SSL/TLS-Unterstützung für TN3270

Entire Connection unterstützt TN3270-SSL. Dies ermöglicht eine sichere Verbindung zwischen Entire Connection und einem Telnet-TN3270-Server. In einer SSL-Session werden alle Daten verschlüsselt, bevor sie an den Telnet-Server gesendet werden. Vor der weiteren Verarbeitung werden die vom Server empfangenen verschlüsselten Daten entschlüsselt.

Als Voraussetzung benötigen Sie einen Telnet-TN3270-Server mit einem Port, der für SSL aktiviert wurde. Damit SSL benutzt werden kann, muss der Server einen privaten Schlüssel und ein hiermit verknüpftes Server-Zertifikat haben.

Dieser Abschnitt behandelt die folgenden Themen:

- In Entire Connection unterstützte SSL-Funktionalität
- Eine TN3270-Session mit SSL aufbauen
- SSL für Entire Connection konfigurieren
- Server-Zertifikate mit Entire Connection überprüfen
- Client-Authentifizierung
- Mehr zu Zertifikaten

Anmerkung:
Dieses Produkt enthält Software, die vom OpenSSL Project für die Benutzung im OpenSSL Toolkit entwickelt wurde (*http://www.openssl.org/*).

In Entire Connection unterstützte SSL-Funktionalität

In Entire Connection steht die SSL-Unterstützung für TN3270-Anzeige-Sessions und TN3270-Drucker-Sessions zur Verfügung. Die folgenden SSL-Optionen werden unterstützt:

- **Server-Authentifizierung**
  Die Server-Authentifizierung dient dazu, den Server beim Client zu legitimieren. Die Server-Authentifizierung kann für eine verschlüsselte SSL-Session ein- und ausgeschaltet werden. Sie kann mit oder ohne Client-Authentifizierung benutzt werden.

  Bevor die Session aufgebaut wird, prüft der Client (Entire Connection) das Server-Zertifikat, das mit dem privaten Schlüssel des Servers verknüpft ist.

- **Überprüfung des Hostnamens**
  Der Name des Hosts zu dem der Client (Entire Connection) eine Verbindung aufbaut, wird mit dem Wert für den Common Name (CN) im Server-Zertifikat verglichen. Diese Option verstärkt die Server-Authentifizierung.

- **Client-Authentifizierung**
  Die Client-Authentifizierung dient dazu, den Client beim Server zu legitimieren.

Die SSL-Client-Authentifizierung bietet eine zusätzliche Authentifizierungs- und Zugriffskontrolle durch das Überprüfen der Client-Zertifikate auf dem Server. Dies verhindert, dass ein nicht berechtigter Client auf dem Server Zugriff erhält.

Eine TN3270-Session mit SSL aufbauen

Es gibt zwei Möglichkeiten, eine TN3270-Session mit SSL aufzubauen.

Die eine Möglichkeit ist, eine SSL-Verbindung mit einem SSL-Handshake direkt zu öffnen. Das heißt, dass der Client die Verbindung zu einem Port herstellt, der für SSL aktiviert wurde und dass das SSL-Protokoll von Anfang an benutzt wird.

Die andere Möglichkeit ist verhandelbare Telnet-Sicherheit. In diesem Fall wird eine normale Telnet-Verbindung zwischen dem Client und dem Telnet-TN3270-Server geöffnet. Der Telnet-Server sendet dann einen speziellen Befehl (`IAC DO START_TLS`) an den Client, um zu prüfen, ob der Client die SSL-Verhandlung starten möchte. Bei einer positiven Antwort macht der Server mit dem SSL-Handshake weiter. Wenn keine positive Antwort empfangen wird, wird - in Abhängigkeit von der Server-Konfiguration - eine normale Telnet-Session benutzt oder die Verbindung wird beendet.

SSL für Entire Connection konfigurieren

Der folgende Ordner (abhängig vom Betriebssystem) enthält mehrere Server-Zertifikate von unterschiedlichen Zertifizierungsstellen (auch "Certification Authority" oder kurz "CA" genannt).

- Windows 2000, XP und Server 2003:

  \Dokumente und Einstellungen\Alle Benutzer\Anwendungsdaten\Software AG\Entire Connection\certs

- Windows Vista:

  \ProgramData\Software AG\Entire Connection\certs

1. Wenn die Server-Authentifizierung eingeschaltet ist, überprüfen Sie, ob das Server-Zertifikat, das Sie für Ihren Telnet-SSL-Server erhalten haben, bereits im Ordner *certs* enthalten ist. Wenn Ihr Server-Zertifikat von einer anderen Zertifizierungsstelle ist, oder wenn Sie ein selbstsigniertes Zertifikat benutzen, müssen Sie es ebenfalls im Ordner *certs* ablegen und in die Datei *CAList.pem*, die sich auch in diesem Ordner befindet, eintragen. Ausführliche Informationen hierzu finden Sie im Abschnitt *Server-Zertifikate mit Entire Connection überprüfen*.

