**Ръководство за работа с KDE Application "Kleopatra"**

Contents

[**1. Инсталиране на gpg4win-4.4.0.** 2](#_Toc194310368)

[**2. Експорт на публичен ключ.** 9](#_Toc194310369)

[**3. Експорт на частен ключ.** 10](#_Toc194310370)

[**4. Импорт на публичен ключ.** 13](#_Toc194310371)

[**5. Криптиране на файл.** 19](#_Toc194310372)

[**6. Декриптиране на файл.** 27](#_Toc194310373)

[**7. Импорт на архивиран частен ключ.** 31](#_Toc194310374)

[**8. Генериране на нова двойка ключове.** 39](#_Toc194310375)

# **[1. Инсталиране на gpg4win-4.4.0.](https://support.brother.com/g/s/id/htmldoc/mfc/dcp_mfc9010cn/bg/html/ug/appendix15_7.html)**

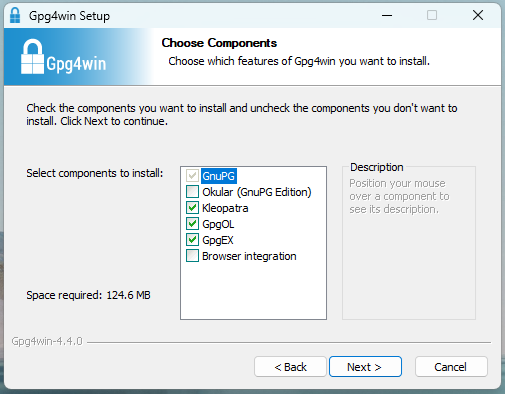
При инсталиране на Gpg4win (GNU Privacy Guard for Windows), версия "gpg4win-4.4.0" (gpg4win-4.4.0.exe) се инсталира и мениджър на сертификати KDE Applications "Kleopatra" за обработка на OpenPGP.

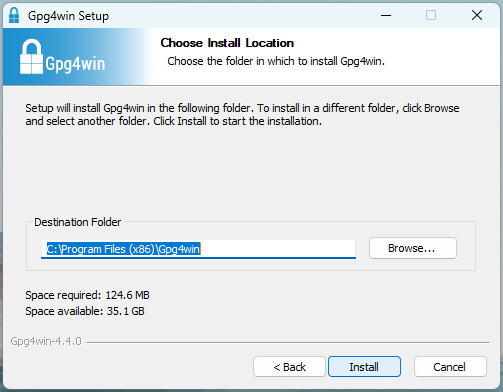
Мениджър на сертификати "Kleopatra" генерира автоматично двойка ключове "public" и "secret".

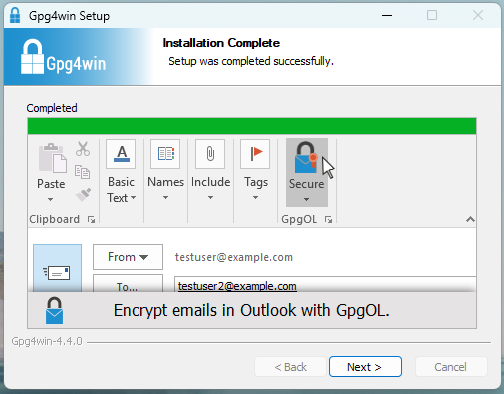
"Public key" се предоставя на контргентите, които ще криптират с него файлове за Вас.

"Secret key" си остава само за Вас. Чрез него се декриптират получените файлове от контрагентите, криптирани с Вашия публичен ключ.

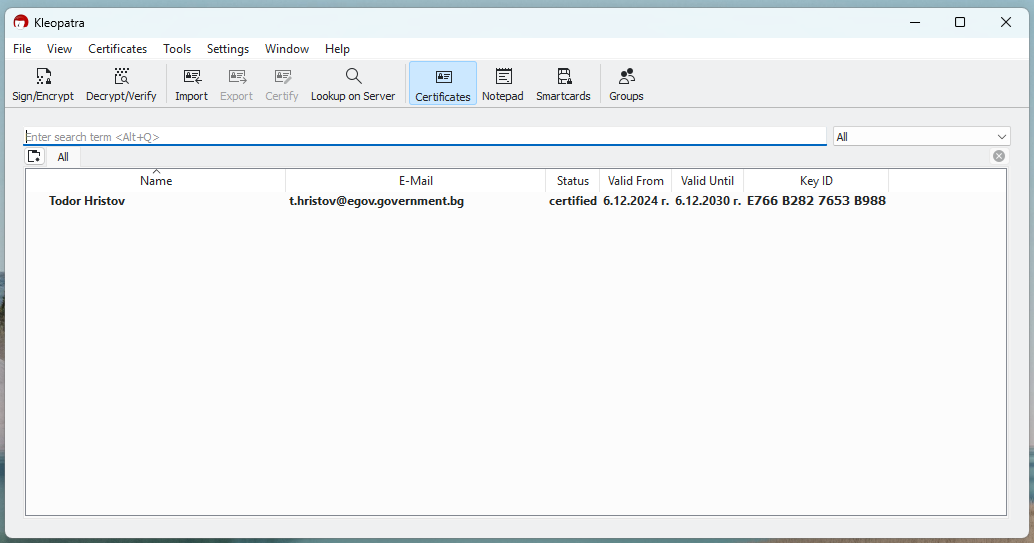












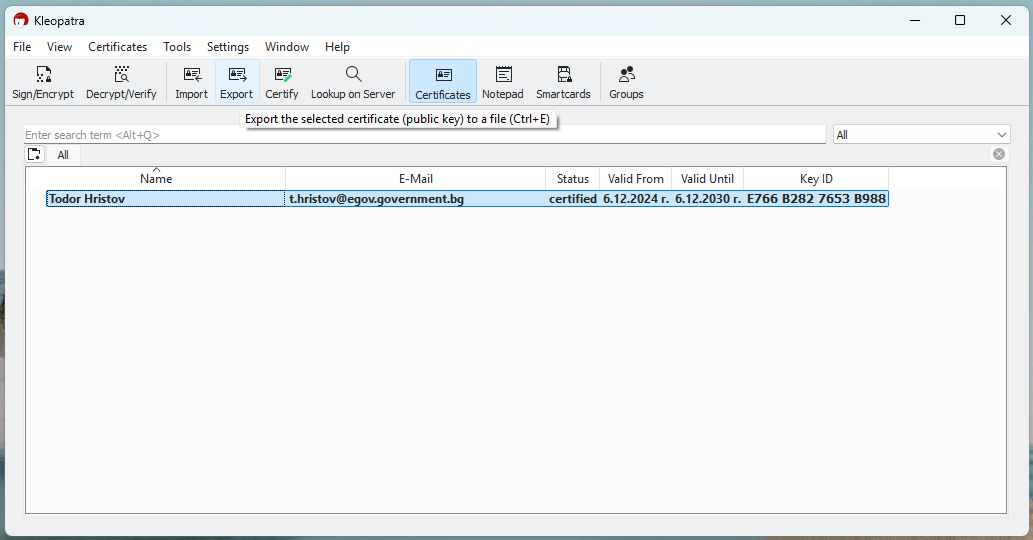
# **[2. Експорт на публичен ключ.](https://support.brother.com/g/s/id/htmldoc/mfc/dcp_mfc9010cn/bg/html/ug/appendix15_7.html)**

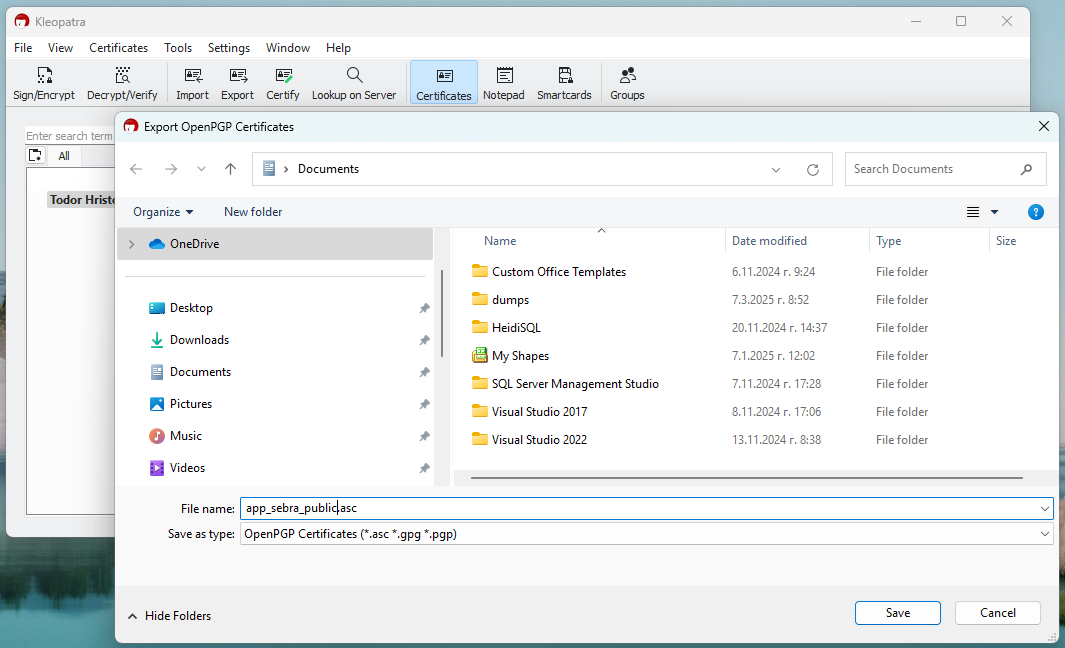
За криптиране на файл (app\_sebra.7z) се използва публичен ключ (borika\_public.asc).

