

Nachnutzung des Windows - Login in einer SAML-basierten Föderation mittels Shibboleth Kerberos Login Handler

**56. DFN-Betriebstagung, Forum AAI
Berlin, 13. März 2012**

**Peter Gietz, Martin Haase,
DAASI International GmbH**

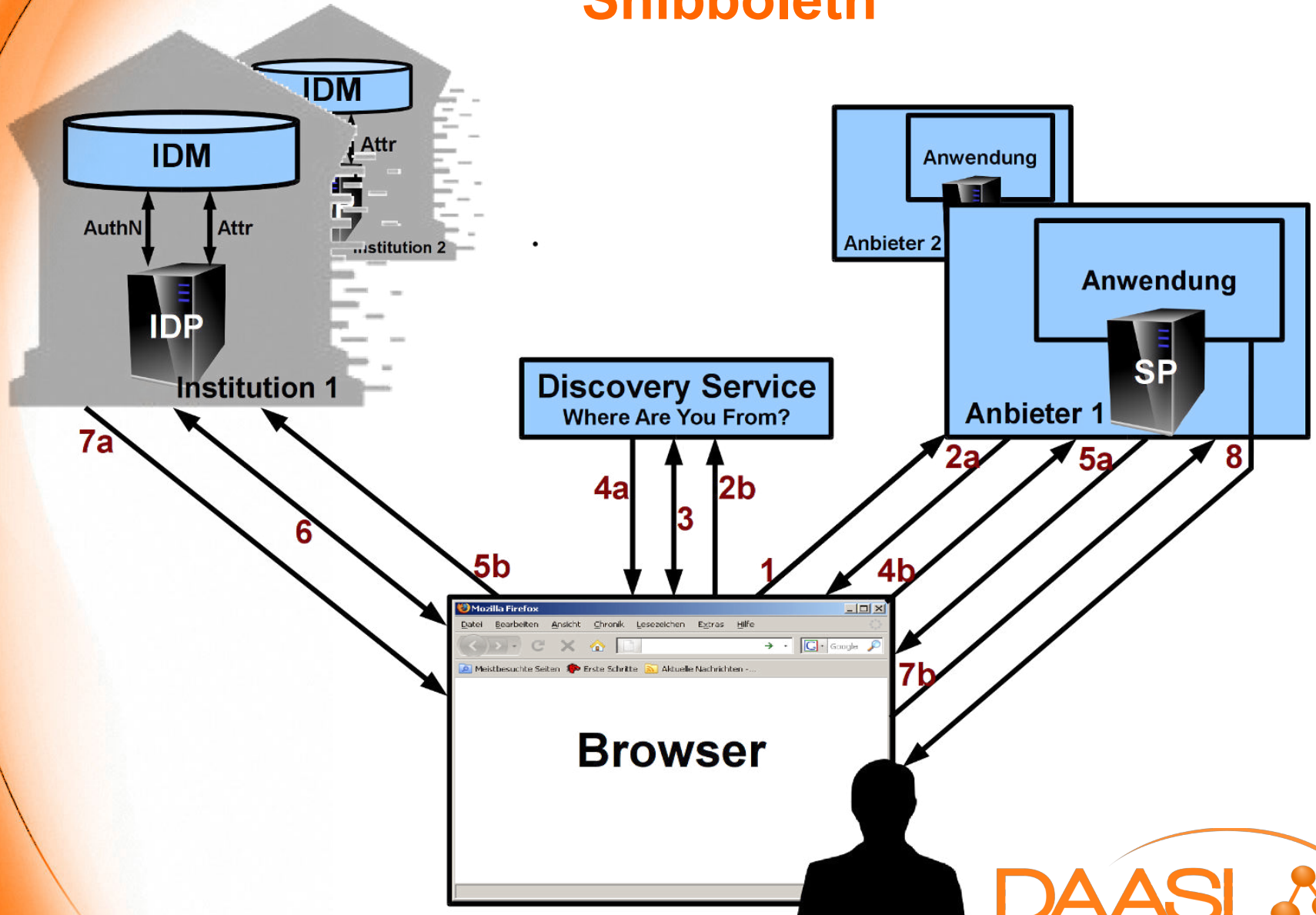
