datenschutz cert

Version 1.3
März 2014

Merkblatt: Sichere E-Mail-Kommunikation zur datenschutz cert GmbH

1. Relevanz der Verschlüsselung

E-Mails lassen sich mit geringen Kenntnissen auf dem Weg durch die elektronischen Netze leicht mitlesen oder verändern. Daher ist das Verschlüsseln Ihrer E-Mails, gerade bei vertrauenswürdigen Inhalten, sehr wichtig.

Aus diesem Grund möchten wir Ihnen mit diesem Dokument einen kleinen Überblick verschaffen, wie Sie möglichst einfach vertraulich mit der datenschutz nord GmbH per E-Mail kommunizieren können.

Dazu schlagen wir vor, dass weit verbreitete GnuPG-Verfahren (GNU Privacy Guard) zu nutzen, wobei nach Absprache natürlich auch andere kryptographische Verfahren zur sicheren Kommunikation möglich sind. GnuPG ist ein asymmetrisches Verfahren und wurde als freie Alternative zum bekannten Quasi-Standard PGP (Pretty Good Privacy) entwickelt. GnuPG stellt in diesem Kontext die Grundlage zum Ver- und Entschlüsseln von E-Mails und Dateien mit asymmetrischem Krypto-Verfahren bereit. GnuPG wird von der kostenlosen Software Gpg4win, das auf einem Windows-Betriebssystem eingesetzt werden kann, verwendet.

In diesem Dokument wird das Programm und dessen Installation, Konfiguration und Nutzung erläutert. Im Anhang finden Sie weitere Informationen über den praktischen Einsatz von asymmetrischer Kryptographie.

2. Gpg4win

Gpg4win ist eine freie Kryptografiesoftware, die das einfache Ver- und Entschlüsseln sowie Signieren von Dateien und E-Mails unter Windows erlaubt.

Die Software ist kompatibel mit Windows XP, Vista, 7 (32bit und 64bit) und 8 (32bit und 64bit). Für die Installation werden Administratorrechte benötigt.

2.1 Installation und Konfiguration von Gpg4win

Das Installationspaket Gpg4win ist auf der Projekthomepage http://www.gpg4win.de/ erhältlich. Nach dem erfolgreichen Herunterladen, starten Sie bitte dessen Installation.

Bitte beachten Sie: Das Paket Gpg4win enthält ein Plug-In namens GpgOL, das die Verschlüsselung von E-Mails direkt in Outlook 2003, 2007, 2010 und 2013 erlaubt. Aufgrund diverser Einschränkungen (bspw. keine Unterstützung von Exchange-Servern) verzichten wir auf die Nutzung dieses Plug-Ins und empfehlen stattdessen die Nutzung von GpgEX, dass die Verschlüsselung unabhängig vom verwendeten E-Mail-Clienten ermöglicht.

Bei der Selektion der Programmteile sollten ausgewählt werden:

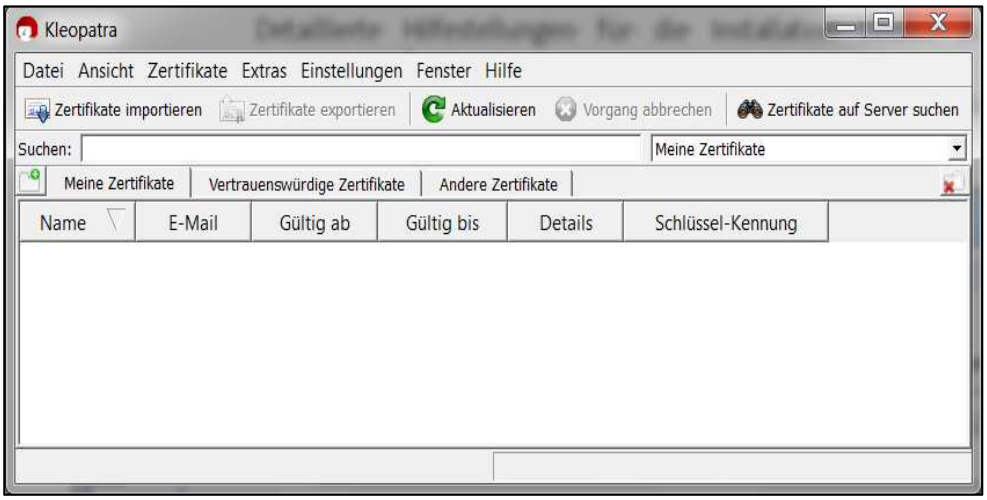
--- GnuPG – der Kern der Verschlüsselungssoftware

