

# PGP/GnuPG Key Signing Party

---

*Practical Guidance to Joining the Web of Trust*

*Version 1.0*

## Document Revision History

Date	Version	Description
July 2024	1.0	Initial Release

This guidance document has been developed to provide a quick reference for PGP/GnuPG Key Signing Parties. The content is based on public information and not solely the view of ETDA. It is a guideline and may be updated from time to time.

Third party sources are quoted as appropriate. ETDA is not responsible for the content of the external sources, including external websites, nor their continued availability, referenced in this introduction.

Where specific vendors or product names are given, those do not mean endorsement from ETDA, but serve as examples only.

This document is intended for educational and information purposes only. Neither ETDA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this document. All information contained herein is provided on an “As Is” basis with no warranty whatsoever. ETDA does not promise any specific result, effects, or outcome from the use of the information herein.



This guidance document is published under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License<sup>1</sup>.

Copyright © Electronic Transactions Development Agency, 2024  
Written by Martijn van der Heide

---

<sup>1</sup> Creative Commons License: <<https://creativecommons.org/licenses/by-nc-sa/4.0/>>

## Table of Contents

PREFACE.....	2
INTENDED AUDIENCE.....	2
ACKNOWLEDGEMENTS.....	3
ACRONYMS.....	3
1 PHASE 1: CREATING A PGP/GNUPG KEY.....	4
1.1 PRIVACY NOTES.....	4
1.2 CREATING A KEY PAIR WITH KLEOPATRA.....	5
1.2.1 <i>Publishing your key on a Key Server</i> .....	6
1.2.2 <i>Exporting your key to a file</i> .....	7
1.3 CREATING A KEY PAIR WITH THUNDERBIRD.....	8
1.3.1 <i>Publishing your key on a Key Server</i> .....	9
1.3.2 <i>Exporting your key to a file</i> .....	9
1.4 KEY SERVER NOTES.....	10
1.5 KEY DISTRIBUTION AND EXPIRY.....	10
2 PHASE 2: THE PGP/GNUPG KEY SIGNING PARTY.....	11
2.1 ORGANIZER(S) PREPARATION.....	11
2.2 CONDUCTING THE PARTY.....	12
2.2.1 <i>Viewing your key fingerprint in Kleopatra</i> .....	12
2.2.2 <i>Viewing your key fingerprint in Thunderbird</i> .....	12
3 PHASE 3: SIGNING THE VERIFIED KEYS.....	14
3.1 KEY SIGNING WITH KLEOPATRA.....	14
3.2 KEY SIGNING WITH THUNDERBIRD.....	17
4 CONSOLIDATING ALL NEW SIGNATURES TO YOUR KEY.....	19

## Preface

Communications, in terms of both the messages themselves and their transport, are increasingly conducted in electronic form and use the Internet for easy, fast, cheap, and global delivery. Such electronic interactions these days include much more than just e-mails and bulletin board postings: indeed, every aspect of our day-to-day lives have moved online, either to complement our regular offline activities (such as talking to our family and friends), or in its entirety (working from home, online gaming or ordering from shops).

All electronic communications require a certain amount of security and trust. While we have, thankfully, mostly left the era behind where infrastructure shortcomings caused significant problems to get data across without requiring several retries (do you remember modems?), there are still several things that need our attention. Who can see your messages in transit? How can you make sure that the message was not altered before (or even after) arriving? How can you prove that it was you who sent the message?

Cryptography is the science of writing or reading coded messages; it is the basic building block that enables the mechanism of authentication (which establishes the identity of the sender or receiver of information, or both), integrity (which ensures that the data has not been altered in transit for at rest) and confidentiality (which ensures that only authorized entities can view the data). While digital certificates are used to attest the validity of a public key that's part of asymmetric encryption and a common format is the X.509 standard, in the CSIRT community we use a different but similar standard called PGP or GnuPG.

This document provides practical guidance to the three phases involved in PGP/GnuPG Key Signing Parties. Key signing parties are social events, typically held during security conferences or seminars. Their purpose is a mass key signing opportunity to increase the Web of Trust.

Those who are unfamiliar with PGP/GnuPG or the Web of Trust are invited to read our guide "An Introduction to PGP/GnuPG<sup>2</sup>" first. This introduction is also referenced at relevant locations in this document.

## Intended audience

This guidance is designed for anyone who wishes to join a PGP/GnuPG Key Signing Party, either for official purposes or as a required part of a training program such as TRANSITS I.

The intended audience is CSIRT teams, but the introduction can also be used as a reference guide for any other type of organization, or individuals.

---

<sup>2</sup> An Introduction to PGP/GnuPG: <[https://www.first.org/pgp/An\\_Introduction\\_to\\_PGP-GnuPG\\_v1.0.pdf](https://www.first.org/pgp/An_Introduction_to_PGP-GnuPG_v1.0.pdf)>

## Acknowledgements

Special thanks go to all individuals in the international information security community who kindly peer reviewed this document.

