

# Certification management with GnuPG VS-Desktop®

Recommendations for a scaling setup

Target group administrators and security officers

This document applies accordingly to GnuPG Desktop®

Version GnuPG VS-Desktop® 3.x

Document version: 1.0

## Manufacturer / Distributor

g10 Code GmbH  
Bergstr. 3a  
40699 Erkrath / Germany  
+49 2104 4938 790  
info@gnupg.com  
[www.gnupg.com](http://www.gnupg.com)

## Table of contents

1 Introduction.....	3
2 Definitions.....	4
3 Concept trust model.....	5
3.1 Trusted key.....	5
3.1.1 Validity of certifications.....	6
3.2 Trusted introducer.....	6
4 Key distribution.....	7
4.1 LDAP / AD / LDS.....	7
4.2 WKD.....	7
4.3 Certificate files.....	8
4.4 Kleopatra groups.....	8
5 Instructions.....	9
5.1 Create trusted key.....	9
5.2 Create certifications (exportable).....	9
5.3 Certification of a key as a Trusted Introducer.....	10
6 Automation options certification.....	11
6.1 Rohde & Schwarz identity management.....	11
6.1.1 Internal certificates.....	11
6.1.2 External certificates.....	11
6.2 Actium.....	11
7 Certification management by the users.....	12

# 1 Introduction

We recommend institutions, government agencies and larger enterprises to establish an certification management for a scaling VS-NfD compliant certificat administration. Certification management helps to automate the process and make it more secure.

This document first describes the concepts of certification management and then illustrates how it can be implemented in practice with an example.

The key and certificate manager Kleopatra is used as the graphical user interface. Everything described - and much more - is also possible on the command line and can be scripted as well as automated.

Users in an organization without institutional certification management must authenticate the keys of all their communication partners themselves or perform certification management at user level. For more information on this - and how you can prevent it in the case of a functioning institutional certification management - see Chapter 7.

## 2 Definitions

In asymmetric or public key cryptography, some terms are used ambiguously. For example, "key" can mean an OpenPGP key pair, a public key, or a private (=secret) key. It is about cryptographic parameters in any case.

**OpenPGP key pair:** A secret key together with the corresponding public key.

**Public key:** The part of the key pair that is required for encrypting messages and verifying signatures. It is usually published.

**Private key** or secret key: The part of the key pair that is required for decrypting and signing messages. It must be kept secret.

**Certificate:** A public key with additional information (name and/or mail address, validity). Often also called "public key" colloquially.

**Fingerprint:** The unique and immutable checksum over the public key.

**Certification:** A signature contained in the certificate that marks its information as verified. It technically confirms the verification of the authenticity of the public key based on the fingerprint, which is necessary for VS-NfD and NATO-restricted.

**Certification Authority (CA):** A person or role that is authorized to perform fingerprint verification on behalf of others.

**OpenPGP:** A widely used standard for encryption and signing of data and emails. Uses OpenPGP certificates resp. keys.

**S/MIME:** A widely used standard for encryption and signing of mostly email. Uses X.509 certificates.

**Root certificate:** A top-level trust anchor in the S/MIME standard, the certificate of a root CA.

**Intermediate certificate:** An X.509 certificate authenticated by the root certificate that serves as a trust anchor.

**Trusted Key:** Highest level trust anchor for certification management with GnuPG VS-Desktop®, equivalent to a root certificate.

**Trusted Introducer:** Trust anchor in certification management with GnuPG VS-Desktop®, equivalent to an intermediate certificate.

**VS-NfD compliant:** Corresponds to the German approval for encryption of VS-NfD classified data. Refers to the conformity of the software or the certificates used, depending on the context. *VS-NfD* corresponds to the security level *EU Restricted* and *NATO Restricted*.

## 3 Concept trust model

The hierarchical trust management of a classic PKI (Public Key Infrastructure), as is common with S/MIME or X.509 certificates, is quite well known.

OpenPGP allows to apply a hierarchical trust model, too, which has the advantage over the classic PKI that it is much more flexible: certification managers can decide for themselves which authority they want to trust for which domains. The root certificate is called "trusted key" and the intermediate certificates "trusted introducer". However, these behave somewhat differently than their S/MIME equivalents.

