Certificate Management with GnuPG VS-Desktop®

Scaling Solutions for Secure Trust Management

Document Version: 1.0

Abstract

This whitepaper provides an explanation of basic encryption methods, with a particular emphasis on asymmetric encryption. It also introduces distributed and hierarchical trust models, discusses the utilization of trusted keys and trusted introducers for key management, and explores various methods for distributing certificates. GnuPG VS-Desktop®, along with its included programs and plugins, facilitates the accomplishment of these tasks within both small and large organizations, particularly in security-critical environments.

Introduction

Authorities and institutions dependent on electronic communication and data sharing should put data security and integrity first. This imperative is particularly important for organizations entrusted with sensitive data labeled as "VS-Nur für den Dienstgebrauch (Restricted)", VS-NfD. GnuPG VS-Desktop® simplifies the generation, distribution, and validation of certificates in small and large organizations. The open source software is not only VS-NfD compliant, it also offers process automation capabilities.

g10 Code GmbH ▪ Bergstr. 3a ▪ 40699 Erkrath, Germany ▪ +49 2104 4938 790 ▪ info@gnupg.com ▪ www.gnupg.com

Contents

1 Encryption Methods

In essence, an encryption method comprises a cryptographic algorithm and, at a minimum, one secret key (also referred to as private key). While symmetric encryption relies on a single secret key, asymmetric encryption uses key pairs: a private key and a public key.

1.1 Symmetric Encryption

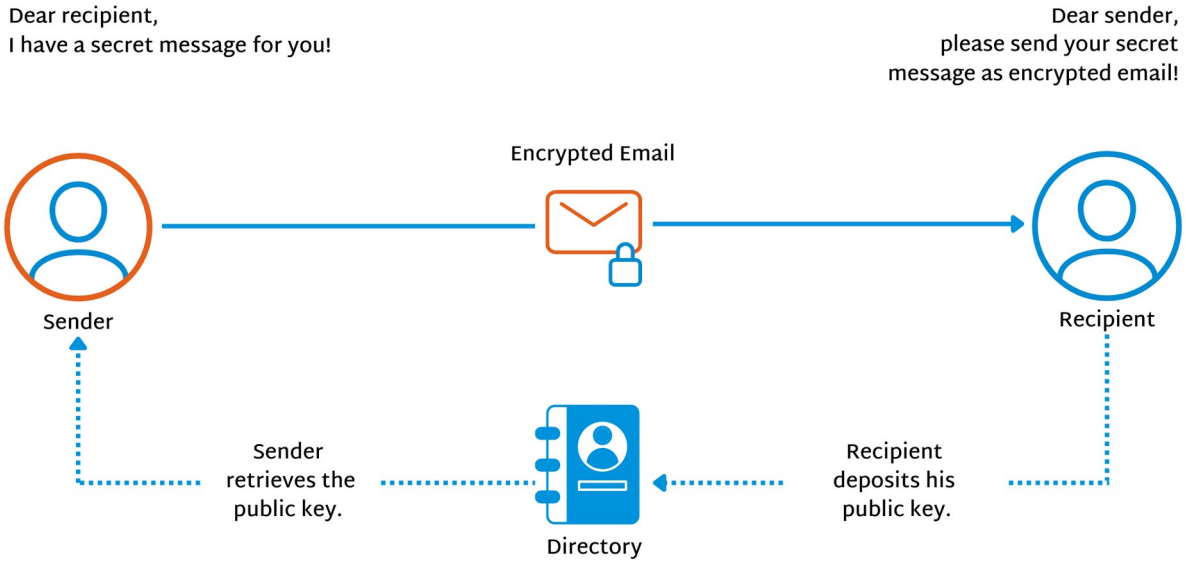
When there's a single key for both encryption and decryption, the process is typically straightforward and, most importantly, intuitive for users. For instance, in the case of a password-protected document, the recipient only requires the password to decrypt it.

However, the challenge lies in securely transmitting the secret key to the involved communication partners. Additionally, as more users gain knowledge of the secret key and participate, the procedure becomes increasingly insecure and susceptible to vulnerabilities. With each new receiver, a new password must be introduced, demanding participants to remember or securely store them (i.e. in a password manager).

