BusinessMail X.400
Zugang über P7 mit Strong Authentication

Seit Jahren ist X.400 das bevorzugte Protokoll zur verlässlichen Übertragung von Geschäftsdaten (Electronic Data Interchange EDI). Ausschlaggebend hierfür sind unter anderem bekannte, vertraglich abgesicherte Übertragungswege sowie standardisierte Reports zur Verfolgung jeder Mitteilung. Verschiedene Zugangsarten ermöglichen die automatisierte Kommunikation zwischen Kundenanwendungen. Vor allem Firmen mit besonders hohen Sicherheitsansprüchen nutzen das geschlossene System BusinessMail X.400 für den Austausch geschäftlicher Nachrichten.

Was bietet der Zugang über P7 mit Strong Authentication (erweiterte Authentifizierung)?

BusinessMail X.400 bietet Ihnen schon seit vielen Jahren einen Zugriff auf die X.400 Mailbox mittels P7 Protokoll. Dabei muss sich Ihr X.400-Client mittels seiner X.400 Adresse und eines Passwortes beim Message Store authentifizieren, um Zugriff auf die dort gespeicherten Mitteilungen zu erhalten bzw. um Mitteilungen versenden zu können. Dieses Verfahren hat sich über die Jahre bewährt. Da aber immer mehr Anwendungen für den Zugriff über Internet konfiguriert werden und hier die Gefahr eines Missbrauchs deutlich höher ist als bei dem Zugriff über dedizierte Zugänge (ISDN, MPLS etc.), wurde zur Verbesserung der Applikationssicherheit beim P7 Zugang die Option „Strong Authentication“ (erweiterte Authentifizierung) eingeführt. Hierbei wird zur Authentifizierung kein Passwort benutzt. Stattdessen sendet der P7 Client ein sogenanntes Secure Token, das mit einem beim Client hinterlegten privaten elektronischen Schlüssel signiert wurde und durch den Message Store mittels des dort hinterlegten öffentlichen Zertifikats verifiziert wird.

Den für den Client benötigten privaten Schlüssel können Sie bei der Administration von BusinessMail X.400 anfordern und dann über WebConfig (ein Web basiertes Konfigurationstool zur Verwaltung von Mailboxdaten und Partnerschaften, siehe Informationen unter http://www.service-viat.de/?WebConfig) abholen. Für diesen Schlüssel bieten wir Ihnen folgende Möglichkeiten:

- Kostenlose PKCS12 Datei mit privatem Schlüssel und Zertifikat, das von der nicht öffentlichen Zertifizierungsstelle (CA, Certificate Authority) von WebConfig signiert wurde
- Kostenpflichtige PKCS 12 Datei mit privatem Schlüssel und Zertifikat, das von einer öffentlichen Zertifizierungsstelle (Shared Business CA der T-Systems International GmbH) signiert wurde

Beide PKCS12 Dateien können nur dann abgeholt werden, wenn ein Exportpasswort mit mindestens 12 Zeichen Länge unter Benutzung von Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen angegeben wird. Dieses Passwort schützt den privaten Schlüssel vor Missbrauch und muss auch beim Import in den Client angegeben werden.

Alternativ dazu können Sie auch den privaten Schlüssel mit zugehörigen Zertifikat bei einer anderen CA beschaffen und nur das Zertifikat im entsprechenden Menü von WebConfig hochladen. Dann wird dieses Zertifikat zur Authentifizierung verwendet. Das Zertifikat muss aber gültig und sollte mit SHA256 signiert worden sein.

Nach Import des privaten Schlüssels können Sie in WebConfig die „Strong Authentication“ im Message Store aktivieren und den Client entsprechend konfigurieren. Nach der Aktivierung des Leistungsmerkmals wird der interaktive Zugriff auf die Mailbox über den Local User Agent (LUA) gesperrt, da dieser eine Authentifizierung mittels Passwort nutzt. Falls Sie das Leistungsmerkmal wieder deaktivieren wollen, müssen Sie dies bei der Administration von BusinessMail X.400 beauftragen.

Es können zwei Zertifikate pro Mailbox verwaltet werden, um bei Ablauf eines Zertifikats (normalerweise 3 Jahre Laufzeit) einen reibungslosen Austausch zu gewährleisten. Die Laufzeit des für Strong Authentication benutzten Zertifikats bekommen Sie beim Login in WebConfig angezeigt.

Falls Sie keine eigene Schlüsselverwaltung implementiert haben, empfehlen wir Ihnen dringend, in regelmäßigen Abständen durch Login in WebConfig die Gültigkeitsdauer Ihres Zertifikats zu prüfen, um rechtzeitig ein neues Zertifikat zu beauftragen. Ist das Zertifikat abgelaufen, ist kein Zugriff auf die Mailbox möglich!

Bitte beachten Sie auch, dass der vom Client erzeugte Secure Token aus einem Zeitstempel besteht, den der Hostrechner mittels hinterlegten Zertifikats verifiziert. Der Hostrechner akzeptiert zwar momentan eine Zeittoleranz von +/- 24 Stunden, aber dies könnte aufgrund geänderter Sicherheitsvorgaben noch reduziert werden. Wir empfehlen Ihnen deshalb, Ihren Applikationsrechner mit korrekter Systemzeit (Zeitsynchronisiert) zu betreiben, um Fehlversuche beim Verbindungsaufbau über die erweiterte Authentifizierung zu vermeiden.

Neben den von BusinessMail X.400 angebotenen P7 Clients (FileWork ab V4.8, UA-FI ab V4.3) bieten u.a. auch einige Softwarehäusereine entsprechende Erweiterung für deren neueste Version ihrer P7 Clients an. Bitte setzen Sie sich mit den entsprechenden Helpdesks der Softwarehäuser in Verbindung, um Details zu erfahren.

Kontakt
Tel.: 0800 5 229230
E-Mail: helpdesk.businessmailx400@telekom.de