

Das nachfolgende Dokument wird unter der GPL- Lizenz veröffentlicht.

- Technical Whitepaper -

- Konfiguration L2TP-IPSEC Verbindung unter Windows - - VPN Gateway basiert auf StrongSwan -

Voraussetzungen zur Client Konfiguration:

- vorhandenes gültiges x509-Zertifikat mit allen Schlüsseln und CA-Teilen (am besten im pkcs12- Format)
- Vorhandensein des Import-Passwortes
- Administratorrechte des Rechners, auf dem die VPN Verbindung konfiguriert werden soll
- eingerichtete mobile VPN Verbindung auf einem VPN-Gateway (Roadwarrior Connection)

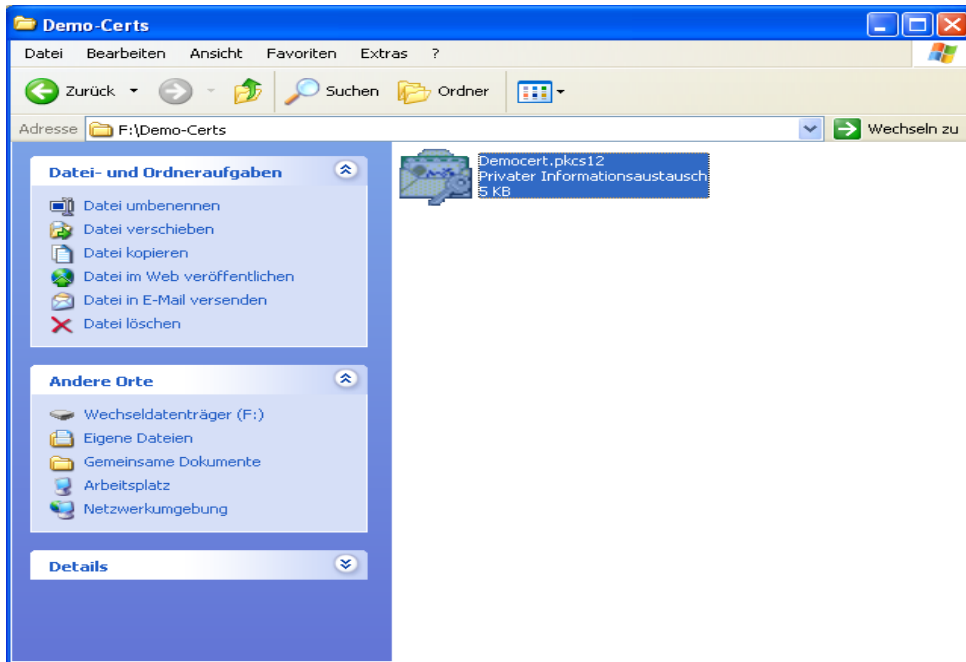
Einrichtung des mobilen VPN-Client:

Der Client wird in 2 prinzipiellen Schritten eingerichtet:

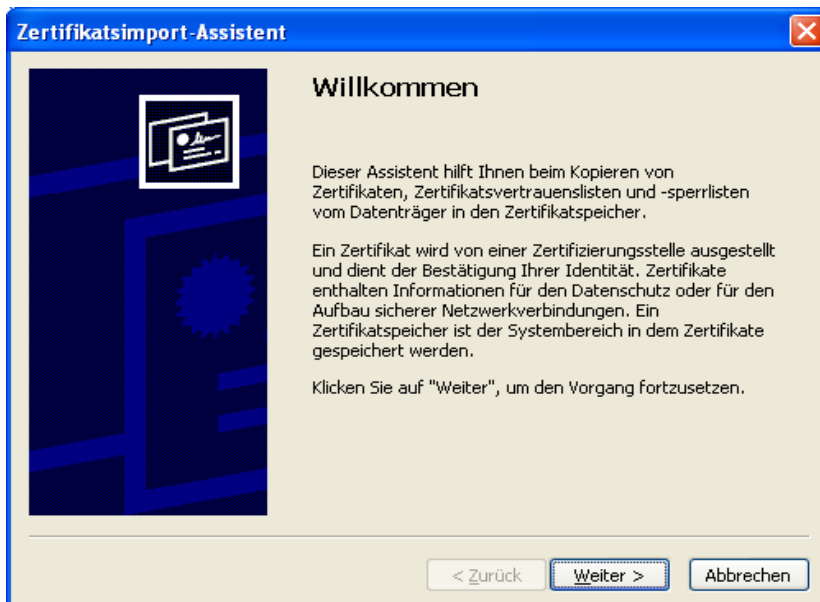
1. Import des vorliegenden gültigen Zertifikates
2. Einrichtung der L2TP-IPSEC Verbindung

Zertifikatimport:

Starten Sie den Explorer und wechsel Sie in den Path, im das Zertifikat gespeichert ist.



