

Beglaubigungsmanagement mit GnuPG VS-Desktop®

Empfehlungen für einen skalierenden Aufbau

Zielgruppe Administratorinnen und Sicherheitsbeauftragte

Dieses Dokument gilt entsprechend für GnuPG Desktop®

Version GnuPG VS-Desktop® 3.x

Dokumentversion: 1.0

Hersteller / Vertreiber

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

Inhaltsverzeichnis

1	Einleitung.....	3
2	Begriffsdefinitionen.....	4
3	Konzept Vertrauensmodell.....	6
3.1	Trusted Key.....	6
3.1.1	Gültigkeitsdauer von Beglaubigungen.....	7
3.2	Trusted Introducer.....	7
4	Schlüsselverteilung.....	8
4.1	LDAP / AD / LDS.....	8
4.2	WKD.....	8
4.3	Zertifikatsdateien.....	9
4.4	Kleopatra Gruppen.....	9
5	Anleitungen.....	10
5.1	Trusted Key anlegen.....	10
5.2	Beglaubigungen erstellen (exportierbar).....	10
5.3	Beglaubigung eines Schlüssels als Trusted Introducer.....	11
6	Automatisierungsmöglichkeiten Beglaubigung.....	12
6.1	Rohde & Schwarz Identitätsmanagement.....	12
6.1.1	Interne Zertifikate.....	12
6.1.2	Externe Zertifikate.....	12
6.2	Actium.....	12
7	Beglaubigungsmanagement durch die Anwender.....	13

1 Einleitung

Wir empfehlen Institutionen, Behörden und größere Unternehmen ein Beglaubigungsmanagement für eine skalierende, VS-NfD konforme Zertifikatsverwaltung zu etablieren. Ein Beglaubigungsmanagement hilft den Prozess zu automatisieren und sicherer zu gestalten.

In diesem Dokument werden zunächst die Konzepte des Beglaubigungsmanagements beschrieben und dann eine Umsetzungsmöglichkeit in der Praxis beispielhaft abgebildet.

Dabei wird als grafische Benutzeroberfläche der Schlüssel- und Zertifikatsmanager Kleopatra verwendet. Alles Beschriebene – und vieles mehr – ist ebenfalls auf der Kommandozeile möglich und kann sowohl gescriptet, als auch automatisiert werden.

Anwender in einer Organisation ohne institutionelles Beglaubigungsmanagement müssen die Schlüssel aller ihrer Kommunikationspartner selber beglaubigen bzw. ein Beglaubigungsmanagement auf Anwenderebene betreiben. Siehe dazu – und wie Sie dies im Falle eines funktionierenden institutionellen Beglaubigungsmanagements unterbinden können – Kapitel 7.

2 Begriffsdefinitionen

In der asymmetrischen bzw. Public Key Kryptografie werden einige Begriffe mehrdeutig verwendet. So kann mit „Schlüssel“ ein OpenPGP Schlüsselpaar, ein öffentlicher oder ein privater (=geheimer) Schlüssel gemeint sein. In jedem Fall geht es um kryptografische Parameter.

OpenPGP Schlüsselpaar: Ein geheimer Schlüssel zusammen mit dem dazugehörenden öffentlichen Schlüssel.

Öffentlicher Schlüssel (engl. Public Key): Der Teil des Schlüsselpaares, der für die Verschlüsselung von Nachrichten und Überprüfung von Signaturen benötigt wird. Dieser wird i.d.R. veröffentlicht.

Privater / Geheimer Schlüssel (engl. Private Key oder Secret Key): Der Teil des Schlüsselpaares, der für das Entschlüsseln und Signieren von Nachrichten benötigt wird. Dieser ist unbedingt geheim zu halten.

Zertifikat: Ein öffentlicher Schlüssel mit zusätzlichen Informationen (Name und/oder Mailadresse, Gültigkeit). Umgangssprachlich oft auch „Public-Key“ oder „öffentlicher Schlüssel“ genannt.

Fingerabdruck: Die eindeutige und unveränderliche Prüfsumme über den öffentlichen Schlüssel.

Beglaubigung: Eine im Zertifikat enthaltene Signatur, die dessen Informationen als geprüft kennzeichnet. Sie bestätigt technisch die für VS-NfD notwendige Prüfung der Authentizität des öffentlichen Schlüssels anhand des Fingerabdrucks.

