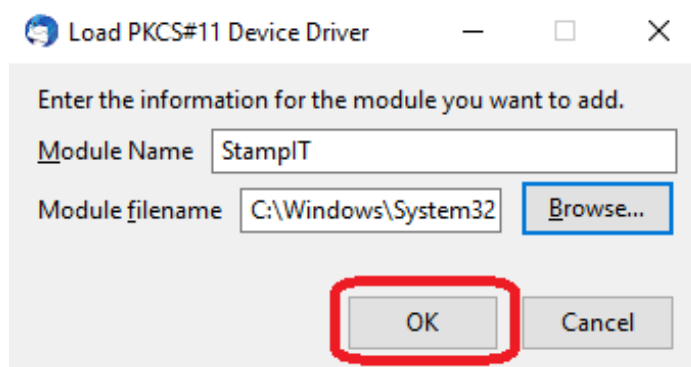
**/фиг. 1.1.3/**

- намерете и изберете файла **cmP11.dll** или **cmP1164.dll**, който се намира в папка **..WINDOWS\system32** - **фиг. 1.1.5** и натиснете бутона <Open>



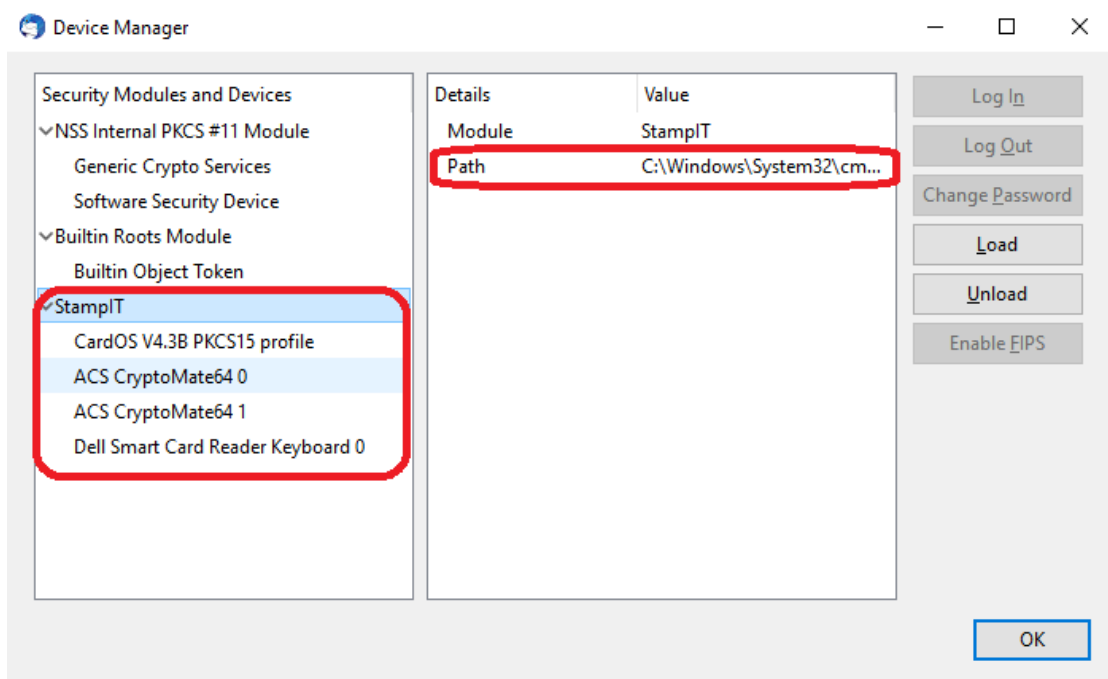
**фиг. 1.1.5**

- натиснете <OK>



**фиг. 1.1.6**

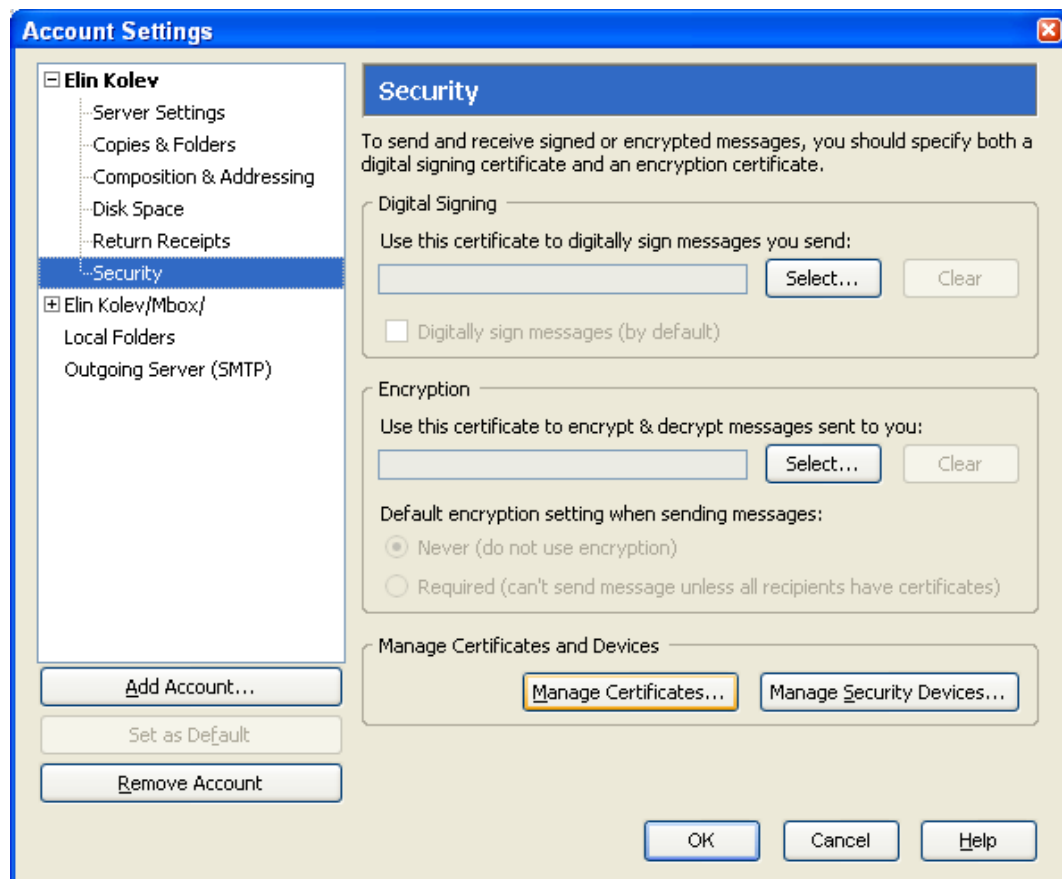
- След коректна инсталация трябва да видите екран подобен на този от **фиг. 1.1.8** и **фиг. 1.1.9**



