Installationshandbuch Stammportal

V. 1.0

egora Stammportal
V 1.0

Aus Gründen der einfacheren Lesbarkeit wird auf die geschlechtsspezifische Differenzierung, z. B. Benutzer/Innen, verzichtet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für beide Geschlechter.

Inhalt

1. Einführung

Das egora Stammportal ist eine ASP.NET 2.0 Anwendung, die unter dem IIS 6.0 läuft. Es besteht im wesentlichen aus zwei Teilen:

- Der Reverse Proxy
- Das (die) für die Authorisierung zuständige(n) Service(s)

Hier wird die Installation des Reverse Proxy beschrieben.

2. Voraussetzungen Software

2.1. Betriebssystem

Als Betriebssystem wird Windows Server 2003 – Standard Edition empfohlen. Die im Folgenden angeführten Komponenten des Betriebssystems sind erforderlich:

- Windows Server 2003 – Standard Edition (Englisch)
- Microsoft Update für Windows Server 2003
- Internet Information Services-Komponenten
- DotNet Framework 2.0 mit ASP.NET Komponenten

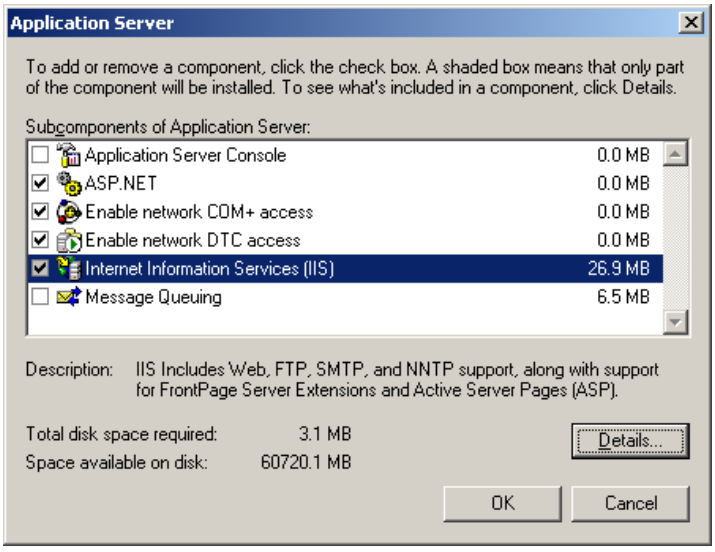


Abbildung 1: Installation Applikationsserverkomponenten

3. Konfiguration Internet Information Services

3.1. Kopieren der Dateien

Kopieren Sie aus der Zip Datei das Verzeichnis HttpReverseProxy in das Verzeichnis C:\Inetpub\wwwroot\HttpReverseProxy.

3.2. Konfiguration Application-Pool

Für den Betrieb des Reverse Proxy empfehlen wir einen eigenen Application Pool.

Legen Sie dazu einen neuen Application-Pool mit der Bezeichnung „Stammportal“ an und übernehmen Sie ansonsten die Standard-Einstelllungen. Wir empfehlen, die Netzwerkkonfiguration so vorzunehmen, dass sich der Reverse Proxy direkt mit dem Internet (bzw. den Zielapplikationen) verbinden kann. Der Zugriff auf das Internet über einen Proxy ist prinzipiell möglich und kann konfiguriert werden (siehe Kapitel 5.1)

3.3. Konfiguration Web-Applikation

Legen Sie ein neues virtuelles Verzeichnis „stammportal“ im Microsoft Internet Information Services Manager an.