The concept described in this chapter can be used very well for large organizations together with an identity management system. This supports or automates the authentication of user certificates, see chapter 6. The integration of smart cards is also possible here.

### 3.1 Trusted key

A trusted key is the anchor of trust in certification management with GnuPG VS-Desktop®. It is trusted in exactly the same way as the user's own key (= ultimate trust). It can therefore effectively authenticate any public key, regardless of whether it is from the user's own domain or a third-party domain. Certificates certified by the trusted key are displayed as VS-NfD compliant in the users' certificate list in Kleopatra without any action on their part.

An OpenPGP key becomes a trusted key when it is entered in the registry<sup>1</sup> on a Windows system. On a Linux system, it is set in the `gpg.conf` file.

Typically, one person (or a group of people) in an organization takes over the certification management for the same; they hold the role of CA. They create a trusted key in the form of an OpenPGP key pair and store its secret key and password in a VS-NfD-compliant manner. We recommend storing the secret key on a smart card (if necessary, see the documentation "Setting up smart cards with GnuPG VS-Desktop®").

Multiple (up to 5 in the default configuration) trusted keys can be used, so that each certification manager has its own trusted key.

For more details see chapter 5.

<sup>1</sup> See: <https://gnupg.com/vsd/registry-settings.html>

### 3.1.1 Validity of certifications

A hierarchical trust model with a trusted key also allows trust to be managed centrally by means of the validity period of the trusted key's credentials.

For example, an expiration date can be set according to organizational guidelines, or in the event of an employee leaving or a lost key, the certificate's certification can be revoked without the aid of the nominal user.

Alternatively, revocation keys can be stored centrally or a designated revoker can be added to new keys.

### 3.2 Trusted introducer

In addition to the *trusted key*, there is also the *trusted introducer*. Such a certificate is only fully trusted for a specific domain. Otherwise, they have the same properties as trusted keys.

An OpenPGP key becomes the trusted introducer of a domain, by entering it as the trusted introducer for this domain during certification in the advanced menu (under "Advanced"). See 5.3.

Typically, this will be used to trust a trusted key from another organization only for certifications within their domain. Thus, a compromised key from an external organization cannot issue certificates for your own organization. This provides a security advantage over the practice with S/MIME, where CAs can usually authenticate anything for any domain, since issuers often do not restrict the "jurisdiction" of their certificates.

## 4 Key distribution

There are several ways to distribute the certificates authenticated by the trusted key or trusted introducer to the users of GnuPG VS-Desktop®:

- LDAP / ActiveDirectory / LDS (internal)
- WKD - WebKeyDirectory (usually external)
- Certificate files (.asc, .pgp)
- Cleopatra group files (.kgrp)

**Note:** The transfer path can be completely insecure. The integrity and correctness of the certificates is secured by the certifications.

### 4.1 LDAP / AD / LDS

Within an organization, it makes sense to set up an internal keyserver. For this, we recommend LDS (Lightweight Directory Services) for Windows and OpenLDAP for Linux.

Setup and configuration is described in the documentation "How to install an LDS for use with GnuPG VS-Desktop®". Corresponding instructions for OpenLDAP on Linux are also available from g10 Code.

To use Kleopatra for publishing a certificate in the LDS / LDAP or to update it after adding an exportable certification, all you have to do is right-click →[Publish to Server] after successful configuration.

Kleopatra and the Outlook plugin (GpgOL) automatically find the associated certificates in the LDS / LDAP when a mail address is specified as the recipient. Alternatively, they can be found in Kleopatra via "Search".

### 4.2 WKD

A WebKeyDirectory (WKD) can be set up so that external communication partners can also access the certificates of your own organization.<sup>2</sup> It is effectively the public phone book for OpenPGP certificates of a organization or domain.

A WKD can be mirrored from an existing LDS, making it easier to maintain the data. Instructions for this can be found here: <https://gnupg.com/kb/mirror-ldap-to-wkd.html>

2 See: <https://wiki.gnupg.org/WKD>

In order for your communication partners to be able to use the trusted introducer feature, all keys stored in the WKD should be *exportably* certified by a trusted key from your organization (see 5.2). You should provide the certificate of this trusted key separately and inform your communication partners how the fingerprint check can be performed for it.

