Ein Handbuch im Auftrag des
Bundesamtes für Sicherheit in der Informationstechnik

Projekt 194 („Gpg4VS-NfD“)

Handbuch zur Zulassung von GnuPG VS-Desktop

Version 3.2

Stand vom 2024-01-18

Autoren

Stephan Müller

atsec information security GmbH
Steinstr. 70
81667 München
https://www.atsec.de

Andre Heinecke
Werner Koch

g10code GmbH
Bergstr. 3a. 61
40699 Erkrath
https://g10code.com

Unter Mitwirkung von:

Emanuel Schütze
Bernhard Reiter

Intevation GmbH
Neuer Graben 17
49074 Osnabrück
https://intevation.de

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einführung

GnupG VS-Desktop unterstützt viele verschiedene Funktionen und kryptografische Mechanismen. Ein Teil dieser Funktionen sind für die Verarbeitung von Verschlusssachen (VS) geeignet.

Dieses Handbuch stellt Hinweise bereit, GnuPG VS-Desktop für die Verwendung im Rahmen von Verschlusssachen (VS-NfD) zu konfigurieren und korrekt zu nutzen. Wenn eine Kommunikation mit dem Produkt GnuPG VS_Desktop so durchgeführt wird, dass sie den Anforderungen an VS-NfD entspricht, wird das im Folgenden als *konform* bezeichnet.

Dieses Handbuch ist speziell für die Zulassung zur Verarbeitung von Verschlusssachen erstellt worden. Hingegen decken andere Handbücher rund um die verschiedenen Teile von GnuPG VS-Desktop die generelle Nutzung unabhängig von den Regeln zu Verschlusssachen ab. Demzufolge hat dieses Handbuch Vorrang vor allen anderen Handbüchern. Falls sich andere Handbücher mit diesem Handbuch zur Zulassung widersprechen, gelten die Aussagen in diesem Zulassungshandbuch.

Das Handbuch deckt folgende Programme ab:

- **GnuPG VS-Desktop** für Windows: GnuPG (bestehend aus den Programmen gpg und gpgsm), Kleopatra, GpgOL und GpgEX.
- **GnuPG VS-Desktop** für Linux**:** GnuPG (bestehend aus den Programmen gpg und gpgsm), Kleopatra sowie die Module von Dolphin und Kontact Mail (auch KMail genannt), welche mit Kleopatra und GnuPG kommunizieren.

Die von den genannten Programmen verwendeten Bibliotheken werden nicht gesondert dokumentiert, da sie nicht losgelöst von den Programmen zulassungsrelevante Funktionen anbieten. Damit wird auch festgehalten, dass andere, nicht genannte Programme, diese Bibliotheken nutzen können. In diesem Fall stellen diese anderen Programme weder zulassungsrelevante Mechanismen bereit, noch bieten sie solche Mechanismen, noch können sie Funktionen von Gpg4win und Gpg4KDE beeinflussen.

1.1 Struktur des Handbuchs

Das Handbuch unterteilt sich in die folgenden Abschnitte:

- Kapitel 2 erläutert allgemeine Nutzungshinweise
- Kapitel 3 gibt Hinweise zur VS-Verarbeitung

2 Generelle Nutzungshinweise

Die sichere Nutzung von GnuPG VS-Desktop zur Achtung und Wahrung von Regeln zu Verschlusssachen basiert auf den folgenden generellen Nutzungshinweisen. Diese Hinweise gelten unabhängig von konkreten Nutzungsszenarien, die in den Folgekapiteln erläutert werden.

2.1 Einleitung

GnuPG VS-Desktop erlaubt dem Benutzer, schutzwürdige Daten konform (nach VS-NfD) mit Kommunikationspartnern über unsichere Netzwerke, wie zum Beispiel dem Internet, auszutauschen.

Der Schutz der Daten erfolgt mittels Signaturen und Verschlüsselung. Beide Mechanismen, Signaturen und Verschlüsselung, können unabhängig voneinander oder zusammen verwendet werden, um unterschiedliche Nutzungsszenarien und Schutzanforderungen abzudecken. Grundsätzlich ist es immer sinnvoll, schutzwürdige Daten sowohl zu verschlüsseln als auch zu signieren. Signatur und Verschlüsselung schützen Daten wie folgt:

- Eine Signatur von Daten erlaubt es dem Kommunikationspartner die Authentizität und die Integrität der Daten zweifelsfrei zu verifizieren. Authentizität heißt, dass die Daten wirklich vom Sender stammen und nicht von einer anderen Person, die vorgibt, der Sender zu sein. Integrität impliziert, dass die Daten während der Übertragung durch ein unsicheres Netzwerk nicht verändert wurden. Dies bedeutet, wenn GnuPG VS-Desktop eine Signatur als korrekt verifiziert hat, ist sichergestellt, dass die geschützten Daten sowohl vom eigentlichen Sender stammen, als auch unverändert übertragen wurden.
- Die Verschlüsselung von Daten stellt die Vertraulichkeit der Daten während der Übertragung durch ein unsicheres Netzwerk zweifelsfrei sicher. Unter Vertraulichkeit wird verstanden, dass andere Personen außer dem Sender und Empfänger die geschützten Daten nicht lesen können.