Beglaubigungsinstanz bzw. **Certification Authority (CA):** Eine Person oder Rolle, die berechtigt ist, stellvertretend für Andere eine Fingerabdruck-Prüfung vorzunehmen.

OpenPGP: Ein weit verbreiteter Standard für Verschlüsselung und Signatur von Daten und E-Mails. Verwendet OpenPGP Zertifikate bzw. Schlüssel.

S/MIME: Ein weit verbreiteter Standard für Verschlüsselung und Signatur von überwiegend E-Mails. Verwendet X.509 Zertifikate.

Wurzelzertifikat bzw. **Root-Certificate:** Ein Vertrauensanker höchster Ebene beim S/MIME Standard, das Zertifikat einer Root-CA.

Zwischenzertifikat: Ein vom Wurzelzertifikat beglaubigtes X.509 Zertifikat, das als Vertrauensanker dient.

Trusted Key: Vertrauensanker höchster Ebene beim Beglaubigungsmanagement mit GnuPG VS-Desktop®, entspricht einem Wurzelzertifikat.

Trusted Introducer: Vertrauensanker beim Beglaubigungsmanagement mit GnuPG VS-Desktop®, entspricht einem Zwischenzertifikat.

VS-NfD konform: Entspricht der deutschen Zulassung zur Verschlüsselung von VS-NfD eingestuftem Daten. Bezieht sich je nach Kontext auf die Konformität der Software oder der verwendeten Zertifikate. *VS-NfD* entspricht dem Sicherheitslevel *EU Restricted* und *NATO Restricted*.

3 Konzept Vertrauensmodell

Recht bekannt ist das hierarchische Vertrauensmanagement einer klassischen PKI (Public Key Infrastructure), wie es bei S/MIME bzw. X.509 Zertifikaten üblich ist.

Auch mit OpenPGP lässt sich ein hierarchisches Vertrauensmodell abbilden, welches gegenüber der klassischen PKI den Vorteil hat, dass es wesentlich flexibler ist und Beglaubigungsmanagerinnen selber entscheiden können, welcher Autorität sie für welche Domains vertrauen wollen. Das Wurzelzertifikat wird dabei „Trusted Key“ genannt und die Zwischenzertifikate „Trusted Introducer“. Diese verhalten sich aber etwas anders als ihre S/MIME-Entsprechungen.

Das in diesem Kapitel beschriebene Konzept lässt sich für große Organisationen sehr gut in Verbindung mit einem Identitätsmanagementsystem einsetzen. Dieses unterstützt oder automatisiert die Beglaubigung von Nutzer-Zertifikaten, siehe Kapitel 6. Auch die Integration von Smartcards ist hierbei möglich.

3.1 Trusted Key

Ein Trusted Key ist der Vertrauensanker beim Beglaubigungsmanagement mit GnuPG VS-Desktop®. Ihm wird genau so vertraut wie dem eigenen Schlüssel (= ultimates Vertrauen). Er kann also jeden öffentlichen Schlüssel „wirksam“ beglaubigen, egal ob von der eigenen oder einer fremden Domain. Vom Trusted Key beglaubigte Zertifikate werden in der Zertifikatsliste der Anwender in Kleopatra ohne deren Zutun als VS-NfD konform angezeigt.

Ein OpenPGP Schlüssel wird zum Trusted Key, wenn er auf einem Windows-System in der Registry¹ eingetragen wird. Auf einem Linux System wird er in der Datei gpg.conf gesetzt.

Typischerweise übernimmt eine Person (oder Gruppe von Personen) in einer Organisation das Beglaubigungsmanagement für selbige, sie hat die Rolle CA inne. Sie legt einen Trusted Key in Form eines OpenPGP Schlüsselpaares an und bewahrt dessen geheimen Schlüssel und Passwort VS-NfD konform auf. Wir empfehlen die Speicherung des geheimen Schlüssels auf einer Smartcard (siehe hierzu ggf. die Dokumentation „Smartcards einrichten mit GnuPG VS-Desktop®“).

Es können mehrere (in der Standardkonfiguration bis zu 5) Trusted Keys verwendet werden, so dass jeder Beglaubigungsmanager über einen eigenen Trusted Key verfügt.

