Zertifikatsverwaltung mit GnuPG VS-Desktop®

Skalierende Lösungen für sicheres Vertrauensmanagement

Dokumentversion: 1.0

Abstract

Dieses Whitepaper erklärt grundlegende Verschlüsselungsverfahren, insbesondere die asymmetrische Verschlüsselung. Darüber hinaus führt es in verteilte und hierarchische Vertrauensmodelle ein, erörtert die Verwendung von Trusted Keys und Trusted Introducers zur Schlüsselverwaltung sowie verschiedene Methoden zum Verteilen der Zertifikate. GnuPG VS-Desktop®, die enthaltenen Programme und Plugins, helfen bei der Bewältigung dieser Aufgaben in kleinen und großen Organisationen, insbesondere in sicherheitskritischen Umgebungen.

Einleitung

Behörden und Institutionen, die auf elektronische Kommunikation und Datenaustausch angewiesen sind, sollten Sicherheit und Integrität der Daten an die erste Stelle setzen. Das gilt insbesondere für Organisationen, die mit sensiblen Informationen umgehen, die als „Verschlusssache – Nur für den Dienstgebrauch" (VS-NfD) eingestuft sind. GnuPG VS-Desktop® vereinfacht das Erstellen, Verteilen und Beglaubigen von Zertifikaten in kleinen und großen Organisationen. Die Open-Source-Software ist nicht nur VS-NfD-konform, sie ermöglicht auch die Automatisierung von Prozessen.

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

Inhalt

1 Verschlüsselungs-Verfahren

Grundsätzlich besteht ein Verschlüsselungs-Verfahren aus einem kryptografischen Algorithmus und mindestens einem geheimen Schlüssel (Private Key). Während es bei der symmetrischen Verschlüsselung nur einen geheimen Schlüssel gibt, kommen bei der asymmetrischen Verschlüsselung Schlüsselpaare zum Einsatz: ein geheimer und ein öffentlicher Schlüssel.

1.1 Symmetrische Verschlüsselung

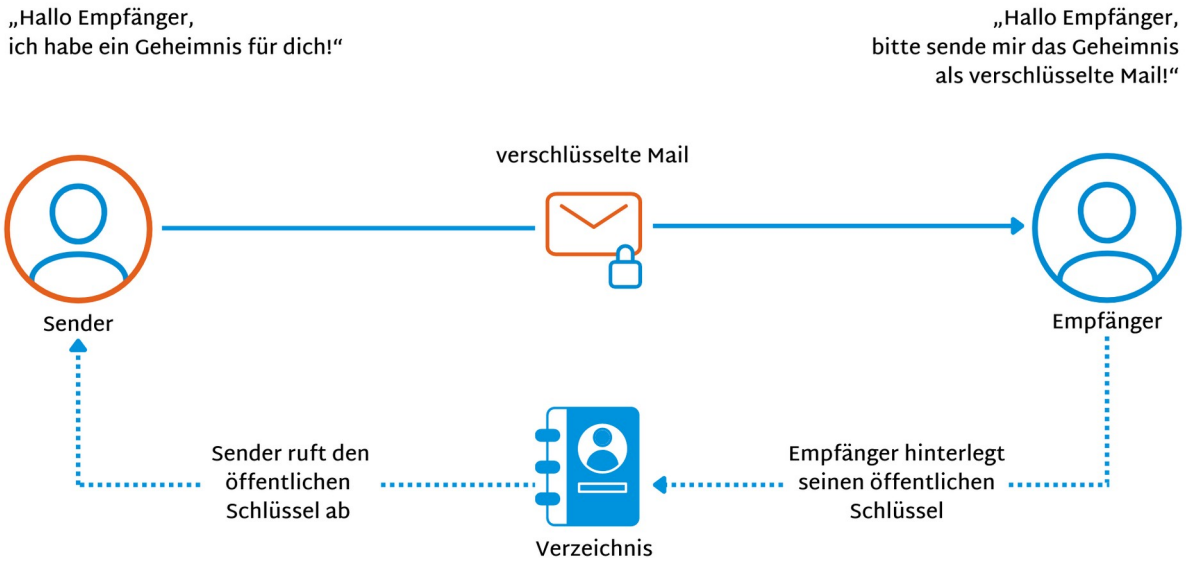
Wenn es nur einen einzigen Schlüssel zum Verschlüsseln und Entschlüsseln gibt, ist das meist recht unkompliziert und vor allem einleuchtend für die Benutzer. Ist ein Dokument z. B. mit einem Passwort geschützt, dann braucht die Empfängerin des verschlüsselten Dokuments lediglich das Passwort, um es zu entschlüsseln.

Wie aber gelangt der geheime Schlüssel über einen sicheren Kanal an die beteiligten Kommunikationspartner? Weitere Nachteile liegen auf der Hand: Je mehr Benutzer den geheimen Schlüssel kennen und beteiligt sind, desto unsicherer und anfälliger wird das Verfahren. Mit jedem neuen Empfänger kommt ein neues Passwort dazu, das sich die Beteiligten merken oder sicher notieren müssen (Stichwort: Passwortmanager).

1.2 Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung (Public-Key-Kryptografie) erzeugt jede Anwenderin anstelle eines einzelnen Schlüssels ein eigenes Schlüsselpaar, das aus einem geheimen, privaten und einem öffentlichen Schlüssel besteht und in einem Schlüsselbund (Keyring) zusammengehalten wird. Nur wer über den öffentlichen Schlüssel verfügt, kann verschlüsselte Daten an den Besitzer des privaten Schlüssels schicken und auch dessen digitale Signatur überprüfen. Der private Schlüssel kommt beim Entschlüsseln der verschlüsselten Daten und beim Erzeugen von digitalen Signaturen zum Einsatz. Er bleibt stets geheim und bei der Besitzerin. Da lediglich der öffentliche Schlüssel ausgetauscht werden muss, muss der Transportweg nicht besonders gesichert werden.

