Net at Work
Building IT-Excellence.

NoSpamProxy 13.2

Anbindung an digiSeal server 2.0

- Encryption
- Large Files

Impressum

Net at Work GmbH
Am Hoppenhof 32a
D-33104 Paderborn

Handelsmarken

13. Februar 2020

Inhalt

1. Systemanforderungen

Der digiSeal server und NoSpamProxy Encryption können gemeinsam auf einem System betrieben werden. Sie können aber auch auf verschiedenen Computern installiert werden. Die Kommunikation zwischen dem digiSeal server und NoSpamProxy Encryption erfolgt standardmäßig über TCP/IP, Port 2001. Für diesen Port müssen auf den beteiligten Computern ggf. Ausnahmeregeln in vorhandenen Firewalls erstellt werden.

2. Zertifikatskonfiguration

Die Kommunikation zwischen NoSpamProxy Encryption und dem digiSeal server wird mit Hilfe von Zertifikaten verschlüsselt. Standardmäßig wird dafür das Zertifikat mit dem Namen „ `CN=<ComputerName>, CN=Net at Work Mailgateway` “ verwendet. Sind die beiden Dienste auf unterschiedlichen Computern installiert, muss dieses Zertifikat zunächst von NoSpamProxy Encryption zum digiSeal server übertragen werden.

Öffnen Sie dazu den Zertifikatsspeicher des lokalen Computer-Kontos. Öffnen Sie den Knoten **Persönliche Zertifikate / Personal** und wählen Sie das Zertifikat mit dem Namen Ihres Computers aus. (Bild 1).

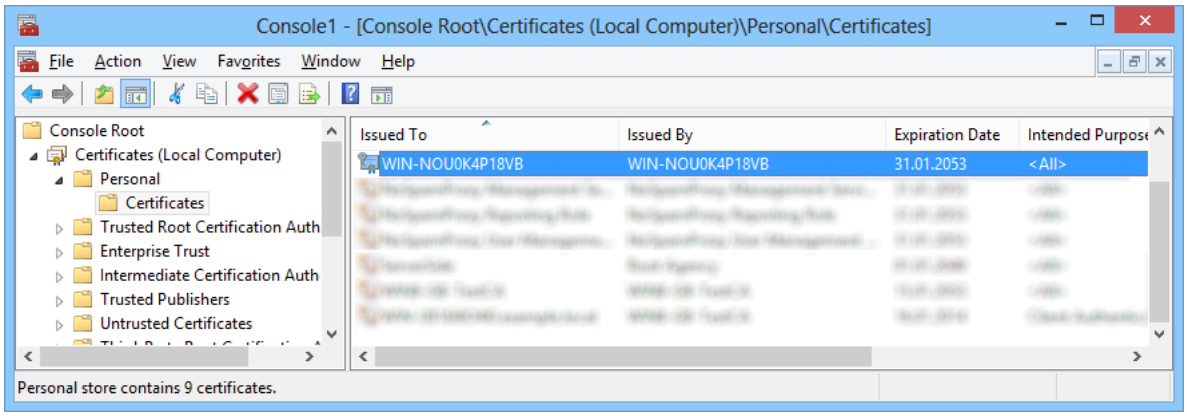

Bild 1: Das Zertifikat der Gateway Rolle

Wählen Sie auf dem Zertifikat die Aktion **Alle Aufgaben / All Tasks** und dann **Exportieren / Export**. Es erscheint der Assistent für den Zertifikatsexport.

Klicken Sie **Weiter / Next** und wählen danach den Export dieses Zertifikats ohne den privaten Schlüssel (Bild 2).

