

Implementierung eines TLS-gesicherten Nachrichtenaustausches mit dem Service BusinessMail X.400 der Telekom Deutschland GmbH

Die Telekom Deutschland GmbH betreibt mit dem Service BusinessMail X.400 ein System zur elektronischen Nachrichtenübermittlung auf Basis des X.400-Standards der ITU.

Dieser Service wird ausschließlich von Unternehmen genutzt, die bei der Übertragung von sensiblen EDI- und Geschäftsdaten Wert auf eine hohe Datensicherheit legen. Diese Datensicherheit wird dadurch erreicht, dass nur registrierte Benutzer Zugriff auf eine passwortgeschützte Mailbox haben. Zum anderen findet der Austausch von Nachrichten mit anderen X.400-Providern über eindeutige, vertraglich gesicherte Verbindungswege statt.

Trotzdem wurde von Kundenseite immer häufiger der Wunsch geäußert, auch über eine bereits bestehende Internetverbindung mit der X.400-Mailbox zu kommunizieren. Die relative Unsicherheit einer Nachrichtenübermittlung über das Internet ist zunächst nicht vereinbar mit hohen Sicherheitsanforderungen an den Service BusinessMail X.400.

Um diese Sicherheitsanforderungen erfüllen zu können, ist es notwendig, die Kommunikation mit der X.400-Mailbox über eine gesicherte Internetverbindung zu betreiben. Dies wurde erreicht, indem das entsprechende Kommunikationsmodul (UA-FITCP) erweitert wurde, um mittels des TLS-Protokolls eine verschlüsselte und somit sichere Übertragung der Nachrichten zu gewährleisten.

Diese TLS-Erweiterung wurde bereits vor mehr als 10 Jahren in die Windows-Version des Kommunikationsmoduls integriert, bei der Linux-Version aber erst mit der V5.1.1 im Jahre 2016. Bei modernen Linux OS, bei denen bereits die OpenSSL Bibliothek V1.0.0 und neuer installiert ist, empfehlen wir den Einsatz einer Linux UA-FI mit integrierter TLS Erweiterung (Secure P7). Damit ist dann auch sichergestellt, dass die Verbindung mit Hilfe der V1.2 von TLS erfolgen kann (Default Einstellung Cipher Suite ECDHE-RSA-AES256-GCM-SHA384).

Wird ein älteres Linux OS verwendet oder kann wegen Einschränkungen bei der Kundenapplikation keine neuere Linux UA-FI eingesetzt werden, muss die TLS-Verschlüsselung durch einen entsprechenden Wrapper-Prozess erfolgen. Unsere Empfehlung ist hier den Stunnel-Prozess einzusetzen (<https://www.stunnel.org/>), der bei vielen Linux Distributionen in den Paketquellen enthalten ist.

Im Folgenden wird beschrieben, wie mittels dieser OpenSource-Software auch unter einem alten Linux OS eine TLS-gesicherte Nachrichtenübermittlung stattfinden kann. Bitte aber beachten, dass bei älteren Distributionen nur OpenSSL V0.9.8 verfügbar ist. Hier wird maximal die V1.0 von TLS unterstützt, die bereits heute (2018) schon als unsicher angesehen wird. Es ist aktuell unklar, wie lange der Secure-P7-Zugang von BusinessMail X.400 dieses Protokoll noch unterstützen kann.

Voraussetzungen

Stunnel (V4.x) und OpenSSL müssen installiert sein. Diese sind meistens in den Paketquellen der jeweiligen Distributionen enthalten oder können eventuell über separate RPM-/DEB-Pakete nachinstalliert werden. Möglich ist auch ein Download der aktuellen Versionen von www.stunnel.org bzw. www.openssl.org mit anschließender Installation/Kompilierung (hängt vom jeweiligen Linux-Derivat ab).

Das Beispiel basiert auf Debian und gilt auch für kompatible Derivate (z.B. Ubuntu, Kubuntu etc.). Die dabei beschriebenen Dateien finden Sie vorkonfiguriert in der UA-FI-Linux-howto.zip auf der Service-Seite www.service-viat.de.

Stunnel konfigurieren

Nach der Installation von Stunnel muss unter „/etc/stunnel“ die Datei „stunnel.conf“ erstellt und angepasst werden. Alternativ können Sie auch die vorbereitete Konfigurationsdatei aus dieser zip-Datei nutzen. Falls bei Ihrer Distribution bereits unter „/etc/stunnel“ eine „stunnel.conf“ liegen sollte, sichern Sie diese, denn eventuell wurden bei der Installation abweichende Nutzer erstellt. Sollten Sie die Beispielkonfiguration nutzen, können Sie anschließend die Datei „certs.tar“ aus dieser zip-Datei im Verzeichnis „/var/run/stunnel4“ entpacken. Darin befinden sich die bereits für Debian 7-9 (getestet) geshashten Zertifikate.

