

# Password based encryption with GnuPG VS-Desktop<sup>®</sup>

## Quick guide for users

The guide applies accordingly to GnuPG Desktop<sup>®</sup>

Document version 2.1

## Introduction

This handout is a tutorial for users to get started with password based / symmetric encryption with GnuPG VS-Desktop<sup>®</sup>. 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 asymmetric public key encryption. This is described in our guide "Encrypt and sign with GnuPG VS-Desktop<sup>®</sup>".

## Functional description

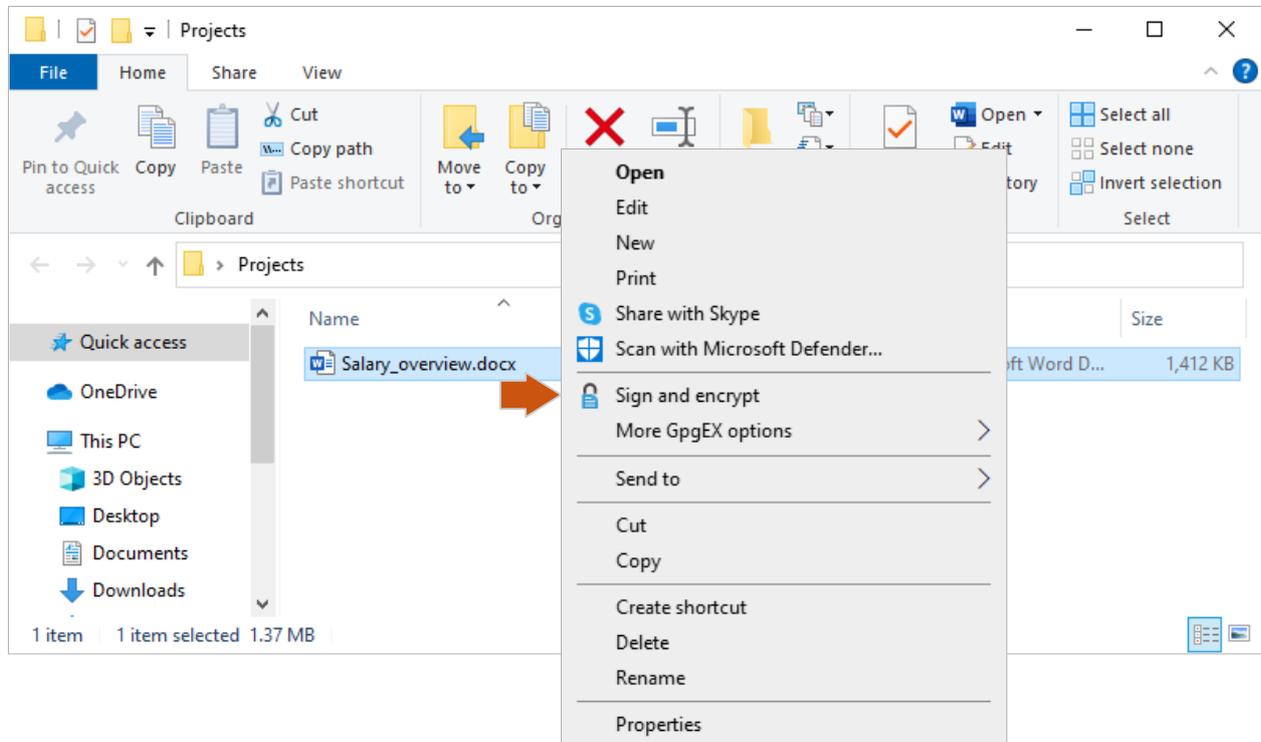
GnuPG VS-Desktop<sup>®</sup> allows you to encrypt and decrypt files and folders easily and quickly by entering a suitable password.