фиг. 1.1.9

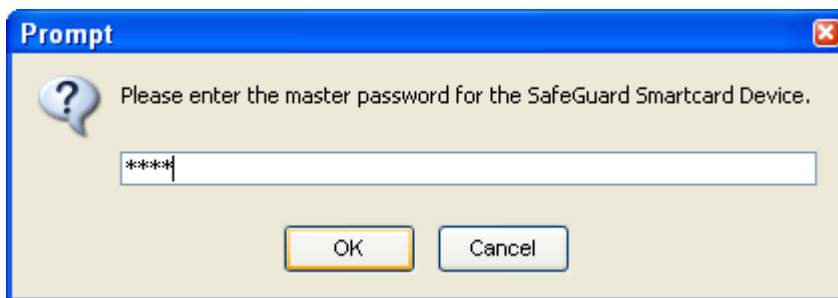
## 1.2. Инсталиране на сертификатите

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



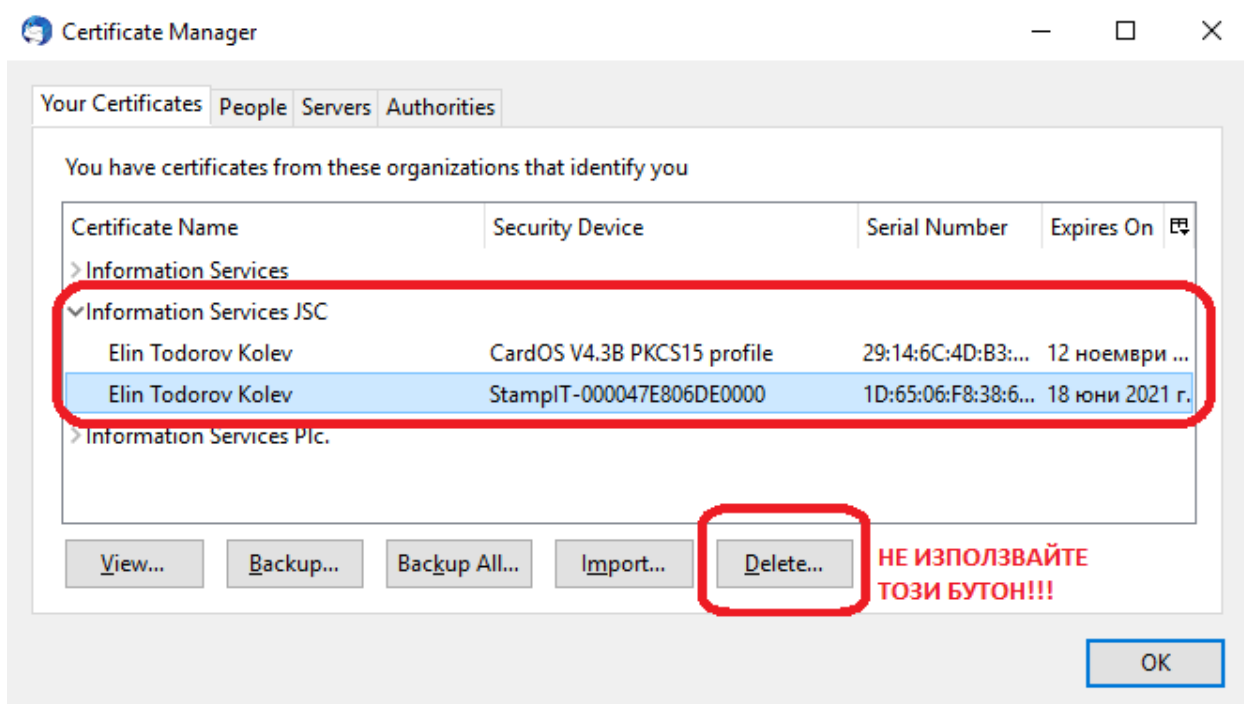
фиг. 1.2.1

- Въведете ПИН кода на смарт картата, който я защитава от неотризиран 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



