E-Mail-Sicherheit – OpenPGP, S/MIME und DKIM

Voraussetzungen (Debian)

Für die Arbeit mit OpenPGP-Dateien:

```
sudo apt install gnupg
```

Für S/MIME-Befehle mit OpenSSL:

```
sudo apt install openssl
```

Unterschiedliche Schutzebenen

E-Mail-Sicherheit umfasst mehrere unabhängige Verfahren. **OpenPGP und S/MIME** können Inhalte Ende-zu-Ende verschlüsseln und signieren. **DKIM** signiert ausgewählte Nachrichtenbestandteile auf Ebene der sendenden Domain. **SPF und DMARC** ergänzen die Domain-Authentifizierung, sind aber keine Ende-zu-Ende-Verschlüsselung.

Praktische Entschlüsselung

OpenPGP-Datei entschlüsseln:

```
gpg --decrypt --output nachricht.txt nachricht.gpg
```

Dazu muss der passende geheime Schlüssel verfügbar sein. Siehe GnuPG und OpenPGP für Verschlüsselung, Signatur und Schlüsselimport.

S/MIME-Nachricht entschlüsseln (nur bei passendem PEM-Format):

```
openssl cms -decrypt -inform PEM -in nachricht.pem -recip empfaenger-
zertifikat.pem -inkey empfaenger-key.pem -out nachricht.txt
```

Hierzu werden das passende Empfängerzertifikat und der private Schlüssel benötigt. In E-Mail-Programmen erfolgt die Entschlüsselung üblicherweise direkt im Client. DKIM wird nicht entschlüsselt, sondern geprüft.

OpenPGP

OpenPGP verwendet öffentliche und private Schlüssel. Für verschlüsselte E-Mails benötigt der Absender einen vertrauenswürdig zugeordneten öffentlichen Empfängerschlüssel. Signaturen lassen sich mit dem öffentlichen Signaturschlüssel prüfen. Siehe GnuPG und OpenPGP.

S/MIME

S/MIME verwendet X.509-Zertifikate für Signaturen und Verschlüsselung. Die Vertrauensbeziehung wird üblicherweise über Zertifizierungsstellen und Zertifikatsketten hergestellt. Die Verwaltung von Zertifikaten und privaten Schlüsseln ist Teil der E-Mail-Client-Konfiguration.

DKIM

Bei DKIM signiert ein Mailserver ausgewählte Header und den Nachrichteninhalt mit einem privaten Schlüssel. Der öffentliche Prüfschlüssel wird über DNS veröffentlicht. Empfänger können die Signatur prüfen. DKIM beweist nicht die persönliche Identität des Verfassers und verschlüsselt die Nachricht nicht.

SPF und DMARC

SPF beschreibt, welche Server für eine Domain E-Mails versenden dürfen. DMARC legt fest, wie Empfänger Ergebnisse aus SPF und DKIM in Bezug auf die sichtbare Absenderdomain bewerten und melden sollen. Beide sind Ergänzungen zu DKIM, keine Alternative zur Inhaltsverschlüsselung.

Transportverschlüsselung

SMTP kann TLS für den Transport verwenden. Das schützt einzelne Transportstrecken, bedeutet aber nicht zwangsläufig Ende-zu-Ende-Verschlüsselung. Auch Metadaten wie Empfänger und Versandzeitpunkt können weiterhin sichtbar sein.

Schlüsselverwaltung

Private S/MIME- und OpenPGP-Schlüssel sowie DKIM-Signaturschlüssel müssen geschützt werden. DKIM-Schlüssel können regelmäßig gewechselt werden; dabei sind DNS-Einträge und Mailserver-Konfiguration koordiniert anzupassen.

E-Mails verschlüsseln

Mozilla: E-Mails digital signieren und verschlüsseln

In diversen E-Mail-Programmen ist OpenPGP bereits enthalten und neue Schlüssel können direkt

damit erstellt werden.
Der öffentliche Schlüssel wird an den Kommunikationspartner geschickt, der die von ihm verfassten E-Mails damit verschlüsselt. (Nur) der Besitzer des privaten Schlüssels kann die E-Mail dann wieder entschlüsseln.
Lesen klappt nur mit einem System, auf dem der Schlüssel hinterlegt ist. Ist der private Schlüssel nur auf dem Notebook hinterlegt, kann dieselbe E-Mail z.B. auf dem Handy nicht entschlüsselt werden. Der private Schlüssel könnte aber auch dort hinterlegt werden.

Thunderbird

Schlüsselpaar erzeugen:
Extras → OpenPGP-Schlüssel verwalten → erzeugen → neues Schlüsselpaar.

Beim Einrichten von OpenPGP muss bei Thunderbird die Anwendung des privaten Schlüssels in den Konten-Einstellungen unter Ende-zu-Ende-Verschlüsselung aktiviert werden.

Zurück zur Übersicht

From:
https://wiki.bluegnu.de/ - **wiki**

Permanent link:
https://wiki.bluegnu.de/doku.php/open:it:secure:email

Last update: **2026/11/15 18:01**