Das Gpg4win-Kompendium[1] bietet eine umfassende Beschreibung, wie Signaturen und Verschlüsselung genutzt werden. Es wird erläutert, wie die Schlüssel zum Schutz der Daten verwendet werden. Diese Beschreibung trifft im vollen Umfang auf GnuPG VS-Desktop zu und wird in diesem Zulassungshandbuch nicht wiederholt.

Die Nutzung von GnuPG VS-Desktop im Rahmen von Verschlusssachen führt zu einigen grundlegenden Einschränkungen, die im Folgenden klargestellt werden.

Die VS-Konfiguration grenzt die erlaubten kryptografischen Mechanismen ein, die zum Schutz der Daten verwendet werden dürfen. Um dennoch eine reibungslose Nutzung von GnuPG VS-Desktop zu gewährleisten, wird folgender Grundsatz verwendet:

[1] https://files.gpg4win.org/doc/gpg4win-compendium-de.pdf

GnuPG VS-Desktop stellt sicher, dass nur Verschlusssachen-konforme kryptografische Algorithmen verwendet werden, wenn GnuPG VS-Desktop diese auswählen kann. Hingegen werden alle Algorithmen akzeptiert und verarbeitet, wenn diese von einem Kommunikationspartner spezifiziert wurden. In diesem Falle zeigt GnuPG VS-Desktop klar an, wenn die Kommunikation VS-NfD-konform ist. Dieser Ansatz erlaubt immer eine geschützte Kommunikation. Falls GnuPG VS-Desktop anzeigt, dass eine nicht-VS-NfD-konforme Kommunikation vorliegt, sollte der Benutzer dem Kommunikationspartner bitten, seine kryptografischen Algorithmen anzupassen.

Falls GnuPG VS-Desktop anzeigt, dass nicht-konform kommuniziert wird, sollte der Datenaustausch abgebrochen werden und das Problem mit dem Kommunikationspartner gelöst werden. Falls aber dennoch unbedingt ein Datenaustausch stattfinden soll, erlaubt GnuPG VS-Desktop dies. In diesem Fall muss der Nutzer sich im Klaren sein, dass die ausgetauschten Daten nicht entsprechend der VS-NfD-Regeln geschützt werden. Dennoch werden die Daten geschützt, was zweifelsfrei besser ist, als ohne jeglichen Schutz (und damit ohne Hilfe von GnuPG VS-Desktop) Daten auszutauschen.

Folgendes Beispiel soll den Grundsatz klarstellen: Ein Mitarbeiter in der Bundesverwaltung sendet eine verschlüsselte Nachricht an eine Person außerhalb der Bundesverwaltung, mit der er die Schlüssel bereits ausgetauscht hat. Hierbei kann es passieren, dass GnuPG VS-Desktop anzeigt, dass der Datenaustausch nicht konform geschützt ist, da der Schlüssel der Person außerhalb der Bundesverwaltung nicht den notwendigen Algorithmus aufweist. In diesem Fall sollte diese Person gebeten werden, einen neuen Schlüssel zu erstellen, der konforme Algorithmen nutzt. Falls aber zwingend der Datenaustausch stattfinden soll, kann der Mitarbeiter der Bundesverwaltung sich über den Hinweis von GnuPG VS-Desktop bezüglich der Nicht-Konformität hinwegsetzen.

Ein weiteres Beispiel ist folgendes: Ein Mitarbeiter der Bundesverwaltung prüft eine Signatur, die von einer Person außerhalb der Bundesverwaltung erstellt wurde. In diesem Fall kann es ebenfalls sein, dass GnuPG VS-Desktop eine nicht-konforme Signatur anzeigt. In diesem Fall hat der Ersteller der Signatur einen Schlüssel mit einem nicht-konformen Algorithmus verwendet. Der Mitarbeiter der Bundesverwaltung sollte nun den Kommunikationspartner bitten, einen neuen Schlüssel zu erstellen, mit dem diese Daten nochmal signiert werden.

Wenn ein Datenaustausch zwischen Mitarbeitern der Bundesverwaltung stattfindet, sollte GnuPG VS-Desktop niemals eine nicht-konforme Kommunikation feststellen, da beide Seiten zwingend konforme kryptografische Algorithmen nutzen müssen. Falls dennoch ein nicht-konformer Datenaustausch signalisiert wird, sollte die Kommunikation abgebrochen und der Systemadministrator zu Rate gezogen werden.