--- Kleopatra – eine Software zum Verwalten der Schlüssel

--- GpgEX – Verschlüsselung von Dateien direkt in Windows

Detaillierte Hilfestellungen für die Installation finden sich im Gpg4win-Kompendium online unter http://www.gpg4win.de/documentation-de.html.

Nach der Installation von Gpg4win starten Sie bitte über das Windows Startmenü die Schlüsselverwaltung Kleopatra.



2.2 Erstellen eines eigenen Schlüsselpaares

Zur sicheren Kommunikation wird zuerst ein eigenes Schlüsselpaar benötigt. Dieses besteht aus dem öffentlichen Schlüssel (kann gefahrlos publik gemacht werden) und dem privaten Schlüssel (darf nur dem Besitzer bekannt sein).

Wählen Sie in Kleopatra über das Menü „Datei“ den Punkt „Neues Zertifikat“ und dort die Option „Persönliches OpenPGP-Schlüsselpaar erzeugen“ aus.

Im nun gestarteten Assistenten tragen Sie Ihren eigenen Namen und Ihre E-Mail-Adresse ein. Die erweiterten Einstellungen können auf den Standardwerten belassen werden. Anschließend bestätigen Sie Ihre Angaben durch Klick auf „Weiter“.

Im nächsten Fenster müssen die Daten von Ihnen bestätigt werden und die Schlüsselerstellung beginnt dann durch Klick auf „Schlüssel erzeugen“.

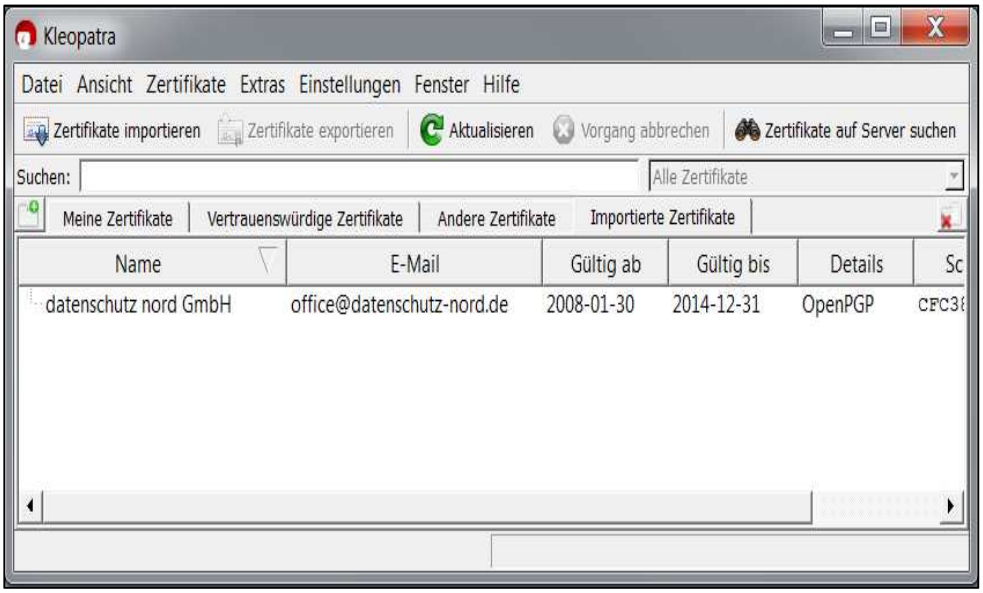
Während der Schlüssel erzeugt wird, erscheint ein Fenster zur Eingabe des Passworts. Diese wird zur Benutzung des privaten Schlüssels benötigt und sollte entsprechend sicher gewählt werden, d.h. es sollten mindestens 8 Zeichen, Klein- und Großbuchstaben sowie Zahlen und Sonderzeichen verwendet werden.

