GpgOL Outlook Add-In

Kurzanleitung für Anwender

Dokumentversion 2.0

Einleitung

Dies ist eine Kurzanleitung zum schnellen Einstieg in GpgOL. Es wird Schritt-für-Schritt beschrieben, wie man Mails in Microsoft Outlook verschlüsselt und signiert. Darüber hinaus erhalten Sie nützliche Hinweise, die Sie während Ihrer Arbeit mit GpgOL unterstützen.

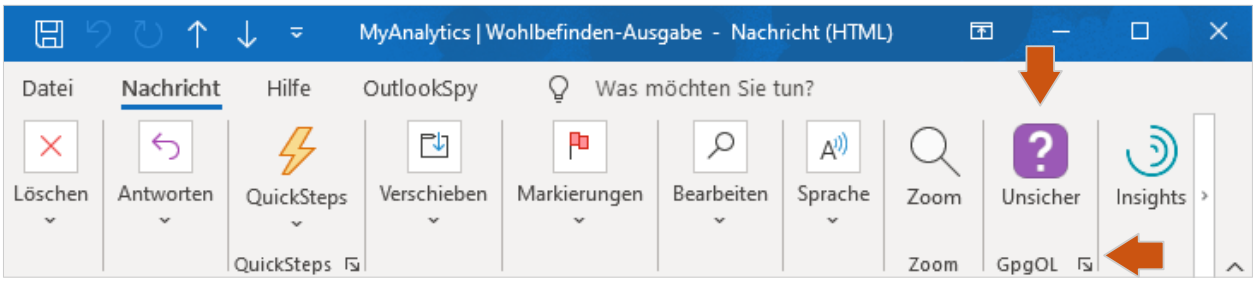
GpgOL ist ein Bestandteil von GnuPG VS-Desktop® und GnuPG Desktop® und funktioniert im Zusammenspiel mit dem Zertifikatsmanager Kleopatra.

Das GpgOL Outlook Add-In hat das Ziel, dass sich abgesicherter Mailverkehr so unkompliziert anfühlt wie der bisherige, nicht abgesicherte. Als sicherer Mailverkehr wird angesehen, wenn Mails auf dem Übertragungsweg nicht verändert, gefälscht oder mitgelesen werden können. Eine gute Analogie ist eine Postkarte, die vor dem Versenden in einen blickdichten Briefumschlag gesteckt und der zudem mit Wachs versiegelt wird. Ihr Empfänger kann am Wachssiegel erkennen wer der Absender war und ob der Umschlag zuvor von Dritten geöffnet und ggf. verfälscht wurde.

Bei Mails, die vom GpgOL Outlook Add-In als unsicher angezeigt werden, kann technisch nicht sichergestellt werden, dass sie unverändert sind. Für diese Mails ist die Analogie eine normale Postkarte: Jeder, der sie auf dem Transport in der Hand hat, kann sie lesen, verändern oder ganz fälschen. Bei solchen Mails ist stets Vorsicht geboten. Selbst wenn Sie eine Mail vom eigenen Server empfangen und diese aus dem eigenen Netzwerk stammt, bietet das keine Sicherheit. Ein Angreifer könnte den Server übernommen und damit die Kontrolle über Ihren gesamten unsicheren Nachrichtenverkehr erhalten haben.

1 Der GpgOL-Button in Outlook

Das GpgOL Outlook Add-In verwendet als Interface nur einen einzigen Button:

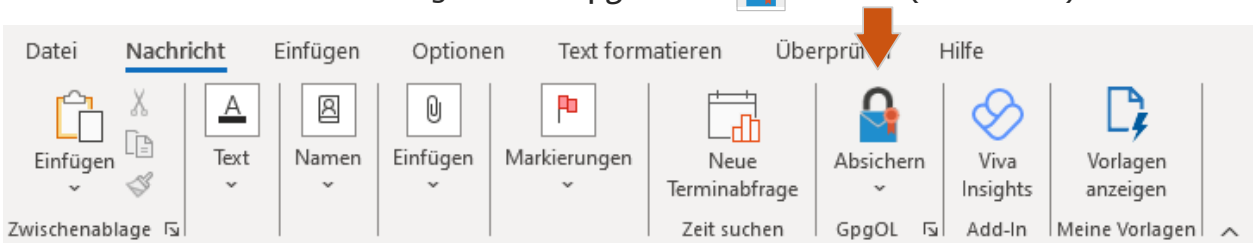


- Der Button zeigt die jeweilige Sicherheitsstufe einer Mail an
- Wird er in einer neuen Mail aktiviert, wird diese verschlüsselt und signiert
- Bewegt man den Mauszeiger über den Button, erscheint der GpgOL-Tooltip
- Das Konfigurationsmenü erreicht man über das Eck-Symbol neben dem Text GpgOL

Hinweis	Verwenden Sie die Outlook-Option "Menüband anpassen", um GpgOL individuell in Ihren Arbeitsbereich zu integrieren.