Für mehr Details siehe Kapitel 5.

¹ Siehe: <https://gnupg.com/vsd/registry-settings.de.html>

3.1.1 Gültigkeitsdauer von Beglaubigungen

Ein hierarchischen Vertrauensmodells mit einem Trusted Key ermöglicht es auch, dass das Vertrauen mittels Gültigkeitsdauer der Beglaubigungen des Trusted Keys zentral verwaltet werden kann.

Es kann z.B. ein Ablaufdatum entsprechend der Organisationsrichtlinien festgelegt oder bei Ausscheiden eines Mitarbeiters oder einem verlorenen Schlüssel die Beglaubigung des Zertifikats ohne Beihilfe des nominellen Nutzers widerrufen werden.

Alternativ können Revokation Keys zentral hinterlegt werden oder man kann neuen Schlüsseln einen Designated Revoker hinzufügen.

3.2 Trusted Introducer

Ergänzend zum *Trusted Key* gibt es den *Trusted Introducer* (= *Vertrauenswürdiger Vermittler*). Einem solchen Zertifikat wird das volle Vertrauen nur für eine bestimmte Domain ausgesprochen. Ansonsten haben sie die gleichen Eigenschaften wie Trusted Keys.

Ein OpenPGP Schlüssel wird zum Trusted Introducer einer Domain, indem man ihm bei der Beglaubigung im erweiterten Menü (unter „Fortgeschritten“) für diese Domain als vertrauenswürdigen Vermittler einträgt. Siehe 5.3.

Typischerweise wird man dies nutzen, um einem Trusted Key einer anderen Organisation nur für Beglaubigungen innerhalb deren Domain zu vertrauen. So kann ein kompromittierter Schlüssel einer externen Organisation keine Zertifikate für die eigene Organisation ausstellen. Dies bietet einen Sicherheitsvorteil gegenüber der Praxis bei S/MIME, wo CAs meist für jede Domain alles beglaubigen können, da die Herausgeber die „Zuständigkeit“ ihrer Zertifikate oft nicht einschränken.

4 Schlüsselverteilung

Es gibt verschiedene Möglichkeiten, die vom Trusted Key oder Trusted Introducer beglaubigten Zertifikate an die Nutzer von GnuPG VS-Desktop® zu verteilen:

- LDAP / ActiveDirectory / LDS (intern)
- WKD – WebKeyDirectory (in der Regel extern)
- Zertifikatsdateien (.asc, .gpg)
- Kleopatra Gruppen-Dateien (.kgrp)

Hinweis: Der Übertragungsweg kann dabei vollkommen unsicher sein. Die Integrität und Korrektheit der Zertifikate wird durch die Beglaubigungen abgesichert.

4.1 LDAP / AD / LDS

Innerhalb einer Organisation ist es sinnvoll, einen internen Keyserver einzurichten. Dafür empfehlen wir unter Windows LDS (Lightweight Directory Services) und unter Linux OpenLDAP.

Aufsetzen und Konfiguration ist in der Dokumentation „How to install an LDS for use with GnuPG VS-Desktop®“ beschrieben. Eine entsprechende Anleitung für OpenLDAP unter Linux kann ebenfalls bei g10 Code angefragt werden.

Um mit Kleopatra ein Zertifikat im LDS / LDAP zu veröffentlichen oder nach Hinzufügen einer exportierbaren Beglaubigung zu aktualisieren, muss man nach erfolgreicher Konfiguration nur darauf Rechtsklicken→[Auf Server veröffentlichen].

Kleopatra und das Outlook Plugin (GpgOL) finden im LDS / LDAP bei Angabe einer Mailadresse als Empfänger automatisch die zugehörigen Zertifikate. Alternativ können sie in Kleopatra über „Suchen“ gefunden werden.

4.2 WKD

Damit auch externe Kommunikationspartnerinnen auf die Zertifikate der eigenen Organisation zugreifen können, kann ein WebKeyDirectory (WKD) aufgesetzt werden.² Dies ist quasi das öffentliche Telefonbuch für OpenPGP Zertifikate der eigenen Organisation bzw. Domain.