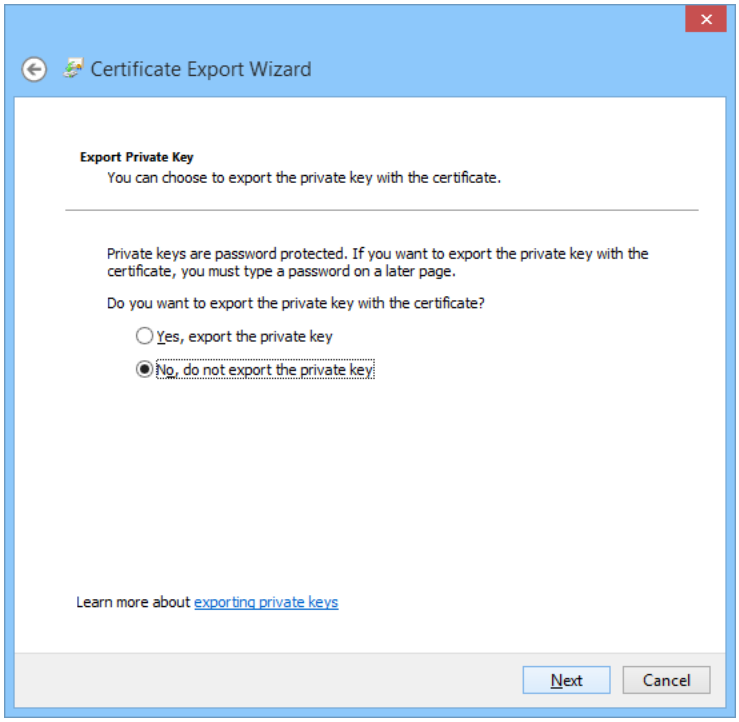

Bild 2: Export ohne privaten Schlüssel

Wählen Sie im nächsten Schritt als Dateiformat das DER-Format aus (Bild 3).

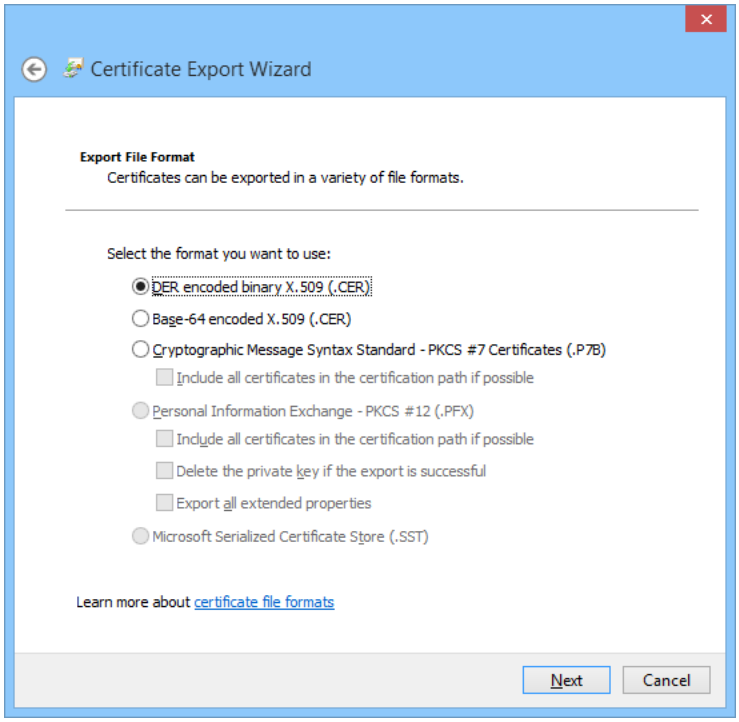

Bild 3: Wahl des DER-Dateiformats

Legen Sie als letzte Einstellung den Speicherort fest (Bild 4). Bestätigen Sie danach die gewählten Einstellungen und beenden Sie dann den Assistenten mit **Beenden / Finish**