Nach kurzer Zeit sind die Schlüssel erfolgreich erstellt. An dieser Stelle sollte auf jeden Fall die Möglichkeit genutzt werden, eine Sicherheitskopie des privaten Schlüssels zu erstellen und diese auf einem externen Medium (USB-Stick o.ä.) zu sichern.

2.3 Import unseres öffentlichen Schlüssels

Der öffentliche Schlüssel der datenschutz cert GmbH kann auf unserer Homepage http://www.datenschutz-cert.de/ueber-uns/ unter „Ansprechpartner“ heruntergeladen werden.

Nachdem die Datei auf dem eigenen Computer gespeichert wurde, wird in Kleopatra im Menü „Datei“ der Punkt „Zertifikate importieren“ gewählt und im erscheinenden Dialog die gerade heruntergeladene Datei ausgewählt.



Damit sind alle notwendigen Vorbereitungen zum erfolgreichen verschlüsselten Versand von Daten an uns abgeschlossen.

3. Nutzung von GpgEX

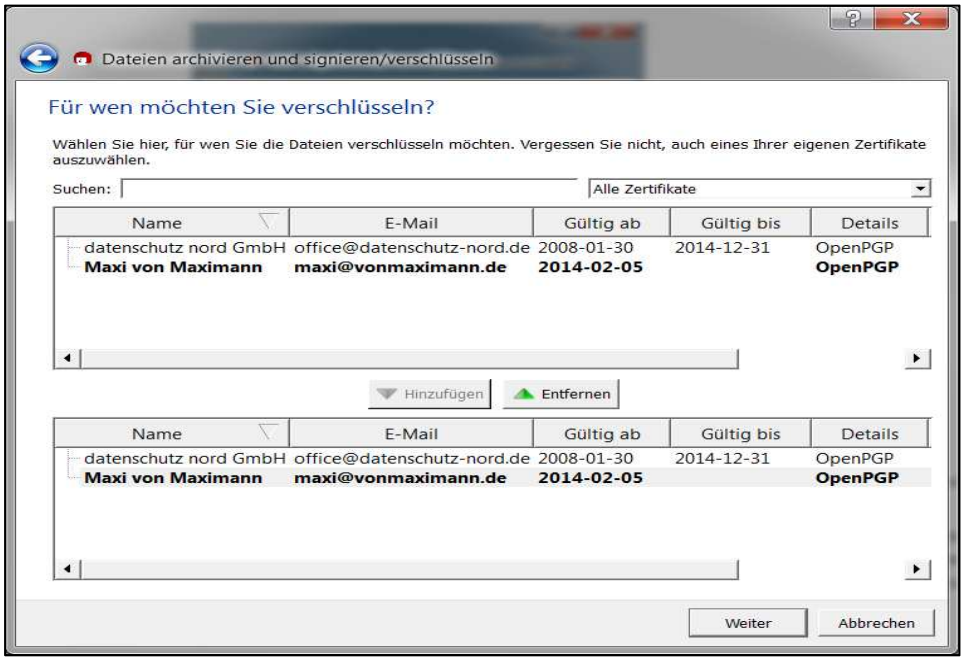
GpgEX ist eine Erweiterung von Gpg4win, die das Ver- und Entschlüsseln von Dateien direkt in Windows möglich macht.

Eine mit GpgEX verschlüsselte Datei kann auf jedem gewünschten Weg, z.B. per E-Mail oder USB-Stick, einem Kommunikationspartner übermittelt werden.