Ein Beispiel: Möchte ein Empfänger von jemand geheime, verschlüsselte Botschaften enthalten, dann fertigt der Empfänger ein Schloss an, das sich nur mit seinem privaten Schlüssel öffnen lässt. Das geöffnete Schloss gibt er an den Sender weiter, den eigenen Schlüssel bewahrt er sicher auf. Der Sender verfasst die Nachricht, legt sie in eine Kiste, die er mit dem geöffneten Schloss des Empfängers verschließt. Die gut verpackte Nachricht macht sich auf den Weg zum Empfänger. Dieser öffnet mit seinem privaten Schlüssel die Kiste und freut sich, dass die Nachricht unterwegs nicht gelesen werden konnte.



1.3 Herausforderungen beim Public-Key-Verfahren

Wie aber kann der Empfänger sicher sein, dass die verschlüsselte Nachricht von einem bestimmten Sender stammt? In der Praxis kann (und soll) jede Person den öffentlichen Schlüssel verwenden, um Nachrichten zu chiffrieren. Und wie stellen Sender und Empfänger sicher, dass es sich um den „richtigen“ öffentlichen Schlüssel handelt? Bei der asymmetrischen Verschlüsselung muss es Mechanismen geben, um die Authentizität der Kommunikationspartner zu überprüfen:

- Digitale **Signaturen** haben zwei Einsatzzwecke: Mit ihrer Hilfe lässt sich einerseits die Herkunft von Daten überprüfen. Andererseits dienen sie zum Validieren von Zertifikaten.
- Die eindeutige und unveränderliche Prüfsumme über den öffentlichen Schlüssel heißt **Fingerabdruck**.
- Digitale **Zertifikate** fassen Informationen zur Inhaberin, zum öffentlichen Schlüssel und zu den Beglaubigungs-Signaturen zusammen. Zertifikate enthalten Angaben zum Aussteller des Zertifikats, für wen es ausgestellt wurde und wie lange es gültig ist.

Beim Public-Key-Verfahren gibt es also vor allem zwei Fragen zu beantworten:

1. Wie stellt man sicher, dass der Schlüssel bzw. das Zertifikat und die Inhaberin zusammengehören?
2. Welche Möglichkeiten zum Verteilen und Verwalten der Zertifikate bzw. der öffentlichen Schlüssel gibt es?

Die nächsten Abschnitte stellen mögliche Antworten und Lösungsansätze vor, die sich insbesondere für große Umgebungen und Organisationen eignen.

2 Vertrauensmodelle

Die Zugehörigkeit öffentlicher Schlüssel bzw. der digitalen Zertifikate muss zweifelsfrei überprüfbar sein – genau hier setzt die Public Key Infrastructure (PKI) an. Eine PKI stellt Dienste bereit, die das Überprüfen und Verteilen von digitalen Zertifikaten übernehmen. Außerdem sorgt eine PKI für einen sicheren Austausch der Zertifikate zwischen Sendern und Empfängern. Wenn mehrere solcher PKIs vertrauenswürdig miteinander kommunizieren sollen, dann sind Vertrauensmodelle erforderlich.

Es gibt unterschiedliche Ansätze für Vertrauensmodelle, die sich im Wesentlichen in der Rolle der Beglaubigungsinstanz unterscheiden. Diese Certification Authority (CA) ist eine Person oder Rolle mit der Berechtigung, Fingerabdrücke der öffentlichen Schlüssel zu prüfen und zu bestätigen sowie Zertifikate auszustellen.

2.1 Verteiltes Vertrauen

In einem Netz des Vertrauens versichern sich Kommunikationspartner gegenseitig, dass ein Zertifikat echt ist. Dazu tauschen sie ihre Personalien und die Fingerabdrücke der Schlüssel aus. Signiert Benutzerin A den Schlüssel von Benutzerin B (nachdem A die Identität von B überprüft hat), spricht Benutzerin A der Schlüsselsignatur von B das Vertrauen aus. Damit kann Benutzerin A auch allen anderen Schlüsseln vertrauen, die B signiert hat.

In diesem verteilten Szenario tauscht jede Certification Authority ihre öffentlichen Schlüssel selbstständig mit allen anderen CAs aus. Der Vertrauensgrad steigt mit der Anzahl der Personen, die einen öffentlichen Schlüssel signiert haben. Viele Benutzer treten in diesem **Web of Trust** also als Vertrauens-Instanzen auf. Der Prozess der Zertifizierung ist mit einem gewissen Aufwand verbunden und setzt in der Regel ein persönliches Treffen voraus. Dieses Vertrauensmodell skaliert nicht und wird daher in größeren Organisationen und Umgebungen schnell unpraktisch.

2.2 Hierarchisches Vertrauen

Da das Ausdrucken und Vergleichen von Fingerabdrücken unpraktisch und aufwändig ist, gibt eine Alternative, die eine weitere Partei ins Spiel bringt: Im hierarchischen Vertrauensmodell existiert innerhalb der Public Key Infrastructure eine übergeordnete Certification Authority, welche die Wurzelzertifikate der untergeordneten CAs aufnimmt. Das heißt, dass alle anderen Instanzen, die zu dieser PKI gehören, den Wurzelzertifikaten vertrauen. Benutzer und auch andere CAs vertrauen der Wurzel-CA (auch Root-CA genannt).