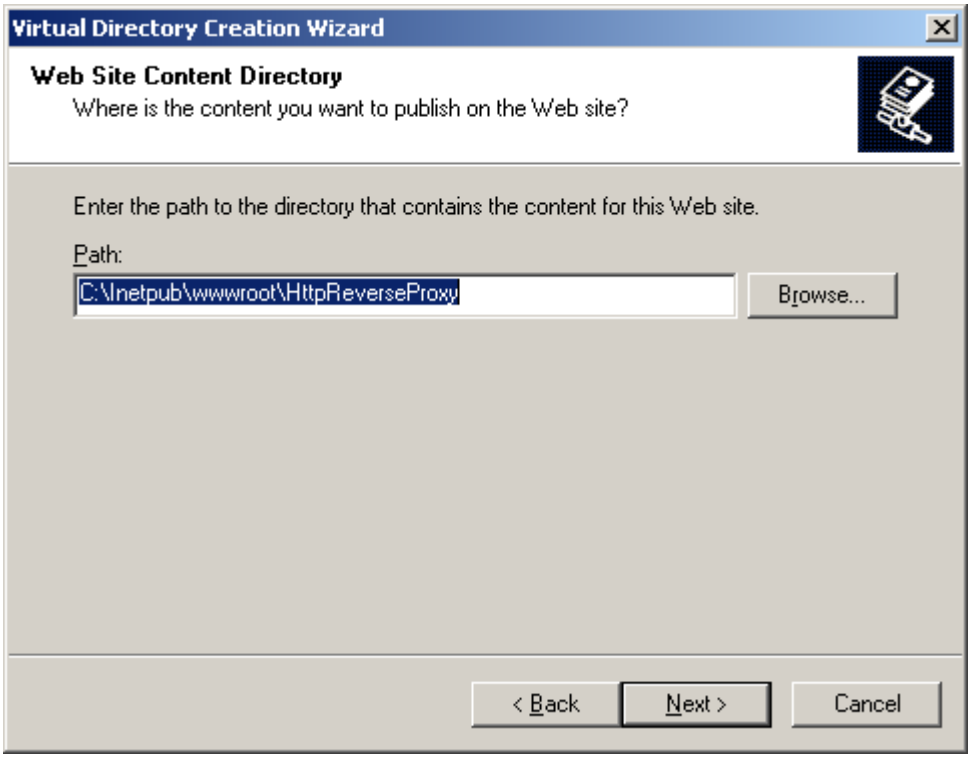


Abbildung 2: Anlegen virtuelles Verzeichnis

Einstellungen – Virtuelles Verzeichnis

Richten Sie das soeben erzeugte virtuelle Verzeichnis „stammportal“ ein, indem Sie die folgenden Schritte ausführen:

1. Vergeben Sie den lokalen Pfad auf das HttpReverseProxy-Verzeichnis.
2. Übernehmen Sie die Standard-Einstellungen für virtuelle Verzeichnisse.
3. Setzen Sie als Execute permissions den Wert „scripts only“.
4. Erzeugen Sie für das soeben erzeugte virtuelle Verzeichnis eine Web-Applikation, indem Sie die Schaltfläche CREATE betätigen.
5. Wählen Sie als Application Pool den zuvor erzeugte Application Pool „Stammportal“ aus.

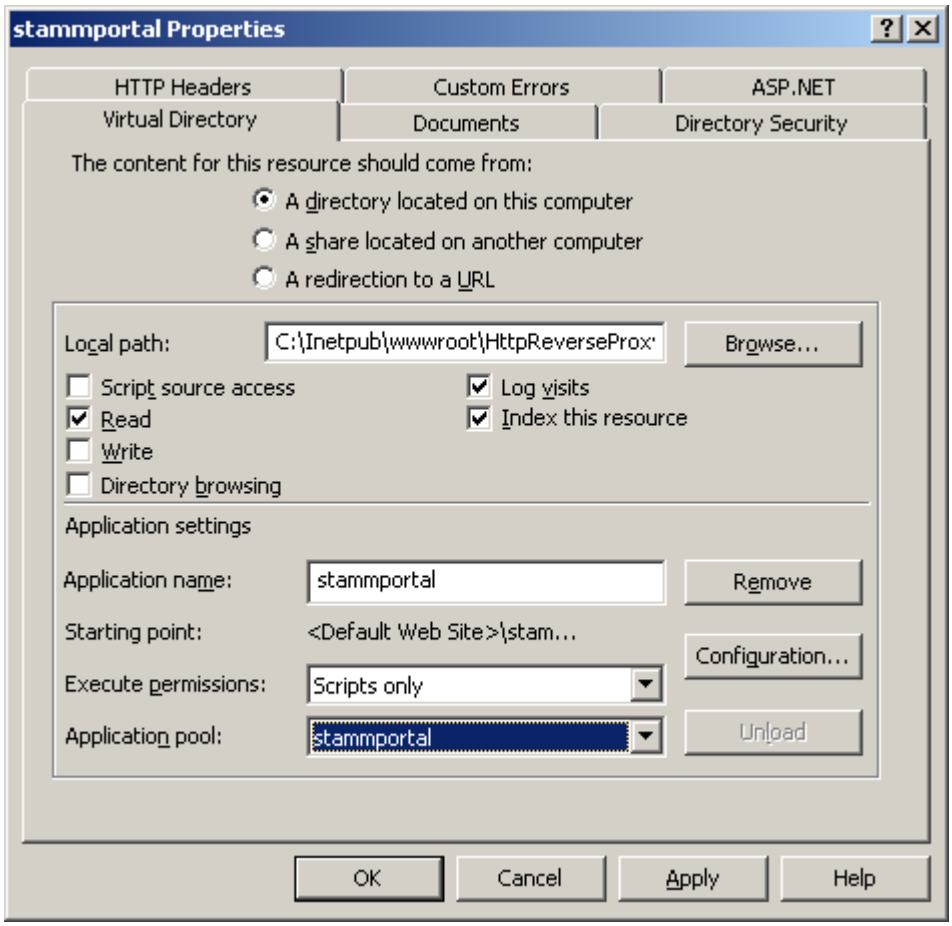


Abbildung 3: Virtuelles Verzeichnis - stammportal

6. Bearbeiten Sie anschließend die Konfigurationseinstellungen (Schaltfläche „Configuration“) um eine Erweiterung des Mappings vorzunehmen.

