Secure Socket Layer (SSL)

Gilt für die Geräte:

HL-4040CN	✓
HL-4050CDN	✓
HL-4070CDW	✓
DCP-9040CN	✓
DCP-9045CDN	✓
MFC-9440CN	✓
MFC-9840CDW	✓

Inhalt

1: Allgemeiner Überblick

Mit Secure Socket Layer (SSL) können Daten beim Senden über ein LAN (Local Area Network) oder WAN (Wide Area Network) effektiv geschützt werden. Brother setzt dieses Protokoll jetzt auch für die neue Produktreihe an Farblaser-Netzwerkgeräten ein. Daten eines Druckauftrages werden beim Senden über das Netzwerk verschlüsselt. Jeder der versucht diese Daten abzufangen, wird die verschlüsselten Daten nicht lesen können.

Das Protokoll kann in verkabelten und drahtlosen Netzwerken konfiguriert werden. Mit anderen Sicherheitsmaßnahmen wie WPA Key und Firewall ist es ebenfalls einsetzbar.

2: Kurzer geschichtlicher Rückblick

Ursprünglich wurde SSL zum Schutz von Internetverkehrsdaten erstellt, insbesondere für den Datenaustausch zwischen Web-Browsern und Servern. Falls Sie Online-Banking nutzen und Sie in der URL-Zeile https:// und das kleine Vorhängeschloss unten rechts im Rahmen Ihres Web-Browser-Fensters sehen, dann nutzen Sie SSL. SSL wurde z. B. für den Einsatz mit Telnet, Druckern und FTP-Software weiter entwickelt und wurde so zur einheitlichen Lösung für die Online-Sicherheit. Der ursprüngliche Verwendungszweck wird auch heute noch von vielen Banken und Händlern zum Sichern vertraulicher Daten wie Kreditkarten- und Kundendaten im Internet genutzt.

SSL nutzt einen sehr hohen Verschlüsselungsgrad und wird weltweit von vielen Banken eingesetzt, da es als vertrauenswürdiges und sicheres Schutzinstrument angesehen wird. Laut VeriSign™ (führende Zertifizierungsstelle (CA)[1] für SSL) würde ein Hacker mit dem Entschlüsseln eines normal SSL-verschlüsselten Dokumentes zu Lebzeiten nicht fertig werden.

3: Vorteile für den Kunden

SSL wird von Brother in den Farblaser-Netzwerkgeräten eingesetzt, um den sicheren Druck über ein IP-Netzwerk zu gewährleisten. Nicht autorisierte Nutzer werden am Lesen der zum Drucker gesendeten Daten gehindert. Das entscheidende Verkaufsargument ist, vertrauliche Daten sicher zu drucken. Eine Personalabteilung von einem großen Unternehmen druckt zum Beispiel die Gehaltsabrechnungen regelmäßig selbst aus. Ohne Verschlüsselung ist es für andere Nutzer im Netzwerk möglich, die Daten dieser Gehaltsabrechnungen einzulesen. Versucht ein Nutzer jedoch die mit SSL-verschlüsselten Daten einzulesen, werden anstelle der Gehaltsabrechnungsdaten nur kodierte Datenmengen angezeigt.

4: Anwendung (Standardinstallation)

Zum Drucken über ein gesichertes Netzwerk sind installierte digitale Zertifikate erforderlich. Diese Zertifikate müssen auf dem Drucker und dem Gerät, das die Daten zum Drucker sendet wie z. B. ein Computer, installiert sein. Zum Konfigurieren des Zertifikats muss sich der Benutzer beim Drucker über einen Web-Browser mit der IP-Adresse anmelden und auf "Netzwerkkonfiguration" und "Zertifikat konfigurieren" klicken. Der Benutzer hat jetzt folgende zwei Optionen:

1. Privates Zertifikat erstellen und installieren

2. Zertifikat von einer Zertifizierungsstelle[1] (CA) nutzen

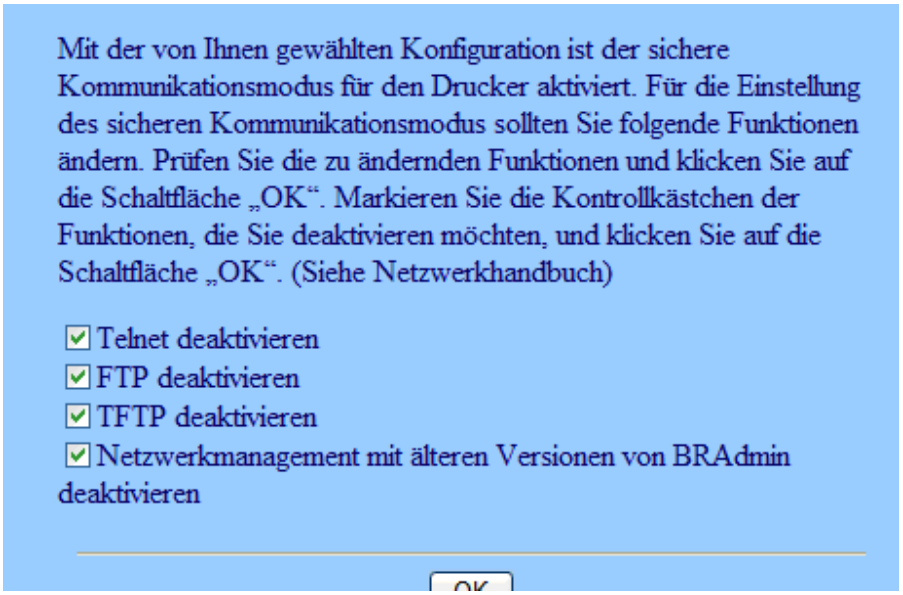
[1] *Die Zertifizierungsstelle (CA) ist eine Organisation, die digitale Zertifikate bestätigt und herausgibt.*