Das Vertrauen basiert also nicht auf einzelnen Schlüsseln der Benutzer, sondern auf den öffentlichen Schlüsseln und den Signaturen der angeschlossenen CAs. Diese sind hierarchisch angeordnet und bilden eine Vertrauenskette, eine **Chain of Trust**.

Hinweis

In größeren Organisationen ist das hierarchische Vertrauensmodell die bevorzugte Methode. In Verbindung mit einem Identitäts-Management-System (IdM) lassen sich viele Vorgänge automatisieren (siehe Abschnitt 4.5), z. B. die Beglaubigung von Benutzer-Zertifikaten.

Das hierarchische Vertrauensmodell kommt bei klassischen PKIs zum Einsatz, etwa bei S/MIME und den dort verwendeten X.509-Zertifikaten.

2.3 Flexibles Vertrauensmodell bei OpenPGP

Auch mit OpenPGP lässt sich ein hierarchisches Vertrauensmodell abbilden. Es hat gegenüber der klassischen PKI den Vorteil, dass es wesentlich flexibler ist und Beglaubigungsmanager selbst entscheiden können, welcher Autorität sie für welche Domains vertrauen wollen.

- Das Wurzelzertifikat heißt **Trusted Key**.
- Die „Zwischenzertifikate" heißen **Trusted Introducer**.

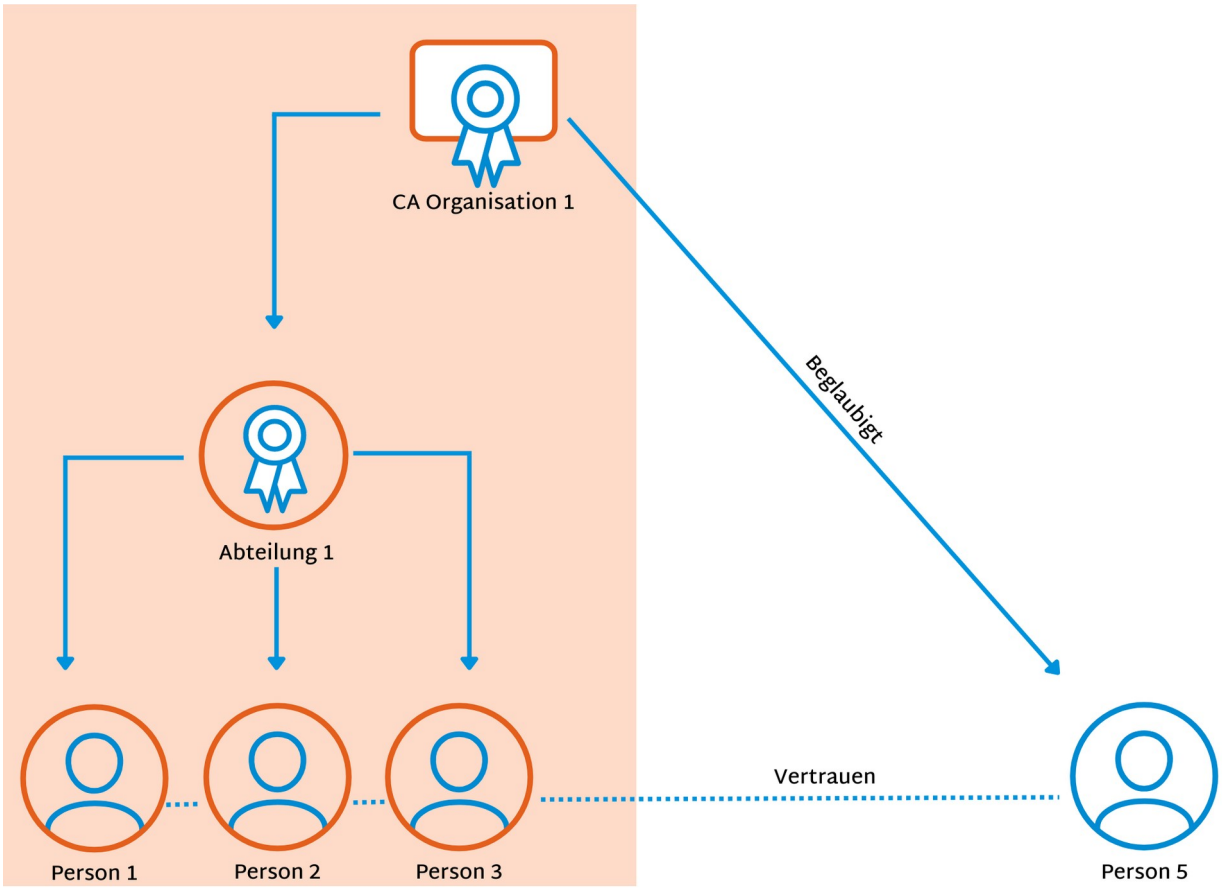
a) Trusted Key

Der Trusted Key ist der Vertrauensanker im Beglaubigungsmanagement mit GnuPG VS-Desktop®. Dem Trusted Key wird genauso vertraut wie dem eigenen Schlüssel (ultimatives Vertrauen). Das kann er jeden öffentlichen Schlüssel „wirksam" beglaubigen, egal, ob dieser zur eigenen oder einer fremden Domain gehört.