2. Führen Sie einen Doppelklick mit der Maus auf dem gewünschten Zertifikat aus.



Anschliessend „Weiter“.

Zertifikatsimport-Assistent

Importdateiname
Geben Sie die zu importierende Datei an.

Dateiname:
F:\Demo-Certs\Democert.pkcs12.p12 Durchsuchen...

Hinweis: Es können mehrere Zertifikate in einer einzigen Datei in folgenden Formaten gespeichert werden:

- Privater Informationsaustausch - PKCS #12 (.PFX, .P12)
- Syntaxstandard kryptografischer Meldungen - "PKCS #7"-Zertifikate (.P7B)
- Microsoft Serieller Zertifikatspeicher (.SST)

< Zurück **Weiter** > Abbrechen

Geben Sie den privaten Schlüssel des Zertifikates ein.

Zertifikatsimport-Assistent

Kennwort
Der private Schlüssel wurde mit einem Kennwort geschützt, um die Sicherheit zu gewährleisten.

Geben Sie das Kennwort für den privaten Schlüssel ein.

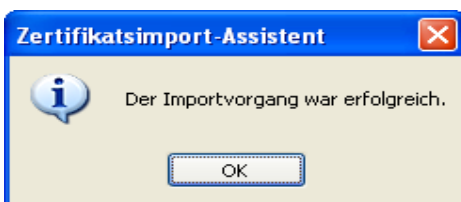
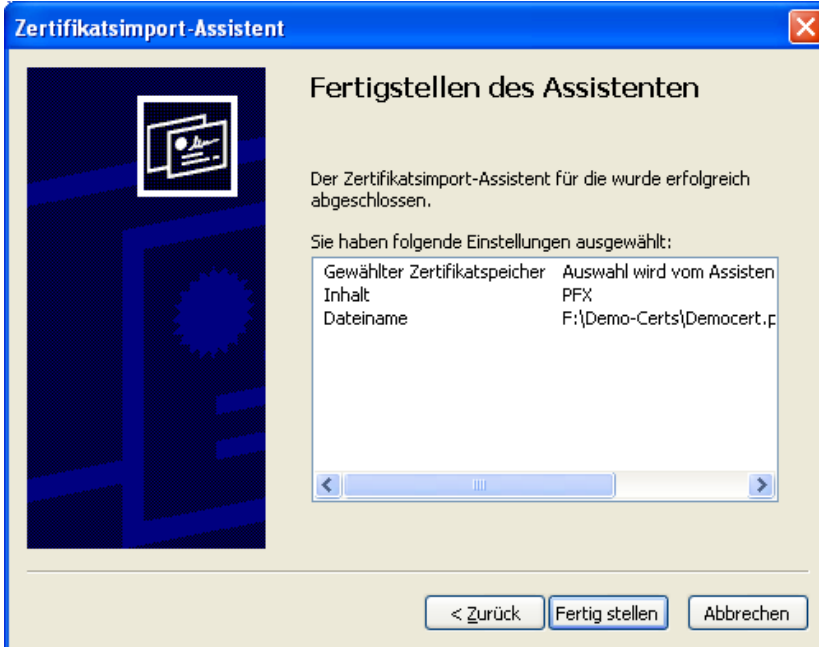
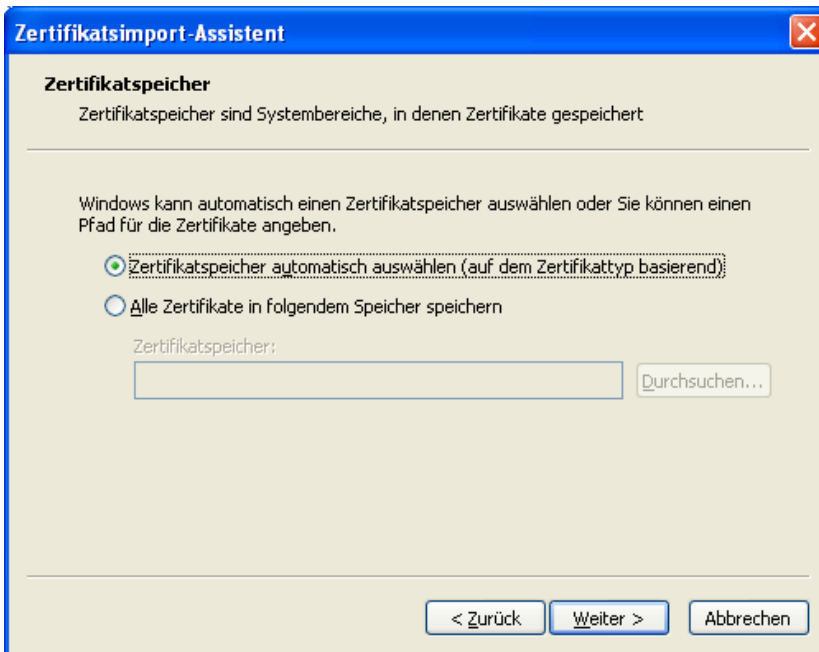
Kennwort:

