„Echtes“ Single Sign-On mit APEX

Niels de Bruijn
MT AG
Ratingen

Schlüsselworte
Single Sign-On (SSO), Apache 2.x, Oracle Application Express 4.2.5 (APEX), Oracle REST Data Services 2.0.x (ORDS), Kerberos.

Einleitung

Man muss nur seine Webapplikation öffnen und schon ist die Anmeldung erfolgt! Ein Traum der nur selten in Unternehmen Wahrheit wird. Dabei lässt sich Single Sign-On (SSO) für interne (APEX) Webapplikationen in kürzerer Zeit und ohne Zusatzkosten einrichten. Bei einem Unternehmen mit 200 Mitarbeitern, die sich jeden Tag 15 Sekunden mit der Anmeldung an diversen APEX Applikationen beschäftigen müssen, lassen sich somit locker pro Jahr über 6 Personentage einsparen.

Zentrale Benutzerverwaltung als Basis für Single Sign-On

Der erste Schritt in Richtung wahres Single Sign-On ist die Einrichtung einer zentralen Ablage von Benutzerdaten. In fast allen Unternehmen ist zu diesem Zweck bereits ein LDAP Server wie beispielsweise das MS Active Directory vorhanden, der zentral gepflegt wird. In nur wenigen Minuten lässt sich auf dieser Basis die Authentifizierung über einen LDAP Server für eine APEX Anwendung einrichten (siehe Abbildung 1). Der Benutzer muss sich zwar noch pro APEX Anwendung mit seinem Benutzernamen und Passwort anmelden, das Passwort liegt in diesem Fall aber nicht mehr lokal in der Anwendung vor. Alleine dies spart in der Entwicklung Zeit und erhöht die IT Sicherheit. Scheidet beispielsweise ein Mitarbeiter aus, muss nur im LDAP Verzeichnis das Konto deaktiviert werden.

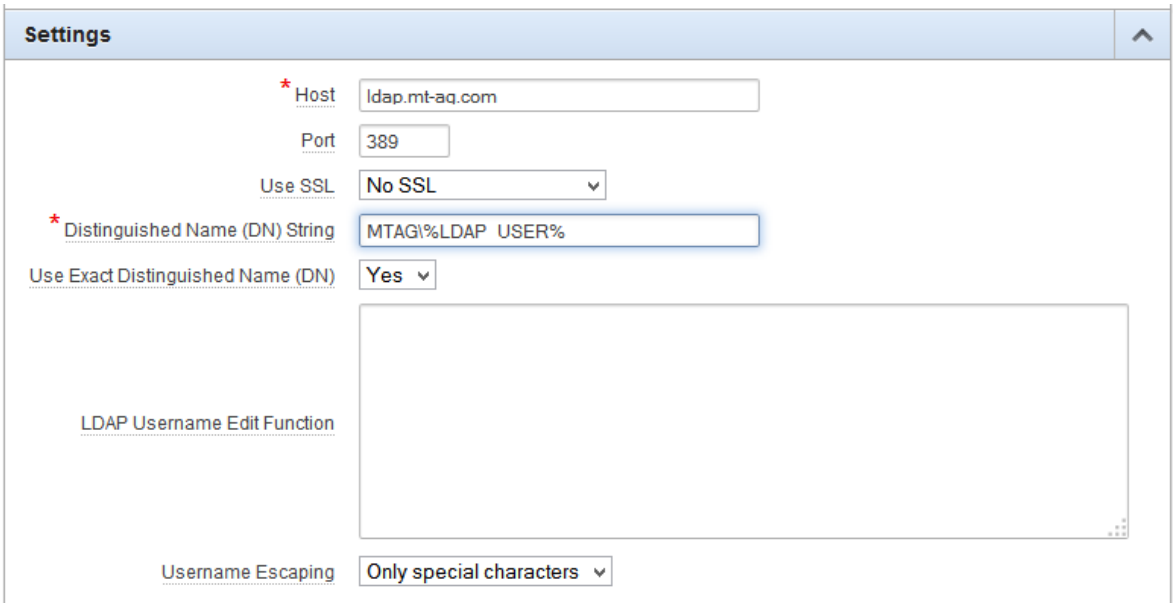


Abb. 1: LDAP Authentifizierung für eine APEX Anwendung in einer Minute einrichten.