### 4.3 Certificate files

If you do not want to automate the distribution, you can also distribute the certificates (resp. public keys) individually, in the form of certificate files or as Kleopatra groups (see 4.4). Users can thus exchange certificates among themselves without any special infrastructure, for example by sending them by mail or storing them in a shared network drive.

To create a certificate file, select any number of certificates and then use the "Export" function of Kleopatra.

### 4.4 Kleopatra groups

Kleopatra groups are certificate files that contain additional group information.

For Kleopatra groups there is a separate guide (see Help → Group Configuration) which describes both the creation and the usage.

They have the advantage that you can use them to encrypt for all members of a group at the same time by selecting only the group as recipient. Kleopatra groups can also be used in Outlook, as long as the name is a shared mail address.

A typical use case is that a responsible person collects the certificates of all participants at the beginning of a project, makes sure that they are all certified in an exportable way (if necessary, she certifies them herself), and then distributes them to the project participants via any channel (e.g. by mail).

## 5 Instructions

### 5.1 Create trusted key

The certification manager has a compliant OpenPGP key, the trusted key. This can be generated using the Kleopatra program included in GnuPG VS-Desktop® (see Help → Quick Start Guide). We have named this key "GnuPG.com OpenPGP CA" in our example. In practice, it should have your own organization designation in its name so that it can be easily identified. The trusted key does not require a mail address.

The fingerprint of the trusted key is entered in the registry for all GnuPG VS-Desktop® installations in your organization (see <https://gnupg.com/vsd/registry-settings.html>). If you need more than the 5 trusted keys defined by default, we will provide you with a customized version of GnuPG VS-Desktop® on request .

The public key of the trusted key is usually distributed to the users via the Active Directory. See "How to install an LDS for use with GnuPG VS-Desktop®" for setup instructions. Under Linux you need LDAP for this, see "How to use LDAP with GnuPG".

### 5.2 Create certifications (exportable)

You want to authenticate the new key of an employee with the trusted key for all to see. For this purpose, the employee has exported her public key and sent it to you, e.g. by e-mail. You import this key as follows:

- Right-click the key you want to edit in the certificate list
- Select [Certify]
- Make sure that the public key you are authenticating belongs to the correct person by matching the fingerprint via a 2nd source (e.g. telephone)
- Select your trusted key from the "Certify with" drop-down menu. In our example this is *"GnuPG.com OpenPGP CA"*.
- Expand the "Advanced" menu by clicking on the arrow.
- Select "Certify for everyone to see (exportable)" here.
- If you have configured an internal LDS as key server, select "Publish on key server". You can also do this at any time with the action "Publish on server".

- Select an expiration date for the certification. The usual is 3 years.

**Certify Certificate: Ted Tester - Kleopatra** [Close]

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: **9811 1E67 AE06 F2BE FD2B DE10 C5D6 C919 005F 36A4**

Certify with:  Ted Tester <Ted.Tester@demo.gnupg.com> (★ VS-NfD-konform, OpenPGP, created: 08.03.2023) ▾

Ted Tester <Ted.Tester@demo.gnupg.com>

▼ **Advanced**

Certify for everyone to see (exportable)  
 Publish on keyserver afterwards

Tags:  ⓘ

Expiration:  ▾ ⓘ

Certify as trusted introducer ⓘ

Domain:

- Execute the certification by clicking on [Certify].
- You will be asked for the password of the trusted key. Enter it and confirm with [OK].

### 5.3 Certification of a key as a Trusted Introducer

If you want to authorize a key to authenticate all keys of a certain domain, proceed as described above, but with the following difference:

- In the "Advanced" menu, additionally check "Certify as trusted introducer".
- Also specify the domain that will be trusted with this certificate there.

## 6 Automation options certification

### 6.1 Rohde & Schwarz identity management

#### 6.1.1 Internal certificates

The combination with the Rohde & Schwarz Trusted Object Manager (TOM) and Trusted Identity Manager (TIM) automates the certification system.

