BENUTZERDOKUMENTATION (ALEPHINO 5.0)

Single-Sign-On

Inhalt

Der Alephino Web-OPAC bietet ein einfaches Single-Sign-On Verfahren, das ohne spezielle Konfiguration auf Anwendungsseite nutzbar ist.

1 Wirkungsweise

Stimmt der in der Variablen **REMOTE_USER** des HTTP-Headers gelieferte Code mit dem **Barcode** oder der **Matrikelnummer** (auch sekundäre Benutzer-ID) eines in Alephino registrierten Benutzers überein, ist der betreffende Benutzer automatisch angemeldet und erhält ohne weitere Passwortabfrage Zugang zu personalisierten Funktionen.

2 Windows Benutzer (Domain User)

Das nachfolgend beschriebene Verfahren erlaubt es, die bereits erfolgte proprietäre Windows-Authentifizierung zu den besuchten Webseiten „mitzunehmen“. Im Ergebnis wird REMOTE_USER mit dem Login-Namen (mit vorangestellter Domain) belegt.
Beim erstmaligen „Betreten“ einer geschützten Website mit dem Internet Explorer wird hierbei keine separate Authentifizierung erforderlich, andere Browser hingegen verlangen beim ersten Aufruf des geschützten Bereiches eine erneute Windows-Anmeldung.
Verwenden Sie Mozilla Firefox, ist die automatische Authentifizierung durch Bearbeiten des Parameters ***network.automatic-ntlm-auth.trusted-uris*** zu aktivieren, womit ein dem Internet Explorer vergleichbares Verhalten erzielt wird.
Die Funktionen zur erweiterter Konfiguration des Firefox sind mit der URL ***about:config*** erreichbar. Suchen Sie den vorgenannten Parameter und fügen Sie die Adresse des OPAC dessen Wert hinzu. Bei Angabe mehrerer URLs sind diese durch Kommata zu separieren.

2.1 Konfiguration für Apache

Wird ein Apache http-Server verwendet, ist die Übergabe der Windows Benutzerkennung via REMOTE_USER durch Einbindung des Moduls **mod_auth_sspi** realisierbar.

httpd.conf:

```
LoadModule sspi_auth_module modules/mod_auth_sspi.so
```

vhost.alephino:

```
# OPAC
<VirtualHost *:8060>
…

# Authentication
<IfModule mod_auth_sspi.c>
 <Directory "C:/Programme/ExLibris/AlephinoServer_50/bin">
      AuthName "Alephino OPAC – Benutzerbereich"
      AuthType SSPI
      SSPIAuth On
      SSPIAuthoritative On
      SSPIOfferBasic On
      require valid-user
  </Directory>
</IfModule>
</VirtualHost>
```

3 Konfiguration mit Microsoft Internet Information Server

Das Zusammenwirken von IIS und „Internet Explorer“ erlaubt die Weiterleitung der Windows-Benutzerkennung auf besonders einfache Weise.

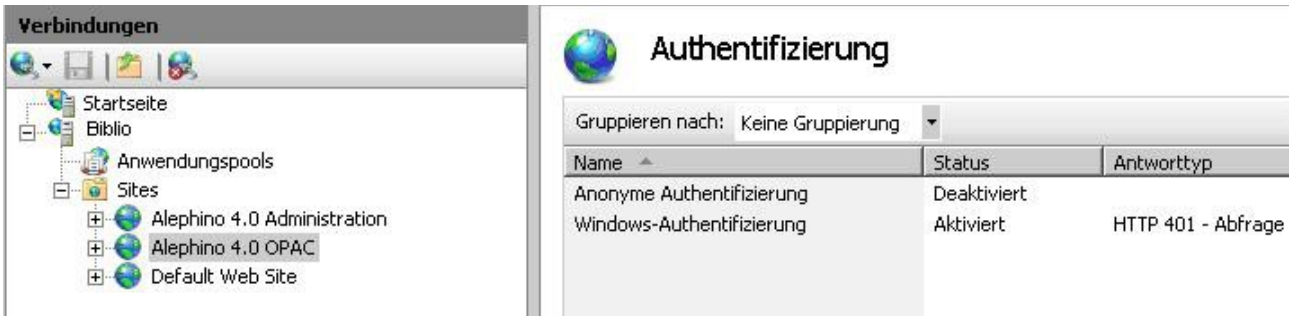
3.1 IIS 6.0 (Windows Server 2003)

Im IIS Konfigurationsdialog sind die Optionen:
„Basic authentication“
und
„Enable Integrated Windows authentication“ zu wählen.