1.2 Asymmetric Encryption

In asymmetric encryption, also known as public key cryptography, each user creates their own key pair, comprising a confidential private key and a corresponding public key, which are stored together in a keyring. Only individuals possessing the public key can transmit encrypted data to the holder of the private key, or authenticate the user's digital signature. The private key is employed for decrypting the encrypted data and for generating digital signatures, and is always kept confidential and in the possession of its owner. Since only the public key needs to be exchanged, there's no need for a specially secured transport route.

A useful analogy is that when a recipient wishes to receive confidential, encrypted messages from a sender, the recipient creates a lock that can only be unlocked with her private key. He passes the opened lock on to the sender, keeping his own key safe. The sender then composes the message, places it in a box, and locks it with the recipient's opened lock. The securely packaged message is sent to the recipient. The recipient opens the box with his private key, pleased that the message could not be read on its journey.



1.3 Challenges in Public Key Cryptography

However, a crucial question arises: how can the recipient ascertain the origin of the encrypted message, specifically identifying the sender? In practice, any person can (and should) utilize the public key to encrypt messages. The challenge remains: how can both sender and recipient confirm the legitimacy of the "correct" public key? In asymmetric encryption, mechanisms must be in place to authenticate the identities of the communicating parties:

- Digital **signatures** have two purposes: firstly, they can verify the source of data, and secondly, they are employed for certificate validation.
- The distinctive and unchangeable checksum associated with the public key is referred to as a **fingerprint**.
- Digital **certificates** contain information about the certificate holder, the public key, and authentication signatures. Certificates also store information about the certificate issuer, the recipient, and how long it is valid.

In public key cryptography, two main questions must be addressed:

1. How can one ensure that the key, respectively the certificate and the owner, belong together?
2. What are the options for distributing and managing the certificates and public keys?

The next sections will present possible answers and solutions that are particularly suitable for large environments and organizations.

2 Trust Models

The affiliation of public keys and digital certificates must be verifiable beyond doubt, and this is precisely where the Public Key Infrastructure (PKI) plays a crucial role. A PKI provides services that verify and distribute digital certificates. In addition, a PKI ensures the secure exchange of certificates between senders and recipients. When multiple PKIs need to communicate in a mutually trustworthy manner, the establishment of trust models becomes imperative.

Various trust models exist, differing primarily in the role of the certification authority (CA). The CA is a person or role responsible for verifying and validating public key fingerprints, and for issuing certificates.

2.1 Distributed Trust Model

In this scenario, communication partners mutually validate the authenticity of a certificate. To achieve this, they exchange their personal information and the key fingerprints. If user A signs user B's key (after A has verified B's identity), user A expresses trust in B's key signature. Consequently, user A may also trust all other keys signed by B.

In this distributed scenario, each Certification Authority autonomously shares its public keys with all other CAs. The level of trust increases with the number of individuals who have signed a public key. Thus, many users act as trust entities in this **Web of Trust**. However, the certification process demands substantial effort and usually requires a face-to-face meeting. As a result, this trust model lacks scalability, quickly rendering it impractical within larger organizations and environments.

2.2 Hierarchical Trust Model

Due to the impracticality and time-consuming nature of printing and comparing fingerprints, an alternative approach involves introducing another entity: in the hierarchical trust model, a higher-level Certification Authority operates within the Public Key Infrastructure and maintains the root certificates of the lower-level CAs. As a result, all other entities belonging to this PKI trust the root certificates. Users and also other CAs trust the root CA.

Hence, trust is not based on individual user keys but on the public keys and signatures of the connected CAs. These CAs are organized hierarchically, forming a **Chain of Trust**.

Note

In larger organizations, the hierarchical trust model is the preferred approach. When combined with an identity management system (IdM), numerous processes can be automated (see section 4.5), such as the validation of user certificates.

The hierarchical trust model is employed in traditional PKIs, including S/MIME and the X.509 certificates used there.

2.3 OpenPGP's Flexible Trust Model

OpenPGP also allows for the implementation of a hierarchical trust model, offering the advantage of greater flexibility compared to traditional PKI. Certification managers can decide for themselves which authorities they choose to trust for specific domains.

- The root certificate is called a **Trusted Key**.
- The "intermediate certificates" are known as **Trusted Introducers**.