In einer Organisation übernimmt entweder eine Person oder eine Gruppe von Personen das Beglaubigungsmanagement und damit die Rolle der Certificate Authority. Sie erstellt einen Trusted Key in Form eines OpenPGP-Schlüsselpaares und bewahrt dessen geheimen Schlüssel und das Passwort VS-NfD-konform auf. Eine sichere Möglichkeit zur Aufbewahrung bieten Smartcards.

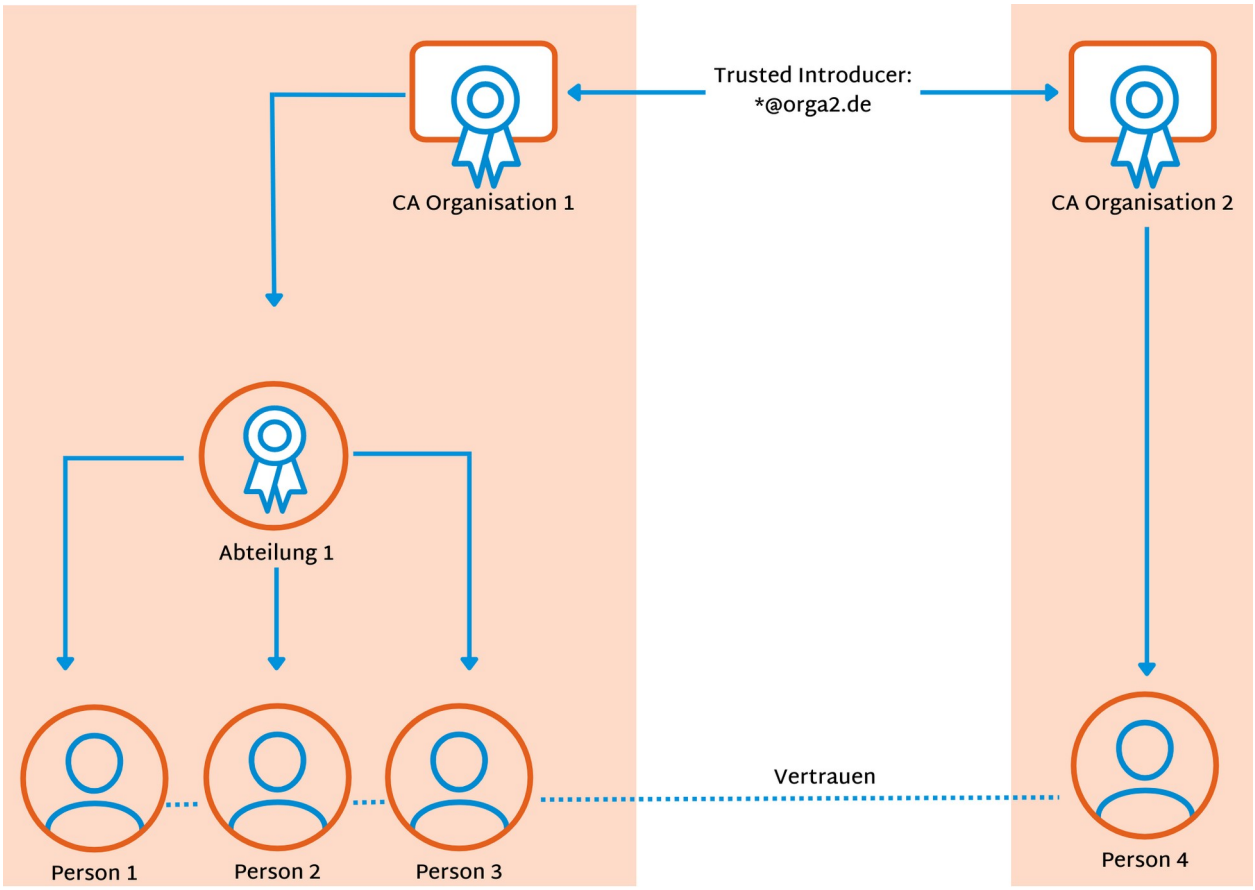
In einem hierarchischen Vertrauensmodell mit einem Trusted Key ist es möglich, das Vertrauen über eine Gültigkeitsdauer der Beglaubigungen zentral zu verwalten. So kann beispielsweise ein Ablaufdatum festgelegt werden, das den Richtlinien der Organisation entspricht. Es ist ebenfalls möglich, die Beglaubigung des Zertifikats zu widerrufen, etwa wenn eine Mitarbeiterin ausscheidet, ein Benutzer einen Schlüssel verloren hat oder es den begründeten Verdacht gibt, dass ein Schlüssel kompromittiert wurde.

Ein manuelles Eingreifen mit einem Revocation Key (Widerrufsschlüssel) oder einem Designated Revoker (autorisierte Person, die bereits veröffentlichte öffentliche Schlüssel ungültig macht), ist ebenfalls möglich.



b) Trusted Introducer

Ergänzend zum Trusted Key gibt es den Trusted Introducer (vertrauenswürdiger Vermittler). Einem solchen Zertifikat wird das volle Vertrauen ausschließlich für eine bestimmte Domain ausgesprochen. Das ist beispielsweise dann sinnvoll, wenn man einem Trusted Key einer anderen Organisation nur für Beglaubigungen innerhalb deren Domain vertrauen möchte. Ein kompromittierter Schlüssel einer externen Organisation kann dann keine Zertifikate für die eigene Organisation ausstellen.



GnuPG VS-Desktop® bietet damit einen wesentlichen Sicherheitsvorteil gegenüber S/MIME – dort können CAs meist für jede Domain alles beglaubigen, da die Herausgeber die „Zuständigkeit" ihrer Zertifikate oft nicht einschränken.