Hohe Sicherheit für den privaten Schlüssel aktivieren. Immer wenn der private Schlüssel von einer Anwendung verwendet wird, werden Sie zur Eingabe aufgefordert, wenn Sie diese Option aktivieren.

Schlüssel als exportierbar markieren. Dadurch können Sie Ihre Schlüssel zu einem späteren Zeitpunkt sichern bzw. überführen.

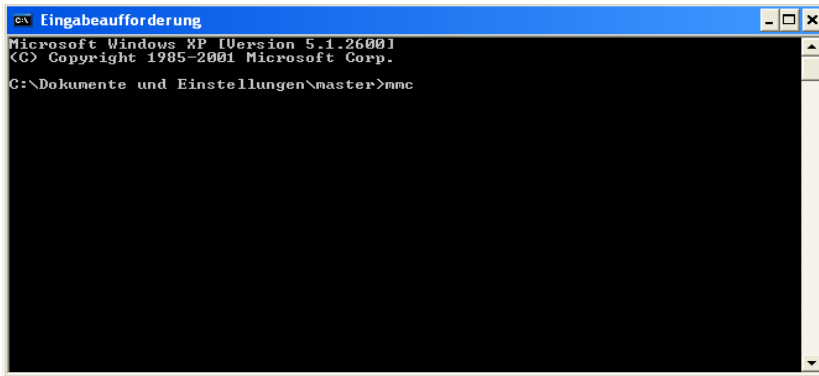
< Zurück **Weiter** > Abbrechen

Damit die einzelnen Teile des Zertifikates in den richtigen Speicher kopiert werden, sollten Sie „automatisch“ auswählen“.

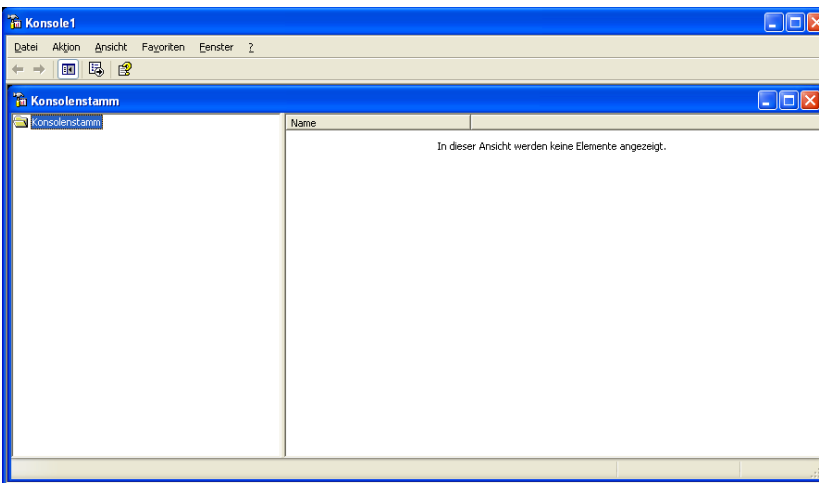


Überprüfung des erfolgreichen Zertifikatimports im Zertifikatsspeicher

Starten Sie hierzu eine Eingabekonsole (cmd) und starten Sie die Managementkonsole mit der Eingabe des Befehls mmc.