## Acronyms

This introduction uses the following acronyms:

Acronym	Term
CSIRT	Computer Security Incident Response Team
GnuPG	GNU Privacy Guard, also abbreviated as GPG
MISP	Malware Information Sharing Platform
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure

Table 1: List of acronyms

# 1 Phase 1: Creating a PGP/GnuPG key

The first phase (your homework) involves creating a suitable PGP/GnuPG key pair that will be submitted to the Key Signing Party. We will create a key pair using the RSA algorithm and a key length of 3072 bits.

More information about Key Life Cycle Management is available in chapter 3 of [An Introduction to PGP/GnuPG](#).

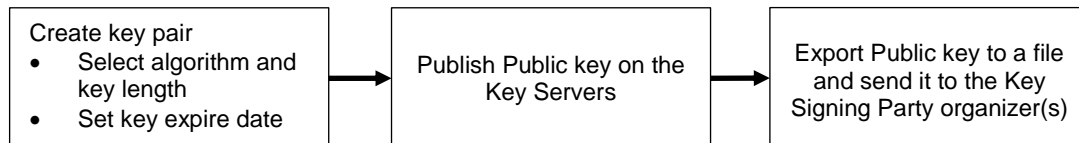


Figure 1: Steps covered in this chapter

There are many PGP/GnuPG tools that can be used, for almost all platforms. An overview of those can be found in Appendix A of the introduction to PGP/GnuPG document. This guide looks at Kleopatra (part of the Gpg4win suite<sup>3</sup>) and Thunderbird<sup>4</sup>, two commonly used alternatives. Note that the user interface may look different on your system compared to the shown screenshots in this document, depending on the software version or the platform you run it on.

The created keys can be copied (exported/imported) to and used in all other applications as well, so choose your favorite one.

If you already have a suitable key pair, please export the Public key to a file and send it to the organizer(s). You can refer to chapter 1.2.2 for Kleopatra or chapter 1.3.2 for Thunderbird to see how exporting is performed.

## 1.1 Privacy notes

PGP/GnuPG Public keys are generally uploaded to the public Key Servers to be found by anyone who wishes to communicate securely with you – *never share your Private (secret) key*. This exposes your e-mail address. If you are only interested, or required, to participate in a Key Signing Party but do not want your e-mail address exposed to the entire world, there are 2 options you can consider:

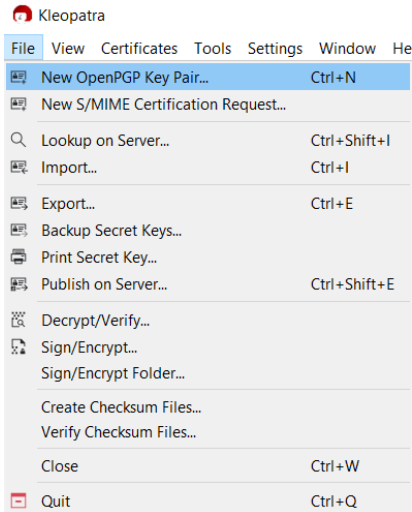
- 1) If you do want your key to be signed by your peers but not uploaded to the Key Servers for public consumption, make sure to inform the organizer(s) of the event in phase 2.
- 2) If you do not intend to use PGP/GnuPG at all, you can register an e-mail address at one of the free webmail providers and still participate in the event. Again, make sure to inform the organizer(s) of the event in phase 2.

<sup>3</sup> Gpg4win: <<https://www.gpg4win.org/>>

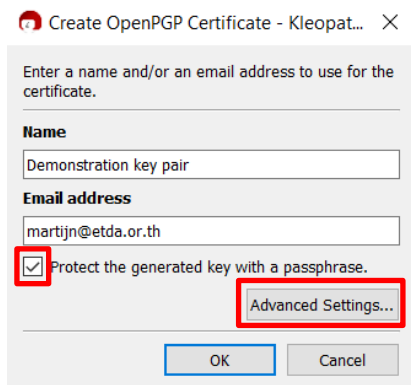
<sup>4</sup> Thunderbird: <<https://www.thunderbird.net/>>

## 1.2 Creating a key pair with Kleopatra

Select menu option “File” → “New OpenPGP Key Pair...”:

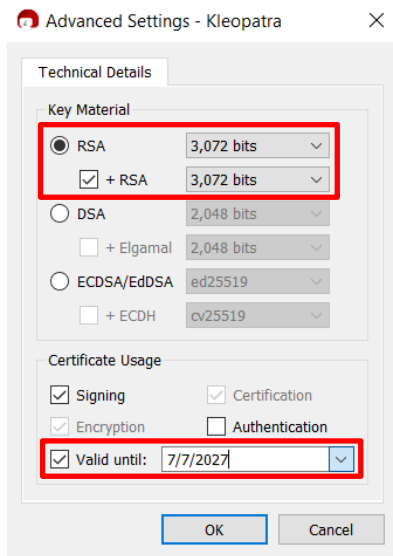


This opens the following window to configure the key name and e-mail address:



Make sure to tick the option to set a passphrase to protect your Private (secret) key, as the default in Kleopatra for some reason is to *not* have one. The passphrase can be changed at any time later.