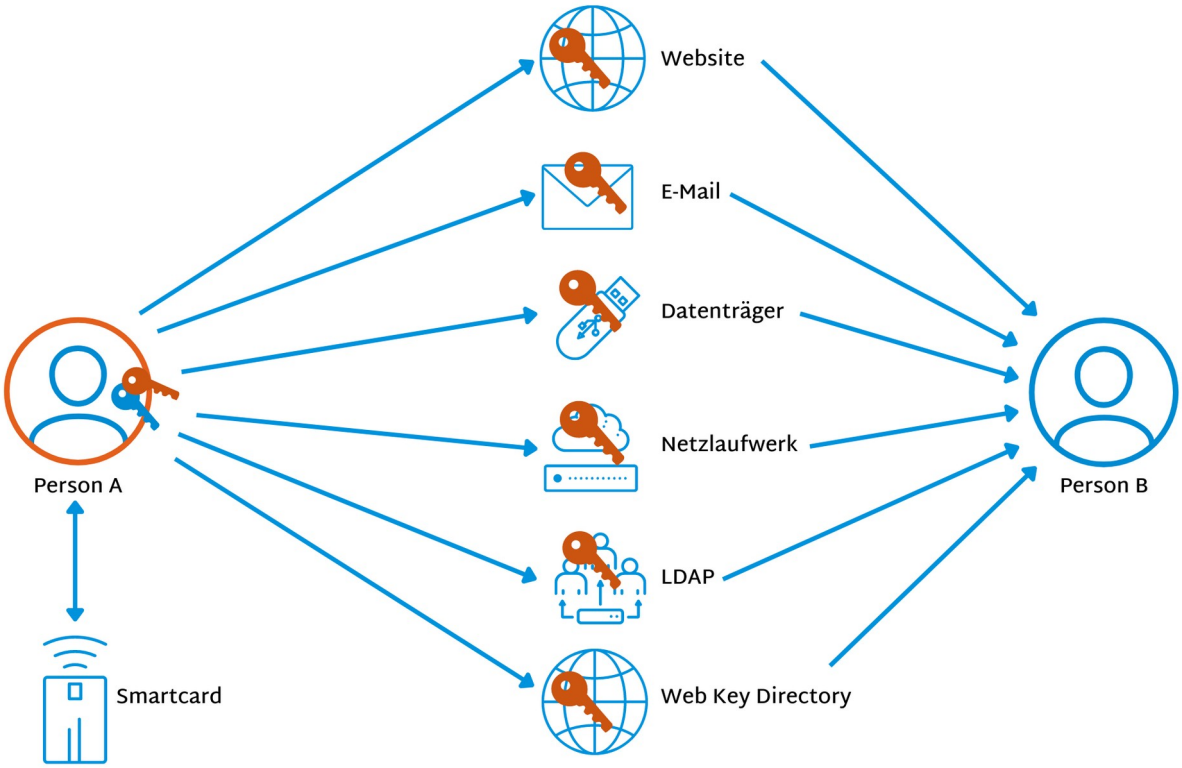
3 Zertifikate verteilen

Es gibt verschiedene technische Möglichkeiten, die vom Trusted Key oder die vom Trusted Introducer beglaubigten Zertifikate an Benutzer von GnuPG VS-Desktop® zu verteilen. Zur Erinnerung: Die öffentlichen Schlüssel müssen nicht besonders geschützt oder geheim gehalten werden. Die Integrität und Korrektheit der Zertifikate wird durch die Beglaubigungen abgesichert.

Wenn die Verteilung nicht automatisiert laufen soll, dann reicht es aus, die Zertifikate auf einer Website zu veröffentlichen, auf einem Netzlaufwerk abzulegen oder sie per Datenträger oder per E-Mail zu verteilen. Anwenderinnen können so ohne spezielle Infrastruktur untereinander Zertifikate austauschen.

In Organisationen sind vor allem folgende Alternativen interessant:

- Interner Keyserver (LDAP, AD, LDS)
- Web Key Directory (WKD), Web Key Service (WKS)
- Kleopatra-Gruppen



3.1 Interner Keyserver (AD, LDS, LDAP)

In Organisationen ist es sinnvoll, einen internen Keyserver einzurichten und zu betreiben. Dieser übernimmt dann die Verwaltung von OpenPGP- und X.509-Zertifikaten. Dazu bietet sich ein Verzeichnisdienst an

- Active Directory Domain Services (AD DS) bzw. Active Directory Lightweight Directory Services (AD LDS) unter Windows
- OpenLDAP unter Linux

Unter Windows empfehlen wir, einen Keyserver mit LDS einzurichten. Er ist schlanker als Active Directory und kann entweder unabhängig betrieben oder in einen bestehenden AD-Verzeichnisdienst integriert werden. Der Vorteil eines eigenen LDS-Servers für die Speicherung von GnuPG-Schlüsseln ist, dass ein vorhandenes Active Directory nicht um ein neues Schema erweitert werden muss. Unter Linux ist OpenLDAP der empfohlene Verzeichnisdienst.

Das Setup der jeweiligen Verzeichnisdienste erfordert die Installation eines eigenen Schemas. Wir haben das Ende der 1990er-Jahre entwickelte Schema erweitert und zusätzliche Attribute hinzugefügt. Diese ermöglichen es unter anderem, Zertifikate anhand der Fingerabdrücke zu suchen, Informationen zu Unterschlüsseln und zu Mailadressen zu speichern.