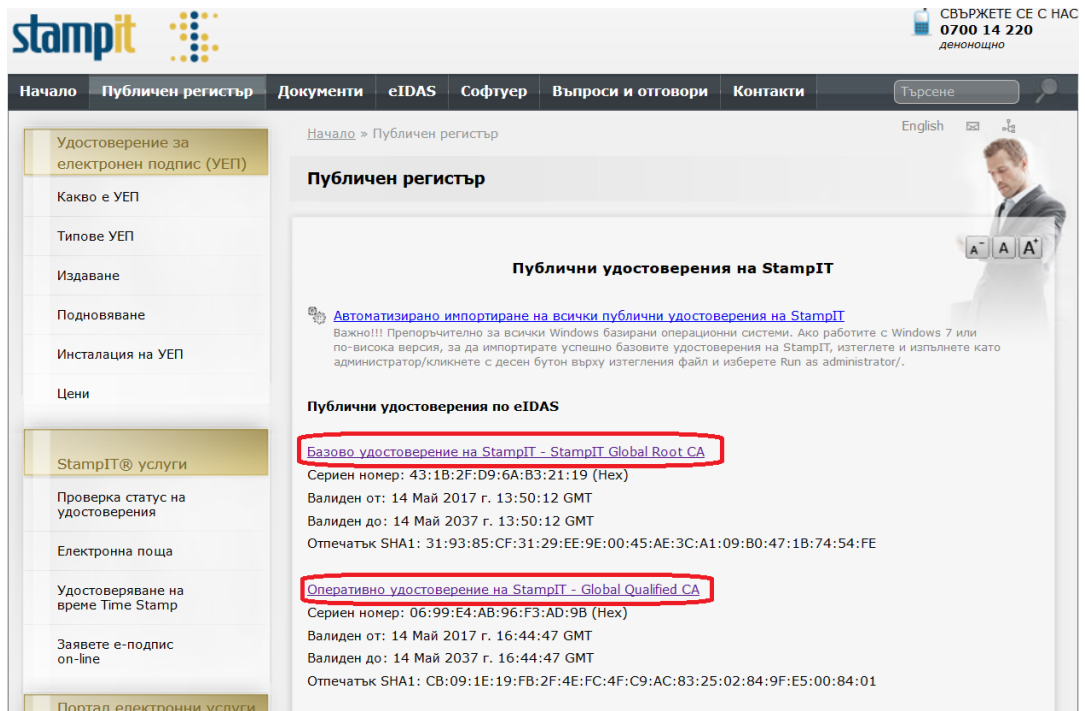
фиг. 1.2.3

**!!!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.

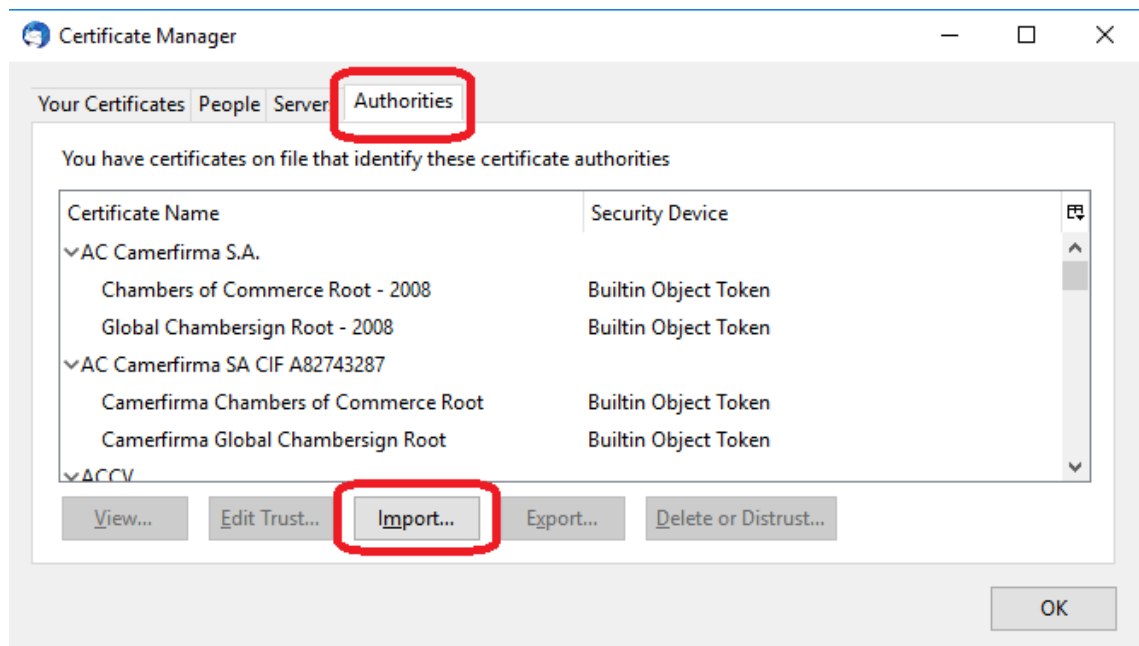
Изпълнете следното:

Изтеглете предварително от [www.stampit.org](http://www.stampit.org), секция <Публичен регистър> публичните удостоверения на StampIT - StampIT Global Root CA и StampIT Global Qualified CA - фиг. 1.2.4

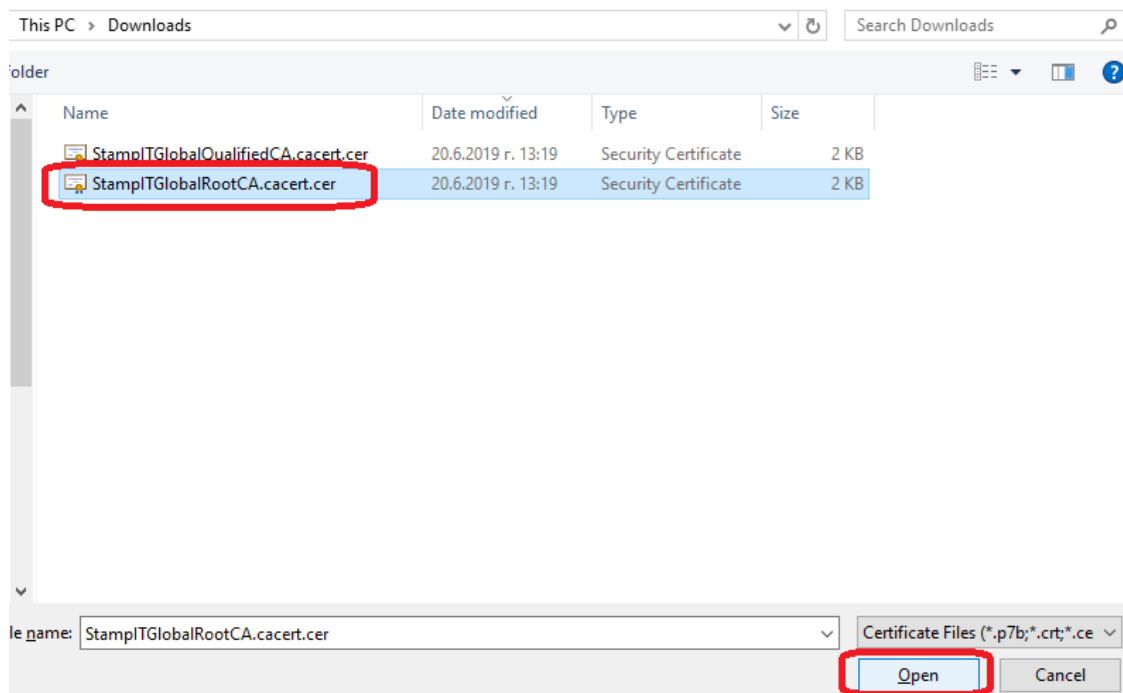


фиг. 1.2.4

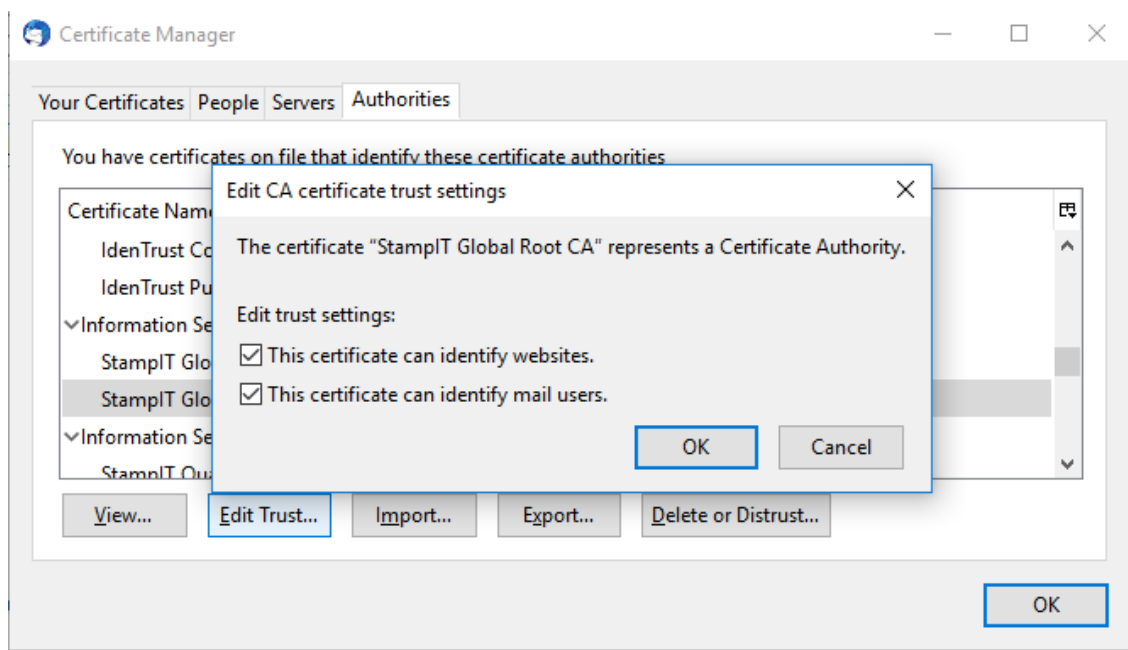
Изберете <Authorities> tab и след това бутона <Import> фиг. 1.2.5