Im nachfolgenden Konsolenprogramm wählen Sie bitte Datei -> Snap-In hinzufügen



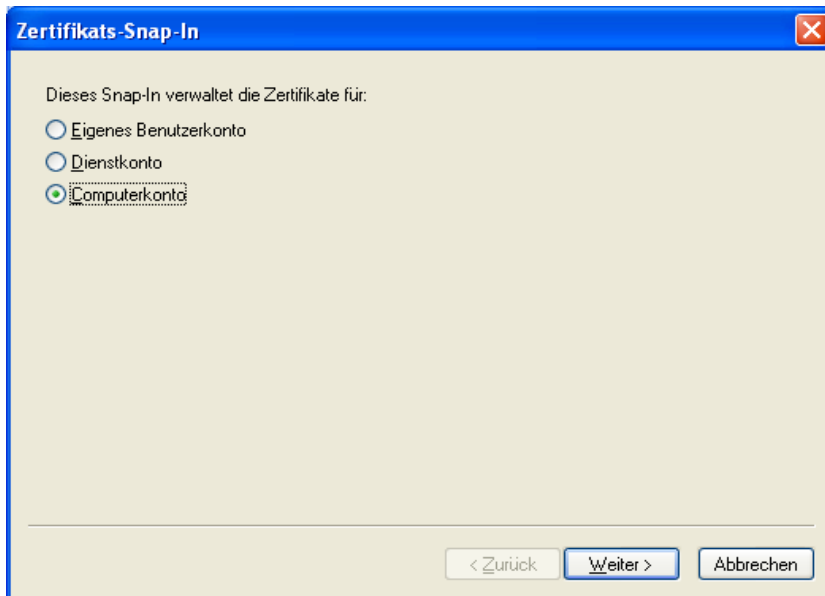
Im nachfolgenden Fenster wählen Sie „Hinzufügen ...“.



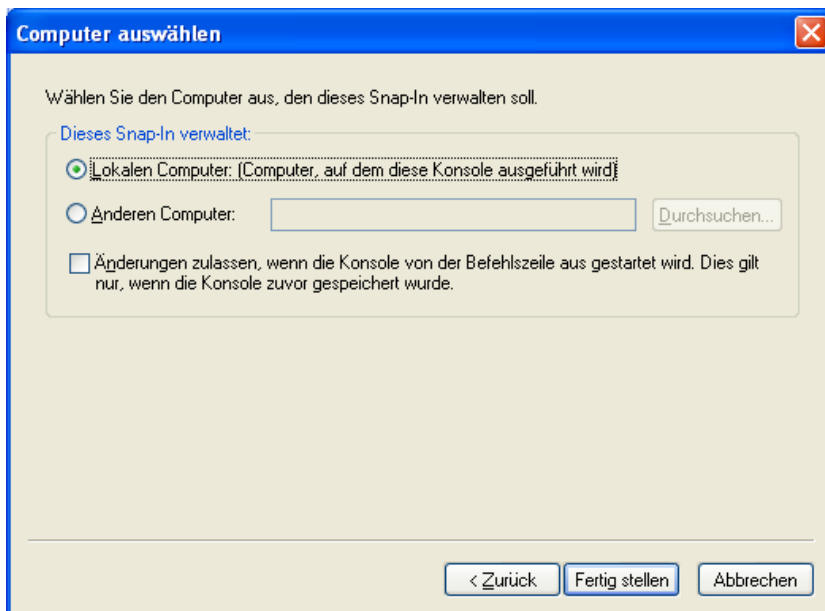
In den nun angezeigten Auswahl wählen Sie Zertifikate.



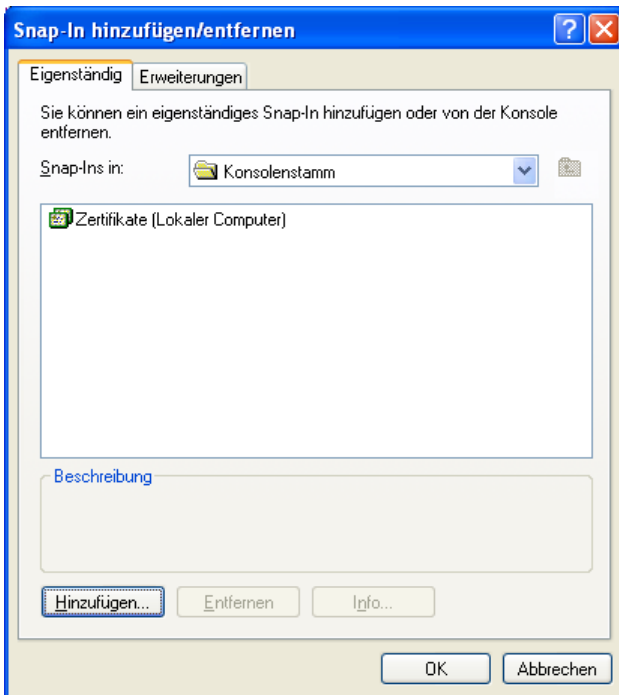
Je nach dem wie die Administration erfolgt und die Sicherheitsrichtlinien Festlegungen treffen ist nachfolgend die Auswahl zutreffen.