4.1. Privates Zertifikat erstellen

Nachdem Sie auf "Privates Zertifikat erstellen" geklickt haben, geben Sie den Hostnamen oder die IP-Adresse sowie die Gültigkeitsdauer (oft bereits ausgefüllt) an. Klicken Sie auf "Senden". Das Gerät übernimmt diese Daten in ein Zertifikat.

Sie werden dann aufgefordert, die Sicherheit der SSL-Verbindung durch Deaktivieren bestimmter Funktionen festzulegen.

Brother empfiehlt zur Sicherung der Kommunikation die Protokolle Telnet, FTP, TFTP und das Netzwerkmanagement mit älteren Versionen von BRAdmin (2.8 oder niedriger) zu deaktivieren. Sind diese aktiviert, so ist die Benutzerauthentifizierung nicht gesichert.

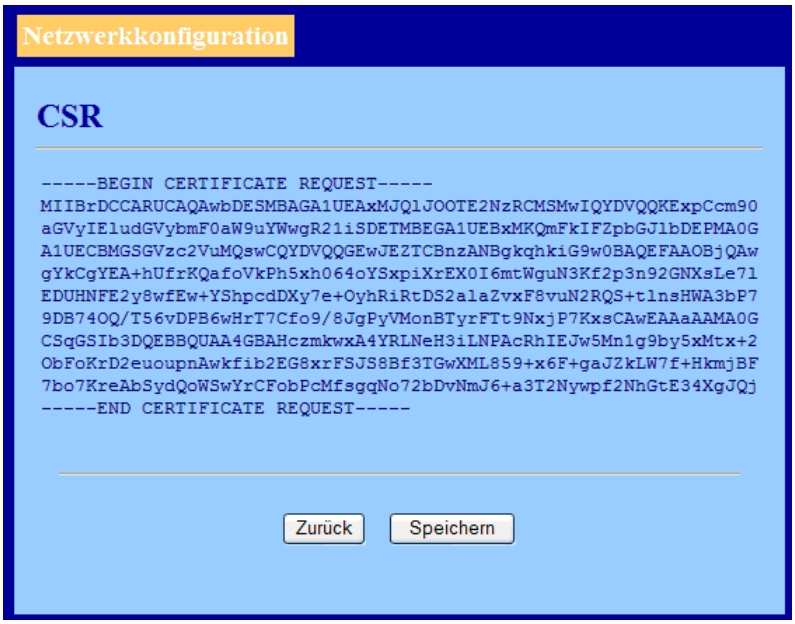


4.2. Zertifikatsignieranforderung (CSR) erstellen

Mit der Zertifikatsignieranforderung wird bei der Zertifizierungsstelle die Ausstellung eines Zertifikats beantragt und somit die Beurkundung des Zertifikatinhalts.

Geben Sie nach dem Klicken auf "Zertifikat erstellen" Ihre Firmendaten ein. Klicken Sie auf "Weiter". Ihre Firmendaten sind erforderlich, damit die Zertifizierungsstelle Ihre Identität bestätigen und für Dritte bescheinigen kann.

Nach kurzer Zeit erhalten Sie das Zertifikat. Das Zertifikat kann als kleine Datei gespeichert oder kopiert und direkt online in ein Zertifikatsignieranforderungsformular der Zertifizierungsstelle kopiert werden. Zertifizierungsstellen sind unter anderem VeriSign™ und Thawte™. Folgen Sie den Bestimmungen Ihrer Zertifizierungsstelle, um eine Zertifikatsignieranforderung zu senden.

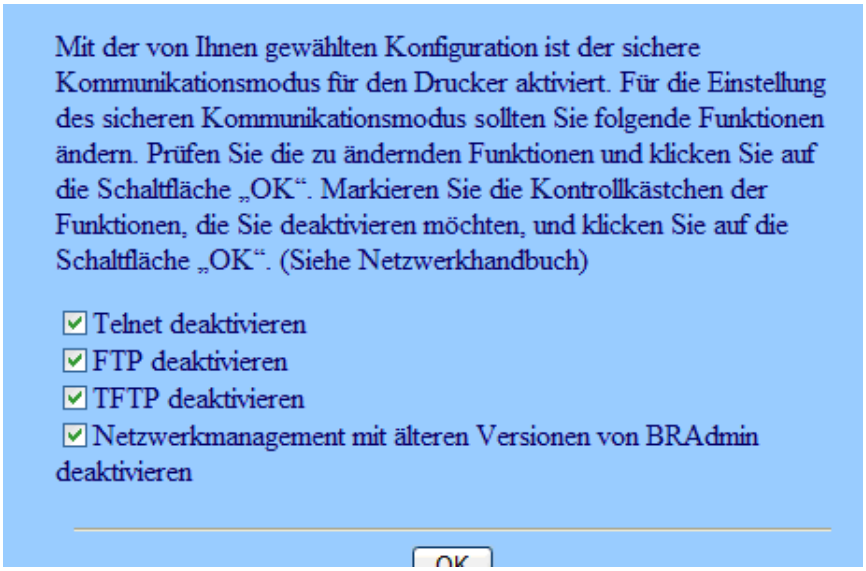


Sobald Sie das Zertifikat von der Zertifizierungsstelle erhalten haben, folgen Sie zum Installieren des Zertifikats auf Ihrem PrintServer den nachfolgenden Schritten (nur das für die Zertifikatsignieranforderung dieses Druckers ausgestellte Zertifikat kann installiert werden).

