

**AUSTAUSCH SECURE P7 ZERTIFIKAT BEI STUNNEL 12/12 AM 02.12.2015, 09:10 UHR**  
**ABSCHALTUNG PORT 5433 BEI STUNNEL11/21 AM 03.12.2015, 08:00 UHR**

Für UA-FI/FileWork-Kunden:

Von den ursprünglich 3 Workarounds, die wir am 13.10.2015 angeboten hatten, verbleibt durch den Ablauf des alten Zertifikats nur noch der Dritte:

Ersetzen Sie die TCP/IP UA-FI inkl. der beiden OpenSSL Bibliotheksdateien nach entsprechender Sicherung/bzw. Umbenennen der alten Dateien im Programmverzeichnis Ihrer Anwendung (Standard Standalone UA-FI ist c:\programme\uafiwin\uafitc32.exe, Standard FileWork ist c:\programme\telebox 400\ua-fitcp.exe und Standard ElreTrans ist c:\programme\eletrans\uafi\uafitc32.exe) durch die Dateien der V3.25, die Sie in den beiden ZIP-Datei (UA-FI V3.25 gilt auch für ElreTrans) finden:

Patch FileWork:

[http://www.service-viat.de/userfiles/downloads/fix/patch\\_sha2\\_fur\\_FileWork.zip](http://www.service-viat.de/userfiles/downloads/fix/patch_sha2_fur_FileWork.zip)

Patch UA-FI:

[http://www.service-viat.de/userfiles/downloads/fix/patch\\_sha2\\_fuer\\_UAFI.zip](http://www.service-viat.de/userfiles/downloads/fix/patch_sha2_fuer_UAFI.zip)

Fremdhersteller-Software z.B. (Seeburger)

Hier besteht die Möglichkeit, die verschlüsselte Verbindung durch einen Stunnel Proxy im Client-Modus übernehmen zu lassen. Sie müssten sich dann auf Ihrem Applikationsrechner diese Software installieren und so konfigurieren, dass diese lokal auf den Port 102 lauscht und dann eine Verbindung zu unserer Plattform über „securep7.telebox400.de“ und Port 5432 aufbaut. Bei den meisten Linux-Distributionen ist Stunnel schon im Repository enthalten oder kann als RPM nachinstalliert werden. Falls Sie Windows oder andere Betriebssysteme einsetzen, können Sie die Software hier

<https://www.stunnel.org/downloads.html>

herunterladen. Sollte unter Windows die Fehlermeldung **"Diese Anwendung konnte nicht gestartet werden, weil die Anwendungskonfiguration nicht ordnungsgemäß ist. Zur Problembehebung sollten Sie die Anwendung neu installieren."** erscheinen, fehlt Microsoft Visual C++ 2008 Redistributable Package (x86) auf dem System. Dies kann unter <https://www.microsoft.com/de-de/download/details.aspx?id=29> heruntergeladen und anschließend installiert werden.

Nachfolgend finden Sie ein Beispielkonfiguration für den Stunnel (Stunnel.conf) unter Windows:

<http://www.service-viat.de/userfiles/downloads/fix/stunnel.zip>

Sie können diese Datei verwenden, um die in der Distribution mitgelieferte zu ersetzen. Bei anderen OS müssten Sie die Pfade entsprechend anpassen. In der Beispielkonfiguration ist vorgesehen, dass das Hostzertifikat anhand des hinterlegten Root-Zertifikats verifiziert wird. Das beim Secure P7-Zugang

verwendete Root-Zertifikat können Sie unter

[http://www.service-viat.de/userfiles/downloads/Root\\_CA\\_Cert.zip](http://www.service-viat.de/userfiles/downloads/Root_CA_Cert.zip)

herunterladen, auspacken und in dem in der Konfigurationsdatei angegebenen Pfad (im Beispiel "C:\Programme\Stunnel\) hinterlegen. Danach können Sie Stunnel starten.

Ihr X.400 Kommunikationsmodul müssen Sie nun so konfigurieren, dass dieses eine unverschlüsselte TCP/IP Verbindung auf die Local Loop IP Adresse Ihres Rechners (127.0.0.1) und den Port 102 aufbaut. Wenn Sie FileWork oder UA-FI einsetzen, müssen Sie statt „fw\_secure.prf“ das Profil „fw\_tcp.prf“ verwenden und dieses editieren, um die IP Adresse (MS\_IPADDRESS=) anzupassen. Bei Kommunikationsmodulen anderer Hersteller bitte die entsprechende Dokumentation heranziehen.

Weitere Informationen zu den beim Secure P7 Zugang eingesetzten Zertifikaten finden Sie unter:

<http://www.service-viat.de/?Root-Zertifikat>