Този ключ се експортира като:

В Tab All, маркирате сертификата, използвате бутон "Export" и записвате публичния ключ.

Публичния ключ се изпраща на контрагента, който трябва да криптира негов файл за Вас.





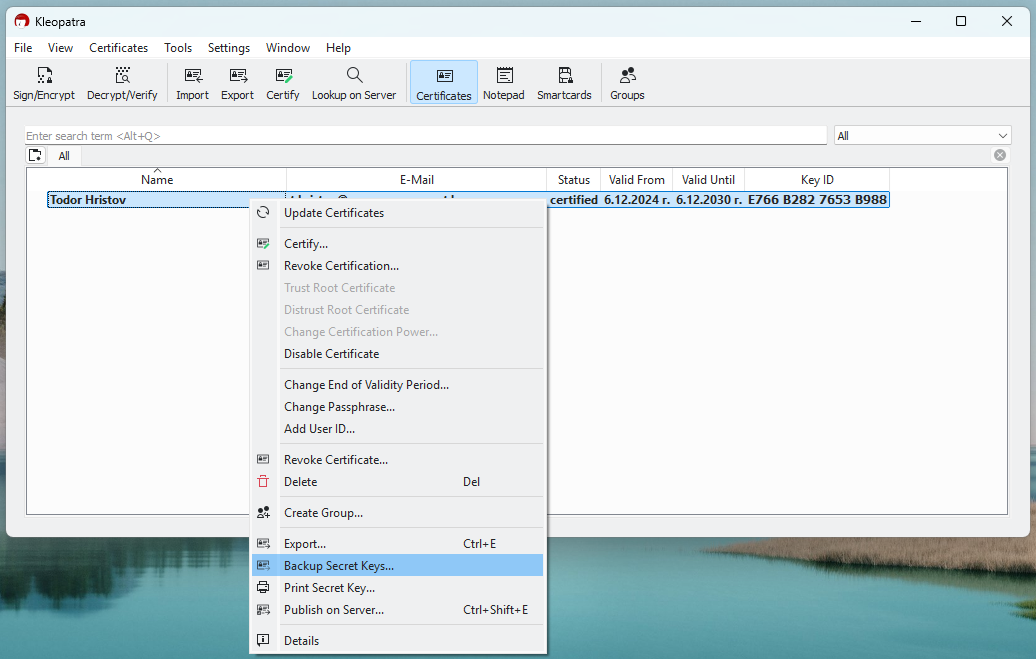
# **[3. Експорт на частен ключ.](https://support.brother.com/g/s/id/htmldoc/mfc/dcp_mfc9010cn/bg/html/ug/appendix15_7.html)**

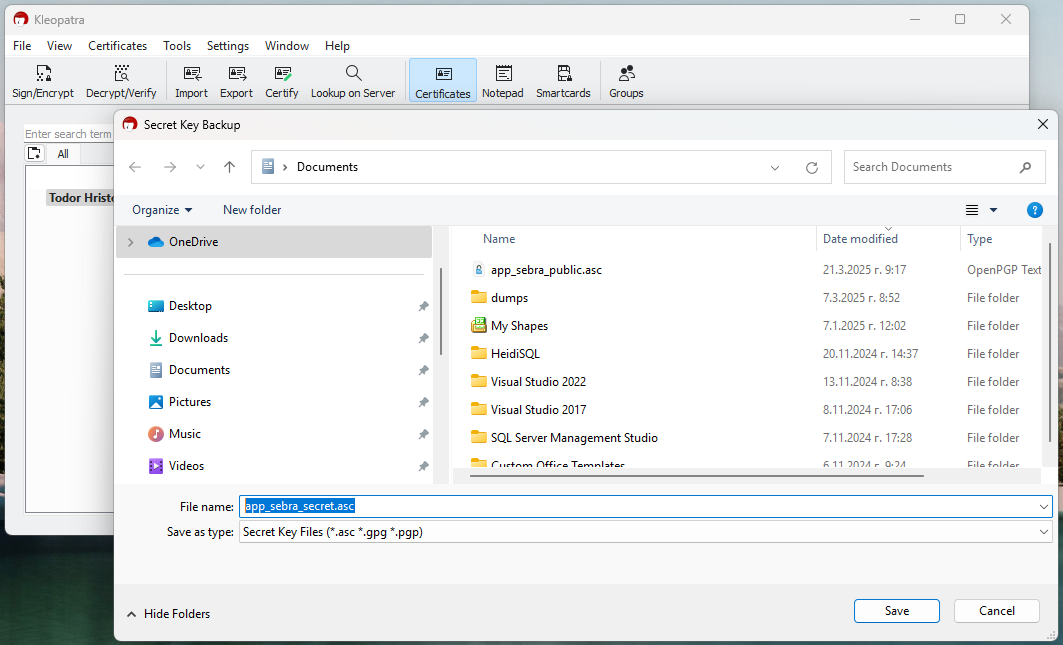
За да използвате същата двойка ключове на друга машина или след възстановяване на същата машина при срив, Ви е необходим архив на частния ключ.

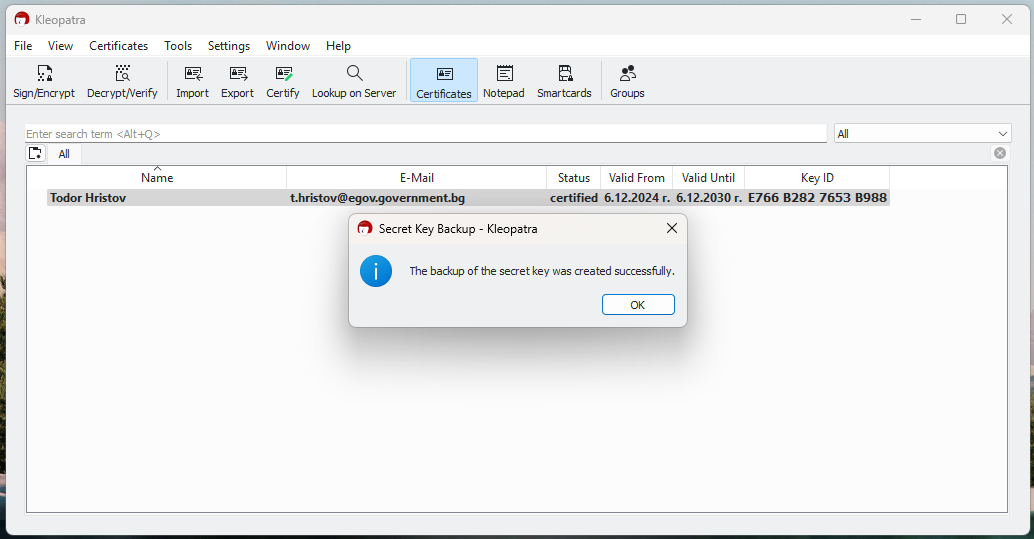
Този ключ се експортира като:

В Tab "All", маркирате сертификата и кликвате с десен бутон на мишката.

От падащото меню избирате "Backup Secret Keys" и записвате частния ключ.







# **[4. Импорт на публичен ключ.](https://support.brother.com/g/s/id/htmldoc/mfc/dcp_mfc9010cn/bg/html/ug/appendix15_7.html)**

За да криптирате файл за даден контрагент, то Ви е необходим неговия публичен ключ.

Този ключ се импортира като:

Кливате върху бутон "Import" и избирате публичния ключ.

