-----BEGIN PGP MESSAGE-----

hQGMA4zJmb2qRccfAQv+PP0ICikBlEraqIREjf67wz1aG44Fcsi/0nZpzq53cn1b
dy0OIcziXtKXI27PNK0hmYN8mBcjo5Pc2ZFgnacnVR/gVMk00GoWkHf9TCZ/ExmQ
XK4CGR7ETkRY7NdBVTct+NsMQA9UJynCf0TlZFWvJcSwLKlDHn/qK6kF9YkH7Ebi
tAJk63Xkkh76iqzx+ohAGAvxc8w/7N/cCdSclZ+xswpSB7EP0tSc37i1FbDtzGAm
vcTHYbuMlbs9ieANOxv/zWP1+PmAYV/FKmR41j33Sor1oAXmTukb0H9hYw01bOPP

GnuPG.com

Encrypt and sign with GnuPG VS-Desktop®

Quick guide for users

The guide applies accordingly to GnuPG Desktop®

Document version 2.3

Introduction

This guide is a tutorial for users to get started with the public key encryption of GnuPG VS-Desktop®. Below you will find a step-by-step description of VS-NfD (RESTRICTED) compliant encryption and decryption of files via the Windows Explorer.

The software also supports the less secure symmetric or password based encryption. This is covered in the quick guide "Password based encryption with GnuPG VS-Desktop®".

Please also be sure to note the information provided by your security officer.

Functional description

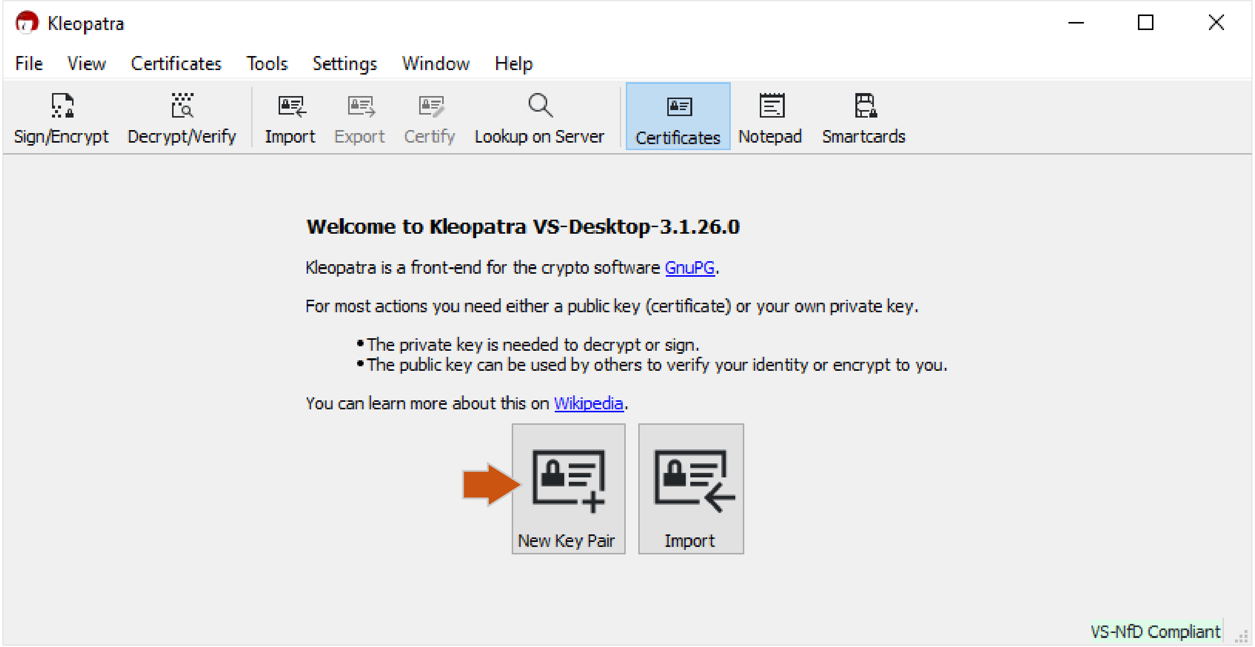
GnuPG VS-Desktop® provides you with end-to-end encryption, allowing you to encrypt and decrypt mails and files, as well as generate and verify digital signatures. It consists of independently developed programs, including the certificate manager Kleopatra, the Outlook Add-In GpgOL for mail encryption and the Windows extension GpgEX for file encryption.

Smartcards resp. security tokens can be used optionally when using GnuPG VS-Desktop®. The secret key material is then stored there and is thus significantly better protected against unauthorized access.

It is recommended that you ask your IT administrator / support if you have any technical questions.

1 Create a key

If you have not yet created or imported your own OpenPGP key pair, you will see the “Welcome” message when you start Kleopatra. If you already have your own key, you can now import it. Otherwise, click on the button New Key Pair :



Welcome to Kleopatra VS-Desktop-3.1.26.0

Kleopatra is a front-end for the crypto software GnuPG.

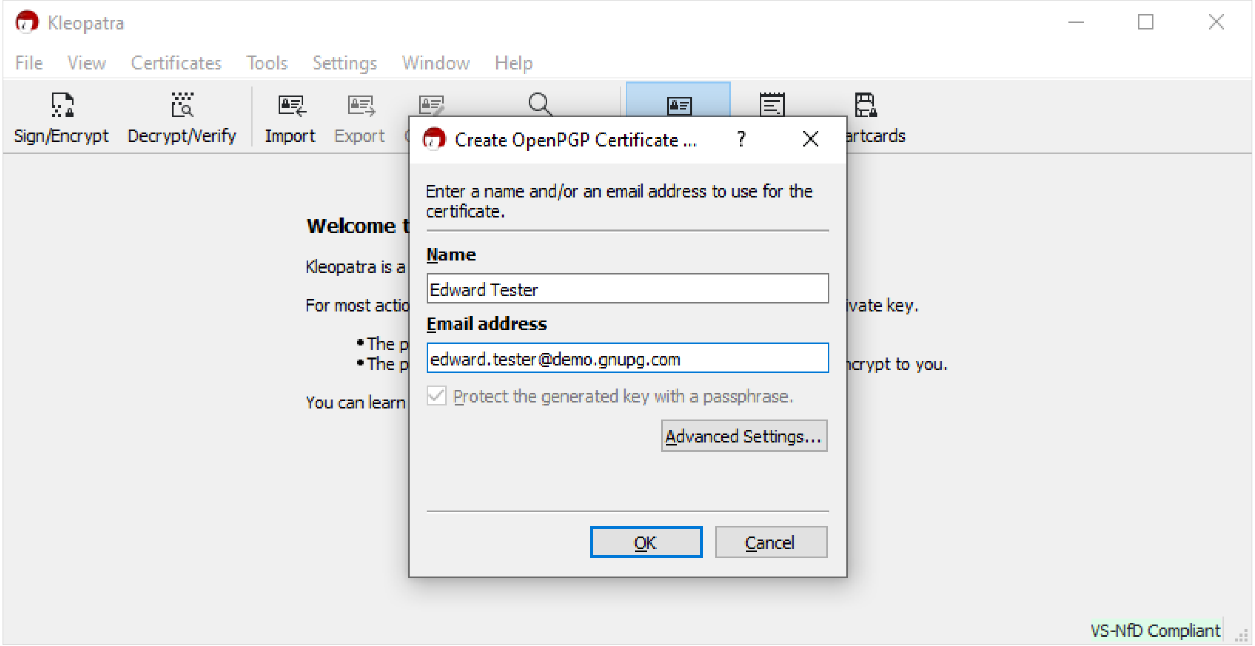
For most actions you need either a public key (certificate) or your own private key.

- The private key is needed to decrypt or sign.
- The public key can be used by others to verify your identity or encrypt to you.

You can learn more about this on Wikipedia.

If no welcome message appears, because keys have already been pre-installed by your organization, new keys can be created via File > New Key Pair.

Enter your name and mail address and click on OK :



Enter a name and/or an email address to use for the certificate.

Name

Edward Tester

Email address

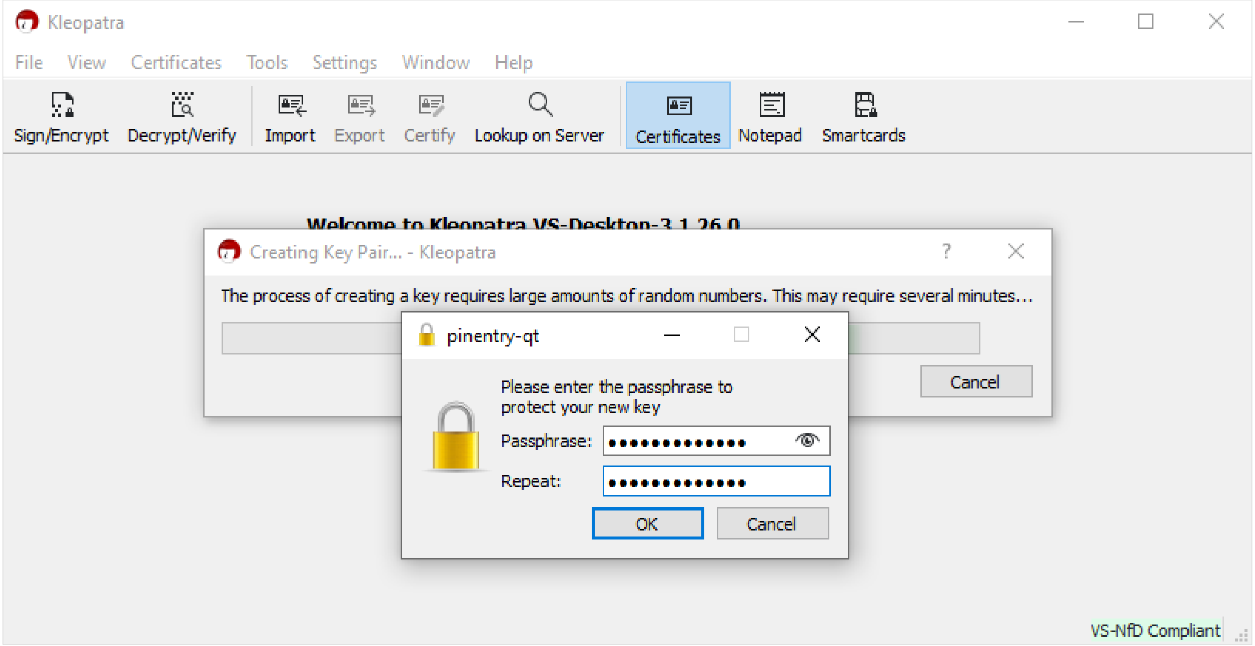
edward.tester@demo.gnupg.com

☑ Protect the generated key with a passphrase.