2.2 Allgemeine Annahmen zur Nutzung

Der Nutzer oder der Administrator muss sicherstellen, dass folgende Annahmen an die Einsatzumgebung umgesetzt werden:

Es wird angenommen, dass die technische Einsatzumgebung, einschließlich der Hardware, während der Laufzeit der Programmkomponenten von GnuPG VS-Desktop mit einem physischen Schutz ausgestattet ist, der dem Wert der zu schützenden Objekte entspricht.

Die Programmkomponenten von GnuPG VS-Desktop werden von einem oder mehreren kompetenten Administratoren verwaltet. Diese Administratoren sind vertrauenswürdig und befolgen die bereitgestellte Dokumentation.

Jeder Benutzer erkennt den Unterschied in der Darstellung, wann eine konforme bzw. nicht-konforme Kommunikation vorliegt.

Jeder Benutzer ist für den Schutz der Geheimnisse, wie zum Beispiel Passwörter, welche seine eigenen Schlüssel schützen, verantwortlich.

Jeder Benutzer prüft neu erhaltene OpenPGP-Schlüssel von Kommunikationspartnern auf deren Eigenschaften, bevor der Benutzer diese Schlüssel als authentisiert und damit als vertrauenswürdig markiert.

Das zugrundeliegende Betriebssystem stellt die korrekte Zeit bereit.

Das zugrundeliegende Betriebssystem implementiert die Unterstützung für benutzerspezifische Dateizugriffsrechte, Speicherseparierung und Prozessisolation. Des Weiteren stellt das Betriebssystem notwendige Unterstützungsfunktionen bereit und stellt deren korrekte Funktion sicher.

Das zugrundeliegende Betriebssystem stellt die von den Programmkomponenten von GnuPG VS-Desktop erzeugten Informationen für Benutzer unverändert dar.
Hinweis: Wenn GnuPG VS-Desktop Informationen wie Schlüsselprüfungen über die Benutzerschnittstellen von GnuPG VS-Desktop dem Benutzer zugänglich machen will, werden teilweise umfangreiche Softwarekomponenten des Betriebssystems verwendet. Zum Beispiel muss das grafische Programm Kleopatra unter GNU/Linux den gesamten QT- und X11-Softwarestapel plus die Grafiktreiber verwenden, um die Informationen über Resultate von Schlüsselprüfungen am Bildschirm anzuzeigen. Die Annahme stellt klar, dass dieser Softwarestapel die von den Programmkomponenten von GnuPG VS-Desktop gewünschten Informationen unverändert anzeigt.

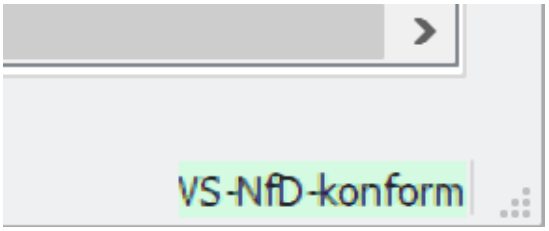
GnuPG VS-Desktop kann nur unter GNU/Linux und unter Windows verwendet werden, da diese Betriebssysteme den nötigen Schutz der Interprozesskommunikation zwischen den Teilen von GnuPG VS-Desktop sicherstellen. Des Weiteren ist bei diesen Betriebssystemen gewährleistet, dass die von den Programmkomponenten von GnuPG VS-Desktop erzeugten Informationen dem Benutzer unverändert angezeigt werden.

Das zugrundeliegende Betriebssystem und Hardware stellt ausreichend Entropie für den Zufallszahlengenerator von GnuPG VS-Desktop bereit.

3 Hinweise zur VS-Verarbeitung

Die folgenden Bildschirmfotos der grafischen Benutzeroberfläche zeigen auf, wie die Konformität angezeigt wird.

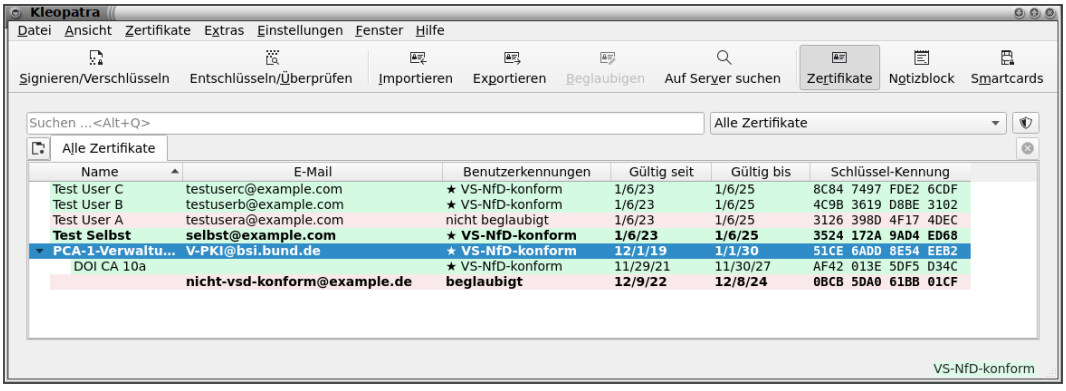
3.1 VS-Konformität der Software



In der Statusleiste von Kleopatra wird immer die konforme Installation von GnuPG VS-Desktop angezeigt. GnuPG VS-Desktop darf für VS-NfD Daten nur verwendet werden wenn dieser Text dort erscheint. Die Alternativen „VS-NfD compliant“, „EU Restricted“ und „NATO Restricted“ sind als gleichwertig anzusehen.