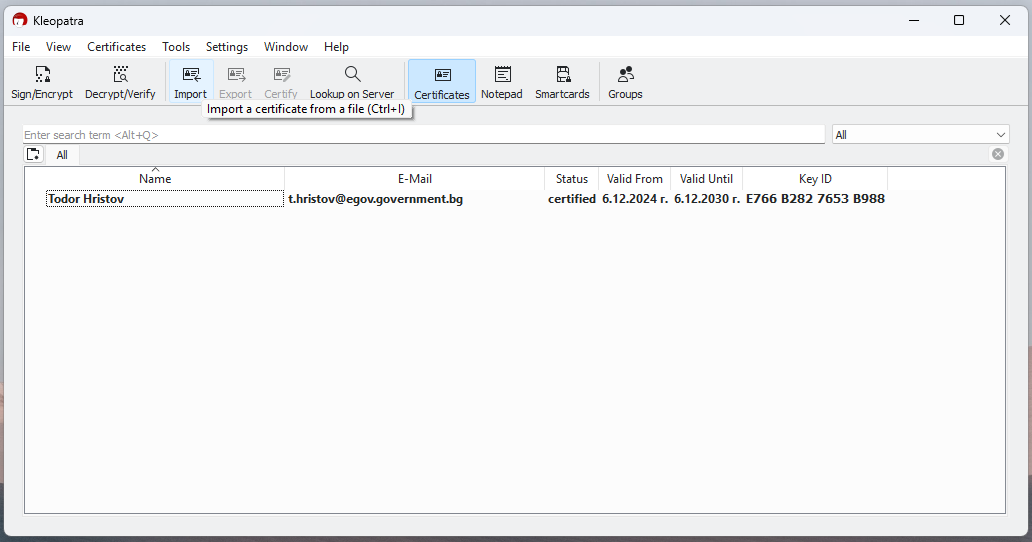
От появилия се панел с въпрос дали искате да продължите процеса, се избира бутон: "Certify".

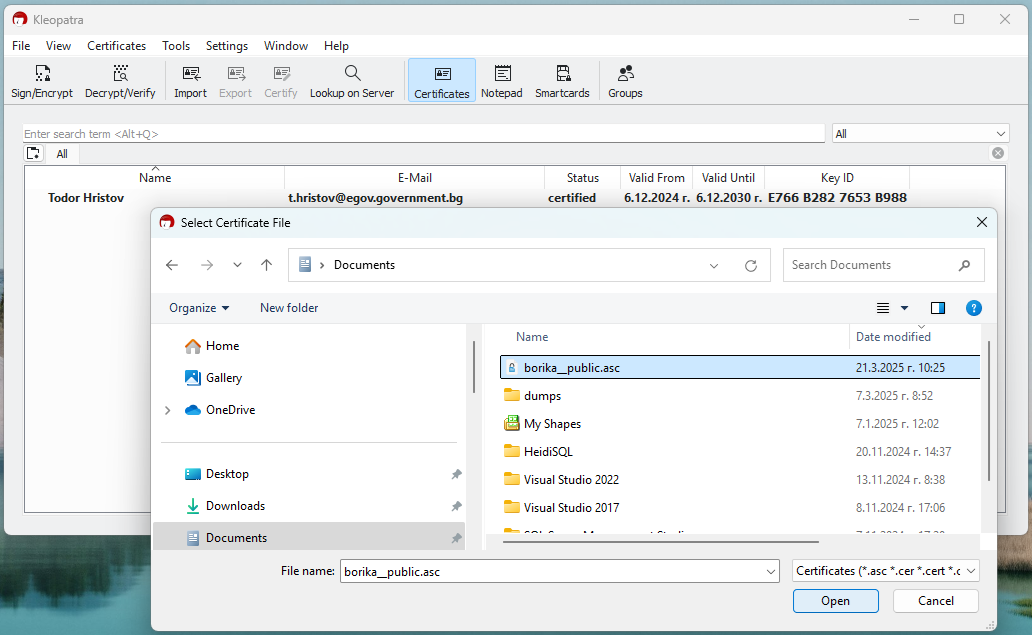
От появилия се панел "Certify Certificate: ..." се избира бутон: "Certify".

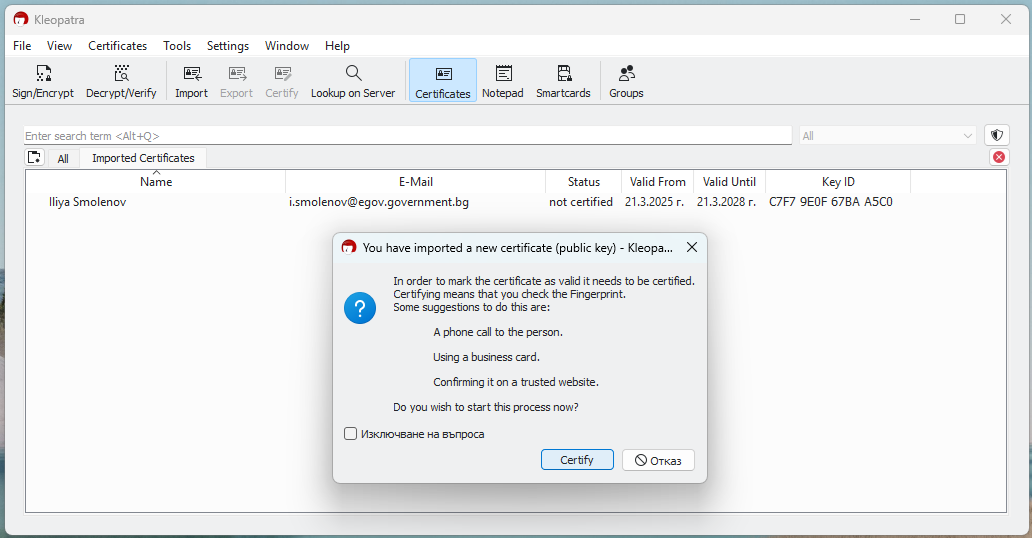
Потвърждавате с бутон "ОК" информацията "Certification successful".

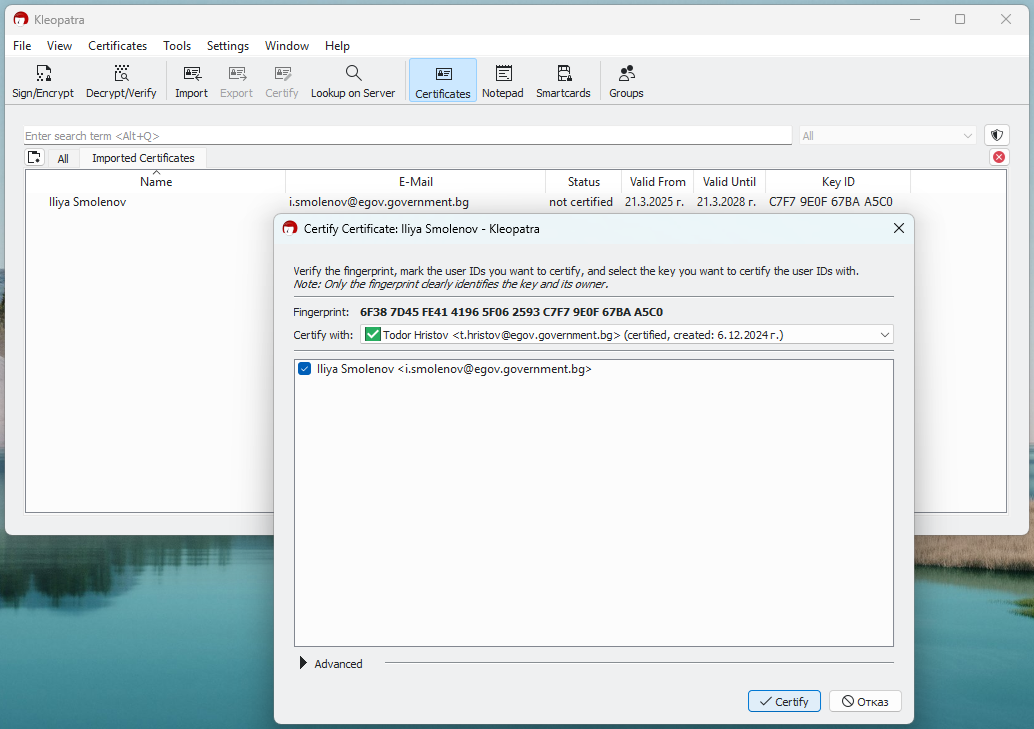
В Tab "Imported Certificates" се вижда импортирания сертификат.