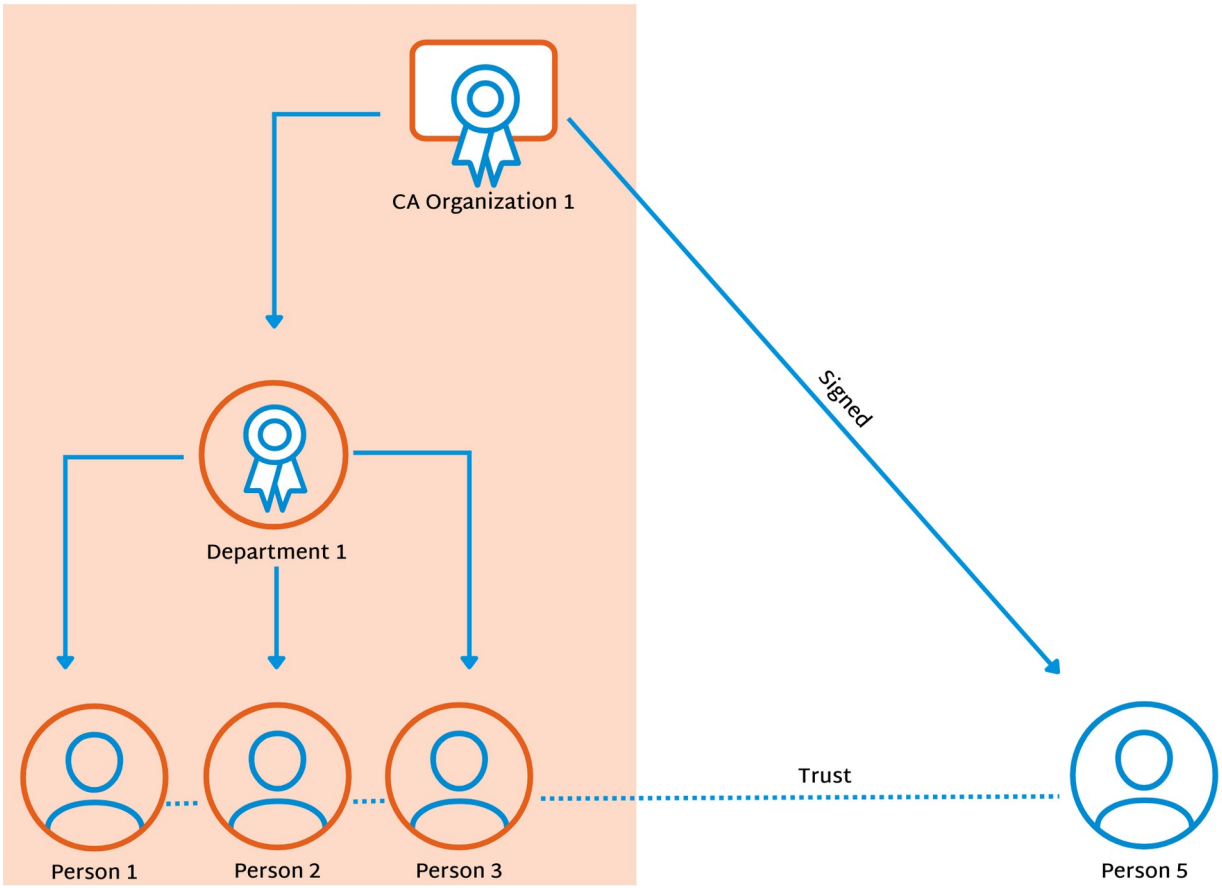
a) Trusted Key

In authentication management with GnuPG VS-Desktop®, the trusted key serves as the trust anchor. It holds the same level of trust as the user's own key (ultimate trust). It can effectively authenticate any public key, regardless of whether it belongs to the user's own domain or to a third-party domain.

Within an organization, either an individual or a designated group assumes the responsibility of authentication management, effectively acting as the Certificate Authority. This individual or group generates a trusted key in the form of an OpenPGP key pair and securely stores its secret key and password in compliance with VS-NfD regulations. Smart cards provide one secure method for key storage.

