Federated Identity Management in der öffentlichen Verwaltung

PITS 2012

Berlin, 25.-26.09.2012

Peter Gietz, Geschäftsführer,

DAASI International GmbH

peter.gietz@daasi.de

DAASI International GmbH

Agenda

1) Begriffe Identity Management und Federated Identity Management
2) Motivation für Federated Identity Management in der öffentlichen Verwaltung
3) Der Standard SAML
4) Open Source Implementierung Shibboleth
5) Beispielprojekt in der öffentlichen Verwaltung

DAASI International GmbH

1) Begriffe
Identity Management
und
Federated Identity Management

Identity Management

- **Definition von Spencer C. Lee:**
  - ***Identity Management bezieht sich auf den Prozess der Implementierung neuer Technologien zum Verwalten von Informationen über die Identität von Nutzern und zur Kontrolle des Zugriffs auf Firmenressourcen.***
  - ***Das Ziel von Identity Management ist es Produktivität und Sicherheit zu erhöhen und gleichzeitig Kosten der Verwaltung von Benutzern, ihrer Identitäten, Attribute und Berechtigungsnachweise zu senken***
- **In Bezug auf Föderationen:**
  - **Identity Management ist Voraussetzung für Federated Identity Management da Zusagen über Aktualität und Richtigkeit der Identitätsdaten gemacht werden**

DAASI International GmbH

Federated Identity Management

- *FIdM-Definition von Peter Valkenburg, et.al (SURF):*
  - *Kollektiver Begriff für alle Prozesse, Standards und Technologien, die den Austausch von Identitäts-informationen über organisatorische Grenzen hinweg unterstützen*
- **FidM setzt eine Föderation voraus**
  - **Ein Vertrauensbund, der es ermöglicht, verteilte Ressourcen gemeinsam zu nutzen**
  - **Vertrauen wird durch Verträge und Einhaltung von entsprechenden Sicherheitspolicies gewährleistet**

DAASI International GmbH

Vorteile von FIdM

- Identitätsdaten eines Benutzers müssen nur an einer Stelle gespeichert werden
  - Name, Kontaktdaten, Passwort, etc.
  - im IdP der „Heimatorganisation“
- Personenbezogene Daten
  - werden nur über gesicherte Verbindungen an Mitglieder des Vertrauensbunds geschickt
  - müssen aber gar nicht übertragen werden, da es oft nur auf anonyme Autorisierungsattribute ankommt
- Die Föderationstechnologien ermöglichen Single Sign-On
- Föderation ähnelt einer PKI (Public Key Infrastructure), ist aber wesentlich einfacher zu implementieren:
  - nur Serverzertifikate notwendig
  - Passwort anstelle der Benutzerzertifikate

DAASI International GmbH

Grundbausteine einer Föderation

- Eine Föderation besteht aus drei Bausteinen:
  - Föderationsverwaltung
    - zentraler Vertragspartner für Föderationsmitglieder
    - verwaltet Zugangsdaten zu den einzelenen Bausteinen (“Metadaten”)
    - betreibt zentrale Infrastrukturkomponenten
  - Identity Provider (IdP)
    - Benutzerverwaltung der Heimatorganisation
    - verantwortlich für Authentifizierung und Attribute
  - Service Provider (SP)
    - verantwortlich für Ressourcen
    - entscheidet aufgrund von Aussagen des IdP

DAASI International GmbH

2) Motivation für Federated Identity Management in der öffentlichen Verwaltung

Motivation im Verwaltungsumfeld

- Erste Föderation im Verwaltungsumfeld war die Föderation der Hochschulen (DFN-AAI)
  - Studenten werden immer mobiler, wechseln die Hochschule öfters, bzw. belegen Kurse an anderen Hochschulen (E-Learning)
  - Forschung funktioniert immer vernetzter
    - eScience und Grid-Computing
    - Forscher aus verschiedenen Hochschulen benötigen Zugriff auf im Netz verteilte Ressourcen („Virtuelle Organisationen“)
  - Verlagslizenzen erfordern Föderationen
    - z.B. für Datenbanken, die von Hochschulbibliotheken online gestellt werden
    - Verlage wollen Autorisierungsattribute (anstelle von IP-Ranges)
    - Lizenzen können auch an Hochschulverbünde erteilt werden

DAASI International GmbH

Motivation im Behördenkontext

- Viele Behörden sind dezentral organisiert, wollen aber zentrale Dienste anbieten, z.B.:
  - Bundesbehörden mit vielen Dienststellen im gesamten Bundesgebiet
  - Kultusministerien, die für alle Schulen Dienste anbieten
  - Alle Behörden eines Ministeriums
  - Behörden verschiedener Ministerien, die auf gleiche Anwendungen zugreifen
- In all diesen Fällen können die Benutzerdaten in der Heimatbehörde bzw. Heimatorganisation Schule bleiben