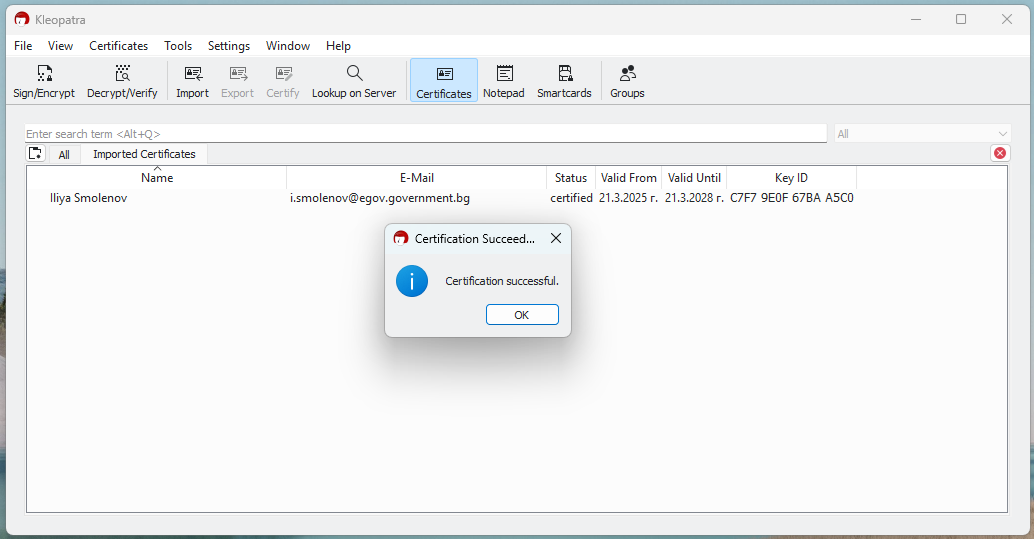
В Tab "All" се виждат всички сертфикати.

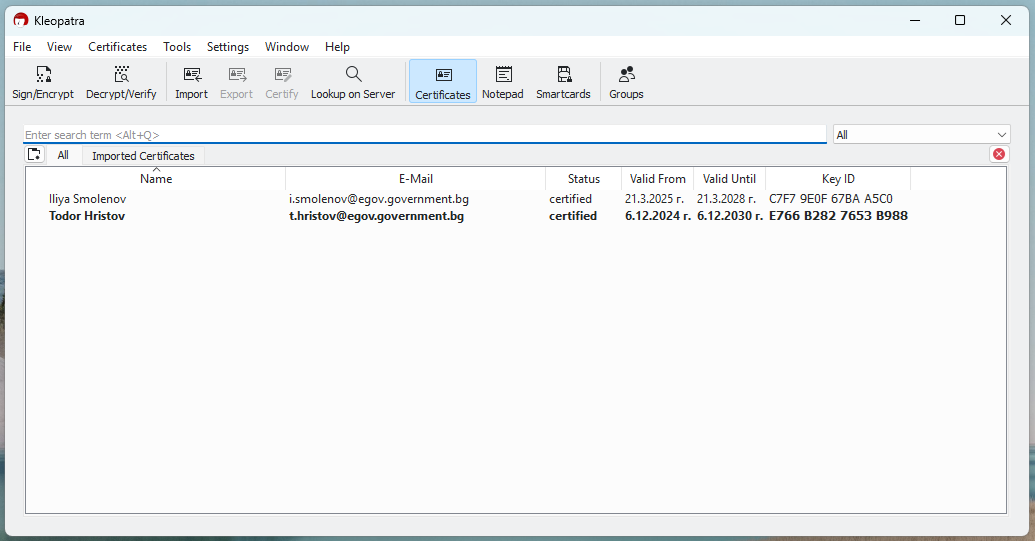












# **[5. Криптиране на файл.](https://support.brother.com/g/s/id/htmldoc/mfc/dcp_mfc9010cn/bg/html/ug/appendix15_7.html)**

За да криптираме цялата папка "app\_sebra", първо я архивираме чрез файлов архиватор "7z" и получаваме файл: "app\_sebra.7z".

В мениджър на сертификати "Kleopatra" се кликва върху бутон "Sign/Encrypt" и избираме архивирания файл (app\_sebra.7z).

Oт панел "Sign/Encrypt Files - Kleopatra":

- отмаркира се chckbox "Sign as:".

- отмаркира се chckbox "Encrypt for me:".

- маркира се chckbox "Encrypt for others:" и кликваме върху бутон [+] (отдясно на полето).

Oт панел "Certificate Selection - Kleopatra", се избира публичния сертификат на контрагента, за който е предназначен файла и се натиска бутон "OK".

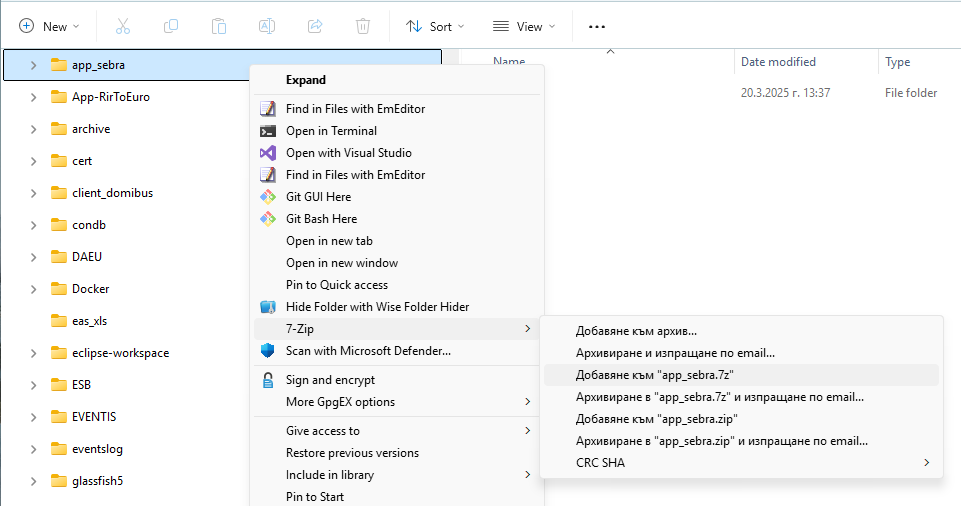
В панел "Sign/Encrypt Files - Kleopatra", в полето "Encrypt for others:" се визуализира избрания сертификат с маркиран checkbox.

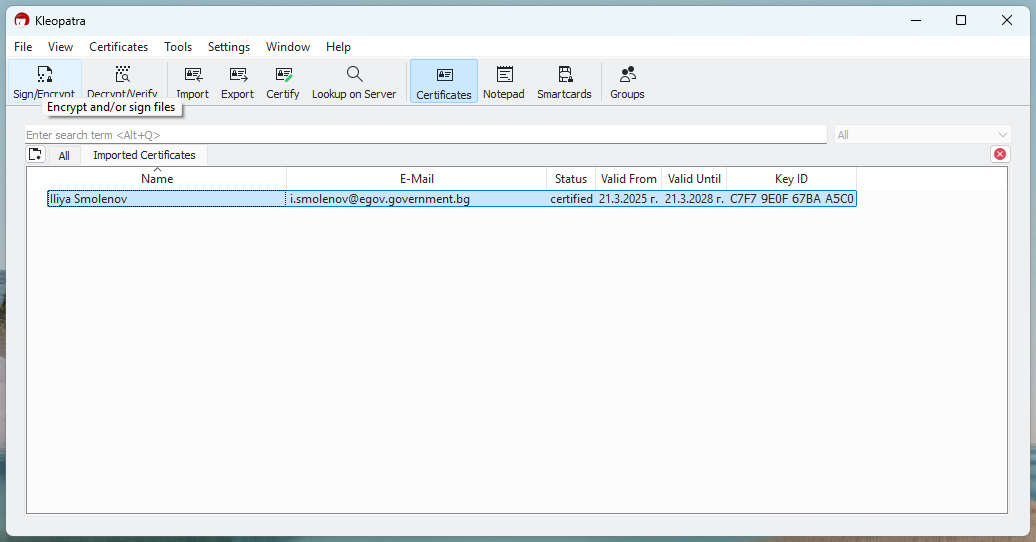
Кликва се върху бутон "Encrypt".