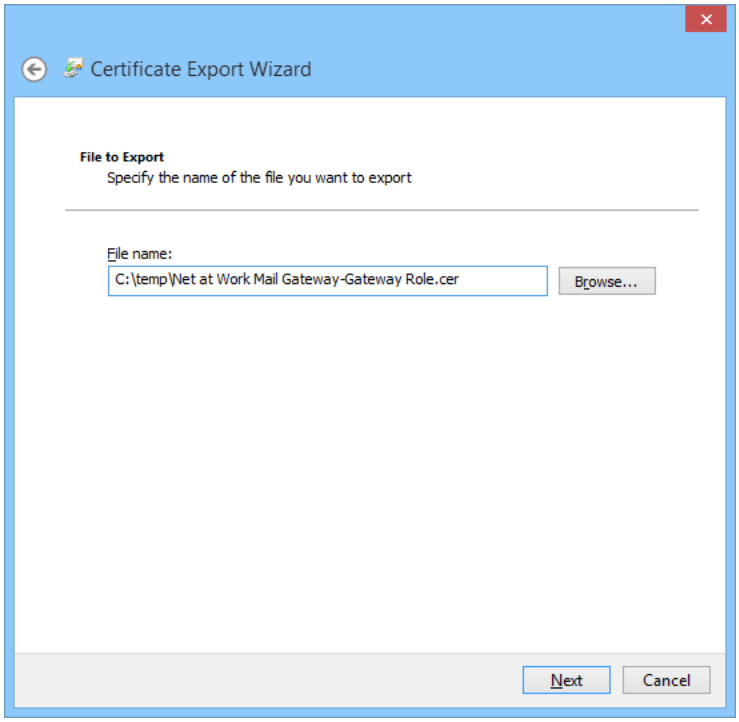

Bild 4: Abspeichern des exportierten Zertifikats

Wenn sich der digiSeal server auf einem entfernten Server befindet, kopieren Sie die Datei mit dem Zertifikat dorthin.

Stellen Sie sicher, dass auf dem digiSeal server die API aktiviert ist (Bild 5).

