DOCUMENTS

SINGLE SIGN ON
Einrichtung und Installation

VERSION 1.2.2 / DOCUMENTS 5

Inhaltsverzeichnis

1. Allgemein

1.1 Nutzen von Single Sign-On

Durch die Verwendung von Single Sign-On (SSO) muss sich ein Benutzer nur einmal an einem Arbeitsplatz authentifizieren und kann dann auf alle Ressourcen und Dienste zugreifen, für die er eine Berechtigung hat. Eine erneute Anmeldung ist nicht erforderlich. **DOCUMENTS 5** unterstützt im Hinblick auf SSO mehrere Standardverfahren zur Authentifizierung. Die Einrichtung der Systemlandschaft zur Nutzung dieser Authentifizierungsverfahren mit **DOCUMENTS 5** ist in diesem Dokument beschrieben.

1.2 Voraussetzungen

Um SSO einsetzen zu können müssen folgende Voraussetzungen für die Systemlandschaft gegeben sein:

1.2.1 Domänencontroller

Es muss eine Domäne existieren, die von einem Domänencontroller verwaltet wird, der ein *Active Directory* bereitstellt. Voraussetzung ist hier als Betriebssystem *Microsoft Windows Server* (getestet mit Version 2008).

1.2.2 Applikationsserver

Der Applikationsserver, auf dem die **DOCUMENTS 5**-Installation läuft, muss vom Domänencontroller und von den Arbeitsplätzen aus im Netzwerk erreichbar sein. Er muss allerdings nicht zwingend Mitglied in der Domäne sein.

1.2.3 Arbeitsplatz

Jeder Arbeitsplatz-Rechner von dem aus SSO nutzbar sein soll, muss Mitglied der Domäne sein. Ebenso muss jeder Benutzer der sich per SSO anmelden soll Mitglied in der Domäne sein und unter dem gleichen Benutzernamen im **DOCUMENTS 5** - oder bei vorhandener LDAP-Kopplung - im LDAP angelegt sein. Das Passwort des Benutzers muss in der Domäne und im **DOCUMENTS 5** bzw. LDAP identisch sein.

Wird von einem Arbeitsplatz zugegriffen, der nicht Mitglied der Domäne ist, so wird ein Standarddialog des Browsers (Basic-Auth) verwendet, um Benutzername und Passwort vom Benutzer abzufragen (vgl. Abb. 1). Der Benutzer wird dann gegen die Domäne authentifiziert und erhält Zugang zu **DOCUMENTS 5**.

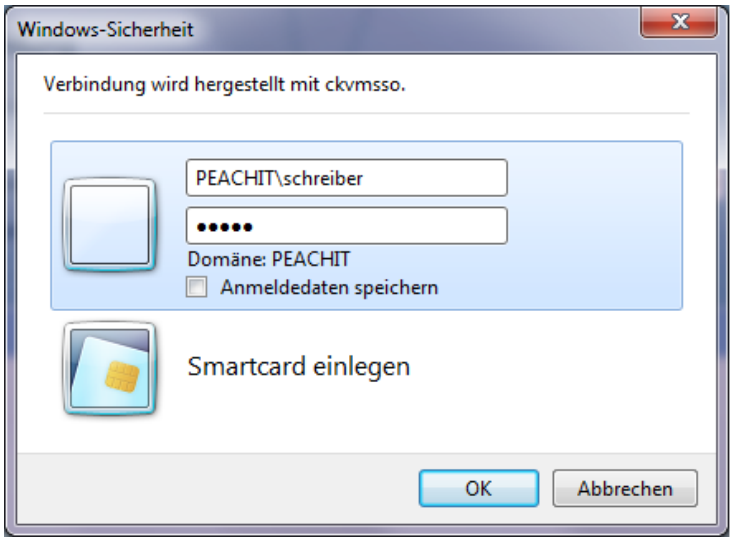

Abb. 1: Standard-Anmeldedialog unter Windows 7

1.2.4 Authentifizierungsmethode

Für die Einrichtung von SSO ist es nötig die zu verwendende Authentifizierungsmethode zu kennen. Es werden *NTLMv1, NTLMv2* und *Kerberos* unterstützt. Welche Authentifizierungsmethode verwendet werden soll, muss vom Systemadministrator des Kunden festgelegt werden.

1.3 Einrichtung des DOCUMENTS 5 Servers

Um die Anmeldung mittels SSO im **DOCUMENTS-Manager** zu erlauben, müssen die neue Eigenschaften `autoLogin = 1` und `singleSignon = true` für den *Mandanten* hinzugefügt werden (Abb. 2).

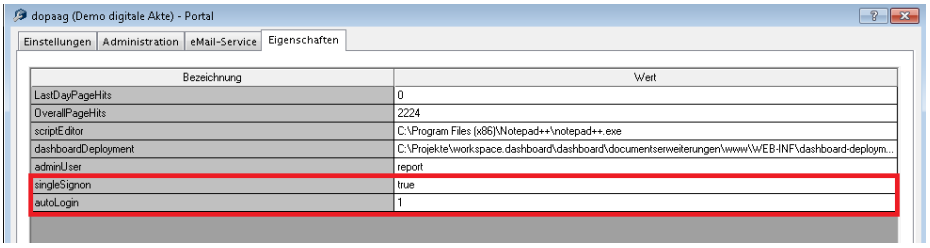

Abb. 2: Eigenschaften des Mandanten

Es muss sichergestellt sein, dass die Einstellung „Automatischer Login“ im Menü „Documents -> Einstellungen“ ausgeschaltet ist. Diese Funktion kann nicht gleichzeitig mit SSO benutzt werden, da der Automatische Login und SSO zwei konkurrierende Anmeldeverfahren sind.

1.4 Auswahl des Authentifizierungsmoduls

Zur Durchführung der Authentifizierung am Active-Directory stehen mehrere Authentifizierungsmodule zur Verfügung. Die Auswahl des Moduls hängt davon ab, welche Methode zur Authentifizierung verwendet werden soll.

Anhand der folgenden Tabelle kann mithilfe der Authentifizierungsmethode das passende Authentifizierungsmodul ausgewählt werden.

Auth.-Modul	**NTLMv1**	**NTLMv2**	**Kerberos**
JCIFS	Ja	Nein	Nein
WAFFLE*	Ja	Ja	Nein
JESPA	Ja	Ja	Nein
SPNEGO	Nein	Nein	Ja

* Für Waffle muss der Anwendungsserver auf einem Windows System laufen.