Single Sign-On innerhalb APEX Anwendungen
Sind alle APEX Anwendungen im gleichen APEX Workspace, dann lässt sich eine Art Single Sign-On schnell einrichten. Dazu ist in jeder APEX Anwendung unter „Shared Components > Authentication Scheme“ ein beliebiger Cookie Name einzutragen. Das Ergebnis ist, dass der Endanwender sich nur einmalig bei der ersten APEX Anwendung anmelden muss. Wechselt er in der gleichen Session die Anwendung, ist kein erneutes anmelden mehr notwendig.

Abb. 2: Cookie Name in einer APEX Anwendung setzen

„Echtes“ Single Sign-On
Mit „echtem“ SSO ist in diesem Artikel gemeint, dass die Anmeldung nur einmalig auf Betriebssystemebene stattfindet und anschließend beliebige Applikationen gestartet werden können, ohne dass hierfür eine erneute Authentifizierung notwendig ist. Diese Variante implementieren Sie am besten, wenn die APEX Applikationen Workspace übergreifend vorliegen und/oder weitere (nicht APEX) Webapplikationen SSO fähig gemacht werden müssen. Damit dies funktioniert, müssen einige Voraussetzungen erfüllt sein.
Erste Voraussetzung ist das vorhanden sein eines zentralen Authentifizierungsservers. In Linux/ Unix Umgebungen wird hierfür meist Samba eingesetzt, im Microsoft Umfeld ist Active Directory die Regel.
Zweite Voraussetzung ist der Einsatz von einem Webserver wie Apache. Alle Anfragen werden vom Browser über Apache an APEX weitergeleitet. Ist der Benutzer auf Apache Ebene authentifiziert, wird durch APEX eine Session erstellt ohne den Endanwender mit einer Anmeldemaske zu konfrontieren. Durch die Vertrauensstellung zwischen der APEX Umgebung und Apache, wird die Identität angenommen die Apache über eine HTTP Header Variable weiterreicht.

