

Kurzanleitung zur Email-Verschlüsselung mittels SMIME in Outlook

Hintergrund:

Sie haben die Möglichkeit uns E-Mails verschlüsselt zu schicken (sog. SMIME Verfahren).

Hierfür benötigen Sie ein bestimmtes Zertifikat, d.h. eine Art digitales Ausweis. Mit dem Ausweis erhalten Sie einen **öffentlichen Schlüssel** und einen **privaten Schlüssel**. Der öffentliche Schlüssel muss Ihrem Korrespondenzpartner zur Verfügung gestellt werden. Mit diesem öffentlichen Schlüssel kann Ihr Korrespondenzpartner eine E-Mail an Sie verschlüsseln. Diese E-Mail kann dann nur der Korrespondenzpartner wieder mit seinem privaten Schlüssel entschlüsseln.

Wir übersenden Ihnen unsere öffentlichen Schlüssel, damit Sie Ihre E-Mails an uns verschlüsseln können. Damit wir Ihnen verschlüsselte Antworten schicken können, benötigen wir Ihren öffentlichen Schlüssel.

Voraussetzung zur Verschlüsselung:

Voraussetzung um uns verschlüsselte E-Mails zu senden:

- Ihr E-Mailprogramm unterstützt das Verschlüsselungsverfahren SMIME (z.B. Microsoft Outlook ab Version 2010).
- Sie haben unseren öffentlichen Schlüssel (des jeweiligen ieMitarbeiters) in Ihrem E-Mailprogramm gespeichert*.

Voraussetzung um Ihnen verschlüsselte E-Mails schicken zu können:

- Ihr E-Mailprogramm unterstützt das Verschlüsselungsverfahren SMIME (z.B. Microsoft Outlook ab Version 2010).
- Sie verfügen über ein entsprechendes Zertifikat (öffentlicher Schlüssel).
- Sie haben uns Ihren öffentlichen Schlüssel geschickt.

Sollten Sie noch nicht über ein Zertifikat verfügen, so muss dieses zuerst beantragt und eingerichtet werden. schmidt IT führt diesen Schritt gerne für Sie aus.

Für die Einrichtung eines Schlüssels für Sie benötigen wir im Normalfall nur wenige Stunden.

Die Kosten für ein Zertifikat von unserem Partner liegen bei einer Laufzeit von 3 Jahren bei 129,00€ netto. Die Beauftragung, Einrichtung sowie eine kurze Einweisung in die Handhabung übernehmen wir gerne für Sie. Hierfür erheben wir eine Einrichtungspauschale von 99,00€ netto.

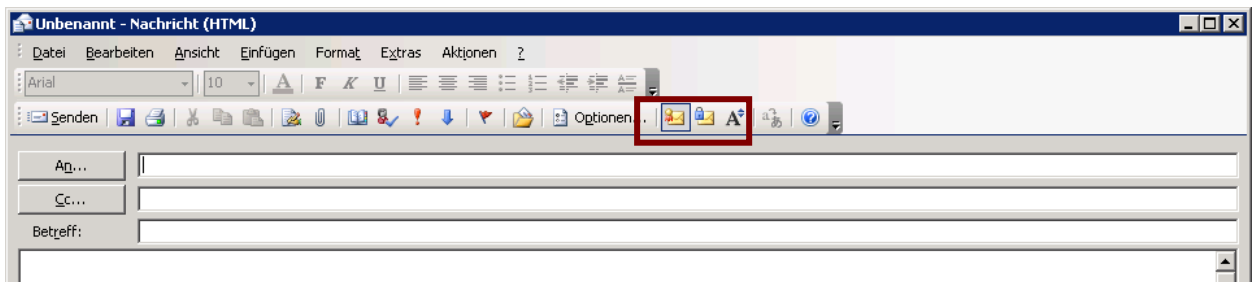
** Die Speicherung erfolgt bei verschiedenen E-Mailprogrammen unterschiedlich. Bei neueren Outlook-Versionen erfolgt die Speicherung automatisch. Wenn die Speicherung nicht automatisch erfolgt, müssen Sie den Schlüssel manuell extrahieren und speichern.*

Vorgehen - Schlüsselaustausch:

Zum Versand Ihres öffentlichen Schlüssels an Ihren Korrespondenzpartner reicht es aus, eine signierte Email an selbigen zu versenden.

Hierzu gehen Sie bitte wie folgt vor:

1. Starten Sie Outlook
2. Erzeugen Sie eine neue Email an Ihren Korrespondenzpartner
3. Sie finden nun in der Menüleiste zwei neue Symbole (siehe nachfolgenden Bildausschnitt). Diese dienen der Signatur bzw. Verschlüsselung von Emails.



4. Aktivieren Sie bitte das linke Symbol und versenden Sie die Nachricht.
5. Bitten Sie Ihren Korrespondenzpartner, Ihnen ebenfalls eine signierte Email zuzusenden.

Empfehlung:

Versenden Sie alle Email mit digitaler Signatur, damit versetzen Sie alle Ihre Korrespondenzpartner in die Lage Ihnen verschlüsselte Nachrichten zuzusenden!

Vorgehen – Versand verschlüsselter Email:

Zum Versand einer verschlüsselten Email gehen analog des obigen Punktes vor, aktivieren jedoch das rechte Icon mit dem blauen Schloss.

Outlook prüft nun bei Versand der Nachricht, ob alle Voraussetzungen zum Versand als verschlüsselte Nachricht erfüllt sind.

Ist dies der Fall so wird die Nachricht verschlüsselt versendet und kann ausschließlich vom gewählten Empfänger entschlüsselt werden.

Tritt bei der Prüfung in Outlook ein Fehler auf so erscheint ein Hinweisfenster, welches Sie darüber informiert dass ein verschlüsselter Versand nicht möglich ist – prüfen Sie in diesem Fall bitte, ob alle genannten Voraussetzungen erfüllt sind.