Hinweis

Anleitungen zum Einrichten von LDAP- und LDS-Keyservern stellen wir gerne als eigene Handbücher zur Verfügung. Bitte kontaktieren Sie uns per E-Mail: info@gnupg.com

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

Ein Web Key Directory (WKD) ermöglicht es auch externen Kommunikationspartnern, auf die Zertifikate der eigenen Organisation zuzugreifen. Es stellt aktuelle öffentliche Schlüssel für bestimmte E-Mail-Adressen über HTTPS bereit. Das WKD ist quasi ein öffentliches Telefonbuch für OpenPGP-Zertifikate der eigenen Organisation bzw. Domain.

Um ein Web Key Directory für die eigene Organisation einzurichten, ist lediglich ein Webserver für die Domain erforderlich. Für größere Organisation empfehlen wir, einen kompletten Web Key Service (WKS) einzurichten, um die Veröffentlichung des Web Key Directory zu automatisieren.

3.3 Kleopatra-Gruppen

Der Zertifikatsmanager Kleopatra (siehe Abschnitt 4) unterstützt Gruppen, um regelmäßig dieselben Kommunikationspartner zu adressieren. Kleopatra-Gruppen sind Zertifikatsdateien (S/MIME oder OpenPGP) mit zusätzlichen Informationen. Benutzerinnen können Nachrichten für alle Mitglieder einer Gruppe gleichzeitig verschlüsseln, indem sie die Gruppe als Empfänger auswählen.

Ein typischer Anwendungsfall: Eine Verantwortliche sammelt zu Beginn eines Projektes die Zertifikate aller Teilnehmerinnen ein, kümmert sich dann um die Beglaubigung der Zertifikate bzw. führt diese selbst durch. Danach verteilt sie die Zertifikate über einen beliebigen Kanal (z. B. via E-Mail) an alle Projektteilnehmer.

Hinweis

Kleopatra-Gruppen können auch in Outlook genutzt werden, sofern der Name der Gruppe eine Mailverteiler-Adresse ist.

4 GnuPG VS-Desktop®: Best Practices

Das Open-Source-Softwarepaket GnuPG VS-Desktop® besteht aus den folgenden, voneinander unabhängig entwickelten Programmen:

- **GnuPG**: der Kryptokern (im jeweils vom BSI zugelassenen Konstruktionsstand)
- **Kleopatra**: Schlüssel- und Zertifikatsmanager
- **GpgOL**: Plugin für Microsoft Outlook zur Verschlüsselung von E-Mails (Unterstützung für IMAP/SMTP und MS Exchange)
- **GpgEX**: Plugin für den Windows Explorer (Dateiverschlüsselung)

Im Jahr 2019 hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) GnuPG VS-Desktop® für die Übertragung von vertraulichen Dokumenten der Geheimhaltungsstufe „Verschlusssache – nur für den Dienstgebrauch" (VS-NfD) zugelassen. Diese Zulassung erstreckt sich außerdem auf die entsprechenden internationalen Sicherheitslevels EU RESTRICTED und NATO RESTRICTED.

GnuPG VS-Desktop® und seine Komponenten bewältigen die angesprochenen Herausforderungen beim Herstellen von Vertrauen und beim Verteilen der Zertifikate.

4.1 Trusted Key anlegen

Die Beglaubigungsmanagerin erzeugt einen Trusted Key in Form eines OpenPGP-Schlüsselpaares, beispielsweise mit dem Programm Kleopatra. Der Trusted Key sollte den Namen der Organisation enthalten, damit er sich leicht zuordnen lässt. Eine Mailadresse benötigt dieser Schlüssel nicht. Der dazugehörige Fingerabdruck gehört bei allen Installationen der eigenen Organisation in die Windows-Registry bzw. in die Datei *gpg.conf* auf Linux-Systemen.

Hinweis

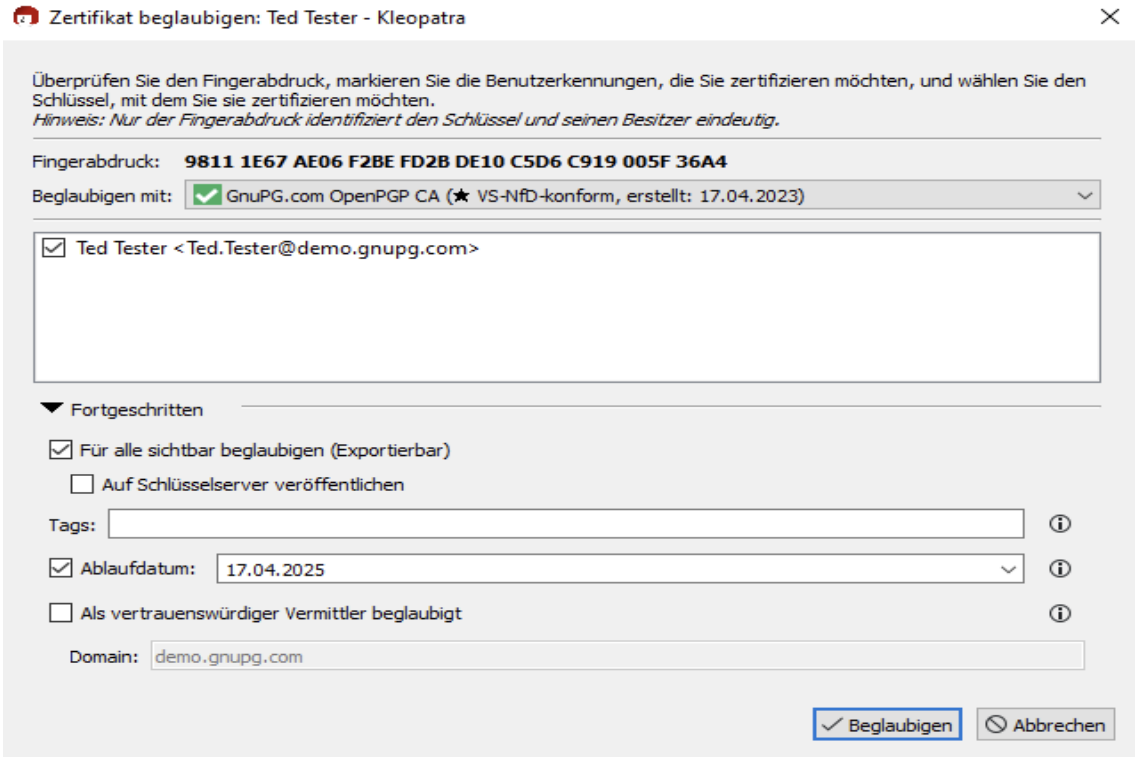
In der Standardkonfiguration unterstützt GnuPG VS-Desktop® bis zu fünf Trusted Keys. Sollten Sie mehr als fünf Trusted Keys benötigen, stellen wir auf Anfrage eine angepasste Version von GnuPG VS-Desktop® zur Verfügung.

