

Group-feature of GnuPG VS-Desktop®

Quick guide for users

The guide applies accordingly to GnuPG Desktop®

Document version 2.1

Introduction

The group-feature of GnuPG VS-Desktop® allows you to combine several recipients into a project or work group. You can encrypt to all members of a group simultaneously if you select the group as recipient for the encrypted data.

In a nutshell:

- Groups are created and managed in Kleopatra.
- If the group name is a mail address, the group can be used with the Outlook Add-in GpgOL.
- Mixed groups with S/MIME and OpenPGP certificates only work for file encryption.
- When importing or exporting groups, all included certificates resp. public keys are im- or exported including the exportable certifications.

1 Create a group

There are several ways to create a group:

1.1 Via the context menu

In Kleopatra's certificate list, select all the certificates you want to include in a group. Then right-click to open the context menu and select "👤 Create Group...". The "New group" dialog box opens with the previously selected certificates in the lower table, representing the group to be created. See screenshot on the following page. Give the group a suitable name and complete the creation by clicking **Save**.

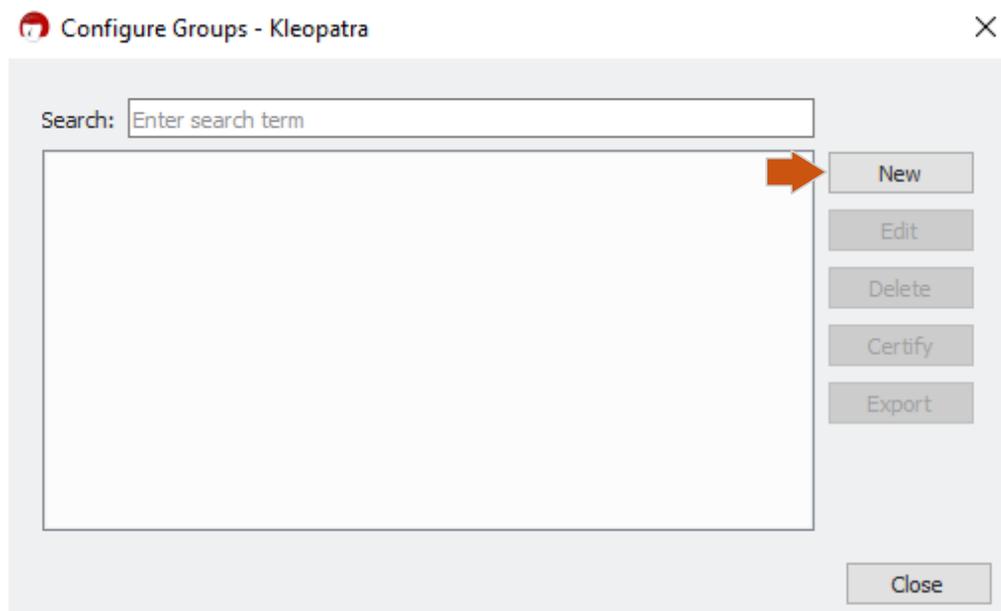

Note

If the group is to be used for encryption in Outlook, the name must be a mail address, e.g. <mailinglist@my-organization.example.com>