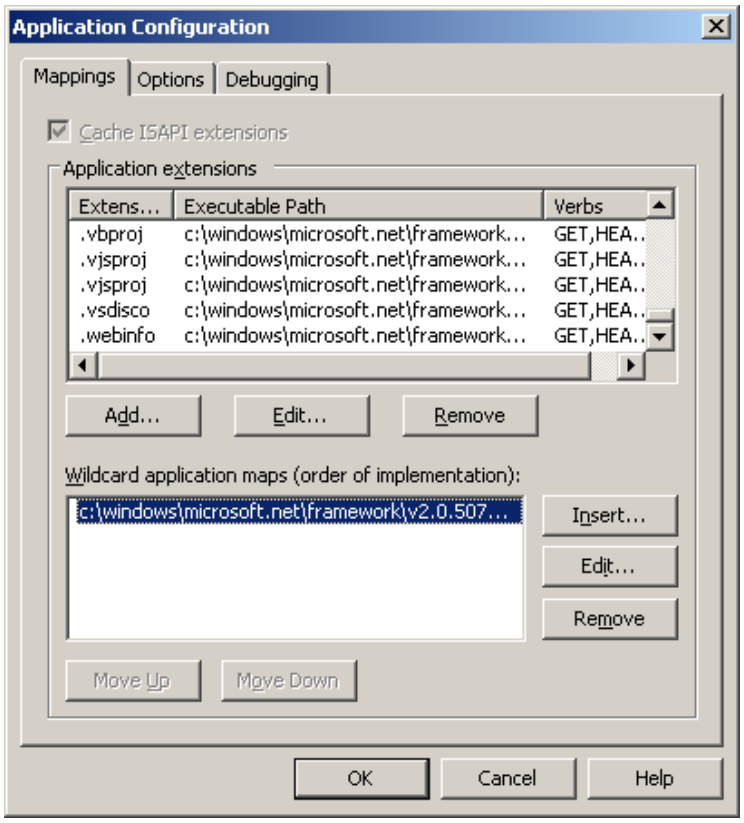


Abbildung 4: Virtuelles Verzeichnis - Erweiterung Mapping

7. Tragen Sie ein Wildcard Mapping in der Liste der Wildcards ein, wählen Sie dabei die Datei „aspnet_isapi.dll“. Am Einfachsten bei dem Mapping Eintrag für .aspx aus der Liste der Applikationserweiterungen kopieren und einfügen.

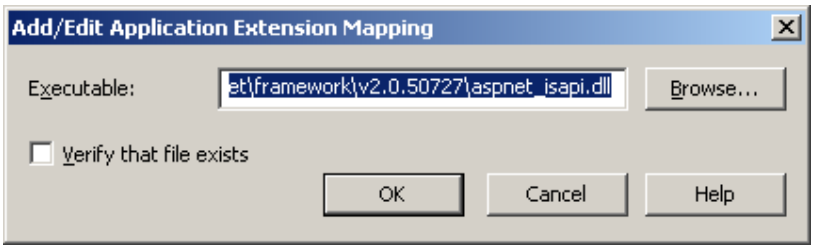
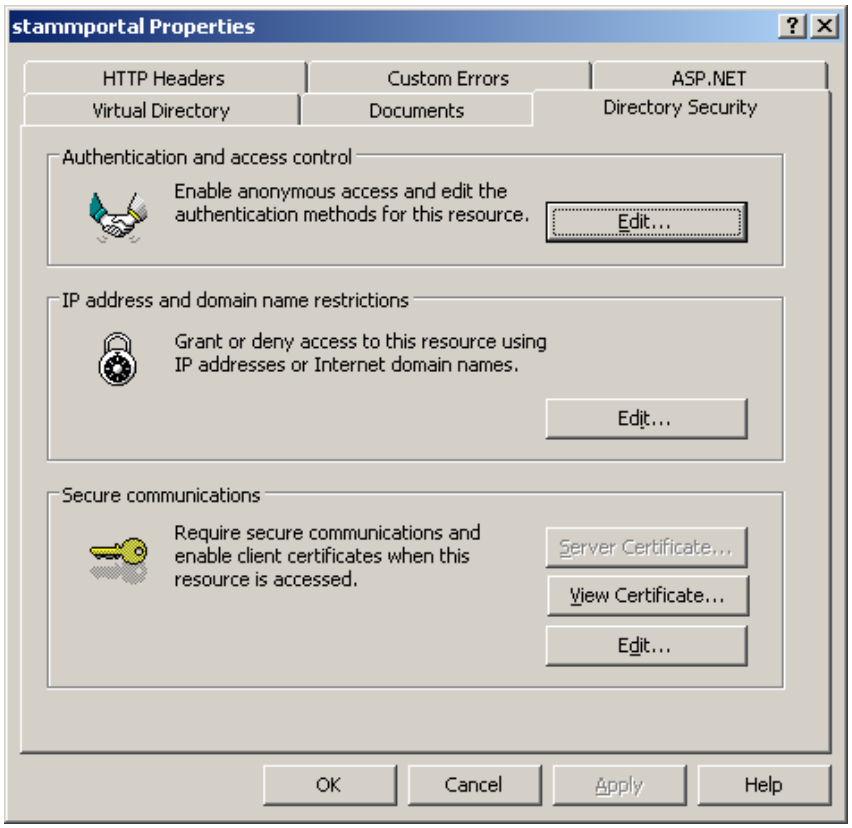


Abbildung 5: Wildcard Mapping

8. Bearbeiten Sie die Sicherheitseinstellungen für dieses Verzeichnis und entfernen Sie den Zugriff für anonyme Benutzer. Stellen Sie sicher, dass Integrated Windows Authentication aktiviert ist.