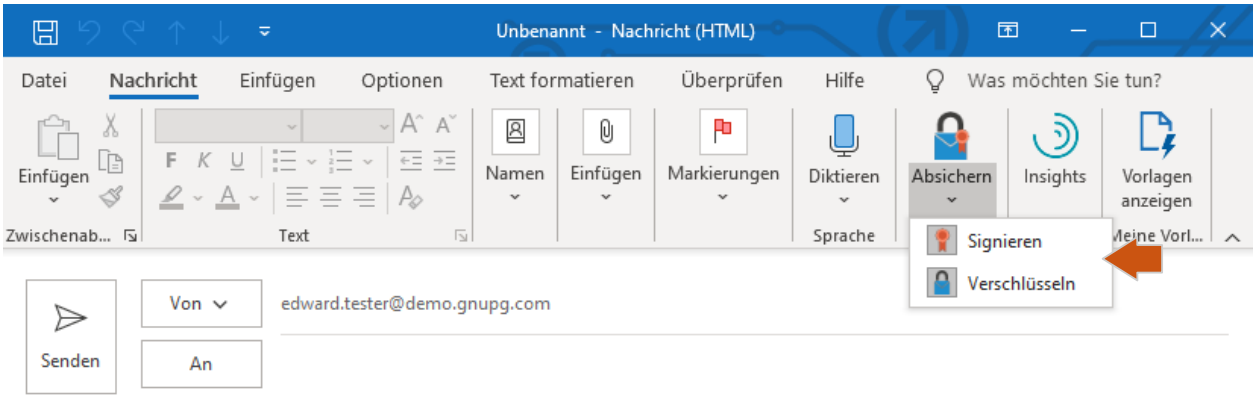
2 Mails versenden

Beim Verfassen von Mails zeigt Ihnen GpgOL den -Button (Absichern) an:



Wird dieser aktiviert, ist er farblich hervorgehoben, Ihre Mail wird dann signiert und verschlüsselt:

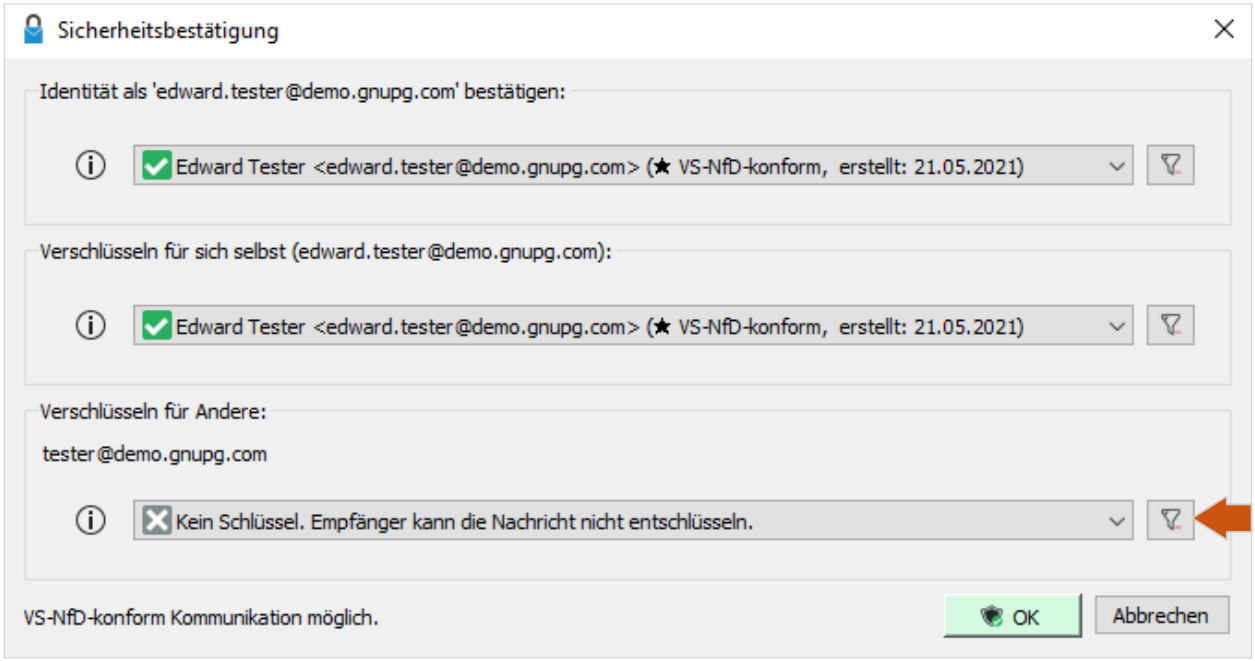
Das Untermenü erlaubt es Ihnen zudem, Nachrichten wahlweise nur zu Signieren oder nur zu Verschlüsseln. Empfehlenswert ist aber, beides gleichzeitig anzuwenden:



2.1 Der Sicherheitsbestätigungs-Dialog

Der Dialog "Sicherheitsbestätigung" wird in der Standardeinstellung nur dann angezeigt, wenn für mindestens eine Empfängeradresse kein passendes beglaubigtes, VS-NfD konformes[1], Zertifikat gefunden wurde. In diesem Fall bietet Ihnen der Dialog die Möglichkeit, für den Empfänger ein anderes Zertifikat auszuwählen.

Durch Klicken auf den -Button (Filter entfernen) rechts neben der Empfängerzeile können Sie beliebige Zertifikate auswählen, auch solche, denen keine Mailadresse zugeordnet ist:



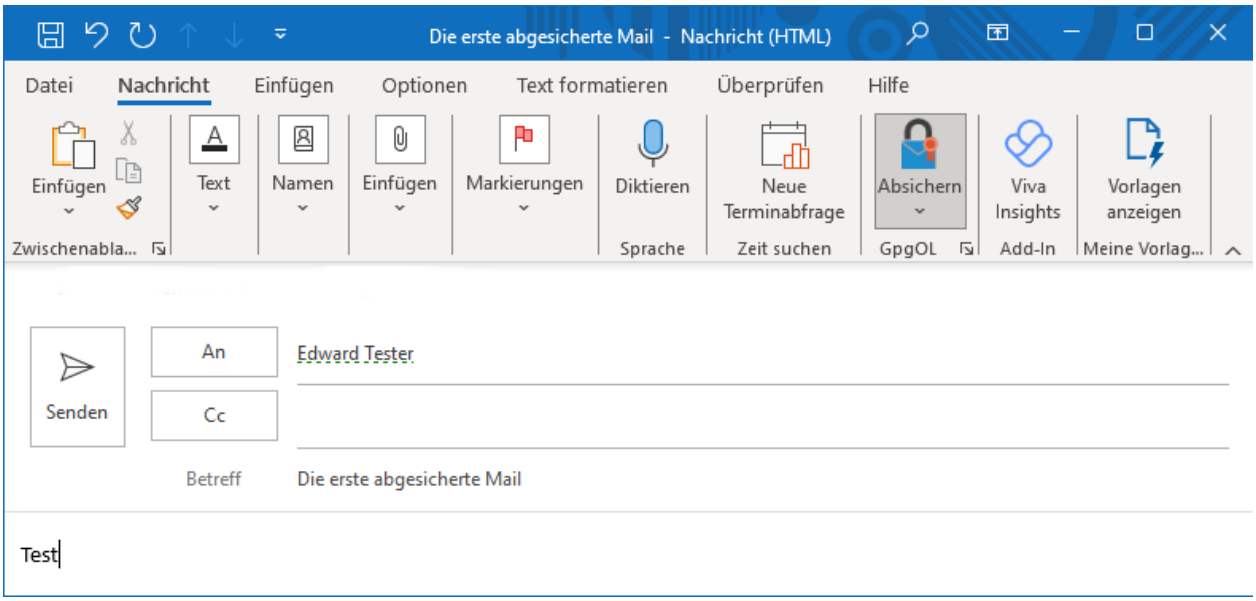
1 Bei GnuPG Desktop® ist kein VS-NfD konformer Schlüssel erforderlich

Wichtig

Falls Sie kein Zertifikat für "Verschlüsseln für Andere" auswählen bzw. weniger als Empfänger vorhanden sind, ist der bzw. sind diese Empfänger nicht in der Lage, Ihre Nachricht zu entschlüsseln! Sie erhalten keine unverschlüsselte Mail. Die versandte Mail kann ausschließlich mit einem der Schlüssel entschlüsselt werden, die Sie ausgewählt haben.

2.2 Die erste abgesicherte Mail versenden

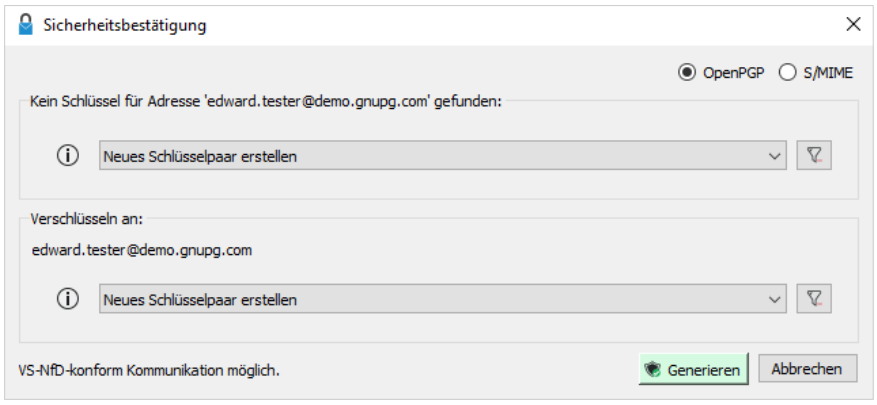
Wir empfehlen, die erste abgesicherte Mail zu Test- bzw. Übungszwecken erst einmal an sich selbst zu senden. Aktivieren Sie dafür den Absichern-Button, verfassen dann eine kurze Nachricht, setzen einen Betreff und fügen ggf. einen Anhang hinzu:



Wichtig

Mails werden einschließlich aller Anhänge verschlüsselt. **Die Betreffzeile bleibt unverschlüsselt**, so dass Empfänger immer erkennen können, worum es in der Nachricht geht.

GpgOL verwendet zum Absichern von Mails sogenannte "Schlüssel" bzw. "Zertifikate". Sollten Sie noch keinen eigenen Schlüssel haben, erhalten Sie nach dem Klick auf Senden den Dialog "Sicherheitsbestätigung" angezeigt. Um Ihr persönliches OpenPGP Schlüsselpaar zu erzeugen, klicken Sie hier auf Generieren:



Hinweis

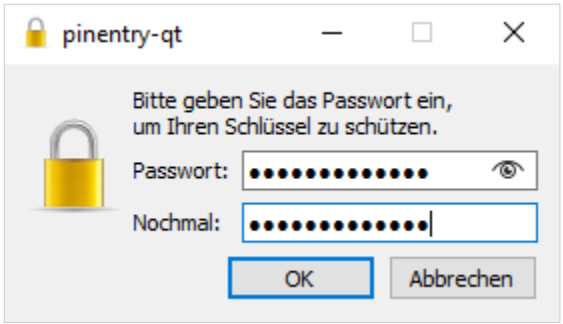
Wenn Sie dem Schlüssel außer der Mailadresse noch einen Namen hinzufügen oder eine der Standardeinstellungen ändern möchten, generieren Sie diesen bitte vorab in Kleopatra.

Sie werden nach dem Passwort gefragt, dass Sie für den Schlüssel verwenden möchten.

Wichtig

Das Passwort schützt Ihren eigenen geheimen Schlüssel in Ihrem Dateisystem. **Es kann weder wiederhergestellt noch zurückgesetzt werden - ist es einmal verloren, ist Ihr Schlüssel unbrauchbar!** Es ist daher wichtig, dass Sie das Passwort aufschreiben und sicher sowie VS-NfD konform aufbewahren!

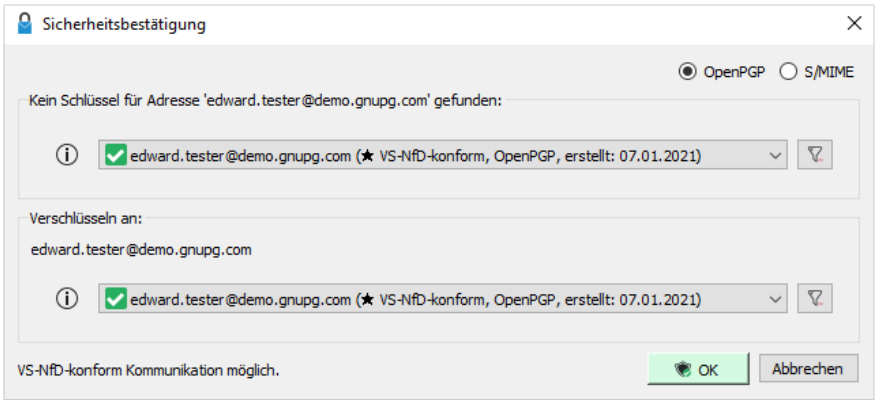
Geben Sie ein sicheres, ihren organisatorischen Passwortrichtlinien entsprechendes Passwort ein und klicken Sie auf OK:



Hinweis

Wie lange das Passwort nicht mehr neu eingegeben werden muss, können Sie im Konfigurationsmenü unter "GnuPG System" > "Geheime Schlüssel" > "Lösche unbenutzte Passwörter nach N Sekunden aus dem Cache" einstellen.