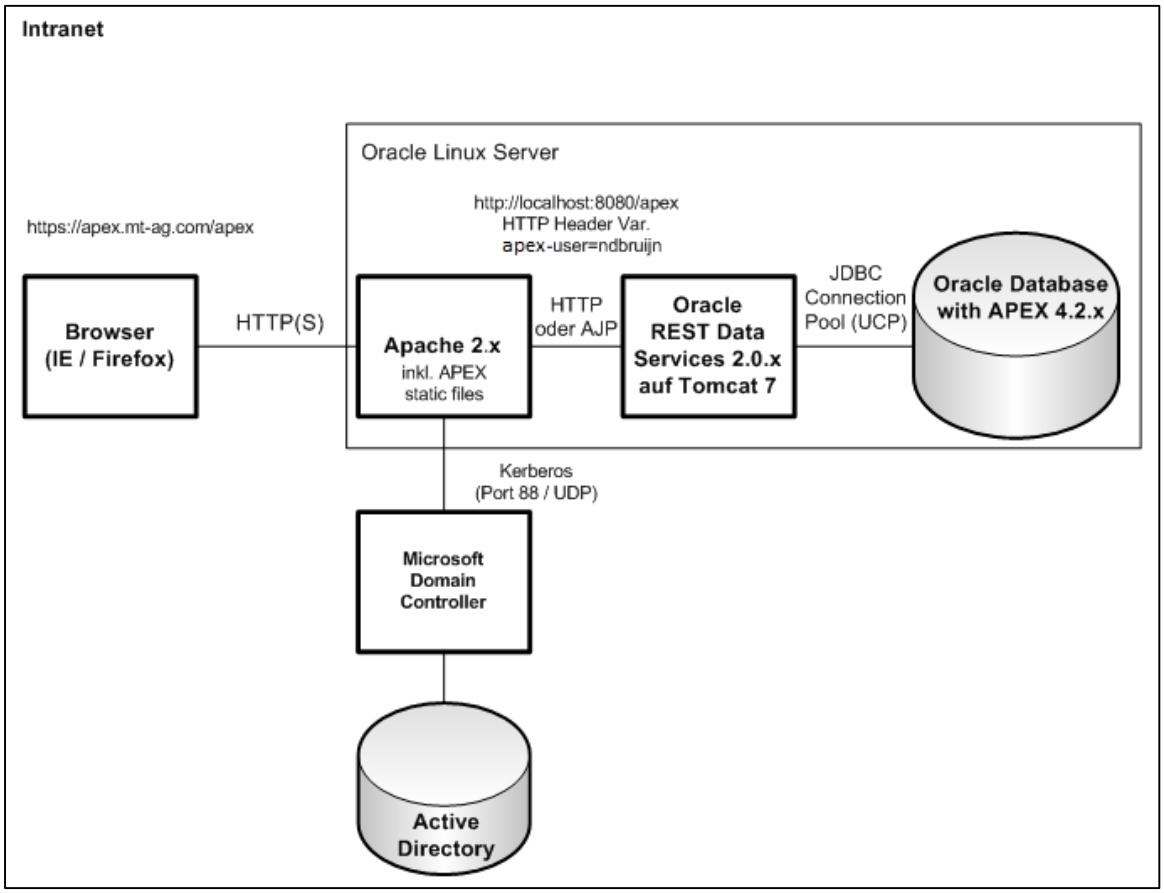


Abb. 3: Architektur für „echtes“ Single Sign-On.

Und so wird es gemacht…
Nachfolgend wird beispielhaft Schritt-für-Schritt gezeigt wie „echtes“ SSO für eine bestehende APEX Applikation erreicht wird.

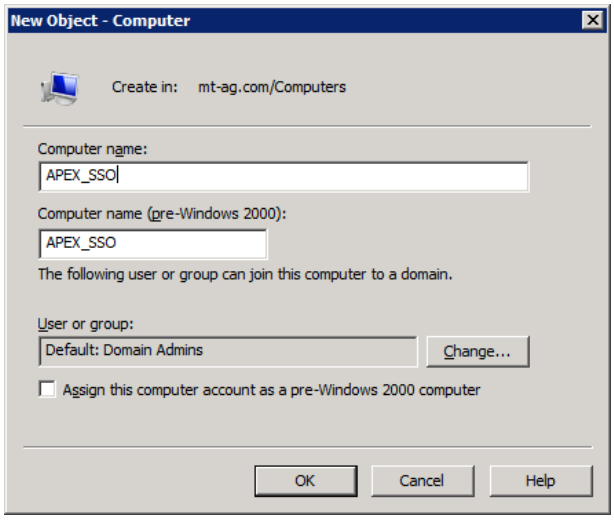
1. DNS Eintrag für Apache

Um die automatische Anmeldung über Kerberos nutzen zu können muss die Webseite über einen DNS Namen im Browser geöffnet werden. Dazu wird ein DNS Eintrag im DNS Server benötigt. In diesem Dokument gehen wir vom DNS Namen **apex.mt-ag.com** aus.

Achten Sie darauf, dass der FQDN als (zusätzlicher) Host im DNS Server eingetragen wurde und nicht als Alias. Mit dem Befehl nslookup apex.mt-ag.com können Sie dies verifizieren.
Ist der DNS Name als Alias eingetragen, erfolgt die SSO-Authentifizierung nicht über Kerberos, sondern wird mittels Basic Authentication durch die Eingabe des Benutzernamens und Passworts durchgeführt.

2. Kerberos Service Benutzer in Active Directory erstellen

Für die Kerberos Authentifizierung wird ein aktives Computer-Konto, z.B. APEX_SSO, in Active Directory benötigt.