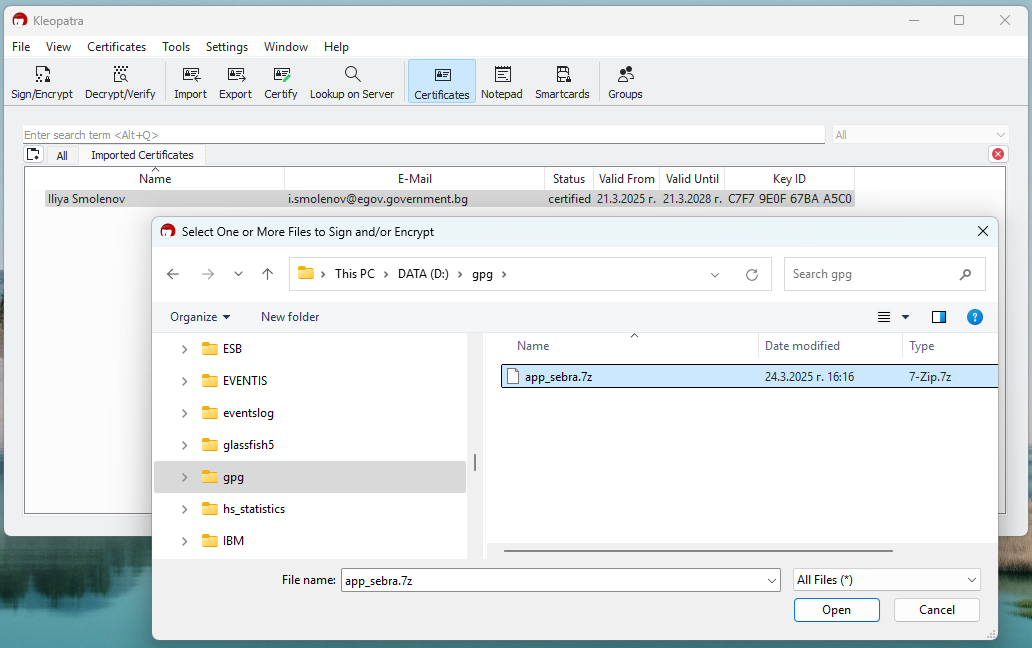
В появилия се панел "Encrypt-To-Self-Warning - Kleopatra" се избира бутон "Продължаване".

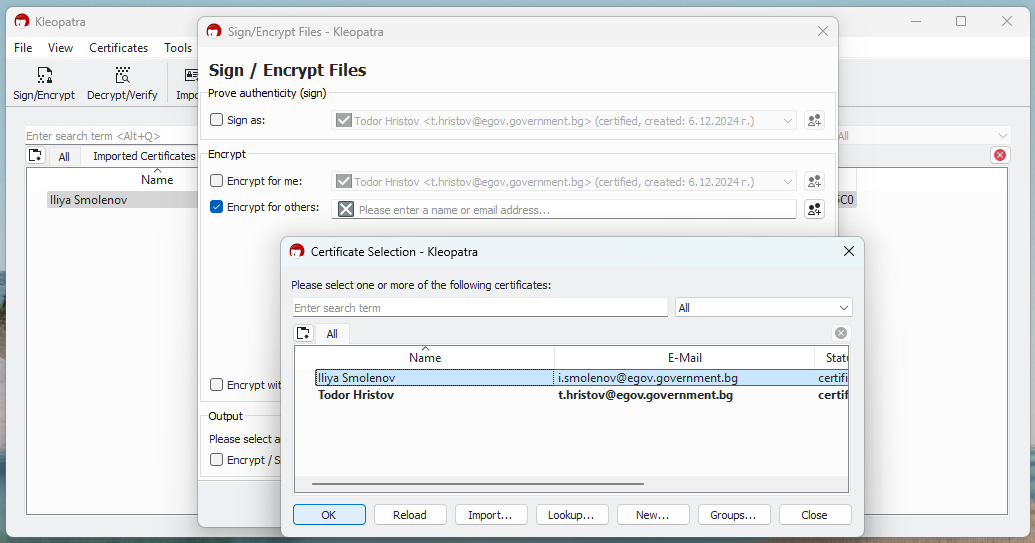
В панел "Sign/Encrypt Files - Kleopatra", се избира бутон "Finish".

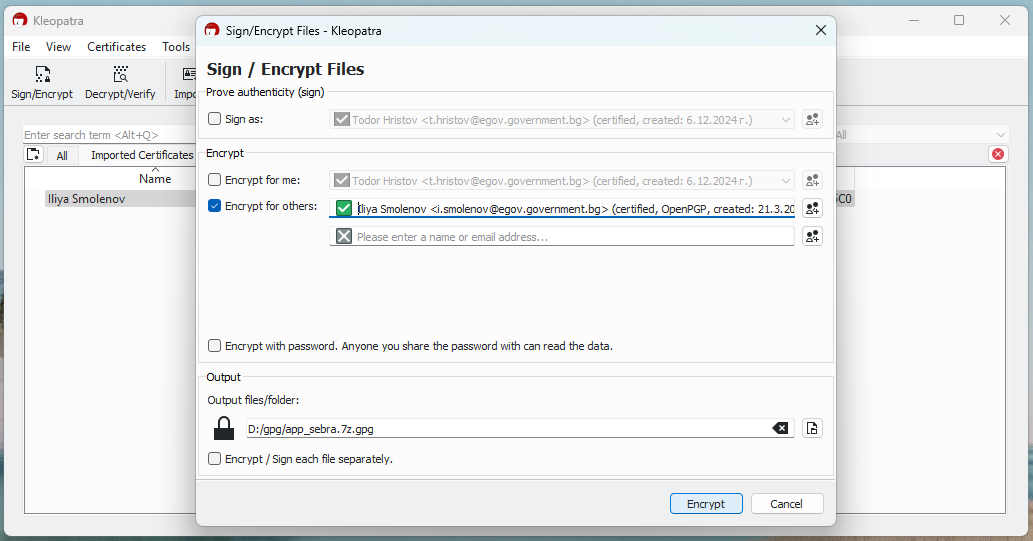
Криптиранея файл "app\_sebra.7z.gpg" може да се види в изпбраната от Вас папка, а ако е оставена по подразбиране, това е папката с файла за криптиране.