💡 **Note**

Keys do not always have to be bound to a mail address. You can also use project or group names, for example.

After that you will be asked to enter a passphrase (= password) with at least 9 characters. It is best to use nonsensical strings of words or phrases, which you can easily remember. If applicable, keep in mind your organizational password policies:



The process of creating a key requires large amounts of random numbers. This may require several minutes...

Please enter the passphrase to protect your new key

Passphrase: •••••••••••••

Repeat: •••••••••••••

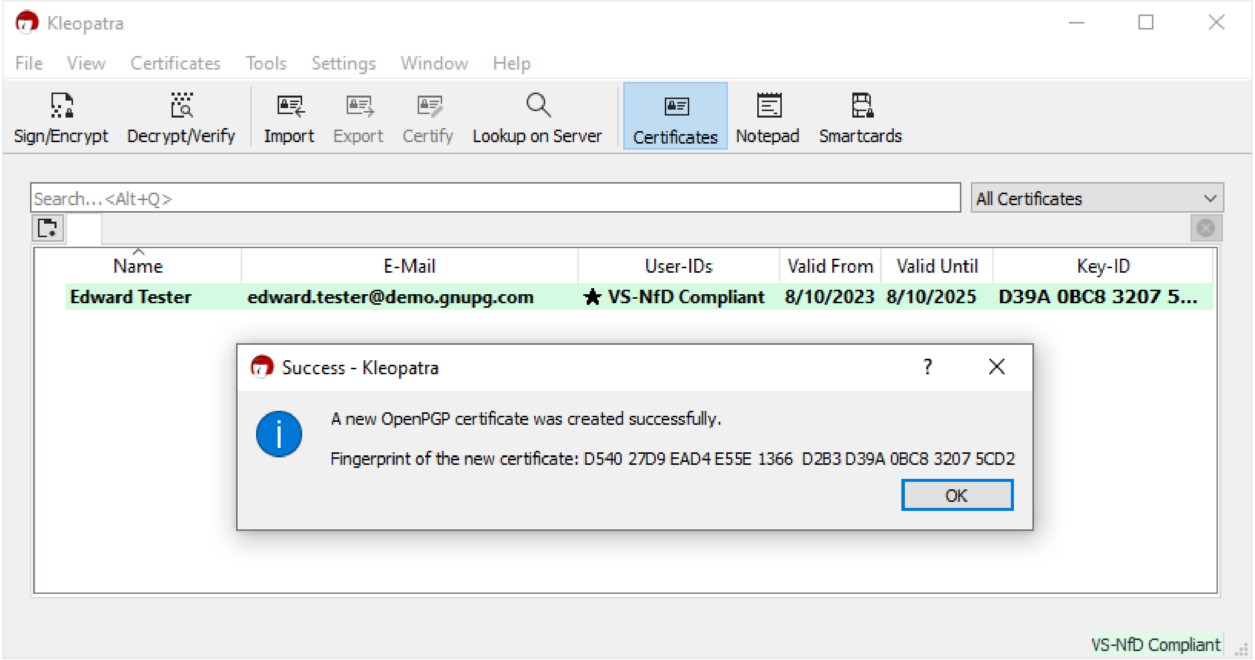
⚠️ **Important**

The password (= passphrase) of the key **cannot be reset**. If you loose the password, you will no longer be able to decrypt data encrypted to this key. You should therefore make a note of the password immediately and store it securely and in compliance with VS-NfD or other security regulations, whichever applies.

However, you have an infinite number of attempts to guess a password for an OpenPGP key which is stored on disk. The 3 attempts displayed can always be repeated. (**This does not apply to PINs**, i.e. if the key is on a smartcard.).

Both the secret part of the OpenPGP key and the associated password must be treated as classified information, the corresponding protective measures apply.

Kleopatra finally shows you whether the generation was successful. Confirm this dialog by clicking OK. Your new key is displayed in the certificates menu:



Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Edward Tester	edward.tester@demo.gnupg.com	★ VS-NfD Compliant	8/10/2023	8/10/2025	D39A 0BC8 3207 5...

Success - Kleopatra

A new OpenPGP certificate was created successfully.

Fingerprint of the new certificate: D540 27D9 EAD4 E55E 1366 D2B3 D39A 0BC8 3207 5CD2

By default, a key created with GnuPG VS-Desktop® has a validity period of 3 years (since version 3.2.0, previously 2 years), which is the period recommended by the German BSI.

Some time (e.g. one month) before your key expires, you should extend it by right-clicking → Change end of validity period.

Both after creating and extending your OpenPGP key, you must distribute the corresponding certificate (= public key) to your communication partners, see the next chapter.

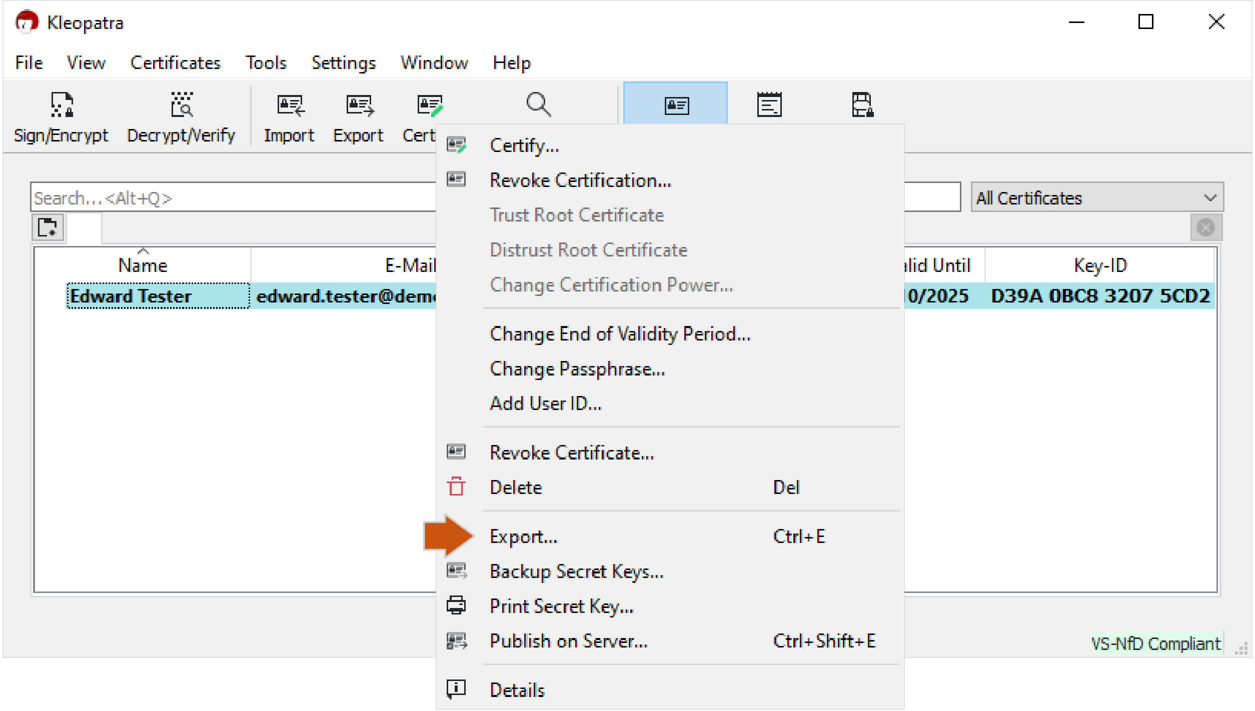
💡 **Note**

If you are asked for the corresponding password when using the OpenPGP key **stored on your computer**, you will be informed that you only have 2 attempts left if you fail, and so on. This only applies to the current process. You can repeat the process as often as you like and have 3 attempts each time.

Please note: **This does not apply when using smartcards!** Smartcards are blocked as soon as their PIN has been entered incorrectly 3 times.