фиг. 1.2.5



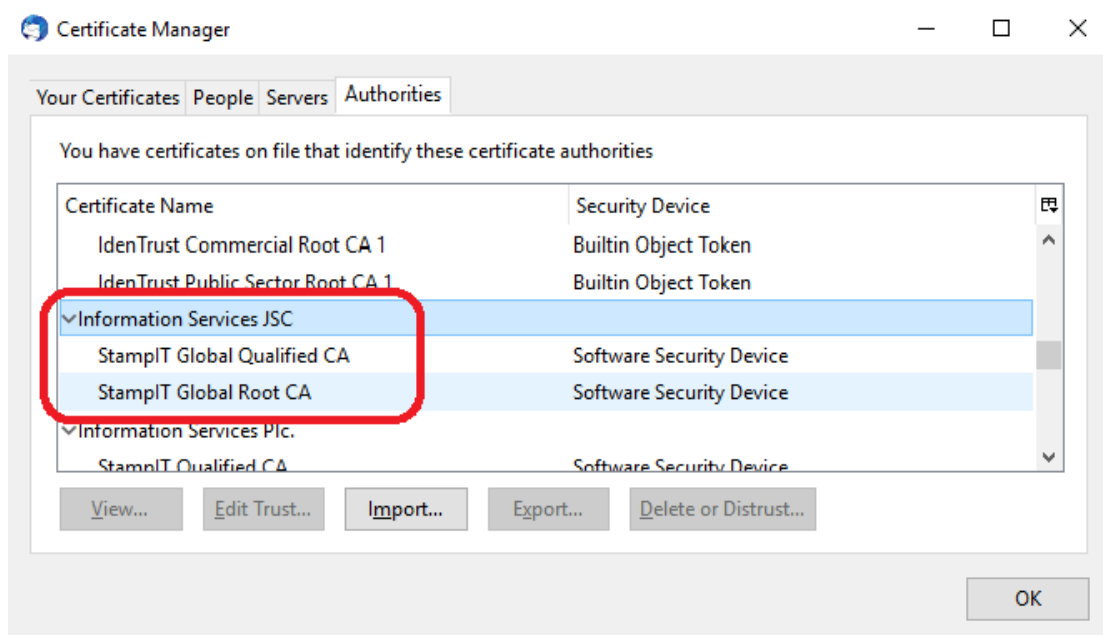
фиг. 1.2.6



фиг. 1.2.7

По аналогичен начин импортирайте и оперативното удостоверение <StampIT Global Qualified CA>.

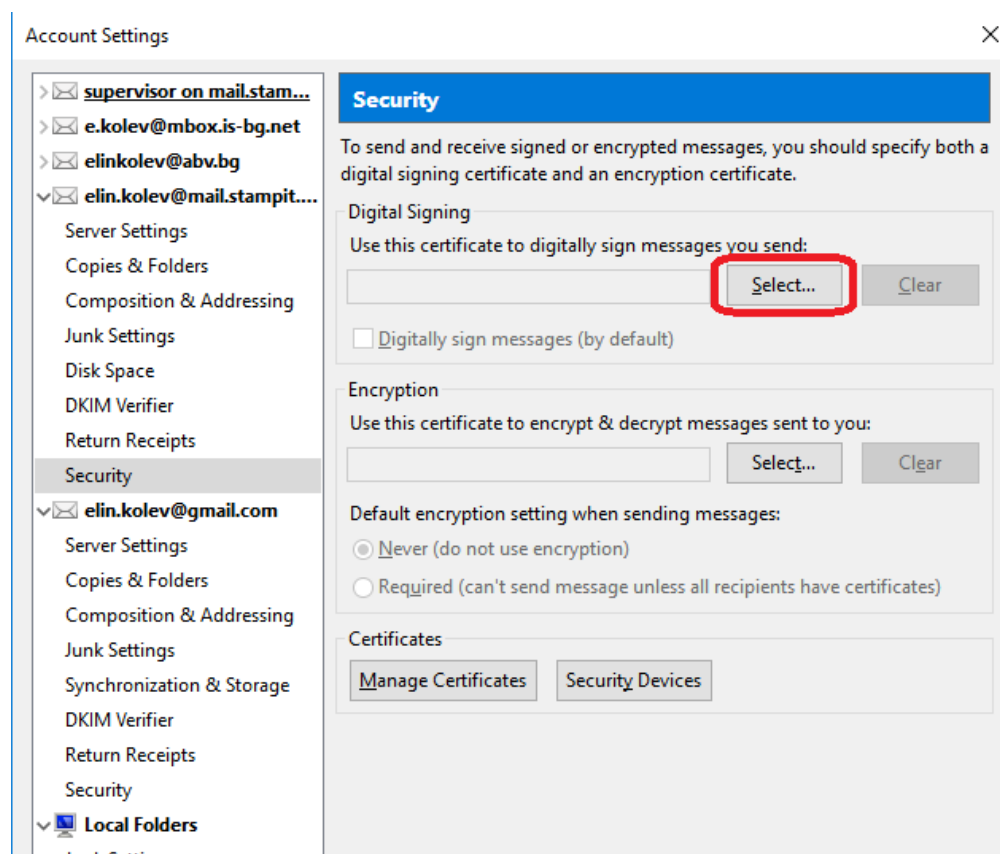
След успешна инсталация в крайна сметка трябва да виждате прозорец подобен на този от фиг. 1.2.8



фиг. 1.2.8

- Потвърдете с <OK> и ще видите първоначалния прозорец на секцията <security> **фиг. 1.2.9**
- Следващата стъпка е да изберете сертификат за подписване и криптиране, който ще се използва от клиента за електронна поща Mozilla Thunderbird. Картата трябва да бъде поставена в карточечящото устройство.