DAASI International GmbH

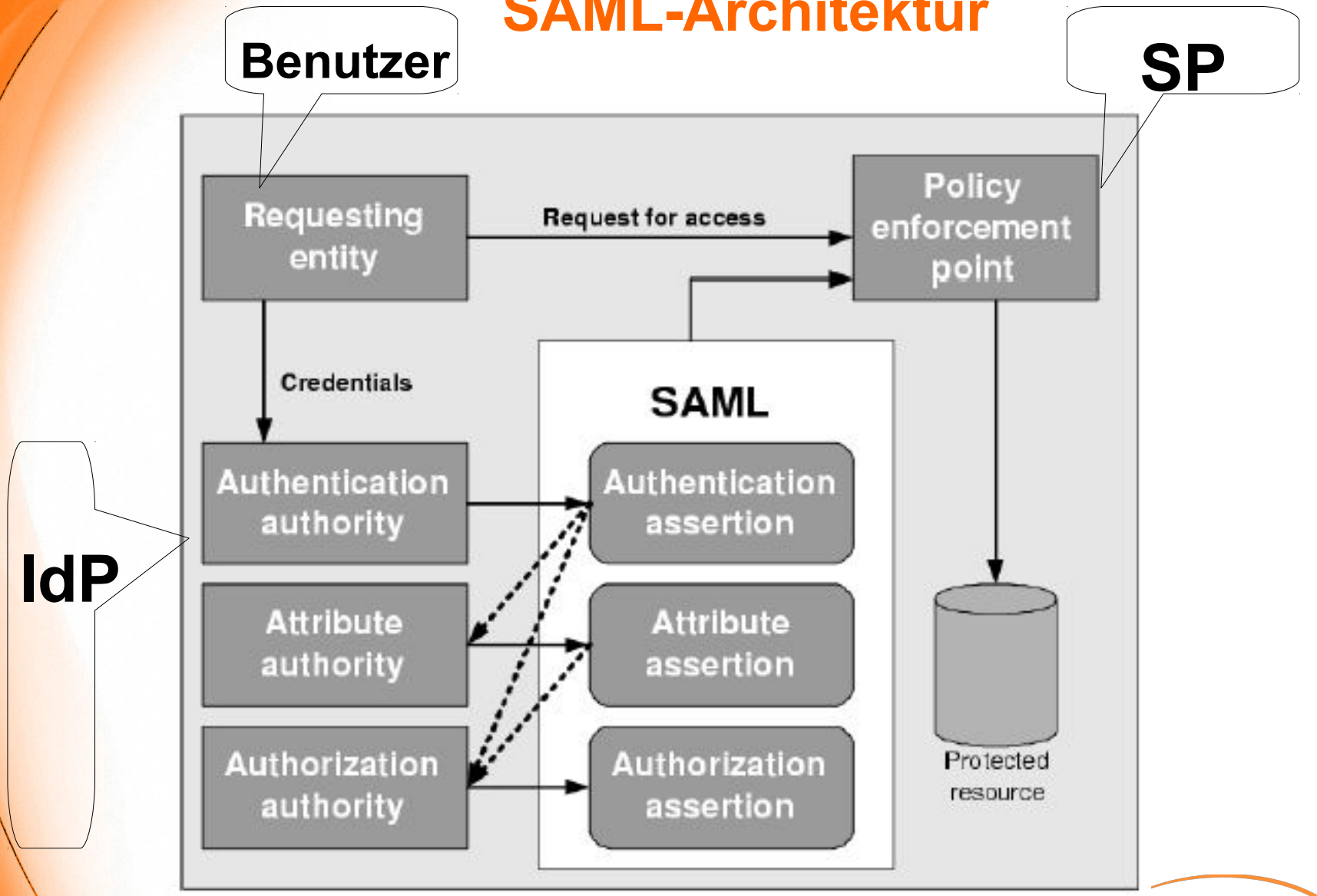
3) Der Standard SAML

SAML

- Security Assertion Markup Language
  - OASIS-Standard
- XML-Dokumente enthalten Zusicherungen (Assertions), die ein IdP über Benutzer macht:
  - Authentication Statements, Zusicherung, dass sich ein Benutzer authentifiziert hat
  - Authorization Statement, Zusicherung über bestimmte Zugriffsrechte
  - Attribute Statement, Zusicherung über bestimmte Eigenschaften eines Benutzers, die in Form von Attributen weitergegeben werden und den SP bei der Entscheidung über Zugriff unterstützen
- Profile spezifizieren welche Assertions wie zwischen IdP und SP ausgetauscht werden