3.2 Darstellung der Schlüssel in Kleopatra

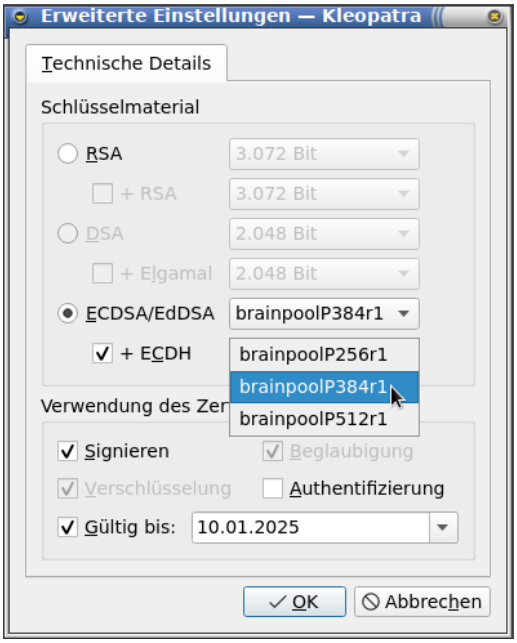
Alle Schlüssel und Zertifikate werden farblich hinterlegt: grün für VS-NfD-konform, rot für nicht VS-NfD-konform. VS-NfD-konforme Schlüssel und Zertifikate sind zusätzlich mit einem Stern-Icon markiert. Das Icon dient hier als Erkennungsmerkmal und findet sich als Zeichen für VS-NfD-konforme Zertifikate auch an anderer Stelle wieder (z.B. im Outlook-Plugin GpgOL).



Eigene Schlüssel sind durch Fettdruck hervorgehoben (hier „Test Selbst“ sowie der letzte Schlüssel). OpenPGP Schüssel müssen immer beglaubigt sein; deswegen wird im Beispiel „Test User A“ nicht als konform angezeigt.

3.3 Schlüsselerstellung

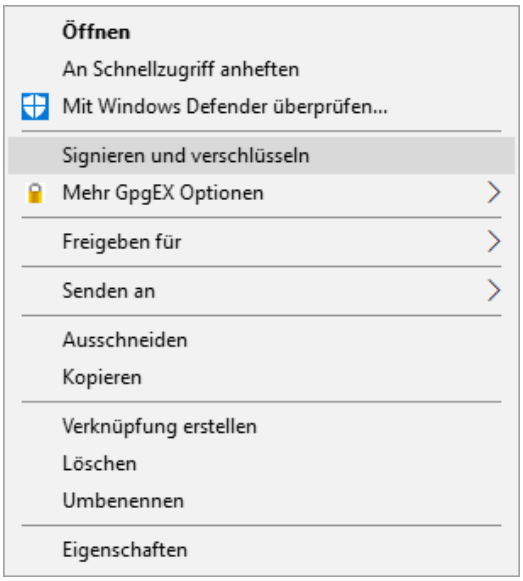
Es werden stets nur konforme Schlüssel und Zertifikate erstellt. In den erweiterten Optionen bei der Schlüsselerstellung sind keine nicht-konformen Algorithmen und Schlüssellängen auswählbar.



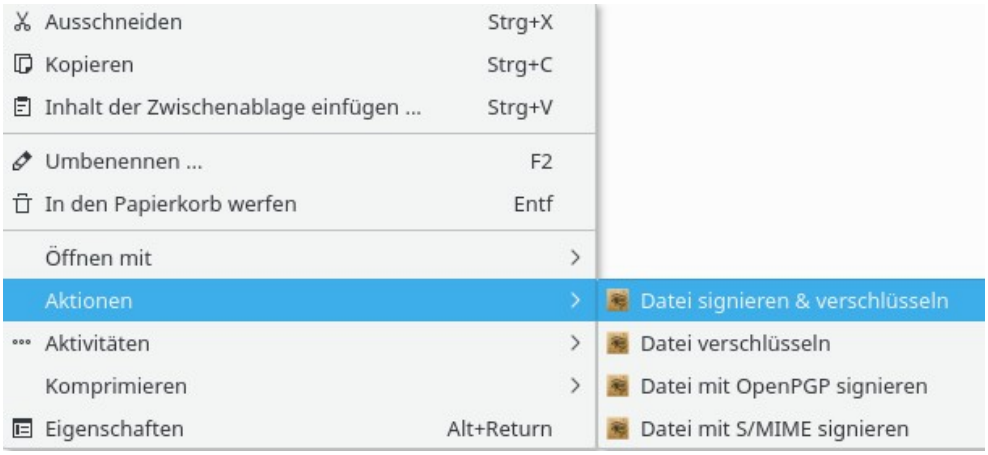
3.4 Datei-Verschlüsselung

Dateien können über das Rechtsklick-Menü im Windows Explorer ver- und entschlüsselt werden. Die Entschlüsselung kann auch mit einem Doppelklick angestoßen werden.

