DOCUMENTS 4

SINGLE SIGN-ON

Installation and Administration

VERSION 1.2.1

Table of Contents

1. General

1.1 Benefit of single sign-on

The use of single sign-on (SSO) requires that users authenticate themselves on a workstation only once and can then access all resources and services for which they have permission. Renewed login is not required. With regard to SSO, DOCUMENTS 4 supports several standard procedures on authentication. This document describes setting up the system environment for using these authentication methods in combination with DOCUMENTS 4.

1.2 Requirements

To be able to use SSO, the following requirements must be met for the system environment:

1.2.1 Domain controller

A domain must exist which is managed by a domain controller providing an *Active Directory*. This requires the *Microsoft Windows Server* operating system (tested with version 2008).

1.2.2 Application server

The application server on which the DOCUMENTS 4 installation is running must be accessible by the domain controller and by the workstations from the network. However, it does not necessarily be a member of the domain.

1.2.3 Workstation

Each workstation computer from which SSO should be used must be a member of the domain. Also, each user to log on via SSO should be a member of the domain and be created under the same user name in DOCUMENTS 4 - or, when LDAP coupling is available - be created in LDAP. The user's password must be identical in the domain an in DOCUMENTS 4 or LDAP.

When accessing a workstation that is not a member of the domain, a standard browser dialog (Basic-Auth) will be used to query the user's user name and password (see Fig. 1). The user will then be authenticated against the domain, and gain access to DOCUMENTS 4.

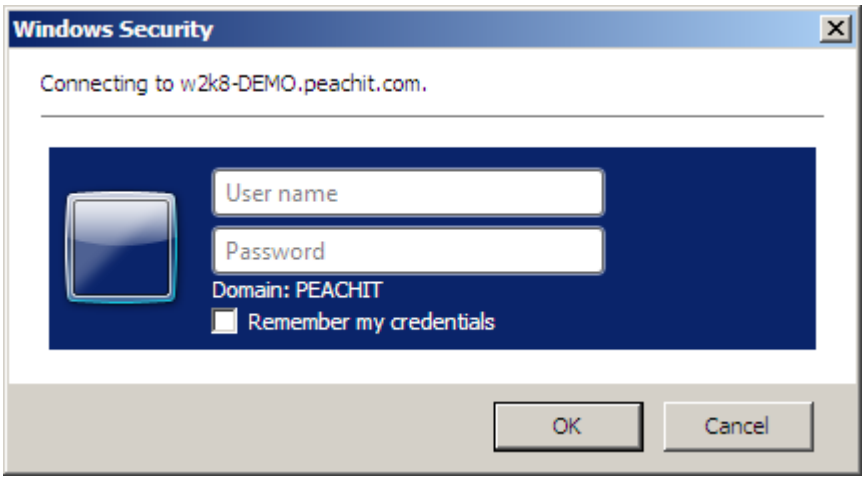

Fig. 1: Standard logon dialog under Windows 7

1.2.4 Authentication method

SSO setup requires that you are familiar with the authentication method to be used. *NTLMv1, NTLMv2* and *Kerberos* are supported. The customer's system administrator must define which authentication method is to be used.

1.3 Setting up the DOCUMENTS 4 server

To allow login via SSO in the DOCUMENTS Manager, you need to add a new property named `autoLogin = 1` for the ***principal*** (Fig. 2).

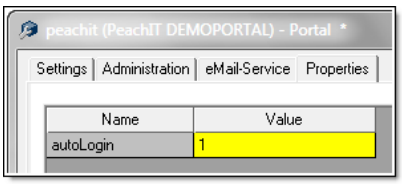

Fig. 2: Properties of the principal

> *You need to ensure that the "Auto-login" setting on the "DOCUMENTS -> Settings" menu is turned off. This function cannot be used with SSO at the same time because auto-login and SSO are two competing login procedures.*

1.4 Selecting the authentication module

To perform authentication on the Active Directory, multiple authentication modules are available. Module selection depends on which method is to be used for authentication.

Based on the following table, the suitable authentication module can be used using the authentication method.