Klicken Sie auf der Seite Zertifikat konfigurieren auf Zertifikat installieren.

Geben Sie die Datei mit dem von der Zertifizierungsstelle ausgestellten Zertifikat an und klicken Sie auf Senden.
Das Zertifikat wurde jetzt erfolgreich erstellt. Aktivieren Sie die Kontrollkästchen der Funktionen, die Sie deaktivieren möchten. Klicken Sie abschließend auf OK.

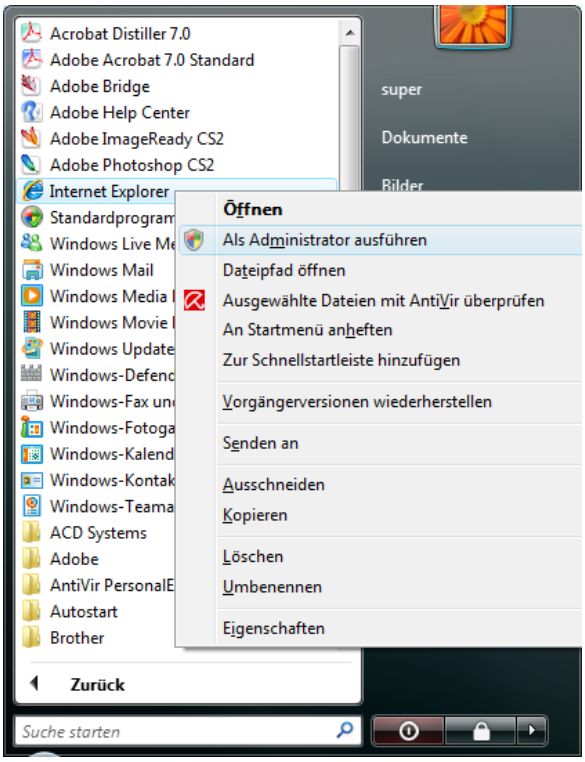
Brother empfiehlt zur Sicherung der Kommunikation die Protokolle Telnet, FTP, TFTP und das Netzwerkmanagement mit älteren Versionen von BRAdmin (2.8 oder niedriger) zu deaktivieren. Sind diese aktiviert, so ist die Benutzerauthentifizierung nicht gesichert.



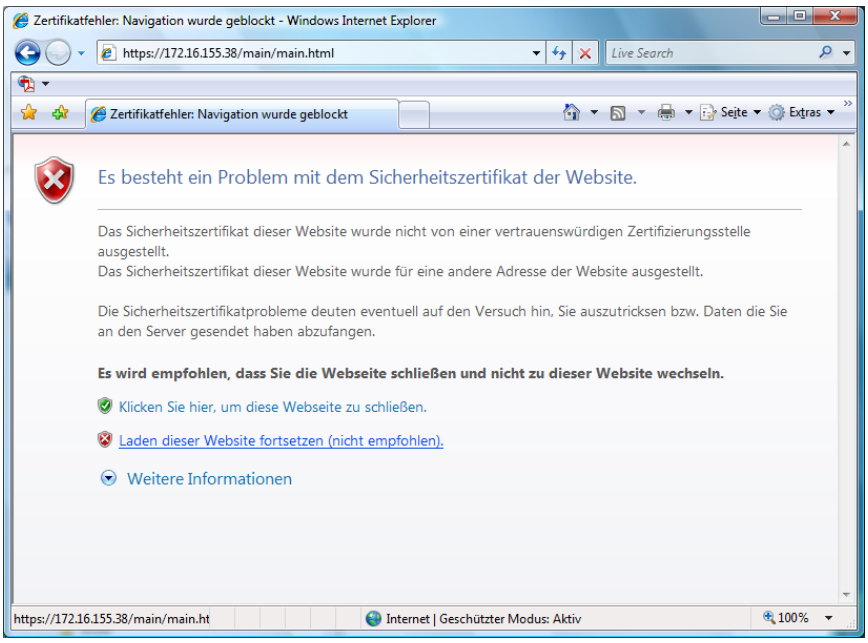
Um die Konfiguration zu aktivieren, starten Sie den Drucker neu.