**Mark Pröhl,
science + computing ag**



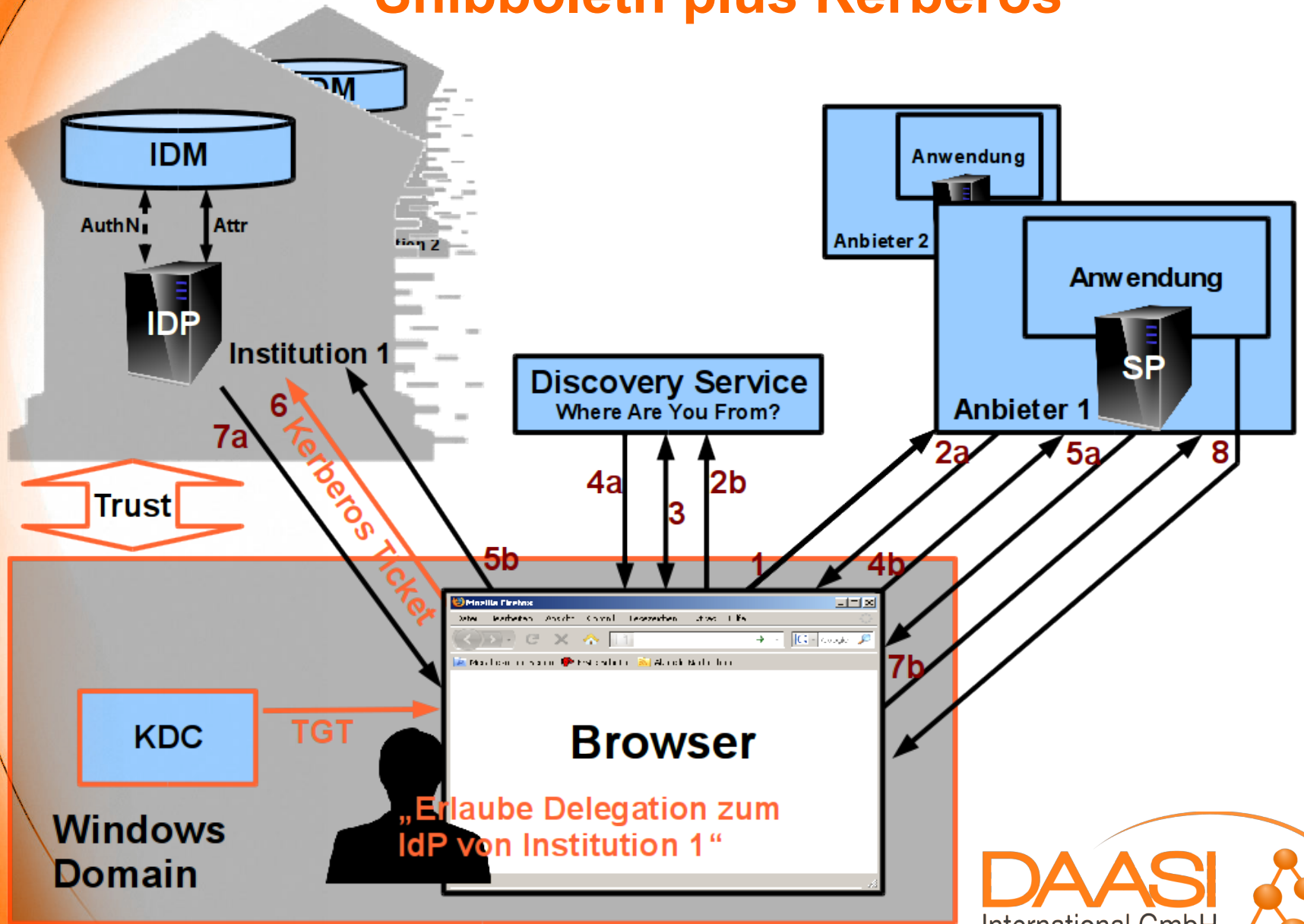
Agenda

- **Shibboleth ohne und mit Kerberos**
- **Voraussetzungen des Kerberos Login Handlers von SWITCH**
- **Vor- und Nachteile**
- **Einsatz am Beispiel einer Behörde**