Auth. Module	**NTLMv1**	**NTLMv2**	**Kerberos**
JCIFS	Yes	No	No
WAFFLE*	Yes	Yes	Yes
JESPA	Yes	Yes	No
SPNEGO	No	No	Yes

* For Waffle the application server must run on a Windows system.

The other configuration steps are explained below to use the respective authentication module.

> *NOTE! Consider the following when using NTLMv2:*
>
> *JESPA and WAFFLE allow authentication both via NTLMv1 and NTLMv2. If you want to ensure that NTLMv2 is used, you must set this in the Domain Controller's group policies.*

This setting can be found in the Domain Controller under: "*Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies > Security Options*"; its name is "*Network Security: LAN Manager authentication level*". You need to select the appropriate option.

1.5 Overview of the system environment

Fig. 3 shows the structure of the system environment for the use of SSO with DOCUMENTS 4:

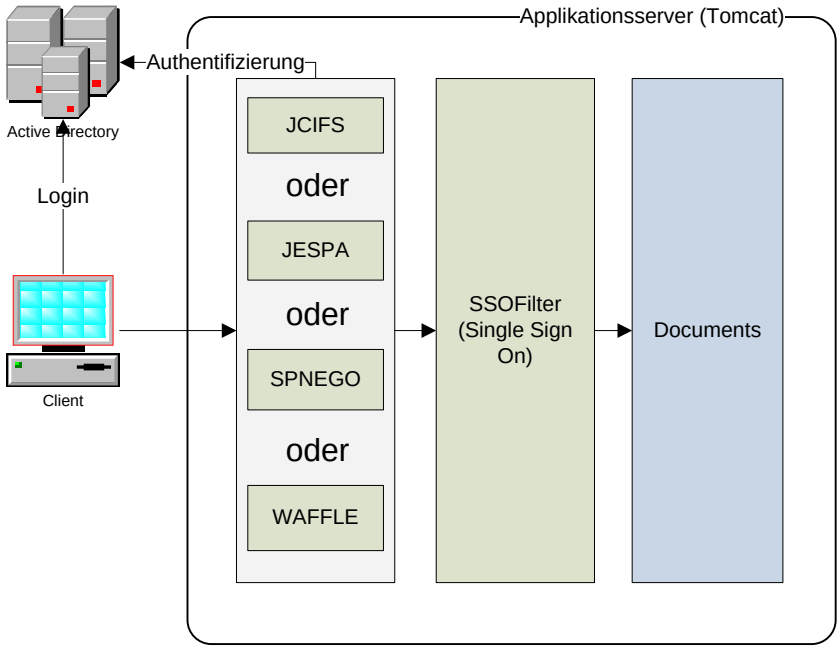

Fig. 3: System environment

The sections below describe which steps must be carried out to set up the different authentication modules.

2. SSO Using JCIFS (NTLMv1)

JCIFS is a program library that provides, among others, the functionality for authentication via NTLMv1. Details can be obtained at http://jcifs.samba.org/.

2.1 Installing JCIFS

As a rule, JCIFS version 1.1.9 is already preinstalled. If this is not the case, you can download a current version at http://jcifs.samba.org/. The downloaded archive named `jcifs_1.1.9.zip` contains the `jcifs_1.1.9.jar` file. This file must be copied to the `www/WEB-INF/lib` directory. You will then have to restart Tomcat. JCIFS version 1.1.9 has been successfully tested.

2.2 Adding the JCIFS filter

To enable authentication via NTLMv1, you need to add a filter in the `web.xml` file of the DOCUMENTS 4 application. To do this, you must insert the following text after the last `<filter>` element and before the first `<filter mapping>` element.

```
<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>PASSWORD</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 Customizing the parameters

- `jcifs.http.domainController` :Domain Controller's DNS name
- `jcifs.smb.client.username`: User name of any user with access to the domain (administrator rights not required). That user is used to query information on authenticating the user to be logged in.
- `jcifs.smb.client.password`: User's password
- `jcifs.smb.client.domain`: Domain name

> ***Note to specifying the url pattern:*** *The different options for setting the url pattern and its effects are described in section 6.3.*

3. SSO Using WAFFLE (NTLMv2 + Kerberos)

3.1 Installing Waffle

First you need to download the current Waffle package at http://waffle.codeplex.com/. The downloaded archive named `waffle.1.3.zip` contains the `Waffle/Bin` directory. All files with the "`.jar`" extension must be copied to the `www/WEB-INF/lib` directory. You will then have to restart Tomcat. Waffle version 1.3 has been successfully tested.

3.2 Adding the filter

To be able to use WAFFLE, adding the following filter to the `web.xml` file is enough.