Im Folgenden werden die weiteren Konfigurationsschritte erläutert, um das jeweilige Authentifizierungsmodul zu verwenden.

HINWEIS! Bei Verwendung von NTLMv2 beachten:

JESPA und WAFFLE erlauben die Authentifizierung sowohl mit NTLMv1 als auch mit NTLMv2. Wenn sichergestellt werden soll, dass NTLMv2 verwendet wird, muss dies in den Gruppenrichtlinien des Domain Controllers eingestellt werden.

Die Einstellung ist am Domänencontroller zu finden unter: „*Computerkonfiguration > Richtlinien > Windows-Einstellungen > Sicherheitseinstellungen > Lokale Richtlinien > Sicherheitsoptionen*“ und heißt „*Netzwerksicherheit: LANManager-Authentifizierungslevel*“. Hier ist die jeweils zutreffende Option zu wählen.

1.5 Übersicht über die Systemumgebung

Abb. 3 zeigt den Aufbau der Systemumgebung für die Nutzung von SSO mit **DOCUMENTS 5**:

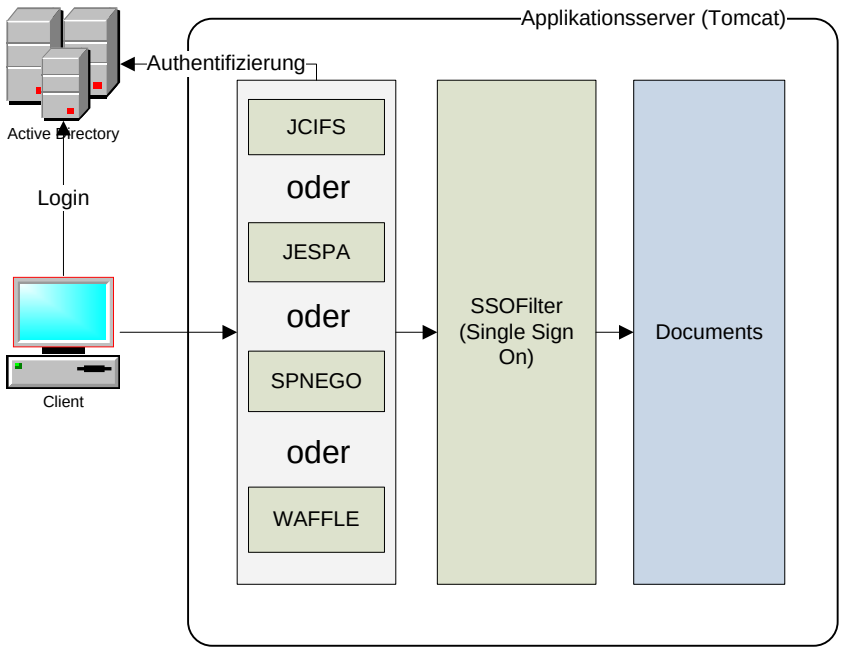

Abb. 3: Systemumgebung

In den folgenden Abschnitten wird beschrieben, welche Schritte für die Einrichtung der verschiedenen Authentifizierungsmodule durchgeführt werden müssen.

2. SSO mit JCIFS (NTLMv1)

JCIFS ist eine Programmbibliothek die unter anderem die Funktionalität zur Authentifizierung mit NTLMv1 zur Verfügung stellt. Genauere Informationen können unter **http://jcifs.samba.org/** abgerufen werden.

2.1 Installation von JCIFS

JCIFS in der Version 1.1.9 ist in der Regel bereits vorinstalliert. Sollte dies nicht der Fall sein, kann eine aktuelle Version von **http://jcifs.samba.org/** heruntergeladen werden. In dem heruntergeladenen Archiv mit dem Namen `jcifs_1.1.9.zip` befindet sich die Datei `jcifs_1.1.9.jar`. Diese Datei muss in das Verzeichnis `www/WEB-INF/lib` kopiert werden. Danach ist ein Neustart des Tomcat erforderlich. JCIFS wurde in der Version 1.1.9 erfolgreich getestet.

2.2 Hinzufügen des JCIFS-Filters

Zur Aktivierung der Authentifizierung mit NTLMv1 muss in der Datei `web.xml` der **DOCUMENTS 5** - Applikation ein Filter hinzugefügt werden. Dazu muss folgender Text nach dem letzten `<filter>` Element und vor dem ersten `<filter-mapping>` Element eingefügt werden.

```
<filter>
  <filter-name>NtlmHttpFilter</filter-name>
  <filter-class>jcifs.http.NtlmHttpFilter</filter-class>
  <init-param>
    <param-name>jcifs.http.domainController</param-name>
    <param-value>peachitdc</param-value>
  </init-param>
  <init-param>
    <param-name>jcifs.smb.client.username</param-name>
    <param-value>Administrator</param-value>
  </init-param>
  <init-param>
    <param-name>jcifs.smb.client.password</param-name>
    <param-value>PASSWORT</param-value>
  </init-param>
  <init-param>
    <param-name>jcifs.util.loglevel</param-name>
    <param-value>3</param-value>
  </init-param>
  <init-param>
```

```
    <param-name>jcifs.smb.client.domain</param-name>
    <param-value>peachit</param-value>
  </init-param>
  <init-param>
    <param-name>jcifs.netbios.wins</param-name>
    <param-value></param-value>
  </init-param>
  <init-param>
    <param-name>jcifs.netbios.cachePolicy</param-name>
    <param-value>0</param-value>
  </init-param>
  <init-param>
    <param-name>jcifs.smb.client.soTimeout</param-name>
    <param-value>15000</param-value>
  </init-param>
  </filter>

  <filter-mapping>
        <filter-name>NtlmHttpFilter</filter-name>
        <url-pattern>/jsp/autologin</url-pattern>
  </filter-mapping>
```

2.2.1 Anpassungen der Parameter

- `jcifs.http.domainController` :DNS-Name des Domänen Controllers
- `jcifs.smb.client.username`: Benutzername eines beliebigen Benutzers der Zugang zur Domäne hat (Administratorrechte nicht benötigt). Dieser User wird dazu verwendet um Informationen zur Authentifizierung des anzumeldenden Benutzers abzurufen.
- `jcifs.smb.client.password`: Passwort des Benutzers
- `jcifs.smb.client.domain`: Name der Domäne

Hinweis zur Angabe des url-pattern: *Die verschiedenen Möglichkeiten für die Einstellung des url-pattern und deren Auswirkungen sind im Abschnitt 6.3 beschrieben.*

Hinweis (SSOFilter): *Unabhängig von der Wahl der Authentifizierungsmethode ist die Einrichtung des SSOFilters notwending. (Abschnitt 6).*

3. SSO mit WAFFLE (NTLMv2)

3.1 Installation von Waffle

Zunächst muss das aktuelle Waffle Paket von **http://waffle.codeplex.com/** heruntergeladen werden. In dem heruntergeladenen Archiv mit dem Namen `waffle.1.3.zip` befindet sich das Verzeichnis `Waffle/Bin`. Alle Dateien mit der Endung „`.jar`“ müssen in das Verzeichnis `www/WEB-INF/lib` kopiert werden. Danach ist ein Neustart des Tomcat erforderlich. Waffle wurde in der Version 1.3 erfolgreich getestet.