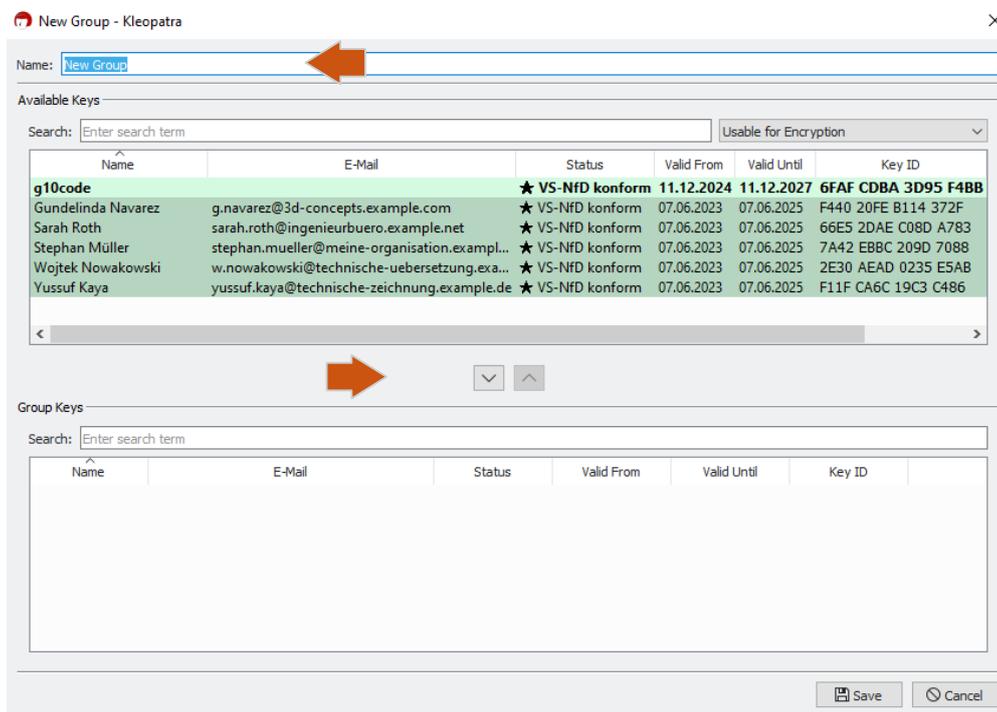
1.2 Via the group settings

Open Kleopatra and select the "Groups" button  on the far right of the toolbar.

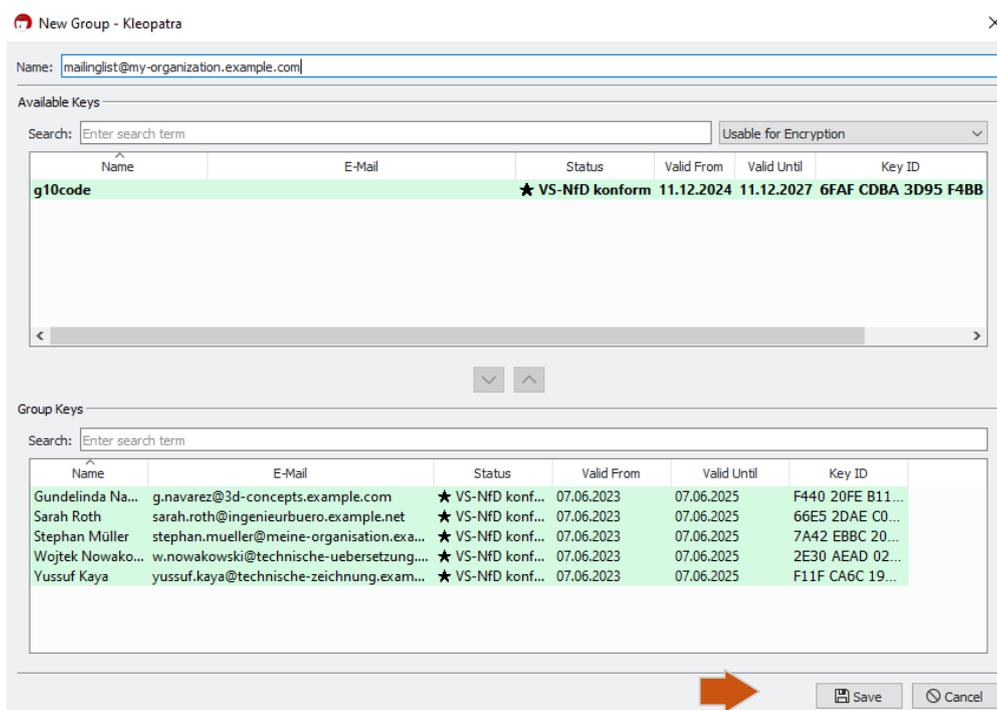
Click on **New** in the window that opens to create a new group:



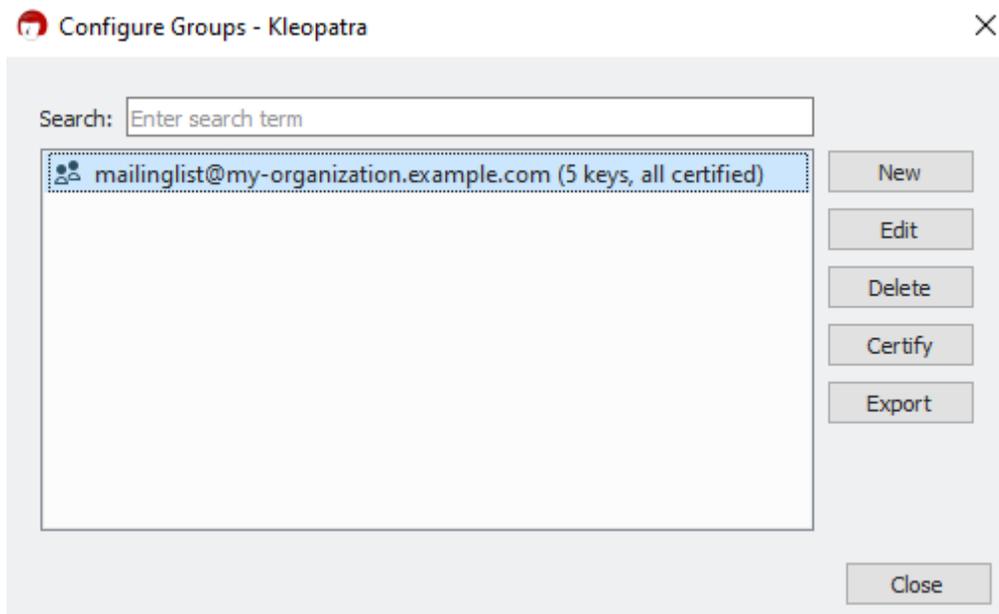
The group participant selection will open. Enter a name and mark the recipients you want to include in your group:



After clicking the button, the chosen recipients will be added to your selection. Confirm afterwards with .



The group was created:



End the process by clicking **Close** or choose another of the available actions.

2 Export a group

Select the group entry in the "Configure Groups"-window and click **Export**.

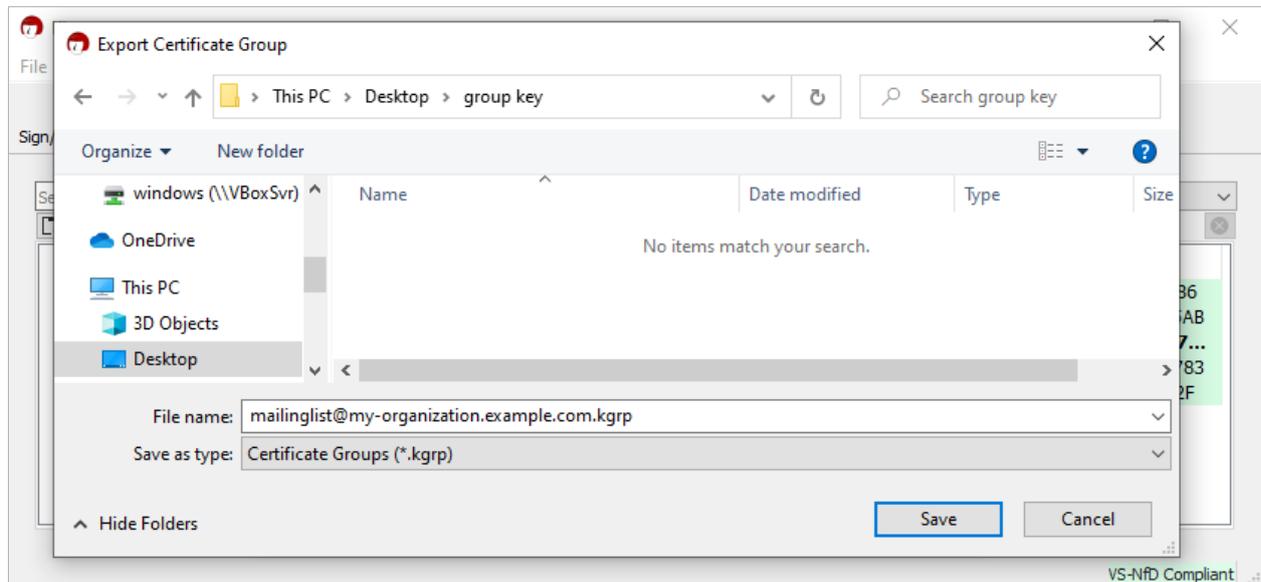
You may now be notified that not all certificates are certified in the exportable way and asked if you still want to export:



If you created the group to share it with others and also want to spare the recipients the additional step of certifying each certificate in the group, you should abort here and first select the "Certify" action; see section 2.1.

Otherwise, click **Export Group**.

Then choose a folder to store the file and click **Save** :



The created file with the group definition has the extension ***.kgrp** (short for "key group").

2.1 Certify

The default setting for certifications in Kleopatra is a local certification, which is not exportable.

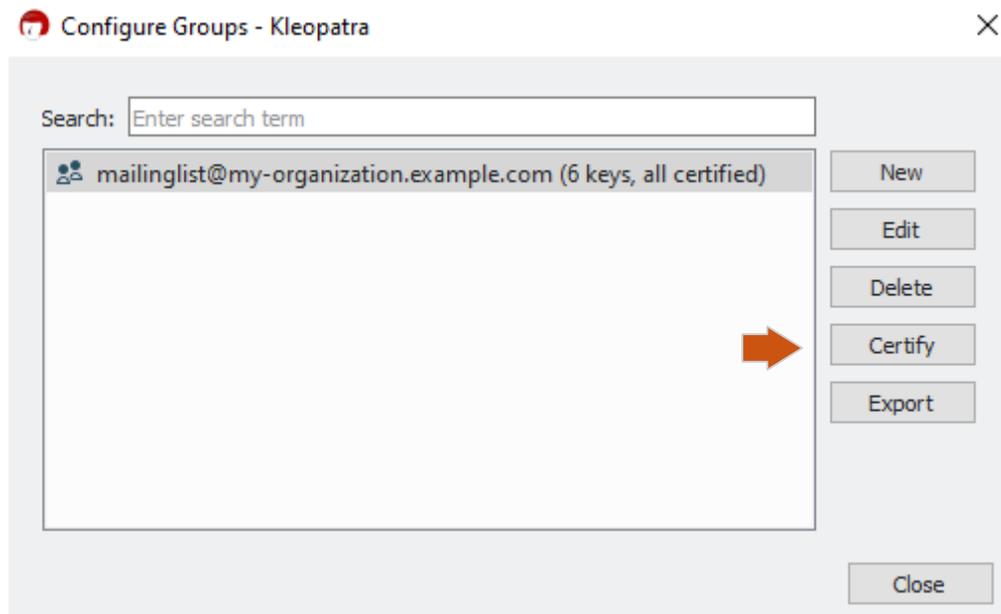
If you want to share the .kgrp file and don't want the recipients to have to check and certify all the certificates in it themselves, it is necessary that all the certificates in the group are certified in an exportable way with the same key before you export the group.

If a trusted key is configured in your GnuPG VS-Desktop®, this should be used for the exportable certification.