This is possible because the TOM already has an identity relationship via the smart card. Thanks to this identity relationship, VS-NfD-compliant identification with a certificate is possible. Therefore, the TOM can automatically certify the certificates and provide them via an LDS.

The identification and internal key distribution is thus already done.

#### 6.1.2 External certificates

To communicate with external parties, create another trusted key as described in chapter 2 and enter it. Ideally, you can now use this to authenticate the certificate of an external TOM as a trusted introducer. If this is not possible, you can still check individual certificates and make them available in your key distribution.

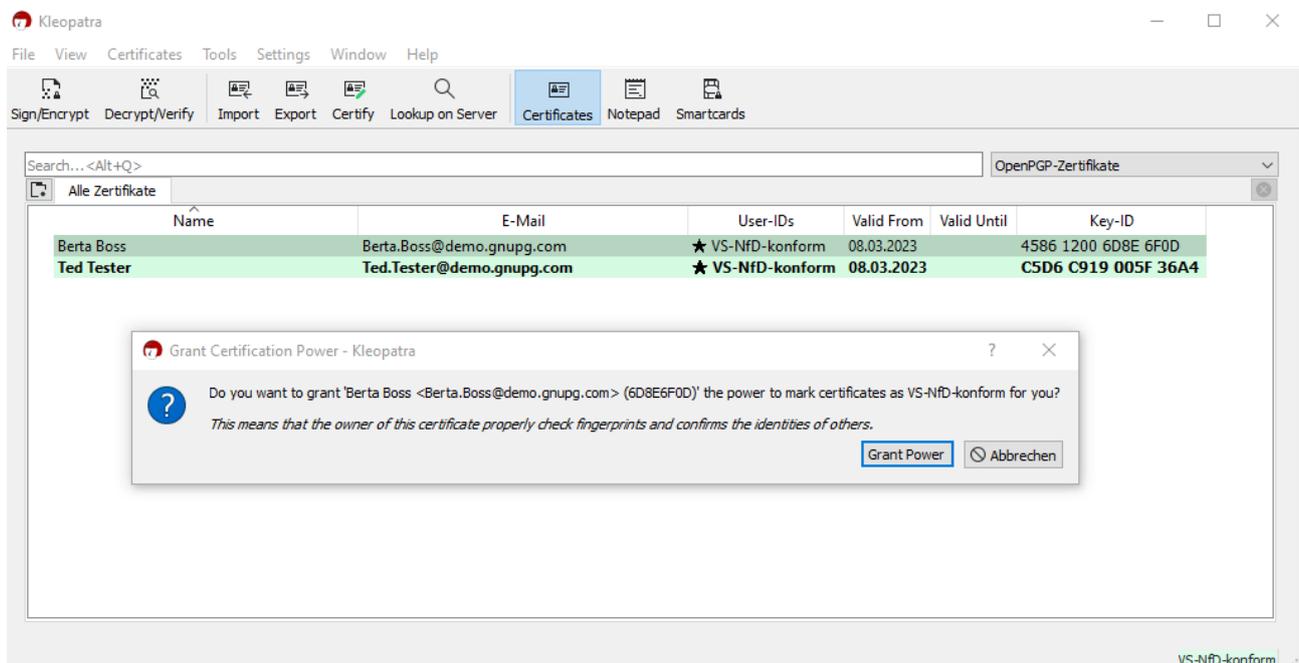
### 6.2 Actium

Actium is a server software for automated certification of certificates from your organization's LDAP.

It will be published by g10 Code GmbH in 2023.

## 7 Certification management by the users

In the default configuration of GnuPG VS-Desktop®, users can both certify a public key as a trusted introducer and grant certification authority to any certificate. This is done by right-clicking on the certificate → [Change Certification Power] → [Grant Power]:



A key with certification authority (trust level=full) corresponds to a trusted key in practical use.

If you want to prevent users in an organization from managing certifications themselves, you can configure Kleopatra so that the corresponding options are not offered.

For this, you need to set the Kleopatra action *certificates\_change\_owner\_trust* to *false* in the registry, for details see the description on <https://gnupg.com/vsd/kleopatra-settings.html>.

To disallow certifications by users in general, if all attestations are to be managed centrally only, you can set *certificates\_certify\_certificate* to *false*.