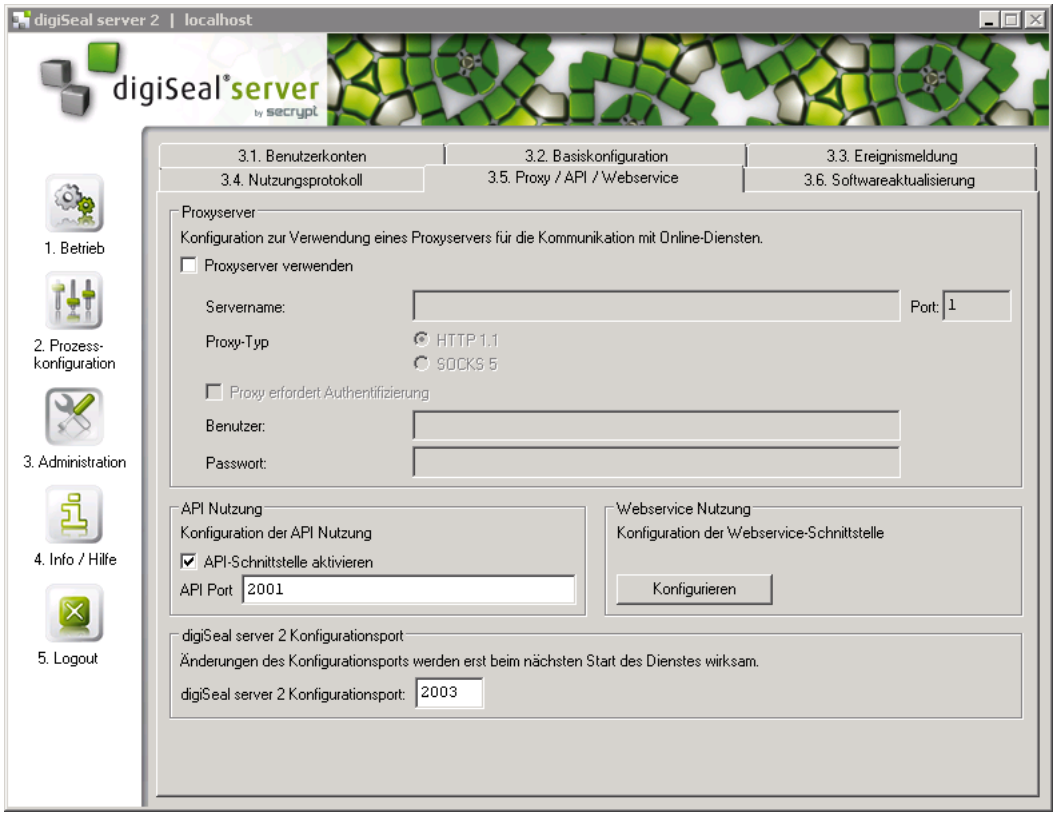

Bild 5: Aktivierung der API-Schnittstelle

Aktivieren Sie die API für jeden Prozess, der von NoSpamProxy Encryption verwendet werden soll. Stellen Sie dazu sicher, dass das Häkchen für **API-Schnittstelle aktivieren** gesetzt ist. Die Schnittstelle wird nur für Programme aktiviert, die ein Zertifikat verwenden, das in der Liste **API-Schnittstelle** aufgeführt ist. In diese Liste muss das zuvor exportierte Zertifikat aufgenommen werden (Bild 6).

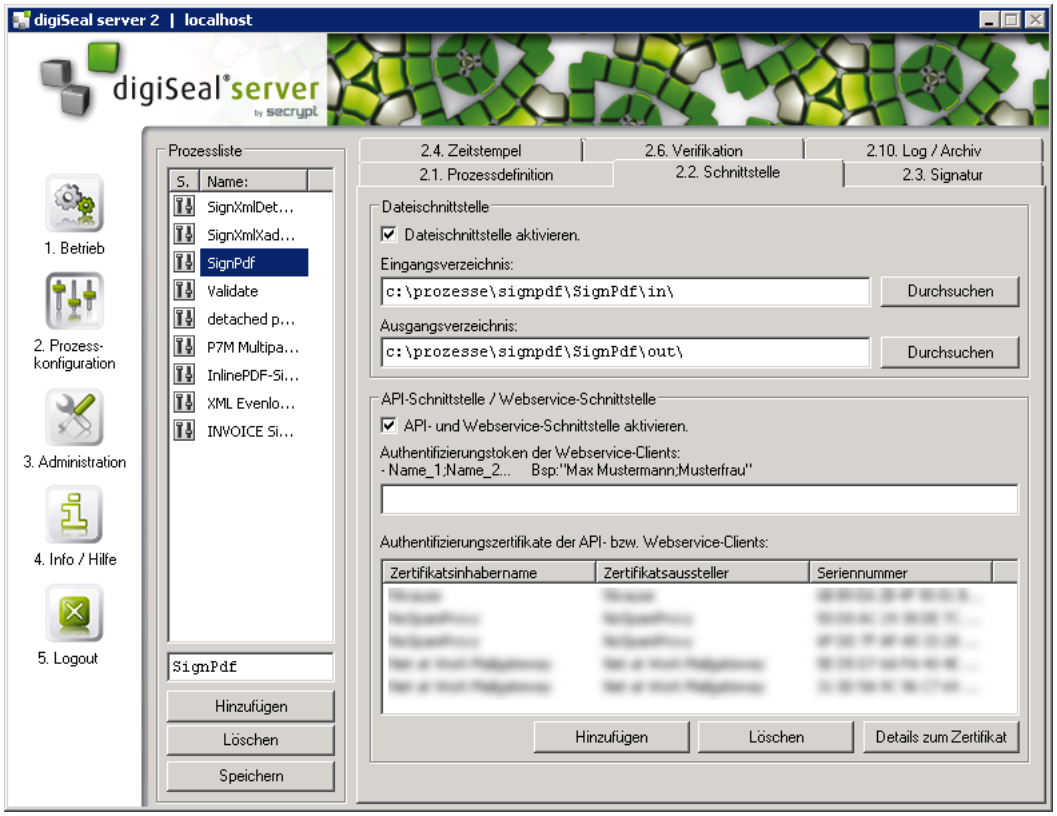

Bild 6: Aktivierung der API-Schnittstelle auf dem eingerichteten Prozess

3. Konfiguration von NoSpamProxy

NoSpamProxy Encryption benötigt einige Dateien aus dem digiSeal server Verzeichnis. Kopieren Sie die Dateien „ `dsServerAPI.dll` “, „ `dsServerAPI.dll.p7s` “ und „ `dsServerAPI.signature` “ aus dem digiSeal server Programmverzeichnis in das Verzeichnis „ `%ProgramFiles%\Net at Work Mail Gateway\Gateway Role` “. Starten Sie nun die Gateway Rolle neu.