Select “Advanced Settings...” to configure the key length, validity period, and what the key pair will be used for. The “Valid until” (expiry) date can be extended at any time later.

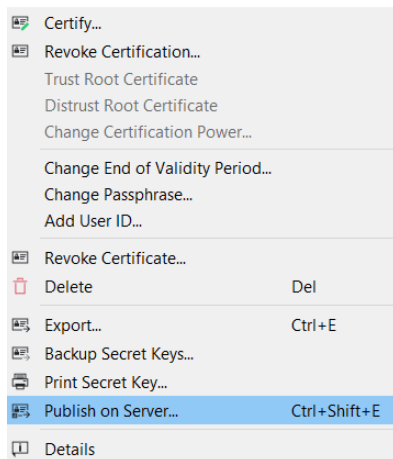


The key pair will now be generated.

### 1.2.1 Publishing your key on a Key Server

After generation of the key pair, it will appear in the list of certificates. Unless you do not want your key to be publicly available (chapter 1.1), it should be uploaded to the Key Servers.

Right-click on it and select option “Publish on Server...”

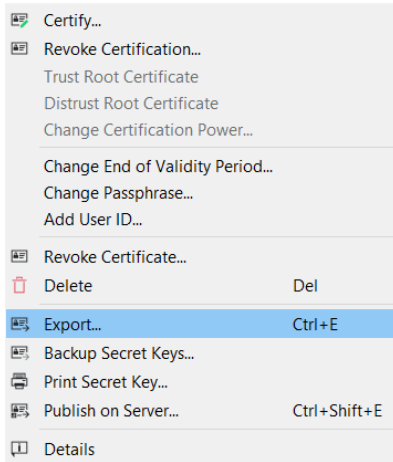


This may take some time to execute. If you receive a time-out or other error message, please refer to chapter 1.4 to perform this step manually.



## 1.2.2 Exporting your key to a file

To export your Public key to a file, right-click on it in the list of certificates and select option “Export”:



This option will export your newly generated Public key to a file with a filename such as “Demonstration key pair\_0x14669552\_public.asc”.

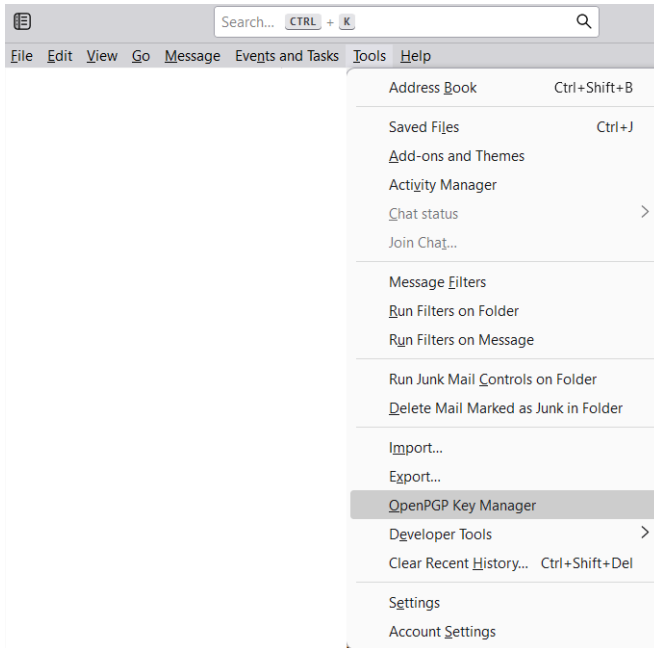
Note that the filename has the word “public” in it, to indicate that only your Public key is in it, *never share your Private (secret) key!*

This file can be sent to the Key Signing Party organizer(s).

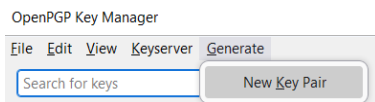
### 1.3 Creating a key pair with Thunderbird

First click on the “Alt” key to bring up the menu strip at the top of the window.