```
<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 Customizing the parameters

- `waffle.servlet.spi.NegotiateSecurityFilterProvider`: This parameter is used to set which authentication procedure to use. In our example, NTLMv1 or NTLMv2 is used. Which version is used depends on the Domain Controller settings. See: "NOTE! Consider the following when using NTLMv2." in section 1.4.

To use Kerberos, you need to enter "Negotiate" here.

> ***Note to specifying the url pattern:*** *The different options for setting the url pattern and its effects are described in section 6.3.*

4. SSO Using JESPA (NTLMv1 + NTLMv2)

4.1 Installing JESPA

JESPA is a program library **subject to a charge** which, among others, provides functions for authentication via NTLMv1 and NTLMv2. JESPA must be purchased from the manufacturer at www.ioplex.com. The downloaded .jar file must be placed in the "www/WEB-INF/lib" directory of the Portal installation. You will then have to restart Tomcat. JESPA version 1.1.6 has been successfully tested.

4.2 Setting up a JESPA user

To be able to use authentication via JESPA, you need to create a COMPUTER account in the Active Directory, and assign it a password. This account can be created directly in the Active Directory. Although an existing computer account can be used, it is recommended that you create a new account so that this can be deleted later, if necessary, without dependencies on the existing system.

To allocate a password to the created account, you need to run the "SetComputerPassword" script that comes with JESPA on the console.

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

When starting it, you need to append a $ sign to the name of the account!

4.3 Adding a JESPA filter

To enable authentication via JESPA, you need to add a filter to the `web.xml` file of the DOCUMENTS 4 application. To do this, you must insert the following text after the last `<filter>` element and before the first `<filter mapping>` element.

```
<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 Customizing the parameters

JESPA provides the option to transfer the filter parameters to Properties files. In this example, the settings were transferred to the `example_ntlm.rpr` file. While downloading, JESPA already has several different configurations.

```
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 = 192.168.7.73
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` : **Complete** DNS name of Domain Controller
- `jespa.dns.servers` : DNS server's IP address
- `jespa.service.acctname`: Name of created JESPA user
- `jespa.service.password`: Password of created JESPA user:
- `jespa.domain.netbios.name`: The domain's Netbios name
- `jespa.domain.dns.name`: **Complete** DNS name of the domain
- `jespa.authority.dns.names.resolve`: Must be set to `false` in this configuration.

> ***Note to specifying the url pattern:*** *The different options for the url pattern setting and its effects are described in section 6.3.*

5. SSO Using SPNego (Kerberos)

5.1 Setting up the Active Directory

To use Kerberos authentication, you need to make two settings on the Domain Controller.

5.1.1 Creating the required user account

Authentication via Kerberos requires setting up a user account in the Active Directory. It is important here that the following options are selected (see Fig. 4):