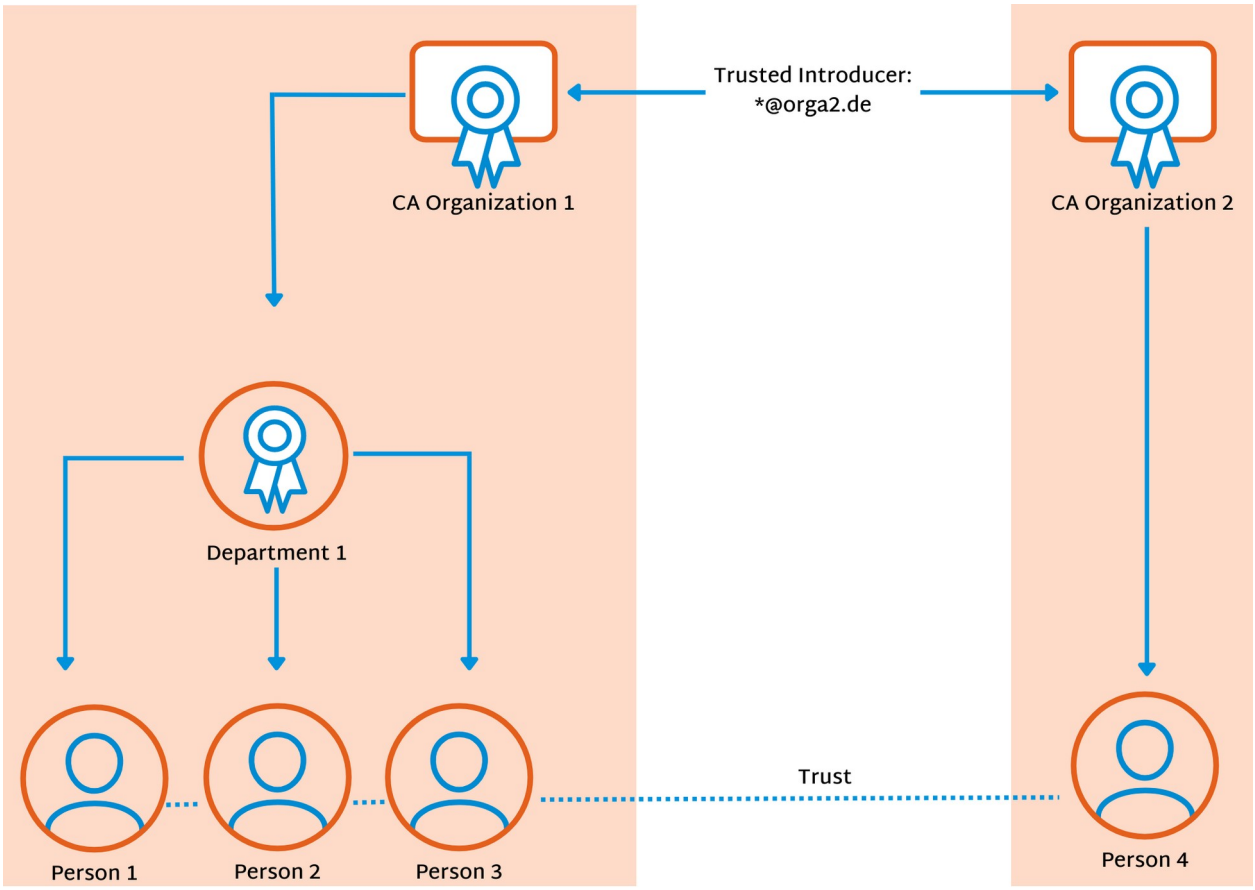
In a hierarchical trust model with a trusted key, it's possible to centrally manage trust over a credential's validity period. This includes the ability to establish an expiration date in accordance with the organization's policies. Furthermore, the model allows for the revocation of certificate authentication when necessary, such as in cases of employee departures, lost keys, or reasonable suspicions of key compromise.

Manual intervention utilizing a revocation key or a designated revoker, an authorized individual responsible for invalidating previously published public keys, is also a viable option in this hierarchical trust model.



b) Trusted Introducer

In addition to the trusted key, the trusted introducer plays a vital role. A trusted introducer certificate is exclusively trusted for a specific domain. This proves valuable when trusting a key from another organization, but only for authentications within its designated domain. This approach ensures that even if a key from an external organization becomes compromised, it can't be used to issue certificates for its own organization.



GnuPG VS-Desktop® provides a notable security advantage over S/MIME. In S/MIME, CAs can usually authenticate anything for any domain, since the issuers often do not restrict the "jurisdiction" of their certificates.