3.2 Hinzufügen des Filters

Um WAFFLE nutzen zu können, ist es ausreichend den folgenden Filter in die `web.xml` Datei hinzuzufügen.

```
<filter>
    <filter-name>WaffleFilter</filter-name>
    <filter-class>waffle.servlet.NegotiateSecurityFilter</filter-class>
    <init-param>
      <param-name>
waffle.servlet.spi.NegotiateSecurityFilterProvider/protocols
      </param-name>
      <param-value>NTLM</param-value>
    </init-param>
  </filter>

  <filter-mapping>
    <filter-name>WaffleFilter</filter-name>
    <url-pattern>/jsp/autologin</url-pattern>
  </filter-mapping>
```

3.2.1 Anpassung der Parameter

- `waffle.servlet.spi.NegotiateSecurityFilterProvider/protocols`: Mit diesem Parameter wird eingestellt, welches Authentifizierungsverfahren genutzt werden soll. Im Beispiel wird NTLMv1 oder NTLMv2 verwendet. Welche Version verwendet wird, hängt von den Einstellungen des Domain Controllers ab. Siehe: „HINWEIS! Bei Verwendung von NTLMv2 .“ Im Abschnitt 1.4.

Hinweis zur Angabe des url-pattern: *Die verschiedenen Möglichkeiten für die Einstellung des url-pattern und deren Auswirkungen stehen im Abschnitt 6.3.*

Hinweis (SSOFilter): *Unabhängig von der Wahl der Authentifizierungsmethode ist die Einrichtung des SSOFilters notwending. (Abschnitt 6).*

4. SSO mit JESPA (NTLMv1 + NTLMv2)

4.1 Installation von JESPA

JESPA ist eine **kostenpflichtige** Programmbibliothek die unter anderem Funktionen zur Authentifizierung mit NTLMv1 und NTLMv2 zur Verfügung stellt. JESPA muss vom Hersteller **www.ioplex.com** bezogen werden. Die heruntergeladene .jar Datei muss in das Verzeichnis „www/WEB-INF/lib“ der Portalinstallation gelegt werden. Danach ist ein Neustart des Tomcat erforderlich. JESPA wurde in der Version 1.1.6 erfolgreich getestet.

4.2 Einrichtung eines JESPA-Benutzers

Damit die Authentifizierung mit JESPA genutzt werden kann, muss im Active Directory ein COMPUTER Konto erstellt werden und mit einem Passwort versehen werden. Die Erstellung des Kontos kann direkt im Active Directory erfolgen. Es kann zwar auch ein bestehendes Computerkonto verwendet werden, es empfiehlt sich aber ein neues Konto anzulegen, damit dieses ggf. ohne Abhängigkeiten zum bestehenden System später wieder gelöscht werden kann.

Um das angelegte Konto mit einem Passwort zu versehen, muss das mit JESPA mitgelieferte Script „SetComputerPassword“ auf der Konsole ausgeführt werden.

```
SetComputerPassword jespa$@peachit.local passwort
```

Im Aufruf muss dem Namen des Kontos ein $-Zeichen angehängt werden!

4.3 Hinzufügen eines JESPA-Filters

Zur Aktivierung der Authentifizierung mit JESPA muss in der Datei `web.xml` der **DOCUMENTS 4** - Applikation ein Filter hinzugefügt werden. Dazu muss folgender Text nach dem letzten `<filter>` Element und vor dem ersten `<filter-mapping>` Element eingefügt werden.

```
<filter>
        <filter-name>HttpSecurityFilter</filter-name>
        <filter-class>jespa.http.HttpSecurityFilter</filter-class>
        <init-param>
            <param-name>properties.path</param-name>
            <param-value>/WEB-INF/example_ntlm.prp</param-value>
        </init-param>
 </filter>
 <filter-mapping>
        <filter-name>HttpSecurityFilter</filter-name>
        <url-pattern>/jsp/autologin</url-pattern>
 </filter-mapping>
```

4.3.1 Anpassung der Parameter

JESPA bietet die Möglichkeit die Filter-Parameter in Properties-Dateien auszulagern. In diesem Beispiel wurden die Einstellungen in die Datei `example_ntlm.prp` ausgelagert. Beim Download liegen JESPA bereits mehrere verschiedene Konfigurationen bei.

```
provider.classname = jespa.ntlm.NtlmSecurityProvider

http.parameter.username.name = username

http.parameter.password.name = password

http.parameter.logout.name = logout

http.parameter.anonymous.name = anon

fallback.location = /jespa/Login.jsp

excludes = /Login.jsp

#groups.allowed = W\\Domain Admins


jespa.log.path = /tmp/jespa.log

jespa.log.level = 5

jespa.account.canonicalForm = 3



jespa.bindstr = peachitdc.peachit.local

jespa.dns.servers = 192.168.7.75

jespa.service.acctname = jespa$@peachit.local

jespa.service.password = password

jespa.domain.netbios.name = PEACHIT

jespa.domain.dns.name = peachit.local

jespa.authority.dns.names.resolve = false
```

- `jespa.bindstr` **: Vollständiger** DNS-Name des Domänen-Controllers
- `jespa.dns.servers` **:** IP-Adresse des DNS-Server
- `jespa.service.acctname`**:** Name des angelegten JESPA-Benutzers
- `jespa.service.password`**:** Passwort des angelegten JESPA-Benutzers
- `jespa.domain.netbios.name`**:** Der Netbios-Name der Domäne
- `jespa.domain.dns.name`**: Vollständiger** DNS-Name der Domäne
- `jespa.authority.dns.names.resolve`**:** Ist in dieser Konfiguration auf `false` zu setzen.