3.1 Verschlüsseln einer Datei

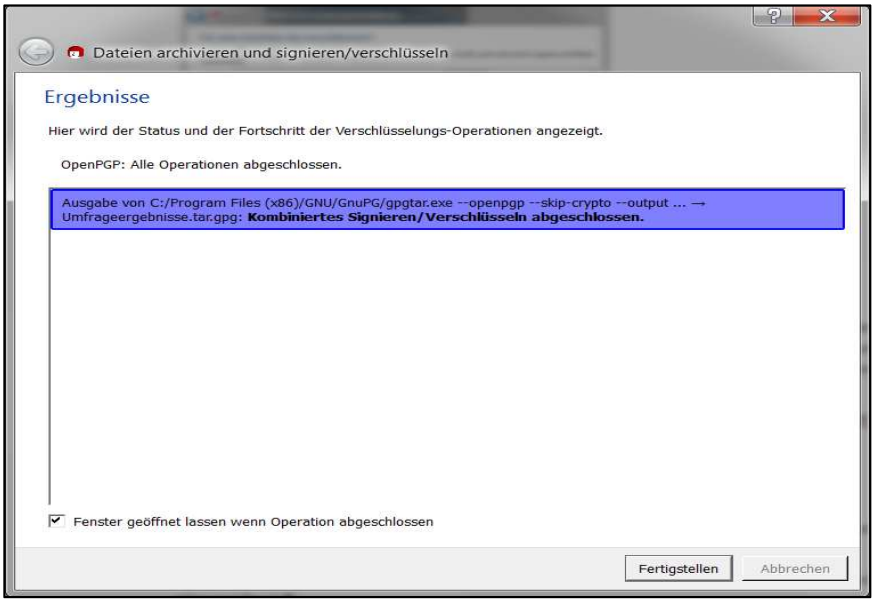
Zum Verschlüsseln einer Datei unter Windows reicht es aus, diese mittels Rechtsklick anzuwählen (z.B. auf dem Desktop) und im Kontextmenü den Punkt „Signieren und verschlüsseln“ auszuwählen.

Der nächste Bildschirm wird mit „Weiter“ bestätigt.



Daraufhin erscheint die Auswahl der „Zielschlüssel“ – also die Schlüssel der Personen, die die Datei später entschlüsseln können sollen. Hier ist es wichtig, auch den eigenen Schlüssel zu wählen, wenn man die Datei später selbst auch entschlüsseln können möchte.

Nach der Auswahl bestätigen Sie mit „Weiter“ – daraufhin beginnt der Verschlüsselungsprozess. Sobald dieser beendet ist, kann das Fenster geschlossen werden und es findet sich eine Datei mit dem Dateinamen der zu verschlüsselnden Datei und einem angehängten „.gpg“ im gleichen Verzeichnis.

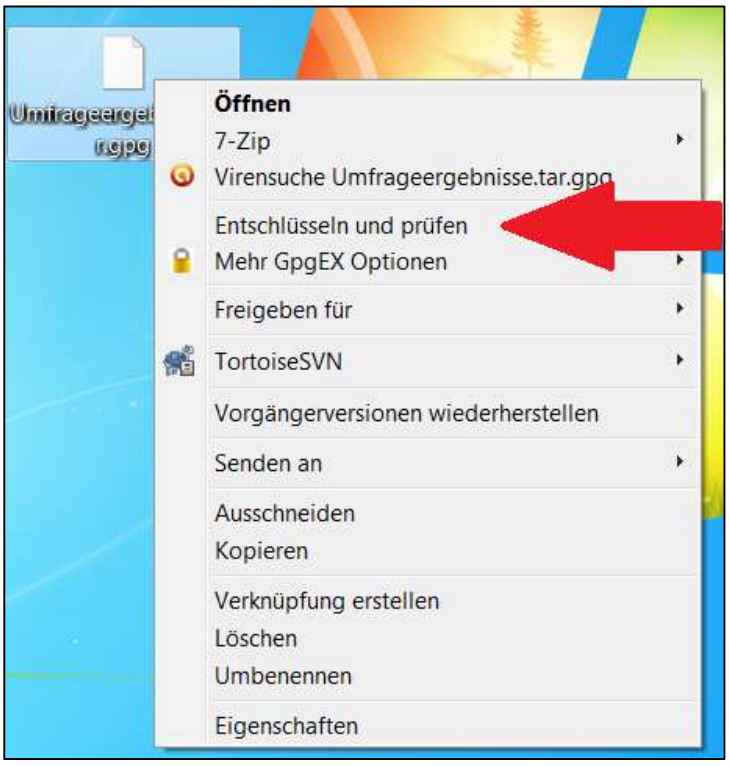


Diese Datei kann nun auf jedem beliebigen Weg sicher an den Empfänger übermittelt werden.

