achermann
ict-services

achermann ict-services ag
Geschäftshaus Pilatushof
Grabenhofstrasse 4
6010 Kriens

zentrale +41 41 417 11 11
support +41 41 417 11 10
www.achermann.swiss
info@achermann.swiss

Benutzerdokumentation Hosted Secure E-Mail

achermann ict-services ag
Geschäftshaus Pilatushof
Grabenhofstrasse 4
6010 Kriens

achermann
cloud services

Version 1.0
02.02.2018

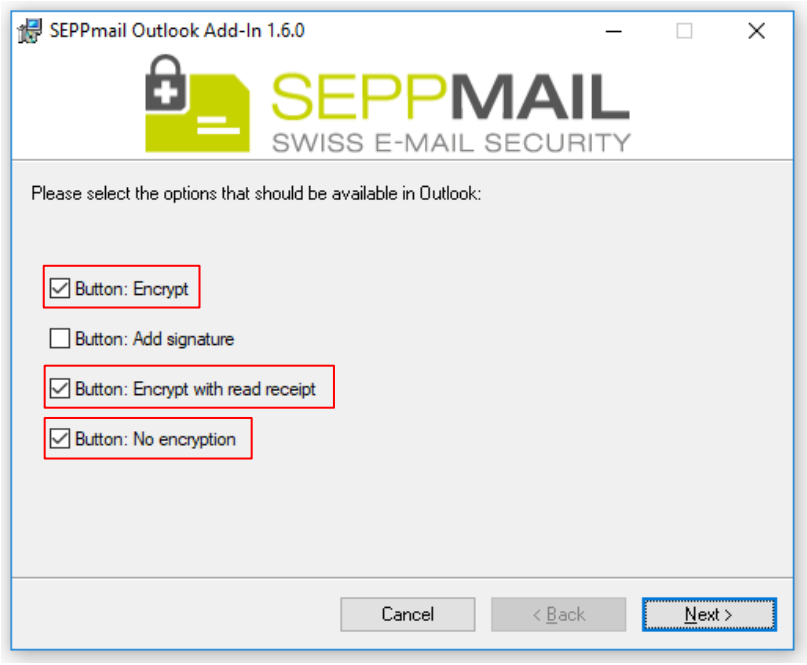
Inhaltsverzeichnis

1 Installation Outlook Add-In

Die aktuellste Version des SEPPmail Outlook Add-In steht auf der Hersteller Webseite unter der URL https://www.seppmail.ch/downloads/ -› **MS Outklook Add-In** zur Verfügung.

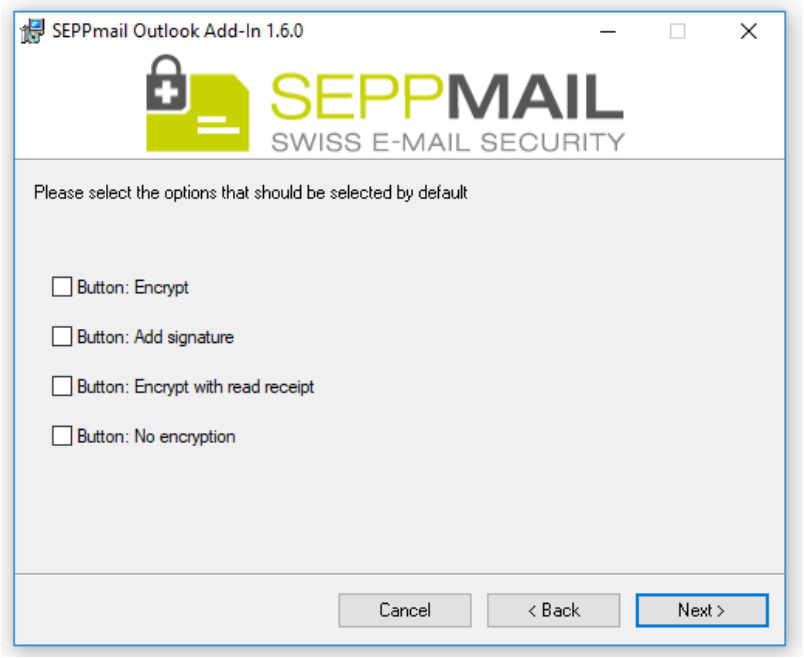
Führen Sie zur Installation die Installationsdatei **SEPPmailOutlookAddInSetup.msi** aus. Die nachfolgenden Schritte führen Sie durch den Installationsprozess:

Schritt 1: Wählen Sie beim ersten Fenster die drei rot markierten Felder aus und klicken Sie auf „Next".

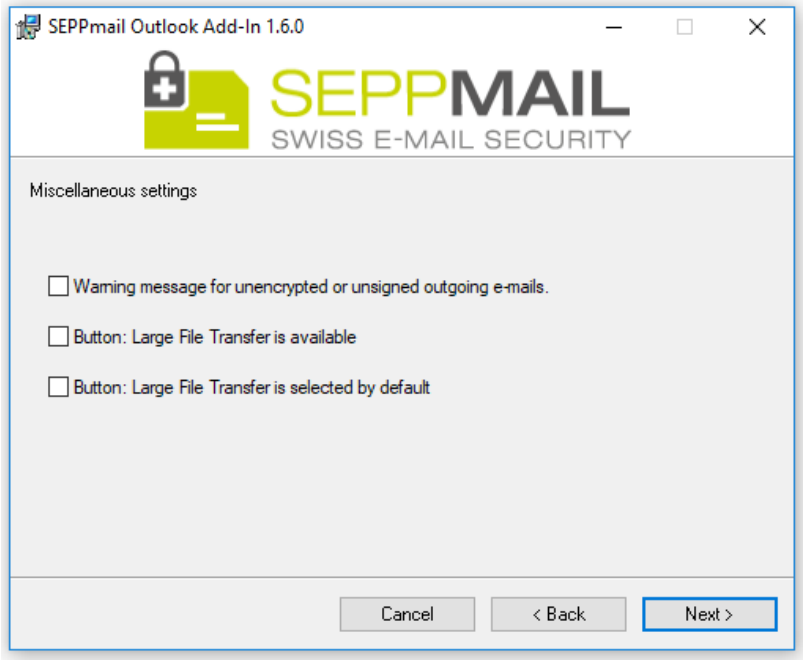


Anmerkung: Die Option **Add signature** *wird nicht benötigt. Signierung ist per default für jedes ausgehende Mail aktiviert und muss bei Bedarf deaktiviert werden. Eine forcierte Signierung ist nicht notwendig.*

Schritt 2: Wählen Sie beim 2. Fenster keine der Optionen aus und klicken Sie erneut auf „Next“.



Schritt 3: Auch beim dritten Fenster müssen keine Felder markiert werden.



Durch klicken auf **Next** wird die Installation gestartet.

Anmerkung: Nach der Installation ist ein Neustart von Outlook notwendig.

2 Funktionen im Microsoft Outlook

Durch die Installation des SEPPmail Add-In stehen in Microsoft Outlook, die folgenden E-Mail Optionen im Menüband zur Verfügung:

2.1 Verschlüsseln

Mit der Funktion **Verschlüsseln** wird die E-Mail, welche abgesendet wird, in jedem Fall verschlüsselt. Je nach vorhandenen Möglichkeiten zur Verschlüsselung, muss sich der Empfänger auf dem GINA Portal (siehe Kapitel 3) anmelden, um die Nachricht wieder entschlüsseln und somit lesen zu können.