Hinweis zur Angabe des url-pattern: *Die verschiedenen Möglichkeiten für die Einstellung des url-pattern und deren Auswirkungen sind im Abschnitt 6.3 beschrieben.*

Hinweis (SSOFilter): *Unabhängig von der Wahl der Authentifizierungsmethode ist die Einrichtung des SSOFilters notwending. (Abschnitt 6).*

5. SSO mit SPNego (Kerberos)

5.1 Einrichtung des Active Directory

Um die Kerberos Authentifizierung zu nutzen, müssen zwei Einstellungen am Domänen-Controller vorgenommen werden.

5.1.1 Anlegen des benötigten Benutzerkontos

Die Authentifizierung mit Kerberos erfordert die Einrichtung eines Benutzerkontos im Active Directory. Wichtig hierbei ist, dass folgende Optionen ausgewählt sind (vgl. Abb. 4):

- Kennwort läuft nicht ab
- keine Kerberos-Präauthentifizierung erforderlich

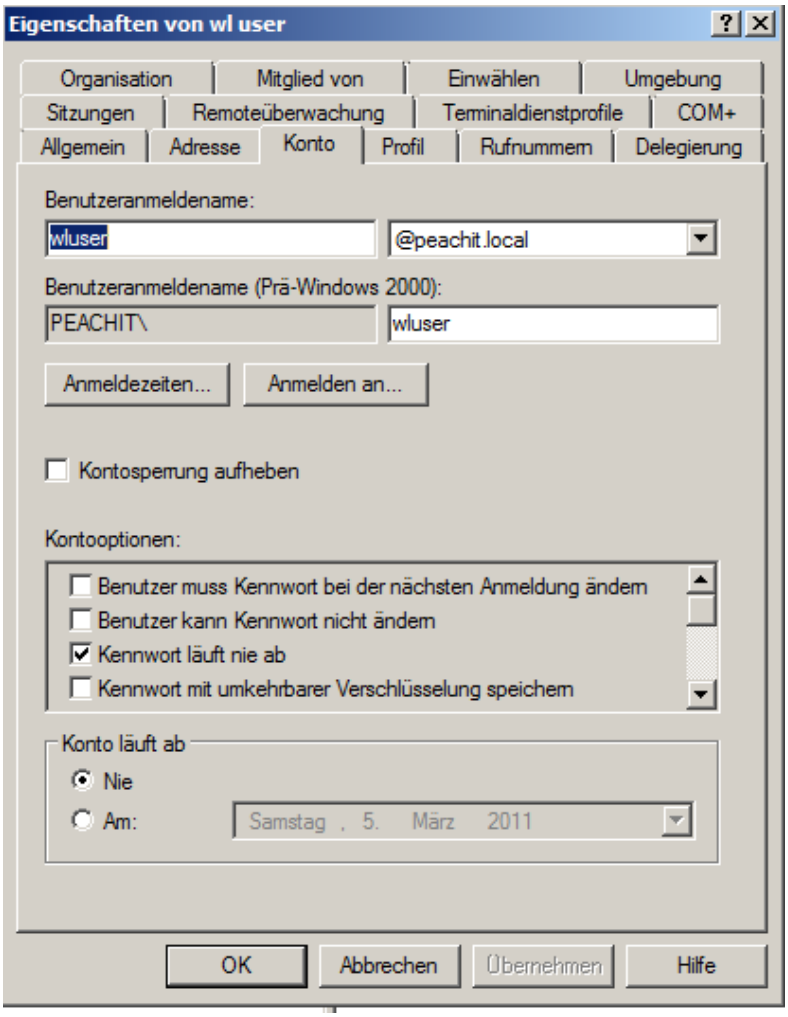

Abb. 4: Beispiel Windows Server 2008

5.1.2 Einrichten der Service Principal Names (SPN)

Zusätzlich müssen für den angelegten Nutzer noch s.g. Service `Principal Names` angelegt werden. Hierfür steht der Befehl „`setspn`“ zur Verfügung. Dieser ist wie folgt zu verwenden und legt eine neue SPN für den HTTP Dienst auf `rechnername` für `username` an:

```
setspn -a HTTP/rechnername username
```

Folgender Befehl zeigt alle dem User `wluser` zugewiesenen SPNs an:

```
setspn -l wluser
```

Befehl zur Suche und Anzeige doppelt zugewiesener SPNs:

```
setspn -x
```

Für die Nutzung mit **DOCUMENTS 5** müssen zwei SPNs für den **DOCUMENTS 5**-Applikationsserver eingerichtet werden. Der Service Name entspricht dem Domänennamen, auf den zugegriffen wird. Angenommen **DOCUMENTS 5** ist auf dem Rechner mit dem Namen „`portalserver`“ in der Domäne „`peachit.local`“ installiert, können die Befehle wie folgt aussehen (vgl. Abb. 5):

```
setspn -a HTTP/portalserver wluser

setspn -a HTTP/portalserver.peachit.local wluser
```

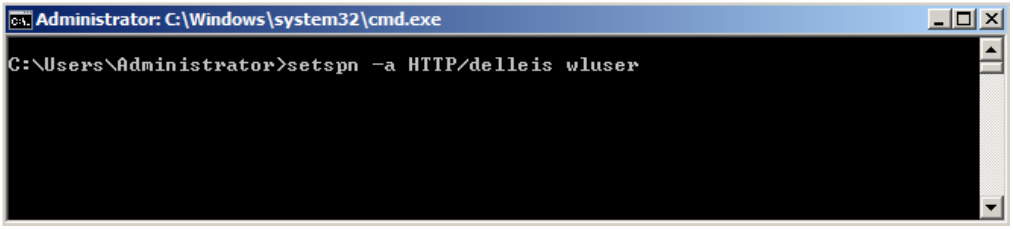

Abb. 5: Befehl setspn in der Kommandozeile

***WICHTIG:** Ein Service (HTTP/portalserver) darf immer nur genau einem User zugeordnet werden. Einem User können aber mehrere SPNs zugeordnet werden. Um sicherzustellen, dass diese Restriktionen eingehalten werden, kann der Befehl „setspn –x“ ausgeführt werden.*

5.2 Konfigurationsdateien für SPNego

Für SPNego müssen zwei Konfigurationsdateien angelegt werden, die an einer beliebigen Stelle im System abgelegt werden können. Später wird der Pfad zu beiden Dateien in die Einstellungen des Filters eingetragen.