2. Erstellen Sie mit dem Konfigurationsmanager von Entire Connection eine Host-Session (Anzeige-Session) vom Typ TN3270. Geben Sie im Dialogfeld **Session-Eigenschaften** einen Session-Namen ein und wählen Sie die Befehlsschaltfläche **Kommunikation**. Geben Sie auf der Eigenschaftenseite **Allgemein** des daraufhin erscheinenden Dialogfelds **Kommunikation** alle erforderlichen Informationen ein. Geben Sie die Nummer eines Ports an, der SSL unterstützt. Zeigen Sie die Eigenschaftenseite **Sicherheit** an und aktivieren Sie SSL. Sie werden zunächst überprüfen, ob eine einfache SSL-Verbindung hergestellt werden kann. Aktivieren Sie hierzu entweder das Kontrollkästchen **SSL/TLS Handshake-Verbindung**, um eine Handshake-Verbindung einzurichten oder Sie deaktivieren dieses Kontrollkästchen, um eine Session mit verhandelbarer Telnet-Sicherheit einzurichten. Aktivieren Sie noch nicht die anderen Optionen auf dieser Eigenschaftenseite. Ausführliche Informationen zu den Kommunikationsparametern finden Sie in der *Übersicht der*

Objekteigenschaften im Abschnitt *TN3270(E) für Anzeige-Sessions*.

3. Rufen Sie die Terminal-Anwendung von Entire Connection auf, um die Session zu testen, die Sie im vorherigen Schritt erstellt haben.

4. Wenn diese einfache SSL-Verbindung korrekt funktioniert, können Sie die restlichen Optionen auf der Eigenschaftenseite **Sicherheit** aktivieren und testen:

   - **Überprüfung des Hostnamens**
     Sie können diese SSL-Option nur dann benutzen, wenn der Wert für den Common Name (CN) im Server-Zertifikat derselbe ist wie der Hostname auf der Eigenschaftenseite **Allgemein** des Dialogfelds **Kommunikation**.

     Um diese SSL-Option zu nutzen, müssen Sie auf der Eigenschaftenseite **Sicherheit** des Dialogfelds **Kommunikation** die Option **Common Name im Zertifikat mit Hostnamen vergleichen** aktivieren.

   - **Client-Authentifizierung**
     Ihr Server muss für die Benutzung der Client-Authentifizierung konfiguriert sein. Sie benötigen einen privaten Schlüssel für den Client und ein Zertifikat für diesen Schlüssel. Dieser Schlüssel und das Zertifikat müssen bei Entire Connection zur Verfügung stehen. Ausführliche Informationen hierzu finden Sie im Abschnitt *Client-Authentifizierung*.

     Um diese SSL-Option zu nutzen, müssen Sie auf der Eigenschaftenseite **Sicherheit** des Dialogfelds **Kommunikation** die Option **Zertifikat an den Server senden, wenn dieser eines verlangt** aktivieren.

5. Wiederholen Sie die oben aufgeführten Schritte, um eine Host-Drucker-Session vom Typ TN3270E zu erstellen. Ausführliche Informationen zu den Kommunikationsparametern finden Sie in der *Übersicht der Objekteigenschaften* im Abschnitt *TN3270E für Drucker-Sessions*.

Server-Zertifikate mit Entire Connection überprüfen

Die Informationen in diesem Abschnitt gelten wenn die Server-Authentifizierung eingeschaltet ist. Es wird beschrieben, wie Sie eine einfache SSL-Verbindung mit Server-Authentifizierung einrichten. Das heißt: Entire Connection stellt eine SSL-Verbindung her und überprüft das Zertifikat des TN3270-Servers. Wenn das Server-Zertifikat nicht gültig ist, wird die Verbindung beendet.

Beim Starten einer TN3270-SSL-Verbindung vergleicht Entire Connection das Server-Zertifikat mit den Zertifikaten in der Datei *CAList.pem*. Diese Datei enthält die (Stamm-) Zertifikate der Zertifizierungsstellen, denen Sie vertrauen. Eine Zertifizierungsstelle ist eine Firma, die Zertifikatsanfragen signiert. Ein Beispiel für eine solche Firma ist VeriSign (siehe *http://www.verisign.de/*).

