fp-francotyp.at

Informationen für Netzwerk-Administratoren zur Einbindung von Frankiermaschinen in das Ethernet

Wien, im August 2017

Betrifft: Frankiermaschinenmodelle der POSTBASE-Serie
Hersteller: Francotyp-Postalia GmbH

Die Frankiermaschinen der POSTBASE-Serie (POSTBASE 30 – 85, POSTBASE *Mini* und POSTBASE *One*) benötigen vorzugsweise einen Netzwerkanschluss (Ethernet) zur Internetanbindung, mit einer minimalen **Übertragungsrate von 10 Mbit/sec**., um u.a. Geld zum Frankieren vom FP-Server in die PostBase zu laden, die täglichen postrelevanten Daten an die ÖPAG zu senden, sowie sonstige Applikationen in die Maschinen zu installieren (Portotariftabellen, Klischees, Einschreib-Codes, etc.).

Netzwerkkabel der Klasse **CAT5E** sind empfohlen.

Für die Übertragung wird das Kommunikationsprotokoll **TCP/IP (v4 only)**, mittels einer **„https“** Verbindung mit **TLS v1.2** Verschlüsselung, über den **Port 443**, verwendet.
In einigen wenigen Fällen (Services) wird auch eine “http“ Verbindung über den **Port 80** benutzt. Diese beiden Ports müssen in Ihrer Firewall geöffnet sein. Es wird versucht eine **Verbindung zu *.francotyp.com** aufzubauen.

URL’s / IP-Adressen, die von der Frankiermaschine angewählt werden:

baut.francotyp.com	193.29.243.32		maaut.francotyp.com	193.29.243.33
baut2.francotyp.com	193.29.243.32		maaut2.francotyp.com	193.29.243.33
ins.francotyp.com	193.29.243.33		mabaut.francotyp.com	193.29.243.33
ins2.francotyp.com	193.29.243.33		mabaut2.francotyp.com	193.29.243.33

Die Frankiermaschinen können für **DHCP** (default), oder alternativ für die Verwendung einer **statischen IP-Adresse**, konfiguriert werden.

Im Falle einer statischen IP Adresse müssen neben der **IP Adresse für die Postbase**, zusätzlich die **Subnetz Maske**, die **IP des Standard Gateway- und des DNS-Servers**, manuell eingegeben werden.

Falls ein **Proxy-Server** verwendet wird, muss zusätzlich die **Proxy-IP** und der verwendete **Port** bekannt gegeben, und manuell in die Postbase eingetragen werden. Es werden Proxy Server ohne **Autentifikation** unterstützt, wenn nötig kann die PostBase auch **‘basic’** oder **‘digest’** Autentifikation Methoden unterstützen (Benutzung eines **Benutzernamen** und **Passwort**; „digest“ benutzt eine MD5 checksum).

NTLM wird als Autentifikations-Methode nicht unterstützt!

fp-francotyp.at

Verbindungsprobleme auf Grund von Zertifikaten und Firewall

In einigen Fällen ist es nicht möglich die PostBase-Frankiermaschinen, in ein Kundennetzwerk einzubinden.
Auch wenn mittels des Verbindungseinstellungs-Assistenten alle Optionen ausprobiert wurden, gibt die Maschine eine Fehlermeldung: ***„Verbindungsaufbau nicht möglich – Überprüfen Sie die Verbindungseinstellungen“*** aus.

Beschreibung mögliche Ursache:
Kundennetzwerke sind sehr individuell und unterschiedlich. Bei einigen Kunden, z.B. Behörden, Geldinstituten, etc. sind besonders hohe Sicherheitsstandards festgelegt.
Ein besonderes Sicherheitsfeature ist die Firewall. In größeren Unternehmen werden in der Regel Firewalls eingesetzt. Je nach Konfiguration einer solchen Firewall, wird unter anderem auch eine Zertifikatsprüfung vorgenommen. Zertifikate sind erforderlich, wenn über den Port 443, eine gesicherte https-Verbindung benutzt wird.

Hierzu gibt es Zertifikate, die gegen ein Entgelt von einer kommerziellen Zertifizierungsstelle (z.B. VeriSign, Thawte, Symantec, GeoTrust, usw.) erworben werden können.

Solche Zertifikate können automatisch geprüft werden, da die Zertifikate, die zu einer solchen Prüfung notwendig sind, typischerweise in den Firewalls bekannt sind. Daneben gibt es auch Zertifikate, die nicht von einem Zertifikatsanbieter ausgestellt sind. Um diese prüfen zu können, braucht man ein weiteres Zertifikat vom Aussteller (FP).

Bei dem bei der Kommunikation der PostBase mit der FP-Infrastruktur verwendeten Zertifikate handelt es sich um Zertifikate, die von FP selbst ausgestellt worden sind. Da das entsprechende Zertifikat, das man zur Prüfung unserer Zertifikate benötigt, in der Kunden- Firewall nicht bekannt ist, stellt die Firewall bei der Datenübertragung zwischen PostBase und unserer FP-Infrastruktur, ein unbekanntes Zertifikat fest und unterbindet die Kommunikation mit der oben beschriebenen Fehlermeldung.

Abhilfe:
Der Netzwerkadministrator sollte in den meisten Fällen die Konfigurationsmöglichkeit an seiner Firewall haben,

a) entweder die Zertifikatsüberprüfung ganz, oder nur für die PostBase abzuschalten,

oder

b) eine entsprechende Regel/Ausnahme zu erstellen.

Dazu müssen unsere URL’s und/oder die entsprechenden IP Adressen bekannt gegeben werden (siehe Seite 1).