4.3 Zertifikat unter Windows Vista™ installieren

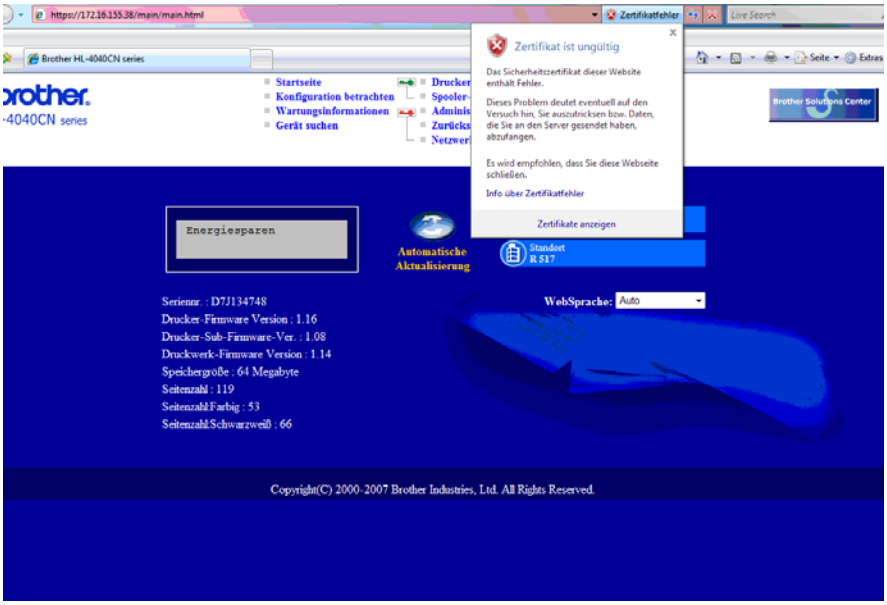
Melden Sie sich zuerst bei Ihrem Computer als Administrator an. Klicken Sie auf "Start" und "Alle Programme". Klicken Sie mit der rechten Maustaste auf "Internet Explorer" und dann auf "Als Administrator ausführen".



Klicken Sie auf "Laden dieser Website fortsetzen".

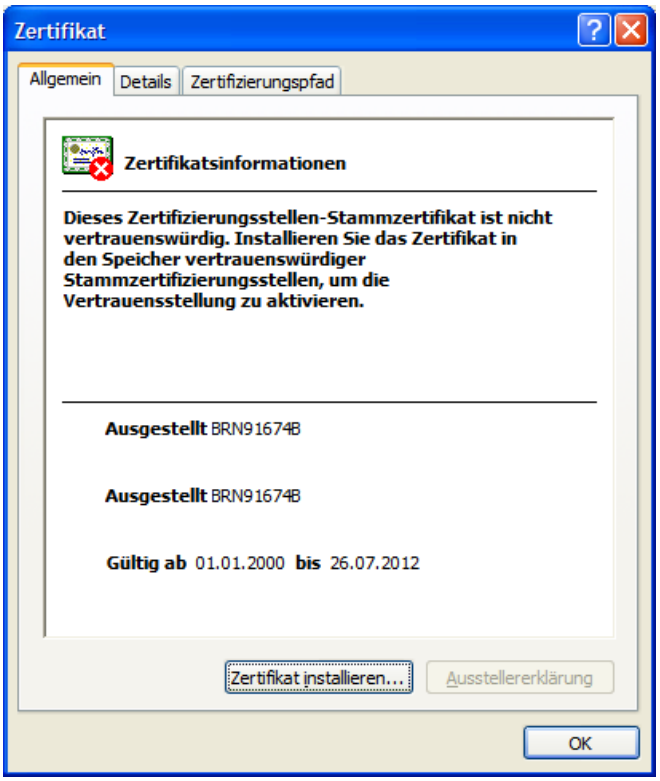


Klicken Sie auf "Zertifikatsfehler" und dann auf "Zertifikat anzeigen". In Abschnitt 4.4 erhalten Sie die Fortsetzung der Installationsanleitung.