Die mit Entire Connection ausgelieferte Datei *CAList.pem* enthält verschiedene Zertifikate von bekannten Zertifizierungsstellen. Wenn Sie für Ihren Server ein selbstsigniertes Zertifikat haben, oder wenn Sie noch ein weiteres Zertikat zur Liste der vertrauenswürdigen Zertifikate hinzufügen möchten, müssen Sie wie nachfolgend beschrieben vorgehen.

Ein Zertifikat in die Datei *CAList.pem* eintragen

1. Gehen Sie zum *certs*-Ordner von Entire Connection.

   Dieser Ordner enthält mehrere Zertifikatdateien (*.crt*) und die Datei *CAList.pem*, die eine Zusammenfassung der *crt*-Dateien darstellt. Mit der Stapelverarbeitungsdatei *create-calist.bat* wird die Datei *CAList.pem* erstellt. Die Datei *create-calist.bat* enthält eine Befehlszeile für jedes Zertifikat, das in die Datei *CAList.pem* geschrieben werden soll.

2. Kopieren Sie Ihre *crt*-Datei (zum Beispiel ein selbstsigniertes Zertifikat oder ein neues Zertifikat von einer Zertifizierungsstelle) in den Ordner *certs*.

3. Editieren Sie die Stapelverarbeitungsdatei *create-calist.bat* und erstellen Sie eine neue Befehlszeile für Ihr Zertifikat.

   Wenn Sie zum Beispiel das Zertifikat in der Datei *meincert.crt* hinzufügen möchten, müssen Sie die folgende Befehlszeile hinzufügen:

   ```
   %OPENSSL% x509 -text -in meincert.crt >> %OUTFILE%
   ```

4. Überprüfen Sie, ob die Variable `OPENSSL` in der ersten Zeile der Stapelverarbeitungsdatei bei Ihnen korrekt gesetzt ist. Sie muss auf *OpenSSL.exe* zeigen. Dieses Programm befindet sich im Stammverzeichnis von Entire Connection.

5. Führen Sie die Datei *create-calist.bat* aus. Die Datei *CAList.pem* wird jetzt mit der neuen Zertifikatsdatei neu erstellt.

Client-Authentifizierung

Mit der Client-Authentifizierung kann der Telnet-Server die Identität des Client überprüfen. Der Server kann nicht nur überprüfen, ob das Zertifikat von einer vertrauenswürdigen CA (unterste Sicherheitsstufe) ausgegeben wurde, es ist auch möglich, das Client-Zertifikat gegen eine interne Datenbank (zum Beispiel RACF) zu registrieren und zu gewährleisten, dass der Client die Verbindung von einer definierten TCP/IP-Adresse und einem definierten Port aus herstellt. Client-Authentifizierung ist optional.

Generieren Sie einen privaten Schlüssel für jeden Benutzer

Für die Client-Authentifizierung muss für jeden Benutzer ein privater Schlüssel generiert werden. Der private Schlüssel wird mit dem Programm *OpenSSL.exe* generiert. Dieses Programm befindet sich im Stammverzeichnis von Entire Connection.

Informationen darüber, wie der private Schlüssel erstellt wird (in englischer Sprache), finden Sie im Dokument *keys.txt*, das sich im Ordner *certs* befindet.

Ihr privater Schlüssel sollte den Namen *clientprivkey.pem* haben.

Einen 2048-Bit-RSA-Schlüssel erstellen (Beispiel)

1. Öffnen Sie ein Fenster für die Eingabeaufforderung.

2. Wechseln Sie in den *certs*-Ordner von Entire Connection.

3. Geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

   ```
   "\Programme\Software AG\Entire Connection n.n.n\OpenSSL.exe" genrsa
   -des3 -out testkey.pem 2048
   ```

   wobei *n.n.n* die Versionsnummer ist.

   Wenn Sie "-des3" angeben, werden Sie beim Generieren des privaten Schlüssels aufgefordert, ein Passwort anzugeben.

Wichtig:
Aus Sicherheitsgründen empfehlen wir, den privaten Schlüssel mit einem Passwort zu generieren. Dadurch wird verhindert, dass der private Schlüssel - falls er in falsche Hände gelangt - ohne Passwort benutzt werden kann.

Erstellen Sie ein auf dem Client-Schlüssel basiertes Zertifikat

Sie müssen auch ein Zertifikat erstellen, das auf dem Client-Schlüssel basiert. Hier zu wird auch das Programm *OpenSSL.exe* benutzt, das sich im Stammverzeichnis von Entire Connection befindet.

Weitere Informationen (in englischer Sprache) finden Sie im Dokument *certificates.txt*, das sich im Ordner *certs* befindet.