- Password does not expire
- no Kerberos preauthentication required

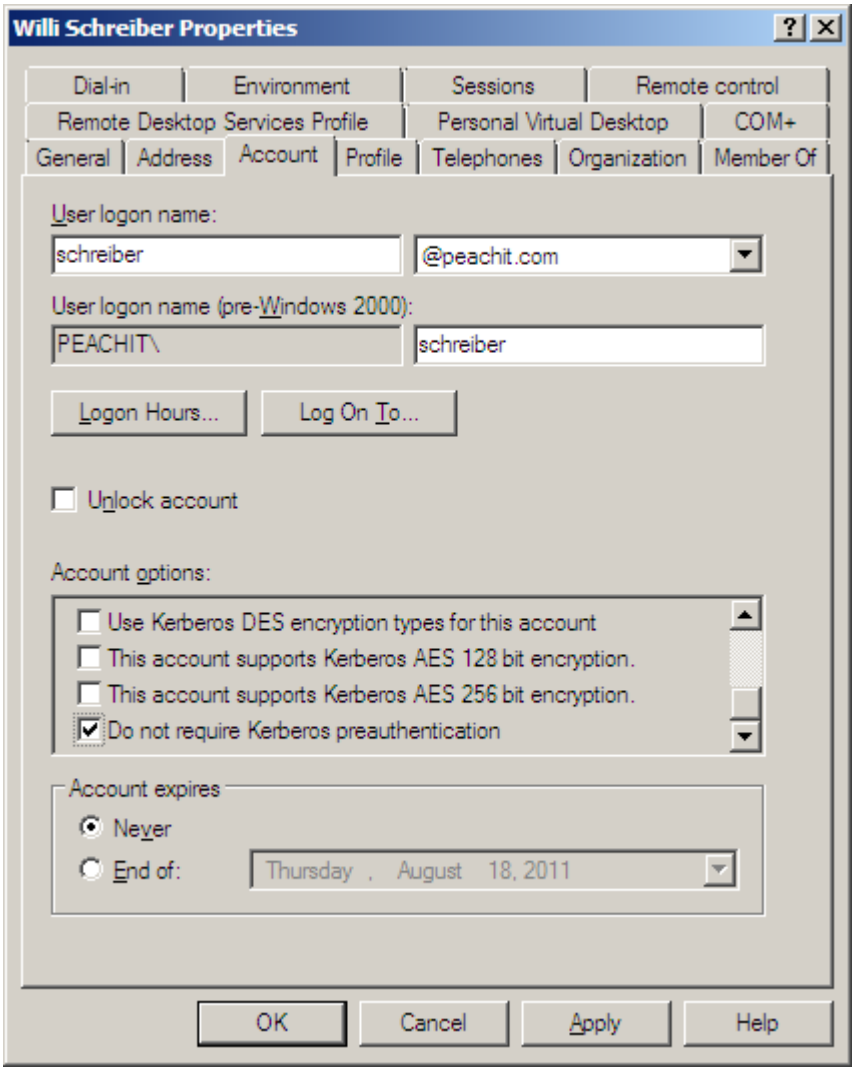

Fig. 4: Example: Windows Server 2008

5.1.2 Configuring the Service Principal Names (SPN)

In addition, you need to create so-called Service `Principal Names` for the created user. To do this, the "`setspn`" command is available. This must be used as follows and creates a new SPN for the HTTP service on `computername` for `username`:

```
setspn -a HTTP/computername username
```

The following command indicates all SPN assigned to the user `wluser`:

```
setspn -l wluser
```

Command for searching and displaying SPNs assigned twice:

```
setspn -x
```

For the use with DOCUMENTS 4 you need to set up two SPNs for the DOCUMENTS 4 application server. The service name corresponds to the domain name that is accessed. Assuming DOCUMENTS 4 is installed on the computer named "`portalserver`" in the "`peachit.local`" domain, then the commands may look as follows (see Fig. 5):

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

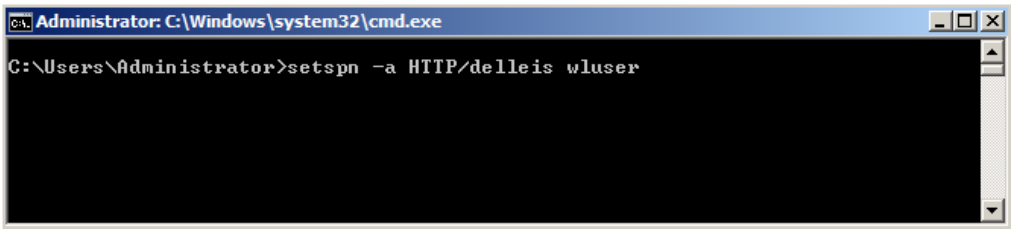

Fig. 5: The setspn command in the command line

> ***IMPORTANT:*** *A service (HTTP/portalserver) may only be assigned to exactly one user. But a user can be assigned several SPNs. To ensure that these restrictions are kept, you can execute the "setspn –x" command.*

5.2 Configuration files for SPNego

For SPNego you need to create two configuration files that can be stored in anywhere within the system. The path to both files is entered later in the filter settings.