Inhalt der Datei `login.conf`

```
spnego-client {
  com.sun.security.auth.module.Krb5LoginModule required;
};

spnego-server {
  com.sun.security.auth.module.Krb5LoginModule required
  storeKey=true
  isInitiator=false
   debug=true;
};
```

Inhalt der Datei `krb5.conf`

```
[libdefaults]
  default_realm = PEACHIT.LOCAL
  default_tkt_enctypes = des-cbc-md5 des-cbc-crc rc4-hmac des3-cbc-sha1 aes128-cts
  default_tgs_enctypes = des-cbc-md5 des-cbc-crc rc4-hmac des3-cbc-sha1 aes128-cts
  permitted_enctypes = des-cbc-md5 des-cbc-crc rc4-hmac des3-cbc-sha1 aes128-cts

[realms]

PEACHIT.LOCAL  = {
    kdc = 192.168.7.75
    default_domain = PEACHIT.LOCAL
}

[domain_realm]
  .PEACHIT.LOCAL = PEACHIT.LOCAL
```

Hier muss der Domänenname "`PEACHIT.LOCAL`" durch den korrekten Domänennamen ersetzt werden.

5.3 Installation von SPNego

Zunächst muss das aktuelle SPNego Paket von **http://spnego.sourceforge.net/** heruntergeladen werden. Die heruntergeladene `.jar` – Datei muss in das Verzeichnis `www/WEB-INF/lib` kopiert werden. Danach ist ein Neustart des Tomcat erforderlich. SPNego wurde in der Version r7 erfolgreich getestet.

5.4 Hinzufügen des SPNego Filters

Für die Einrichtung der Kerberos Authentifizierung muss außerdem der SPNego Filter in die Datei `www/WEB-INF/web.xml` hinzugefügt werden. Dazu muss folgender Text nach dem letzten `<filter>` Element und vor dem ersten `<filter-mapping>` Element eingefügt werden.

```
<filter>
    <filter-name>SpnegoHttpFilter</filter-name>
    <filter-class>net.sourceforge.spnego.SpnegoHttpFilter</filter-class>
    <init-param>
        <param-name>spnego.allow.basic</param-name>
        <param-value>false</param-value>
    </init-param>
    <init-param>
        <param-name>spnego.allow.localhost</param-name>
        <param-value>false</param-value>
    </init-param>
    <init-param>
        <param-name>spnego.allow.unsecure.basic</param-name>
        <param-value>false</param-value>
    </init-param>
    <init-param>
        <param-name>spnego.login.client.module</param-name>
        <param-value>spnego-client</param-value>
    </init-param>
    <init-param>
        <param-name>spnego.krb5.conf</param-name>
        <param-value>C:\tmp\krb5.conf</param-value>
    </init-param>
    <init-param>
        <param-name>spnego.login.conf</param-name>
        <param-value>C:\tmp\login.conf</param-value>
    </init-param>
    <init-param>
```

```
        <param-name>spnego.preauth.username</param-name>
        <param-value>spnego</param-value>
    </init-param>
    <init-param>
        <param-name>spnego.preauth.password</param-name>
        <param-value>passwort</param-value>
    </init-param>
    <init-param>
        <param-name>spnego.login.server.module</param-name>
        <param-value>spnego-server</param-value>
    </init-param>
   <init-param>
        <param-name>spnego.prompt.ntlm</param-name>
        <param-value>true</param-value>
    </init-param>
    <init-param>
        <param-name>spnego.logger.level</param-name>
        <param-value>1</param-value>
    </init-param>
</filter>

<filter-mapping>
    <filter-name>SpnegoHttpFilter</filter-name>
    <url-pattern>/jsp/autologin</url-pattern>
</filter-mapping>
```

5.4.1 Anpassung der Parameter

- `spnego.login.client.module`: Name der für die Einstellung in der Datei `login.conf` verwendet wurde. Standard: `spnego-client`
- `spnego.preauth.username`: Benutzername des angelegten SPNego Benutzers
- `spnego.preauth.password`: Passwort des angelegten SPNego Benutzers
- `spnego.login.server.module`: Name der für die Einstellung in der Datei `login.conf` verwendet wurde. Standard: spnego-server

Hinweis zur Angabe des url-pattern: *Die verschiedenen Möglichkeiten für die Einstellung des url-pattern und deren Auswirkungen sind im Abschnitt 6.3 beschrieben.*

Hinweis (SSOFilter): *Unabhängig von der Wahl der Authentifizierungsmethode ist die Einrichtung des SSOFilters notwending. (Abschnitt 6).*

5.5 Einrichtung von Firefox

Um Kerberos mit Firefox nutzen zu können, muss eine Einstellung im Browser vorgenommen werden. Hierzu wird die Konfiguration aufgerufen, indem in der Adresszeile des Firefox „`about:config`“ angegeben wird (Abb. 6).

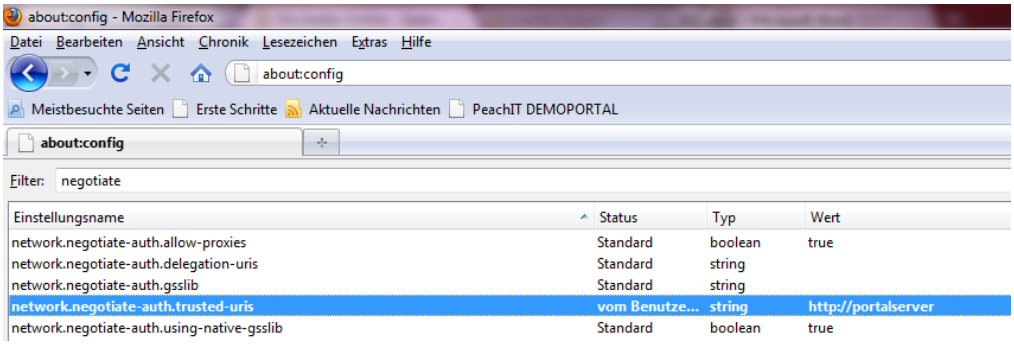

Abb. 6: Firefox-Einstellungen

Hier muss die URL des Anwendungsservers Schlüssel „`network.negotiate-auth.trusted-uris`“ eingetragen werden.

5.6 Einstellungen für den Internet Explorer

Um Kerberos mit dem Internet Explorer nutzen zu können, müssen zwei Einstellungen aktiviert sein. Ab der Version 7 des Internet Explorers, sind diese Einstellungen standardmäßig aktiviert.