Signieren und verschlüsseln im Windows Explorer:

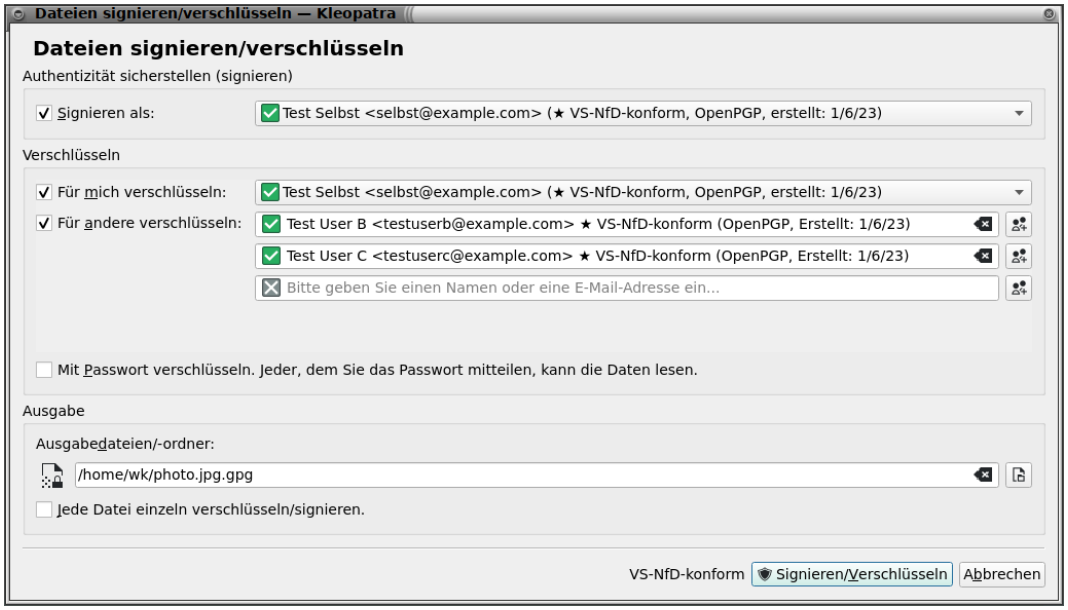


Signieren und verschlüsseln im KDE Dolphin Dateimanager:

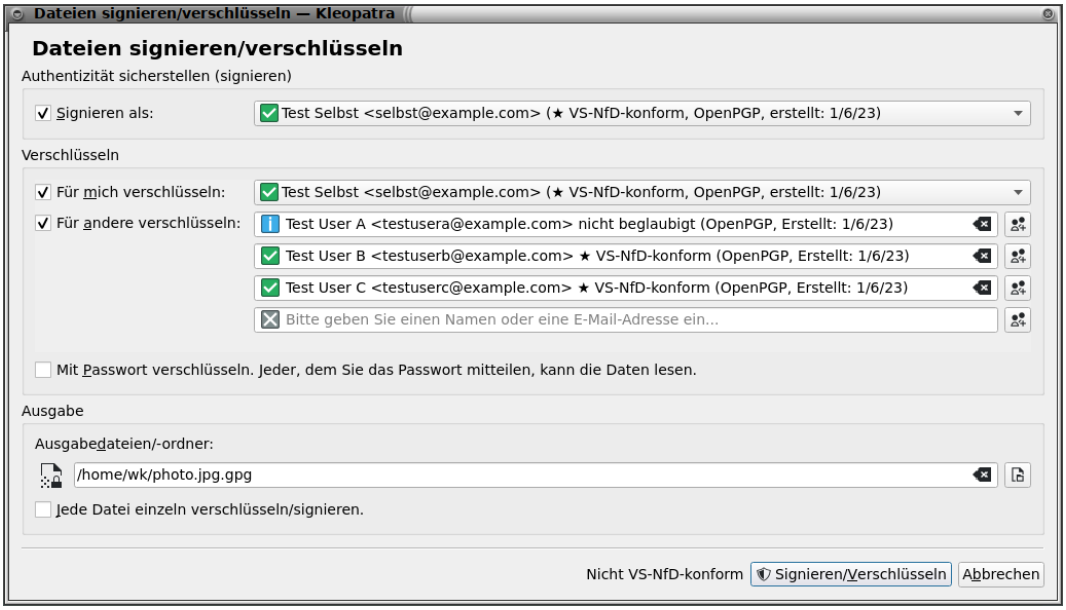


Wenn Dateien verschlüsselt werden und alle Empfänger der Datei die **konforme** Verschlüsselung unterstützen, wird das im entsprechenden Verschlüsselungsdialog unten angezeigt. Zudem ist der Bestätigungsknopf hellgrün gefärbt, um die visuelle Wirkung des Icons zu unterstreichen.