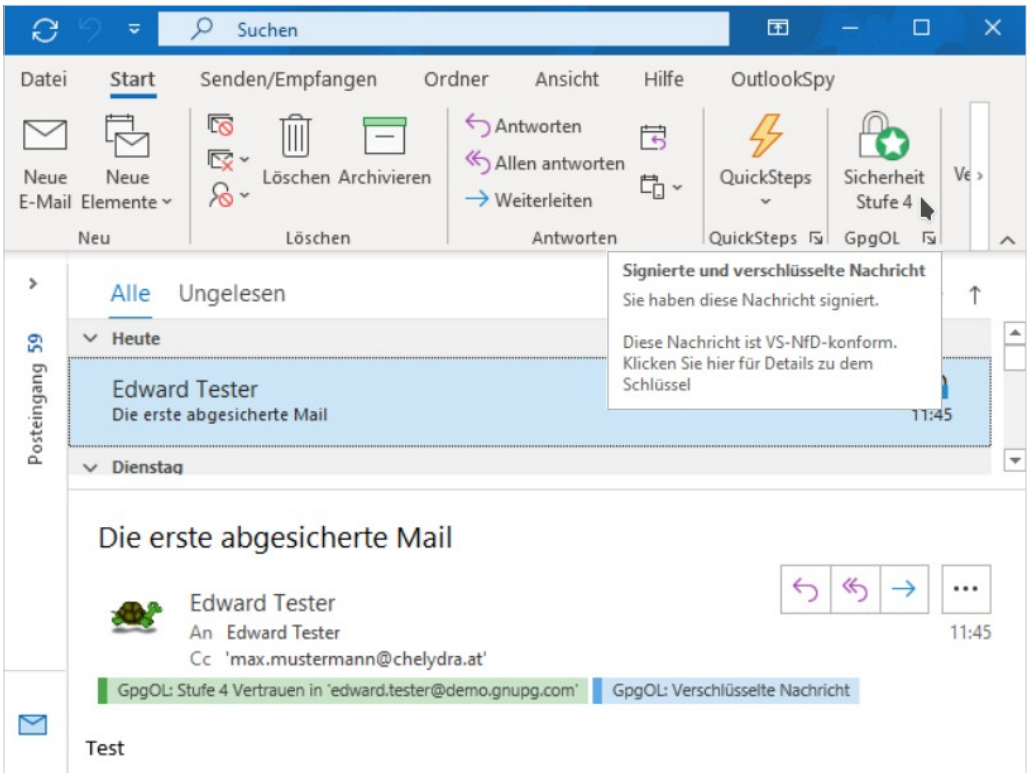
Nach dem Generieren des Schlüssels kann dieser nun sofort verwendet werden. Klicken Sie dafür auf OK :



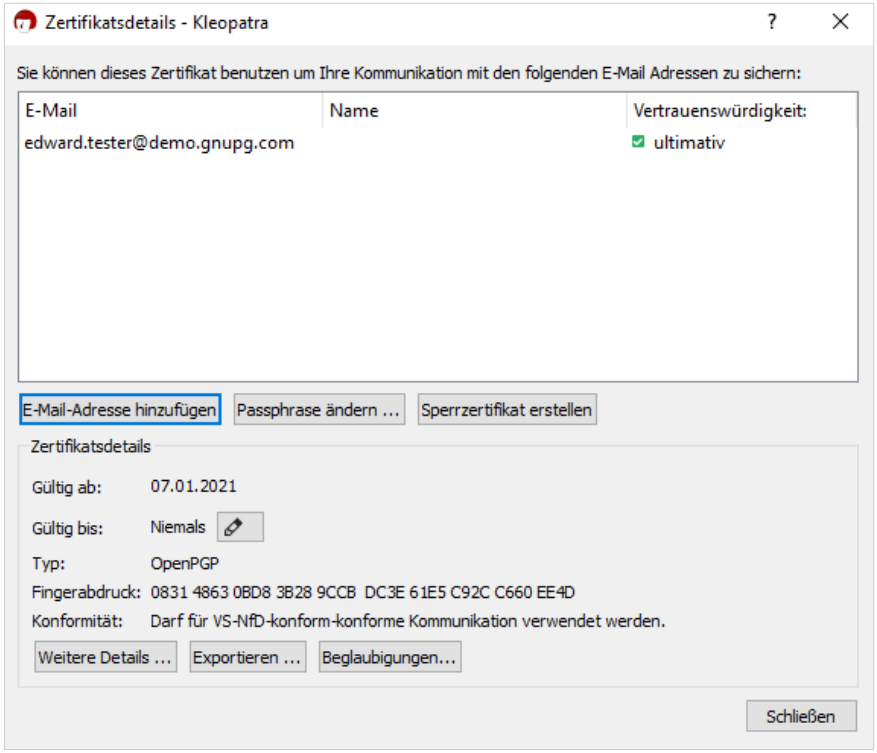
Für weitere Informationen lesen Sie bitte auch die Kurzanleitung "Verschlüsseln und signieren mit GnuPG VS-Desktop®". Sie erfahren dort auch, was Sie tun müssen, damit andere Nachrichten an Sie verschlüsseln können.

