

Emailschlüssel - Anleitung

Um eine „Ende zu Ende Verschlüsselung“ des Emailverkehrs zwischen unserem Büro und den Mandanten sicherzustellen, müssen folgende Voraussetzungen erfüllt werden:

Diese Anleitung wurde mit freundlicher Quellenfreigabe von all-inkl.com erstellt.

Sie benötigen zwingend das kostenlose Programm Gpg4win von www.gpg4win.org

Nach der Installation öffnen Sie das mitinstallierte Programm Kleopatra.

Klicken Sie auf Neues Schlüsselpaar.

Tragen Sie unter Name Ihren Namen ein und unter E-Mail Ihre E-Mail-Adresse. Diese Informationen verwenden Sie als Identifizierung.

Klicken Sie anschließend auf Erweiterte Einstellungen ...

Wählen Sie unter RSA jeweils eine Schlüssellänge von 4096 Bit aus.

Klicken Sie danach auf OK und erstellen.

Sie haben nun die Möglichkeiten eine Sicherheitskopie des Schlüsselpaares zu erstellen, den öffentlichen Schlüssel per E-Mail zu versenden oder an einen Verzeichnisdienst zu übermitteln.

Um einen öffentlichen Schlüssel später zu erstellen, wählen Sie Ihren Schlüssel aus (markieren) und klicken Sie auf Datei -> Exportieren

Diesen öffentlichen Schlüsseln benötigen wir von Ihnen per offener Mail!

Wenn Sie einen öffentlichen Schlüssel von uns bekommen haben, reicht es, diesen nach Installation der genannten Programme per Doppelklick hinzuzufügen.

Sie müssen nur den Schlüssel beglaubigen, also prüfen, ob der Schlüssel wirklich von der Person, also von uns aus dem Büro ist.

Klicken Sie auf Ja und schon können Sie mit uns per Mail hochverschlüsselt kommunizieren.

Die komplette Anleitung inkl. Bildstrecke finden Sie unter folgendem Link:

https://all-inkl.com/wichtig/anleitungen/programme/e-mail/pgp-verschluesselung/installation-unter-windows_512.html