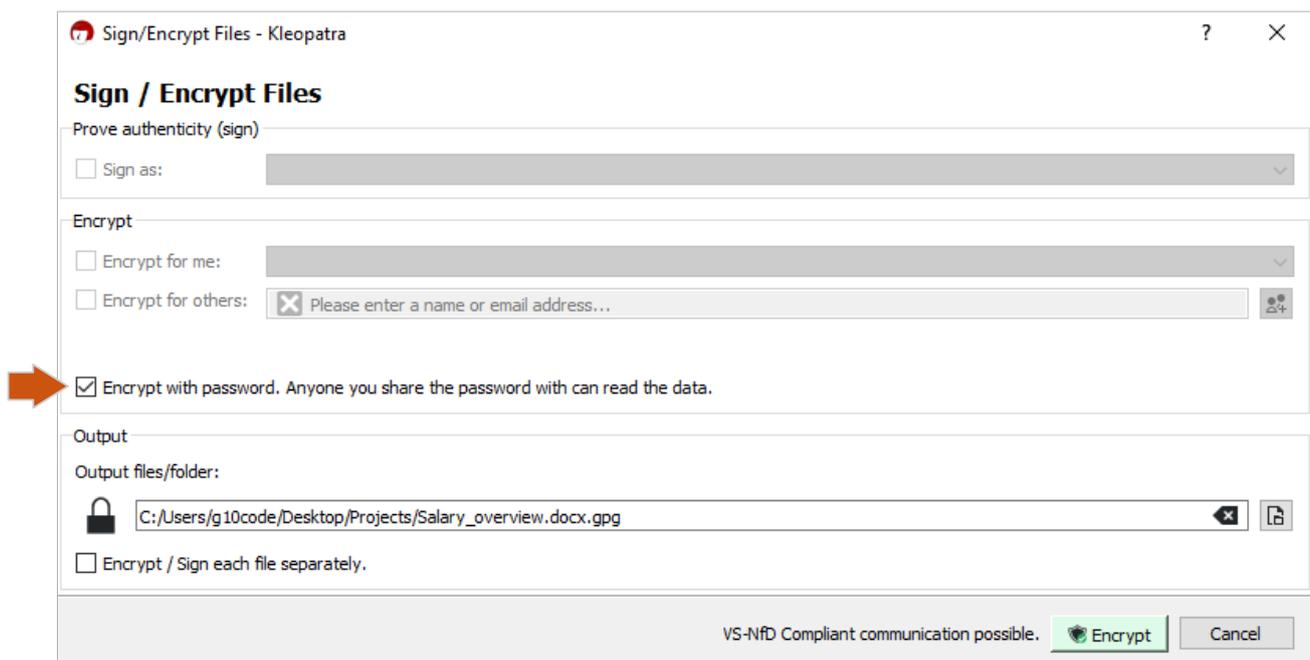
The video tutorial for password based encryption can be found here:  
<https://media.gnupg.org/sc/gnupg-vsd-symmetric-encryption.mp4>

# 1 Encryption

Select one or more files or folders in the Windows Explorer<sup>1</sup> that you want to encrypt. Right-click to open the submenu and select **Sign and encrypt**:



The "Sign / Encrypt data"-dialog opens. If no keys or certificates have been generated or imported into Kleopatra, password-based encryption is the default:



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

If keys already exist, uncheck "Encrypt for me" and "Encrypt for others" and check "Encrypt with password. Anyone you share the password with can read the data".