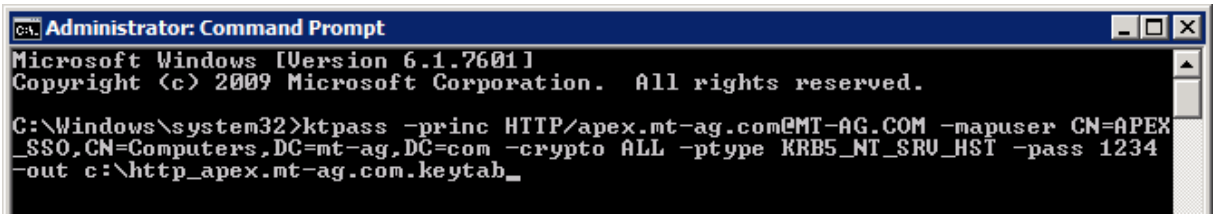


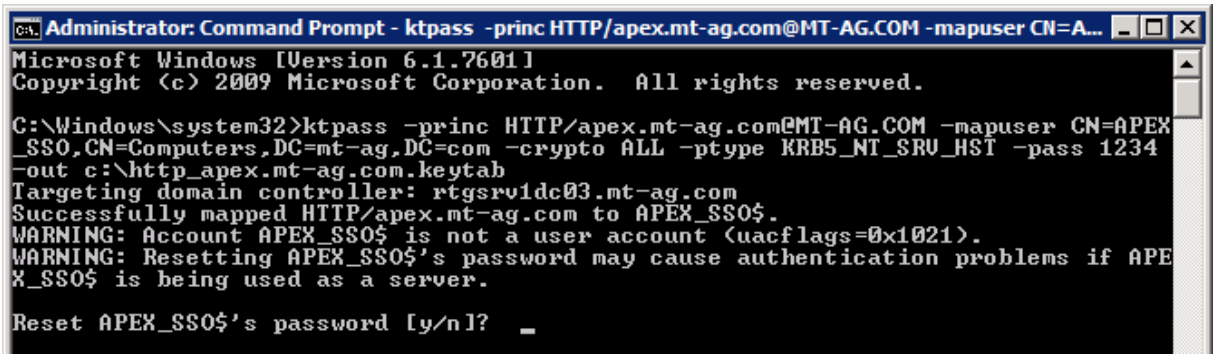
Diesem wird anschließend mit folgendem Befehl der ServicePrincipalName des HTTP Dienstes hinzugefügt und eine Keytab-Datei erstellt:

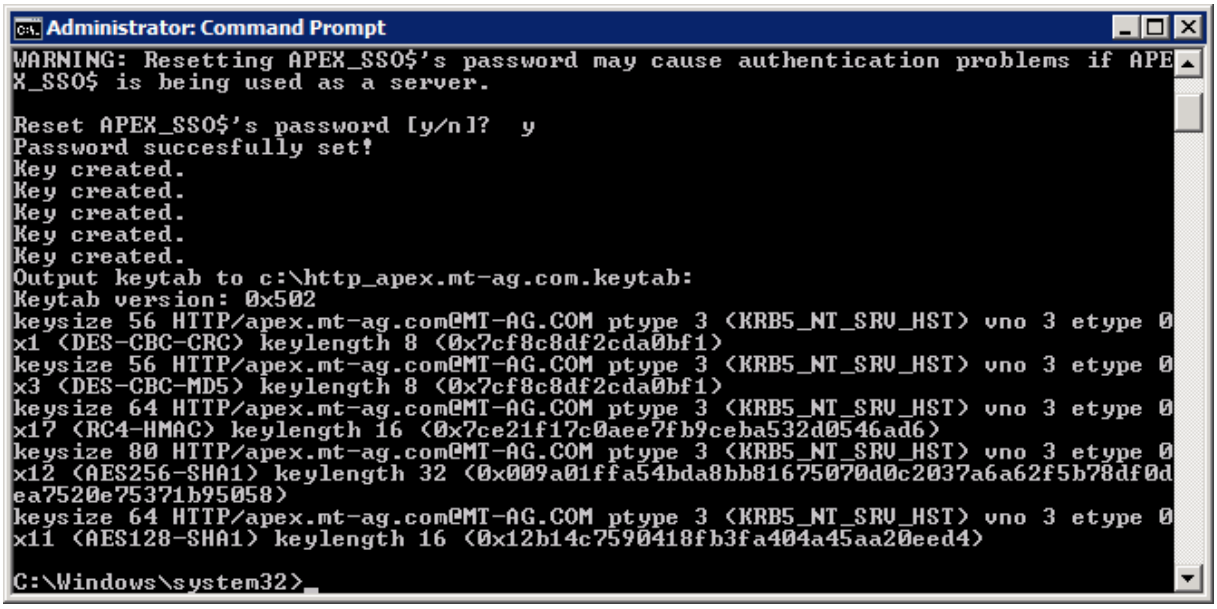
```
ktpass -princ HTTP/apex.mt-ag.com@MT-AG.COM -mapuser
"CN=APEX_SSO,CN=Computers,DC=mt-ag,DC=com" -crypto All -ptype
KRB5_NT_SRV_HST -pass <Passwort> -out c:\http_apex.mt-ag.com.keytab
```