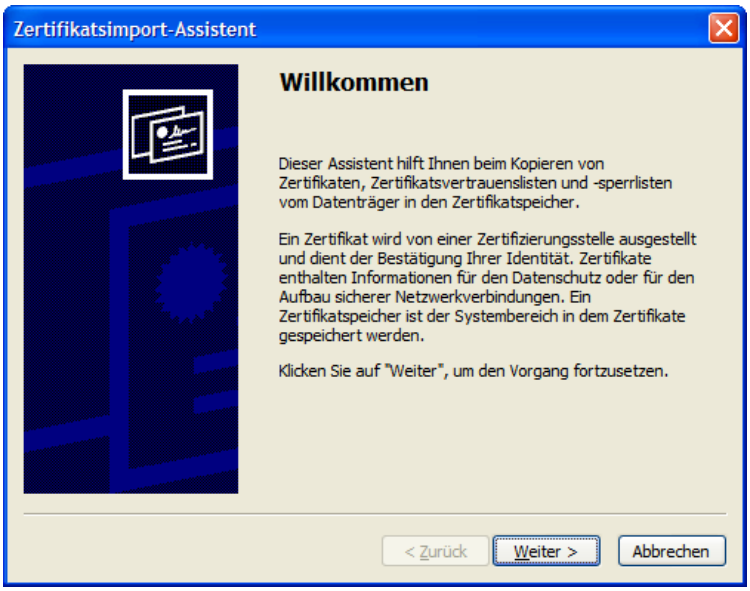


4.4 Zertifikat unter Windows® XP installieren

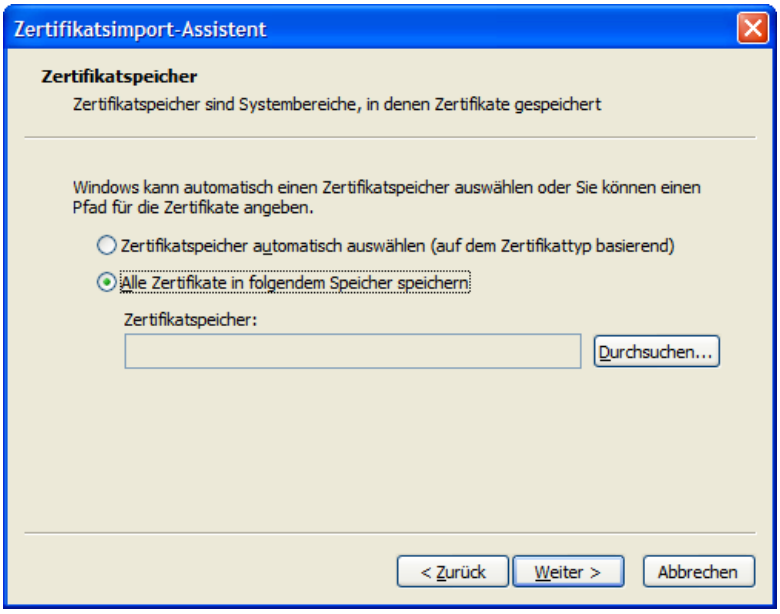
Starten Sie den Internet Explorer und geben Sie zum Zugreifen auf Ihren Drucker “https://IP-Adresse des Druckers/” in die URL-Zeile ein. Klicken Sie danach auf "Zertifikat anzeigen" und "Zertifikat installieren".



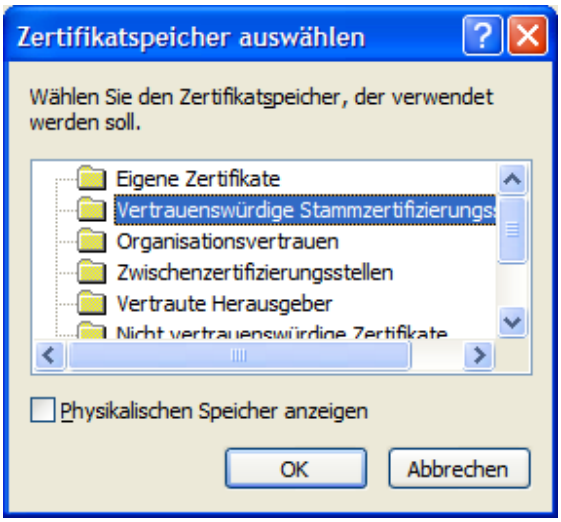
Der "Zertifikatsimport-Assistent" wird angezeigt. Zum Fortfahren klicken Sie auf "Weiter".

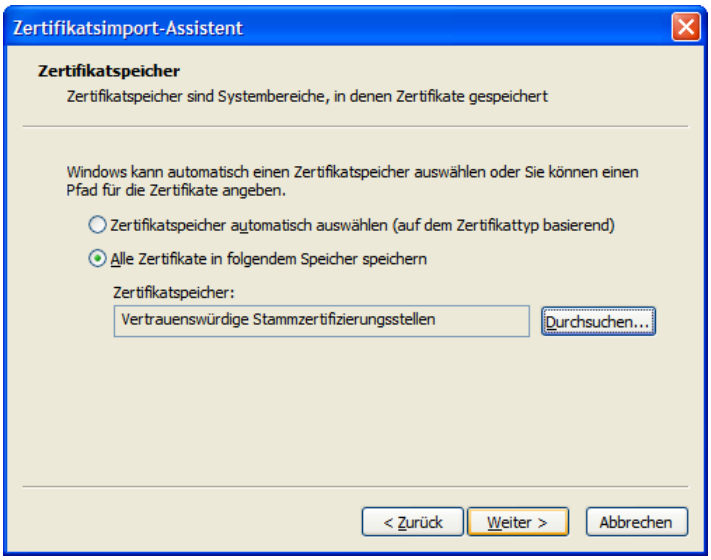


Geben Sie zum Speichern des Zertifikats einen Speicherort an. Brother empfiehlt Ihnen, die Option "Alle Zertifikate in folgendem Speicher speichern" auszuwählen und auf "Durchsuchen" zu klicken.

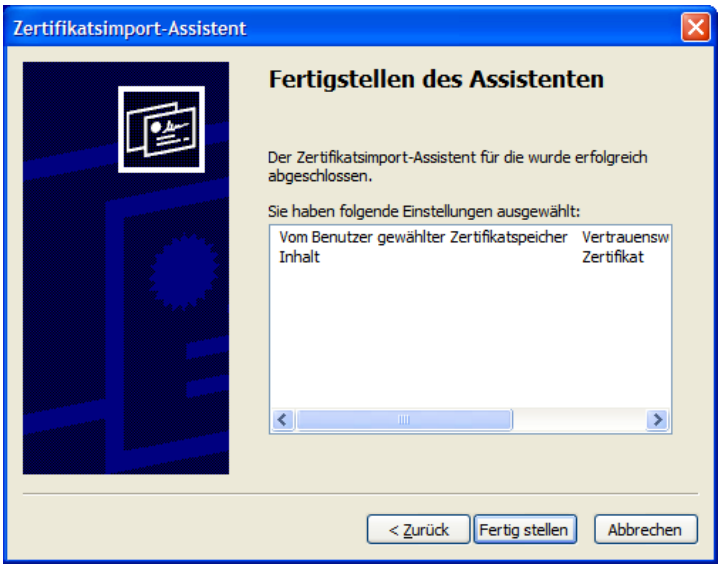


Wählen Sie "Vertrauenswürdige Stammzertifizierungsstellen". Klicken Sie auf "OK" und "Weiter".