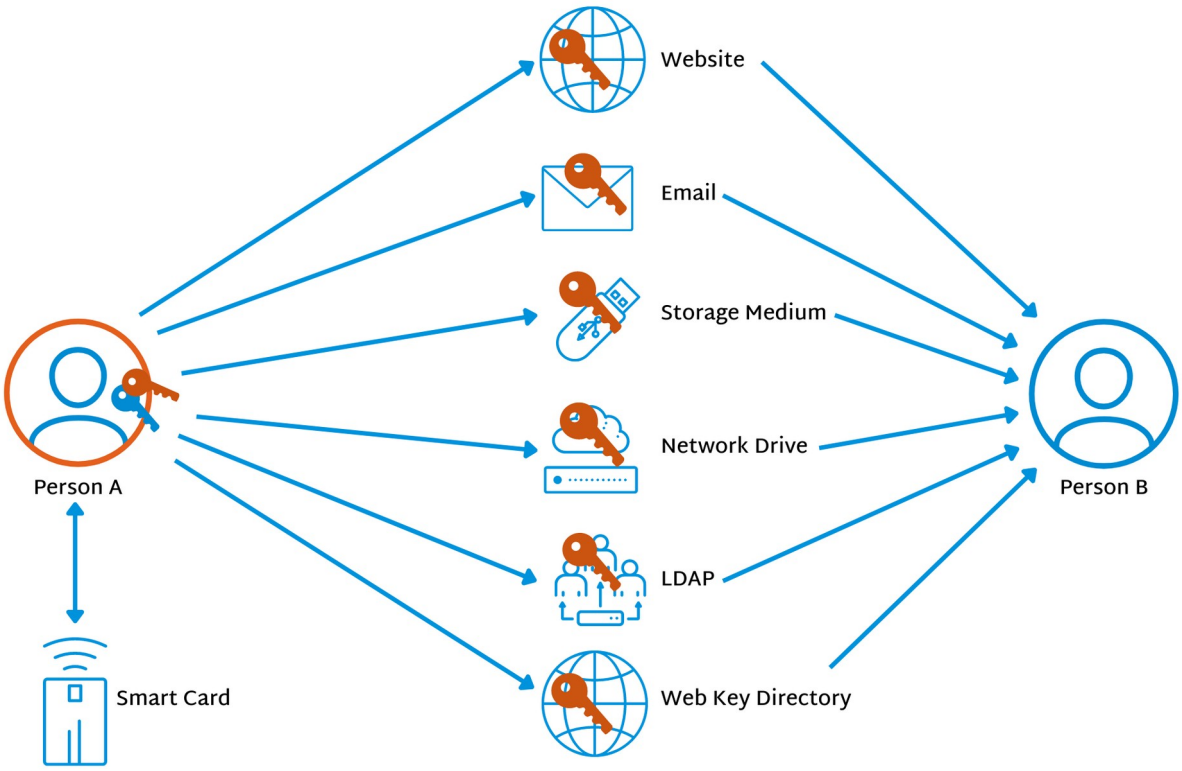
3 Distribution of Certificates

There are several technical methods available for distributing certificates authenticated by the trusted key or trusted introducer to GnuPG VS-Desktop® users. As a reminder, the public keys do not require special protection or secrecy, as the integrity and correctness of the certificates are ensured by the attestations.

If automated distribution is not necessary, the certificates can be published on a website, stored on a network drive, or distributed via storage media or email. This allows users to exchange certificates with each other without the need for a dedicated infrastructure.

For organizations, the following alternatives are particularly noteworthy:

- Internal Key Server (LDAP, AD, LDS)
- Web Key Directory (WKD), Web Key Service (WKS)
- Kleopatra Groups



3.1 Internal Key Server (AD, LDS, LDAP)

In organizations, setting up and operating an internal key server makes sense. This server takes over the administration of OpenPGP and X.509 certificates. A directory service can be used for this purpose:

- Active Directory Domain Services (AD DS) or Active Directory Lightweight Directory Services (AD LDS) on Windows
- OpenLDAP on Linux

On Windows, we recommend setting up a key server with LDS (Lightweight Directory Services). LDS offers a more streamlined solution compared to Active Directory and can function autonomously or seamlessly integrate into an existing AD directory service. One notable advantage of employing a dedicated LDS server for GnuPG key storage is that it eliminates the need to extend an existing Active Directory schema. On Linux, OpenLDAP is the recommended directory service.