Der Dialog wird sowohl für S/MIME als auch für OpenPGP verwendet. Eine Kombination beider Verfahren ist möglich. Die folgenden Screenshots beziehen sich sowohl auf Windows als auch auf GNU/Linux Systeme.

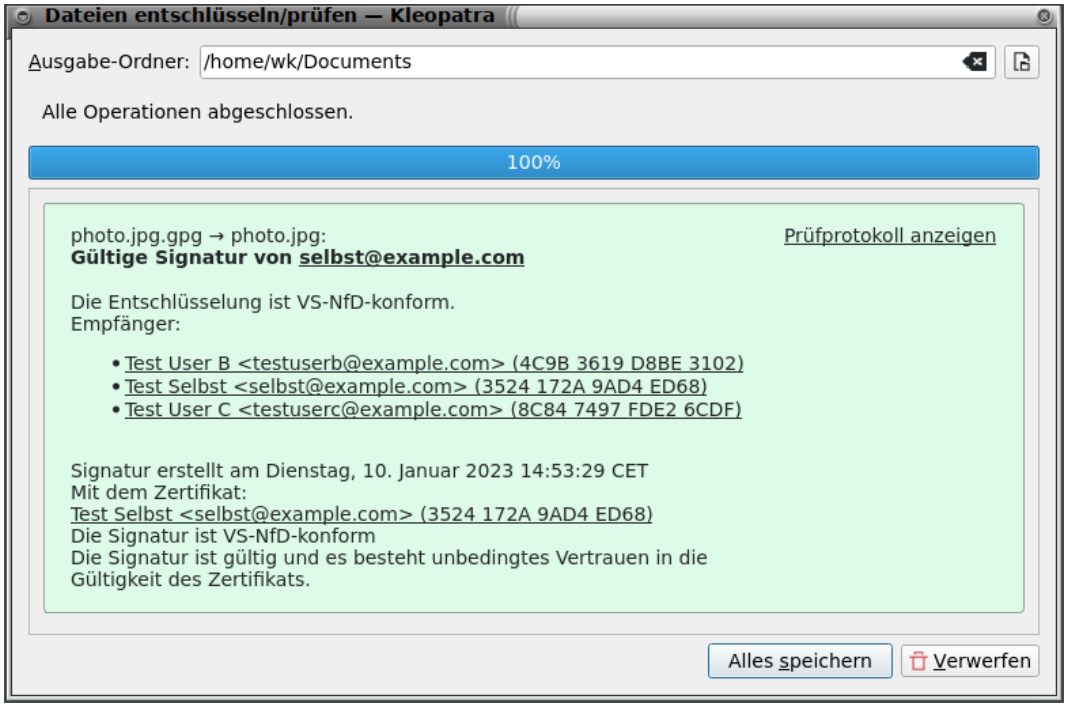


Verwenden Empfängerschlüssel **nicht-konforme** Verschlüsselungs-Algorithmen, wird dies ebenfalls im Verschlüsselungsdialog unten angezeigt.