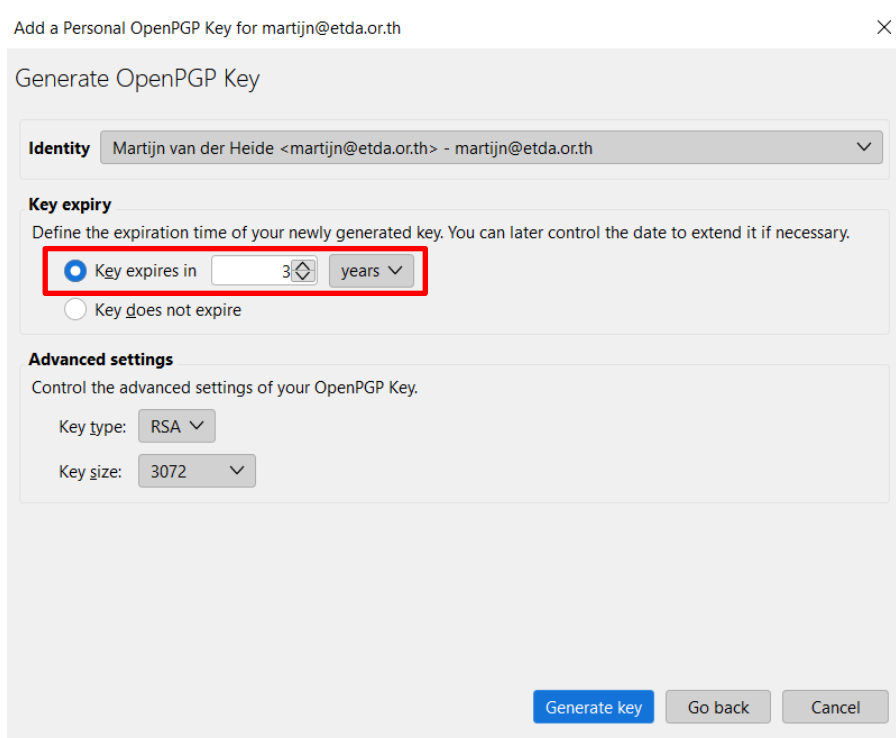
Then select menu option “Tools” → “OpenPGP Key Manager”.



In the OpenPGP Key Manager window select menu option “Generate” → “New Key Pair”:



Notice that you can only create key pairs for identities (e-mail accounts) that you already configured in Thunderbird.



Add a Personal OpenPGP Key for martijn@etda.or.th

Generate OpenPGP Key

**Identity** Martijn van der Heide <martijn@etda.or.th> - martijn@etda.or.th

**Key expiry**  
Define the expiration time of your newly generated key. You can later control the date to extend it if necessary.

Key expires in 3 years

Key does not expire

**Advanced settings**  
Control the advanced settings of your OpenPGP Key.

Key type: RSA

Key size: 3072

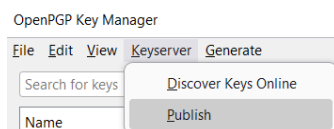
Generate key Go back Cancel

Both the passphrase and expiry date can be changed at any time later.

### 1.3.1 Publishing your key on a Key Server

After generation of the key pair, it will appear in the list of keys. Unless you do not want your key to be publicly available (chapter 1.1), it should be uploaded to the Key Servers.

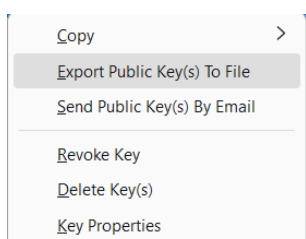
In the OpenPGP Key Manager window select menu option “Keyserver” → “Publish”.



This may take some time to execute. If you receive a time-out or other error message, please refer to chapter 1.4 to perform this step manually.

### 1.3.2 Exporting your key to a file

To export your Public key to a file, right-click on it and select option “Export Public Key(s) To File”:



This option will export your newly generated Public key to a file with a filename such as “Demonstration key pair martijn@etda.or.th-(0xC2CA88EDE14663552)-public.asc”.

Note that the filename has the word “public” in it, to indicate that only your Public key is in it, *never share your Private (secret) key!*

This file can be sent to the Key Signing Party organizer(s).

## 1.4 Key Server notes

PGP/GnuPG Key Servers to be used are preconfigured in the applications. They are interconnected and synchronize the keys between each other. However, they are privately operated systems and may disappear at any time.

If you receive a time-out or another error message, please consider using any of the following. The key to be uploaded must first be exported to a file (see chapter 1.2.2 for Kleopatra or chapter 1.3.2 for Thunderbird). Then open that file in a standard text editor, copy the complete contents and paste them in the Key Server web interface.

- 1) <https://pgp.surfnet.nl/>
- 2) <https://pgp.circl.lu/>
- 3) <https://keys.openpgp.org/>
- 4) <https://keyserver.ubuntu.com/>

To combat the identity fraud problem where miscreants publish fake PGP/GnuPG keys to claim other people’s e-mail addresses, some Key Servers now send e-mails when someone tries to publish a key on them, to verify with the owner of the e-mail address that the publication was authorized. Do not be alarmed when you receive such e-mails as the owner of a key.

If you do not want your key published on a Key Server (see chapter 1.1), this is an effective way to stop that from happening. Not all Key Servers do this, however, so please make sure to notify the Key Signing Party organizer(s) if you do not want your key to be available online.