Klicken Sie im nächsten Fenster auf "Fertig stellen". Zum Installieren des Zertifikats klicken Sie auf "Ja".



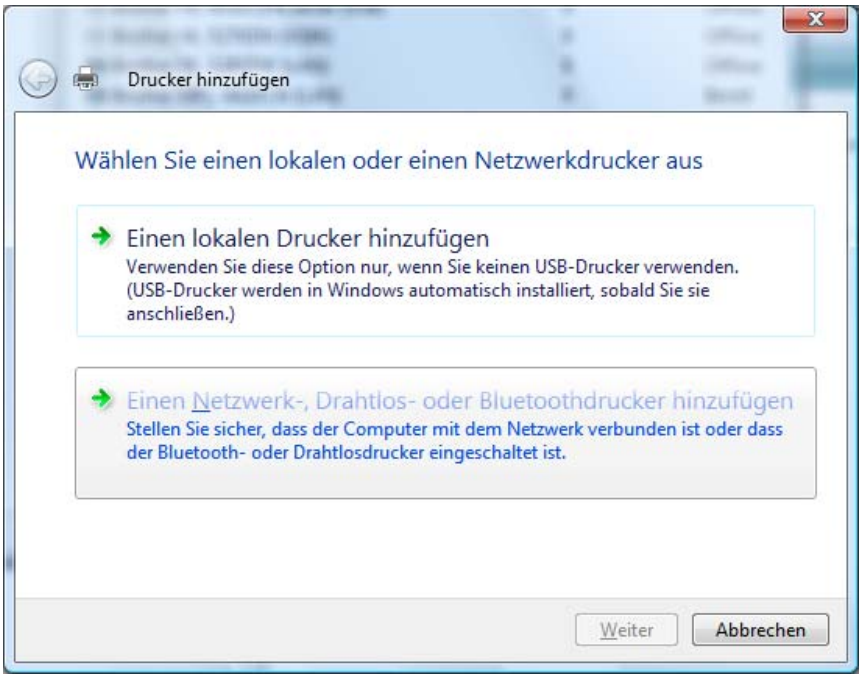
Zum sicheren Drucken muss an jedem Computer derselbe Vorgang ausgeführt werden. Ist das Zertifikat erst einmal installiert, muss es erst dann neu installiert werden, wenn Änderungen am Zertifikat gemacht werden.

Ein sicherer Druck kann nur durch Konfigurieren des Internet Printing Protocol[2] (IPP) und nicht über eine Standardnetzwerkinstallation erfolgen. Informationen zum Konfigurieren mit IPP erhalten Sie im Netzwerkhandbuch.

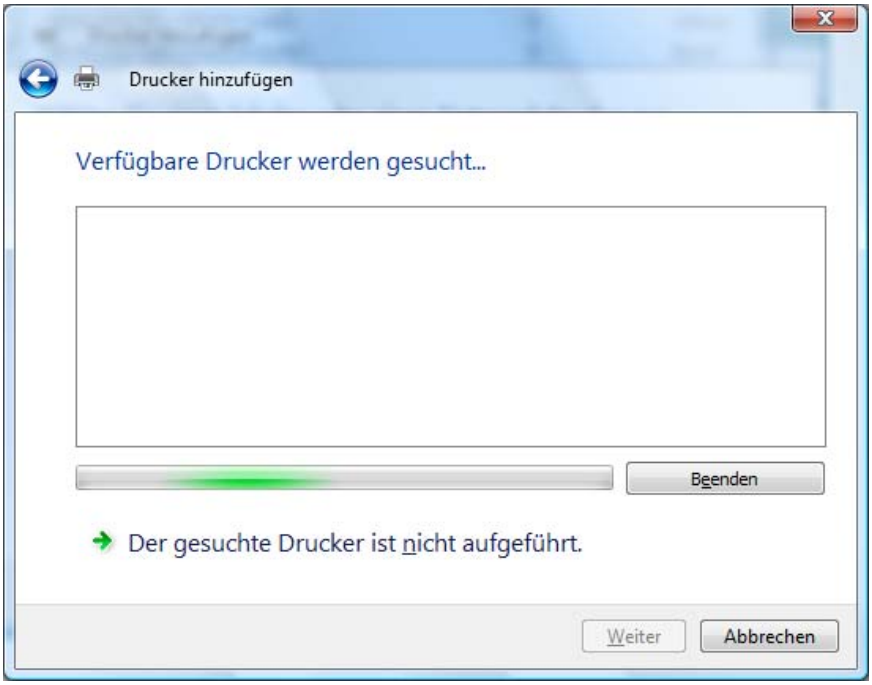
[2] *IPP ist ein Standarddruckprotokoll zum Verwalten und Führen von Druckaufträgen. Es kann sowohl lokal als auch global eingesetzt werden, sodass im Grunde Personen weltweit auf einem Drucker drucken könnten.*

4.5 IPP unter Windows Vista™ konfigurieren

Starten Sie den "Druckerinstallations-Assistent" und klicken Sie auf "Einen Netzwerk-, Drahtlos- oder Bluetoothdrucker hinzufügen".