Falls Sie eine bestehende Konfiguration verwenden möchten, sind folgende Parameter zu beachten:

```
; Die Daten für die eigentliche Verbindung
[P7]
accept = 102
connect = securep7.telebox400.de:5432
client = yes
verify = 2
```

Zur Verifizierung des Hostzertifikates stehen Ihnen zwei Methoden zur Verfügung. Zum einen „CAfile“, bei dem Sie eine explizite Datei angeben. Dies hat den Nachteil, dass bei einem Wechsel des Hostzertifikates die Verbindung fehlschlägt und erst nach dem Austausch der Datei wieder funktioniert. Die Zeile könnte beispielsweise wie folgt lauten:

```
CAfile = /etc/stunnel/3ad48a91.0 ;(für das bis 25.09.2018 gültige Zertifikat)
CAfile = /etc/stunnel/d06393bb.0 ;(für das ab 25.09.2018 gültige Zertifikat bei OpenSSL<v1.0)
CAfile = /etc/stunnel/1e09d511.0 ;(für das ab 25.09.2018 gültige Zertifikat bei OpenSSL ab v1.0)
```

Auf der anderen Seite gibt es die Möglichkeit „CApath“ zu verwenden. Mit diesem Parameter gibt man ein Verzeichnis an, in dem sich geshasht Zertifikate (z.B. 3ad48a91.0) befinden. Dadurch wird bei einem Austausch des Hostzertifikates automatisch das neue Zertifikat genutzt und ein Eingriff zum Zeitpunkt des Wechsels wird unnötig. Ist wie in der Beispielkonfiguration chroot aktiviert, beginnt der absolute Pfad innerhalb des chroot-jail, daher wird bei „CApath = /certs“ im Verzeichnis „/var/run/stunnel4/certs“ nach den .0-Dateien gesucht. Der Nachteil dieser Methode ist die etwas schwierigere Einrichtung, da sich der Hashwert je nach verwendeter OpenSSL-Version unterscheidet, wodurch ein erneutes Hashen der Zertifikate notwendig werden kann. Die Zeile könnte beispielsweise wie folgt lauten:

```
CApath = /certs ;(verweist bei aktiviertem chroot auf „/var/run/stunnel4/certs“)
CApath = /etc/stunnel/certs ;(bei nicht aktiviertem chroot)
```

Wird der Parameter „CApath“ genutzt, muss das certs-Verzeichnis im entsprechendem Pfad angelegt und die Root-Zertifikate dort abgelegt werden.

Download: http://www.service-viat.de/userfiles/downloads/P7_Root.zip

Damit beim Booten des Rechners Stunnel automatisch gestartet wird, muss in der Datei „/etc/default/stunnel4“ der Parameter „ENABLED=1“ gesetzt werden.

Danach sollte sich Stunnel mittels des Befehles „service stunnel4 start“ starten und mittels „service stunnel4 stop“ stoppen lassen. Dies ist nach jeder Konfigurationsänderung erforderlich.

UA-FI konfigurieren

Packen Sie zunächst den Tarball in dem gewünschten Verzeichnis aus. In dem entpackten Ordner finden Sie die Konfigurationsdateien „maxware.ini“ und eine oder mehrere .prf-Dateien.

In der „maxware.ini“ ist in der Sektion „[Communication]“ der Parameter „ServiceProfil=“ zu finden, welcher die genutzte .prf-Datei bestimmt.

Auszug der maxware.ini:

```
[Communication]
ServiceProfile=tbx_tcp
```

In diesem Fall wird die Datei „tbx_tcp.prf“ als Kommunikationsprofil genutzt. Bei der UA-FI ab Version 5.1.1 ist zusätzlich die Datei „tbx_secure.prf“ vorhanden, welche für die verschlüsselte Kommunikation ohne Stunnel genutzt wird.

In der Datei „tbx_tcp.prf“ sind die Parameter „MS_IPADDRESS=“ und „TCPPort=“ relevant. Bei der IP-Adresse muss der Stunnel eingetragen werden (z.B. 127.0.0.1 wenn der Stunnel auf demselben System läuft), der Port ist in der „stunnel.conf“ angeben. In diesem Beispiel wird der Port 102 genutzt.

Abschließend muss der lokale Nutzer erzeugt werden, wofür die Datei „create.cmd“ anzupassen ist. Mittels „./ua-fitcplinux -v create.cmd create.rsp“ wird der Nutzer angelegt, „./ua-fitcplinux -v list.cmd list.rsp tester“ listet alle Nachrichten für den User „tester“ auf.

Die genaue Erklärung der Befehle finden Sie im Handbuch auf www.service-viat.de.

Ihr BusinessMail X.400 Team

Kontakt

Tel.: 0800 5 229 230

E-Mail: helpdesk.businessmailx400@telekom.de