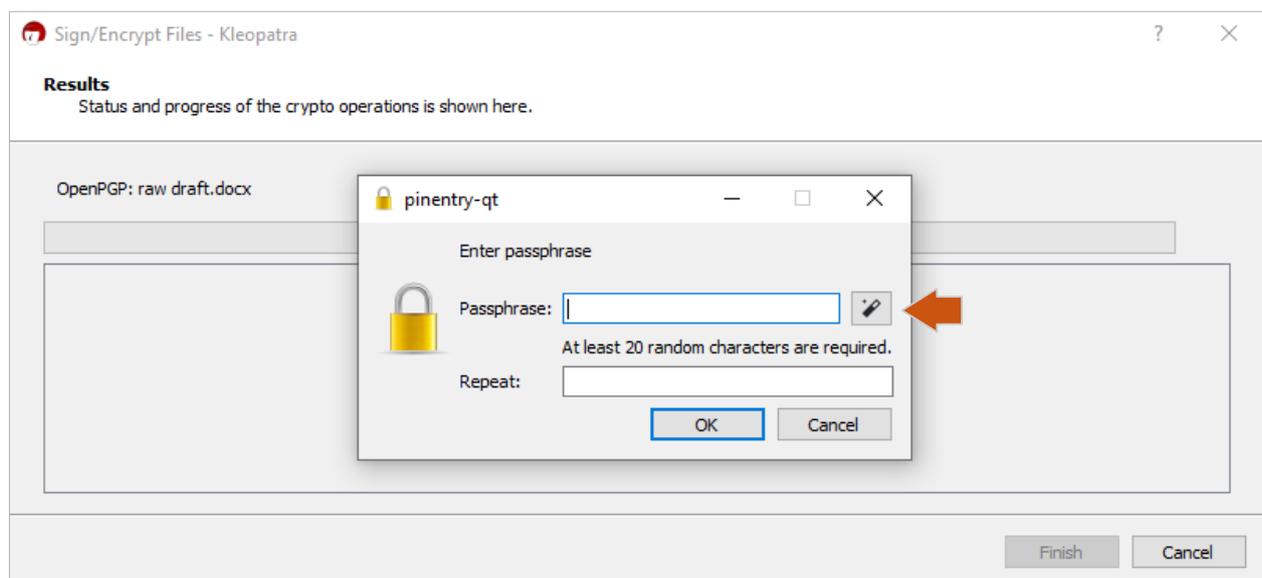
Select the output directory for your encrypted file and click on **Encrypt**. The default is the current folder.

## 1.1 Secure password generation

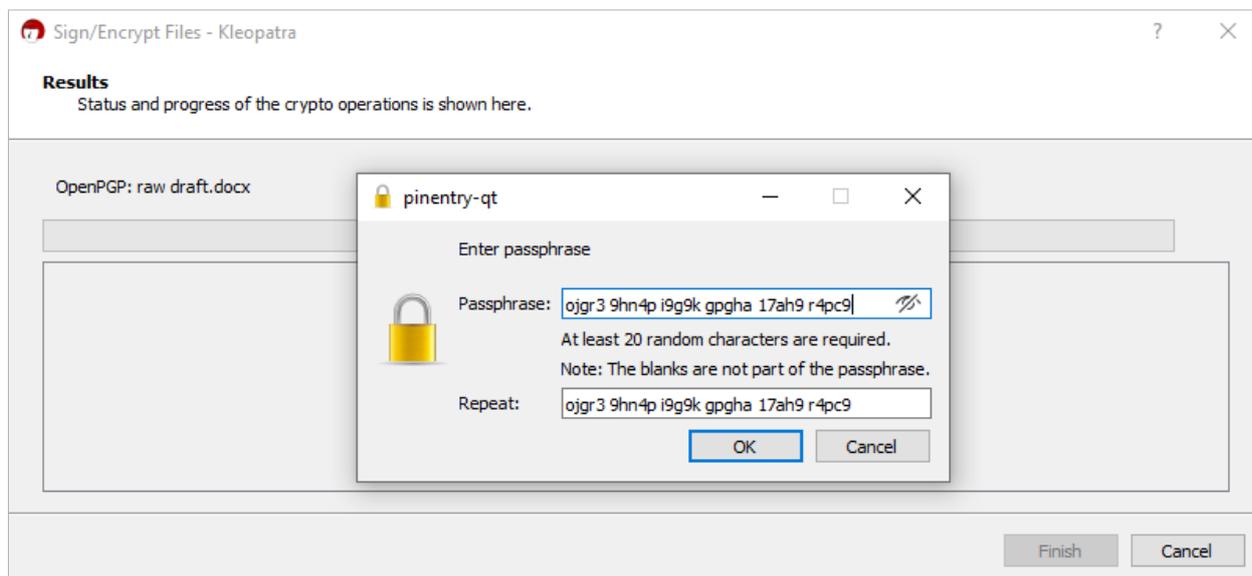
  
**Note**

The mere possession of the password is enough to decrypt the file. Therefore, use our password generator to generate secure passwords.