Shibboleth



Shibboleth plus Kerberos



Ablauf Login

- 1) Benutzer-Login am Windows-Arbeitsplatz an DOMAENE → Windows-Client bekommt ein Ticket Granting Ticket vom Key Distribution Center der DOMAENE
- 2) Benutzer öffnet Web Browser, Browser nutzt TGT, um Service Ticket für IdP anzufordern
- 3) Login am IdP wird durch Besuch einer SP-geschützten Ressource ausgelöst
- 4) Browser präsentiert Service Ticket am IdP
- 5) IdP akzeptiert Service Ticket und extrahiert Kerberos Principal, anschließend...
 - i. LDAP-Lookup nach Attributen des Principals
 - ii. Zusammenstellung der SAML-Assertion, Versand an SP
 - iii. SP empfängt Assertion und liefert Ressource aus

Voraussetzungen

- **IdP-Extension separat installiert:**
<https://wiki.shibboleth.net/confluence/display/SHIB2/Kerberos+Login+Handler>
- **Windows Domain Controller agiert als KDC**
- **Im KDC ist ein Service Principal für den IdP angelegt:**
HTTP/idp.example.org@DOMAE.NE
- **Anpassungen notwendig an**
 - **handler.xml – Konfiguration des Login Handlers, der zugehörigen Realms und jeweiligen Service Principals**
 - **Login-Seite – als Teil der Username/Passwort-Form oder „Kerberos only“**
 - **ggf. Attribut-Resolver – Attributname für Principalname**
 - **ggf. web.xml – Browser-Test-Servlet**
- **Systemweite /etc/krb5.conf**

Service-Principal anlegen

- Auf dem Domain Controller / KDC
- Verwendung des Windows-Befehls **ktpass**
- ktpass erzeugt
 - Principal HTTP/idp.example.org@DOMAE.NE
 - Keytab-Datei (wird anstelle eines Passworts auf dem IdP benötigt)
- Kopieren der Keytab-Datei auf den IdP

Handler.xml

```
<ph:LoginHandler xsi:type="krb:KERBEROS"
    kerberosCfg="/etc/krb5.conf">

    <krb:Realm domain="DOMAE.NE">
        <krb:principal>
            HTTP/idp.example.org@DOMAENE
        </krb:principal>
        <krb:keytab>
            /opt/shibboleth-idp/conf/krb5.keytab
        </krb:keytab>
    </krb:Realm>

    <krb:Realm domain="DOMAE.NEB">
        ...
    </krb:Realm>

</ph:LoginHandler>
```


/etc/krb5.conf

```
[libdefaults]
  default_realm = DOMAENE
```

```
[realms]
```

```
  DOMAE.NE = {
    kdc = 192.168.123.20
    kpasswd_server = 192.168.123.20
  }
```

```
### viele Fomaenen moeglich!!!
  DOMAE.NEB = ....
```

Login-Maske, Kerberos optional

erwahl

WSVDir Login - Mozilla Firefox

Datei Bearbeiten Ansicht Chronik Lesezeichen Extras Hilfe

WSVDir Login

vabaw-test.intern https://shibidp.vabaw-test.intern/idp/AuthnEngine

BAW

Single Sign On Login

Wenn Sie sich hier einloggen, haben Sie für die Dauer Ihrer Web-Browser-Sitzung auf alle Fachanwendungen der BAW Zugriff, die an der Single-Sign-On-Infrastruktur teilnehmen.