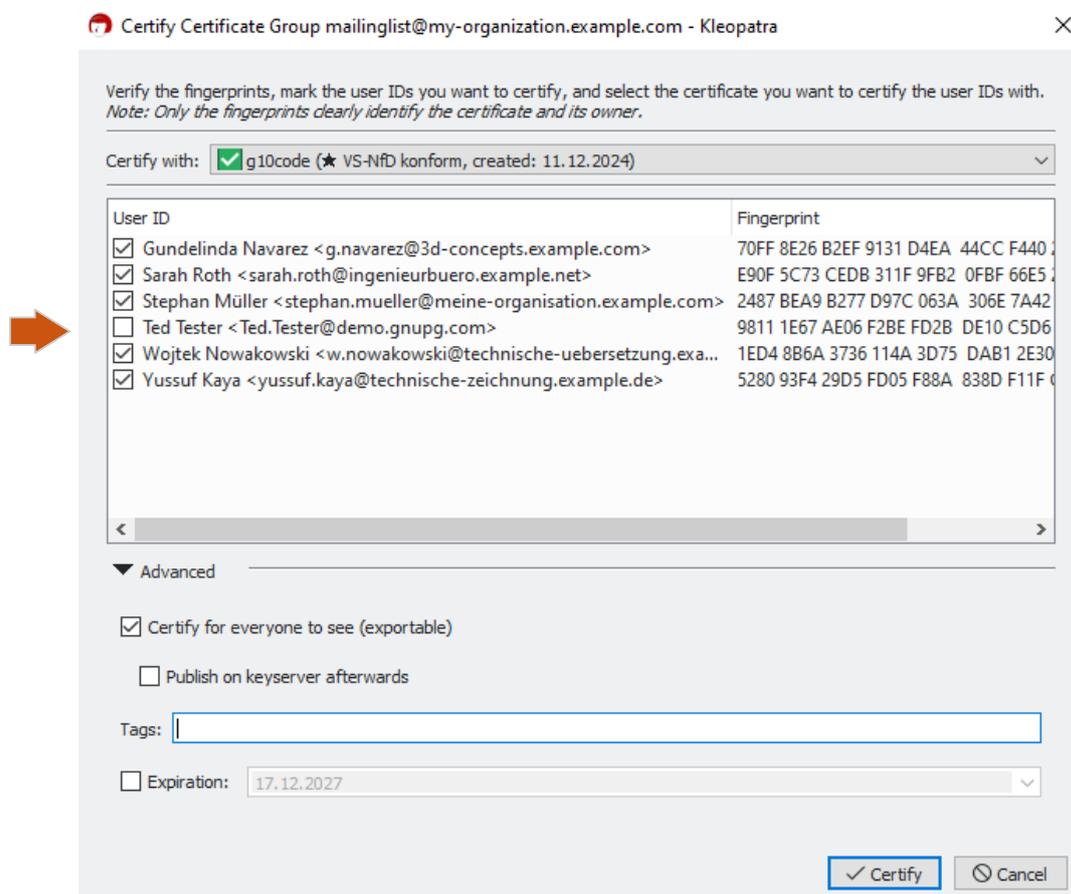
It also works with any other key though. In that case, only the certifying key, i.e. the one of the group creator, has to be certified by the recipients of the group definition after verifying its fingerprint.

Additionally, "certification power" is then granted to him by right-clicking on their certificate → **Change certification powers**. This means that all certificates that have been certified with that key are automatically trusted and, if applicable, displayed as "VS-NfD compliant".

To certify with your key, first select the desired group in the "Configure Groups" dialog and then select **Certify** :



Certificates that have not yet been certified as exportable do not initially have a check mark in the certification list:



Verify the fingerprints of the keys you want to certify and set the appropriate certification check marks.

You can also add a keyword or tag to the certification. This will then be added to the certificates of all chosen group participants. You can use such tags in the certificate list for filtering:

Überprüfen Sie die Fingerabdrücke, markieren Sie die Benutzerkennungen, die Sie beglaubigen möchten, und wählen Sie den Schlüssel, mit dem Sie sie zertifizieren möchten.
Hinweis: Nur die Fingerabdrücke identifizieren Zertifikate und ihre Besitzer eindeutig.

Beglaubigen mit: g10code (★ VS-NfD konform, erstellt: 11.12.2024)