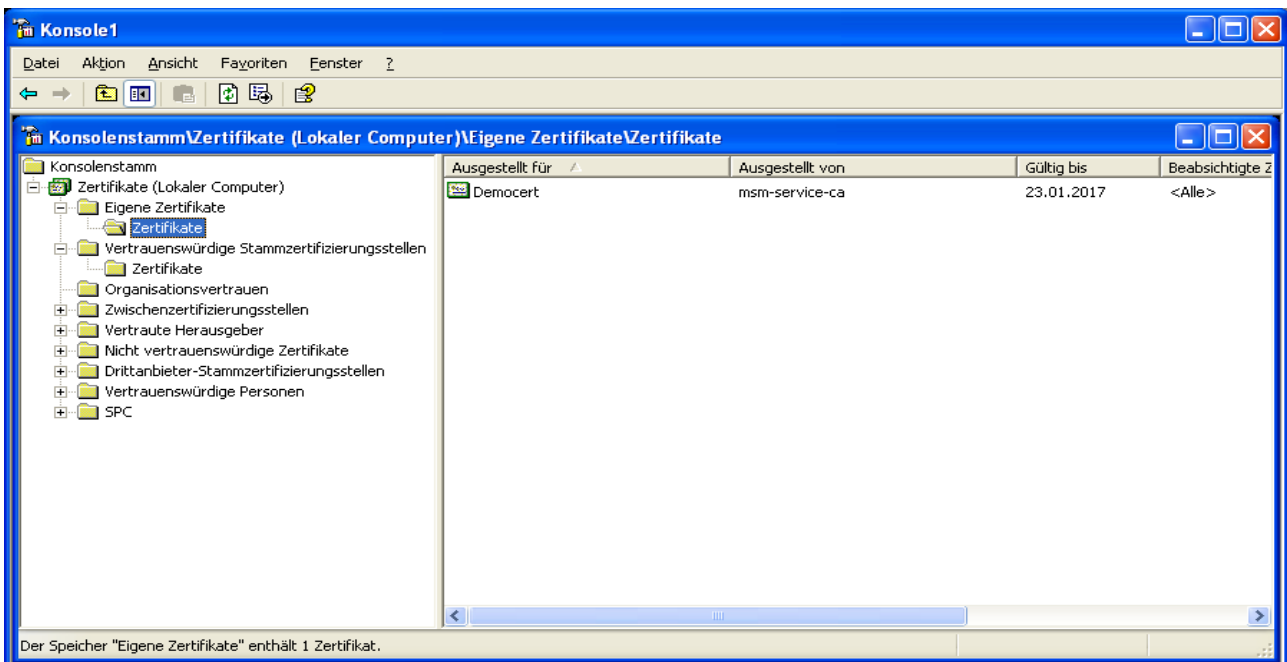
Entsprechend den Sicherheitsrichtlinien Auswahl treffen.



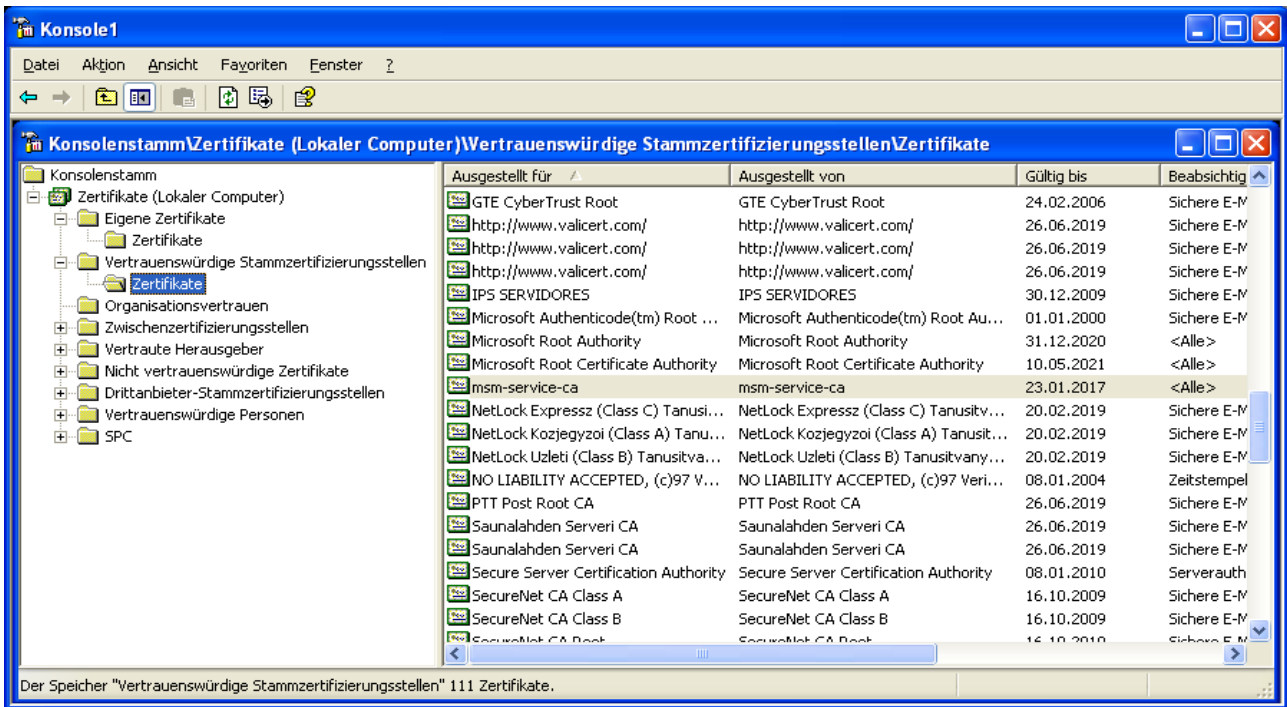
Nach entsprechender Auswahl erscheint wieder das Snap-In Auswahlfenster. Wir sind an dieser Stelle fertig. Also „OK“