Nutzen Sie nun das NoSpamProxy Betriebshandbuch, um die Optionen in der Oberfläche für die Benutzung des digiSeal servers einzurichten. Achten Sie dabei speziell auf die folgenden Punkte:

Im Knoten **Konfiguration** / **Verbundene Systeme**: Konfigurieren Sie die **Verbindung zum digiSeal server**.

Im Knoten **Konfiguration** / **Benutzer-Benachrichtigungen**: Konfigurieren Sie die **E-Mail-Benachrichtigungen** und die **Administrativen E-Mail-Adressen**.

Im Knoten **Konfiguration** / **Regeln**:

- Fügen Sie die Aktion **digiSeal server: Signiere Anhänge an ausgehenden E-Mails** zu einer neuen oder bestehenden ausgehenden Regel hinzu und konfigurieren Sie diese wie im Betriebshandbuch beschrieben.
- Fügen Sie die Aktion **digiSeal server: Überprüfen und Erzwingen von signierten Anhängen auf eingehenden E-Mails** zu einer neuen oder bestehenden eingehenden Regel hinzu und konfigurieren Sie diese wie im Betriebshandbuch beschrieben.

4. Archivierung

Die beiden "digiSeal server"-Aktionen der Regeln von NoSpamProxy stellen Daten für die Archivschnittstelle von NoSpamProxy bereit, falls Sie dort einen Archivkonnektor konfiguriert haben. Bei der Archivierung werden die E-Mails, Signaturen und Prüfprotokolle an den konfigurierten Archivkonnektor übergeben. Details zu diesem Thema können Sie im Kapitel **Archivschnittstelle** des NoSpamProxy Betriebshandbuchs nachlesen. Ein Archivkonnektor für neue, bisher nicht unterstützte Archivsysteme kann in Absprache mit Ihnen durch Net at Work implementiert werden.

5. Vorfälle der qualifizierten Signatur

Nicht immer kann das Signieren oder Überprüfen von Dokumenten korrekt abgeschlossen werden. Es kann zum Beispiel vorkommen, dass die Verbindung zum digiSeal server nicht hergestellt werden kann. Oder der digiSeal server kann einen OCSP Server im Internet nicht erreichen. In diesen Fällen wird die E-Mail von NoSpamProxy Encryption zwar angenommen, aber nicht an den Empfänger weitergeleitet. Stattdessen werden die betroffenen E-Mails zwischengespeichert. Der Administrator erhält in diesem Fall, sofern konfiguriert, eine E-Mail.

In der Oberfläche werden diese E-Mails im Knoten **Monitoring** / **Angehaltene E-Mails** angezeigt. Dort werden alle Vorfälle in einer Liste angezeigt. Der Administrator kann pro Vorfall entscheiden, ob die E-Mail erneut durch NoSpamProxy Encryption zugestellt werden soll oder ob der Vorfall gelöscht wird.

Eine detaillierte Beschreibung über die Benutzung der oben genannten Einstellungen ist im NoSpamProxy Betriebshandbuch nachzulesen.

6. Anhang

Anzeige des Zertifikatsspeichers des lokalen Computers

Um die Zertifikate des lokalen Computers anzuzeigen, sind die folgenden Schritte notwendig:

Starten Sie eine neue MMC-Konsole (Start -> Ausführen -> mmc.exe) (Bild 7).