Abblidung 6: Sicherheitseinstellung

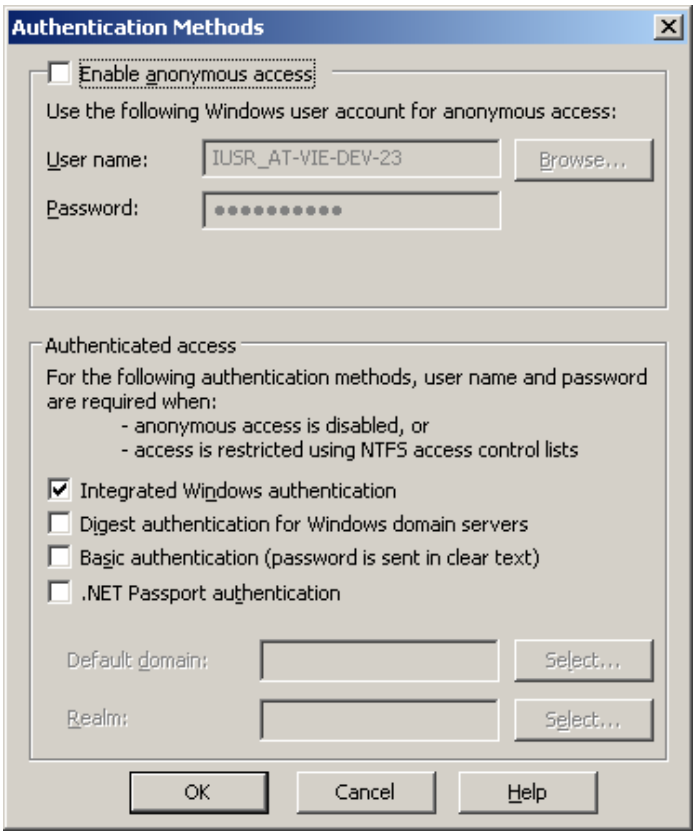


Abbildung 7: Virtuelles Verzeichnis - Authentication Methods

4. Zertifikate

Damit der Reverse Proxy bei dem Aufbau der https Verbindung das erforderliche Zertifikat zur Verfügung hat, sind folgende Schritte erforderlich:

1. Öffnen Sie die Microsoft Management Konsole.
2. Fügen Sie ein Snap-In für die Hinterlegung von Zertifikation am lokalen Computer ein.
3. Öffnen Sie den Zertifikate-Zweig und rufen Sie aus dem Kontextmenü am Ordner *Personal* aus dem Menü ALL TASKS den Menüpunkt IMPORT ... auf.

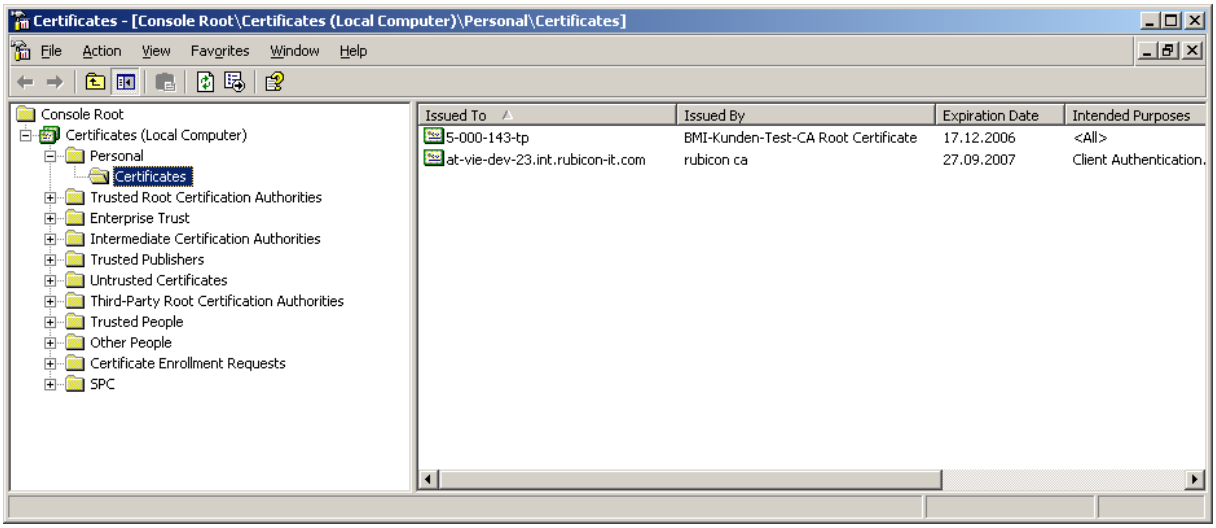


Abbildung 8: Zertifikat - Zertifikat importieren

4. Importieren Sie das Zertifikat. Das Zertifikat muss den öffentlichen als auch privaten Schlüssel beinhalten.
5. Durch den Import des Zertifikates wird im Verzeichnis C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys eine neue Datei erzeugt.