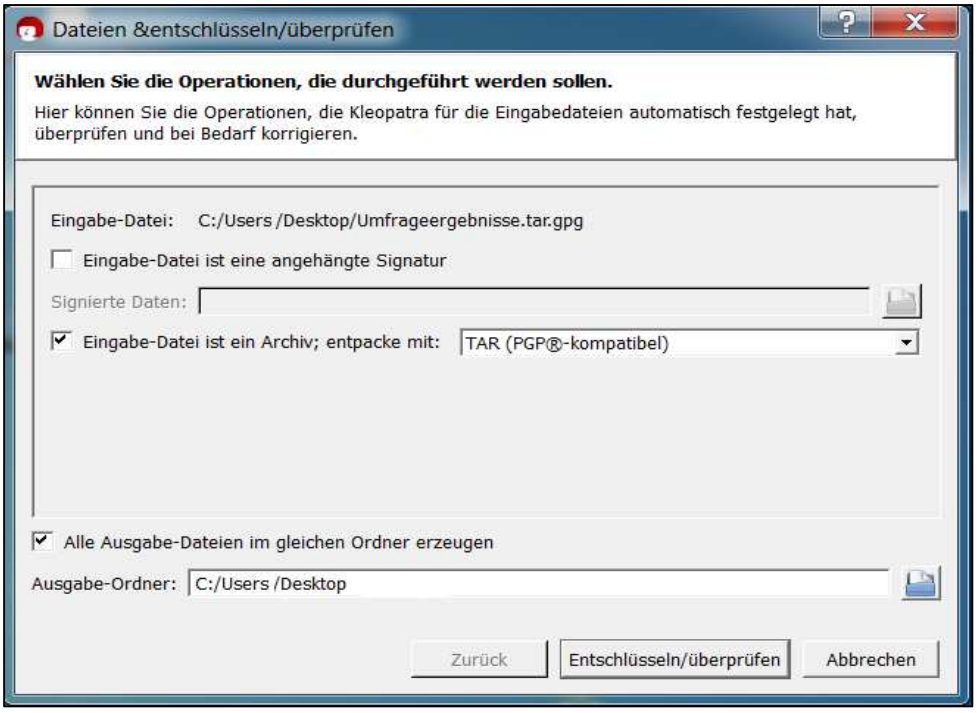
3.2 Entschlüsseln einer Datei

Wenn Sie eine verschlüsselte Datei erhalten, kann das Entschlüsseln auf ähnlichem Weg wie unter 3.1 erfolgen.

Klicken Sie die zu entschlüsselnde Datei mit Rechtsklick an und wählen im Kontextmenü „Entschlüsseln und überprüfen“.



Bestätigen Sie den ersten Dialog mit einem Klick auf „Entschlüsseln“, daraufhin fordert Sie eine Dialogbox zur Eingabe Ihres Passworts auf. Die entschlüsselte Datei wird daraufhin im selben Ordner wie die Originaldatei abgelegt.



Anhang: Exkurs zum Thema „Verschlüsselung“

Verschlüsselungssysteme unterscheidet man generell in symmetrische und asymmetrische Verfahren. Der namensgebende Unterschied besteht darin, dass bei symmetrischen Verfahren derselbe Schlüssel für die Verschlüsselung und die Entschlüsselung verwendet wird. Beide Vorgänge sind daher in gewissem Sinne symmetrisch zueinander. Asymmetrische Verfahren besitzen dagegen ein Schlüsselpaar. Verschlüsselt man eine Nachricht mit dem einen Schlüssel dieses Paares, so lässt sie sich nicht mit demselben Schlüssel wieder entschlüsselt. Dies ist ausschließlich mit dem zweiten Schlüssel dieses Paares möglich. Hierbei sind die Rollen der beiden Schlüssel theoretisch beliebig vertauschbar. In der Praxis aber bestimmt man einen Schlüssel als privaten Schlüssel (private key). Dieser wird geheim gehalten. Den anderen bezeichnet man als öffentlichen Schlüssel (public key) und gibt diesen an seine Kommunikationspartner weiter.