## 1.5 Key distribution and expiry

The key expiry date can be updated at any time to extend its lifetime.

However, as keys are self-contained files, key updates are not automatically known outside your PGP/GnuPG application and the key needs to be re-shared afterward.

Re-publishing on the Key Servers is one of the steps, but your key may also be stored in multiple other locations such as membership portals, your own website’s contact page, or as authentication/encryption key in applications such as MISP. You are advised to keep track of all locations where your key is stored, as it needs to be updated at all of them.

## 2 Phase 2: The PGP/GnuPG Key Signing Party

The last step of phase 1 was to export your Public key to a file and send it to the Key Signing Party organizer(s).

To reiterate: if you worry about the privacy of your e-mail address, as explained in chapter 1.1 please make sure to state your intentions with your key to the organizer(s).

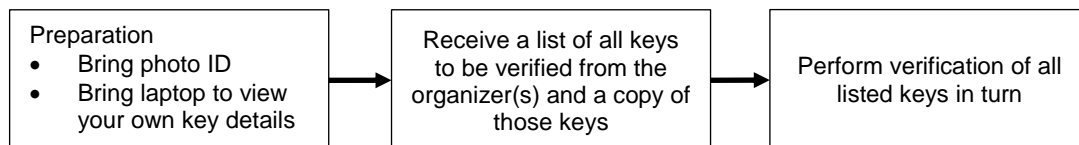


Figure 2: Steps covered in this chapter

All participants are required to bring an official government issued photo ID (passport or drivers' license) to the event.

It is important to understand what “trust” means in PKI. In the real world, the word is typically used to indicate trust in a person or organization; they are known to be trustworthy. However, in the PKI world, trust only means that we can depend on that a presented digital certificate or PGP/GnuPG key has been thoroughly verified to really belong to the identity that is shown in it; it says nothing about trustworthiness of the person or organization themselves, as we may not actually know them at all.

### 2.1 Organizer(s) preparation

The organizer(s) collect the Public keys of all participants in the Key Signing Party (including their own).

All keys are imported into their PGP/GnuPG management tool to obtain the relevant details: key name, e-mail address(es), and fingerprint.

Those details are printed on a sheet of paper, 1 set of details per key, a line under it, next set of details, a line under it, and so on. If a participant indicated that their e-mail address may not be exposed to the public, clearly mark this in their details.

Each participant will be handed a copy of this sheet of paper at the start of the event. Make sure to securely destroy any remaining unused copies as this is sensitive information.

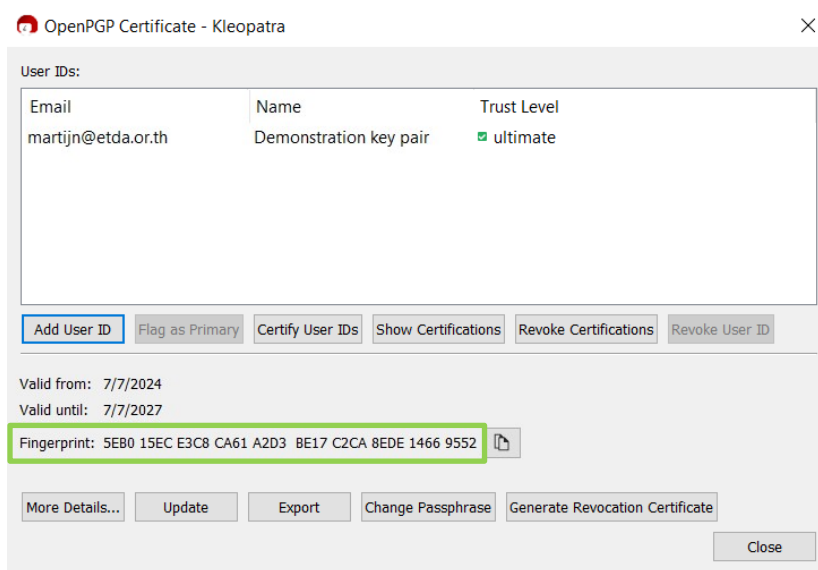
## 2.2 Conducting the Party

Each participant will be handed a copy of the sheet of paper with all key details and a pen at the start of the event, as well as access to download all listed keys.

Downloading all keys can be done first to allow removing keys from the set that failed the verification.

Keep your own key details open on screen in your PGP/GnuPG application when your turn comes, as the key fingerprint will be verified.

### 2.2.1 Viewing your key fingerprint in Kleopatra



### 2.2.2 Viewing your key fingerprint in Thunderbird



The Party involves the event coordinator going through the complete list of keys to verify that everything is correct.

