SEPPMail Benutzungs-Anleitung

Stand: 19. November 2021

Ersteller:

Gesellschaft für Digitale Werte mbH In der Marsch 12a 21339 Lüneburg

Kunde:

Lebensraum Diakonie e.V. Bein Benedikt 8a 21335 Lüneburg

Inhalt

1.	Erklärung zur SEPPMail-Instanz	. 3
2.	Benutzung	.3
	Domänenverschlüsselung	
4.	Abrufen des eigenen Zertifikats	. 4

1. Erklärung zur SEPPMail-Instanz

Es gibt zwischen dem Mailserver des Lebensraums und dem Mailgate (äußerster von GDW kontrollierter Punkt auf der Reise einer E-Mail) die SEPPMail Instanz. Diese kümmert sich bei eingehenden Mails um die Mail-Entschlüsselung und die Prüfung von Mail-Zertifizierung und gleichzeitig kümmert sie sich bei ausgehenden Mails nach Bedarf um Mail-Verschlüsselung und Mail-Zertifizierung.

2. Benutzung

Aktuell ist es noch so konfiguriert, dass ausgehende Mails, falls für den Benutzer ein Zertifikat hinterlegt ist, im Betreff die folgenden zusätzlichen Zeichen benötigen:

- Die Zertifizierung (also die Sicherstellung der Absender-Identität) findet automatisch statt, solange ein gültiges Zertifikat des Benutzers existiert. Wenn man erzwingen möchte, dass die Mail ausschliesslich zertifiziert versandt wird, dann muss ein [S] Teil des Betreffstexts sein. Dieses wird von der SEPPMail Instanz automatisch aus dem Betreff entfernt, sodass der Empfänger dies nicht mitliest.
- Die Verschlüsselung (also die Sicherstellung der Empfänger-Identität) findet ebenfalls automatisch statt. Wenn man erzwingen möchte, dass die Mail ausschliesslich verschlüsselt versandt wird, dann muss ein [V] Teil des Betreffstexts sein. Wenn man stattdessen erzwingen möchte, dass die Mail unverschlüsselt versandt wird, dann mus ein [NV] Teil des Betreffstexts sein. Dieses wird von der SEPPMail Instanz automatisch aus dem Betreff entfernt, sodass der Empfänger dies nicht mitliest.

Wenn Sie keinen public Key (Zertifikat) vom Empfänger besitzen, können Sie keine E-Mail verschlüsselt senden.

Gleichzeitig ist die SEPPMail Instanz ja auch für die Entschlüsselung und die Entzertifizierung bei eingehenden Mails zuständig, entsprechend werden bei eingehenden Mails dann:

- [secure] an den Betreffstext angehängt im Falle einer verschlüsselten Mail.
- [signed OK] an den Betreffstext angehängt im Falle einer signierten Mail.
- **[secure] [signed OK]** an den Betreffstext angehängt im Falle einer signierten **und** verschlüsselten Mail.
- **[signed INVALID**] an den Betreffstext angehängt im Falle einer ungültigen bzw. abgelaufenen Signatur.

3. Domänenverschlüsselung

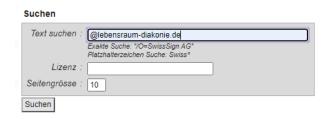
Unter anderem mit 3Net und dem Landkreis Lüneburg ist eine Domänenverschlüsselung umgesetzt, dabei werden alle Mails zwischen den Domänen, unabhängig vom Absender, verschlüsselt. Dies bietet nicht die gleiche Sicherheit (keine persönliche Identität der Mitarbeiter), aber es ist besser als unverschlüsselte Kommunikation.

4. Abrufen des eigenen Zertifikats

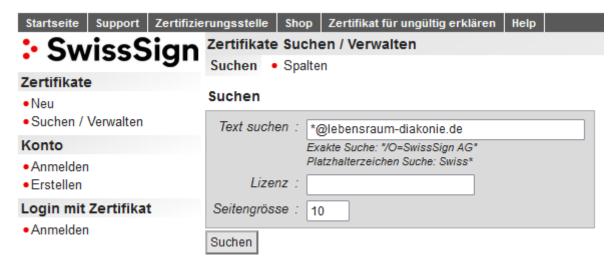
Ohne die GINA-Funktionalitäten (Verfahren E-Mails verschlüsselt an Empfänger zu übermitteln, die keine Verschlüsselungssoftware wie S/Mime einsetzen und keinen Schlüssel besitzen. Dieser wird dann telefonisch oder per SMS dem Empfänger übermittelt damit die E-Mail geöffnet werden kann) müssen die organisationseigenen S/MIME Zertifikate über die SwissSign-Seite abgerufen werden, falls benötigt. Hierfür geht man auf https://swisssign.net/mpki/manage_certs und, nachdem man sich dort als Nicht-Roboter identifiziert hat, kann man dort Zertifikate suchen.



Klicken Sie auf "Weiter ohne Konto"



Dafür kann man entweder die gewünschte Mail-Adresse eingeben oder man sucht über Platzhalter wie *@lebensraum-diakonie.de oder *@neue-arbeit-lueneburg.de. Der Platzhalter Lizenz kann frei gelassen werden. Klicken Sie auf "Suchen".



Dort kann man dann bei dem gewünschten Zertifikat auf "Herunterladen / Attribute" klicken, um die Details des Zertifikats einzusehen.



Dort gibt es dann auch unter anderem einen Abschnitt "Zertifikat herunterladen (ohne privaten Schlüssel)", bei dem man an das Zertifikat herankommt. Hierbei sei gesagt, dass das .cer-Format normalerweise das richtige ist.