Benutzerkennung	Fingerabdruck
<input checked="" type="checkbox"/> Gundelinda Navarez <g.navarez@3d-concepts.example.com>	70FF 8E26 B2EF 9131 D4EA 44CC F440
<input checked="" type="checkbox"/> Sarah Roth <sarah.roth@ingenieurbuero.example.net>	E90F 5C73 CEDB 311F 9FB2 0FBF 66E5
<input checked="" type="checkbox"/> Stephan Müller <stephan.mueller@meine-organisation.example.com>	2487 BEA9 B277 D97C 063A 306E 7A42
<input checked="" type="checkbox"/> Ted Tester <Ted.Tester@demo.gnupg.com>	9811 1E67 AE06 F2BE FD2B DE10 C5D6
<input checked="" type="checkbox"/> Wojtek Nowakowski <w.nowakowski@technische-uebersetzung.exa...>	1ED4 8B6A 3736 114A 3D75 DAB1 2E30
<input checked="" type="checkbox"/> Yussuf Kaya <yussuf.kaya@technische-zeichnung.example.de>	5280 93F4 29D5 FD05 F88A 838D F11F

▼ Fortgeschritten

Für alle sichtbar beglaubigen (Exportierbar)

Auf Schlüsselserver veröffentlichen

Tags:

Ablaufdatum:

Beglaubigen

 **Note**

Each new certification of a certificate overwrites its tags. If you want to keep them, you have to add the tags again each time. Tags can consist of several words.

Complete the process with **Certify** and enter your password if requested. You can now export the group.

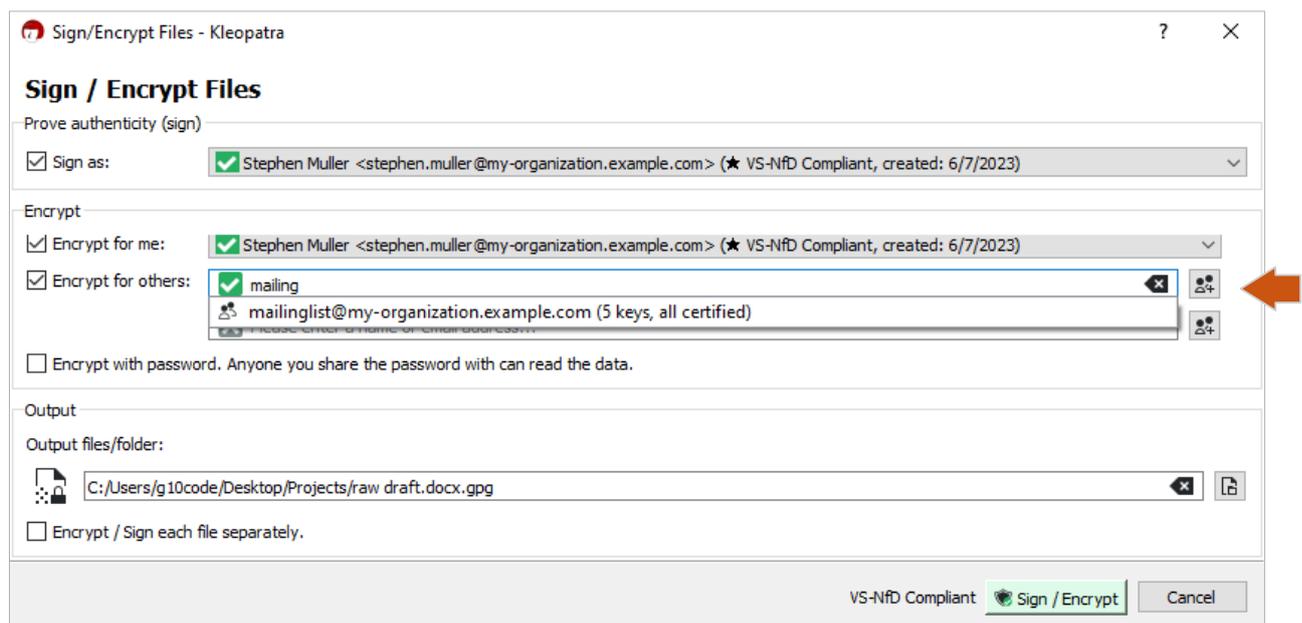
3 Import a group

GnuPG VS-Desktop® group files with the extension ***.kgrp** contain, besides the group name, all certificates resp. public keys of the group and can be imported by double-click, by drag and drop onto the Kleopatra window or by choosing **File** > **Import** in Kleopatra.