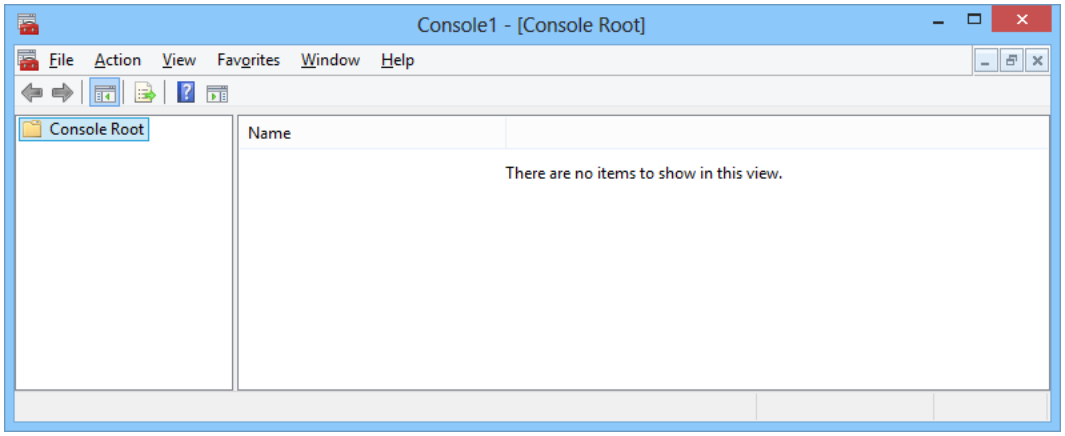

Bild 7: Eine leere MMC

Klicken Sie im Menü **Datei** / **File** auf **Snap-In hinzufügen/entfernen** / **Add/Remove Snap-in**. Wählen Sie das **Zertifikate** / **Certificates** Snap-In aus und klicken Sie auf **Hinzufügen** / **Add** (Bild 8).

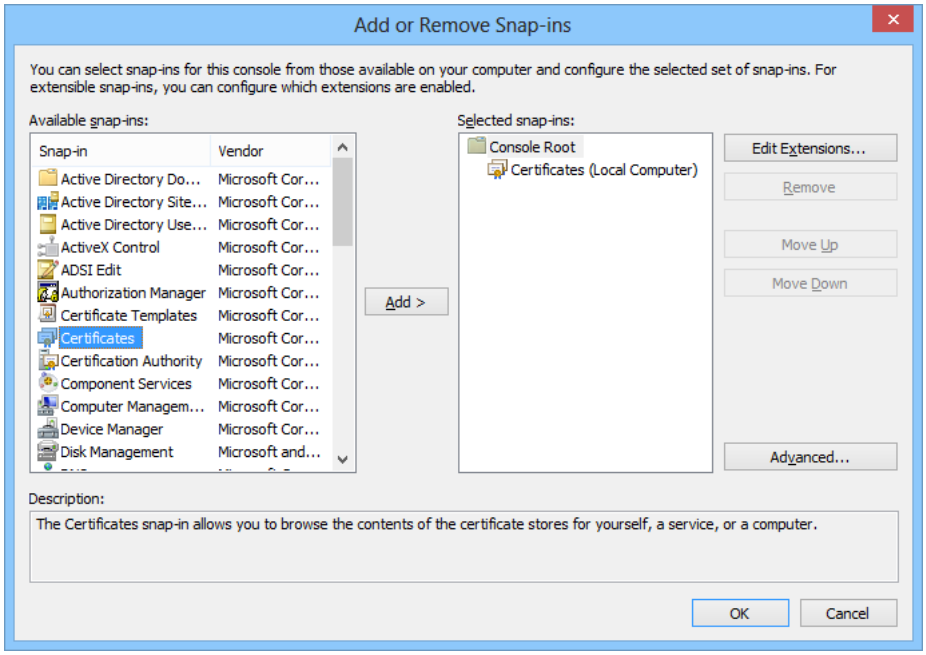

Bild 8: Ein Dialog zum Hinzufügen von Snap-Ins

Es erscheint der Konfigurationsassistent für das Snap-In **Zertifikate**. Wählen Sie hier zuerst das **Computer Konto** / **Computer account** (Bild 9) und im nächsten Schritt **Lokaler Computer** / **Local computer** (Bild 10) lokalen Computer aus und klicken Sie auf **Beenden** / **Finish**.