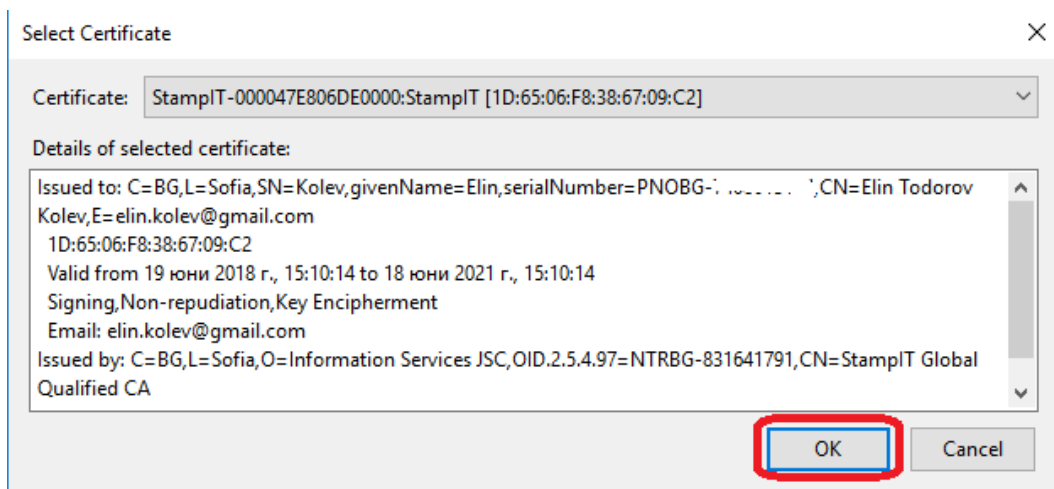
Изберете бутона <Select...> от секцията <Digital Signing> **фиг. 1.2.9**



фиг. 1.2.9

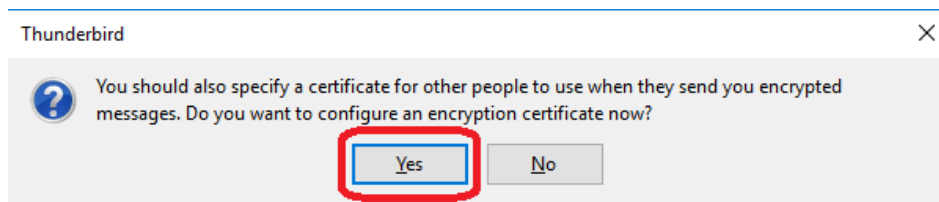


- Потвърдете с <ОК> фиг. 1.2.10.



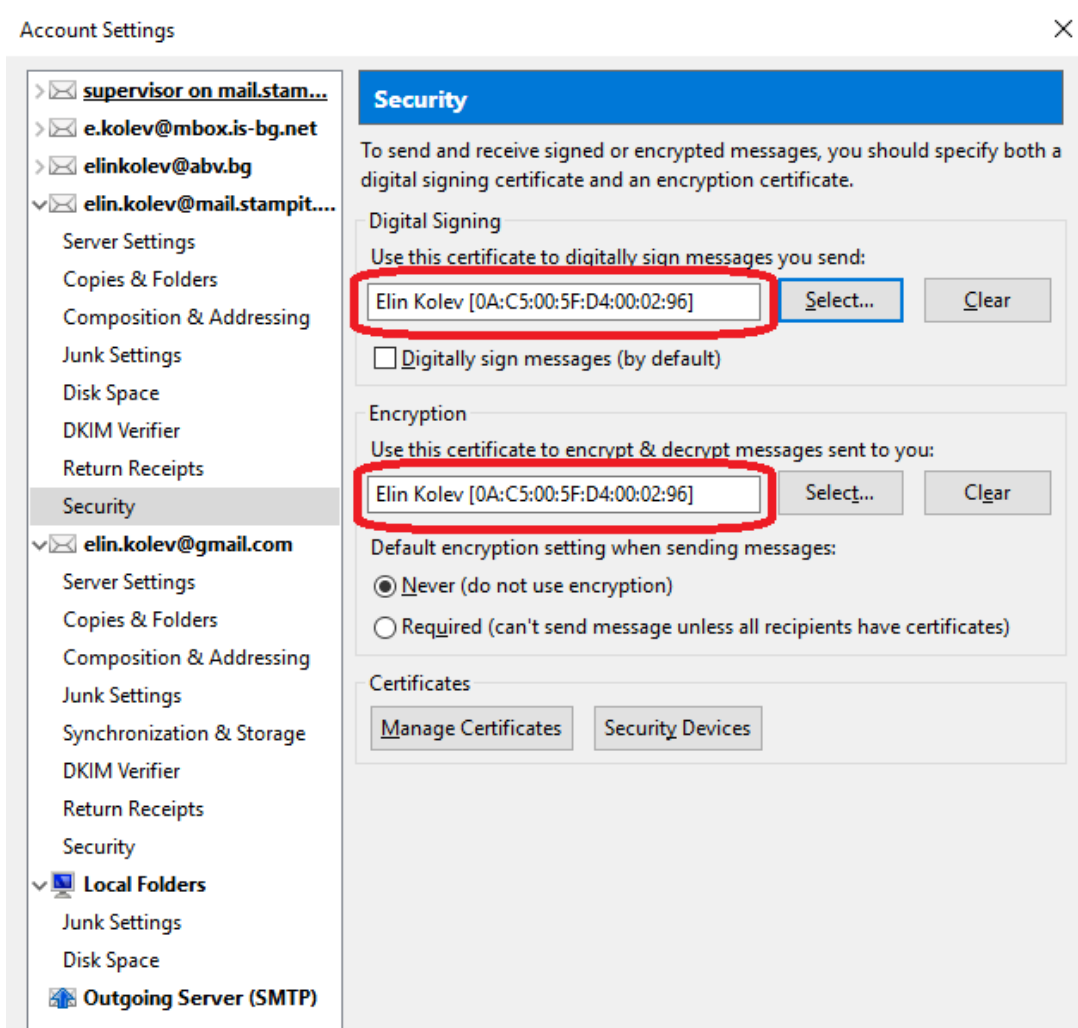
фиг. 1.2.10

- Потвърдете отново с <Yes>



фиг. 1.2.11

Ако процедурата по инсталиране е преминала успешно, следва да виждате екран, подобен на този от фиг. 1.2.12