5.6.1 Aktivierung des automatischen Logins

Um den automatischen Login in der Intranet-Zone zu erlauben, muss folgende Option aus Abb. 7 und Abb. 8 aktiviert werden:

Extras -> Internetoptionen -> Sicherheit -> Lokales Intranet -> Stufe Anpassen -> Benutzer Authentifizierung -> „Automatisches Anmelden nur in der Intranetzone“

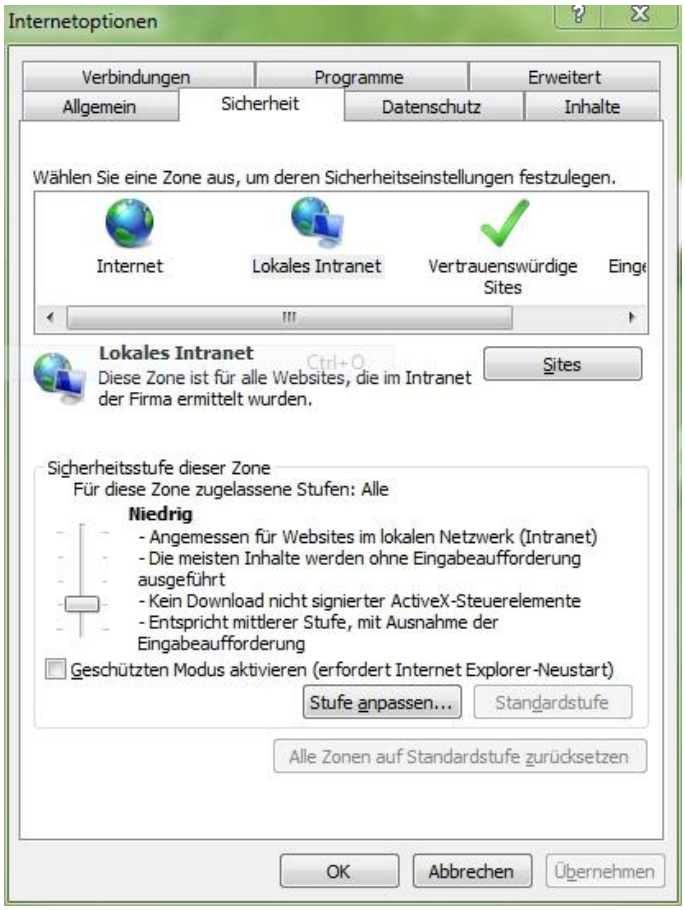

Abb. 7: Dialog "Internetoptionen"

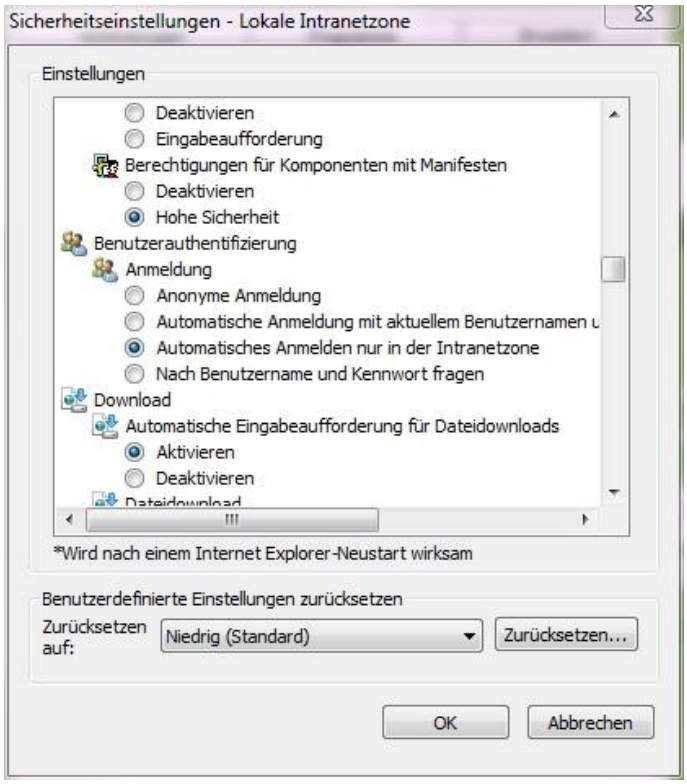

Abb. 8: Automatisches Anmelden nur in der Intranetzone aktiviert

5.6.2 Integrierte Windows-Authentifizierung aktivieren

Die Aktivierung dieser Option erfolgt im Reiter „Erweitert“ des Internetoptionen – Dialogs. Hier muss die Option „Integrierte Windows-Authentifizierung aktivieren“ ausgewählt sein (vgl. Abb. 9).