Content of the `krb5.conf` file

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

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

Content of the *login.conf* file

```
[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
```

The domain name "`PEACHIT.LOCAL`" must be replaced with the correct domain name here.

5.3 Installing SPNego

Initially, you need to download the current SPNego package at http://spnego.sourceforge.net/. The downloaded `.jar` file must be copied to the `www/WEB-INF/lib` directory. You will then have to restart Tomcat. SPNego version r7 has been successfully tested.

5.4 Adding the SPNego filter

To set up Kerberos authentication, you additionally need to add the SPNego filter to the `www/WEB-INF/web.xml` file. To do this, you must insert the following text after the last `<filter>` element and before the first `<filter mapping>` element.

```
<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>password</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 Customizing the parameters

- `spnego.login.client.module`: Name used for the setting in the `login.conf` file. Default: `spondeo-client`
- `spnego.preauth.username`: User name of the created SPNego user
- `spnego.preauth.password`: Password of the created SPNego user
- `spnego.login.server.module`: Name used for the setting in the `login.conf` file. Default: spnego-server

> ***Note to specifying the url pattern:*** *The different options for the url pattern setting and its effects are described in section 6.3.*

5.5 Setting up Firefox

To be able to use Kerberos with Firefox, you need to make a setting in the browser. To do this, you start the configuration by specifying "about:config" in the `Firefox` address line (Fig. 6).

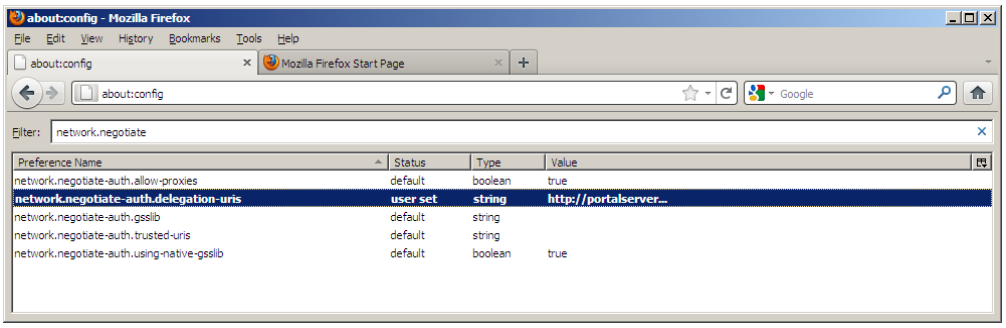

Fig. 6: Firefox settings

You need to enter the URL of the application server key "`network.negotiate-auth.trusted-uris`" here.

5.6 Settings for Internet Explorer

To be able to use Kerberos with Internet Explorer, two settings must be enabled. In Internet Explorer version 7 or higher these settings are enabled by default.

5.6.1 Enabling auto-login

To allow automatic logon in the Intranet zone, the following option from Fig. 7 and Fig. 8 must be enabled:

> *Tools -> Internet Options -> Security -> Local intranet -> Custom Level -> User Authentication -> "Automatic logon only in Intranet zone"*

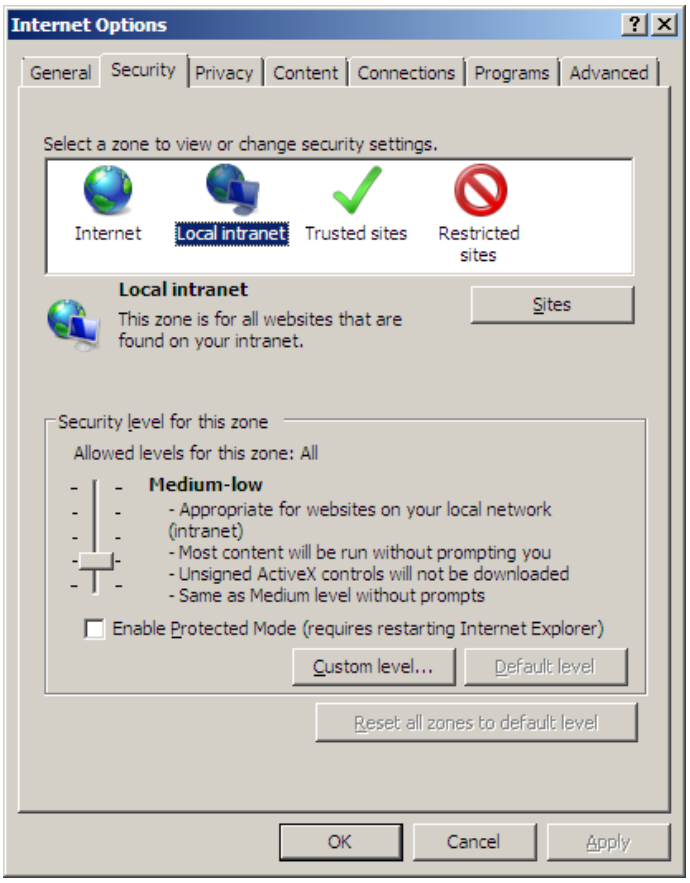

Fig. 7: The "Internet Options" dialog

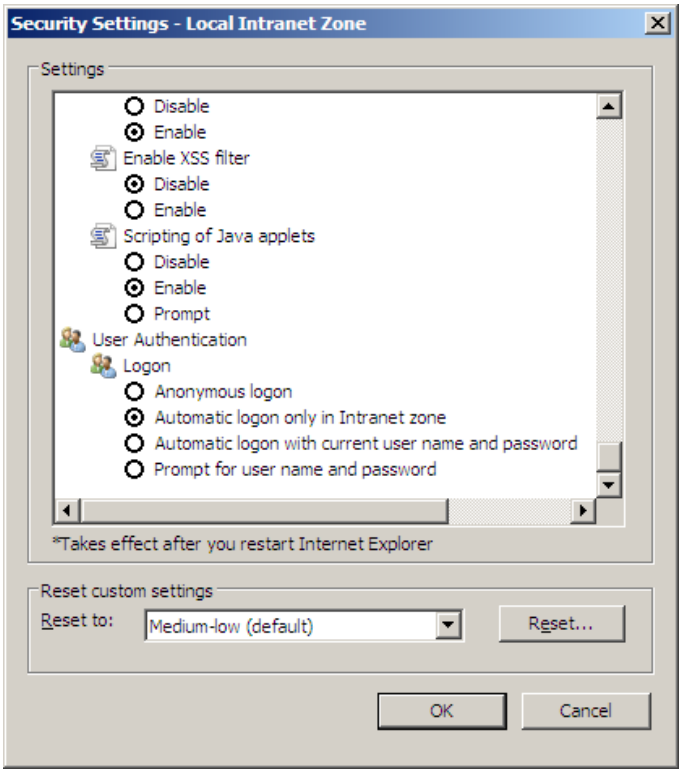

Fig. 8: Automatic logon only in Intranet zone enabled

5.6.2 Enable integrated Windows Authentication