Ein WKD kann aus einem vorhandenen LDS gespiegelt werden, so dass die Pflege der Daten erleichtert wird. Eine Anleitung dazu finden Sie hier: <https://gnupg.com/kb/mirror-ldap-to-wkd.html>

² Siehe: <https://wiki.gnupg.org/WKD>

Damit ihre Kommunikationspartnerinnen das Trusted Introducer Feature nutzen können, sollten alle im WKD abgelegten Schlüssel von einem Trusted Key Ihrer Organisation *exportierbar* beglaubigt sein (siehe 5.2). Dessen Zertifikat sollten Sie gesondert bereitstellen und Ihren Kommunikationspartnern mitteilen, wie die Fingerabdruck Prüfung dafür erfolgen kann.

4.3 Zertifikatsdateien

Wenn Sie die Verteilung nicht automatisieren möchten, können Sie die Zertifikate (bzw. öffentliche Schlüssel) auch einzeln, in Form von Zertifikatsdateien oder als Kleopatra Gruppen (siehe 4.4) übermitteln. Anwender können so ohne spezielle Infrastruktur untereinander Zertifikate austauschen, indem sie sie z.B. per Mail verschicken oder in einem geteilten Netzwerk-Laufwerk ablegen.

Für die Erstellung einer Zertifikatsdatei markiert man beliebig viele Zertifikate und nutzt dann die „Exportieren“ Funktion von Kleopatra.

4.4 Kleopatra Gruppen

Bei Kleopatra Gruppen handelt es sich um Zertifikatsdateien, die zusätzliche Gruppeninformationen enthalten.

Für Kleopatra Gruppen gibt es eine eigene Anleitung (siehe Hilfe → Gruppenkonfiguration) die sowohl die Erstellung als auch die Verwendung beschreibt.

Sie haben den Vorteil, dass man mit ihnen für alle Mitglieder einer Gruppe gleichzeitig verschlüsseln kann, indem man nur die Gruppe als Empfänger auswählt. Kleopatra Gruppen können auch in Outlook genutzt werden, sofern der Name eine Verteiler-Mailadresse ist.

Ein typischer Anwendungsfall ist, dass eine Verantwortliche zu Beginn eines Projektes die Zertifikate aller Teilnehmerinnen einsammelt, sicherstellt, dass diese alle exportierbar beglaubigt sind (ggf. beglaubigt sie sie selber), und dann über einen beliebigen Kanal (z.B. per Mail) an die Projektteilnehmer verteilt.

5 Anleitungen

5.1 Trusted Key anlegen

Die Beglaubigungsmanagerin besitzt einen konformen OpenPGP Schlüssel, den Trusted Key. Dieser kann mit dem in GnuPG VS-Desktop® enthaltenen Programm Kleopatra erzeugt werden (siehe Hilfe → Kurzanleitung). Wir haben diesen Schlüssel in unserem Beispiel „GnuPG.com OpenPGP CA“ genannt. Er sollte in der Praxis ihre eigene Organisationsbezeichnung im Namen haben, damit er sich leicht zuordnen lässt. Eine Mailadresse benötigt dieser Schlüssel nicht.

Den Fingerprint des Trusted Keys trägt man bei allen GnuPG VS-Desktop® – Installationen der eigenen Organisation in der Registry ein (siehe <https://gnupg.com/vsd/registry-settings.html>). Sollten Sie mehr als die normalerweise definierten 5 Trusted Keys benötigen, stellen wir Ihnen auf Nachfrage eine angepasste Version von GnuPG VS-Desktop® zur Verfügung.

Der öffentliche Schlüssel des Trusted Keys wird i.d.R. über das Active Directory an die Nutzerinnen verteilt, siehe Anleitung „How to install an LDS for use with GnuPG VS-Desktop®“ für das Aufsetzen. Unter Linux benötigt man hierfür LDAP, siehe „How to use LDAP with GnuPG“.