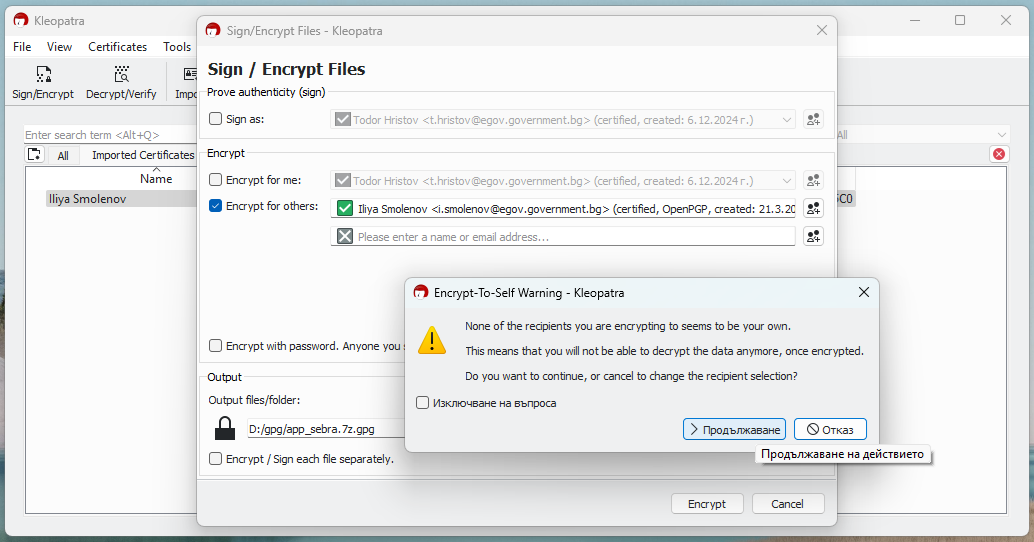


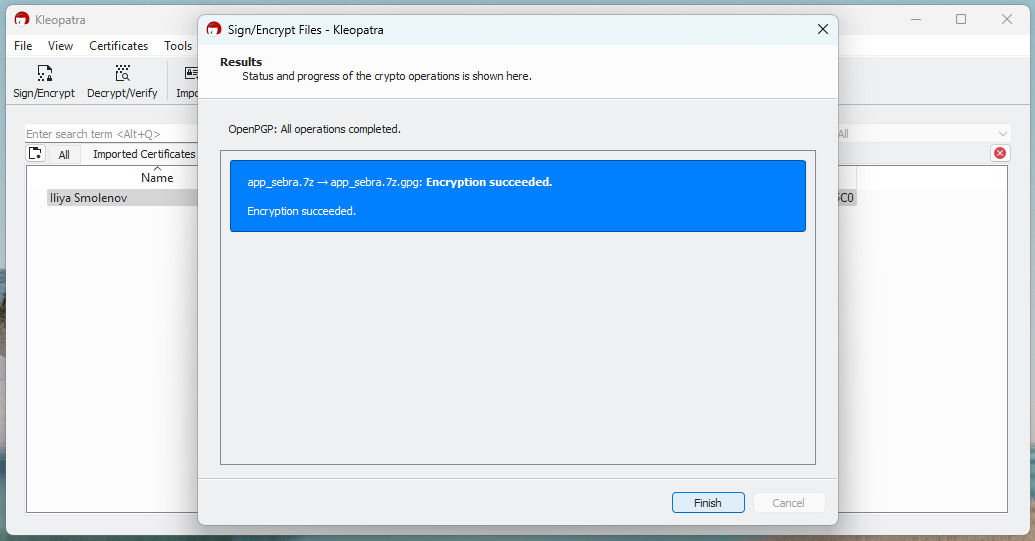


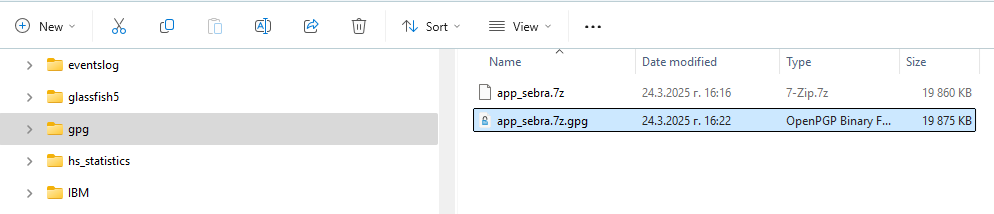










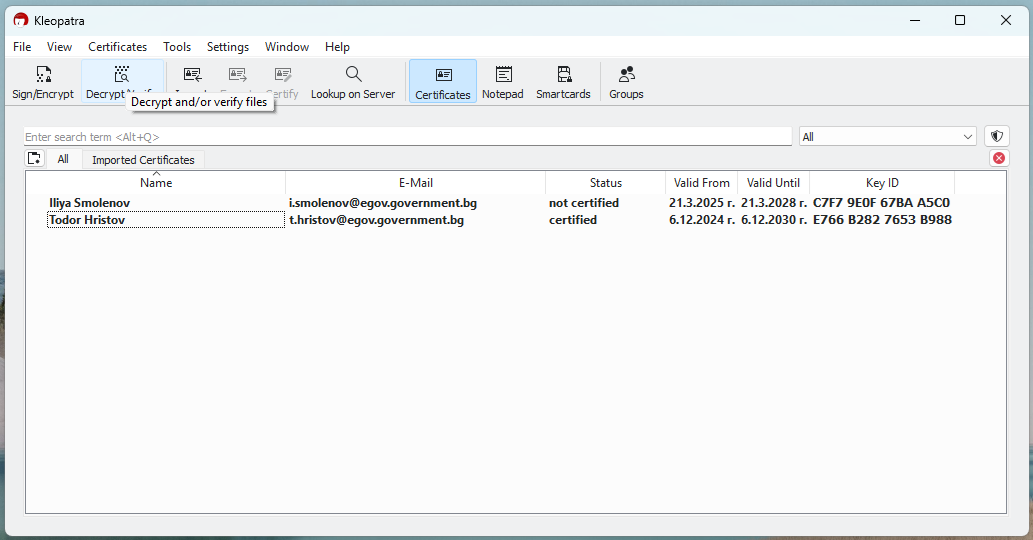


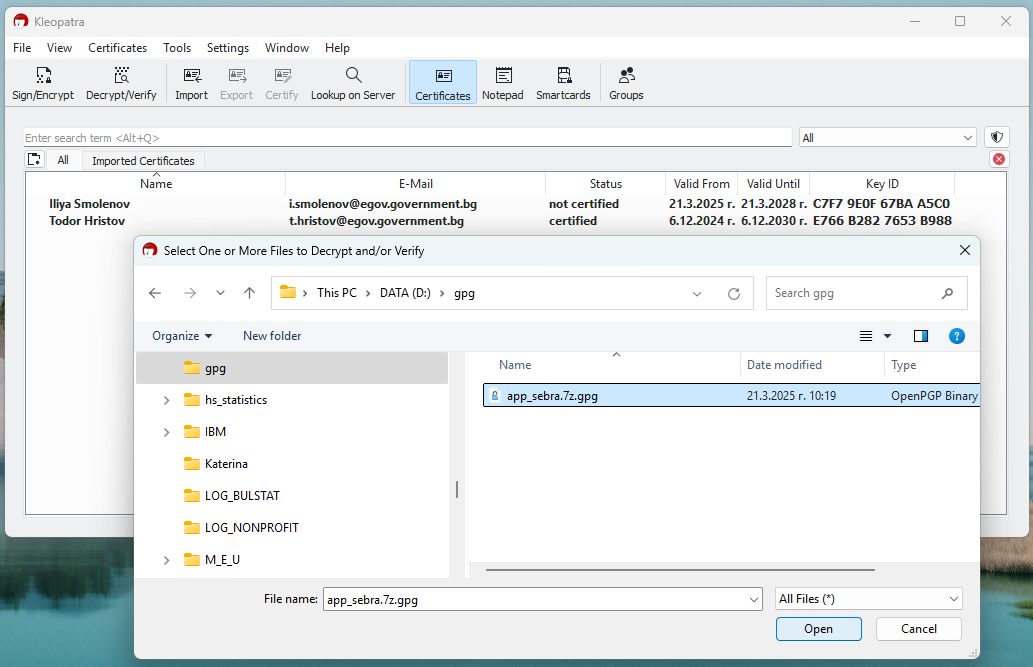
# **[6. Декриптиране на файл.](https://support.brother.com/g/s/id/htmldoc/mfc/dcp_mfc9010cn/bg/html/ug/appendix15_7.html)**

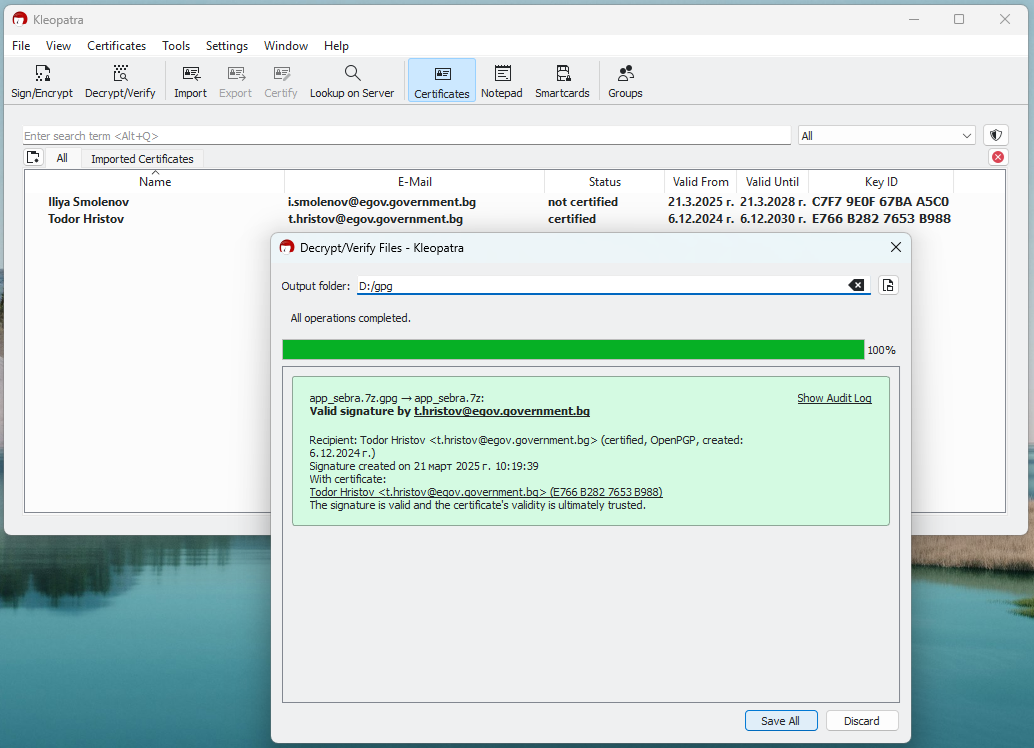
В мениджър на сертификати "Kleopatra" се кликва върху бутон "Decrypt/Verify" и се избира криптирания файл "app\_sebra.7z.gpg".

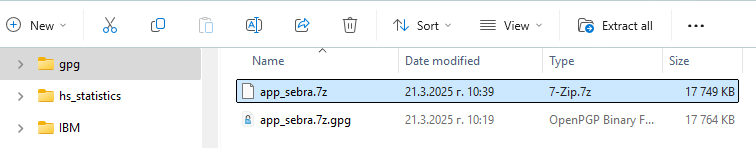
Oт панел "Decrypt/Verify Files - Kleopatra" се избира бутон "Save All"

Във File Explorer можем да видим декриптирания файл "app\_sebra.7z".