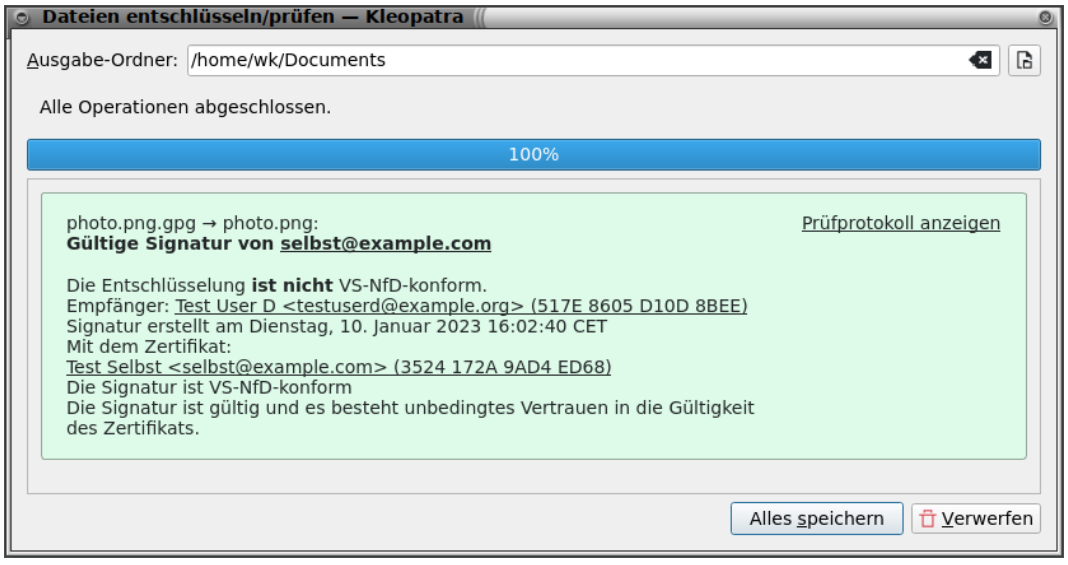


3.5 Datei-Entschlüsselung

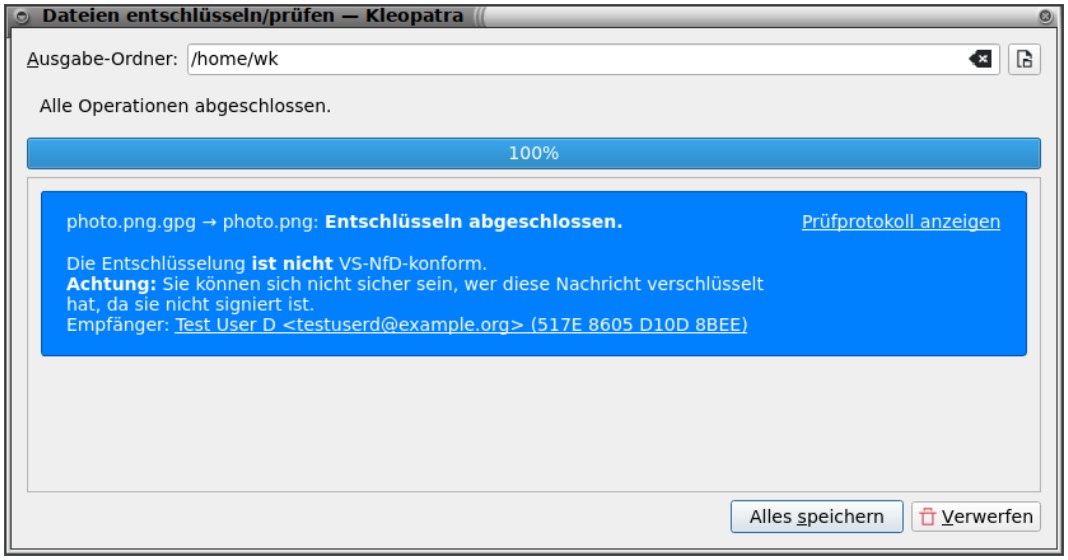
Beim Entschlüsseln einer Datei, die **konform** verschlüsselt wurde, wird dies in der abschließenden Übersicht erwähnt.



Wenn eine Datei **nicht-konform** verschlüsselt wurde, wird darauf hingewiesen. Im folgenden Bild wurde eine konforme Signatur verwendet, aber eine nicht-konforme Verschlüsselung.



Im folgenden Bild wurde keine Signatur verwendet, sowie eine nicht-konforme Verschlüsselung.

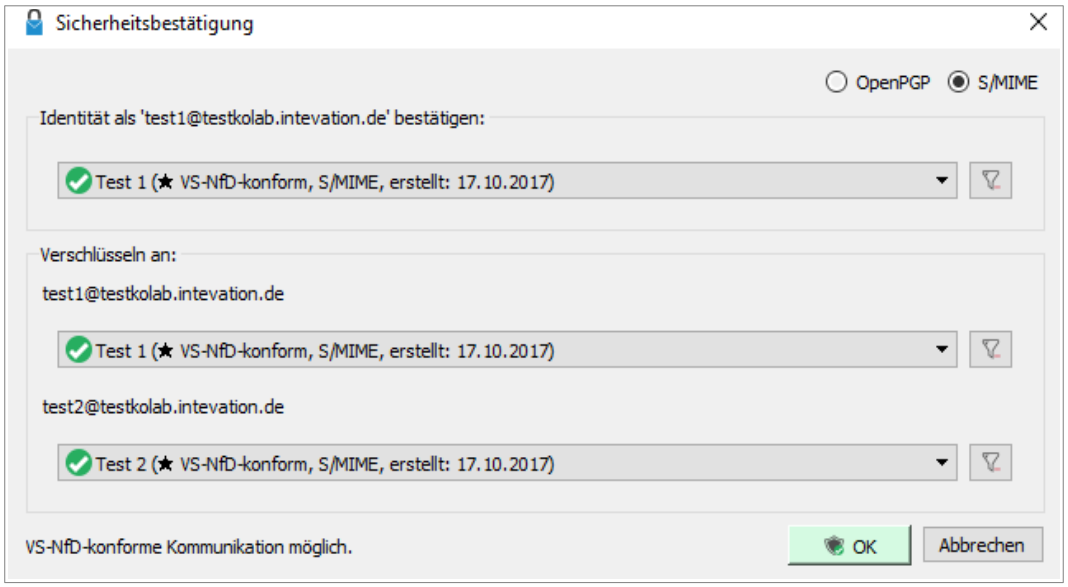


3.6 Signaturerstellung und Signaturprüfung

Der Dialog für die Ver- und Entschlüsselung wird ebenfalls bei der Signaturerstellung und -prüfung verwendet. Die Darstellung der VS-Konformität der Signaturnutzung ist somit exakt gleich wie bei der Ver- und Entschlüsselung.