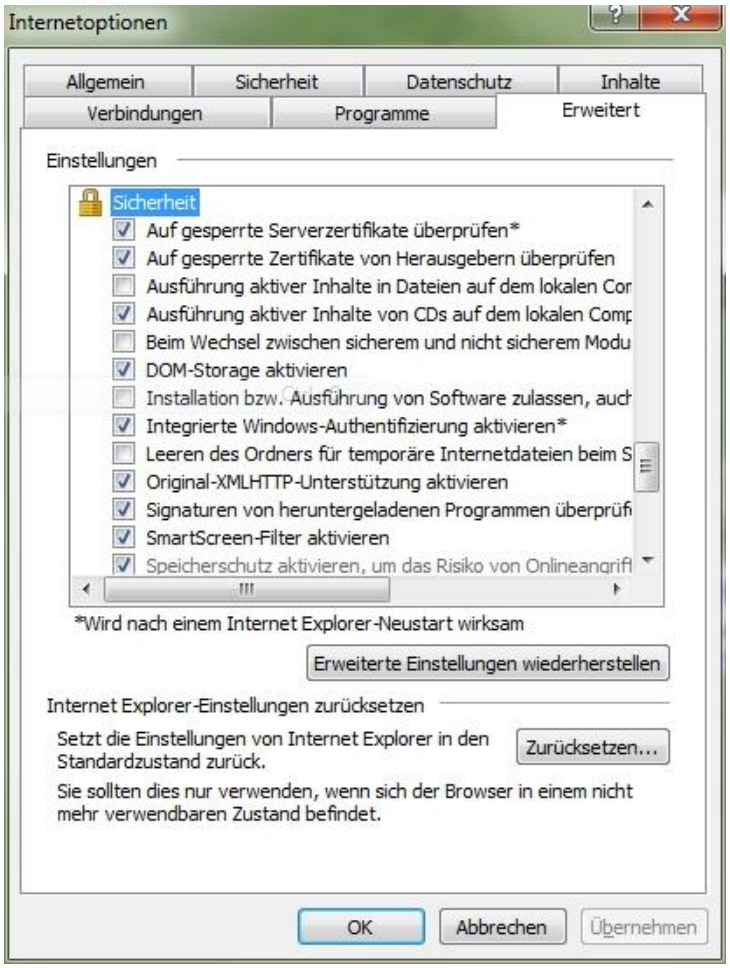

Abb. 9: Integrierte Windows-Authentifizierung aktivieren

5.7 Hilfsmittel

Um die korrekte Konfiguration von Kerberos zu überprüfen, ist es hilfreich zu wissen welche Tickets einem Client-System zugewiesen sind. Dies kann mit dem Programm „Kerbtray“ aus dem Resource-Toolkit überprüft werden. Für die korrekte Funktion muss ein *Ticket Granting Ticket (TGT)* für den angemeldeten Benutzer, sowie ein korrektes *Service Ticket* für den Anwendungsserver vorhanden sein (siehe Abb. 10 und Abb. 11).

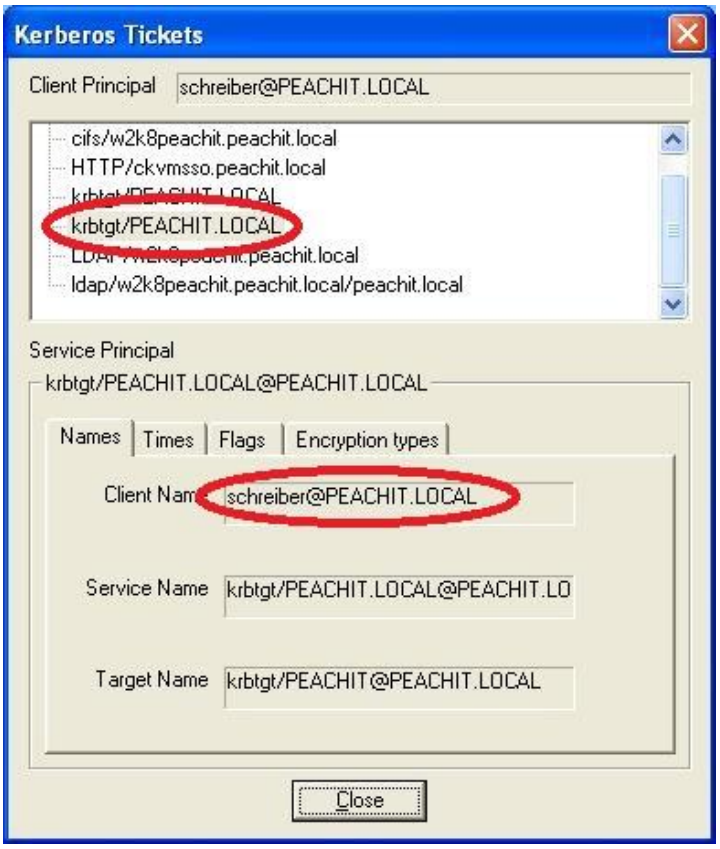

Abb. 10 :Ticket Granting Ticket (TGT) für Benutzer "schreiber"

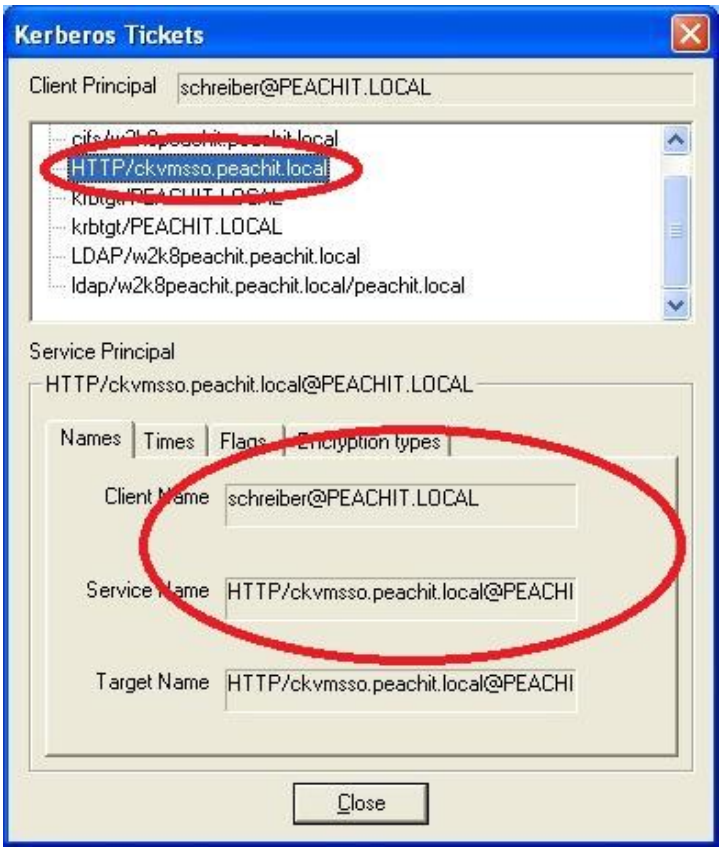

Abb. 11 :Service Ticket für den Server ckvmsso.peachit.local

6. Single Sign-On benutzen

6.1 Installation des SSO-Filters

Der benötigte SSO-Filter (`otrisSSO.jar`) ist bereits installiert und befindet sich im Verzeichnis „`www/WEB-INF/lib`“.

6.2 Hinzufügen des SSO-Filters

Um die SSO Funktionalität für **DOCUMENTS 5** zu nutzen muss zusätzlich zum Filter des jeweiligen Authentifizierungsmoduls noch ein weiterer Filter der Datei `web.xml` hinzugefügt werden. Dazu kann folgender Code in die Filter-Sektion der `web.xml` kopiert werden.

```
<filter>
       <filter-name>SSOFilter</filter-name>
        <filter-class>de.otris.portal.filter.SSOFilter</filter-class>
</filter>

<filter-mapping>
<filter-name>SSOFilter</filter-name>
       <url-pattern>/jsp/autologin</url-pattern>
</filter-mapping>
```

6.3 Einstellung des url-pattern

Die url-pattern der verschiedenen Authentifizierungsmodule und des SSO-Filters können für drei verschiedene Fälle gesetzt werden:

1. `/jsp/epctrl.jsp`
   SSO wird für die Standardadresse des Documents-Systems verwendet.