3.2 IIS 7.0 (Windows Server 2008)

Voraussetzung: Es muß das Feature „Authentifizierung“ installiert sein.

Site **OPAC** wählen, auf Ansicht **Features** wechseln und **Authentifizierung** anklicken. Hier muß nun die **Anonyme Authentifizierung** deaktiviert und **Windows-Authentifizierung** aktiviert werden:



Unter **Anwendungspools Erweiterte Einstellungen > Prozessmodell** muß nun die **Identität** „**NetworkService**“ stehen:

3.3 SSO mit Shibboleth

Shibboleth ist ein Verfahren zur verteilten Authentifizierung und Autorisierung für Webanwendungen und Webservices. Das Konzept von Shibboleth sieht vor, dass der Benutzer sich nur einmal bei seiner Heimateinrichtung authentisieren muss, um ortsunabhängig auf Dienste oder lizenzierte Inhalte verschiedener Anbieter zugreifen zu können (engl. Single-Sign-on). Shibboleth basiert auf einer Erweiterung des Standards SAML.
http://de.wikipedia.org/wiki/Shibboleth_(Internet)

In der Grundkonfiguration kann Shibboleth eine Benutzerkennung genau wie die Apache (Basic) Authentication im REMOTE_USER zur Verfügung stellen.

httpd.conf:

```
LoadModule mod_shib /usr/lib/shibboleth/mod_shib_22.so
Alias /shibboleth-sp/main.css /usr/share/doc/shibboleth/main.css
Alias /shibboleth-sp/logo.jpg /usr/share/doc/shibboleth/logo.jpg
```

vhost.alephino:

```
# OPAC
<VirtualHost *:8060>
…
# Authentication
 <Directory "C:/Programme/ExLibris/AlephinoServer_50/bin">
      AuthName "Alephino OPAC – Benutzerbereich"
      AuthType shibboleth
      ShibRequireSession On
      require valid-user
  </Directory>
</VirtualHost>
```

3.4 SSO mit LDAP

Das *Lightweight Directory Access Protocol* ist zum einen Datenaustauschprotokoll, das die Abfrage und Modifikation von Informationen erlaubt. Die Kommunikation zwischen dem LDAP Verzeichnisdienst und dem jeweiligen Client erfolgt dabei über das TCP/IP Protokoll.

Die durch das LDAP zur Verfügung gestellte Struktur wird als *LDAP Verzeichnis* bezeichnet.

Um die Authentifizierung via LDAP ermöglichen müssen die nachfolgend aufgeführten Module installiert sein. Beispiel: Authentifizierung gegen den LDAP-kompatiblen Windows-Verzeichnisdienst (ActiveDirectory).

httpd.conf:

```
LoadModule ldap_module modules/mod_ldap.so
LoadModule authnz_ldap_module modules/mod_authnz_ldap.so
```

vhost.alephino:

```
<Directory "C:/Programme/ExLibris/AlephinoServer_50/bin" >

  AuthType Basic
  AuthName "Alephino OPAC – Benutzerbereich"
  AuthBasicProvider ldap
  AuthzLDAPAuthoritative off
  AuthLDAPURL ┐
ldap://myldapserver:389/ou=users,ou=Germany,dc=corp,dc=exlibrisgroup,
dc=com?sAMAccountName

  AuthLDAPBindDN "Harry Hurtig"
  AuthLDAPBindPassword "topsecret“
  AuthLDAPRemoteUserAttribute sAMAccountName
  Require valid-user

</Directory>
```

Erläuterungen:

- Da der anonyme Zugang zum Verzeichnisdienstes meist nicht möglich ist, müssen die Zugangsdaten eines repräsentativen Users zur Authentifizierung der Abfrage hinterlegt sein. Hierzu dienen die Direktiven AuthLDAPBindDN und AuthLDAPBindPassword.
- Das Attribut sAMAccountName ist bei einem AD-Verzeichnisdienst typischerweise identisch mit dem Windows-Anmeldenamen des betreffenden Nutzers. Dieses dient zunächst als Attribut-Element in der Direktive AuthLDAPURL womit bestimmt wird, daß dieses Attribut mit dem vom Browser übermittelten Login-Namen übereinstimmen muß.
- Die Direktive AuthLDAPRemoteUserAttribute sorgt dafür, daß die Umgebungsvariable REMOTE_USER, wie von Alephino erwartet, belegt wird. In unserem Falle ebenfalls mit dem Login-Namen des Nutzers. Möchte man ein anderes im Verzeichnisdienst verfügbares Attribut als REMOTE_USER nutzen, muß dieses zugleich in der (komma-separierten) Liste der Attribute in AuthLDAPURL enthalten sein.