3 Mails anzeigen

Beim Betrachten einer Mail, ganz gleich ob in einem eigenem Fenster oder in der Nachrichtenliste, wird diese automatisch entschlüsselt. Sie werden ggf. nach Ihrem Passwort gefragt. Wenn Sie innerhalb einer signierten Mail den Mauszeiger über dem GpgOL-Button schweben lassen, werden Informationen zu Signatur und Verschlüsselung der dargestellten Mail angezeigt:



Wenn Sie innerhalb einer signierten Mail auf den GpgOL-Button klicken, öffnet sich Kleopatra und zeigt Ihnen weitere Informationen über das verwendete Zertifikat an:



Hinweis

Der Zertifikatsmanager Kleopatra, das grafische Frontend von GnuPG VS-Desktop® und GnuPG Desktop®, ermöglicht es Ihnen, Ihre Schlüssel bzw. Zertifikate einfach zu verwalten. Hier können Sie z.B. festlegen, ob Sie einem fremden Zertifikat vertrauen indem Sie es beglaubigen.

3.1 Sicherheitsstufen bei der Identitätsprüfung von empfangenen Mails

Hinweis

Die Sicherheitsstufen bei empfangenen Mails sind nicht relevant für VS-NfD, sondern geben nur einen Anhaltspunkt für die Beurteilung der Authentizität der Mail. Mehr Informationen zeigt Ihnen der Tooltip von GpgOL.

Entscheidend für den Austausch von VS-NfD Informationen ist, dass das Zertifikat Ihres Kommunikationspartners in Kleopatra als VS-NfD konform gekennzeichnet ist. Dies entspricht den nachfolgend aufgeführten Stufen 3 oder 4. Nur dann können Sie mit GpgOL verschlüsselte Mails versenden, ohne eine Warnung zu erhalten.

Das GpgOL Outlook Add-In verwendet je nach Vertrauensstatus unterschiedliche Sicherheitsstufen zum Authentifizieren, wodurch sich organisatorische Maßnahmen einfach abbilden lassen. Es kann eine Sekunde dauern bis die Sicherheitsstufe einer neu angewählten Mail korrekt angezeigt wird:

Sicherheitsstufe 0 (Unsicher/Verschlüsselt); keine Validierung

Der Schlüssel Ihres Kommunikationspartners ist unbekannt oder die Mail ist nicht signiert.

Sicherheitsstufe 1; Validierung über Mail-Adresse

GpgOL trifft hier keine Vertrauensaussagen über die Identität des Schlüsselinhabers, verwendet aber den Schlüssel zur Verschlüsselung. Diese Stufe schützt vor passiven Angreifern, jedoch nicht vor aktiven "Man in the Middle" Angriffen.

Sicherheitsstufe 2; Eingeschränkte Identitätsprüfung

Der Schlüssel des Kommunikationspartners wurde vom Provider automatisch über eine abgesicherte Verbindung ausgeliefert. Das geht nur, wenn dieser das „Web Key Directory“[2] einsetzt. Es besteht ein Grundvertrauen, dass der Absender die Mailadresse kontrolliert, von der aus die Nachricht gesendet wurde.

Sicherheitsstufe 3; Identitätszertifizierung

Die Identität des Kommunikationspartners wurde mit einem vertrauenswürdigen Zertifikat beglaubigt. Diese Stufe schützt vor aktiven Angreifern.

Sicherheitsstufe 4; Validierung durch direktes Vertrauen

Der Nutzer selbst oder ein Beglaubigungsmanager seiner Organisation haben den Fingerabdruck des Schlüssels geprüft und diesen signiert.

4 Der Zertifikatsmanager Kleopatra als Krypto-Adressbuch

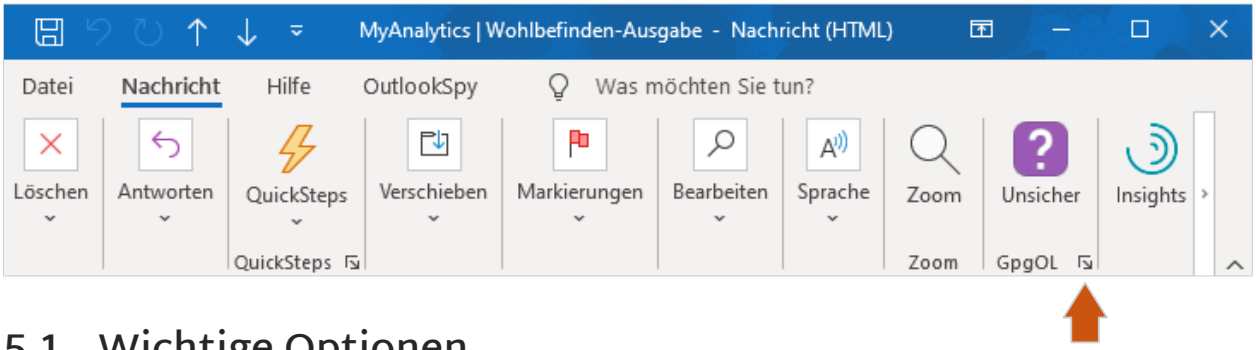
GpgOL nutzt den Zertifikatsmanager Kleopatra, um sich die passenden Zertifikate für ihre Kommunikationspartner zu holen. Basierend auf ihrer Konfiguration wird zusätzlich in externen Quellen (Active Directory, X509 Zertifikatsserver, Web Key Directory, etc.) gesucht. Die Zuordnung erfolgt über die Mailadresse. Sollten mehrere VS-NfD konforme bzw. vertrauenswürdige Zertifikate für eine Mailadresse vorliegen, wird das Neuste ausgewählt.