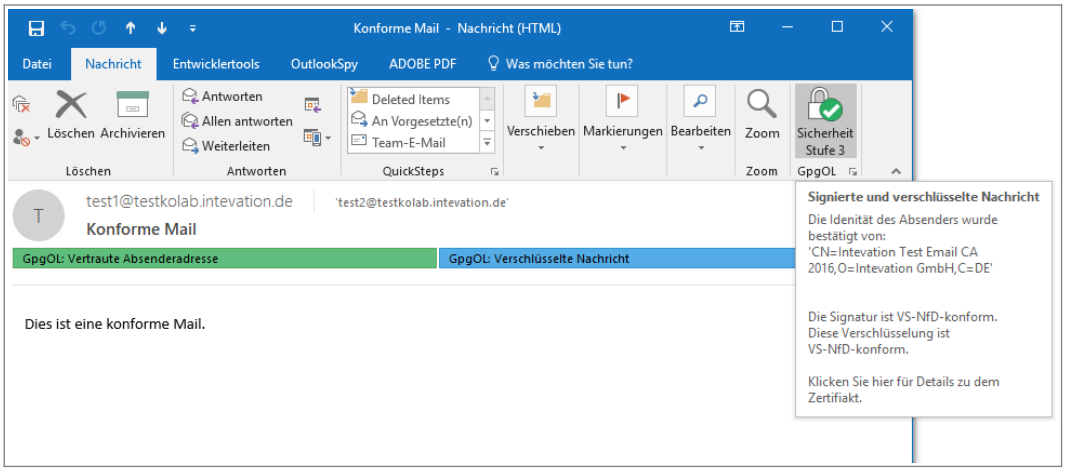
3.7 E-Mail-Verschlüsselung mit dem Outlook-Plugin GpgOL

Bei der Zertifikatsauswahl in GpgOL wird ebenso auf konforme bzw. nicht-konforme Kommunikation hingewiesen.

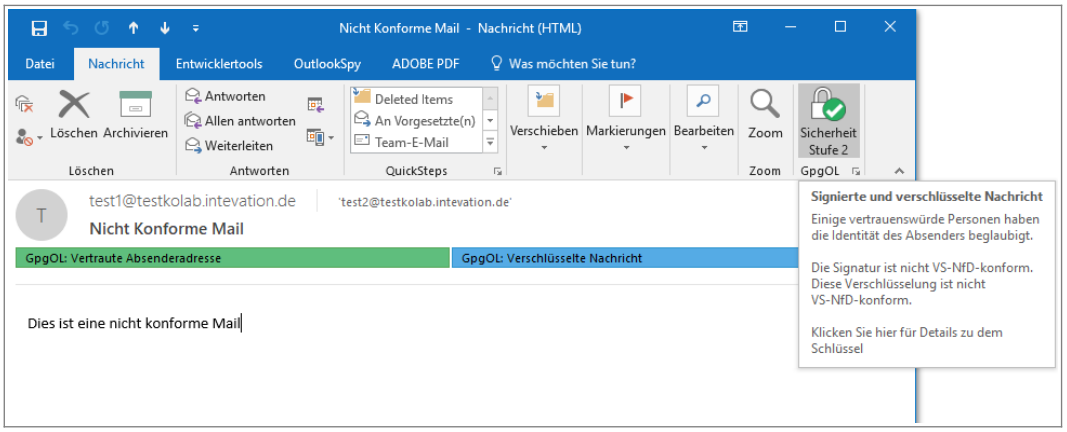


3.8 E-Mail-Entschlüsselung mit dem Outlook-Plugin GpgOL

Bei der Signaturprüfung und Entschlüsselung erreicht eine **konforme** E-Mail mindestens die GpgOL-Sicherheitstufe 3 (von vier Stufen). Details dazu werden im Tooltip angezeigt.



Eine **nicht-konforme** E-Mail kommt in GpgOL nicht über die Sicherheitsstufe 2 hinaus.



Eine detaillierte technische Beschreibung der einzelnen Sicherheits- und Vertrauenstufen in GpgOL finden Sie unter: https://gnupg.com/20200629-vertrauensstufen.html

3.9 Verwendung von Smartcards

Für den Betrieb gemäß der Zulassung sind die dort aufgeführten Smartcards zu verwenden. Beim Betrieb gemäß der Freigabeempfehlung können optional andere vom Hersteller empfohlene Smartcards verwenden werden.

Die Benutzung von Smartcards wird in der Dokumentation des Herstellers erläutert.