Versenden verschlüsselter E-Mails

Ab Release 3.0 ist es möglich, E-Mails zu verschlüsseln, die von PIRS gesendet oder empfangen werden.

Der Standard für die Verschlüsselung von E-Mails ist "S/MIME". Wenn Sie eine verschlüsselte E-Mail versenden möchten, müssen Sie zunächst sicherstellen, dass alle Beteiligten über eine S/MIME Public Key Infrastruktur verfügen. Es ist erforderlich, dass alle E-Mail-Empfänger S/MIME-Zertifikate besitzen und alle E-Mail-Clients S/MIME-Verschlüsselung unterstützen. Wenden Sie sich an Ihren IT-Administrator oder wenden Sie sich an Ihren Projektleiter, um sicherzustellen, dass diese Anforderungen erfüllt werden.

Verschlüsselte E-Mails senden

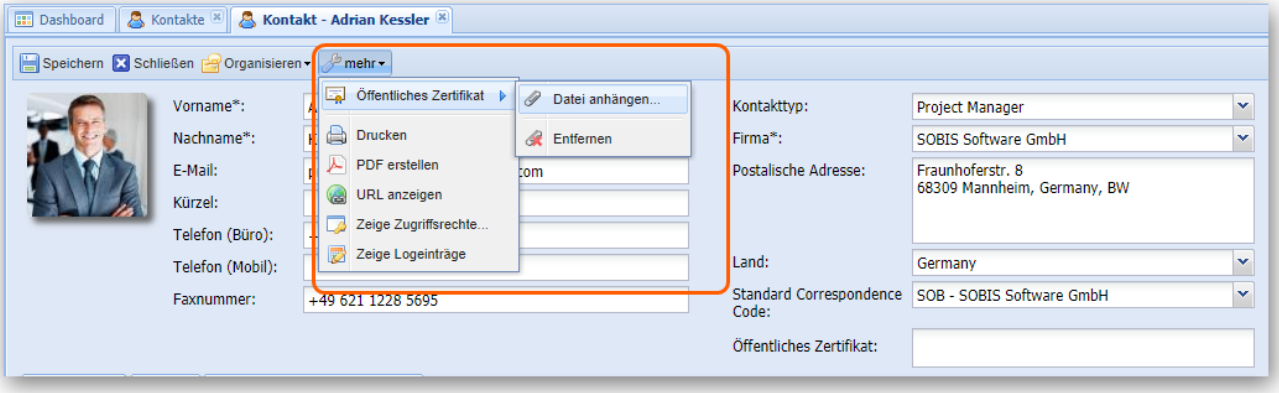
Um eine von PIRS gesendete E-Mail zu verschlüsseln, verwendet das System den öffentlichen Schlüssel des/der Empfänger(s), der hierfür im Kontaktdatensatz im PIRS-Projektadressbuch hinterlegt sein muss.

Die Verschlüsselung erfolgt während des Sendevorgangs. Die in PIRS gespeicherte E-Mail wird nicht als verschlüsseltes Dokument abgelegt, da der Zugriff auf PIRS gesichert ist und alle PIRS-Benutzer in der Lage sein sollten, E-Mails zu lesen, auf die sie in PIRS Zugriff haben.

Sollte ein öffentlicher Schlüssel für einen oder mehrere Ihrer Empfänger nicht verfügbar sein, das heißt kein öffentlicher Schlüssel in ihrem PIRS-Kontakt verfügbar sein, wird die E-Mail für keinen der Empfänger verschlüsselt.

Hochladen eines öffentlichen Schlüssels für Kontaktdatensätzen

Um den öffentlichen Schlüssel Ihrer Empfänger zu speichern, öffnen Sie den jeweiligen Kontakt im PIRS-Adressbuch und wählen Sie die Option "mehr" in Ihrer Symbolleiste. Gehen Sie zu "Öffentliches Zertifikat" und klicken Sie auf "Datei anhängen...". Sie können nun die öffentliche Schlüsseldatei des Empfängers von Ihrer lokalen Festplatte oder dem jeweiligen Server in Ihrer IT-Infrastruktur auswählen. Das Dateiformat muss mit einer ".cer"-Datei übereinstimmen.