2 Share certificates

Open the context menu of your key with the right mouse button and click on Export. You can also find this command in the upper menu ribbon of Kleopatra:

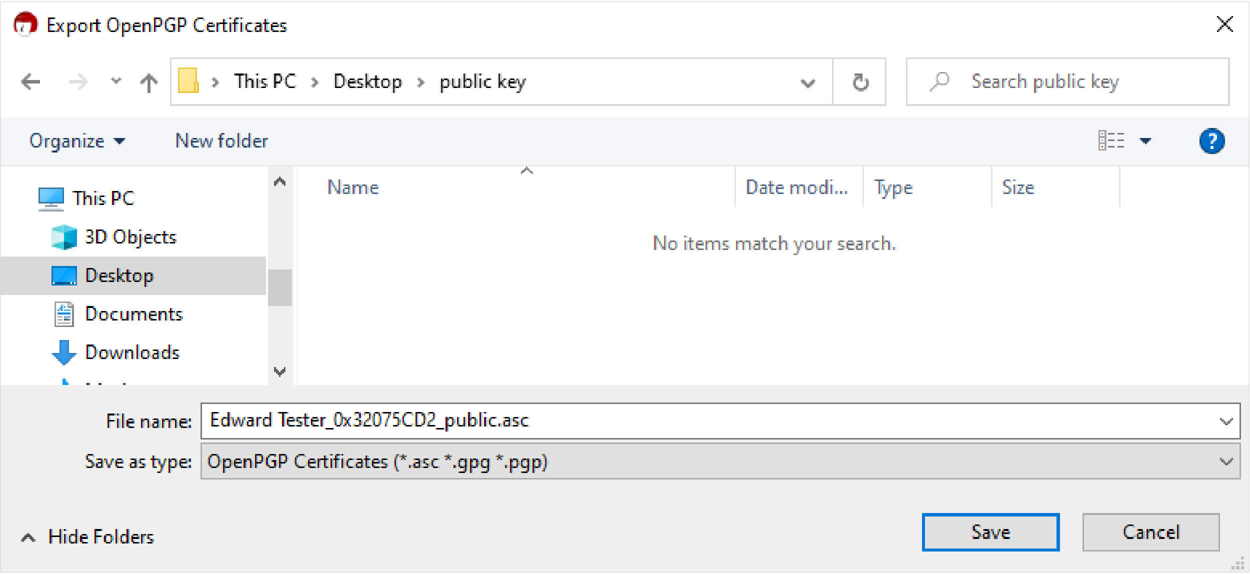


Edward Tester edward.tester@dem 0/2025 D39A 0BC8 3207 5CD2

Note

You can export several public keys (certificates) at once.

Choose a directory and a file name for your public key and click the Save -button:



File name: Edward Tester_0x32075CD2_public.asc

Save as type: OpenPGP Certificates (*.asc *.gpg *.pgp)

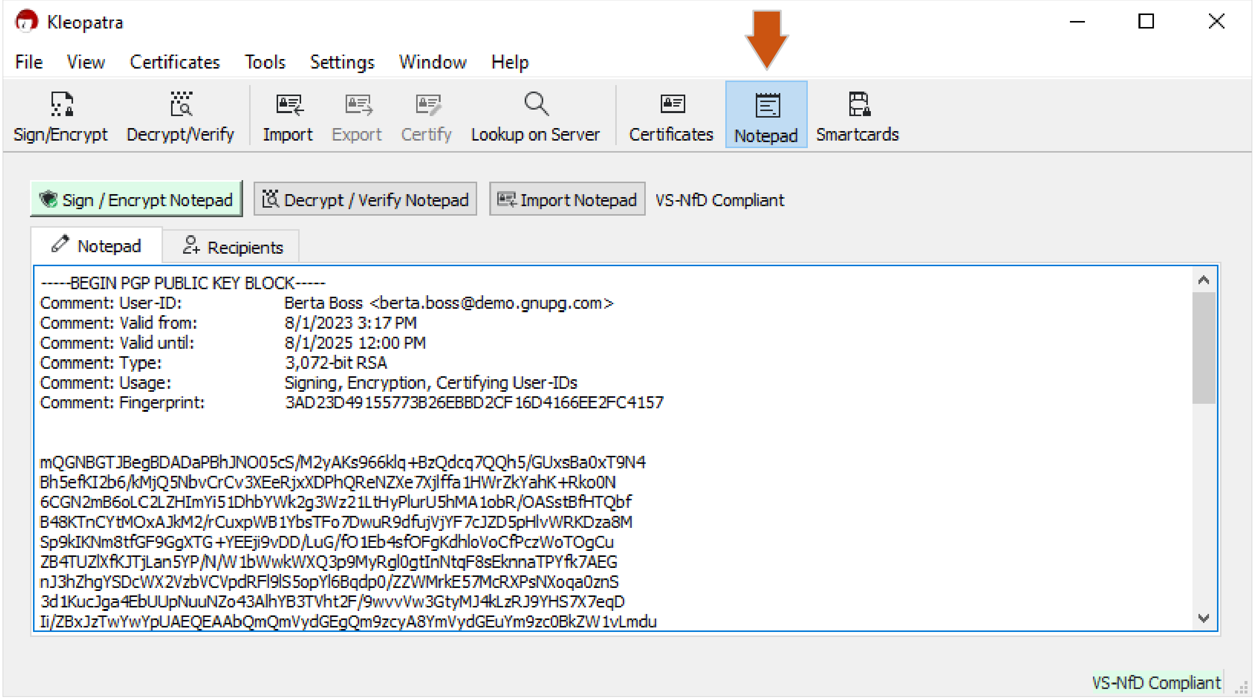
💡 **Note**

Public keys (Certificates) are not classified and may be forwarded unencrypted. The fingerprint ensures the integrity of the key.

3 Import certificates

For secure communication, you need the public keys resp. certificates of your communication partners. If you receive keys as a file, usually with the file extension ***.asc** or ***.key**, import them directly into Kleopatra by double-clicking.

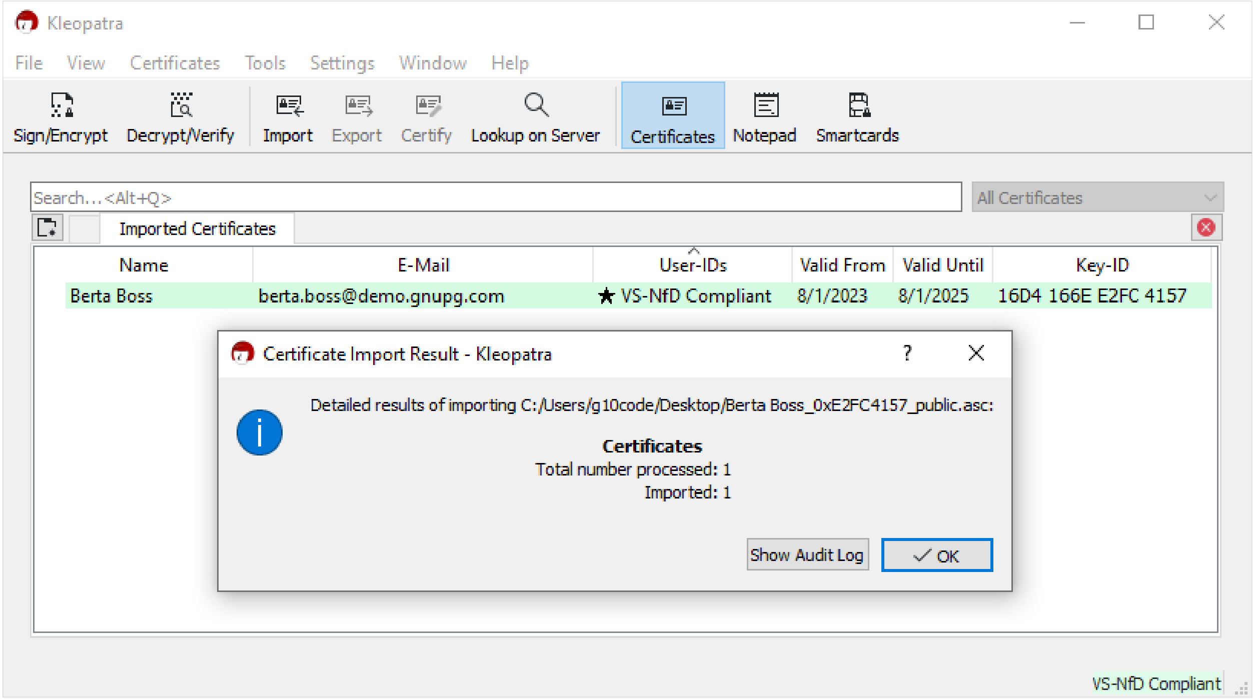
Alternatively, it is also common to import public keys as a text block via copy/paste, e.g. from web pages. To do this, use the Notepad-function:



```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: User-ID:          Berta Boss <berta.boss@demo.gnupg.com>
Comment: Valid from:       8/1/2023 3:17 PM
Comment: Valid until:      8/1/2025 12:00 PM
Comment: Type:             3,072-bit RSA
Comment: Usage:            Signing, Encryption, Certifying User-IDs
Comment: Fingerprint:      3AD23D49155773B26EBBD2CF16D4166EE2FC4157


mQGNBGTJBegBDADaPBhJNO05cS/M2yAKs966klq+BzQdcq7QQh5/GUxsBa0xT9N4
Bh5efKI2b6/kMjQ5NbvCrCv3XEeRjxXDPhQReNZXe7Xjlffa1HWrZkYahK+Rko0N
6CGN2mB6oLC2LZHImYi51DhbYWk2g3Wz21LtHyPlurU5hMA1obR/OASstBfHTQbf
B48KTnCYtMOxAJkM2/rCuxpWB1YbsTFo7DwuR9dfujVjYF7cJZD5pHlvWRKDza8M
Sp9kIKNm8tfGF9GgXTG+YEEji9vDD/LuG/fO1Eb4sfOFgKdhloVoCfPczWoTOgCu
ZB4TUZlXfKJTjLan5YP/N/W1bWwkWXQ3p9MyRgl0gtInNtqF8sEknnaTPYfk7AEG
nJ3hZhgYSDcWX2VzbVCVpdRFl9lS5opYl6Bqdp0/ZZWMrkE57McRXPsNXoqa0znS
3d1KucJga4EbUUpNuuNZo43AlhYB3TVht2F/9wvvVw3GtyMJ4kLzRJ9YHS7X7eqD
Ii/ZBxJzTwYwYpUAEQEAAbQmQmVydGEgQm9zcyA8YmVydGEuYm9zc0BkZW1vLmdu
```

If the imported public key is already certified by your organization, you are merely informed about the import. The key is then highlighted in green and marked as VS-NfD (RESTRICTED) compliant:



Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Berta Boss	berta.boss@demo.gnupg.com	★ VS-NfD Compliant	8/1/2023	8/1/2025	16D4 166E E2FC 4157