Hinweise:

- Obwohl es auch möglich ist ein Benutzerkonto zu verwenden, wird ein Computerkonto empfohlen, weil hiermit keine Anmeldung am Client möglich ist.
- Die Domäne ist in diesem Beispiel MT-AG.COM und die Webadresse ist https://apex.mt-ag.com.
- Der Befehl ktpass ist auf einem AD Domain Controller als Administrator auszuführen.
- Das Passwort des Kontos wird neu gesetzt und in der Keytab-Datei gespeichert und kann daher beliebig gewählt werden.
- Die Angabe apex.mt-ag.com bezieht sich auf die Webadresse, die im Browser durch den Endanwender eingegeben wird.
- Obwohl die APEX Umgebung in diesem Beispiel ausschließlich über HTTPS zu erreichen sein wird, ist die Angabe HTTP hinter –princ korrekt.
- Der Name für die Keytab-Datei kann beliebig gewählt werden.
- Windows 2003 Server kennt die Angabe –crypto all nicht, daher kann stattdessen -crypto RC4-HMAC-NT angegeben werden.







Die unter c:\ erstellte Datei benötigt der Apache und wird auf einem Linux Rechner beispielsweise nach /opt/httpkeytab kopiert. Dank dieser Datei ist es Apache erlaubt zu verifizieren, ob jemand bereits an der Windows Domäne angemeldet ist.

3. Konfiguration Tomcat

Stellen Sie nach der Installation sicher dass in der Datei server.xml die folgenden Direktiven hinzugefügt sind:

```
<Connector port="8080" protocol="HTTP/1.1" connectionTimeout="20000"
maxHeaderCount="-1" maxHttpHeaderSize="65536" URIEncoding="UTF-8" … />
```

Hinweis: Wenn Sie diese Einstellung nicht vornehmen, kann es zu einer „Page not found“ Meldung im Browser kommen oder Probleme bei der Darstellung von z.B. Umlauten, wenn Sonderzeichen in einer URL verwendet werden, geben.

4. NTP installieren

Es ist zwingend erforderlich die Zeit auf allen beteiligten Servern innerhalb einer Windows Domäne synchron zu halten, da ansonsten die automatische Anmeldung nicht funktioniert. Auf einem Linux-Server wird dies über den NTP Dienst gewährleistet. Dieser Dienst wird über das integrierte Installations-Repository installiert:

```
yum install ntp
```

Anschließend wird der NTP Dämon für den automatischen Start aktiviert:

```
chkconfig ntpd on
```

Stellen Sie sicher dass die Zeit auf dem Apache System synchron mit dem Domain Controller läuft.

5. Apache mit mod_auth_kerb installieren

Für den Einsatz von Kerberos als Authentifizierungsprotokoll benötigt der Apache das Modul mod_auth_kerb. Dieses Modul wird zusammen mit Apache über das integrierte Installationsrepository installiert:

```
yum install mod_auth_kerb
```

Mit dem hinzufügen des HTTPD Dienstes in den Systemstart ist die Installation von Apache inkl. mod_auth_kerb abgeschlossen.

```
chkconfig httpd on
```

Dieser Artikel beschreibt nicht wie man Apache so konfiguriert, dass der Zugriff über HTTPS erfolgt. Hierzu gibt es bereits viele Beispiele im Internet zu finden.