Anschliessend erscheint wieder das Konsolenfenster, mit dem Eintrag „Zertifikate (Lokaler Computer)“. Unter „Eigene Zertifikate“ -> „Zertifikate“ wird das Zertifikat „Democert“ angezeigt.



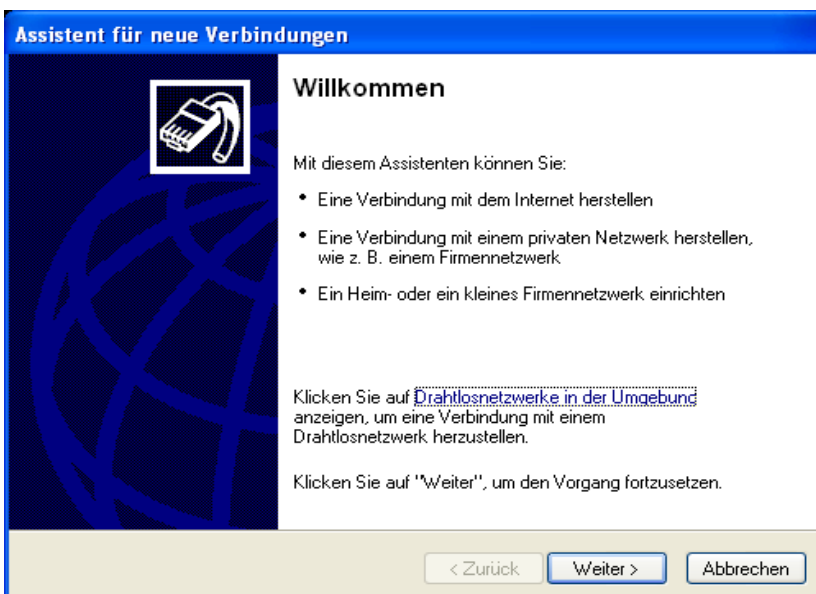
Unter „Vertrauenswürdige Stammzertifizierungsstellen“ -> „Zertifikate“ wird nun auch der CA-Part der importierten Zertifikates „msm-service-ca“ angezeigt.



Sicherheitstechnisch sind jetzt die Voraussetzungen zur Einrichtung einer L2TP-IPSEC Verbindung erfüllt.

Konfiguration der L2TP-IPSEC-Verbindung:


Wählen Sie im Menü Netzwerk „Neue Verbindung einrichten“.



Nachfolgend wählen Sie den Absatz für VPN Verbindungen.

Assistent für neue Verbindungen

Netzwerkverbindungstyp
Wie möchten Sie vorgehen?




- Verbindung mit dem Internet herstellen**
Stellt eine Verbindung mit dem Internet her, so dass Sie den Browser verwenden und E-Mail lesen können.
- Verbindung mit dem Netzwerk am Arbeitsplatz herstellen**
Stellt eine Verbindung mit einem Firmennetzwerk (über eine DFO- oder VPN-Verbindung) her, so dass Sie von zu Hause oder unterwegs arbeiten können.
- Ein Heim- oder ein kleines Firmennetzwerk einrichten**
Stellt eine Verbindung mit einem bestehenden Heim- oder kleinem Firmennetzwerk her oder richtet eine neue Verbindung ein.
- Eine erweiterte Verbindung einrichten**
Stellt eine direkte Verbindung mit einem anderen Computer über einen seriellen, parallelen oder Infrarotanschluss her oder richtet diesen Computer so ein, dass andere Computer darauf zugreifen können.