Certificate Import Result - Kleopatra

Detailed results of importing C:/Users/g10code/Desktop/Berta Boss_0xE2FC4157_public.asc:

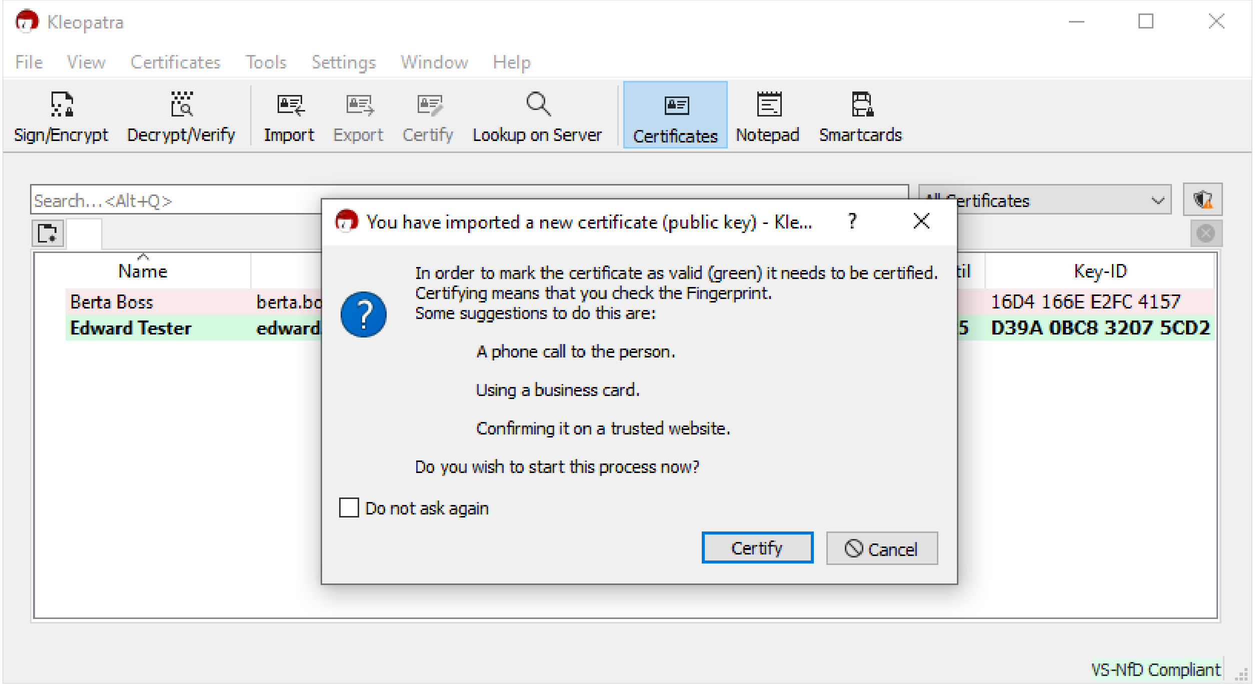
Certificates

Total number processed: 1

Imported: 1

In this case, continue with chapter 5.

Otherwise, you will be asked if you want to certify the public key now:



Name			Key-ID
Berta Boss	berta.bo		16D4 166E E2FC 4157
Edward Tester	**edward**	**5**	**D39A 0BC8 3207 5CD2**

You have imported a new certificate (public key) - Kle...

In order to mark the certificate as valid (green) it needs to be certified.
Certifying means that you check the Fingerprint.
Some suggestions to do this are:

A phone call to the person.

Using a business card.

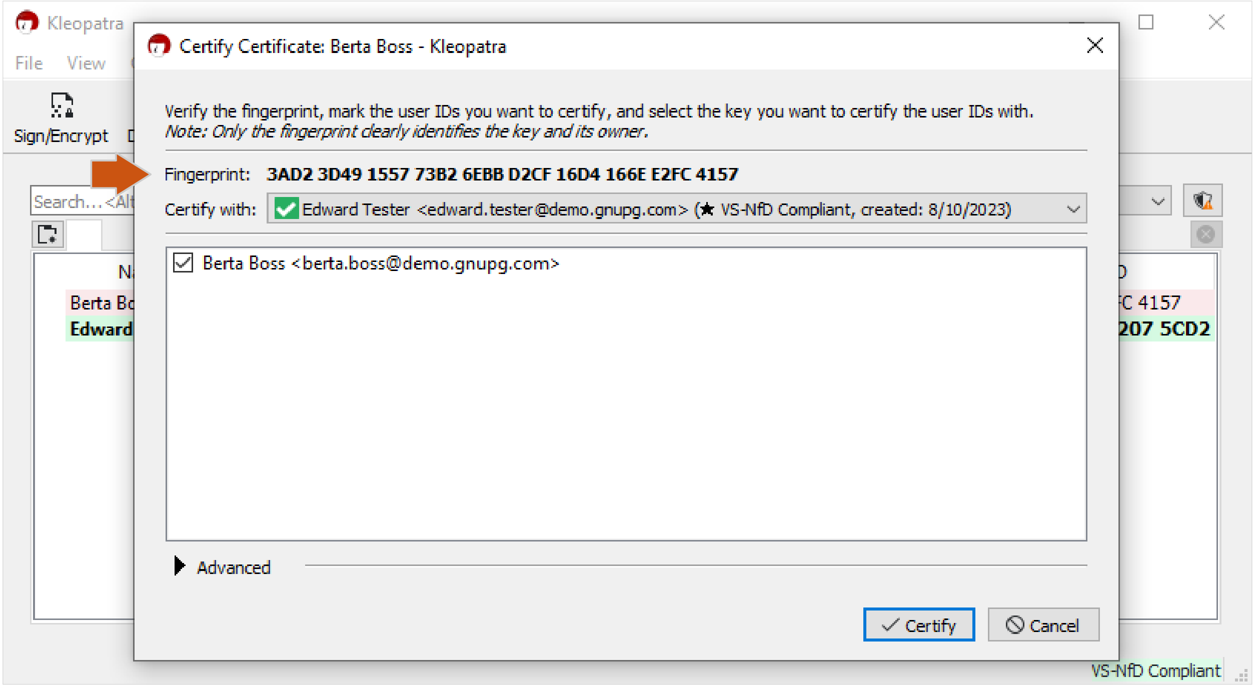
Confirming it on a trusted website.

Do you wish to start this process now?

□ Do not ask again

We recommend that you confirm with Certify.

Verify the Fingerprint via a second channel, e.g. by phone, and after that click on Certify:



Certify Certificate: Berta Boss - Kleopatra

Verify the fingerprint, mark the user IDs you want to certify, and select the key you want to certify the user IDs with.
Note: Only the fingerprint clearly identifies the key and its owner.

Fingerprint: **3AD2 3D49 1557 73B2 6EBB D2CF 16D4 166E E2FC 4157**

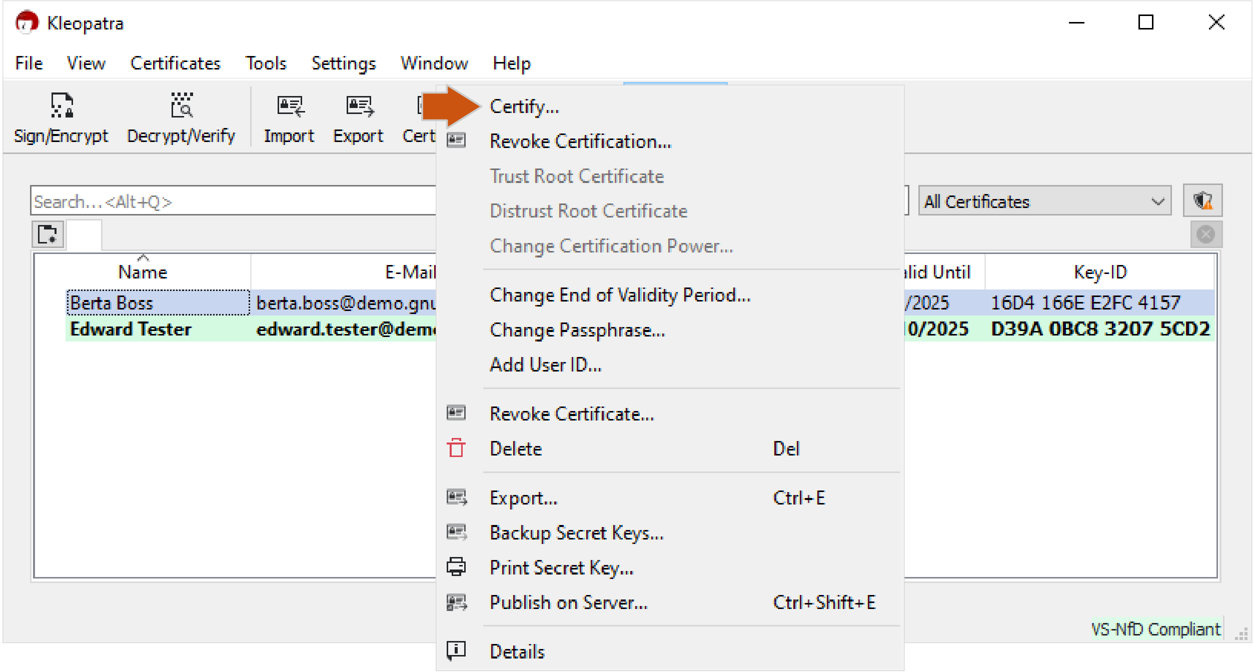
Certify with: ✓ Edward Tester <edward.tester@demo.gnupg.com> (★ VS-NfD Compliant, created: 8/10/2023)