The configuration of the respective directory services requires the installation of a custom schema. GnuPG has extended the schema developed in the late 1990s by incorporating additional attributes. Among other things, these enhancements make it possible to search for certificates based on fingerprints and store additional information related to subkeys and email addresses.

Note

We are happy to provide instructions for setting up LDAP and LDS key servers as separate manuals. For further assistance, please don't hesitate to reach out to us via email at: info@gnupg.com

3.2 Web Key Directory (WKD), Web Key Service (WKS)

A Web Key Directory (WKD) serves as a means for external communication partners to access their organization's certificates. It offers up-to-date public keys for designated email addresses through HTTPS. Essentially, the WKD is more or less a public phone book, housing OpenPGP certificates associated with one's own organization or domain.

To establish a Web Key Directory for your organization, you'll require a web server for the corresponding domain. For larger organizations, it's advisable to implement a comprehensive Web Key Service (WKS) to automate the publication of the Web Key Directory.

3.3 Kleopatra Groups

The certificate manager Kleopatra (see section 4) supports groups to regularly address the same communication partners. Kleopatra groups are essentially certificate files (S/MIME or OpenPGP) with additional information. Users can conveniently encrypt messages for all members of a group simultaneously by selecting the group as the recipient.

Here's a common scenario: At the beginning of a project, a designated person collects the certificates of all participants, verifies their authenticity, and handles the distribution of these certificates to all project members through any suitable means (e.g., via email).

Note

Kleopatra groups can also be used in Outlook, provided that the group's name corresponds to a valid email distribution address.

4 GnuPG VS-Desktop®: Best Practices

The open source software GnuPG VS-Desktop® consists of the following independently developed programs:

- **GnuPG**: the cryptographic core (in its approved design state according to German Federal Office for Information Security)
- **Kleopatra**: key and certificate manager
- **GpgOL**: Plugin for Microsoft Outlook, providing mail encryption (support for IMAP/SMTP and MS Exchange)
- **GpgEX**: Plugin for Windows Explorer (file encryption)

In 2019, the German Federal Office for Information Security (BSI) granted approval to GnuPG VS-Desktop® for the secure transmission of confidential documents classified as "VS-Nur für den Dienstgebrauch (Restricted)", VS-NfD. This approval also extends to the corresponding international security levels EU RESTRICTED and NATO RESTRICTED.

GnuPG VS-Desktop® and its components address the challenges associated with trust establishment and certificate distribution.

4.1 Generating a Trusted Key

The certification manager generates a trusted key in the form of an OpenPGP key pair, for example with the Kleopatra program. The trusted key should contain the organization's name for easy identification. A mail address is not mandatory for this key. The corresponding fingerprint should be stored in the Windows Registry for all installations within the organization or in the *gpg.conf* file on Linux systems.