For each key in the list:

- 1) Ask the stated owner of the key to show his/her official government issued photo ID to all, which should match the name of the key;
- 2) Ask the stated owner of the key to state if their e-mail address is correct;
- 3) Verify with the stated owner of the key whether the key is allowed to be published or not;
- 4) Read the (hexadecimal) key fingerprint aloud using the International Radiotelephony Spelling Alphabet, also known as the NATO phonetic alphabet<sup>5</sup>:

0	Zero	8	Eight
1	One	9	Niner
2	Two	A	Alpha
3	Three	B	Bravo
4	Four	C	Charlie
5	Five	D	Delta
6	Six	E	Echo
7	Seven	F	Foxtrot

**Table 2: International Radiotelephony Spelling Alphabet**

After successful verification, all participants add a checkmark for this key on their sheet.

The coordinator moves to the next key in the list until all keys have been processed.

After all participants had their turn, everyone has a sheet of keys they personally verified ownership of.

<sup>5</sup> International Radiotelephony Spelling Alphabet: <[https://en.wikipedia.org/wiki/NATO\\_phonetic\\_alphabet](https://en.wikipedia.org/wiki/NATO_phonetic_alphabet)>

### 3 Phase 3: Signing the verified keys

At any time after the Key Signing Party, typically on a later date when you have returned to your office, you are requested to import and sign the verified keys and send them back signed to their key owner.

The following steps should be repeated for each key to be signed.

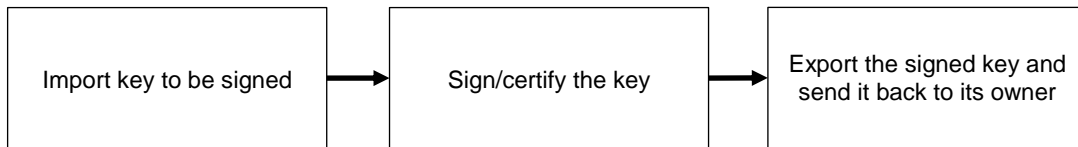


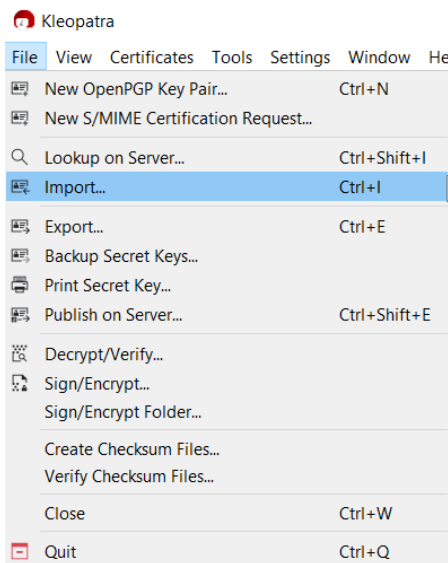
Figure 3: Steps covered in this chapter

#### 3.1 Key signing with Kleopatra

By default, signing (they call it ‘certifying’) a key will only add your signature locally in your personal keychain; exporting the key or uploading it to the Key Servers *will not include your signature*.

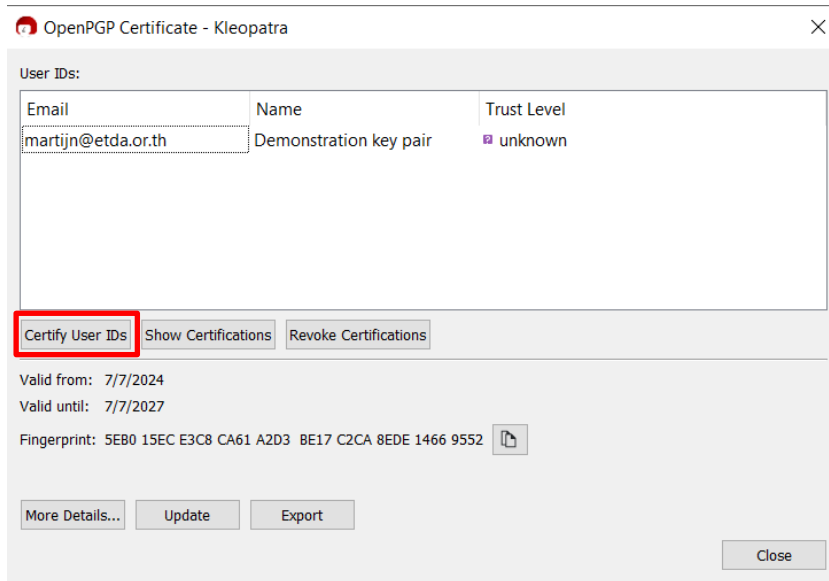
When signing, carefully check what you will be doing.

To import the key, select menu option “File” → “Import...”.