< Zurück Weiter > Abbrechen

Assistent für neue Verbindungen

Netzwerkverbindung
Wie soll die Netzwerkverbindung am Arbeitsplatz hergestellt werden?

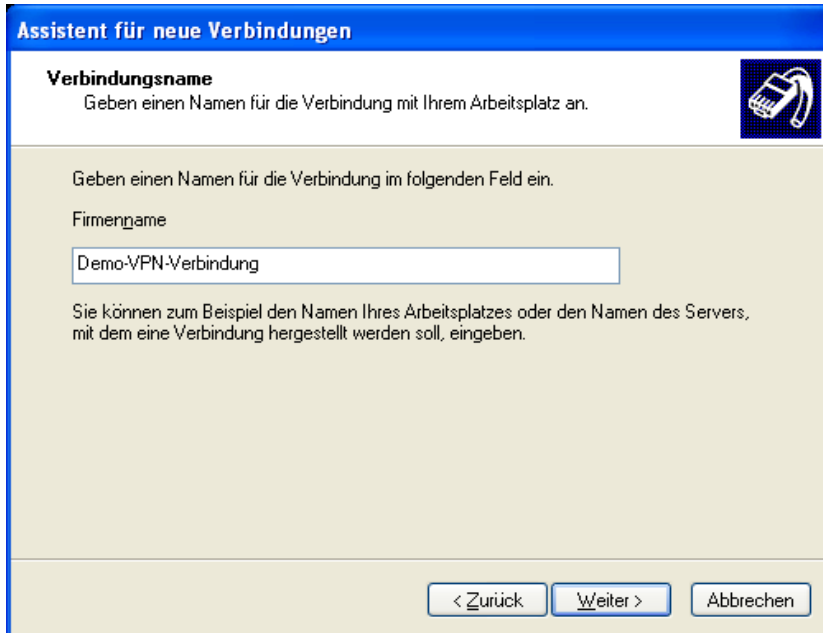


Folgende Verbindung erstellen:

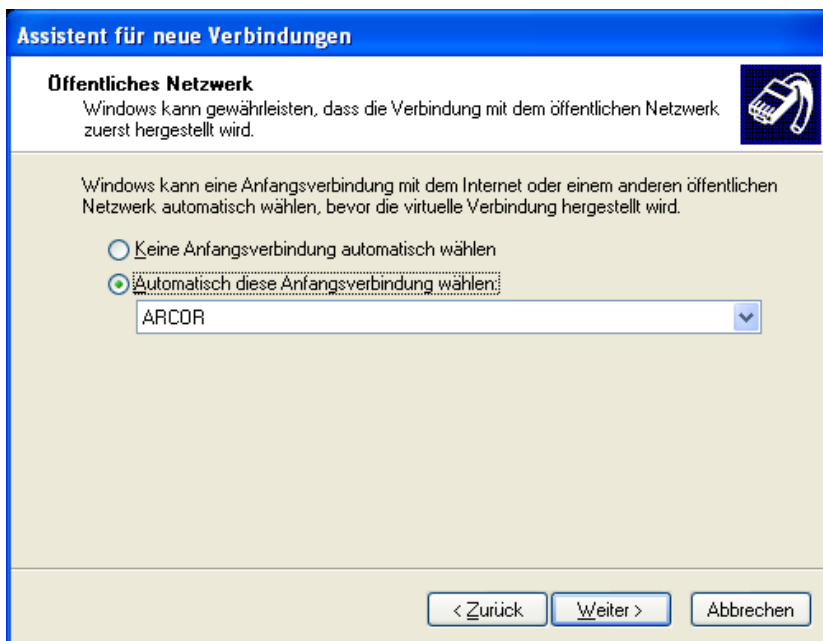
- DFO-Verbindung**
Stellt eine Verbindung über ein Modem und eine reguläre Telefonleitung oder über eine ISDN-Telefonleitung her.
- VPN-Verbindung**
Stellt eine Netzwerkverbindung mit einer VPN-Verbindung (Virtual Private Network) über eine Internetverbindung her.

< Zurück Weiter > Abbrechen

Nachfolgend geben Sie der VPN Verbindung einen Namen.



Die nachfolgende Auswahl trifft nur zu, wenn Sie zur Herstellung einer Internetverbindung sich bei einem Internetprovider einwählen müssen. Aus einem lokalen Netzwerk oder Homenetzwerk heraus können Sie Ihre normal Internetverbindung nutzen. Im nachfolgenden Beispiel wurde zum Beispiel ARCOR als Provider gewählt.