Note

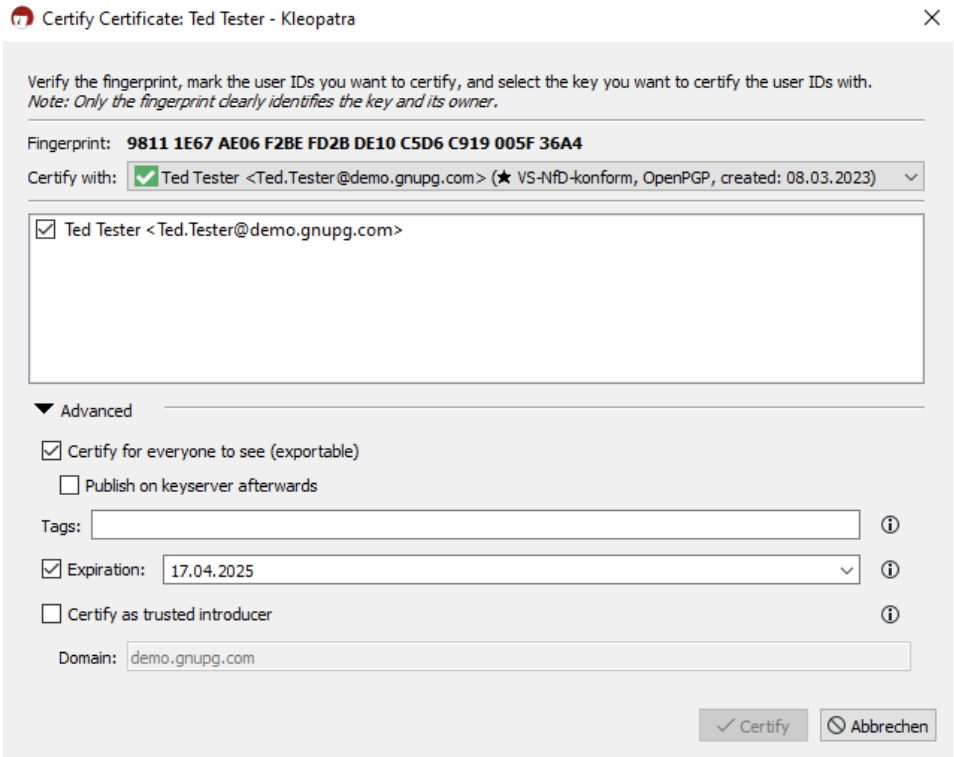
In the default configuration, GnuPG VS-Desktop® is equipped to handle up to five trusted keys. Should you require more than five trusted keys, we are happy to provide a customized version of GnuPG VS-Desktop® upon request.

The distribution of the public key can be accomplished through one of the methods outlined in section 3.

4.2 Creating Certifications (exportable)

To authenticate a newly added employee's key using the publicly visible trusted key, the employee exports the public key and transmits it to the certification manager. To do this, she performs the following steps in Kleopatra:

1. Right click on the key that needs to be edited in the certificate list and select *Certify* from the menu.
2. Verify that the public key belongs to the correct person: she needs to compare fingerprint via a second source, for example, by telephone.
3. In the *Certify with* drop-down menu, she can select the trusted key; in our example, this is *GnuPG.com OpenPGP CA*.
4. After expanding the *Advanced* menu at the bottom of the dialog, she can activate the checkbox *Certify for everyone to see (exportable)*.
5. If an internal key server exists, she can select the checkbox *Publish on keyserver afterwards*. It's also possible to publish the key at a later time.
6. Set the expiration date; three years is common.
7. Click on *Certify*, enter the password of the trusted key, and confirm with *OK*.