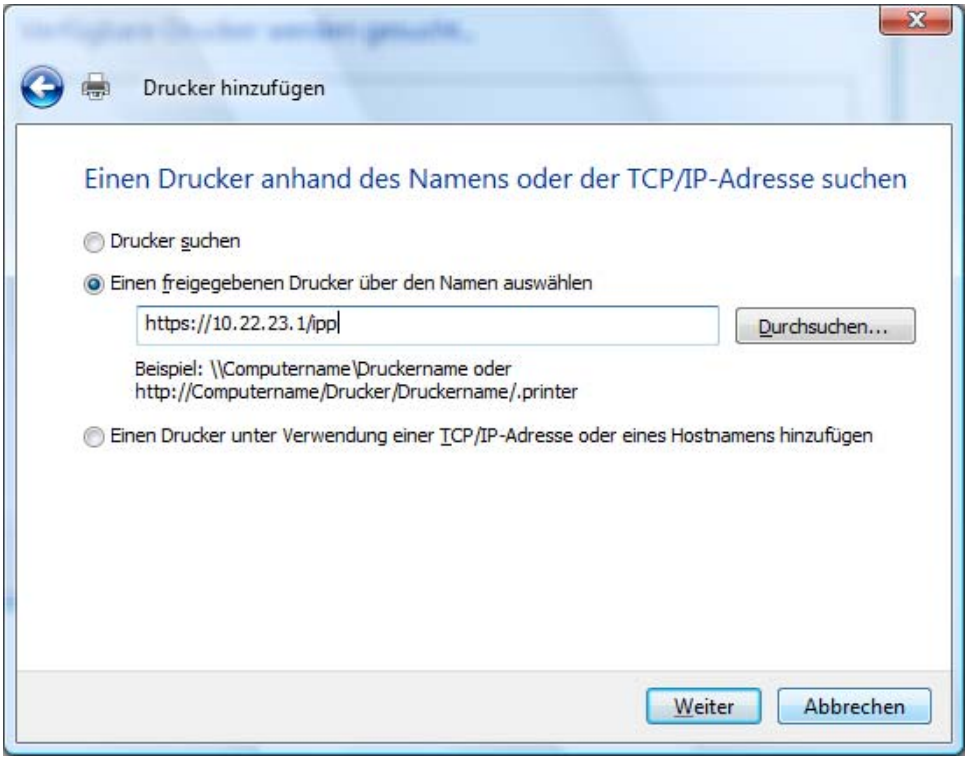


Klicken Sie auf "Der gesuchte Drucker ist nicht aufgeführt".



Wählen Sie "Einen freigegebenen Drucker über den Namen auswählen" und geben Sie die folgende URL ein: https://IP-Adresse_des_Druckers/ipp (“IP-Adresse_des_Druckers” steht für die IP-Adresse oder den Knotennamen Ihres Druckers).

Hinweis:
Geben Sie https://' für das sichere Drucken über IPP ein und verwenden Sie nicht http://.

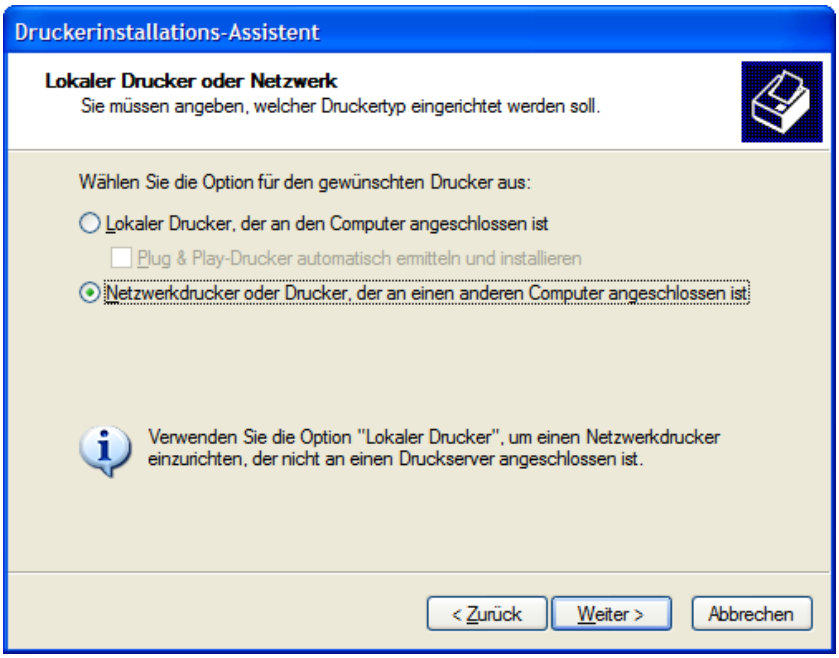


Der Assistent sucht im Netzwerk nach dem Drucker. Entweder findet er die Treiber oder Sie werden aufgefordert, den Druckerhersteller auszuwählen oder den Treiber einzulegen. Falls der Treiber auf einem Datenträger ist, wählen Sie "Durchsuchen" und navigieren Sie zum Speicherort des Treibers.

Der Druckertreiber wird installiert. Sie können den Drucker als Standarddrucker einrichten und eine Testseite drucken. Der Drucker ist fertig installiert und Sie können jetzt sicher drucken.