2. `/jsp/autologin`
   SSO wird für den autologin link aktiviert

3. `/jsp/qv`
   SSO wird für QuickView aktiviert. (Beim Anklicken von Links die auf **DOCUMENTS 4**-Inhalte verweisen, wird der User ebenfalls per SSO authentifziert.

Die verschiedenen url-pattern können in beliebiger Kombination verwendet werden. Wichtig ist, dass sowohl bei der Einstellung des jeweiligen Filters der Authentifizierungsmethode als auch für den SSOFilter die gleiche Einstellung verwendet wird. Sollen mehrere url-patterns gleichzeitig verwendet werden, muss jeweils ein neues „`filter-mapping`“ Element angelegt werden.

Beispiel:

```
<filter-mapping>
    <filter-name>SpnegoHttpFilter</filter-name>
    <url-pattern>/jsp/autologin</url-pattern>
</filter-mapping>

<filter-mapping>
    <filter-name>SpnegoHttpFilter</filter-name>
    <url-pattern>/jsp/qv</url-pattern>
</filter-mapping>

<filter-mapping>
<filter-name>SSOFilter</filter-name>
       <url-pattern>/jsp/autologin</url-pattern>
</filter-mapping>
<filter-mapping>
<filter-name>SSOFilter</filter-name>
       <url-pattern>/jsp/qv</url-pattern>
</filter-mapping>
```

Im obigen Beispiel wird SSO für den autologin-Link und für QuickView aktiviert. Ruft ein Benutzer die Standard-url des **DOCUMENTS 5**-Systems auf `(/jsp/epctrl.jsp)` wird der Anmeldedialog angezeigt.

6.4 Verwendung des Auto-Login-Links

Um automatisch an **DOCUMENTS 5** angemeldet zu werden, kann ein Autologin-Link verwendet werden. Hierzu meldet man sich einmal wie bisher an **DOCUMENTS 5** an.

Nun ersetzt man in der Adressleiste die Zeichenkette „`epctrl.jsp`“ durch „`autologin`“ (Abb. 12 und Abb. 13).

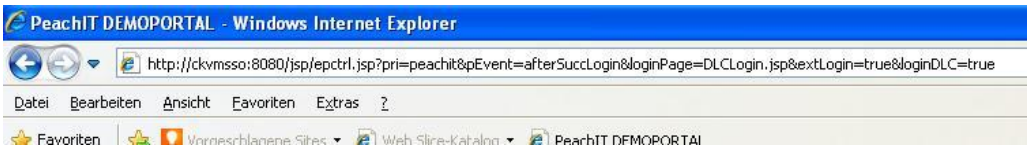

Abb. 12: Ursprüngliche Adresse

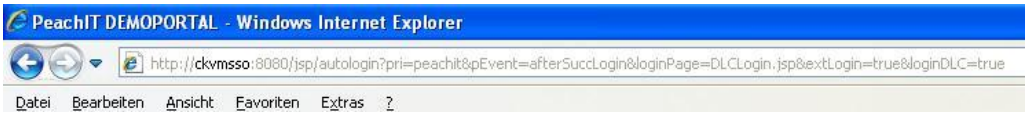

Abb. 13: Neue Adresse

Wenn dieser Link nun aufgerufen wird, wird der aktuell am Windows System angemeldete Benutzer automatisch in **DOCUMENTS 5** angemeldet.

6.4.1 Favoriten im Internet Explorer

Im Internet Explorer kann das Anlegen eines Favoriten für den AutoLogin Link zu Problemen führen (SSO funktioniert beim direkten Aufruf des Links in der Adresszeile, aber nicht beim Aufruf des Favoriten). Um dies zu verhindern, muss der Favorit manuell angelegt werden. (Rechtsklick auf den Desktop -> Neu -> Verknüpfung).

In dem geöffneten Dialog kann nun als „Speicherort“ der AutoLogin Link angegeben werden. Die angelegte Datei kann nun direkt vom Desktop aufgerufen werden oder per Drag & Drop in die Favoritenleiste des Internet Explorers verschoben werden.

7. Häufige Fehler

Genereller Hinweis zum Testen von SSO:

Für jeden neuen Versuch der automatischen Anmeldung per SSO müssen ALLE laufenden Internet Explorer-Fenster und Prozesse beendet sein. Nur so kann sichergestellt werden dass ein neuer Versuch der automatischen Anmeldung unternommen wird.

Nach der Einrichtung von SSO startet der Tomcat nicht mehr bzw. stürzt während des Starts ab.

Die Ursache hierfür sind meistens Fehler in der Datei *web.xml*. Es ist besonders darauf zu achten dass:

- Die Datei **valides XML** enthält d.h. vor allem, dass jedes geöffnete Element auch wieder geschlossen wird. (Vorsicht vor „copy & paste"-Fehlern).
- Bei der Einrichtung der Filter und generell beim Bearbeiten der *web.xml* ist es wichtig auf **Groß- und Kleinschreibung** zu achten, da dies besonders bei der Angabe von Java-Klassennamen wichtig ist.
- Zur Sicherheit sollten außerdem **Leerzeichen und Zeilenumbrüche** innerhalb einzelner XML Element die Konfigurationsinformationen enthalten vermieden werden.

Beim Versuch der automatischen Anmeldung wird ein Windows Login-Fenster angezeigt.

Hierfür gibt es verschiedene Ursachen die teilweise auch in mehrfacher Kombination auftreten. Deshalb sollten folgende Punkte beachtet werden:

- Unabhängig von der verwendeten Authentifizierungsmethode müssen **immer zwei Filter** in der *web.xml* eingerichtet werden.
    - 1.) Der Filter für die Authentifizierung (Waffle, Jespa, SPNego)
    - 2.) Der SSOFilter (Siehe Abschnitt 6.1 und 6.2)
- Es ist absolut wichtig, dass die „filter-mapping"-Elemente für den SSOFilter in der *web.xml* **immer NACH** den „filter-mapping"- Elementen für die Authentifizierungsmethode eingetragen werden.
- Die Datei „**otrisSSO.jar**" muss im Verzeichnis „www/WEB-INF/lib" **vorhanden sein**. Diese wird erst ab Documents 4.0 mitgeliefert.
- Der Internet Explorer muss so eingestellt sein, dass er **die Login Informationen automatisch sendet**. Der einfachste Weg dies zu erreichen ist in den meisten Fällen den Server auf dem die Documents Seiten liegen in die **Intranet-Zone oder zu den Trusted-Sites** hinzuzufügen.

8. Abbildungsverzeichnis