Dieses Login ist für die Fachanwendung im rechten Kasten.

Nutzername:

Passwort:

Login

Windows-Login nutzen (Kerberos) [Schließen](#)

Windows-Login

[Browser-Konfiguration testern](#)

Diese Seite zukünftig nicht mehr anzeigen

shibsp1.vabaw-test.intern

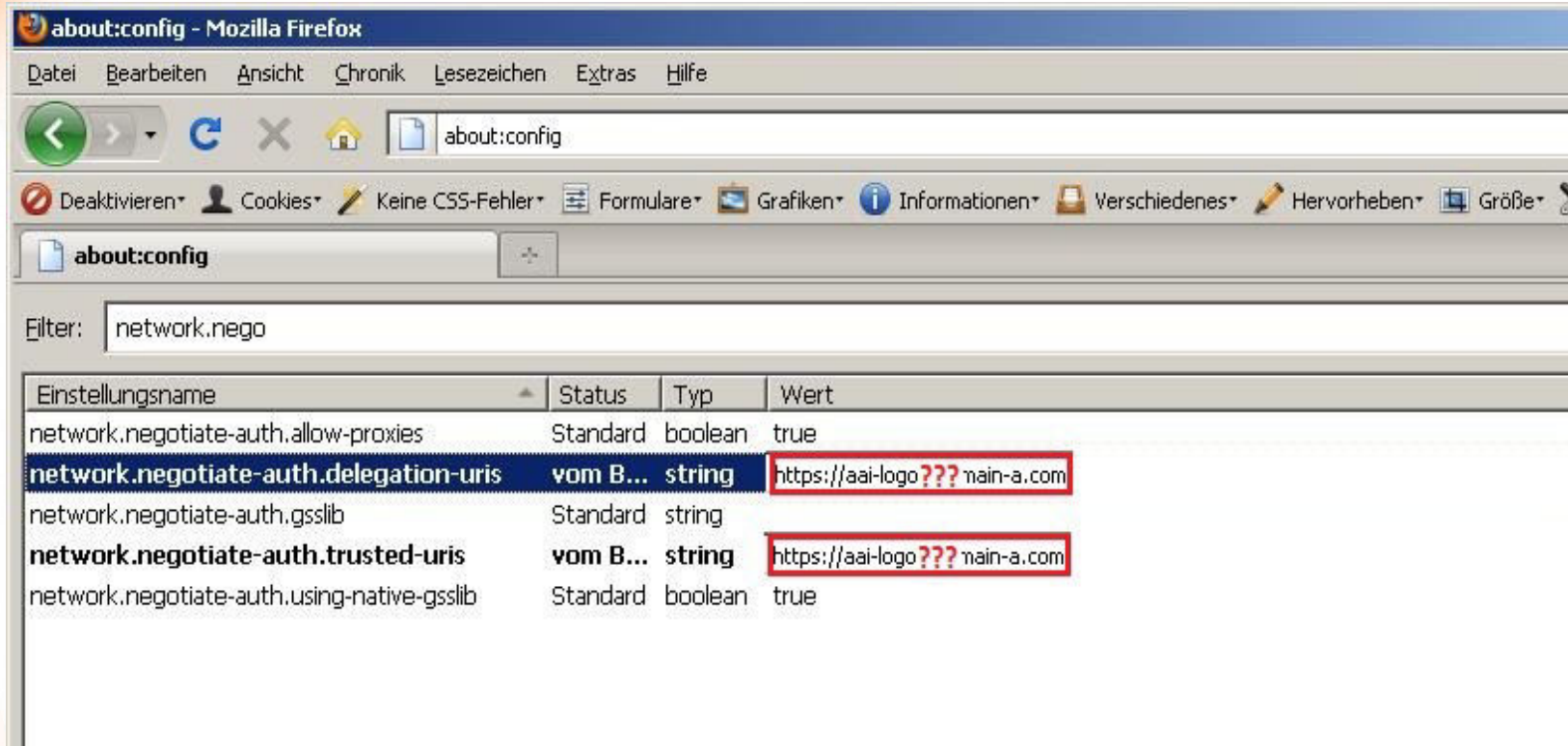
Sie möchten sich für shibsp1.vabaw-test.intern einloggen.