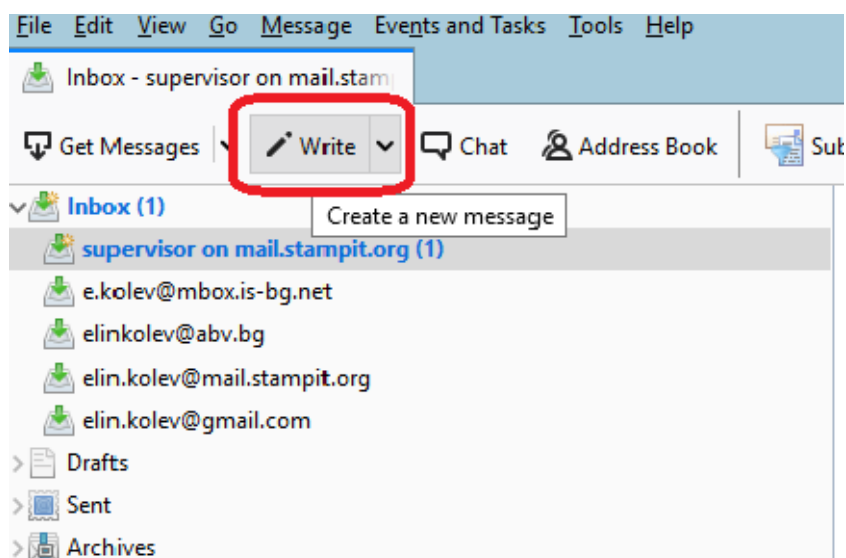


фиг. 1.2.12

## 2. Подписване на електронни съобщения

За да подпишете електронно съобщение изпълнете следните стъпки:

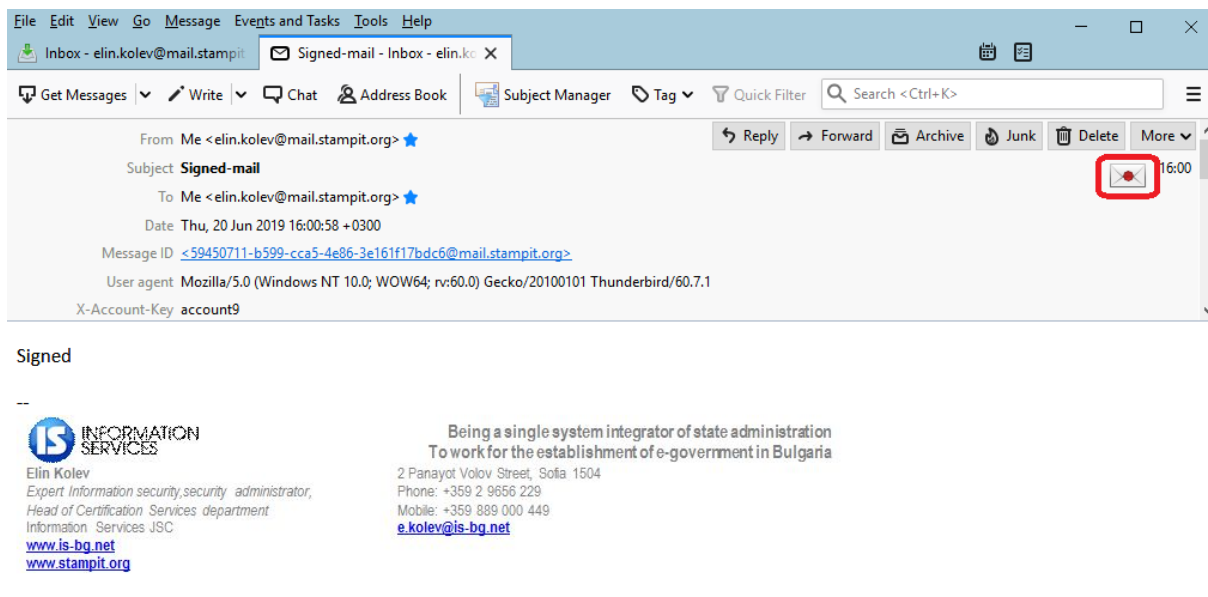
- Създайте ново електронно съобщение като натиснете бутона <Write> **фиг.2.1**



фиг. 2.1

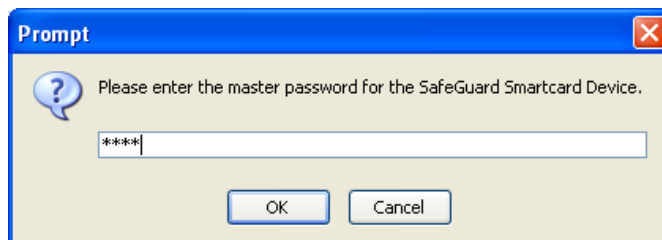
- Въведете необходимите полета за <To:>, <Subject:>
- От падащото меню <Security> изберете <Digitally Sign This Message> и натиснете бутона "Send"-

фиг.2.2



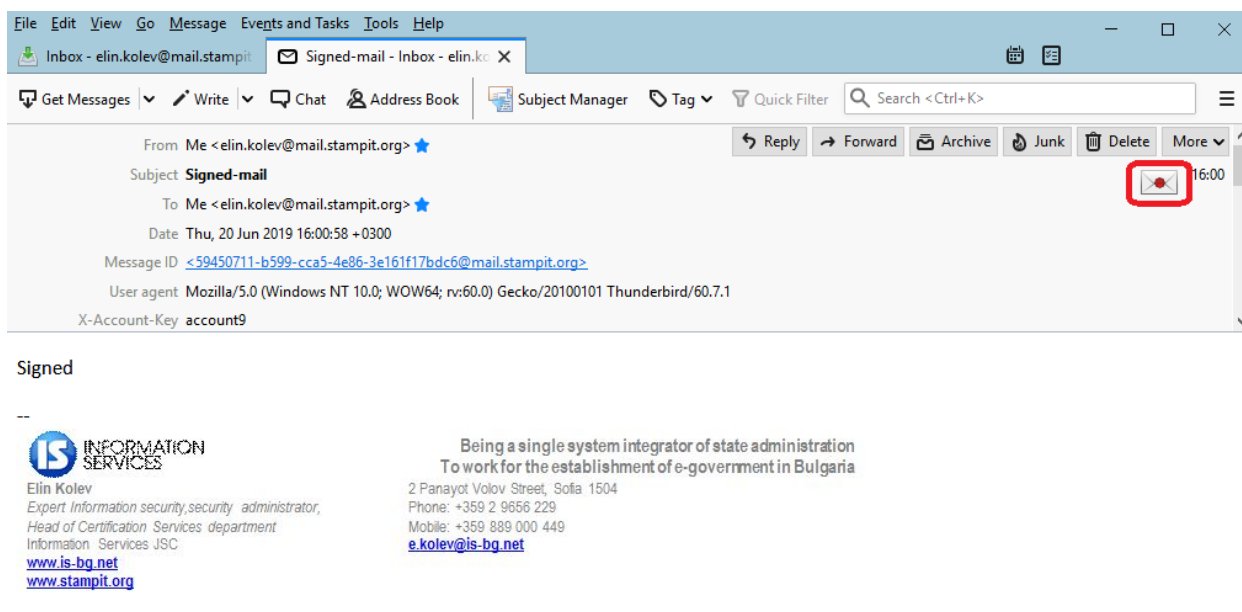
фиг.2.2

- Въведете вашия ПИН код за достъп до смарт картата (ако вече сте въвели еднократно ПИН код и не сте затваряли приложението или изключвали смарт картата, Mozilla Thunderbird няма да поиска повторно въвеждане).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**