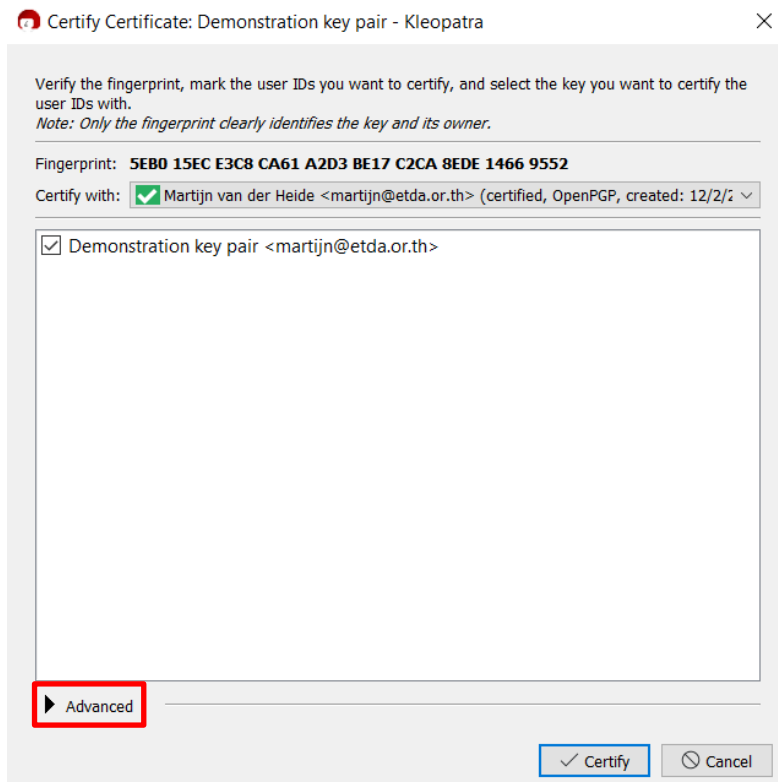




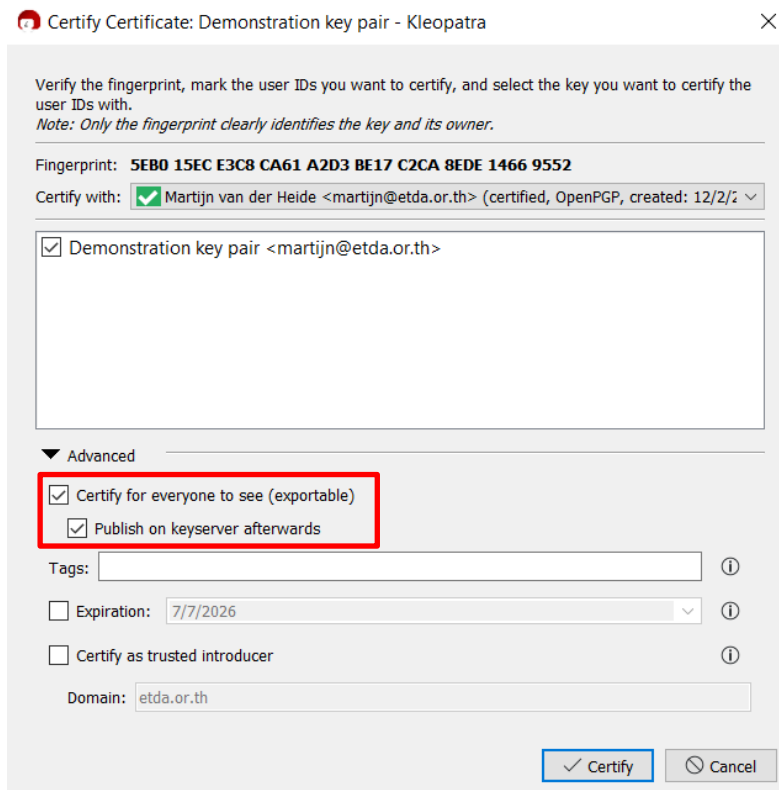
Then double-click on the imported key to get this window:



Select option “Certify User IDs”. This will show the following window where you can select which of your own keys you want to sign (certify) this key with:



Select the “Advanced” option at the bottom to be shown the following:



**Certify Certificate: Demonstration key pair - 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: **5EB0 15EC E3C8 CA61 A2D3 BE17 C2CA 8EDE 1466 9552**

Certify with:  Martijn van der Heide <martijn@etda.or.th> (certified, OpenPGP, created: 12/2/2025)

Demonstration key pair <martijn@etda.or.th>

▼ Advanced

Certify for everyone to see (exportable)

Publish on keyserver afterwards

Tags:  ⓘ

Expiration: 7/7/2026 ⓘ

Certify as trusted introducer ⓘ

Domain:

Note the 2 checkboxes. At least the first one must be checked. The second one must also be checked unless the key owner indicated that their key should not be published on the Key Servers.