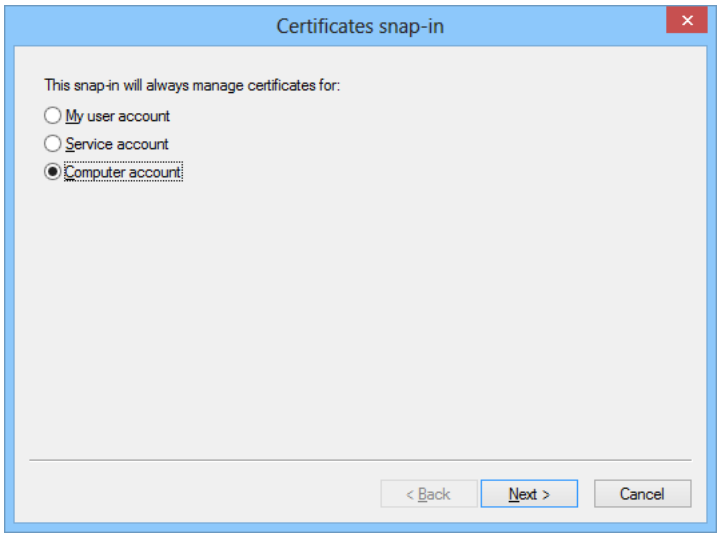

Bild 9: Auswahl des Computer Kontos

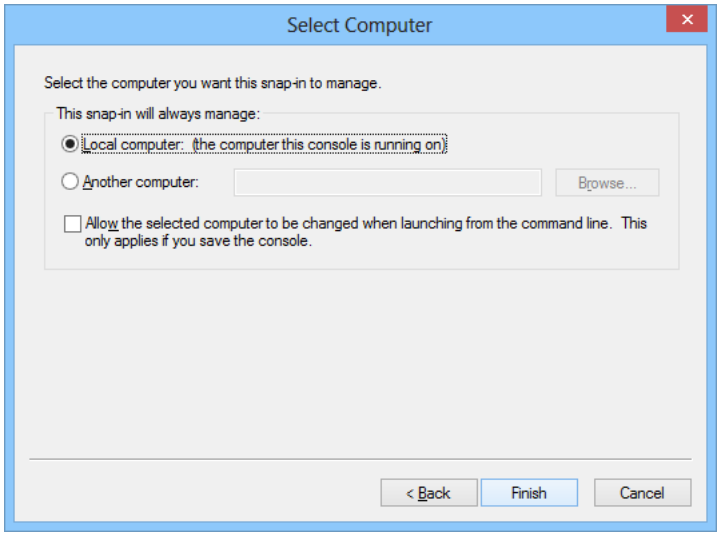

Bild 10: Auswahl des lokalen Computers

Schließen Sie den Dialog **Snap-In hinzufügen oder entfernen / Add or Remove Snap-ins** mit **OK**. Klicken Sie im Fenster **Konsolenstamm** / **Console Root** auf **Zertifikate (Lokaler Computer)** / **Certificates (Local Computer)**, um die Zertifikatsspeicher für den Computer anzuzeigen.

7. Hilfe und Unterstützung

Hilfe und Unterstützung für die Installation und den Betrieb von NoSpamProxy bekommen Sie von Net at Work in vielen Formen.

- **Trainingsvideos**
  Die Trainingsvideos bieten einen Überblick über verschiedene Bereiche und zeigen Möglichkeiten der Konfiguration für konkrete Anwendungsfälle.
- **Blog**
  Das Blog bietet tagesaktuelle Hinweise auf neue Produktversionen, Änderungsvorschläge für Ihre Konfiguration, Warnungen vor Kompatibilitätsproblemen und viele weitere Hinweise, die Sie unterstützen. Die neuesten Nachrichten aus dem Blog werden auch auf der Startseite der NoSpamProxy Konfigurationskonsole eingeblendet, so dass Sie keine wichtigen Hinweise verpassen.
- **Knowledge Base**
  Die Knowledge Base enthält weiterführende technische Informationen zu speziellen Problemstellungen.
- **Support**
  Wenn Sie weitergehende Unterstützung brauchen, besuchen Sie unsere Support-Webseite.