Die Verteilung des öffentlichen Schlüssels erfolgt über einen der in Abschnitt 3 beschriebenen Wege.

4.2 Beglaubigungen erstellen (exportierbar)

Um einen Schlüssel einer neu hinzugekommenen Mitarbeiterin mit dem Trusted Key für alle sichtbar zu beglaubigen, exportiert die Mitarbeiterin den Public Key und übermittelt ihn an die Beglaubigungsmanagerin. Sie führt dazu in Kleopatra die folgenden Schritte aus:

1. Rechtsklick auf den zu bearbeitenden Schlüssel in der Zertifikatsliste und *Beglaubigen* aus dem Menü auswählen.
2. Vergewissern, dass der öffentliche Schlüssel zur richtigen Person gehört: Fingerabdruck über eine zweite Quelle vergleichen, beispielsweise per Telefon.
3. Im Drop-down-Menü *Beglaubigen mit* den Trusted Key auswählen; im Beispiel heißt dieser *GnuPG.com OpenPGP CA*.
4. Menü *Fortgeschritten* unten im Dialog ausklappen und Checkbox *Für alle sichtbar beglaubigen (Exportierbar)* aktivieren.
5. Gibt es einen internen Schlüsselserver, kann sie zusätzlich die Checkbox *Auf Schlüsselserver veröffentlichen* auswählen. Ein nachträgliches Veröffentlichen ist ebenfalls möglich.
6. Einstellen des Ablaufdatums; üblich sind drei Jahre.
7. Auf *Beglaubigen* klicken, das Passwort des Trusted Key eingeben und über *OK* bestätigen.

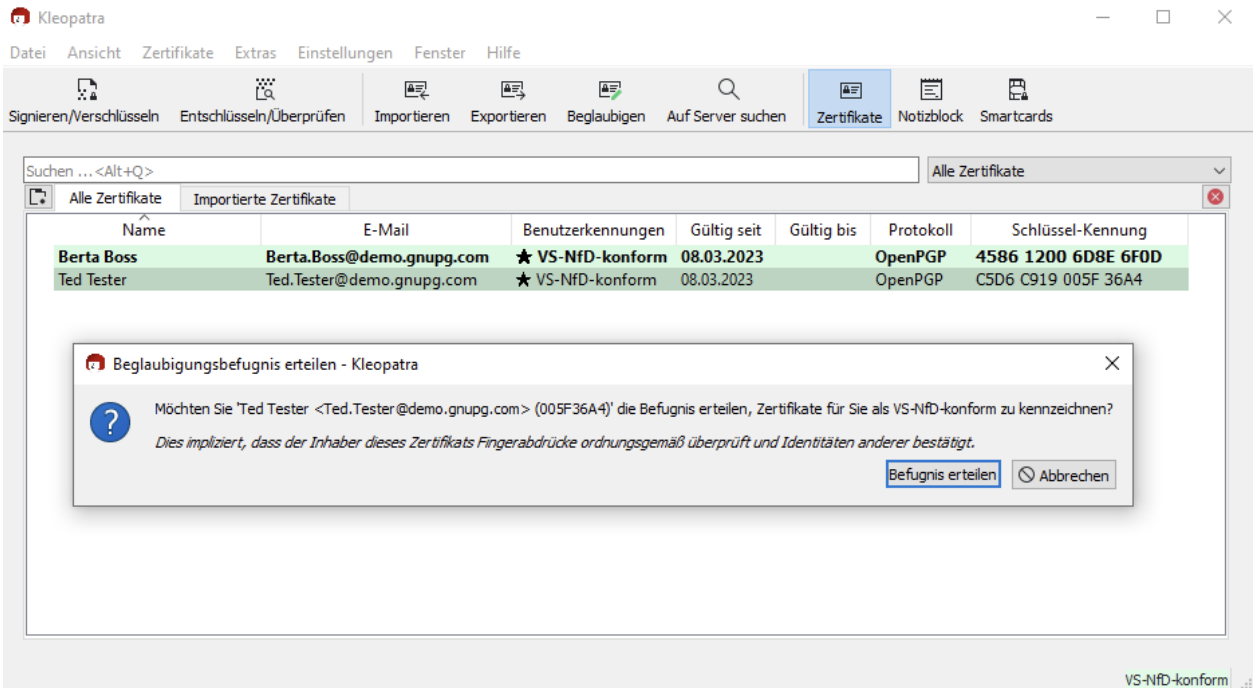


4.3 Trusted Introducer einführen

Soll ein Schlüssel als Trusted Introducer dienen, also zur Beglaubigung aller Schlüssel einer bestimmten Domain bevollmächtigt sein, sieht die Einrichtung genauso aus wie im letzten Abschnitt beschrieben. Zusätzlich muss die Checkbox *Als vertrauenswürdiger Vermittler beglaubigt* aktiviert werden; ins Feld darunter gehört der Domain-Name.