# **[7. Импорт на архивиран частен ключ.](https://support.brother.com/g/s/id/htmldoc/mfc/dcp_mfc9010cn/bg/html/ug/appendix15_7.html)**

В мениджър на сертификати "Kleopatra", в Tab "All", маркирате Вашия сертификат и кликвате с десен бутон на мишката.

От popup менюто избирате "Delete".

От появилия се панел "Delete Certificates - Kleopatra" се избира бутон "Delete".

От появилия се панел "Secret Key Deletion - Kleopatra" се избира бутон "Изтриване".

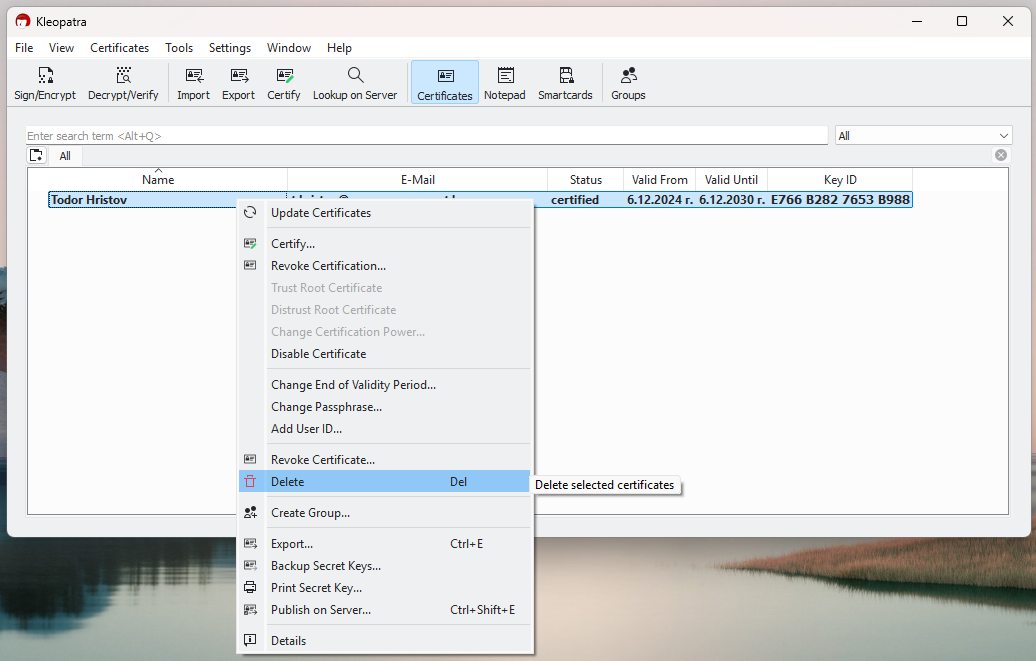
От появилия се панел "pinetry-qt5" се избира бутон "Delete key".

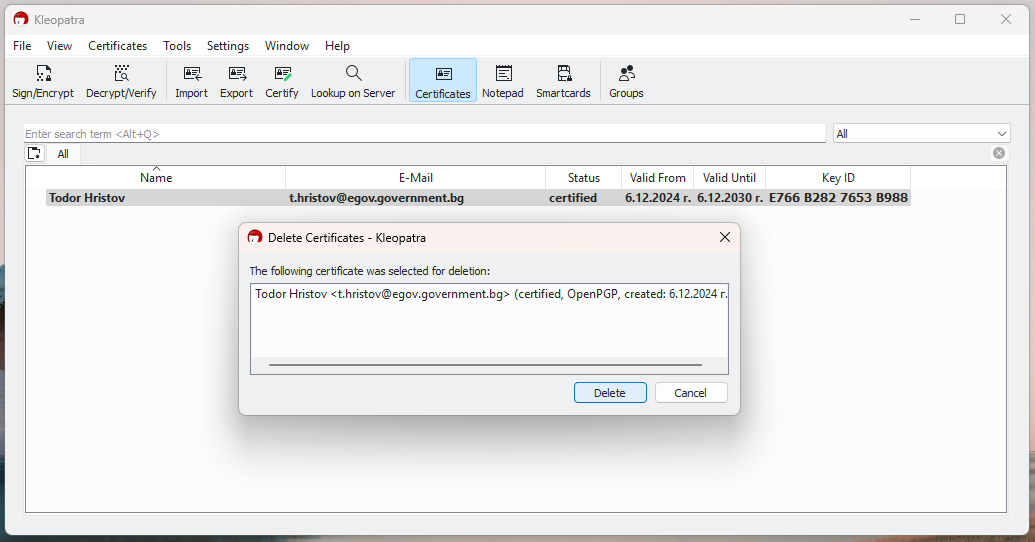
От главния прозорец на мениджър на сертификати "Kleopatra" се избира бутон "Import".

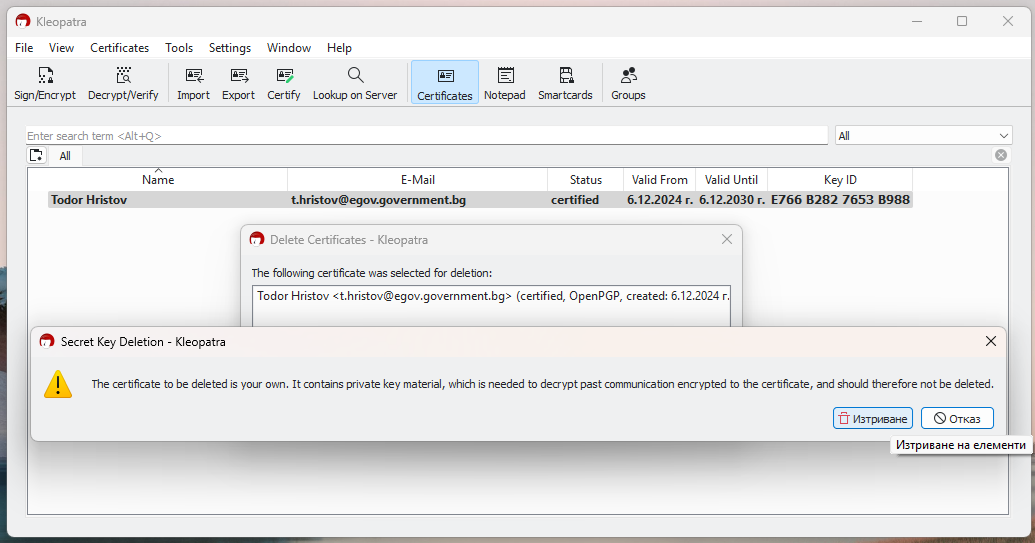
Избирате архивирания секретен ключ.

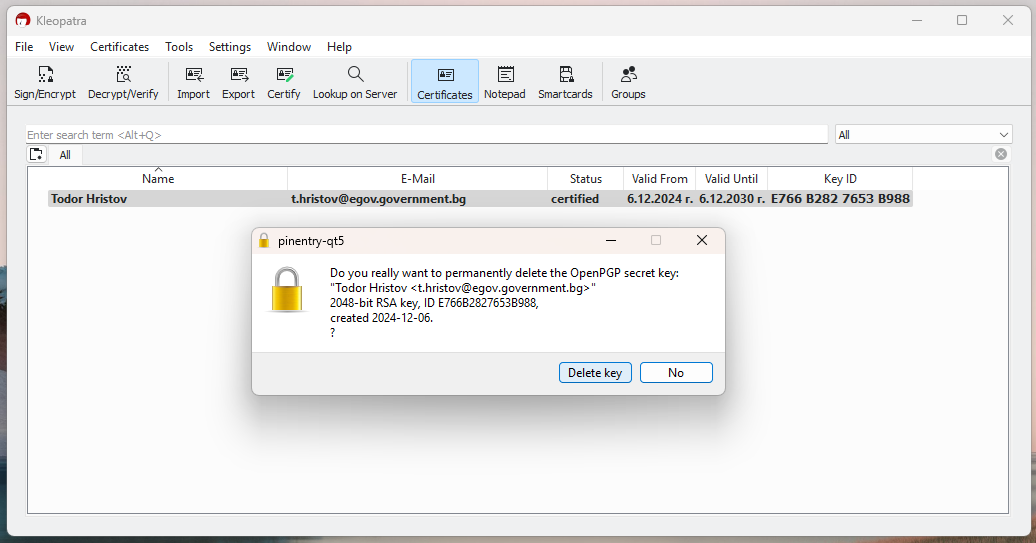
От появилия се панел "Mark Own Certificate - Kleopatra" се избира бутон "Yes, It's Mine".