Ihr Zertifikat sollte den Namen *clientcert.crt* haben.

Ein selbstsigniertes Zertifikat mit der Konfigurationsdatei *openssl.cnf* erstellen (Beispiel)

1. Öffnen Sie ein Fenster für die Eingabeaufforderung.
2. Wechseln Sie in den *certs*-Ordner von Entire Connection.
3. Geben Sie den folgenden Befehl an der Eingabeaufforderung ein:

   ```
   "\Programme\Software AG\Entire Connection n.n.n\OpenSSL.exe" req
   -new -x509 -key clientprivkey.pem -out clientcert.crt -days 1095
   -config openssl.cnf
   ```

   wobei *n.n.n* die Versionsnummer ist.

Denken Sie daran, dass Sie Ihren TN3270-Server für die Client-Authentifizierung konfigurieren müssen und dass Sie auch den Client-Schlüssel und das Zertifikat auf dem Server "installieren" müssen.

Mehr zu Zertifikaten

Zertifikate mit Microsoft Internet Explorer exportieren

Es ist möglich, vertrauenswürdige Zertifikate aus dem Microsoft Internet Explorer heraus zu exportieren. Weitere Informationen (in englischer Sprache) finden Sie bei *http://www.microsoft.com/windows/ie/using/howto/security/digitalcert/using.mspx*.

Exportieren Sie alle vertrauenswürdigen Stammzertifizierungsstellen, die Sie benötigen. Es ist wichtig, dass Sie alles im Format **Base-64-codiert X.509** exportieren.

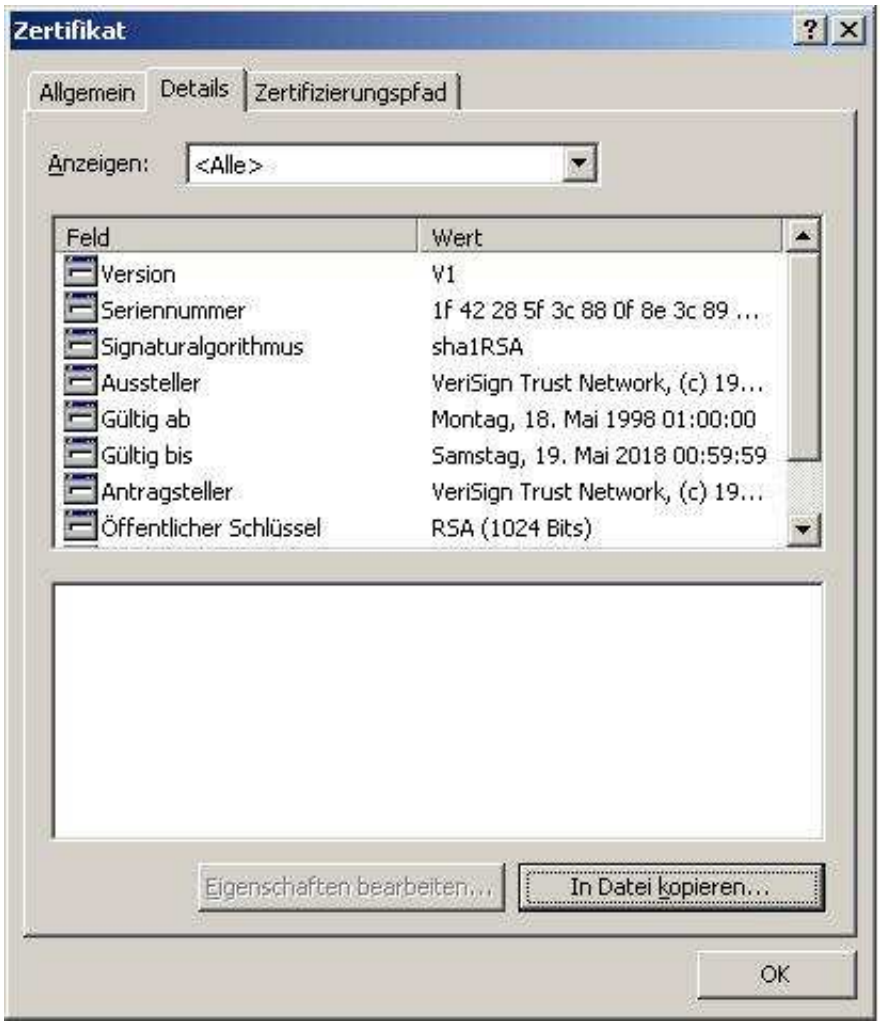
Stammzertifikate von Zertifizierungsstellen herunterladen

Es ist auch möglich, ein Stammzertifikat direkt von der Web-Seite einer Zertifizierungsstelle herunterzuladen. Dieses Zertifiat ist eventuell nicht im richtigen Format (Entire Connection benötigt Base-64). Um zu überprüfen, ob das Zertifikat im Base-64-Format ist, öffnen Sie es mit einem ASCII-Editor (z.B. dem Windows-Editor). Wenn in der ersten Zeile "BEGIN CERTIFICATE" steht und "END CERTIFICATE" in der letzten Zeile, dann ist das Format bereits Base-64 und Sie können das Zertifikat so benutzen wie es ist.