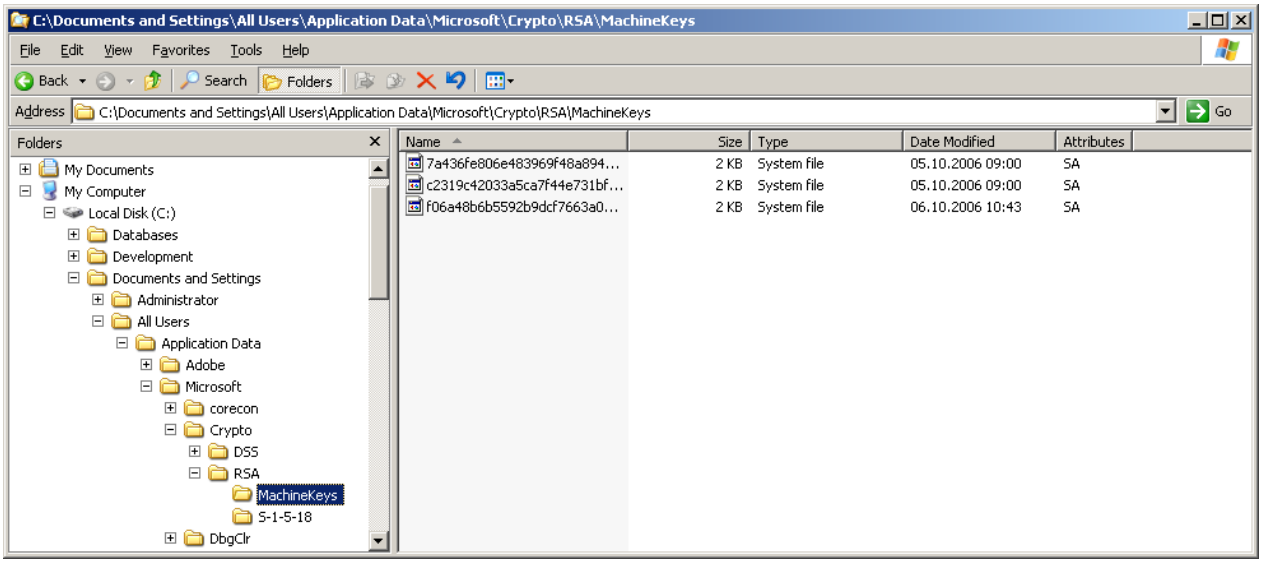


Abbildung 9: Zertifikate - Import

6. Suchen Sie anhand des Erzeugungsdatums die soeben erzeugte Datei und bearbeiten Sie die Eigenschaften von dieser. Fügen Sie den Benutzer des Application Pools (standardmäßig Net-

work-Service) als berechtigten Benutzer auf diese Datei zu, vergeben Sie Lese- und Ausführungsrechte.

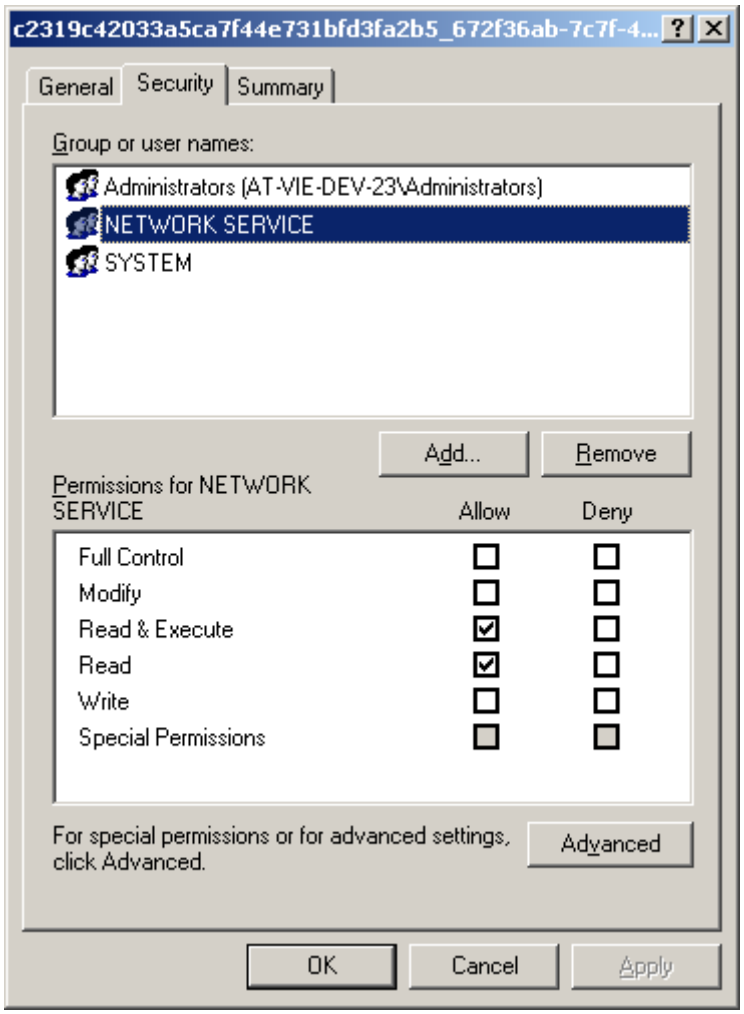


Abbildung 10: Zertifikate - Zusätzliche Rechte

7. Wechseln Sie zurück in die geöffnete Microsoft Management Console und rufen auf dem zuvor importieren Zertifikat das Kontextmenü der rechten Maustaste auf, um das Zertifikat zu exportieren.