apier

Unterschiede zu klassischem WebSSO

- **Single Sign On unter Nachnutzung des Windows-Login**
 - **Windows-integrierte Authentifizierung**
- **Nur für Windows-User innerhalb einer AD-Domäne**
 - **→ Kerberos sollte optional sein**
- **Klartext-Passwort muss nicht zum IdP übertragen werden**
 - **stattdessen kurzlebiges Service Ticket**
- **Logout nur durch Abmelden am Betriebssystem möglich**
 - **→ strenge Regeln für Zugriff auf Clientrechner notwendig**
- **Ein IdP kann für verschiedene Domains konfiguriert werden**
 - **keine Trust-Beziehung zwischen den Domänen notwendig**
- **IdP-spezifische Konfiguration des Browsers erforderlich**
 - **Der URI als vertrauenswürdig konfigurieren**

Beispiel Firefox



The screenshot shows the Mozilla Firefox browser window with the address bar set to `about:config`. The filter `network.nego` is applied, displaying a list of configuration settings. The following table represents the visible data:

Einstellungsname	Status	Typ	Wert
<code>network.negotiate-auth.allow-proxies</code>	Standard	boolean	true
<code>network.negotiate-auth.delegation-uris</code>	vom B...	string	<code>https://aai-logo??? main-a.com</code>
<code>network.negotiate-auth.gsslib</code>	Standard	string	
<code>network.negotiate-auth.trusted-uris</code>	vom B...	string	<code>https://aai-logo??? main-a.com</code>
<code>network.negotiate-auth.using-native-gsslib</code>	Standard	boolean	true

WAYF-Unterstützung

- **SWITCH WAYF unterstützt Kerberos**
- **Voraussetzungen:**
 - **WAYF URL muss mit mod_auth_kerb geschützt sein**
 - **Realms für jeden IdP müssen konfiguriert sein**
 - **Im Browser muss sowohl Heimat-IdP als auch WAYF-Server als vertrauenswürdig konfiguriert werden**
 - **Cross-Realm Trust zwischen den KDCs der IdPs und dem KDC des WAYF (XXX???)**
- **WAYF erkennt am Realm des Kerberos-Principals aus dem Service Ticket den zugehörigen IdP**
 - **keine Benutzerinteraktion notwendig**