☑ Berta Boss <berta.boss@demo.gnupg.com>

4 Trust and certification

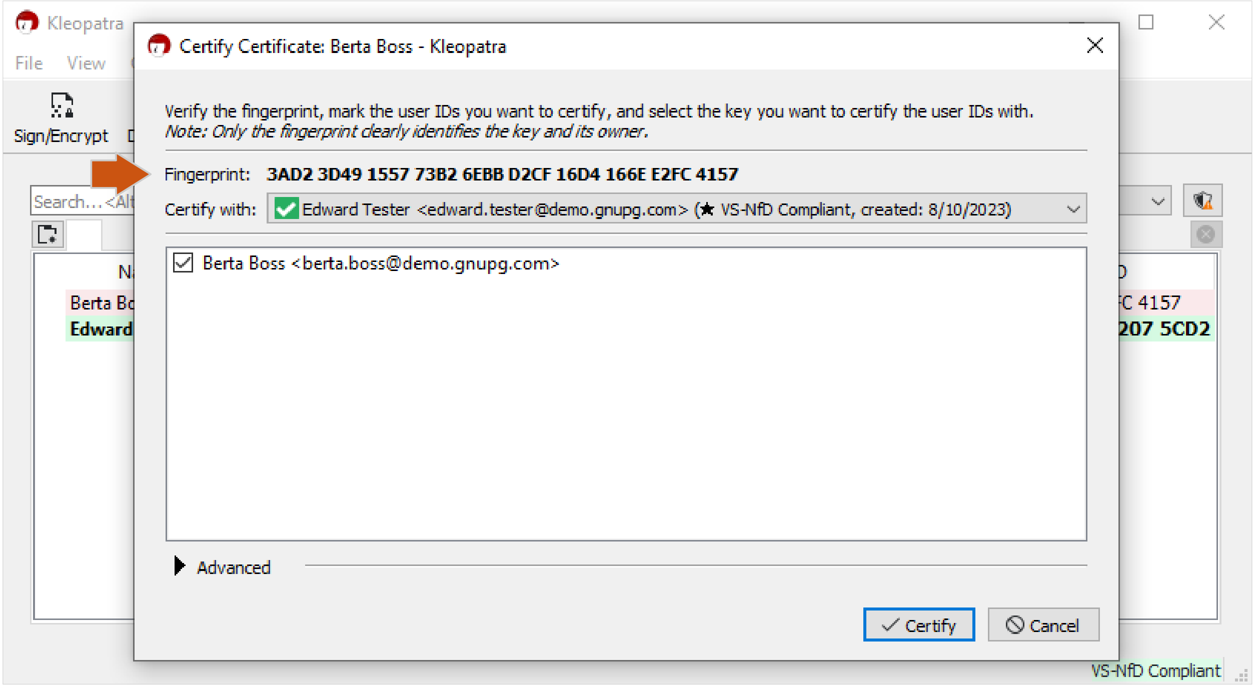
A key has to be certified before it can be used for VS-NfD compliant secure communication. Ideally, your organization has already done this for you.

If no trusted authority has certified this key, it is highlighted in red and marked "not certified". In this case you are responsible for the certification of the key. To do this, right-click to open the context menu of the imported key and select Certify :



Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Cert
Search...<Alt+Q>
All Certificates
Name E-Mail
Berta Boss berta.boss@demo.gnu
Edward Tester edward.tester@dem
lid Until Key-ID
/2025 16D4 166E E2FC 4157
0/2025 D39A 0BC8 3207 5CD2
Certify...
Revoke Certification...
Trust Root Certificate
Distrust Root Certificate
Change Certification Power...
Change End of Validity Period...
Change Passphrase...
Add User ID...
Revoke Certificate...
Delete Del
Export... Ctrl+E
Backup Secret Keys...
Print Secret Key...
Publish on Server... Ctrl+Shift+E
Details
VS-NfD Compliant

Verify the Fingerprint via a second channel - e.g. by phone - and after that click on Certify :



Certify Certificate: Berta Boss - Kleopatra

Verify the fingerprint, mark the user IDs you want to certify, and select the key you want to certify the user IDs with.
Note: Only the fingerprint clearly identifies the key and its owner.

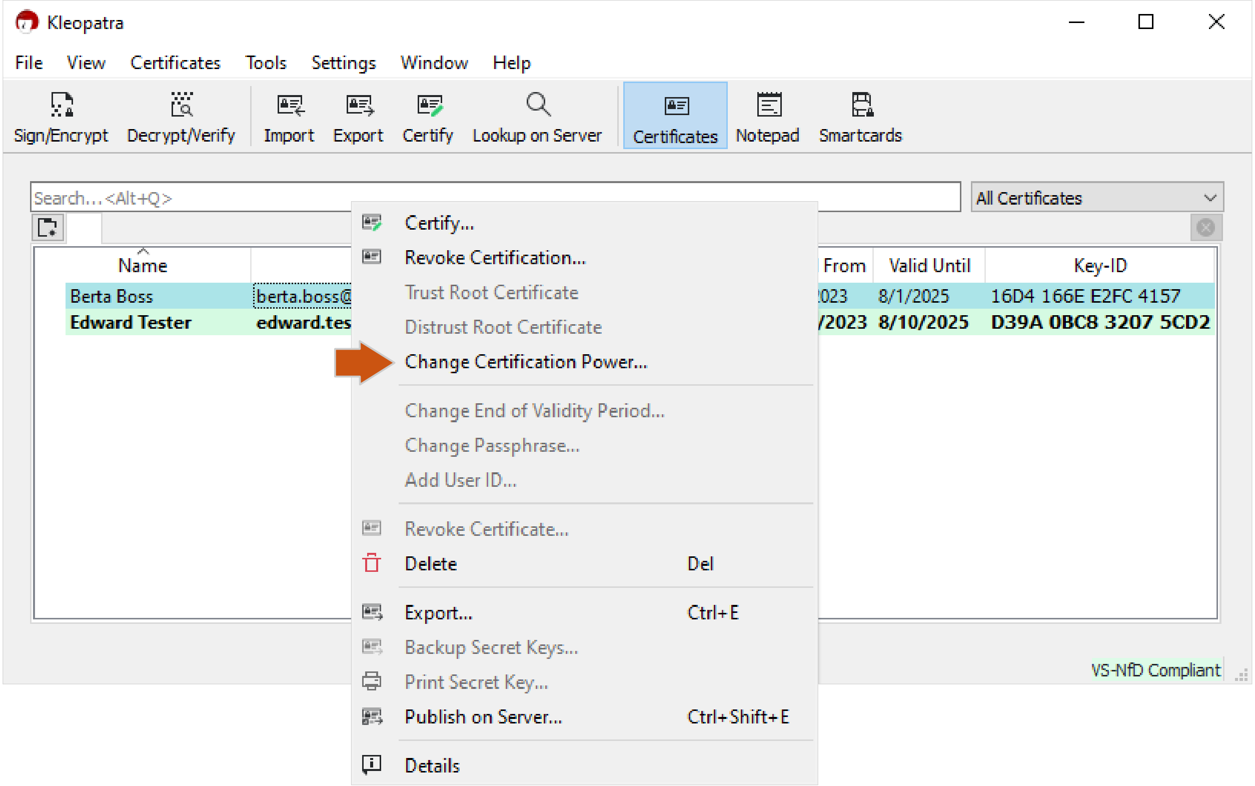
Fingerprint: **3AD2 3D49 1557 73B2 6EBB D2CF 16D4 166E E2FC 4157**

Certify with: ✓ Edward Tester <edward.tester@demo.gnupg.com> (★ VS-NfD Compliant, created: 8/10/2023)

☑ Berta Boss <berta.boss@demo.gnupg.com>

The fingerprint verification must be done once per organization. If e.g. a coworker has already checked the fingerprint by phone, you can set their certification trust on "full trust" and then their certifications will also be accepted by you.

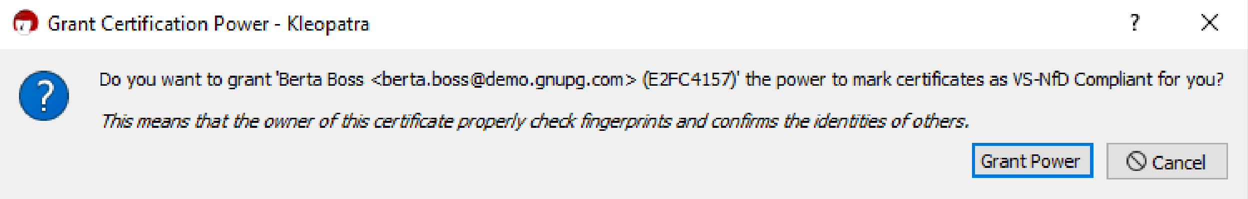
To do this, click on Change Certification Power in the context menu:



Name		From	Valid Until	Key-ID
Berta Boss	berta.boss@	023	8/1/2025	16D4 166E E2FC 4157
Edward Tester	**edward.tes**	**/2023**	**8/10/2025**	**D39A 0BC8 3207 5CD2**

Kleopatra
File View Certificates Tools Settings Window Help
Sign/Encrypt Decrypt/Verify Import Export Certify Lookup on Server Certificates Notepad Smartcards
Search...<Alt+Q>
All Certificates
Certify...
Revoke Certification...
Trust Root Certificate
Distrust Root Certificate
Change Certification Power...
Change End of Validity Period...
Change Passphrase...
Add User ID...
Revoke Certificate...
Delete Del
Export... Ctrl+E
Backup Secret Keys...
Print Secret Key...
Publish on Server... Ctrl+Shift+E
Details
VS-NfD Compliant

Then select Grant Power :



Do you want to grant 'Berta Boss <berta.boss@demo.gnupg.com> (E2FC4157)' the power to mark certificates as VS-NfD Compliant for you?

This means that the owner of this certificate properly check fingerprints and confirms the identities of others.