4 File Encryption to groups

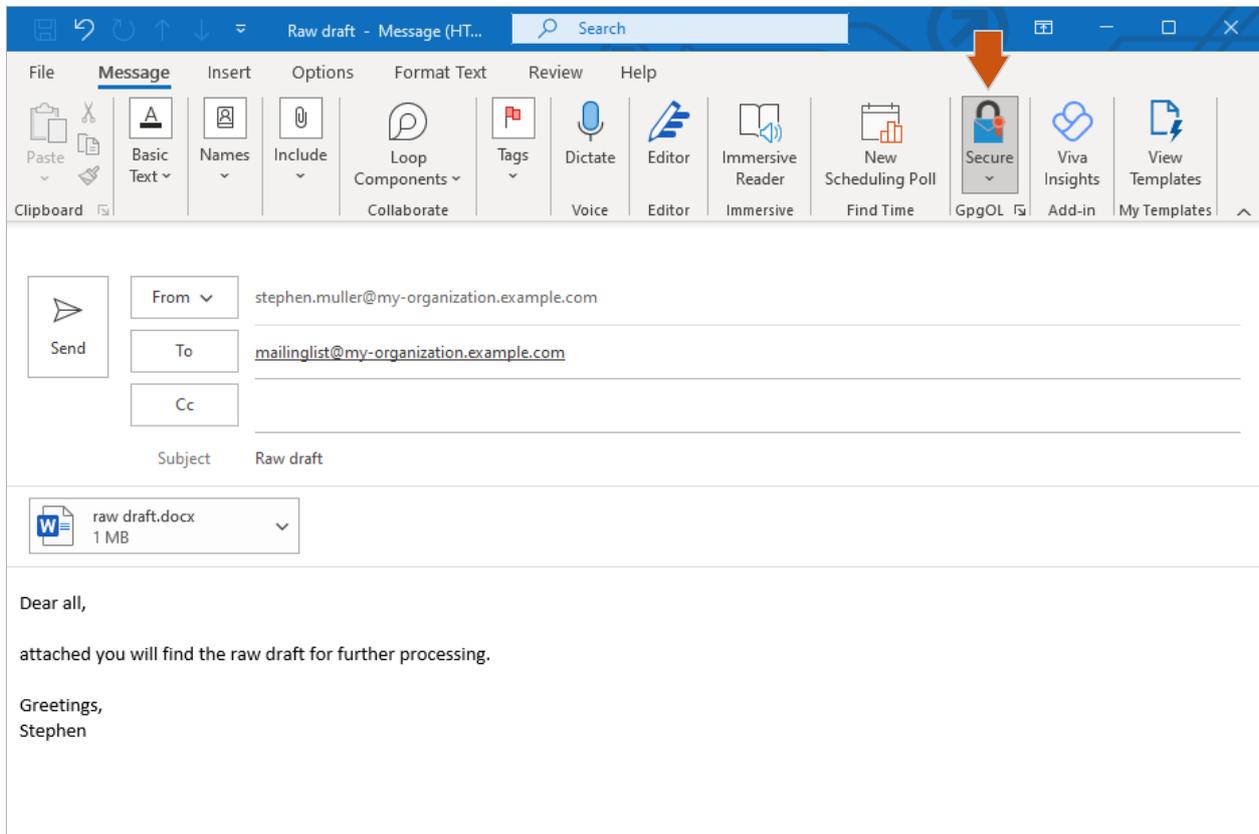
In the "Sign/ Encrypt Files"-dialog, type the name of your group into the text field "Encrypt for others" or alternatively click on the certificate selection to choose the group.

When clicking **Sign / Encrypt** your data will then be encrypted for all group participants:



5 Mail encryption to group

Open an new mail in Outlook and check the  -button if it is not active by default. Write your mail and enter the mail address of the group as recipient:



When you click on **Send**, your mail is automatically encrypted to all recipients in the group.

Note

If you select the option "Always show security confirmation dialog" in the "General" section of the GpgOL configuration, the keys used will be displayed after you click on **Send**. You can then change these if necessary or cancel sending the mail. This can be useful for testing.

For more information on mail encryption please refer to our guide "GnuPG VS-Desktop® Outlook Add-In".

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.