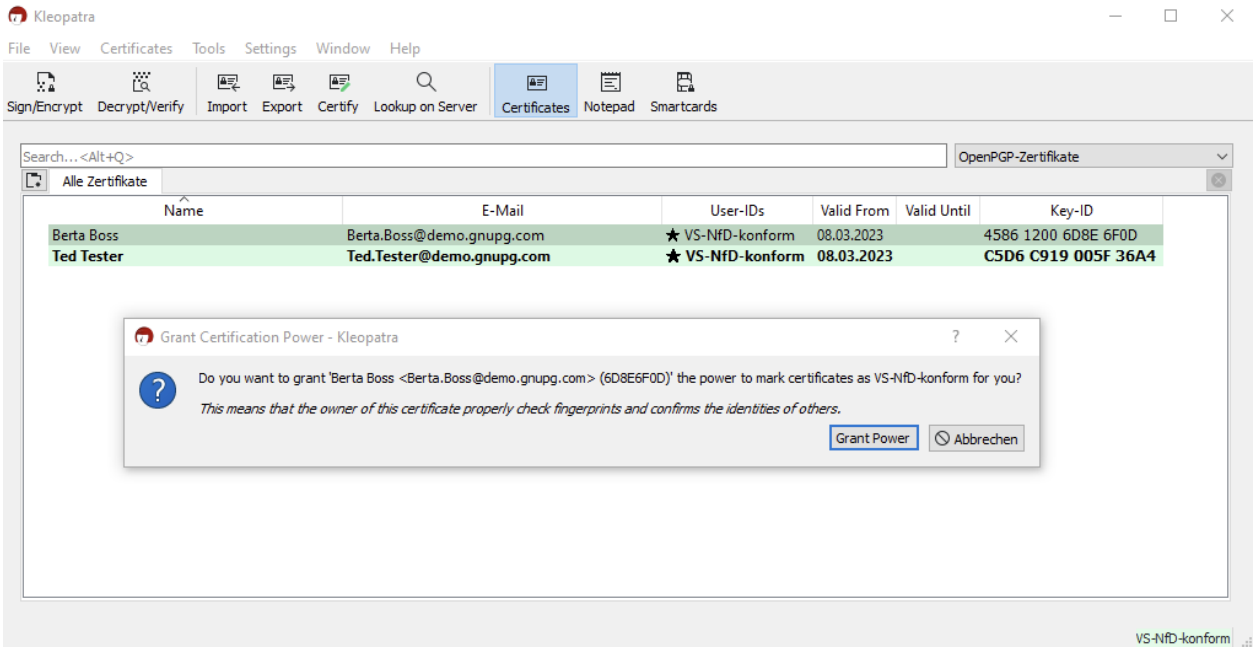


4.3 Creating a Trusted Introducer

To enable a key to act as a trusted introducer, meaning it's authorized to authenticate all keys of a certain domain, the setup process follows the same steps as described in the previous section. Additionally, the checkbox *Certify as trusted introducer* must be activated; the domain name belongs in the field below.

4.4 User-Initiated Certification Management

In the default configuration, users can certify a public key as trusted introducer or grant certification authority to any certificate. This can be done by right-clicking on a certificate and selecting the *Change Certification Power* option. In the next dialog, users can confirm their choice by clicking the *Grant Power* button.



Note

A key with certification authority corresponds in practice to a trusted key.

To prevent users from authenticating certificates themselves, Kleopatra can be configured accordingly. This requires modifying the Windows Registry; the *certificates_change_owner_trust* action must be set to *false*. If all authentications are managed centrally, user-based authentications can be disabled completely. To achieve this, the *certificates_certify_certificate* action must be set to *false*.

4.5 Automating Processes

In larger organizations, it is advisable to automate processes, and this can be achieved through various means:

- **GnuPG actium**: This open source software, developed by g10 Code GmbH, plays a pivotal role in automating the certificate authentication process via an organization's directory service. Here's how it works: Users generate their certificates and effortlessly submit them to the directory service with a simple click. actium then retrieves the newly issued certificates from the directory service and dispatches an encrypted email containing a confirmation link. Only individuals with access to both the email and the generated certificate possess the capability to access and activate the confirmation link. actium then authenticates the certificate, subsequently relaying it back to the directory service.
- **Identity Management**, in collaboration with our partner Rohde & Schwarz: The R&S®Trusted Objects Manager (TOM) combined with the R&S®Trusted Identity Manager (TIM) automate the authentication system. Notably, the TOM's pre-established identity connection via smart card infrastructure enables VS-NfD-compliant authentication using cryptographic keys. Therefore, the TOM can automatically authenticate certificates and provide them via directory service.

5 Conclusion

Reliable and scalable certificate management is essential for many organizations, particularly authorities and institutions with VS-NfD or EU General Data Protection Regulation (GDPR) requirements. GnuPG VS-Desktop® stands out as a well-established open source solution that not only upholds the most stringent security criteria but also facilitates process automation. The software supports distributed and hierarchical trust models and offers flexible approaches to establish and manage trust in keys and certificates.

Organizations benefit from a range of distribution methods, spanning from internal key servers to web key directories, which facilitate the efficient and secure distribution of certificates. GnuPG VS-Desktop® also leads the way in terms of automation. The seamless integration with identity management systems and automated certification processes empowers organizations not only to fulfill their security requirements but also significantly diminish administrative overhead.

6 About GnuPG

GnuPG embodies the principles of independence, sovereignty, and the safeguarding of digital privacy. For over 25 years, this cryptographic software has been meticulously crafted through an open and transparent development process. Since its inception in 1997, GnuPG's encryption code has consistently delivered unparalleled protection against message surveillance and unauthorized data storage by third parties.

Serving as a comprehensive solution, GnuPG VS-Desktop® encrypts and decrypts emails, messages, documents, etc. on Windows and Linux. Since 2019, the software has been approved by the German Federal Office for Information Security (BSI) for for securely transmitting confidential documents classified as "VS-Nur für den Dienstgebrauch (Restricted)", VS-NfD.

The manufacturer, g10 Code GmbH, provides personalized services, training, and support tailored to administrators and IT security officers.

https://gnupg.com/