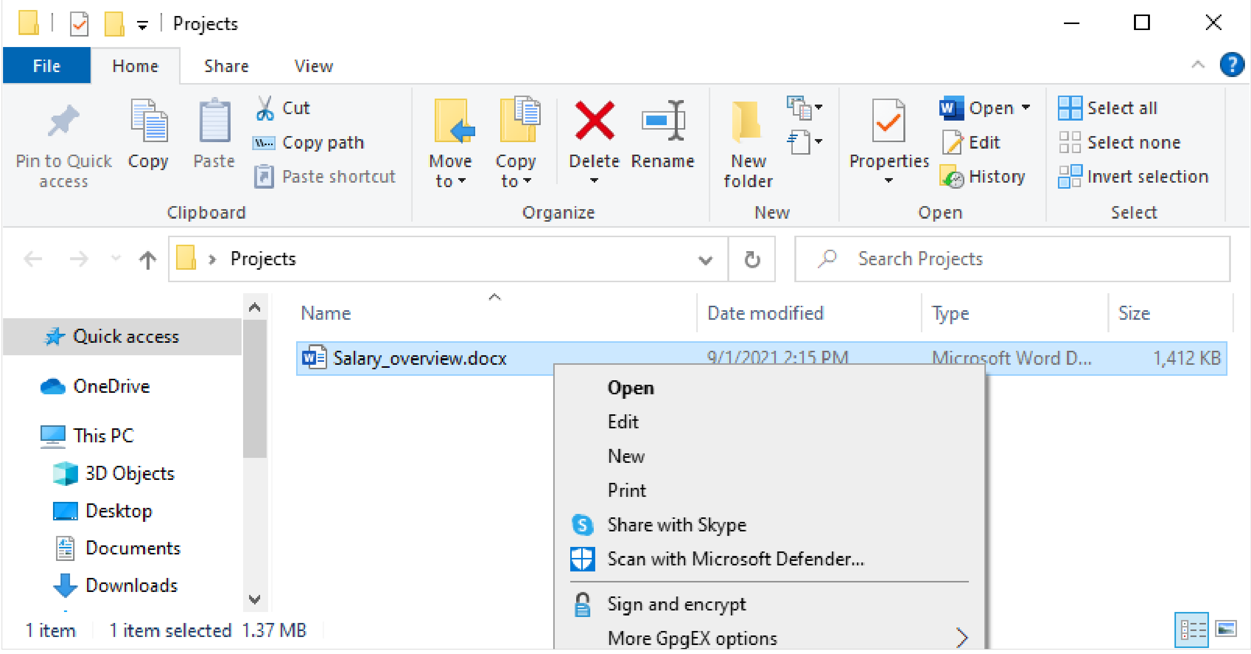
Should a certificate already have certification power, the dialog gives you the option to revoke certification power.

Note

You can add columns to the certificate view via right-click. One of the optional columns is "certification trust". At levels "full" and "ultimate", certification power is granted.

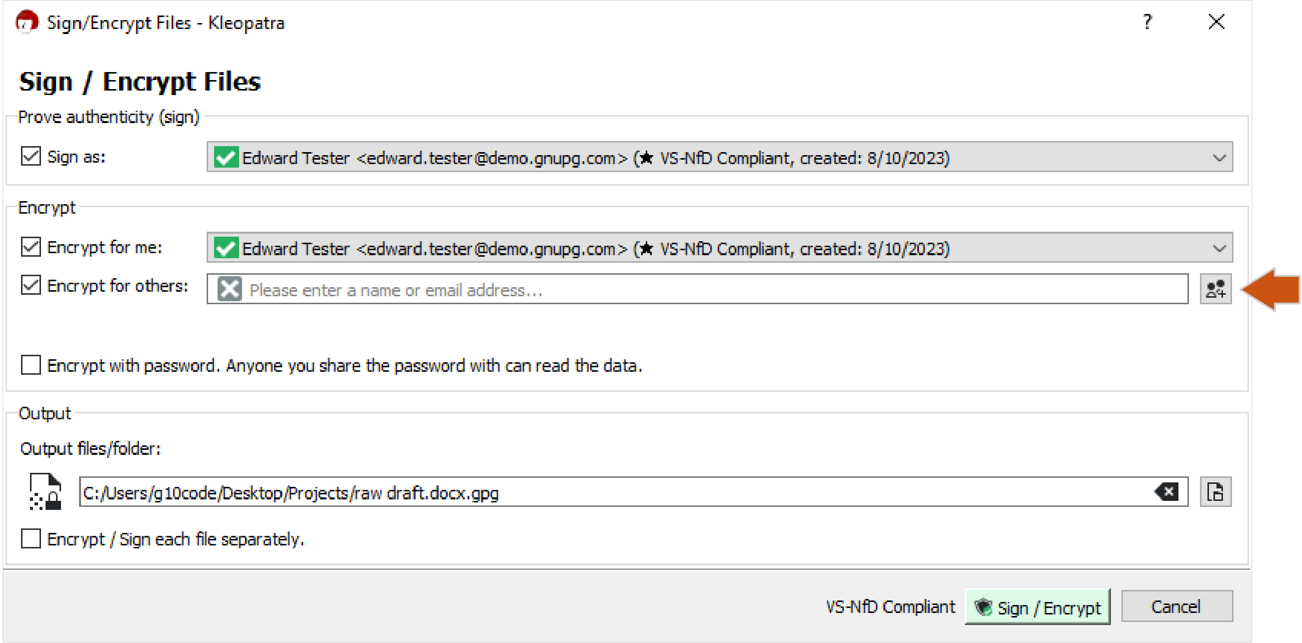
5 Encrypt files

Select one or more files or folders you want to encrypt in the Windows Explorer[1]. Open the context menu with the right mouse button and select Sign and encrypt :



[1] If you take the path via "(Folder) Sign/Encrypt" in Kleopatra instead, note that only folders or only files can be selected there.

Select who should be able to decrypt your file:



Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: Edward Tester <edward.tester@demo.gnupg.com> (★ VS-NfD Compliant, created: 8/10/2023)

Encrypt

☑ Encrypt for me: Edward Tester <edward.tester@demo.gnupg.com> (★ VS-NfD Compliant, created: 8/10/2023)

☑ Encrypt for others: Please enter a name or email address...

□ Encrypt with password. Anyone you share the password with can read the data.

Output

Output files/folder:

C:/Users/g10code/Desktop/Projects/raw draft.docx.gpg

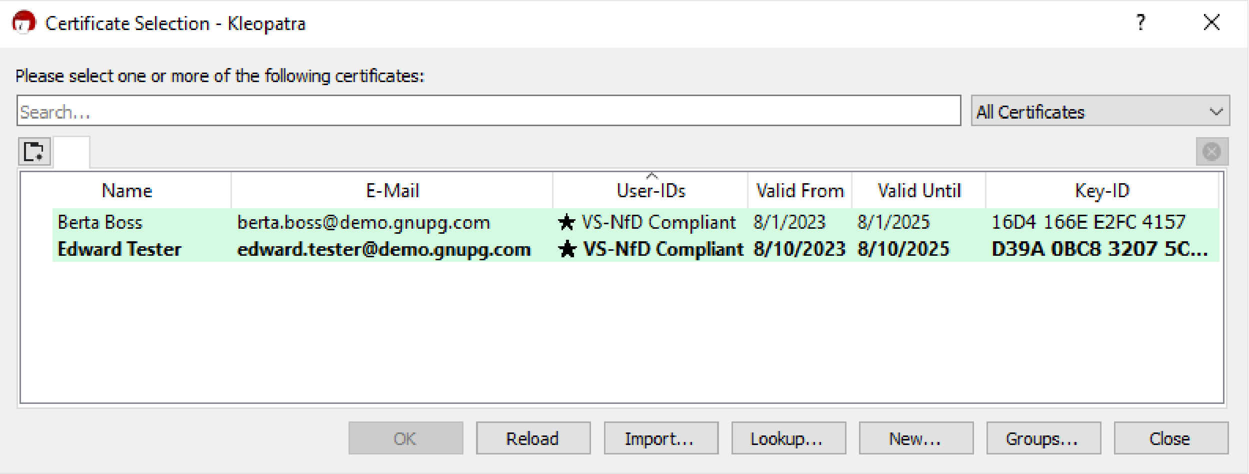
□ Encrypt / Sign each file separately.

VS-NfD Compliant

⚠ **Important**

If you do not add other recipients, no one but you can decrypt the file!

In the "Encrypt for others" field, type the name of the desired recipient to select a certificate. Alternatively, use the button on the right side of the recipient line to open the selection dialog, your personal crypto address book, so to speak:



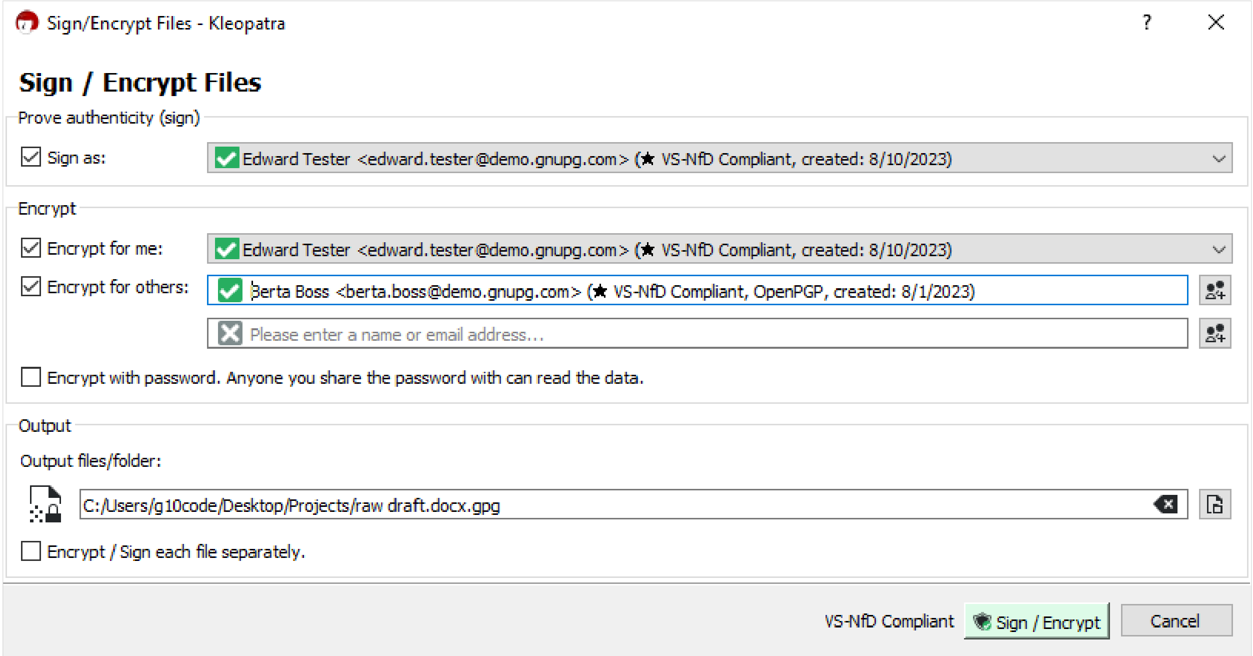
Certificate Selection - Kleopatra

Please select one or more of the following certificates:

Search... All Certificates

Name	E-Mail	User-IDs	Valid From	Valid Until	Key-ID
Berta Boss	berta.boss@demo.gnupg.com	★ VS-NfD Compliant	8/1/2023	8/1/2025	16D4 166E E2FC 4157
Edward Tester	**edward.tester@demo.gnupg.com**	**★ VS-NfD Compliant**	**8/10/2023**	**8/10/2025**	**D39A 0BC8 3207 5C...**

After entering the recipients, select the directory for your encrypted files and click on Sign / Encrypt :



Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: ✓ Edward Tester <edward.tester@demo.gnupg.com> (★ VS-NfD Compliant, created: 8/10/2023)

Encrypt

☑ Encrypt for me: ✓ Edward Tester <edward.tester@demo.gnupg.com> (★ VS-NfD Compliant, created: 8/10/2023)

☑ Encrypt for others: ✓ Berta Boss <berta.boss@demo.gnupg.com> (★ VS-NfD Compliant, OpenPGP, created: 8/1/2023)

☒ Please enter a name or email address...

□ Encrypt with password. Anyone you share the password with can read the data.

Output

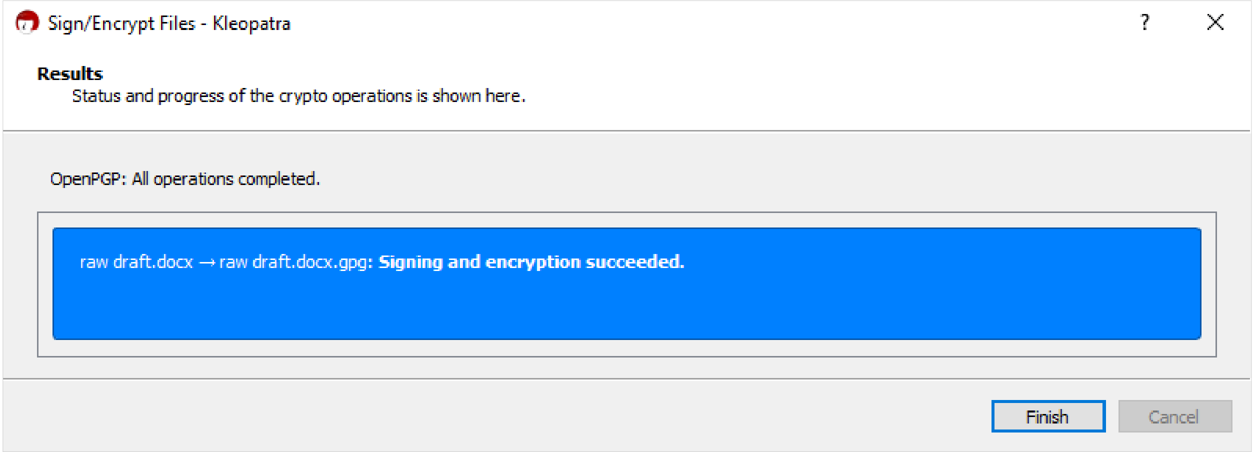
Output files/folder:

C:/Users/g10code/Desktop/Projects/raw draft.docx.gpg

□ Encrypt / Sign each file separately.

VS-NfD Compliant

Kleopatra will show you if the file encryption was successful. Click on Finish to close:



Sign/Encrypt Files - Kleopatra

Results

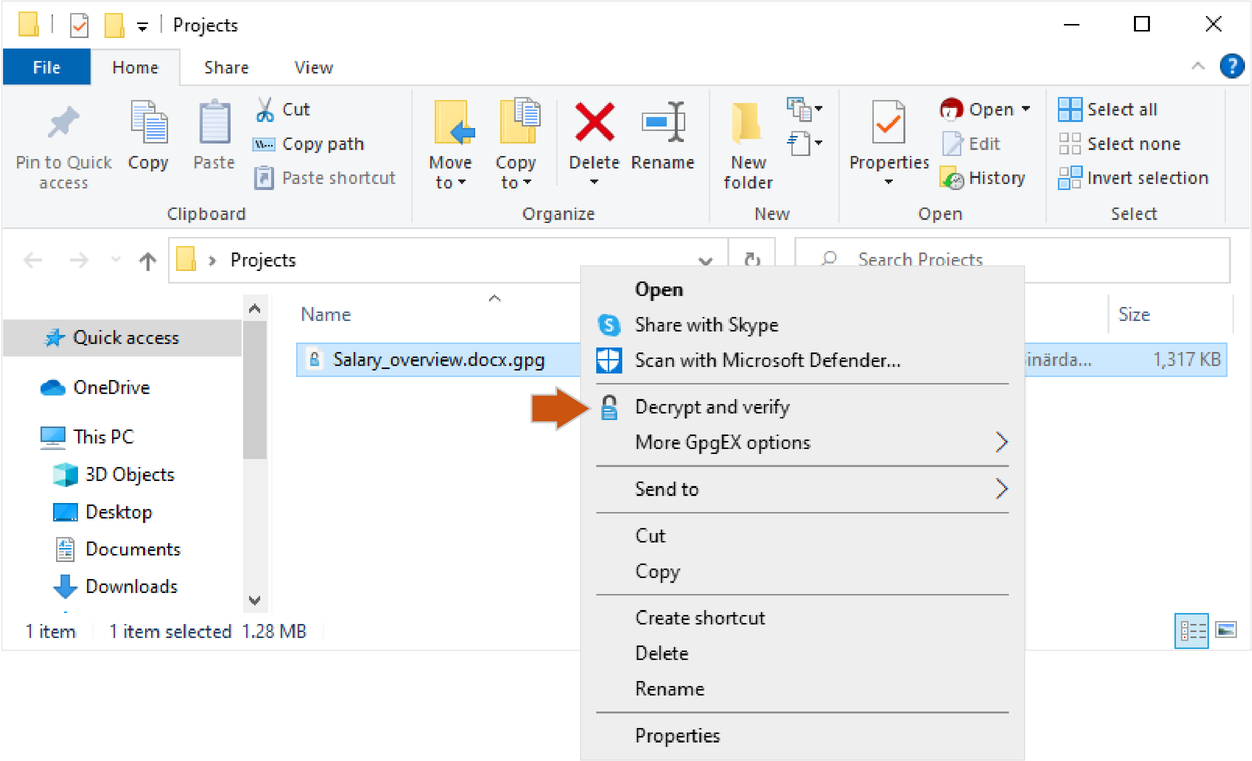
Status and progress of the crypto operations is shown here.

OpenPGP: All operations completed.

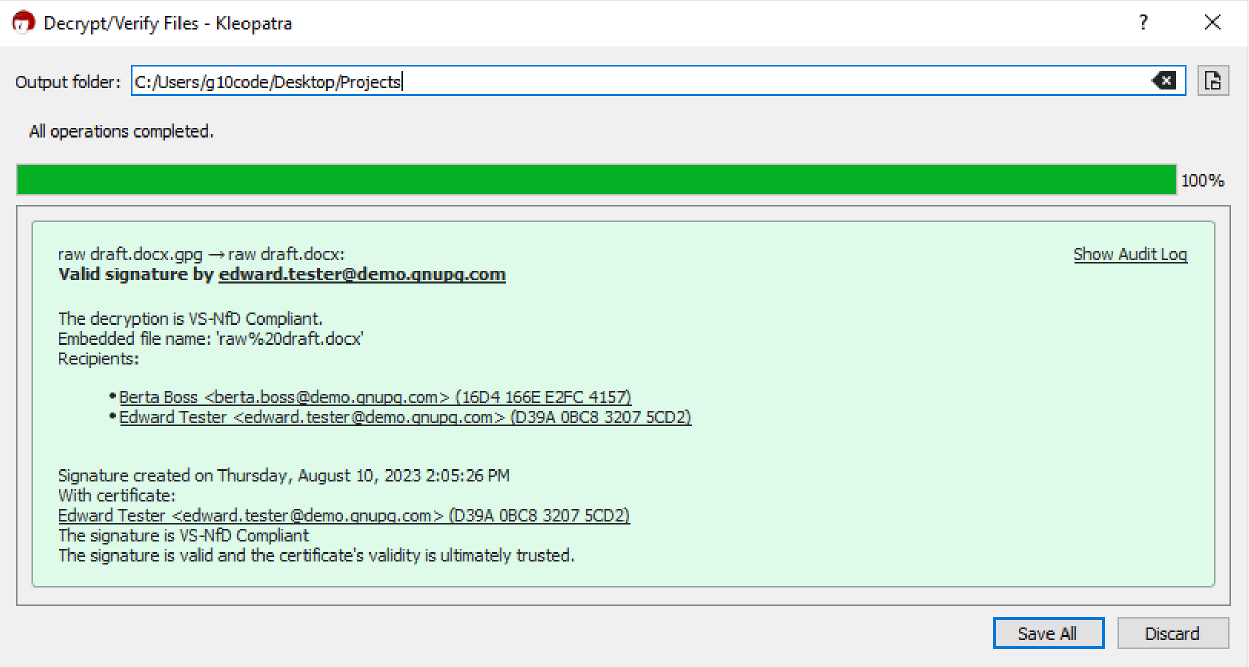
raw draft.docx → raw draft.docx.gpg: **Signing and encryption succeeded.**

6 Decrypt files

Select one or more encrypted files or folders. Open the Explorer menu with the right mouse button and select Decrypt and verify . Alternatively, double-click the file to decrypt:



Kleopatra will show you whether the file decryption was successful and additionally the result of the signature check:



Output folder: C:/Users/g10code/Desktop/Projects

All operations completed.