For symmetric encryption, a password with at least 20 randomly chosen digits is required. We recommend using the **GnuPG password generator** to have a secure password generated automatically. To do this click on the  (suggest) button to the right of the password field:



A 30-digit password consisting of a combination of numbers and letters is entered in both input fields:



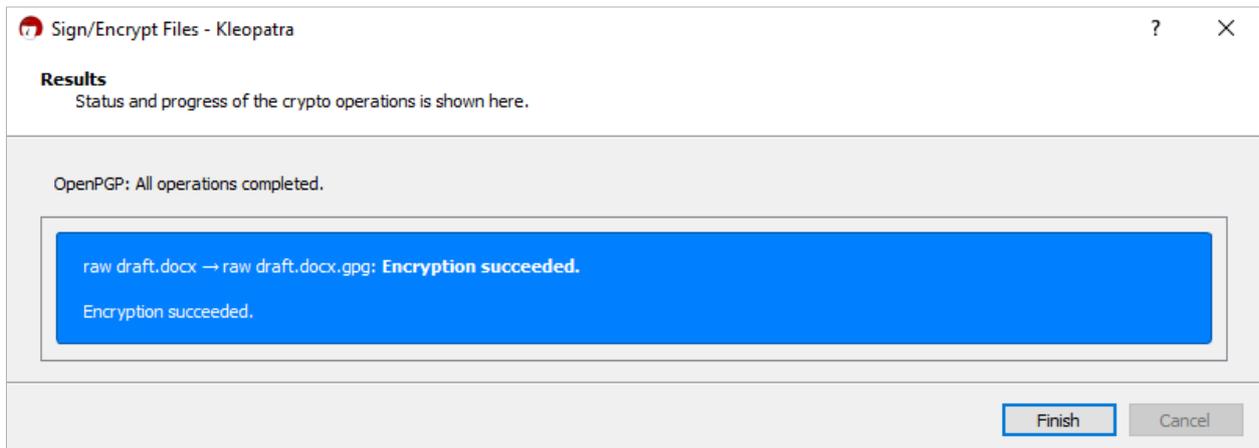
Save the password, for example by copy/paste into a simple text file and saving it in a suitable location protected against unauthorized access.

 **Note** | If you write down the password, please note that the blanks are not part of it. They are only intended to make it easier to read.

As formerly with "Chiasmus", you pass this password over a secure channel to the recipients you want to read your encrypted files.

 **Important** | The password itself is **classified information**. The appropriate protection measures apply here, in particular that it must not be transmitted in cleartext.  
Never transmit a password by unencrypted mail, phone, SMS or fax.

After clicking **OK**, Kleopatra shows you whether the encryption was successful. End the process with **Finish** :