Die Kommunikation in der Praxis

Wenn Sie Ihrem Kommunikationspartner eine verschlüsselte E-Mail senden möchten, verschlüsseln Sie diese E-Mail mit seinem öffentlichen Schlüssel. Diese Chiffre ist nun ausschließlich mit dem zweiten Schlüssel aus dem entsprechenden Schlüsselpaar zu entschlüsseln. Dieser zweite Schlüssel ist sein privater Schlüssel, den nur er kennt.

Die aktuell verwendeten Krypto-Verfahren, wie die Hashfunktionen SHA-256, SHA-384 und SHA-512 mit jeweils 256 – 512 Bit lang erzeugten Hashwerten und die asymmetrischen Verfahren RSA und DAS mit mindestens 2048 - 4096 Bit lang erzeugten Schlüssel, sind gegenwärtig als sicher zu erachten. Dadurch ist es praktisch nicht möglich, aus dem öffentlichen Schlüssel Ihren privaten Schlüssel zu berechnen oder eine verschlüsselte E-Mail ohne den zugehörigen privaten Schlüssel zu entschlüsseln.

Darüber hinaus kann man die GnuPG-Schlüssel verwenden, um eine E-Mail digital zu signieren. Auf diese Weise kann man die Authentizität und die Integrität einer E-Mail überprüfen. Hierfür wird mit einer sogenannten Hashfunktion eine Prüfsumme über den Inhalt der E-Mail gebildet und diese mit dem privaten Schlüssel verschlüsselt. Der Empfänger, der im Besitz des öffentlichen Schlüssels ist, kann die verschlüsselte Prüfsumme entschlüsseln. Hierdurch wird Ihre Identität verifiziert, da nur Sie – im Besitz des privaten Schlüssels – in der Lage waren, die Prüfsumme mit diesem Schlüssel zu verschlüsseln. Außerdem kann der Empfänger nun ebenfalls die Prüfsumme über den Inhalt der E-Mail generieren und mit der von Ihnen verschlüsselten Prüfsumme vergleichen. Auf diese Weise wird überprüft, dass der Inhalt der E-Mail nicht manipuliert worden ist.

Um die Herkunft eines öffentlichen Schlüssels überprüfen zu können, bedient man sich eines sogenannten Fingerprints (Fingerabdruck). Dies ist ein Hashwert über den öffentlichen Schlüssel. Dieser Fingerprint ist deutlich kürzer als der Schlüssel selbst und lässt sich daher leicht z. B. telefonisch mitteilen und abgleichen. Eine Alternative sind die sogenannten Zertifikate, in denen eine vertrauenswürdige Instanz die Verbindung von öffentlichem Schlüssel zum Schlüsselinhaber bestätigt.

Für die sichere Kommunikation ist damit der öffentliche Schlüssel des jeweiligen Empfängers notwendig. Der Austausch der öffentlichen Schlüssel lässt sich auf verschiedene Weise realisieren. So kann dies z.B. über E-Mails erfolgen oder über persönlichen Austausch auf einem Datenträger – beispielsweise einem USB-Stick. Außerdem gibt es sogenannte Schlüsselserver, die die Möglichkeit bieten, seinen eigenen öffentlichen Schlüssel abzulegen, so dass jeder auf diesen Zugriff hat.

Zusammenfassung

Zum Verschlüsseln einer E-Mail verwenden Sie den öffentlichen Schlüssel Ihres Kommunikationspartners. Ausschließlich dieser ist in der Lage, die Nachricht zu entschlüsseln. Auf diese Weise ist eine vertrauliche Kommunikation möglich.

Zum Signieren von E-Mails verwenden Sie Ihren eigenen privaten Schlüssel. Ihr Kommunikationspartner, der im Besitz Ihres öffentlichen Schlüssels ist, kann die Integrität und die Authentizität der E-Mail überprüfen.

Grundsätzlich ist dabei wichtig, dass Sie sicherstellen, dass der Schlüssel tatsächlich zum behaupteten Kommunikationspartner gehört: Die Authentizität stellen Sie beispielsweise dadurch fest, dass der Schlüssel durch einen anderen Schlüssel, dem Sie vertrauen, signiert wurde, oder dass Sie mit Ihrem Kommunikationspartner den Fingerprint telefonisch abgleichen.