6. Anpassung der Kerberos Systemkonfiguration

Die Datei /etc/krb5.conf kann wie folgt konfiguriert werden:

```
[logging]
Default        = FILE:/var/log/krb5libs.log
Kdc            = FILE:/var/log/krb5kdc.log
admin_server   = FILE:/var/log/kadmind.log

[libdefaults]
default_realm                 = MT-AG.COM
dns_lookup_realm              = false
dns_lookup_kdc                = false
ticket_lifetime               = 24h
renew_lifetime                = 7d
forwardable                   = true
default_tkt_enctypes          = rc4-hmac
default_tgs_enctypes          = rc4-hmac

[realms]
MT-AG.COM = {
kdc            = mt-ag.com
admin_server   = MT-AG.COM
default_domain = MT-AG.COM
}

[domain_realm]
.mt-ag.com     = MT-AG.COM
mt-ag.com      = MT-AG.COM
```

Hinweise:

- Hinter Kdc können statt der Domäne auch mehrere Hosts, getrennt durch ein Leerzeichen, eingetragen werden.
- Ein Neustart von Apache ist nicht notwendig, damit die Änderungen in dieser Datei wirksam werden (die Datei wird pro Authentifizierungsvorgang erneut ausgelesen).

7. Anpassung der Apache Konfiguration

Die Konfiguration am Apache vornehmen, damit die APEX URL geschützt ist:

/etc/httpd/conf/httpd.conf:

```
LoadModule auth_kerb_module   /etc/httpd/modules/mod_auth_kerb.so
LoadModule proxy_module       /etc/httpd/modules/mod_proxy.so
LoadModule proxy_http_module  /etc/httpd/modules/mod_proxy_http.so
LoadModule headers_module     /etc/httpd/modules/mod_headers.so

# Schuetzt alle APEX Anfragen
<Location /apex>
  AuthType                    Kerberos
```

```
  AuthName                        "Kerberos Login"
  KrbAuthRealms                   MT-AG.COM
  KrbServiceName                  HTTP/apex.mt-ag.com@MT-AG.COM
  Krb5KeyTab                      /opt/httpkeytab/http_apex.mt-ag.com.keytab
  require valid-user

  # Wenn man eine Proxy-Direktive verwendet, dann wird REMOTE_USER nicht
weitergeleitet, daher wird explizit APEX_USER als Variable gesetzt.
  RewriteEngine On

  RewriteCond %{LA-U:REMOTE_USER} (.+)$
  # Wenn Sie die Windows Domaene nicht uebernehmen moechten, dann
stattdessen diese Zeile aktivieren
  # RewriteCond %{REMOTE_USER} (.+)@.*

  RewriteRule . - [E=RU:%1]
  RequestHeader set APEX_USER %{RU}e

  # Weiterleiten von Anfragen an Oracle REST Data Services
  # Die Weiterleitung kann entweder mit HTTP(S) oder mittels AJP erfolgen.
  # In diesem Fall wird das ungesicherte Protokoll HTTP verwendet, da alles
  # auf einem Server laeuft.
  ProxyPass        /apex  http://localhost:8080/apex
  ProxyPassReverse /apex  http://localhost:8080/apex
</Location>

# Statische Dateien von APEX
Alias /i/ "/var/www/html/images/"
```