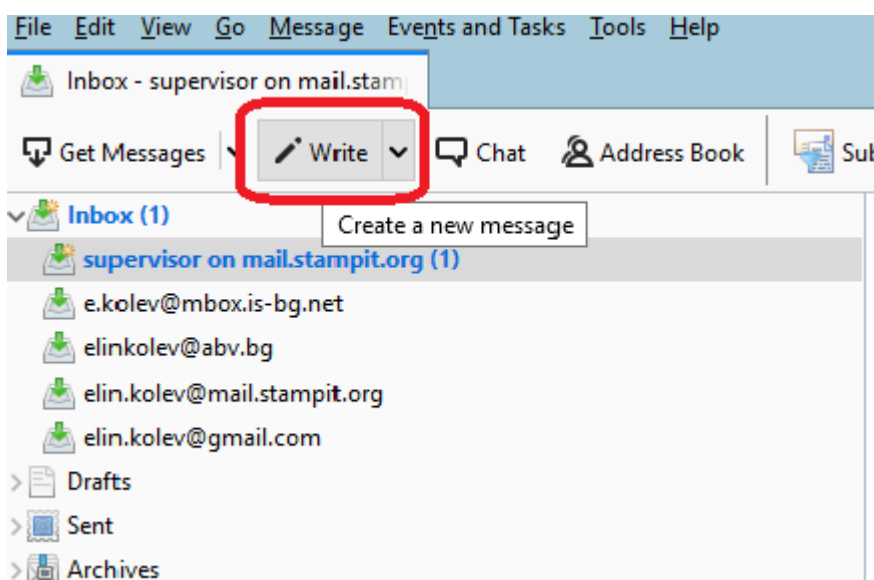
фиг.2.3

### 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/

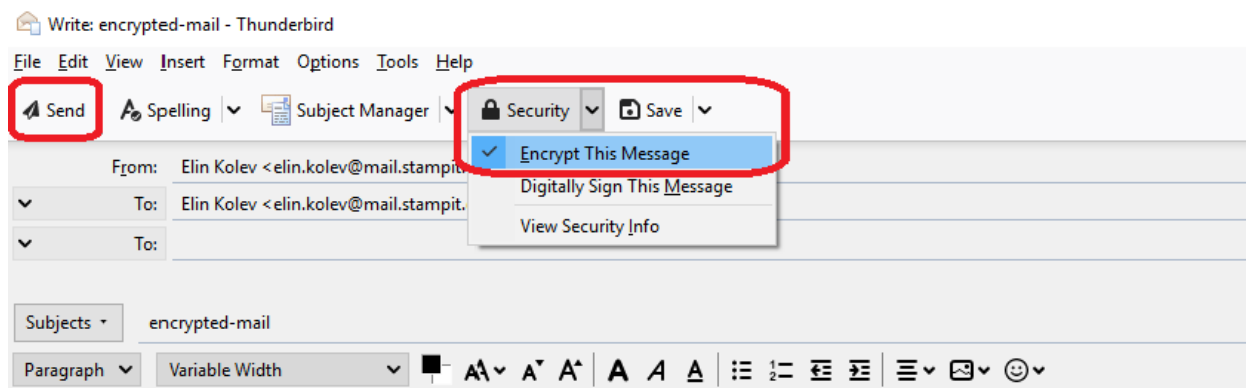
След като имате съхранен публичния ключ изпълнете следните стъпки:

