Automatische E-Mail-Signierung mit Signing-Milter für Postfix

Zielgruppe: IT-Administratoren der WWU *IV-Sicherheitsteam, September 2019*

Der Postfix Mail Transfer Agent (MTA) unterstützt das Sendmail v8 Milter-Protokoll (kurz für *Mail Filter*). Die Milter-Schnittstelle ermöglicht eine Vielzahl von Addons, die E-Mails nach Spam untersuchen oder z.B. automatisch digital signieren. Dadurch können E-Mails von (*vertrauenswürdigen*) Anwendungen, die selbst kein S/MIME unterstützen, nachträglich digital signiert werden.

> Nicht in jedem Fall macht es Sinn eine automatisch versendete E-Mail digital zu signieren! Dies sollte nur geschehen, wenn Inhalt und Absender unter unserer Kontrolle und vertrauenswürdig sind. Keinen Sinn macht es z. B. E-Mails mit von (beliebigen) Nutzern erfassten Informationen per se zu signieren, wie bei Anmelde- oder Kommentarfunktionen.

Signing-Milter Installation auf CentOS/Redhat Linux Systemen

Das Addon signing-milter ermöglicht die automatische S/MIME-Signierung von E-Mails während sie einen Mail Transfer Agent (MTA) durchlaufen.

Abhängigkeiten installieren

Das yum-Repository Fedora Extra Packages for Enterprise Linux (EPEL) aktivieren und Abhängigkeiten per `yum` installieren.

```
yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-
7.noarch.rpm
yum install tinycdb-devel openssl-devel sendmail-milter sendmail-devel
```

Aus dem Quellcode installieren

Den Plugin-Quellcode von der Webseite https://signing-milter.org/ herunterladen und auspacken. Danach folgende Befehle ausführen.

```
make
make install
yum erase sendmail
```

Dienst in systemd konfigurieren

Die Datei `/etc/systemd/system/signing-milter.service` anlegen:

```
[Unit]
Description=Signing specific mails milter deamon
Wants=network-online.target
After=network-online.target
[Service]
ExecStart=/usr/share/signing-milter/run_signing-milter
[Install]
WantedBy=multi-user.target
```

Den Dienst mit folgenden Befehlen aktivieren (automatischer Start nach Reboot) und starten (für aktuelle Session):

```
systemctl enable signing-milter
systemctl start signing-milter
```

Nutzer anlegen (optional)

```
adduser -M -s /sbin/nologin signing-milter
```

Konfiguration

Optionen festlegen

Die globalen Einstellungen werden in `/etc/default/signing-milter` vorgenommen.

Beispielkonfiguration:

```
# use in /etc/default/signing-milter
DISABLE_HOURLY_STATISTIK_LOGGING='yes'
DISABLE_DAILY_STATISTIK_LOGGING='yes'
#OPTIONS="-x -k /var/signing-milter-tmp"
#OPTIONS="-x -u user -g group"
OPTIONS="-x"
```

Bei Bedarf die Option `-k` mit hinzu nehmen. Dann werden alle Mails in unsignierter und signierter Form im Ordner `/var/signing-milter-tmp` abgelegt.

Sollte die Anwendung als `root` ausgeführt werden, muss entweder der Nutzer `signing-milter` existieren oder es müssen Nutzer und Gruppe mittels den Optionen `-u` und `-g` angegeben werden.

Die Option `-f` kann genutzt werden, damit das Tool die Absenderadresse für die Signatur aus dem zusätzlichen Header `X-Signer` ausliest anstatt den `Return-Path` zu nutzen.

Zu Debug-Zwecken kann die Option `-d 7` gesetzt werden.

Zertifikate festlegen

Die Datei `/etc/signing-milter/signingtable` legt fest, welches Zertifikat für welche E-Mail-Adresse genutzt wird. Sie hat die Form:

```
absender@uni-muenster.de /etc/signing-milter/service-cert+key.pem
```

Nach jeder Änderungen muss die Signaturtabelle erneuert werden:

```
cdb -c -m /etc/signing-milter/signingtable.cdb /etc/signing-milter/signingtable
```

Hinweis: Sollte `sendmail` verwendet werden, kann es sein, dass eine Adresse der Form `user@hostname` genutzt wird, die eventuell nicht mit der tatsächlichen Absender-Adresse übereinstimmt. Dies liegt daran, dass das Tool die `Return-Path` Adresse nutzt. Entweder muss dann in der Tabelle diese Adresse eingeben werden oder es muss die Option `-f` genutzt werden, die die Absenderadresse aus dem Header `X-Signer` ausliest.

Schlüsseldatei konvertieren (pkcs12 nach PEM)

Die Schlüsseldateien müssen im PEM Format unverschlüsselt vorliegen:

```
openssl pkcs12 -in export.p12 -out service.pem -nodes
```

Hinweis: Da der unverschlüsselte private Schlüssel einen hohen Schutzbedarf hat, muss sichergestellt werden, dass das System ordnungsgemäß abgesichert ist (siehe *"Standards für sichere Administration"*), um einen fremden Zugriff auf den privaten Schlüssel zu verhindern! Es ist sinnvoll, ein extra Gruppen-Zertifikat zu verwenden, z. B. "*GRP: Automatischer E-Mail-Versand*" mit entsprechender OU-Angabe.

Schlüsseldateien ablegen

Datei	Beschreibung
`/etc/signing-milter/service-cert+key.pem`	Privater Schlüssel und Zertifikat
`/etc/signing-milter/service-chain.pem`	Übergeordnete Zertifikatskette (WWUCA, DFN, Teletrust/Root-Zertifikat)

Zugriffsrechte einschränken

```
chown signing-milter *.pem
chmod 400 *.pem
```

Sollt nicht der Nutzer `signing-milter` verwendet werden, muss an dieser Stelle natürlich der passende Nutzer aus der Konfiguration genutzt werden.

Bei allen Konfigurations-Änderungen muss der Dienst neu gestartet werden:

```
systemctl restart signing-milter
```

Nutzung mit Postfix

Bei Postfix sind folgende Anpassungen in `/etc/postfix/main.cf` nötig, um E-Mails an signing-milter umzuleiten:

```
myhostname = <hostname>.uni-muenster.de
mynetworks = 127.0.0.0/8, ...
relayhost = mail.uni-muenster.de
# Eine oder beide der folgenden Optionen müssen gewählt werden:
# Wenn ankommende E-Mails über SMTP signiert werden sollen
smtpd_milters = inet:localhost:30053
# Wenn lokale Nachrichten (z.B. mittles sendmail-Befehl) signiert werden sollen
non_smtpd_milters = inet:localhost:30053
```

Bei allen Konfigurations-Änderungen muss der Dienst neu gestartet werden:

```
systemctl restart postfix
```