5.2 Beglaubigungen erstellen (exportierbar)

Sie wollen den neuen Schlüssel einer Mitarbeiterin mit dem Trusted Key für alle sichtbar beglaubigen. Dazu hat die Mitarbeiterin ihren Public Key exportiert und ihnen z.B. per Mail zukommen lassen. Sie importieren diesen Schlüssel wie folgt:

- Rechtsklicken auf den zu bearbeitenden Schlüssel in der Zertifikatsliste
- [Beglaubigen] wählen
- Vergewissern Sie sich, dass der öffentliche Schlüssel, den Sie beglaubigen, zu der richtigen Person gehört, indem Sie den Fingerabdruck über eine 2.Quelle (z.B. telefonisch) abgleichen
- Wählen Sie im Dropdown Menü „Beglaubigen mit“ Ihren Trusted Key aus. In unserem Beispiel ist das „*GnuPG.com OpenPGP CA*“
- Klappen Sie das „Fortgeschritten“ Menü durch Klick auf dem Pfeil aus.
- Wählen Sie hier „Für alle sichtbar beglaubigen (Exportierbar)“ aus.
- Wenn Sie einen internen LDS als Schlüsselservers konfiguriert haben, wählen Sie „Auf Schlüsselservers veröffentlichen“ aus. Dies können Sie auch jederzeit mit der Aktion „Auf Server veröffentlichen“ nachholen.

- Wählen Sie ein Ablaufdatum der Beglaubigung aus. Üblich sind 3 Jahre.

Zertifikat beglaubigen: Ted Tester - Kleopatra ✕

Überprüfen Sie den Fingerabdruck, markieren Sie die Benutzerkennungen, die Sie zertifizieren möchten, und wählen Sie den Schlüssel, mit dem Sie sie zertifizieren möchten.
Hinweis: Nur der Fingerabdruck identifiziert den Schlüssel und seinen Besitzer eindeutig.

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

Beglaubigen mit: GnuPG.com OpenPGP CA (★ VS-NfD-konform, erstellt: 17.04.2023) ▼

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

▼ Fortgeschritten

Für alle sichtbar beglaubigen (Exportierbar)
 Auf Schlüsselserver veröffentlichen

Tags: ❗

Ablaufdatum: ❗

Als vertrauenswürdiger Vermittler beglaubigt ❗

Domain:

- Führen Sie die Beglaubigung durch Klick auf [Beglaubigen] aus.
- Sie werden nach dem Passwort des Trusted Keys gefragt. Geben Sie dieses ein und bestätigen mit [OK].

5.3 Beglaubigung eines Schlüssels als Trusted Introducer

Wenn Sie einen Schlüssel bevollmächtigen wollen, alle Schlüssel einer bestimmten Domain zu beglaubigen, gehen Sie wie oben beschrieben vor, aber mit folgendem Unterschied:

- Setzen Sie im „Fortgeschritten“ Menü zusätzlich einen Haken bei „Als vertrauenswürdiger Vermittler beglaubigt“.
- Geben Sie dort auch die Domäne an, der mit diesem Zertifikat vertraut wird.

6 Automatisierungsmöglichkeiten Beglaubigung

6.1 Rohde & Schwarz Identitätsmanagement

6.1.1 Interne Zertifikate

Die Kombination mit dem Rohde & Schwarz Trusted Object Manager (TOM) und Trusted Identity Manager (TIM) automatisiert das Beglaubigungssystem.

Dies ist möglich, da der TOM über die Smartcard bereits eine Identitätsbeziehung hat. Dank dieser Identitätsbeziehung ist eine VS-NfD konforme Identifikation mit einem Schlüssel möglich. Daher kann der TOM automatisch die Zertifikate beglaubigen und über einen LDS bereitstellen.

Damit ist die Identifikation und Schlüsselverteilung intern bereits erledigt.

6.1.2 Externe Zertifikate

Zur Kommunikation mit Externen erstellen Sie sich wie in Kapitel 2 beschrieben einen weiteren Trusted Key und tragen diesen ein. Mit diesem können Sie nun im Idealfall das Zertifikat eines externen TOM als Trusted Introducer beglaubigen. Wenn dies nicht möglich ist, können Sie weiterhin einzelne Zertifikate prüfen und in Ihrer Schlüsselverteilung bereitstellen.