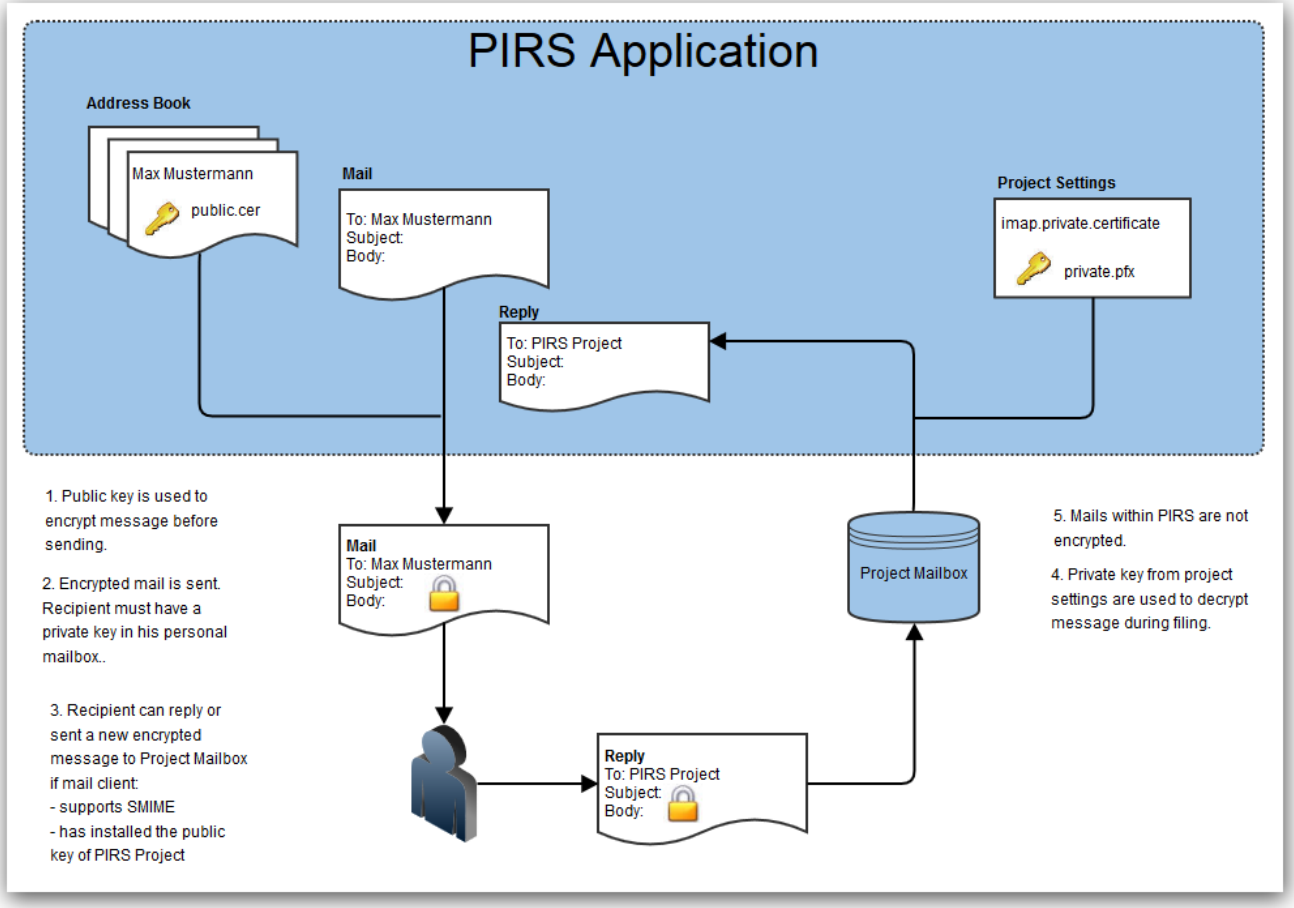
Verschlüsselte E-Mails empfangen

Eine verschlüsselte E-Mail, die Sie in Ihrer persönlichen Mailbox erhalten, kann während des Importvorgangs in PIRS nicht entschlüsselt werden. Nur verschlüsselte E-Mails, die in Ihrem Projektpostfach empfangen werden, können während des Anmeldevorgangs entschlüsselt werden.

Daher müssen alle eingehenden verschlüsselten Mails an das offizielle Projekt-Postfach gesendet werden, da sie sonst nicht entschlüsselt werden können.

Während der Ablage wird die empfangene E-Mail mit dem privaten Schlüssel des Projekt-Postfachs entschlüsselt und anschließend unverschlüsselt in PIRS gespeichert.

Verschlüsselungsprozess mit PIRS


PIRS Application
Address Book
Max Mustermann
public.cer
Mail
To: Max Mustermann
Subject:
Body:
Project Settings
imap.private.certificate
private.pfx
Reply
To: PIRS Project
Subject:
Body:
1. Public key is used to encrypt message before sending.
2. Encrypted mail is sent. Recipient must have a private key in his personal mailbox..
3. Recipient can reply or sent a new encrypted message to Project Mailbox if mail client:
- supports SMIME
- has installed the public key of PIRS Project
Mail
To: Max Mustermann
Subject:
Body:
Project Mailbox
Reply
To: PIRS Project
Subject:
Body:
5. Mails within PIRS are not encrypted.
4. Private key from project settings are used to decrypt message during filing.