4.4 Beglaubigungsmanagement durch Anwender

In der Standardkonfiguration können Benutzerinnen auch ein Zertifikat als Trusted Introducer beglaubigen oder einem beliebigen Zertifikat Beglaubigungsbefugnis erteilen. Dazu klicken sie mit der rechten Maustaste auf ein Zertifikat und wählen den Menüeintrag *Beglaubigungsbefugnis ändern*. Im sich öffnenden Dialogfenster bestätigen sie dies über die Schaltfläche *Befugnis erteilen*.



Hinweis

Ein Schlüssel mit Beglaubigungsbefugnis entspricht in der Praxis einem Trusted Key.

Um zu verhindern, dass Benutzer Zertifikate selbst beglaubigen können, kann Kleopatra entsprechend konfiguriert werden. Dazu ist ein Eingriff in die Registry erforderlich; die Aktion *certificates_change_owner_trust* muss auf *false* gesetzt werden. Sofern alle Beglaubigungen ausschließlich zentral verwaltet werden, kön-

nen Beglaubigungen durch Anwender generell unterbunden werden. Dazu ist die Aktion *certificates_certify_certificate* auf *false* zu setzen.

4.5 Möglichkeiten zur Automatisierung

In größeren Organisationen empfiehlt es sich, Vorgänge zu automatisieren. Dazu gibt es mehrere Möglichkeiten:

- **GnuPG actium**: Die Open-Source-Software wird von der g10 Code GmbH entwickelt und übernimmt die automatisierte Beglaubigung von Zertifikaten aus dem Verzeichnisdienst einer Organisation. Benutzer*innen generieren ihr eigenes Zertifikat und übermitteln es per Knopfdruck zum Verzeichnisdienst. actium lädt neue Zertifikate von dort herunter und verschickt eine verschlüsselte Mail mit einem Bestätigungslink. Nur wenn jemand Zugriff auf die E-Mail und das erstellte Zertifikat hat, kann er oder sie den Bestätigungslink öffnen. actium beglaubigt danach das Zertifikat und übermittelt es wieder zum Verzeichnisdienst.
- **Identitätsmanagement** von unserem Partner Rohde & Schwarz: Der R&S®Trusted Objects Manager (TOM) kombiniert mit dem R&S®Trusted Identity Manager (TIM) automatisieren das Beglaubigungssystem. Da der TOM über eine Smartcard bereits eine Identitätsbeziehung hat, ist eine VS-NfD-konforme Identifikation mit einem Schlüssel möglich. Daher kann der TOM automatisch Zertifikate beglaubigen und per Verzeichnisdienst bereitstellen.

5 Zusammenfassung

Eine sichere und skalierende Zertifikatsverwaltung ist für viele Organisationen unverzichtbar, insbesondere für Behörden und Institutionen mit VS-NfD oder EU-Datenschutz-Grundverordnung (DSGVO). GnuPG VS-Desktop® ist eine bewährte Open-Source-Lösung, die nicht nur den höchsten Sicherheitsstandards entspricht, sondern auch die Automatisierung von Prozessen ermöglicht. Die Software unterstützt verteilte und hierarchische Vertrauensmodelle und bietet flexible Ansätze, um das Vertrauen in Schlüssel und Zertifikate zu etablieren und zu verwalten.

Die verschiedenen Verteilungsmethoden, von internen Keyservern bis hin zu Web Key Directories, ermöglichen es Organisationen, ihre Zertifikate effizient und sicher zu verteilen. Auch in puncto Automatisierung ist GnuPG VS-Desktop® führend. Die Integration von Identitätsmanagement-Systemen und automatisierten Beglaubigungsprozessen wird Organisationen helfen, ihren Sicherheitsanforderungen gerecht zu werden und gleichzeitig den Verwaltungsaufwand zu reduzieren.

6 Über GnuPG

GnuPG steht für Unabhängigkeit, Souveränität und den Erhalt der digitalen Privatsphäre. Seit über 25 Jahren entsteht die Kryptosoftware in einem offenen und transparenten Entwicklungsprozess: Der GnuPG-Verschlüsselungscode bietet seit 1997 einen unerreichten Schutz vor Nachrichtenüberwachung und unberechtigter Datenspeicherung durch Dritte.

Als Komplettlösung ver- und entschlüsselt GnuPG VS-Desktop® E-Mails, Nachrichten, Dokumente usw. unter Windows und Linux. Seit 2019 ist die Software vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Übertragung von vertraulichen Dokumenten der Geheimhaltungsstufe „Verschlusssache – nur für den Dienstgebrauch" (VS-NfD) zugelassen.

Der Hersteller g10 Code GmbH bietet individuelle Service-, Schulungs- und Support-Leistungen für Administratoren und IT-Sicherheitsbeauftragte an.

https://gnupg.com/