2 https://wiki.gnupg.org/WKD

Für eine Funktionsmail-Adresse müssen Sie zunächst eine Gruppe in Kleopatra anlegen. Siehe hierfür die Kurzanleitung "Die Gruppenfunktion von GnuPG VS-Desktop®".

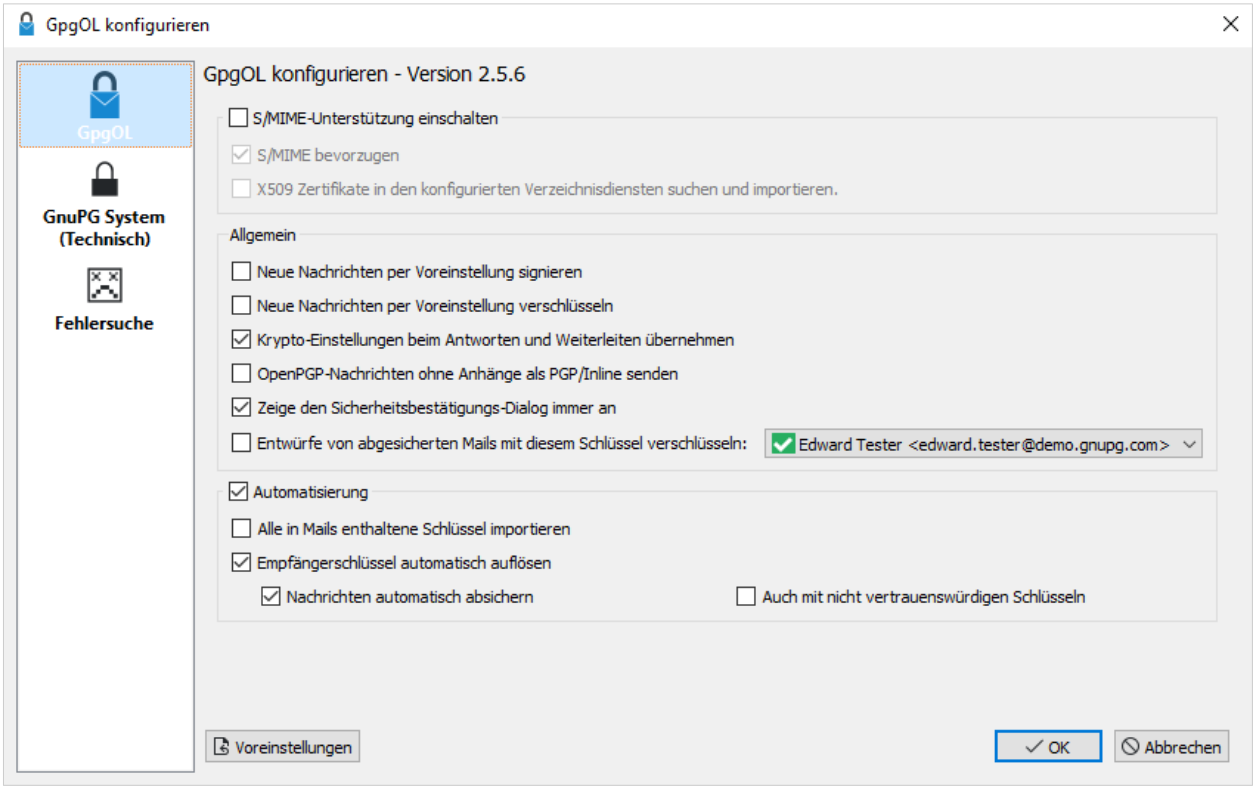
5 Das GpgOL-Konfigurationsmenü

Das Konfigurationsmenü erreicht man über das Eck-Symbol neben dem Text GpgOL:



5.1 Wichtige Optionen

Das GpgOL-Konfigurationsmenü bietet Ihnen viele meist selbsterklärenden Einstellungen.