This option is enabled on the "Advanced" tab of the Internet Options dialog. The "Enable integrated Windows authentication" option must be selected here (see Fig. 9).

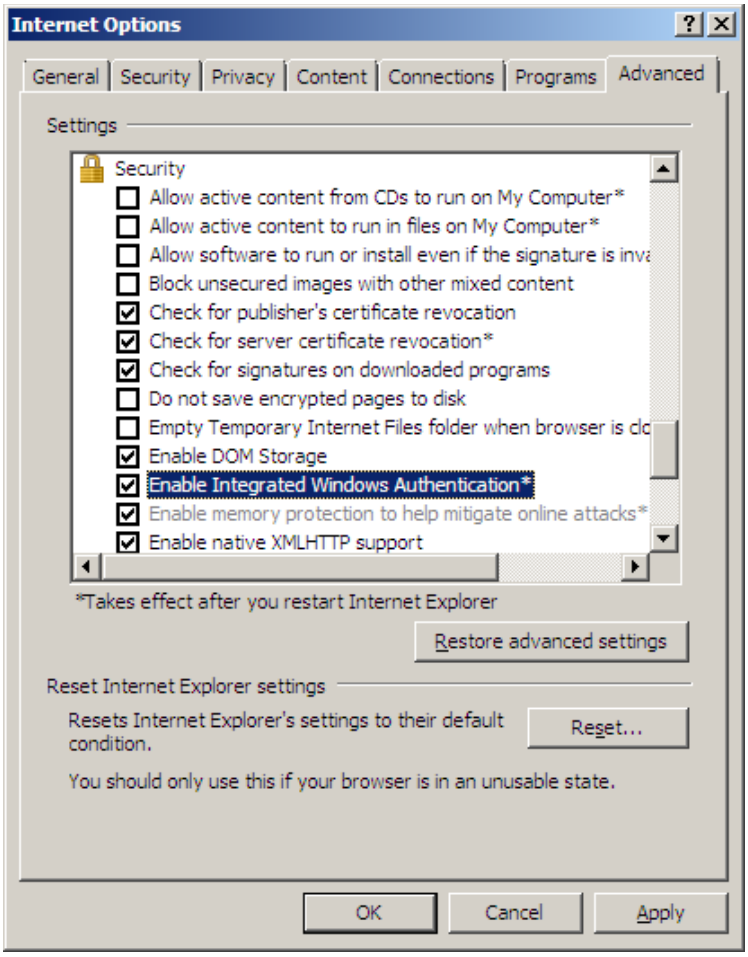

Fig. 9: Enable integrated Windows Authentication

5.7 Aids

To check correct Kerberos configuration, knowing which tickets are assigned to a client system comes in usefully. This can be checked using the "Kerbtray" program from the Resource toolkit. For the correct function a *Ticket Granting Ticket (TGT)* for the logged-in user as well as a correct *Service Ticket* for the application server must be present (see Fig. 10 and Fig. 11).

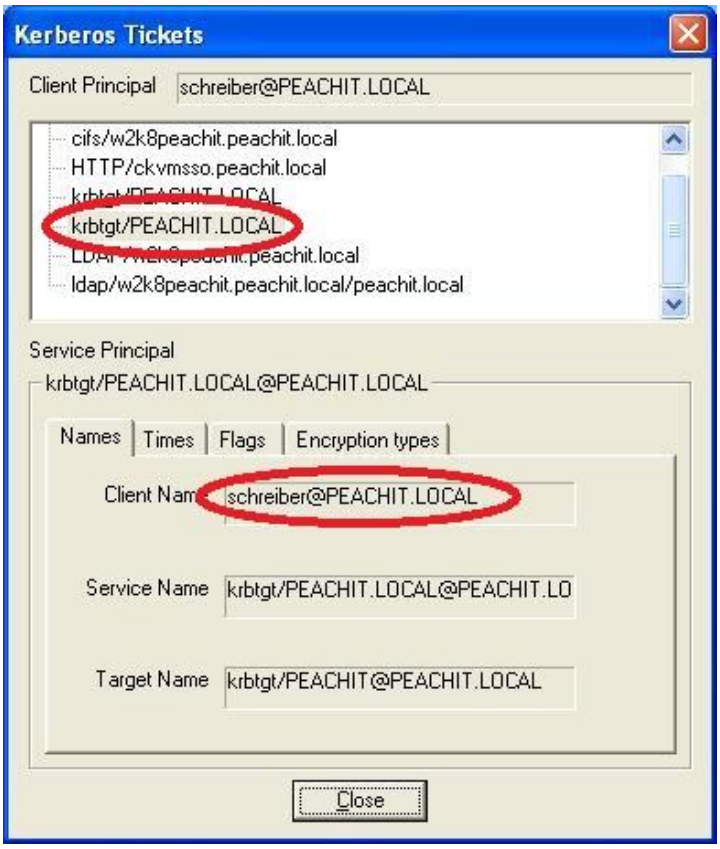

Fig. 10 :Ticket Granting Ticket (TGT) for user "writer"

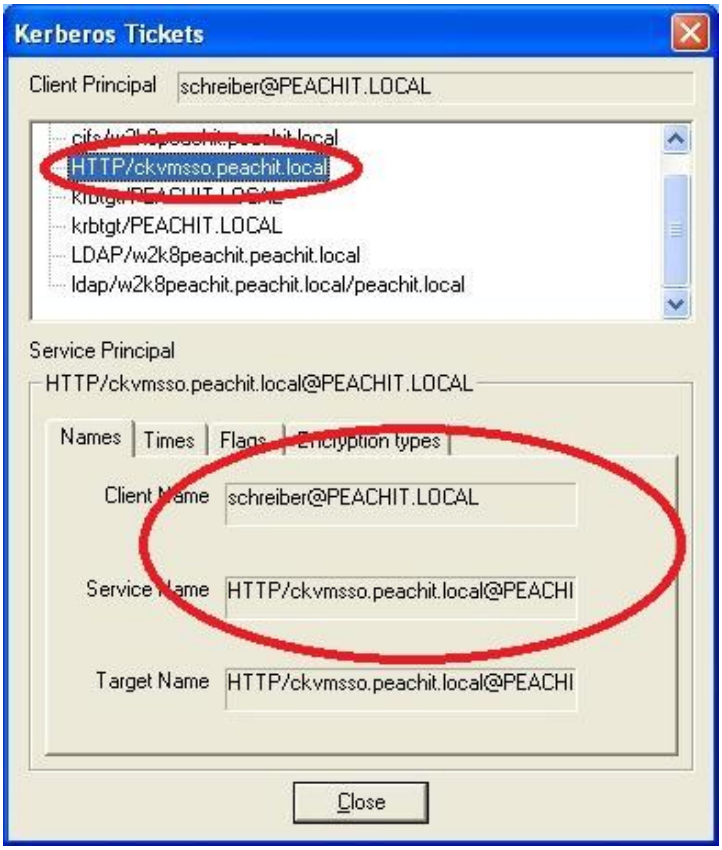

Fig. 11 :Service Ticket for the ckvmsso.peachit.local

6. Using Single Sign-On

6.1 Installing the SSO filter

The required SSO filter (`otrisSSO.jar`) has already been installed; it resides in the "`www/WEB-INF/lib`" directory.

6.2 Adding the SSO filter

To use the SSO functionality for DOCUMENTS 4, you need to add another filter to the `web.xml` file in addition to the filter of the respective authentication module. To do this, the following code can be copied to the filter section of the `web.xml` file.