Technische Details:

Die Verschlüsselung wird mit einer der folgenden Technologien und in dieser Priorität durchgeführt:

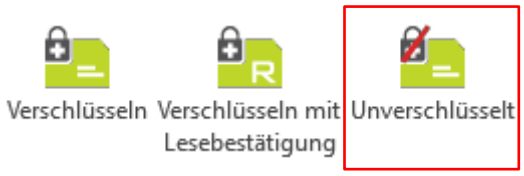
1. Geprüftes S/MIME Zertifikat des Empfängers
   ⇨ Der Empfänger kann das E-Mail ganz normal öffnen und lesen.
2. Geprüfter öffentlicher OpenPGP Schlüssel des Empfängers
   ⇨ Der Empfänger kann das E-Mail ganz normal öffnen und lesen.
3. Geprüftes S/MIME Domänen Zertifikat der Empfänger Domäne
   ⇨ Der Empfänger kann das E-Mail ganz normal öffnen und lesen.
4. Geprüfter öffentlicher OpenPGP Domänen Schlüssel der Empfänger Domäne
   ⇨ Der Empfänger kann das E-Mail ganz normal öffnen und lesen.
5. GINA mit hinterlegtem Empfängerpasswort
   ⇨ Der Empfänger meldet sich mit seinem bereits vorhandenen Login am GINA Portal an kann das E-Mail im Portal lesen und über das Portal auch verschlüsselt Antworten.
6. GINA mit Initialpasswort
   ⇨ Dem Empfänger muss ein Initialpasswort mitgeteilt werden, mit welchem er sich am GINA Portal anmelden kann. Im Portal kann er das E-Mail lesen und darüber auch verschlüsselt Antworten.

2.2 Verschlüsseln mit Lesebestätigung

Die Funktion **Verschlüsseln mit Lesebestätigung** sendet dem Absender eine garantiere Lesebestätigung. Dabei wird forciert ein GINA-Mail erstellt.

Der Versand der Lesebestätigung erfolgt durch das GINA Interface. Der Empfänger kann den Versand der Bestätigung nicht unterdrücken. Dies kann mit dem eingeschriebenen Brief beim Postversand verglichen werden.

2.3 Verschlüsselung / Signierung unterdrücken



Die Option **Unverschlüsselt** sendet das Mail unverschlüsselt. Dabei wird keine Verschlüsselung und auch keine S/MIME Signierung angewendet. Dies kann mit dem Versand einer Postkarte verglichen werden.

3 GINA Mail

GINA bietet eine sichere Möglichkeit zur Verschlüsselung, auch wenn mit dem Kommunikationspartner vorher keine Schlüssel ausgetauscht wurden und keine Domain Verschlüsselung zur Verfügung steht.

Das E-Mail wird verschlüsselt und als Anhang an ein unverschlüsseltes Trägermail angehängt. Der Anhang kann danach mit einem Passwort auf einem HTTPS gesicherten Webportal (GINA Interface) wieder entschlüsselt werden. Hat der Empfänger auf dem GINA Interface noch keinen Account, wird das Initialpasswort an den Absender zugestellt, der es über einen alternativen Kanal (SMS, Telefon etc.) an den Empfänger zustellt.

Der Empfänger kann danach auf dem GINA Portal wieder verschlüsselt auf die ursprüngliche Mail antworten.

Durch GINA ist es möglich „spontan“ (ohne Schlüsselaustausch) mit jedem E-Mail Empfänger verschlüsselte Nachrichten auszutauschen.

4 Betreff [secure]

SEPPmail ver- und entschlüsselt Mails transparent. Das bedeutet, die Ver- und Entschlüsselung von Mails erfolgt durch SEPPmail automatisch. Die Nachricht im Mail Client ist immer unverschlüsselt.

Nach der Entschlüsselung wird der Betreff mit dem Tag **[secure]** ergänzt. Dadurch ist für den Empfänger ersichtlich, ob ein Mail sicher (verschlüsselt) übertragen wurde. Beim Antworten auf ein solches E-Mail wird dieses Tag wieder entfernt, womit der Empfänger dies nie mitbekommt.