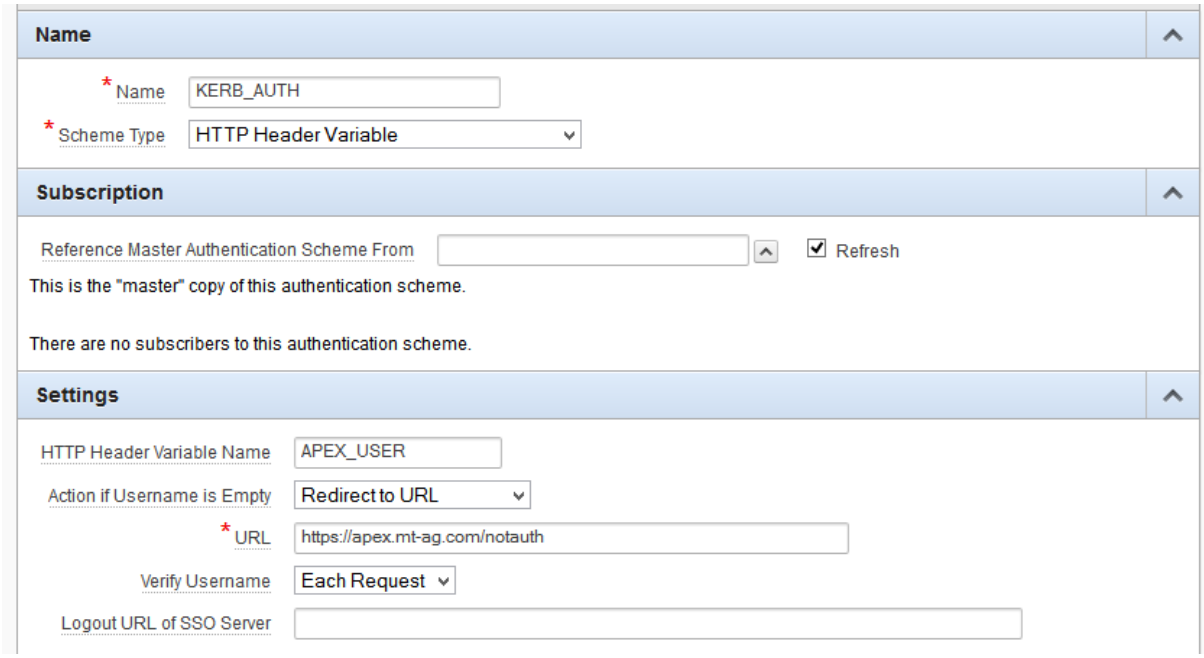
Nach dieser Änderung ist ein Neustart von Apache vorzunehmen.

Hinweis:

- Im Verzeichnis /var/www/html/images sind die statischen Dateien von APEX zu hinterlegen. Diese befinden sich in der APEX Software unter /images.

8. Authentifizierung in der APEX Anwendung

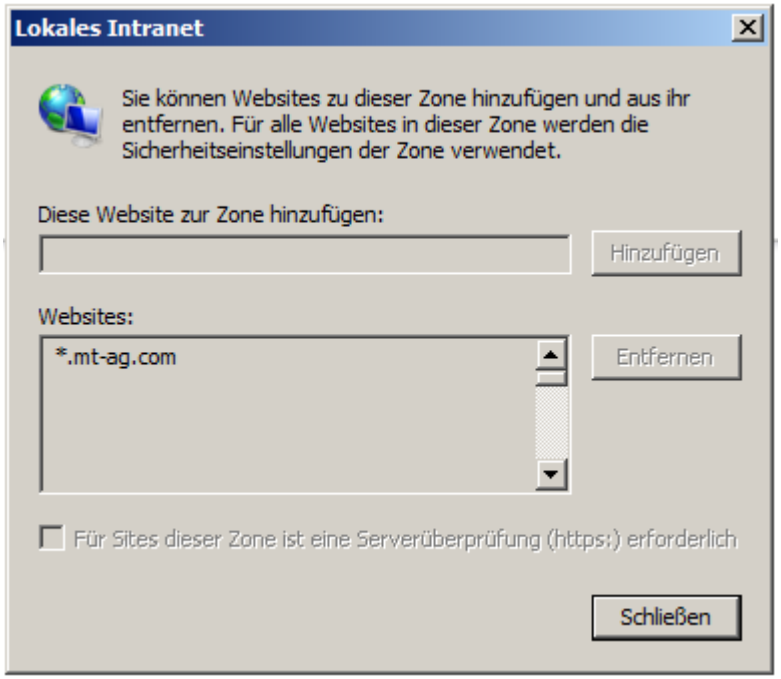
Die APEX Anwendung sollte keine Anmeldeseite an den Browser zurückgeben, sondern die Identität annehmen, welche in der HTTP Header Variable „APEX_USER“ über Apache an APEX weitergegeben wird. Dafür muss ein neues Authentifizierungsschema für die APEX Anwendung erstellt werden:



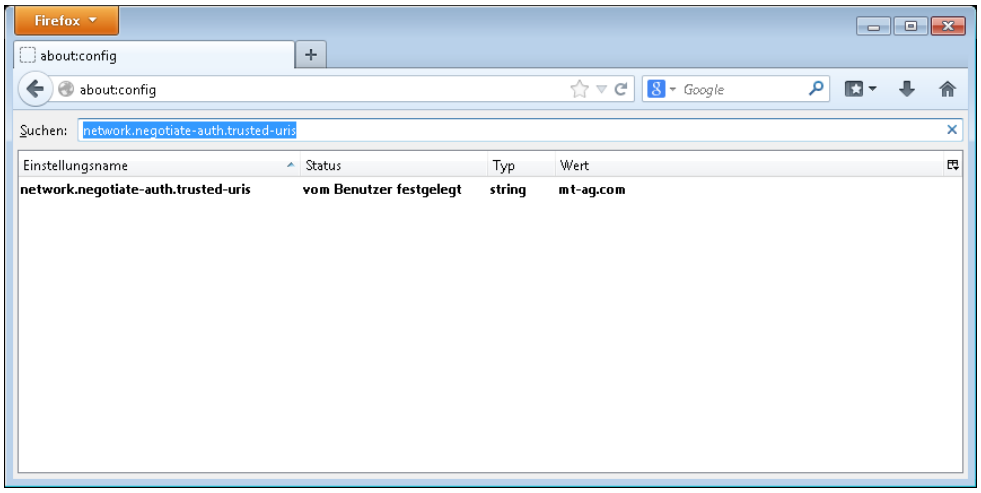
Wenn APEX_USER leer ist, dann wird der Endanwender auf eine statische HTML Seite (index.html) auf Apache weitergeleitet. Diese Seite zeigt dem Endanwender beispielsweise den Text „Sie sind nicht an der Domäne angemeldet.“ an.

9. Konfiguration Client PC

Wenn sich die Webseite im Internet Explorer nicht in der Zone „lokales Intranet“ befindet oder der Benutzer nicht an der Windows Domäne angemeldet ist, wird der Benutzer in einer Dialogbox aufgefordert sich mit dem Benutzernamen und Passwort an der Windows Domäne anzumelden. Erst wenn die Webseite in der Zone "lokales Intranet" aufgenommen wurde und der Benutzer an der Windows Domäne angemeldet ist, erfolgt die Anmeldung über Kerberos automatisch.



Im Firefox kann diese Einstellung vorgenommen werden, indem als URL about:config aufgerufen wird. Die Domäne mt-ag.com ist im Atrribut network.negotiate-auth.trusted-uris einzutragen.



Wenn alles richtig konfiguriert wurde, kann die APEX Anwendung mit einem Browser wie IE 10 oder Firefox 24 aufgerufen werden und die Anmeldung bei APEX erfolgt automatisch.

Wichtig: Stellen Sie sicher, dass die Anfragen an den Hostnamen, hier apex.mt-ag.com, nicht an den Proxy-Server weitergeleitet werden, ansonsten kann das Kerberos Ticket „verloren“ gehen. Falls Sie

einen Proxy-Server im Browser konfiguriert haben, sollte daher der Hostname apex.mt-ag.com als Ausnahme hinterlegt werden, ansonsten erhalten Sie die Fehlermeldung „page not found“.

Kontaktadresse:
Niels de Bruijn
Fachbereichsleiter APEX

MT AG
Balcke-Dürr-Allee 9
40882 Ratingen

Telefon:	+49 (0) 2102 309 61 341
Fax:	+49 (0) 2102 309 61 101
E-Mail	niels.de.bruijn@mt-ag.com
Internet:	http://www.mt-ag.com / https://apex.mt-ag.com