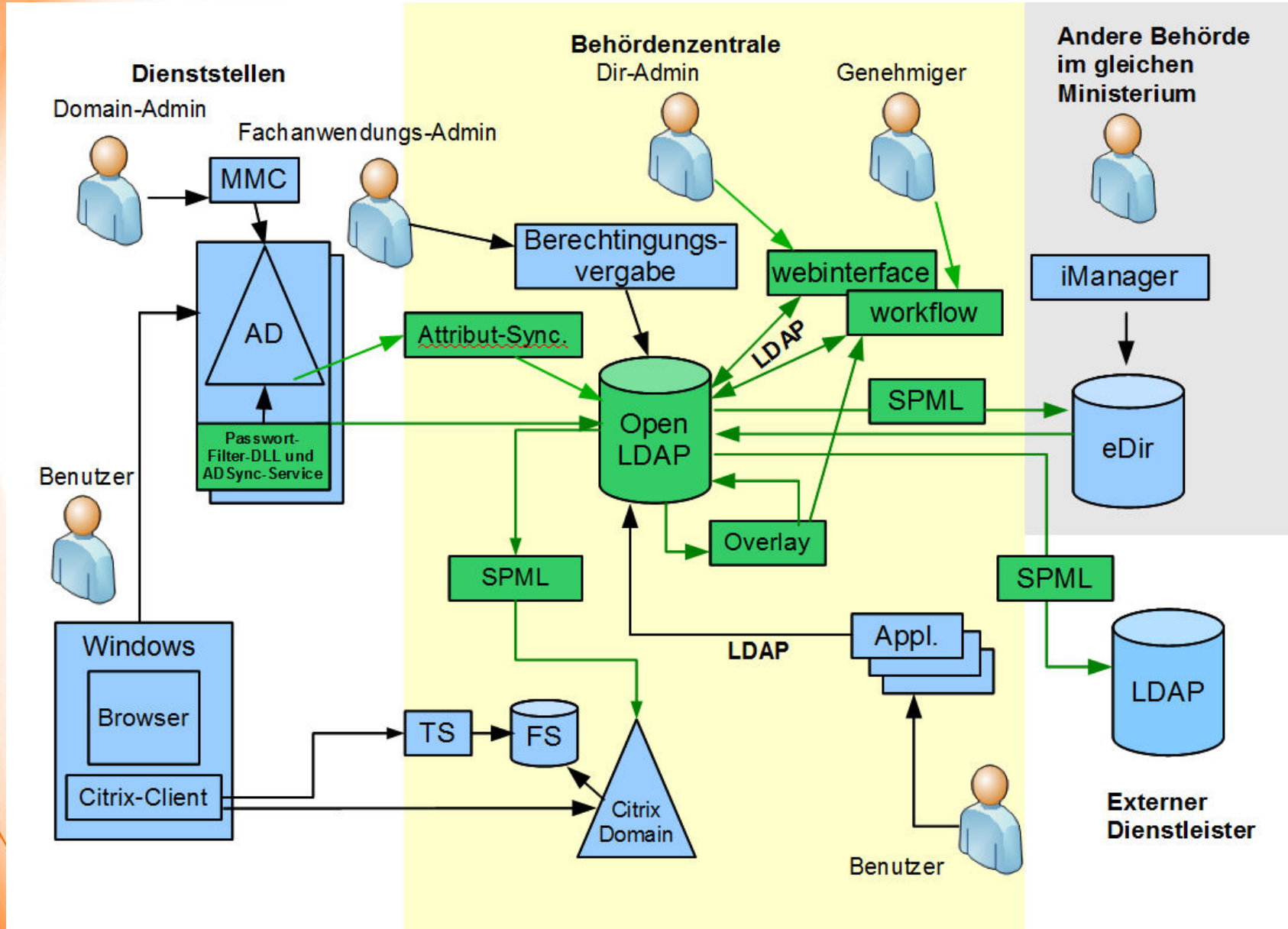
Einsatz in einem Beispielprojekt im Behördenkontext