Wenn das Zertifikat nicht im Base-64-Format ist, müssen Sie es wie unten beschrieben ändern.

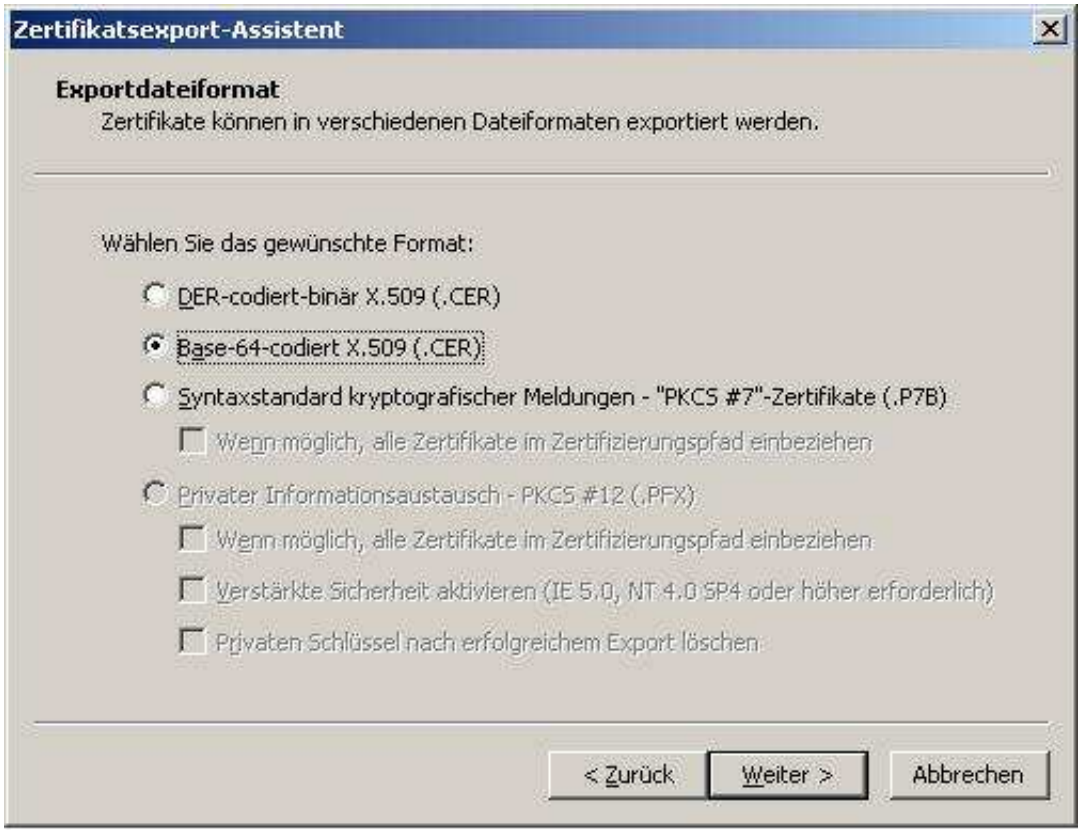
Das Format des Zertifikats in Base-64 ändern

1. Öffnen Sie das Zertifikat und zeigen Sie die Seite **Details** an. Beispiel:



2. Wählen Sie die Befehlsschaltfläche **In Datei kopieren**, um den **Zertifikatsexport-Assistent** aufzurufen.

3. Wählen Sie die Befehlsschaltfläche **Weiter**, um die nächste Seite anzuzeigen.
4. Markieren Sie die Option **Base-64 codiert X.509 (.CER)**.



5. Wählen Sie die Befehlsschaltfläche **Weiter**, um die nächste Seite anzuzeigen.
6. Geben Sie den Namen der Datei an, in die Sie das geänderte Zertifikat exportieren möchten.
7. Wählen Sie die Befehlsschaltfläche **Weiter**, um die nächste Seite anzuzeigen.
8. Wählen Sie die Befehlsschaltfläche **Fertig stellen**.