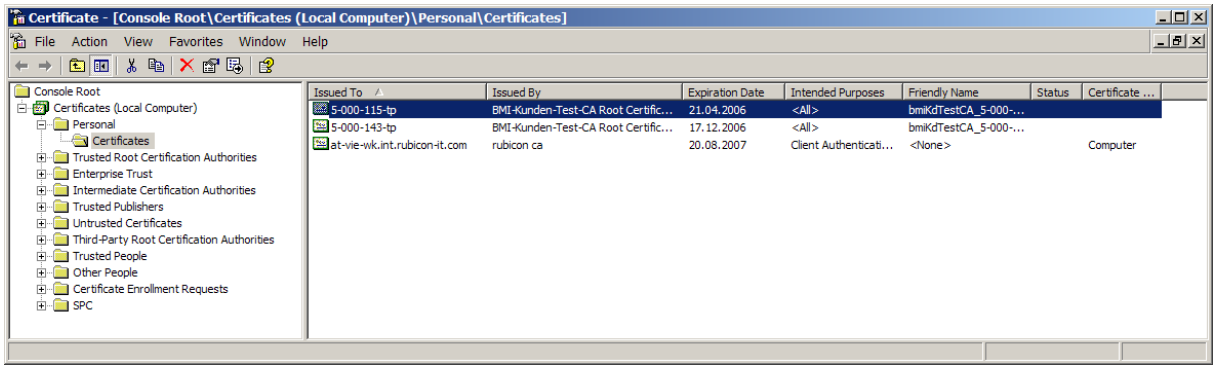


Abbildung 11: Zertifikat - Zertifikat exportieren

8. Speichern Sie das Zertifikat ohne private Key im Verzeichnis C:\Inetpub\wwwroot\httpreverseproxy\Certificates ab. Den Dateinamen, den Sie hier vergeben, müssen Sie im Mapping.xml im HttpReverseProxy-Verzeichnis entsprechend eintragen.

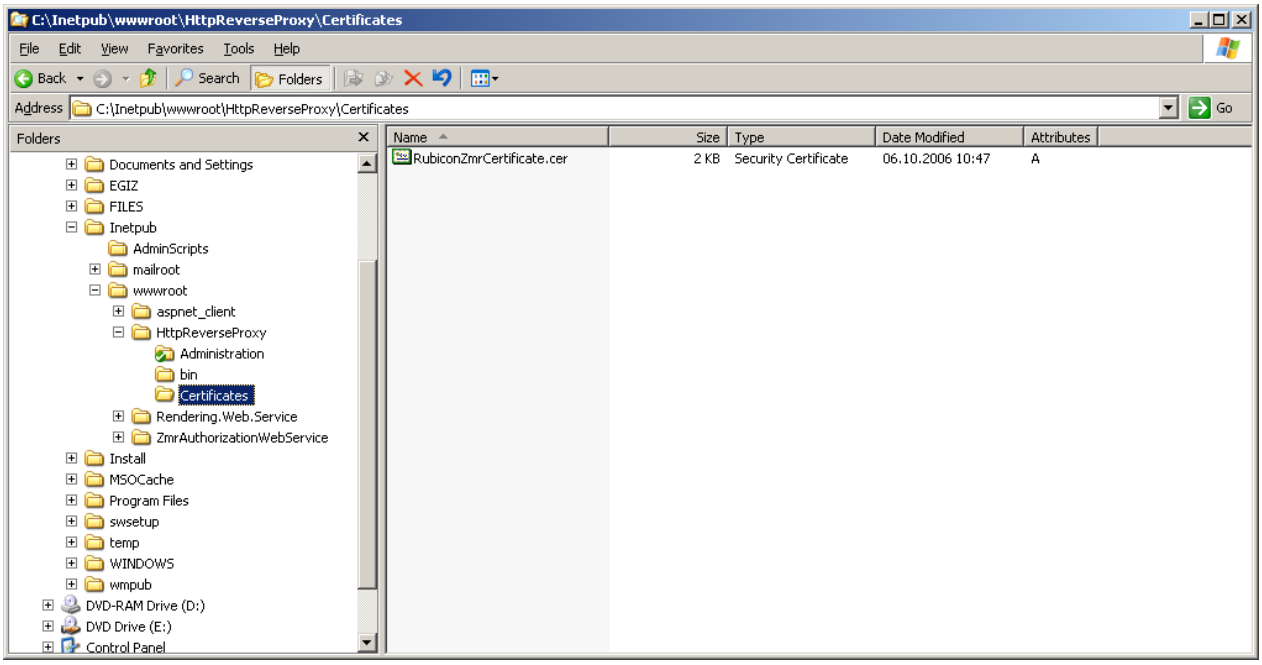


Abbildung 12: Zertifikat - Zertifikat exportieren, Speicherort

9. Beim Exportieren des Zertifikates wird der private Schlüssel des Zertifikates nicht mit exportiert!

5. Konfiguration

5.1. web.config

Die Datei web.config im Verzeichnis HttpReverseProxy kann angepasst werden.

Die Konfiguration einer ASP.NET Anwendung ist sehr mächtig, beispielsweise kann für http Requests ein Defaultproxy definiert werden. Siehe http://msdn.microsoft.com/library/default.asp?url=/library/en-us/cpguide/html/cpconASPNETConfiguration.asp

5.1.1. Tracing

```
<switches>
  <add name="reverseProxySwitch" value="All"/>
  <add name="System.Net" value="Verbose" />
  <add name="System.Net.Sockets" value="Verbose" />
</switches>
```

Hier kann eingestellt werden, wieviel Informationen in den Tracefiles landet.