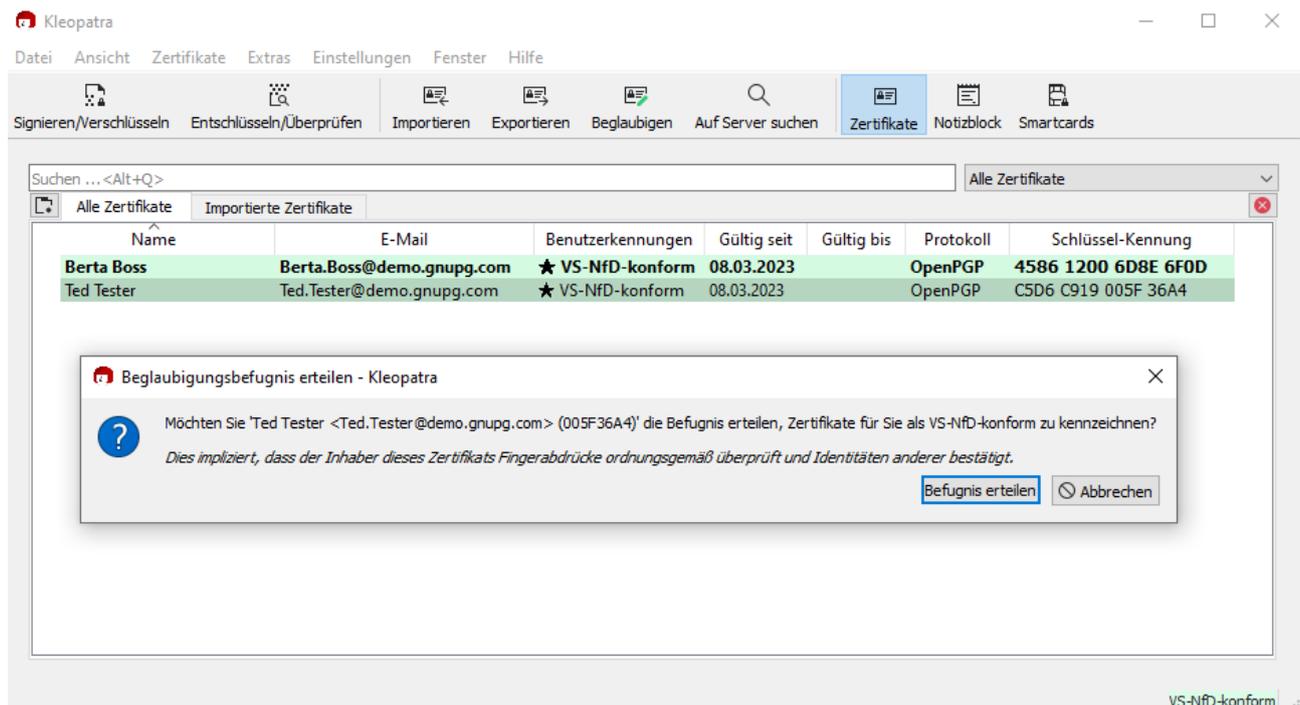
6.2 Actium

Actium ist eine Server Software für die automatisierte Beglaubigung von Zertifikaten aus dem LDAP der eigenen Organisation.

Sie wird von der g10 Code GmbH in 2023 veröffentlicht werden.

7 Beglaubigungsmanagement durch die Anwender

Anwender können in der Standard Konfiguration von GnuPG VS-Desktop® sowohl ein Zertifikat als Trusted Introducer beglaubigen, als auch einem beliebigen Zertifikat Beglaubigungsbefugnis erteilen. Dies geschieht mittels Rechtsklick auf das Zertifikat → [Beglaubigungsvertrauen ändern] → [Befugnis erteilen]:



Ein Schlüssel mit Beglaubigungsbefugnis (Trustlevel=vollständig) entspricht in der praktischen Anwendung einem Trusted Key.

Wenn man in einer Organisation verhindern möchte, dass Nutzer Beglaubigungen selber managen, kann man Kleopatra so konfigurieren, dass die entsprechenden Optionen nicht angeboten werden.

Hierfür müssen Sie für die Erteilung von Beglaubigungsbefugnissen in der Registry die Kleopatra Aktion `certificates_change_owner_trust` auf `false` setzen, für Details siehe die Beschreibung auf <https://gnupg.com/vsd/kleopatra-settings.html>.

Um Beglaubigungen durch die Nutzer generell zu unterbinden, wenn alle Beglaubigungen ausschließlich zentral gemanaged werden sollen, kann man `certificates_certify_certificate` auf `false` setzen.