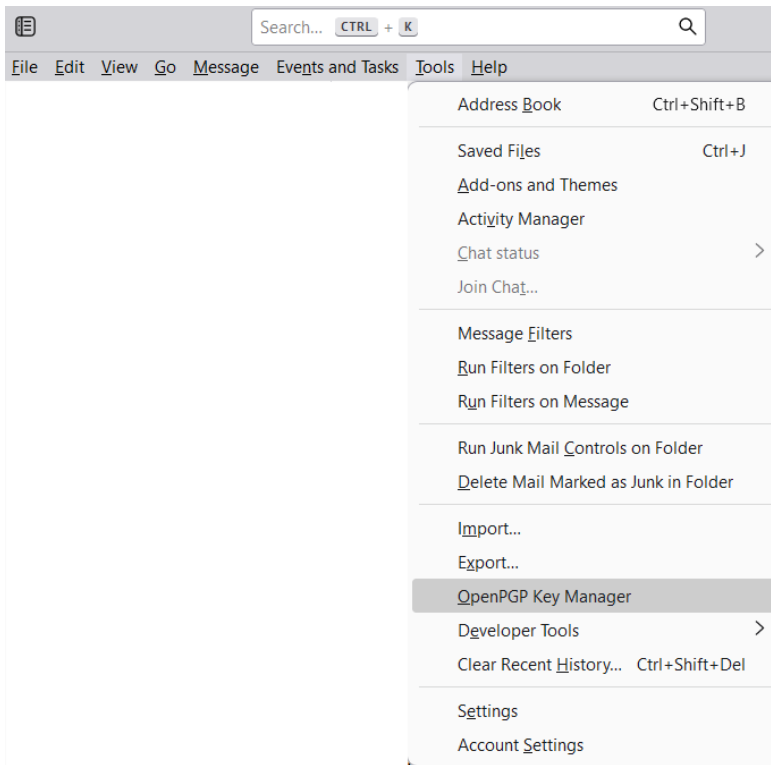
After the key has been signed, you can export it again and send it back to its owner.

If you receive a time-out or another error message during the final step to upload the key to the Key Servers, please refer to chapter 1.4 to perform this step manually.

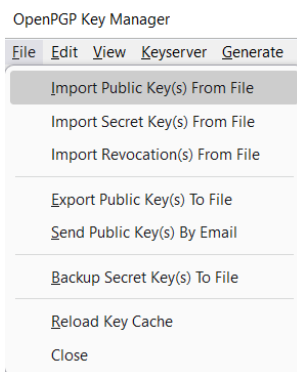
## 3.2 Key signing with Thunderbird

First click on the “Alt” key to bring up the menu strip at the top of the window.

Then select menu option “Tools” → “OpenPGP Key Manager”.



In the OpenPGP Key Manager window select menu option “File” → “Import Public Key(s) from File”.



After the key has been imported it will appear in the list of keys. Double-click it to get the following window:

Key Properties ×

Claimed Key Owner	Demonstration key pair <martijn@etda.or.th>
Type	public key
Key ID	0xC2CA8EDE14669552
Fingerprint	5EB0 15EC E3C8 CA61 A2D3 BE17 C2CA 8EDE 1466 9552
Created	7/7/2024
Expiry	7/7/2027

[Refresh Online](#)

---

[Your Acceptance](#)   Certifications   Structure

Do you accept this key for verifying digital signatures and for encrypting messages?

- No, reject this key.
- Not yet, maybe later.
- Yes, but I have not verified that it is the correct key.
- Yes, I've verified in person this key has the correct fingerprint.

Verify the fingerprint of the key using a secure communication channel other than email to make sure that it's really the key of martijn@etda.or.th.

[OK](#)   [Cancel](#)

As you have personally verified the key during the Key Signing Party, you can select the last option (“Yes, I’ve verified in person this key has the correct fingerprint”) and click OK.

Thunderbird does not let you upload the signed key to the Key Server for privacy reasons (only your own keys), so you must export it again (see chapter 1.3.2), manually upload it (see chapter 1.4), and send it back to its owner.

## 4 Consolidating all new signatures to your key

If all went well, each of the participants of the Key Signing Party signed your key after the event and sent it back to you by e-mail, in phase 3, as you did for them.

There is one final step to be made, as the new signatures are in your e-mailbox rather than attached to your key.

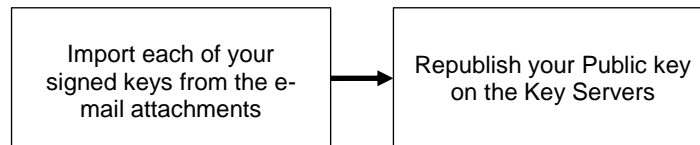


Figure 4: Steps covered in this chapter

For each of the e-mails, save the attachment (your signed key), and import it in your PGP/GnuPG application. This can be done safely as the process only involves adding the new signature. Importing keys is explained in the first step of chapters 3.1 for Kleopatra and 3.2 for Thunderbird.

When finished, you can re-upload your key with all new signatures attached to the Key Servers for all to see. Please refer to chapter 1.2.1 for Kleopatra or 1.3.1 for Thunderbird.