ActivityTracing	Allows the Stop, Start, Suspend, Transfer, and Resume events through.
All	Allows all events through.
Critical	Allows only Critical events through.
Error	Allows Critical and Error events through.
Information	Allows Critical, Error, Warning, and Information events through.
Off	Does not allow any events through.
Verbose	Allows Critical, Error, Warning, Information, and Verbose events through.
Warning	Allows Critical, Error, and Warning events through.

```
      <add
        name="NetTraceFile"
        type="System.Diagnostics.TextWriterTraceListener"
        initializeData=" c:\log\System.Net.trace.log" />

      <add name="fileListener"
        type="System.Diagnostics.DelimitedListTraceListener"
        delimiter="|"
        initializeData="c:\log\ReverseProxy.log"
traceOutputOptions="ProcessId, ThreadId, DateTime">
        <filter type="System.Diagnostics.EventTypeFilter"
          initializeData="All"/>
      </add>
```

Hier kann eingestellt werden, wie die Tracefiles hießen und in welchem Verzeichnis sie liegen. Der Benutzer des Application Pools muss Schreibrechte auf die angegebenen Dateien haben (bzw. das Recht des Anlegens).

5.1.2. Settings

Eine Änderung der Einstellung ist normalerweise nicht nötig. Die Einstellungen sind der Vollständigkeit halber gelistet.

```
<Egora.Stammportal.HttpReverseProxy.Properties.Settings>
  <setting name="AdministrationGroup" serializeAs="String">
    <value>BUILTIN\Administrators</value>
  </setting>
  <setting name="AdministrationPath" serializeAs="String">
    <value>/admin</value>
  </setting>
  <setting name="PathMapFile" serializeAs="String">
    <value>~/Mapping.xml</value>
  </setting>
  <setting name="AuthorizationWebServiceDefault" serializeAs="String">
    <value>
http://localhost/TestAuthorizationWebService/PvpAuthorizer.asmx</value>
  </setting>
  <setting name="HistoryLength" serializeAs="String">
    <value>100</value>
  </setting>
  <setting name="ImpersonateWebRequest" serializeAs="String">
    <value>False</value>
  </setting>
  <setting name="AuthenticationLevel" serializeAs="String">
    <value>MutualAuthRequested</value>
  </setting>
  <setting name="ProcessRequestWithoutAuthorization" serializeAs="String">
    <value>False</value>
  </setting>
  <setting name="RemoveLeftSideAuthorization" serializeAs="String">
    <value>True</value>
  </setting>
  <setting name="RequestTimeoutSeconds" serializeAs="String">
    <value>300</value>
  </setting>
  <setting name="ConnectionsPerServer" serializeAs="String">
    <value>50</value>
  </setting>
  <setting name="ConnectionMaxIdleTimeSeconds" serializeAs="String">
    <value>10</value>
  </setting>
  <setting name="RetryableErrorMessages" serializeAs="String">
    <value>connection that was expected to be kept alive was closed by the
server</value>
  </setting>
  <setting name="RemoveAuthorizationHeader" serializeAs="String">
```

```
    <value>Negotiate NTLM</value>
  </setting>
  <setting name="BufferLeftSide" serializeAs="String">
    <value>False</value>
  </setting>
  <setting name="BufferRightSide" serializeAs="String">
    <value>False</value>
  </setting>
  <setting name="NetworkRetryDelay" serializeAs="String">
    <value>500</value>
  </setting>
  <setting name="NetworkRetryCount" serializeAs="String">
    <value>3</value>
  </setting>
  <setting name="RetryableHosts" serializeAs="String">
    <value>pvawp.bmi.gv.at;localhost</value>
  </setting>
</Egora.Stammportal.HttpReverseProxy.Properties.Settings>
```

AdminstratorGroup

Mitglieder dieser Active Directory Gruppe können die Administrationsseiten des Reverse Proxy aufrufen.

AdministrationPath

Der virtuelle Pfad zu den Administrationsseiten. Standard ist /admin. Die Übersicht der Urls, die vom Proxy bedient werden, findet man daher standardmäßig unter http://server/admin/Applications.aspx

PathMapFile

Diese Angabe verweist zu der Konfiguration für die Urls, die vom Reverse Proxy bedient werden (siehe Kapitel 0).

AuthorizationWebServiceDefault

Default Url des Autorisierungsservice.

HistoryLength

Der Reverse Proxy merkt sich für die Administrationsseiten die hier eingestellte Anzahl an Requests pro konfigurierter Applikation.

ImpersonateWebRequest

Falls ein Proxy definiert ist, der eine Impersonifizierung des Endbenutzers verlangt, muss der Wert auf true gestellt werden.

AuthenticationLevel

MutualAuthRequested	The client and server should be authenticated. The request does not fail if the server is not authenticated. To determine whether mutual authentication occurred, check the value of the WebResponse.IsMutuallyAuthenticated property.
MutualAuthRequired	The client and server should be authenticated. If the server is not authenticated, your application will receive an IOException with a ProtocolViolationException inner exception that indicates that mutual authentication failed
None	No authentication is required for the client and server.

ProcessRequestWithoutAuthorization

Falls vom Autorisierungsservice keine Autorisierung geliefert wird (SoapHeaderXmlFragment ist null und HttpHeaders ist null oder leer), so wird der Request dennoch weitergereicht, wenn diese Einstellung auf „True“ steht.

RemoveLeftSideAuthorization

Falls diese Einstellung auf „True“ steht, so werden alle Pvp-Headers am **ankommenden** (linke Seite) Request entfernt. Falls es sich um einen Soap Request handelt, werden alle pvpToken (Elementname: pvpToken, Namespace: `http://egov.gv.at/pvp1.xsd`) entfernt.

RequestTimeoutSeconds

Der Wert für den Timeout des Requests zum Server (rechte Seite), in Sekunden.

ConnectionMaxIdleTimeSeconds

Connections, die diese Zeitspanne inaktiv waren,.werden geschlossen. Standardwert 14, weil der Standardwert für einen Apache-Server 15 ist.