**Auftraggeber ist eine größere Bundesbehörde mit
im gesamten Bundesgebiet verteilten
Dienststellen**

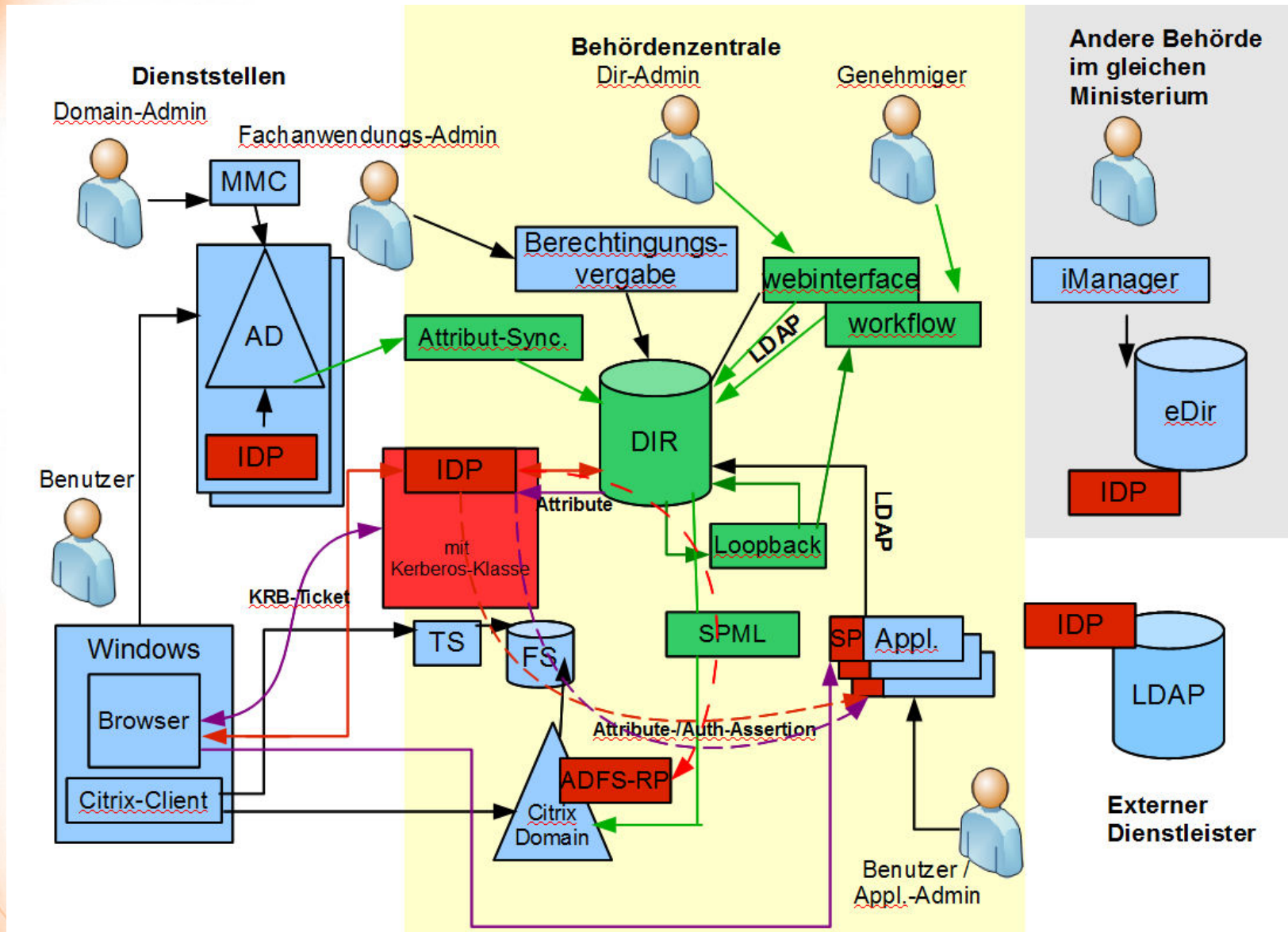
Anforderungen

- Eine existierende auf proprietäre Software basierende Identity-Management-Lösung sollte mit Open-Source-Software nachgebaut werden
 - komplexe Synchronisierungsmechanismen
 - komplexe Berechtigungsattributvergabe
- Zusätzlich sollte WebSSO mithilfe von Shibboleth realisiert werden
 - Ein IdP, der an den zentralen Verzeichnisdienst angeschlossen wird
 - Mehrere SPs, die verschiedene zentrale Fachanwendungen schützen
- Schließlich sollte durch Integration der Windows-Kerberos-Authentifizierung die Synchronisierung von Passwörtern verhindert werden

Migration der jetzigen Lösung



Alles wäre noch einfacher, wenn alle in die Föderation kommen



Vielen Dank für Ihre Aufmerksamkeit!

Fragen ?

➤ **Kontakt und weitere Informationen:**

- **DAASI International GmbH**
Europaplatz 3
D-72072 Tübingen

- **Web: <http://www.daasi.de>**
Mail: info@daasi.de

- **Bei späteren Fragen zum Vortrag:**
Mail: peter.gietz@daasi.de