100%

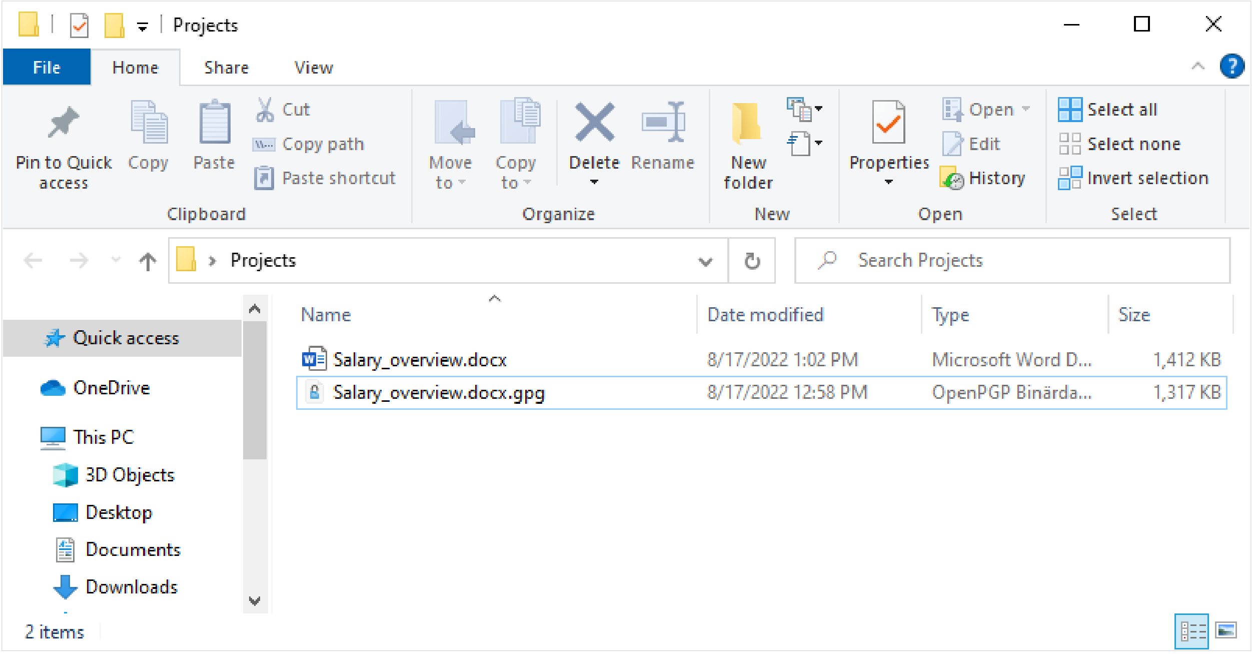
raw draft.docx.gpg → raw draft.docx:
Valid signature by edward.tester@demo.gnupg.com

The decryption is VS-NfD Compliant.
Embedded file name: 'raw%20draft.docx'
Recipients:

- Berta Boss <berta.boss@demo.gnupg.com> (16D4 166E E2FC 4157)
- Edward Tester <edward.tester@demo.gnupg.com> (D39A 0BC8 3207 5CD2)

Signature created on Thursday, August 10, 2023 2:05:26 PM
With certificate:
Edward Tester <edward.tester@demo.gnupg.com> (D39A 0BC8 3207 5CD2)
The signature is VS-NfD Compliant
The signature is valid and the certificate's validity is ultimately trusted.

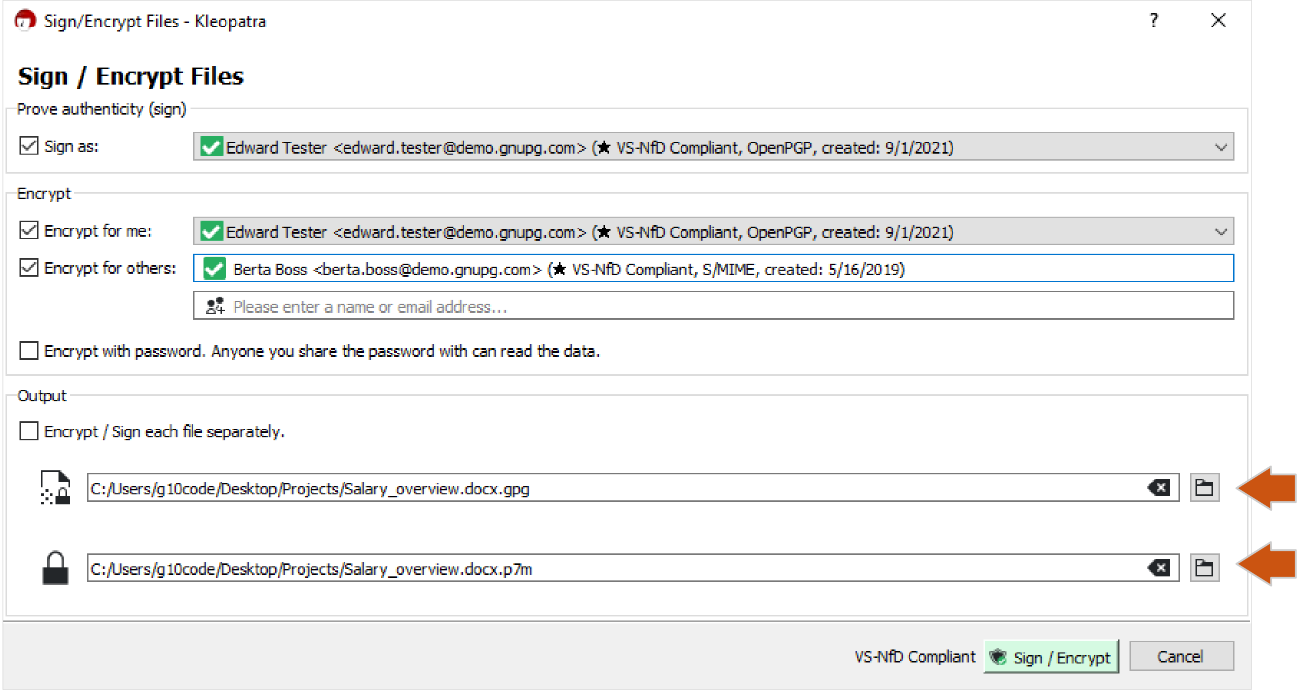
In this window you can also change the location where the decrypted file will be stored. The default is the folder where the encrypted file is located. Click on Save All to save the decrypted file to the chosen folder:



Name	Date modified	Type	Size
Salary_overview.docx	8/17/2022 1:02 PM	Microsoft Word D...	1,412 KB
Salary_overview.docx.gpg	8/17/2022 12:58 PM	OpenPGP Binärda...	1,317 KB

7 Combination OpenPGP and S/MIME

It may happen that your communication partners provide you with S/MIME certificates only. This is not a problem as you do not need a S/MIME certificate yourself to encrypt to S/MIME recipients. In this case you will get two file formats as output:


Sign/Encrypt Files - Kleopatra

Sign / Encrypt Files

Prove authenticity (sign)

☑ Sign as: Edward Tester <edward.tester@demo.gnupg.com> (★ VS-NfD Compliant, OpenPGP, created: 9/1/2021)

Encrypt

☑ Encrypt for me: Edward Tester <edward.tester@demo.gnupg.com> (★ VS-NfD Compliant, OpenPGP, created: 9/1/2021)

☑ Encrypt for others: Berta Boss <berta.boss@demo.gnupg.com> (★ VS-NfD Compliant, S/MIME, created: 5/16/2019)

Please enter a name or email address...

☐ Encrypt with password. Anyone you share the password with can read the data.

Output

☐ Encrypt / Sign each file separately.

C:/Users/g10code/Desktop/Projects/Salary_overview.docx.gpg

C:/Users/g10code/Desktop/Projects/Salary_overview.docx.p7m

VS-NfD Compliant

The ***.p7m**-file is for the S/MIME recipients, the ***.gpg**-file is for the OpenPGP recipients.

8 Key Extension

As the BSI recommends a maximum validity period of 3 years for OpenPGP keys, a GnuPG VS-Desktop® key expires after this period. It can then no longer be used for encryption and signing if it is not extended. In case there is no indication that the key has been compromised (security incident), it will usually be extended.

To extend your own key, simply select "Change end of validity period" in the context menu. You can then select the desired expiration date.

Ideally, you should extend a certificate a little before the expiry date, but an extension is also possible if it has already expired.

After the extension, the certificate must be redistributed. It can either be uploaded again to the configured LDAP server (via the "Publish to server …" context menu) and/or exported and distributed again to the communication partners in any way you like with the instruction to import it. Otherwise, they will continue to see the "old" expiration date for the certificate and will not be able to use it after this date to encrypt data for you.

9 Additional Information

If you have any further questions, please also consult our website:

https://gnupg.com/kb/faq-usage.html

Appendix