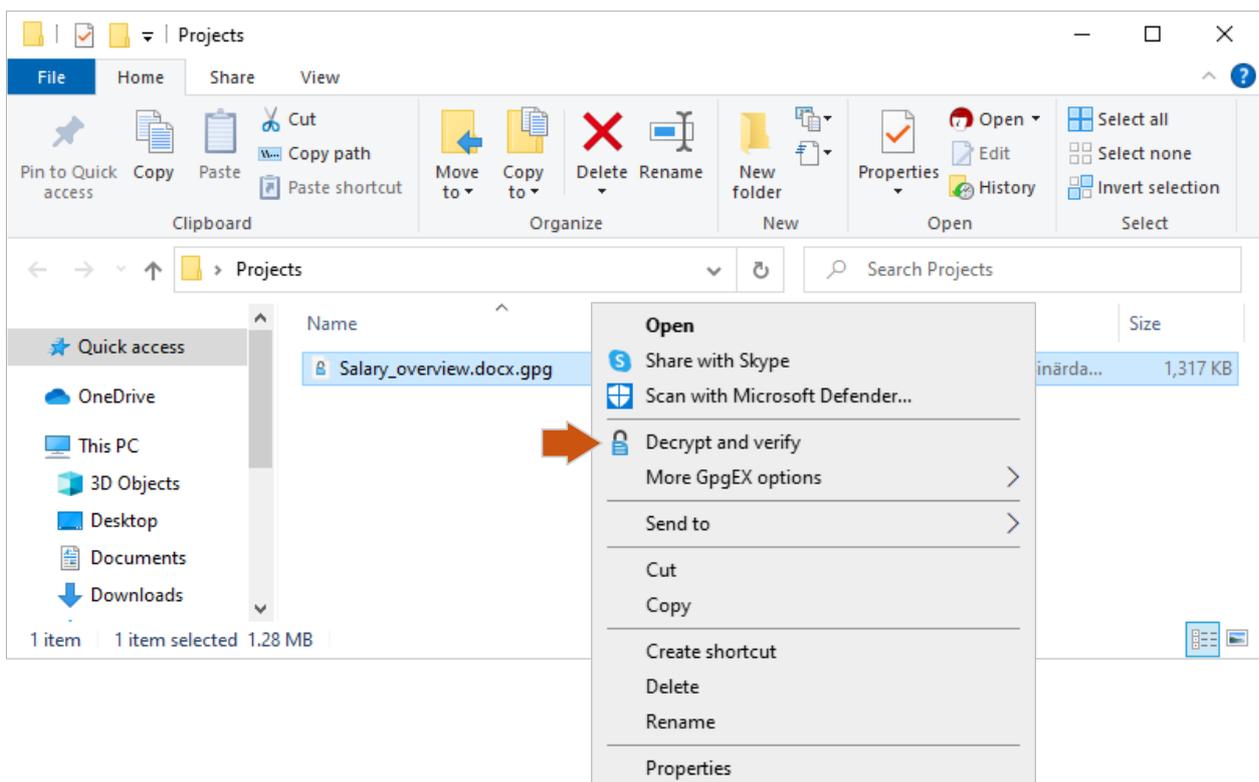


Your file has been encrypted and saved in the chosen folder as a **\*.gpg**-file.

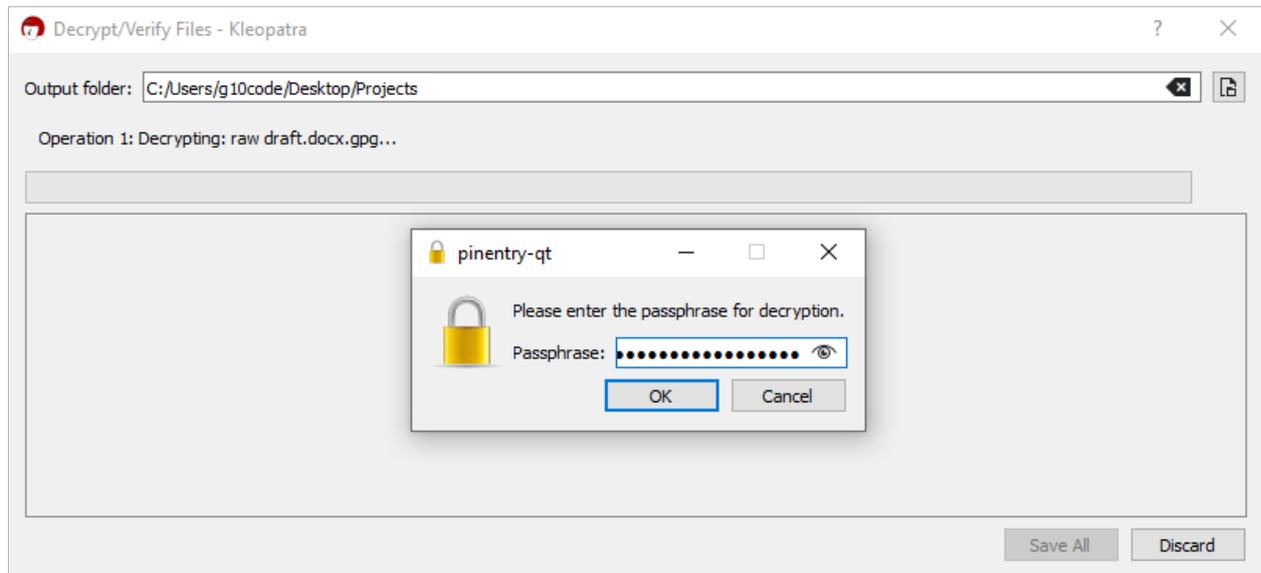
Transfer of such encrypted data can now be done via insecure channels.

