

SDEncrypt Anleitung

Um ein SMIME Zertifikat für die Emailverschlüsselung zu generieren muss man die SDEncrypt.jar ausführen. Dazu wird das Java JRE benötigt. Zum Prüfen ob Java vorhanden ist, einfach folgende Webseite beachten:

https://www.java.com/de/download/help/version_manual.xml

Nach dem die SDEncrypt.jar gestartet wurde (Bild 1) muss man einfach in den vorgesehenen Textfelder Vorname, Nachname, Email Adresse und ein sicheres Passwort mit mindestens 8 Zeichen eingeben. (Für sichere Passwörter das Tool KeyPass oder Passwortgeneratoren verwenden. Oder den entsprechenden Wikiartikel befolgen:

<http://de.wikipedia.org/wiki/Passwort>)

Über den Button „Optionale Einstellungen“ kann man für sein Zertifikat weitere Parameter festlegen.

Zudem hat man die Möglichkeit das Root Zertifikat als eigene P12Datei zu speichern. Damit man weitere Zertifikate oder erneut sein eigenes Zertifikat mit demselben Root Zertifikat signieren kann. Dann muss aber auch ein entsprechendes RootPasswort festgelegt werden mit mindestens 8 Zeichen (s.o.). (Pfeile mit einer 1)

Über den Button „Root Zertifikat“ kann man die entsprechenden Einstellungen für das Root Zertifikat festlegen.

Existiert schon ein Root Zertifikat und man möchte es gerne wieder verwenden, muss man einfach über den Button „Öffnen“ entsprechend das Root Zertifikat auswählen und das dazugehörige Passwort zum Zertifikat im RootPasswort eingeben. (Pfeile mit einer 2)

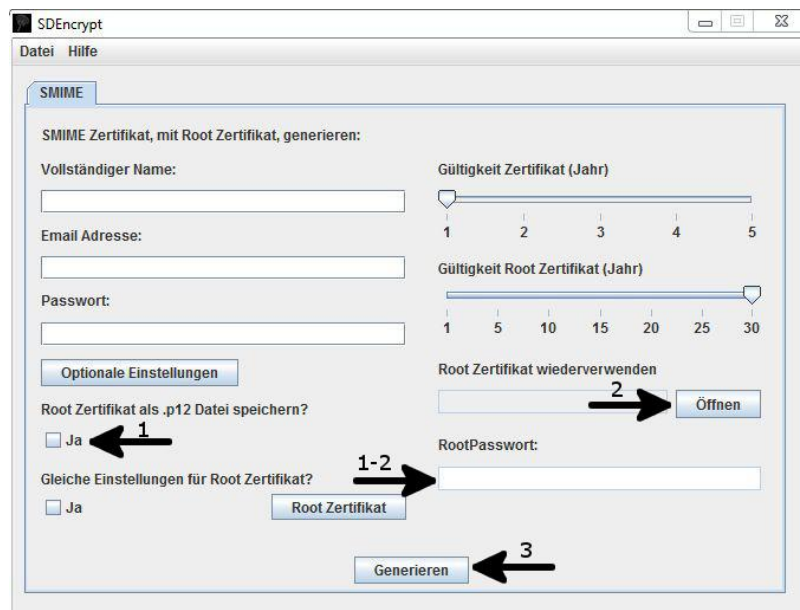


Bild 1 Hauptfenster von SDEncrypt

Wurden alle Eingaben getätigt, kann man sein Zertifikat nun über den Button „Generieren“ erstellen lassen. (Pfeil mit einer 3)

Nach dem man auf den Button gedrückt hat, erscheint ein neues Fenster mit einer Statusbar, diese zeigt an wie weit die Erstellung des SMIME Zertifikats ist. (Bild 2)



Bild 2 Fortschrittsanzeige zum SMIME generieren

Nach dem das SMIME Zertifikat erfolgreich erstellt wurde, erscheint folgender Dialog, dass das Zertifikat erfolgreich generiert wurde. (Bild 3)

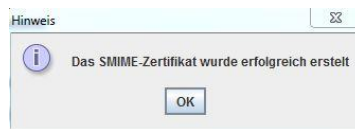


Bild 3 Erfolg beim SMIME Zertifikat erstellen

Nun befindet sich im selben Verzeichnis in dem auch die SDEncrypt.jar gespeichert ist, sowohl der private als auch der öffentliche Schlüssel. (PrivateKey.p12 = privater Schlüssel, PublicKey.p7b = öffentlicher Schlüssel, RootPrivateKey.p12 = privater Schlüssel des RootZertifikats) (Bild 4)

Name	Änderungsdatum	Typ	Größe
Max MustermannPrivateKey.p12	14.06.2015 19:52	Privater Informati...	7 KB
Max MustermannPublicKey.p7b	14.06.2015 19:52	PKCS #7-Zertifikate	3 KB
Max MustermannRootPrivateKey.p12	14.06.2015 19:52	Privater Informati...	6 KB
SDEncrypt.jar	14.06.2015 19:30	Executable Jar File	3.379 KB

Bild 4 Verzeichnisansicht

Wichtig: Nur der öffentliche Schlüssel, sprich die Datei mit der Endung PublicKey.p7b darf weitergegeben werden! Denn wird der private Schlüssel, sprich die Datei mit der Endung PrivateKey.p12 weitergegeben, kann jeder Ihre verschlüsselten Daten/Emails entschlüsseln.

⇒ **Nur öffentlicher Schlüssel (PublicKey.p7b) weitergeben!!!**

Wichtig: Beim Austauschen der öffentlichen Schlüssel sollte immer der digitale Fingerabdruck/Fingerprint mit ausgetauscht werden. (Da jedes Zertifikat einen eindeutigen digitalen Fingerprint hat). Dies soll weiterhin sicherstellen, dass keine gefälschten Zertifikate oder dass das Zertifikat auch wirklich von der Person stammt von dem man das Zertifikat bekam.

Um nun diese für SMIME zu nutzen, braucht man für Emailclients von Microsoft, wie Outlook oder LiveMail nur auf den PrivatenKey.p12 doppelklicken um das Zertifikat zu installieren. Dort einfach den Anweisungen folgen und das Passwort, dass man zuvor festgelegt hat, eintragen.

Für Thunderbird und andere Emailclients die nicht von Microsoft sind, muss man diese direkt in das jeweilige Mailprogramm importieren. Für Thunderbird sieht es wie folgt aus. Im Menüband Extras -> Einstellungen -> Erweitert -> Zertifikate -> Ihre Zertifikate und dort auf Importieren klicken. Dort den Speicherpfad des privaten Schlüssel (.p12) angeben und auf Öffnen klicken. Danach das Passwort eintragen und mit OK bestätigen. Nun ist ebenfalls das Zertifikat installiert. Jetzt muss man nur noch in den Reiter „Zertifizierungsstellen“ wechseln. Hier sucht man nach seinem entsprechenden Namen, wählt das Zertifikat aus und klickt auf „Vertrauen bearbeiten“. Dort bei alle 3 Punkten ein Häkchen setzen und mit OK bestätigen. Nur dann kann man in Thunderbird SMIME einrichten.

Danach kann man direkt in Outlook, LiveMail oder Thunderbird SMIME direkt einrichten, siehe dazu <http://cybernetz.net/smime>

Wichtig: SMIME funktioniert nur, wenn der Empfänger ebenfalls SMIME verwendet!!! Ansonsten werden die Emails unverschlüsselt übertragen.