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

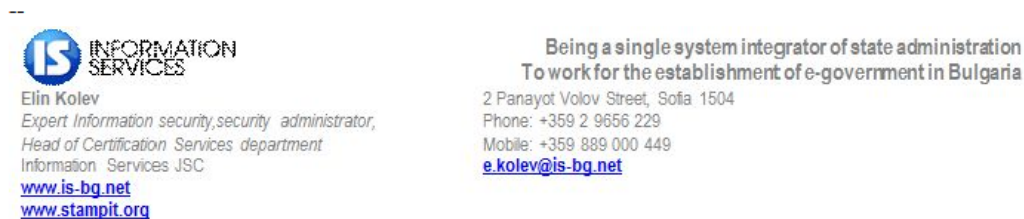


фиг. 3.1

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

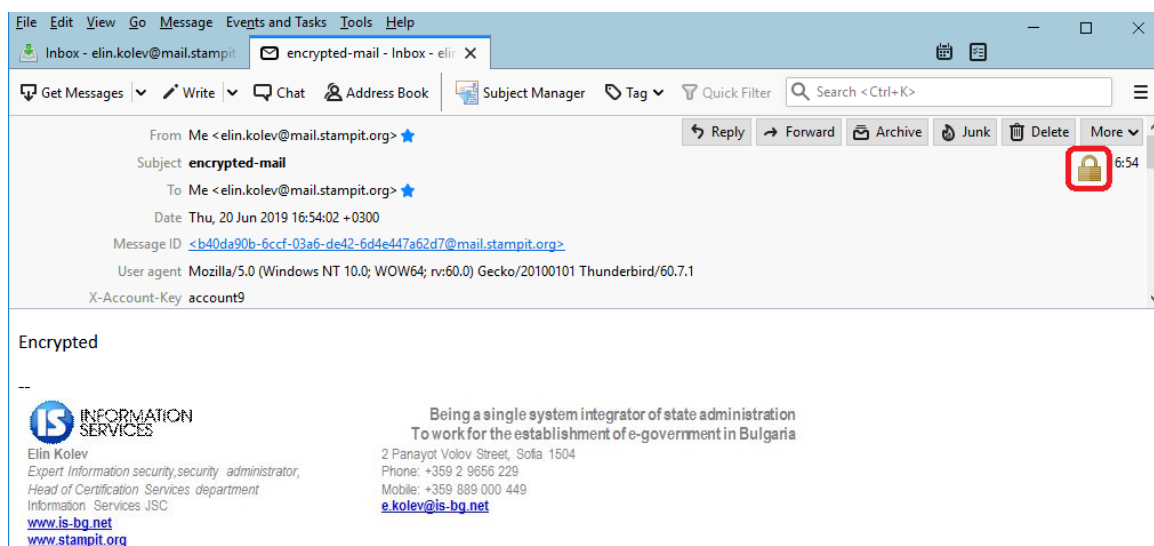


Encrypted



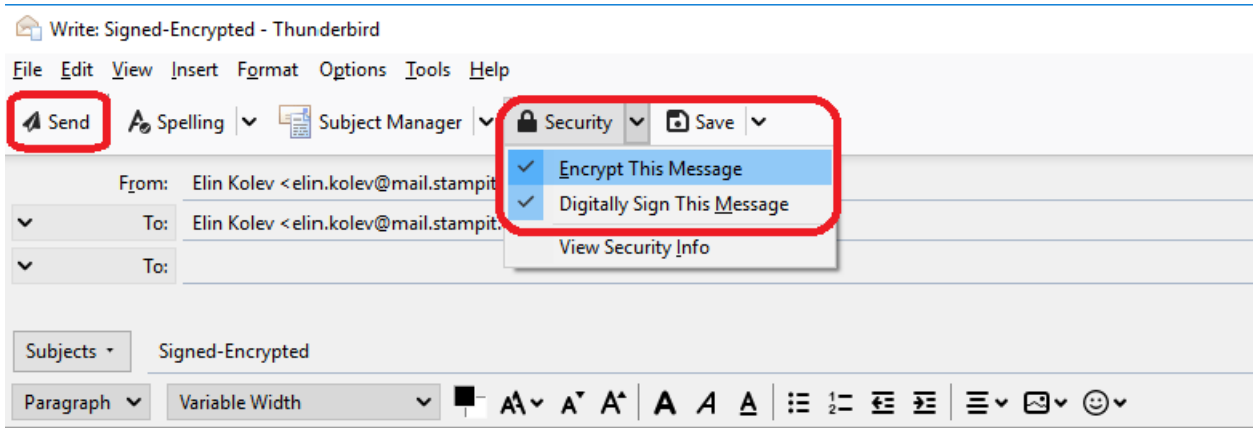
фиг. 3.2

Когато адресатът получи криптираното електронно съобщение, за да го декриптира, следва да въведе ПИН код за достъп до частния ключ на своята смарт карта. Писмото може да бъде декриптирано единствено с частния ключ на лицето, към което е изпратено. 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**.

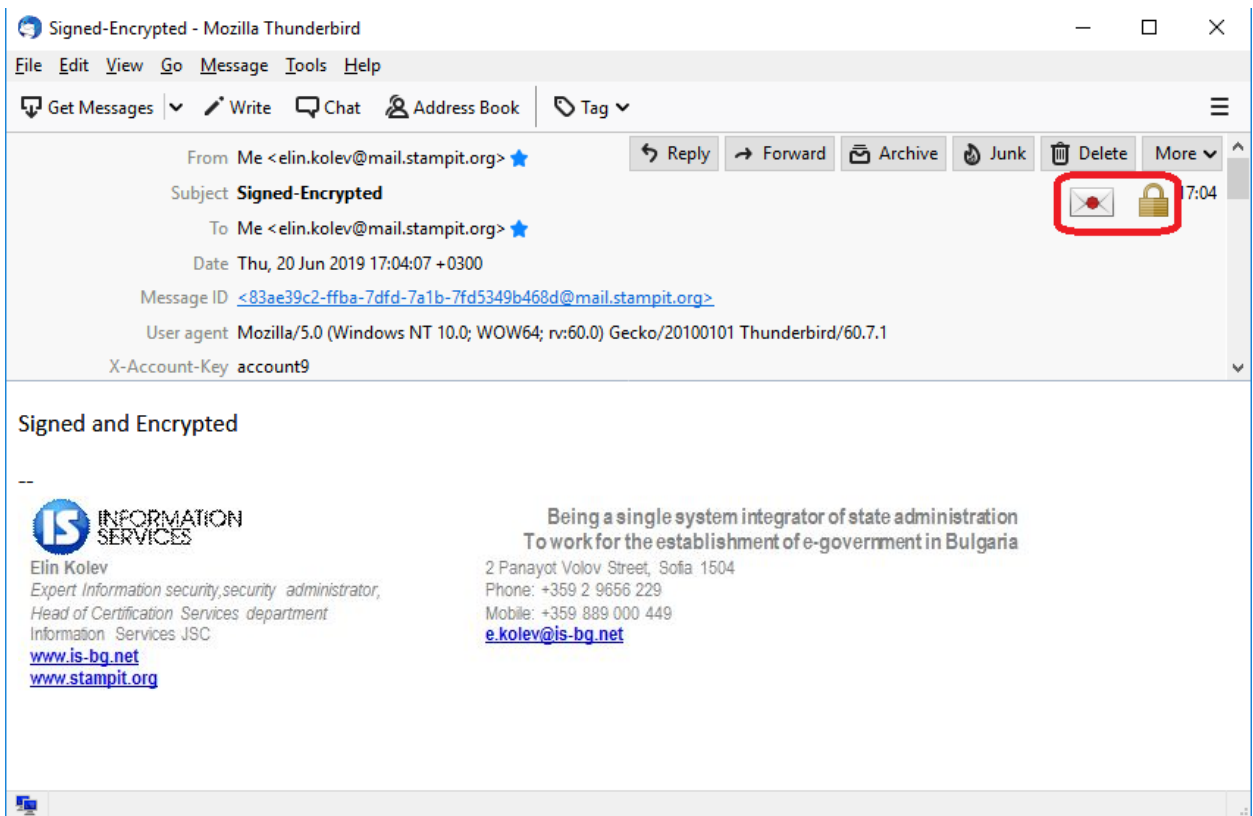


Signed and Encrypted


**Being a single system integrator of state administration  
To work for the establishment of e-government in Bulgaria**  
 2 Panayot Volov Street, Sofia 1504  
 Phone: +359 2 9656 229  
 Mobile: +359 889 000 449  
[e.kolev@is-bg.net](mailto:e.kolev@is-bg.net)

Elin Kolev  
 Expert Information security, security administrator,  
 Head of Certification Services department  
 Information Services JSC  
[www.is-bg.net](http://www.is-bg.net)  
[www.stampit.org](http://www.stampit.org)

фиг. 3.4



фиг. 3.5

Ако имате някакви препоръки или забележки по настоящата инструкция, не се колебайте да се свържете с нас.

**Тел. +359 889000449 – Елин Колев**

**Тел. +359 888772451 – Ивайло Дойнов**

**email: [support@mail.stampit.org](mailto:support@mail.stampit.org)**