## 2 Decryption

Open encrypted **\*.gpg**-files by double-clicking in the Windows file explorer. Alternatively, select the encrypted file, open the submenu with the right mouse button and select **Decrypt and verify** :



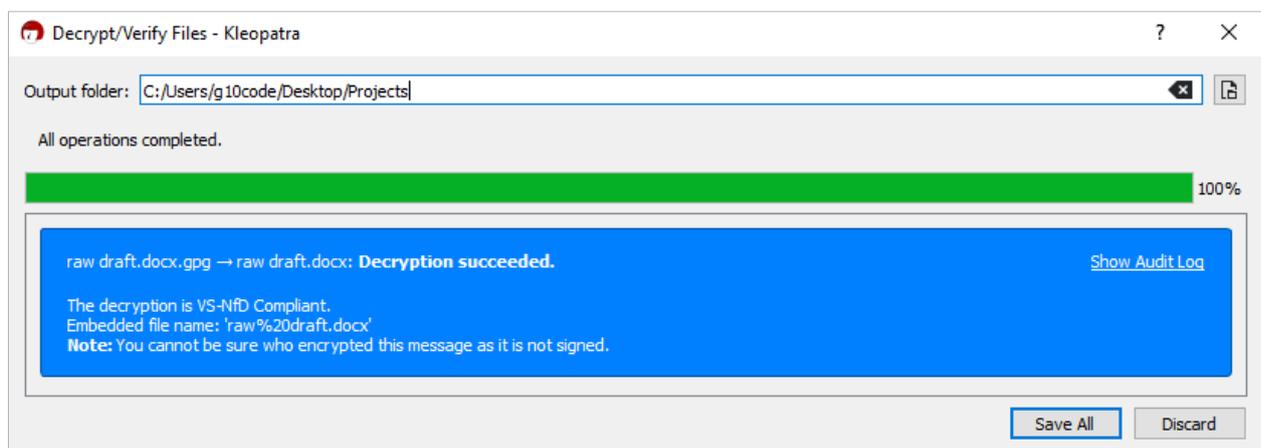
You will be prompted to enter the password that was used for encryption:



Click **OK** after entering the corresponding password.

After the password confirmation, you will be informed whether the decryption was successful. You can ignore the note "You cannot be sure who encrypted this message as it is not signed".

End the process with **Save all** to save the decrypted file in the chosen folder:



## Appendix

This document has been published under the license "Attribution-Share Alike 4.0 International (CC BY-SA 4.0)". The legally binding license agreement can be found at:

<https://creativecommons.org/licenses/by-sa/4.0/deed.en>

GnuPG VS-Desktop® is a registered trademark of g10 Code GmbH.