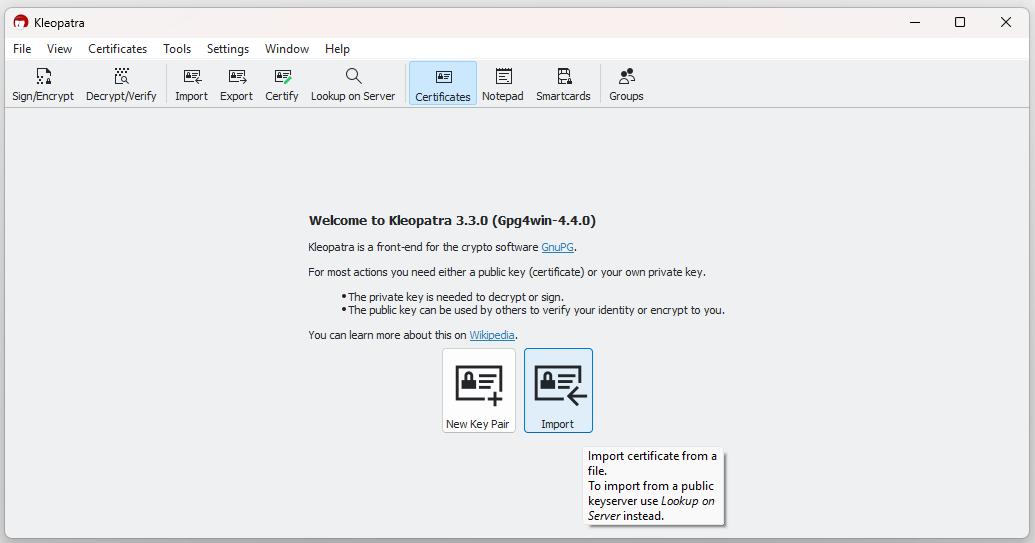
От появилия се панел с резултата "Certificate Import Result - Kleopatra" се избира бутон "Добре".

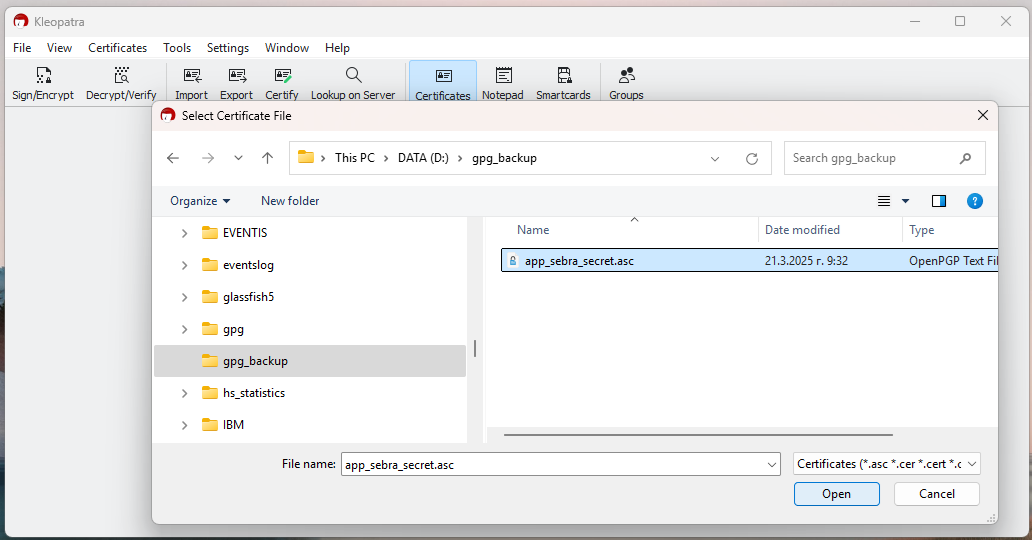


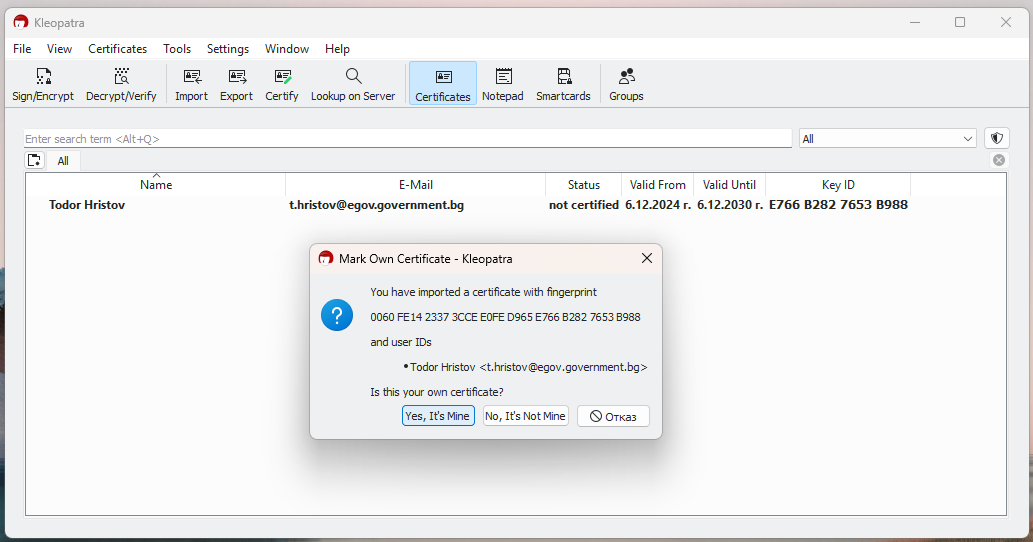


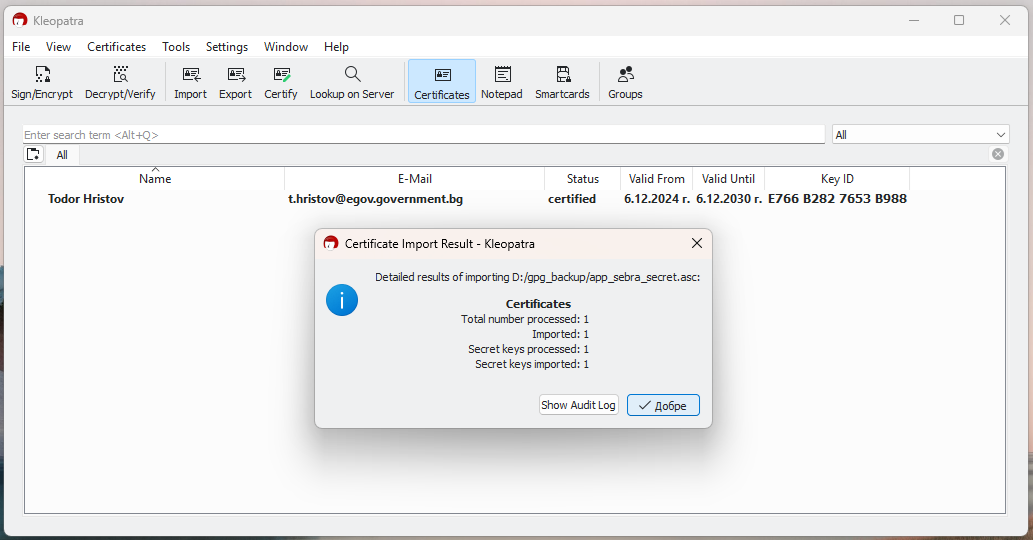












# **[8. Генериране на нова двойка ключове.](https://support.brother.com/g/s/id/htmldoc/mfc/dcp_mfc9010cn/bg/html/ug/appendix15_7.html)**

В мениджър на сертификати "Kleopatra", в Tab "All", маркирате Вашия сертификат и кликвате с десен бутон на мишката.

От popup менюто избирате "Delete".

От появилия се панел "Delete Certificates - Kleopatra" се избира бутон "Delete".

От появилия се панел "Secret Key Deletion - Kleopatra" се избира бутон "Изтриване".

От появилия се панел "pinetry-qt5" се избира бутон "Delete key".

От главния прозорец на мениджър на сертификати "Kleopatra" се избира бутон "New Key Pair".

От появилия се панел "Create OpenPGP Certificate - Kleopatra", може да промените съдържанието на полета "Name" и "Email address" или да ги оставите по подразбиране, и избирате бутон "OK".

От появилия се панел "Success - Kleopatra" потвърждавате успешно създадените ключове с "OK".