Es folgen Erläuterungen zu einigen wichtigen Optionen:

S/MIME bevorzugen

Wenn GpgOL für Empfänger sowohl S/MIME als auch OpenPGP-Zertifikate findet, wird S/MIME verwendet.

X.509 Zertifikate in den konfigurierten Verzeichnisdiensten suchen u. importieren

Mit dieser Option aktivieren Sie, dass GpgOL für jeden Empfänger einer Mail, für den kein gültiges Zertifikat bekannt ist, eine automatische Suchanfrage an den im GnuPG-System konfigurierten Verzeichnisdienst sendet. Diese Zertifikate werden dann automatisch importiert und, sofern ihre Zertifikatskette vertrauenswürdig ist, auch verwendet.

Wenn Sie diese Option mit "Nachrichten automatisch absichern" kombinieren, wird für jede Empfängeradresse eine Suchanfrage generiert, um zu prüfen, ob ein Zertifikat dazu existiert. Der Server kann daran sehen, mit wem Sie kommunizieren. Daher raten wir von dieser Kombination ab, es sei denn, Sie haben den Zertifikatsserver in Ihrer Organisation unter eigener Kontrolle.

Krypto-Einstellungen beim Antworten und Weiterleiten übernehmen

Beim Antworten oder Weiterleiten werden die Krypto-Einstellungen anhand der Ursprungsmail übernommen. Auf verschlüsselte Mails wird also auch verschlüsselt geantwortet bzw. diese werden beim Weiterleiten an den neuen Empfänger verschlüsselt.

OpenPGP-Nachrichten ohne Anhänge als PGP/Inline senden

Ihre Mails werden nicht im PGP/MIME-Format versendet, wenn Sie keinen Anhang besitzen, d.h. der Textkörper der Mail wird durch eine "PGP Message" ersetzt.

PGP/Inline hat den Nachteil, dass Anhänge nicht benutzerfreundlich abgesichert werden können und auch das sogenannte Encoding nicht klar definiert ist. Sie sollten diese Option nur in Ausnahmefällen benutzen, etwa wenn ihr Kommunikationspartner keinen PGP/MIME fähiges Mail Programm verwendet und er den Text im Notizblock von Kleopatra entschlüsseln möchte.

Zeige den Sicherheitsbestätigungs-Dialog immer an

Der Dialog "Sicherheitsbestätigung" wird auch dann angezeigt, wenn für alle Empfänger ein vertrauenswürdiger bzw. VS-NfD konformer Schlüssel gefunden wird.

Entwürfe von abgesicherten Mails mit diesem Schlüssel verschlüsseln

Insbesondere wenn Ihre Entwürfe und Autosaves nicht nur lokal, sondern auch auf dem Mailserver gespeichert werden, kann diese Option für einen Sicherheitsgewinn sorgen. Durch ihre Verwendung werden keine unverschlüs-

selten Inhalte auf dem Server gespeichert, bevor Sie eine abgesicherte Mail versenden.

⚠ Wichtig

GpgOL kann nur wissen, ob Sie eine Mail verschlüsselt speichern möchten, wenn Sie bereits vor dem Verfassen Ihrer Nachricht den Absichern-Button  aktiviert haben.

Alle in Mails enthaltene Schlüssel importieren

Schlüssel, die an Mails angehängt sind bzw. sich im Autocrypt-Header einer Mail befinden, werden importiert. Solche Schlüssel werden, sofern sie nicht beglaubigt wurden, als "nicht beglaubigt" angezeigt. Dies ermöglicht es, Kommunikation mit einem geringen Schutzbedarf automatisch abzusichern.

Empfängerschlüssel automatisch auflösen

Es wird automatisch nach Schlüsseln sowohl lokal als auch in den im GnuPG-System konfigurierten Schlüsselquellen (üblicherweise Active Directory und Web Key Directory) gesucht. Wenn die Option "X.509 Zertifikate in den konfigurierten Verzeichnisdiensten suchen und importieren" aktiviert ist, wird dies auch für S/MIME durchgeführt.

Nachrichten automatisch absichern

GpgOL aktiviert automatisch den Absichern-Button  , wenn für alle Empfänger vertrauenswürdige Schlüssel gefunden werden.

Die Zusatzoption "Auch mit nicht vertrauenswürdigen Schlüsseln" sorgt dafür, dass auch nicht vertrauenswürdige Schlüssel, z.B. aus Autocrypt-Headern, verwendet werden. Dieses bietet in vielen Fällen bereits hinreichenden Schutz vor passiven Angriffen, z.B. vor dem einfachen Mitlesen ihres Mailverkehrs. Da diese Zertifikate aber nicht den Ansprüchen für VS-NfD genügen, muss man vor dem Senden der Mail noch einmal bestätigen, dass trotzdem verschlüsselt werden soll.

Anhang