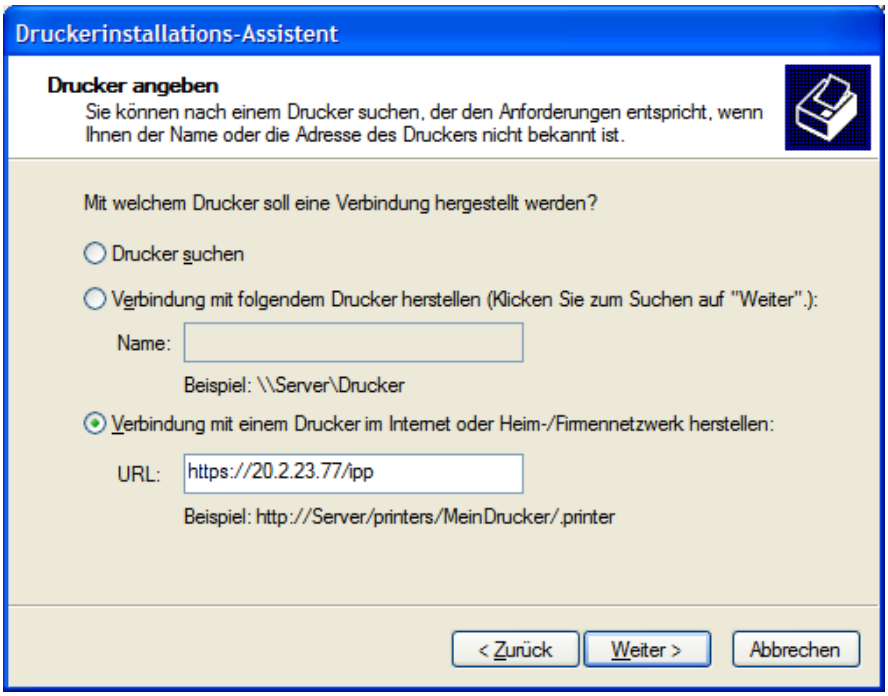
4.6 IPP unter Windows® XP konfigurieren

Starten Sie den "Druckerinstallations-Assistent" und wählen Sie "Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist".



Starten Sie den "Druckerinstallations-Assistent" und wählen Sie "Netzwerkdrucker oder Drucker, der an einen anderen Computer angeschlossen ist". Wählen Sie die Option Verbindung mit einem Drucker im Internet oder Heim-/Firmennetzwerk herstellen und geben Sie Folgendes in das Feld URL ein: https://IP-Adresse_des_Druckers/ipp. Klicken Sie auf Weiter.

Hinweis:
Geben Sie https://' für das sichere Drucken über IPP ein und verwenden Sie nicht http://.



Der Assistent sucht im Netzwerk nach dem Drucker. Entweder findet er die Treiber oder Sie werden aufgefordert, den Druckerhersteller auszuwählen oder den Treiber einzulegen. Falls der Treiber auf einem Datenträger ist, wählen Sie "Durchsuchen" und navigieren Sie zum Speicherort des Treibers.

Der Druckertreiber wird installiert. Sie können den Drucker als Standarddrucker einrichten und eine Testseite drucken. Der Drucker ist fertig installiert und Sie können jetzt sicher drucken.

Eine detaillierte Anleitung erhalten Sie im Benutzerhandbuch.

5: Technischer Überblick

Mit Secure Socket Layer (SSL) werden Daten, die im LAN oder WAN verschickt werden, auf der Transportebene mit Internet Printing Protocol (IPP) geschützt. Nicht autorisierte Benutzer können die Daten daher nicht lesen.
Es werden Authentifizierungsprotokolle in Form von 2 digitalen Schlüsseln eingesetzt.

1. Ein Public Key - der zum Drucken für alle bekannt ist.
2. Ein Private Key - der nur für den Drucker zum Entschlüsseln von Paketen (damit die Daten für den Drucker lesbar sind) bekannt ist.

Der Public Key nutzt 1024-Bit-Verschlüsselung und ist in einem digitalen Zertifikat enthalten, das auf dem Client-Computer installiert sein muss. Diese Zertifikate sind entweder privat oder von einer Zertifizierungsstelle (CA) genehmigt.

Es gibt drei unterschiedliche Schlüssel: Private Key, Public Key und Shared Key.

Der Private Key ist nur dem Drucker bekannt und ist dem Public Key zugeordnet, aber nicht in dem digitalen Zertifikat der Clients (Sender) beinhaltet. Der Drucker sendet beim ersten Verbindungsaufbau den Public Key mit dem Zertifikat. Der Client-Computer erkennt den Public Key vom Drucker mit dem Zertifikat an. Der Client erzeugt den Shared Key und verschlüsselt ihn mit dem Public Key. Anschließend wird der Key zum Drucker gesendet. Der Drucker entschlüsselt den Shared Key mit dem Private Key. Der Drucker und der Client haben den Shared Key jetzt sicher ausgetauscht und eine sichere Verbindung zur Datenübertragung erstellt.

Die Druckdaten werden mit dem Shared Key verschlüsselt und entschlüsselt.

SSL kann Benutzer nicht am unbefugten Zugriff auf Datenpakete hindern, aber die Daten sind ohne Private Key nicht lesbar. Der Private Key ist nur dem Drucker bekannt.

Das Protokoll kann in verkabelten und drahtlosen Netzwerken konfiguriert werden. Mit anderen Sicherheitsmaßnahmen wie WPA Key und Firewall ist es mit entsprechender Konfiguration ebenfalls einsetzbar.