Im nachfolgenden Menü geben Sie bitte den FQDN oder die öffentliche IP Adresse Ihres VPN-Routers (Gateway) an.

Assistent für neue Verbindungen

VPN-Serverauswahl
Wie lautet der Name bzw. die Adresse des VPN-Servers?

Geben Sie den Hostnamen oder die IP-Adresse des Computers ein, zu dem eine Verbindung hergestellt werden soll.

Hostname oder IP-Adresse (z.B. microsoft.com oder 157.54.0.1):

< Zurück Weiter > Abbrechen

Assistent für neue Verbindungen

Fertigstellen des Assistenten

Die erforderliche Schritte zum Erstellen der folgenden Verbindung wurden ordnungsgemäß durchgeführt:

Demo-VPN-Verbindung

- Für alle Benutzer dieses Computers freigeben

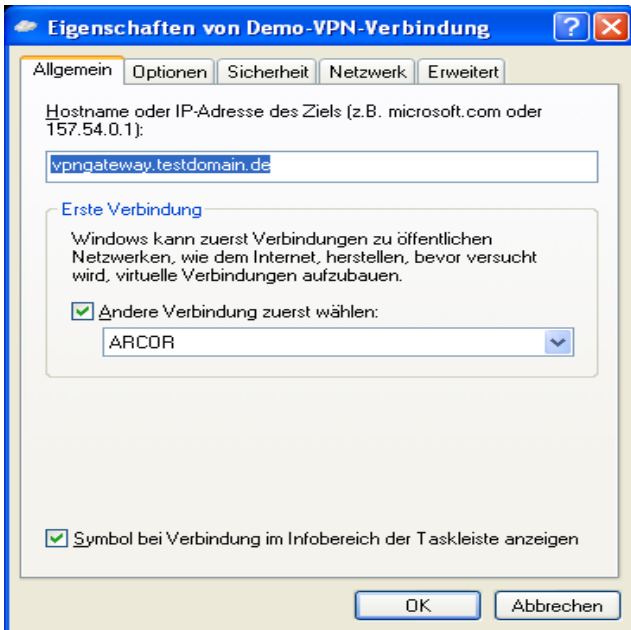
Die Verbindung wird im Ordner "Netzwerkverbindungen" gespeichert.

Verknüpfung auf dem Desktop hinzufügen

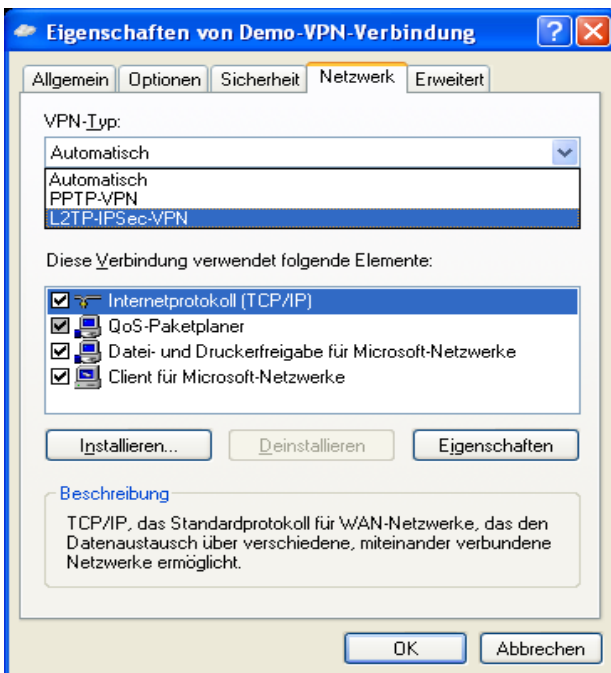
Klicken Sie auf "Fertig stellen", um diese Verbindung zu erstellen und den Vorgang abzuschließen.

< Zurück Fertig stellen Abbrechen

Zur Sicherheit sollten Sie die neu erstellte Verbindung bezüglich Ihrer Einrichtung nochmals überprüfen. Zum Aufruf der Überprüfung wählen Sie bitte im Kontextmenü der neuen Verbindung „Eigenschaften“.



Im Netzwerkmenü prüfen Sie bitte ob als VPN-Typ L2TP-IPSEC-VPN ausgewählt ist. Sollte dies nicht der Fall sein, so wählen Sie diese Verbindungsart aus.



Anschliessend können Sie diese mobile L2TP-IPSEC Verbindung testen. Sie benötigen in jedem Fall noch einen Benutzernamen und ein Passwort,