```
<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 Setting the url pattern

The url patterns of the different authentication modules and the SSO filter can be set for three different cases:

1. `/jsp/epctrl.jsp`
   SSO is used for the default address of the DOCUMENTS system.
2. `/jsp/autologin`
   SSO is enabled for the autologin link
3. `/jsp/qv`
   SSO is enabled for QuickView. (On clicking links referring to DOCUMENTS 4 contents the user will also be authenticated via SSO.)

The different url patterns can be used in any combination. It is important that you use the same setting when setting the respective authentication method filter and for the SSO filter. If multiple url patterns are to be used at the same time, you will have to create the respective new "`filter mapping`" element.

Example:

```
<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>
```

In the above example, SSO is enabled for the autologin link and for QuickView. If a user opens the default url of the DOCUMENTS 4 system (`/jsp/epctrl.jsp`), the login dialog will be displayed.

6.4 Using the auto-login link

To automatically log in to DOCUMENTS 4, you can use an autologin link. To do this, you log in to DOCUMENTS 4 as usual. In the address bar you now replace the "`epctrl.jsp`" string with "`autologin`" (Fig. 12 and Fig. 13).

Fig. 12: Original address

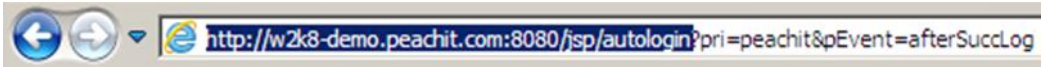

Fig. 13: New address

If you open this link now, the user currently logged in to the Windows system will be automatically logged in to DOCUMENTS 4.

7. Table of Figures