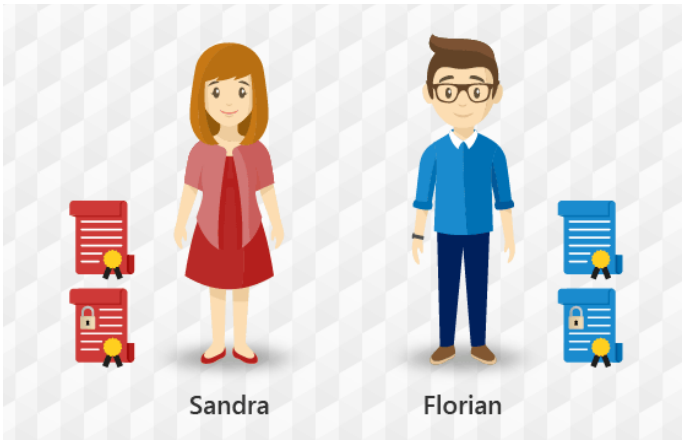
E-Mail-Verschlüsselung mit S/MIME



S/MIME (Secure Multipurpose Internet Mail extensions)

Private key (privater Schlüssel) des Absenders

wird vom Absender zum Signieren einer E-Mail benötigt. Er ist passwortgeschützt und wird nie weitergegeben. Er befindet sich nur auf dem PC des Absenders.

Public key (öffentlicher Schlüssel) des Empfängers

wird benötigt um eine E-Mail an den Empfänger zu verschlüsseln. Dieser key wird als sogenanntes Zertifikat als E-Mail Anhang automatisch weitergegeben.

Private key (privater Schlüssel) des Empfängers

wird vom Empfänger zum Entschlüsseln einer E-Mail benötigt. Er ist passwortgeschützt und wird nie weitergegeben. Er befindet sich nur auf dem PC des Empfängers.

Public key (öffentlicher Schlüssel) des Absenders

wird vom Empfänger benötigt um zu überprüfen und verifizieren, ob eine E-Mail wirklich vom Absender, unversehrt eingetroffen ist.

Unterschied **signieren** und **verschlüsseln**

Signieren	Durch die digitale Signatur gewährleistet der Absender, dass die versendete E-Mail von ihm verfasst und beim Übermitteln nicht verändert wurde.
Verschlüsseln	Es wird gewährleistet, dass eine E-Mail vom Absender zum Empfänger mittels End-to-End-Verschlüsselung von Drittpersonen nicht geöffnet und gelesen werden kann.

1. Zuerst müssen Absender (Sandra) und Empfänger (Florian) gegenseitig ihre öffentlichen Zertifikate, die public keys, austauschen. Dies kann durch eine gegenseitige E-Mail oder via Download-Link erfolgen. Dieser Schlüssel wird jeweils in SEPPMAIL gespeichert. Beide müssen mit S/MIME arbeiten.

2. Mit ihrem private key (Zertifikat), der nur bei Ihnen gespeichert und passwortgeschützt ist, signiert der Absender Sandra ihre E-Mail.

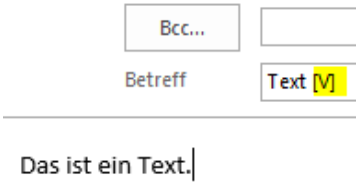
3. Mit dem public key (Zertifikat) vom Empfänger Florian wird eine E-Mail, welche der Absender Sandra erstellt, beim Versenden verschlüsselt.

4. Der Empfänger Florian entschlüsselt die E-Mail des Absenders Sandra mit seinem private key (Zertifikat), der nur bei ihm gespeichert und passwortgeschützt ist.

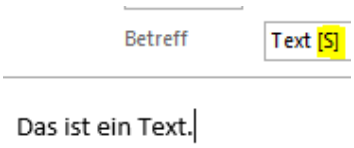
5. Florian prüft mit dem public key (Zertifikat) vom Absender Sandra, ob die E-Mail wirklich unversehrt ist und nicht manipuliert wurde.

Wie können Sie eine E-Mail verschlüsseln?

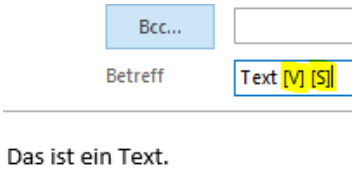
Wenn Sie in der Betreffzeile [V] einfügen, dann wird die E-Mail verschlüsselt geschickt. Der Empfänger sieht [V] nicht. Die **[ ]** erstellen Sie mit der Tastenkombination AltGr + 8 bzw. AltGr + 9



Wenn Sie in der Betreffzeile [S] einfügen, dann wird die E-Mail signiert geschickt. Der Empfänger sieht [S] nicht.



Wenn Sie in der Betreffzeile [V] [S] einfügen, dann wird die E-Mail verschlüsselt und signiert geschickt. Der Empfänger sieht [V] [S] nicht.



Wie sehen Sie, dass eine E-Mail verschlüsselt / signiert an Sie gesandt wurde?

Wenn in der Betreffzeile steht:

AW: Text [secure]

dann ist die E-Mail verschlüsselt an Sie verschickt worden.

Verschlüsselt bedeutet, dass nur der Absender und Sie als Empfänger mit Ihrem Schlüssel die E-Mail lesen können. Ohne den Schlüssel sehen Sie nur den Absender ohne Inhalt und ohne Anhang.

Wenn in der Betreffzeile steht:

AW: Text [signed OK]

dann ist die E-Mail signiert an Sie verschickt worden.

Signiert bedeutet, dass die E-Mail vom Absender, den Sie in der E-Mail sehen, auch wirklich verschickt wurde und die E-Mail auf dem Weg zu Ihnen auch nicht abgefangen oder verändert wurde.

Wenn in der Betreffzeile steht,

AW: Text [secure] und [signed ok]

dann ist die E-Mail signiert und verschlüsselt verschickt worden.