ConnectionsPerServer

Pro Zielserver werden maximal diese Anzahl an Connections aufgemacht. Auf der Administrationseite Connection.aspx kann man die aktuell verwendete Anzahl sehen.

RetryableErrorMessages

Hier können Teile von Fehlemeldungen mit „;“ getrennt angegeben werden. Falls bei einem Request zum upstream Server eine Exception auftritt, kann dieser Request wiederholt werden. Es werden nur solche Request wiederholt, bei denen die Fehlermeldung einen der angegebenen Teile enthält.

RemoveAuthorizationHeader

Grundsätzlich werden alle Headers vom Client zum upstream Server weitergegeben. Authorization Header mit den hier angeführten Typen werden nicht zum upstream Server wetergegeben.

BufferLeftSide

Der Inhalt eines Requests vom Client wird normalerweise direkt in den Request zum upstream Server geschriegen. Steht diese Einstellung auf True, so wird der Inhalt zuerst in einen Puffer geschrieben. Falls NetworkRetryCount > 0 ist, wird unabhängig von dieser Einstellung immer in einen Puffer geschrieben.

BufferRightSide

Der Inhalt einer Response vom upstream Server wird normalerweise direkt in die Response zum Client geschriegen. Steht diese Einstellung auf True, so wird der Inhalt zuerst in einen Puffer geschrieben.

NetworkRetryCount

Ist dieser Wert größer als 0, werden Request zum upstream Server, die entweder mit einer Exception enden oder mit dem Statuscode 500 enden, wiederholt. Dieser Wert bestimmt die Anzahl der Wiederholungen.

NetworkRetryDelay

Ist dieser Wert bestimmt, wielange vor einer Wiederholung einer Requests gewartet wird. Der Wert ist in Millisekunden.

RetryableHosts

Hier können Hostnamen mit „;“ getrennt angegeben werden. Falls einRequest zum upstream Server mit dem Statuscode 500 beantwortet wird, kann dieser Request wiederholt werden. Es werden nur solche Request wiederholt, die zu einem der genannten Server gehen.

SubstituteHostInLocationHeader

Wenn dieser Switch auf True gesetzt ist, wird bei einem Location Header (redirect), der die Authority (Servername) enthält, die Authority ersetzt durch die Authority des Stammportals.

5.2. Admin Seiten

Unter dem in der web.config eingestellen Pfad (siehe 5.1.2) können aspx Seiten aufgerufen werden, die Auskunft geben über den aktuellen Status des Proxy.

5.2.1. Applications.aspx

Diese Seite listet die Applikationen, die vom Proxy derzeit bedient werden. Wenn eine Applikation im Mapping eingetragen ist, aber noch nie aufgerufen wurde, ist sie hier nicht gelistet. Bei Klick auf Details sieht man eine Historie der Requests.

5.2.2. Authorization.aspx

Hier sieht man die im Cache befindlichen Autorisierungsdaten.

5.2.3. Connection.aspx

Hier sieht man die aktuell geöffneten Connections zu den Zielservern.

5.2.4. Reset.aspx

Bei Aufruf dieser Seite wird der Proxy neu initialisiert. Das Mapping wird neu eingelesen und der Cache der Autorisierungsdaten geleert.

5.3. Mapping.xml

Diese Datei definiert die Url, die der Reverse Proxy bedient.

```
<?xml version="1.0" encoding="utf-8" ?>
<PathMap xmlns="http://www.egora.at/Stammportal/PathMap/1.0" >
  <Directories>
    <ApplicationDirectory

AuthorizationWebService="http://localhost/TestAuthorizationWebService/PvpAu
thorizer.asmx"
      RootUrl="https://portals-
test.bmi.gv.at/bmi.gv.at/soapv2/soaphttpengine/soapv2%23pvp1?dest=ZMR&amp;o
pzone=test"
      CertificateFile="~/Certificates/PvpZmrCertificate.cer"
      Name="zmrsoap" />
    <ApplicationDirectory

AuthorizationWebService="http://localhost/TestAuthorizationWebService/PvpAu
thorizer.asmx"
      CertificateFile="~/Certificates/PvpZmrCertificate.cer"
      Name="zmrweb"
      RootUrl="https://portal.bmi.gv.at/portal/zmr-gw/" >
    </ApplicationDirectory>
  </Directories>
</PathMap>
```

5.3.1. ApplicationDirectory

Ein Element ApplicationDirectory definiert eine entfernte Anwendung, die über den Proxy laufen soll. Im obigen Beispiel wird ein Request auf http://server/stammportal/zmrweb/index.htm umgesetzt auf https://portal.bmi.gv.at/portal/zmr-gw/index.htm. Dabei wird beim Aufbau der https Verbindung das

Zeritfikat PvpZmrCertificate.cer verwendet. Der private Key wird dabei von Windows automatisch aus dem Private Key Store verwendet, das Programm selbst hat keinen Zugriff auf den private Key.

RootUrl

Die Basis Url der entfernten Anwendung.

AuthorizationWebService

Die Url für das Autorisierungsservice.

Name

Der relative Name unter dem die entfernte Applikation über den proxy angesprochen wird.

CertificateFile

Die Datei, die Sie beim Exportieren des Zertifikates ohne private Key (siehe Kapitel 4) erzeugt haben.

6. Anhang

6.1. Abbildungsverzeichnis