DAASI International GmbH

SAML-Architektur



Nach: RUBENKING, NEIL J.: Securing web services

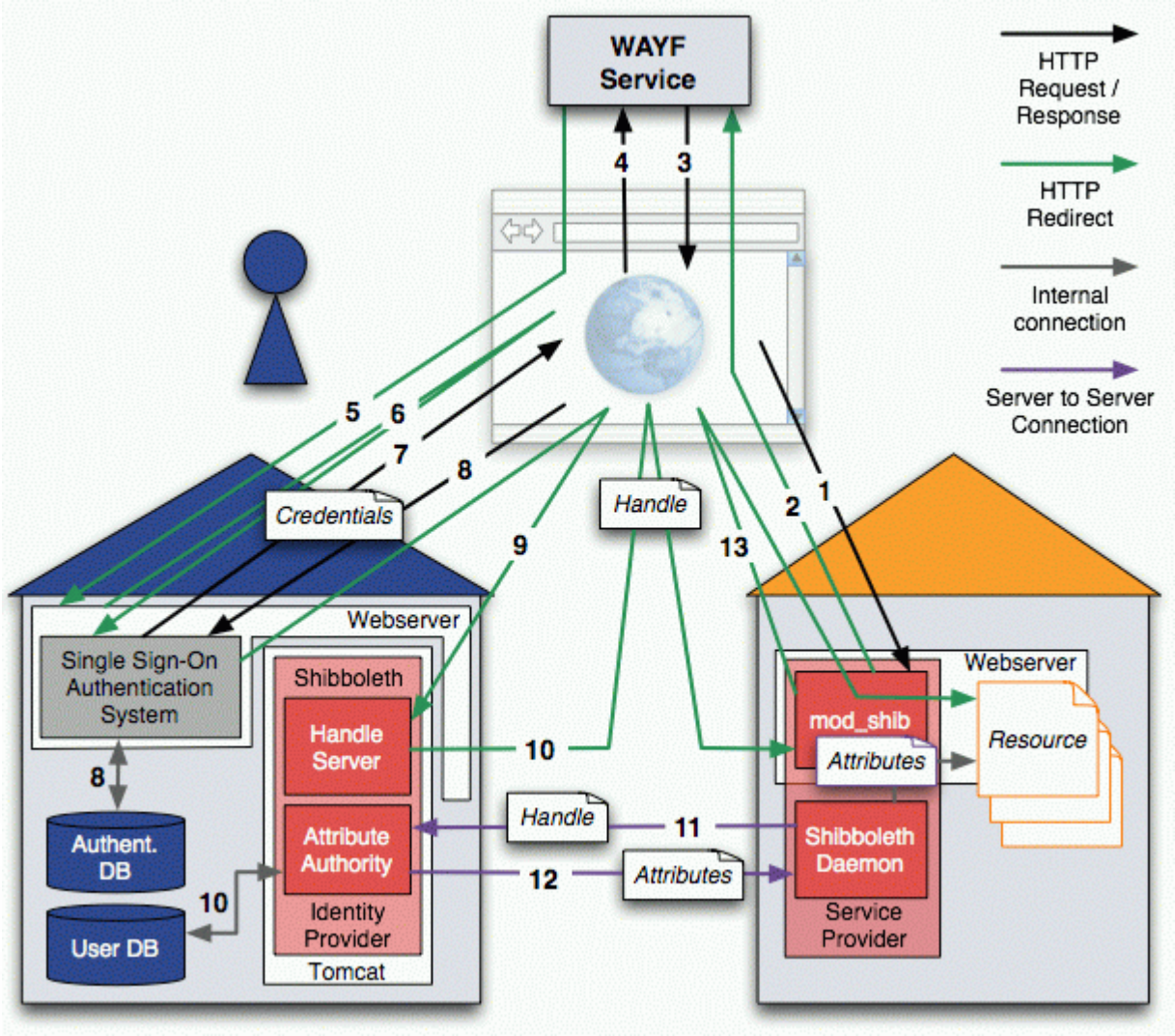
4) Open Source Implementierung Shibboleth

Shibboleth

- Open Source Software vom US-amerikanischen Internet2-Projekt
- Implementiert das SAML-Profil WebSSO
  - nach einmaliger Authentifizierung hat der Nutzer für eine bestimmte Zeit föderationsweit Zugriff auf verschiedene Webanwendungen
- Viele Anwendungen sind bereits „shibboletisiert“
- Das Projekt wird aktiv weiterentwickelt im Rahmen eines internationalen Konsortiums
- Es gibt, z.B. durch DAASI, professionellen kommerziellen Support beim Betrieb aber auch bei kundenspezifischen Weiterentwicklungen

DAASI International GmbH

Shibboleth Architektur



© Switch-AAI

5) Beispielprojekt in der öffentlichen Verwaltung

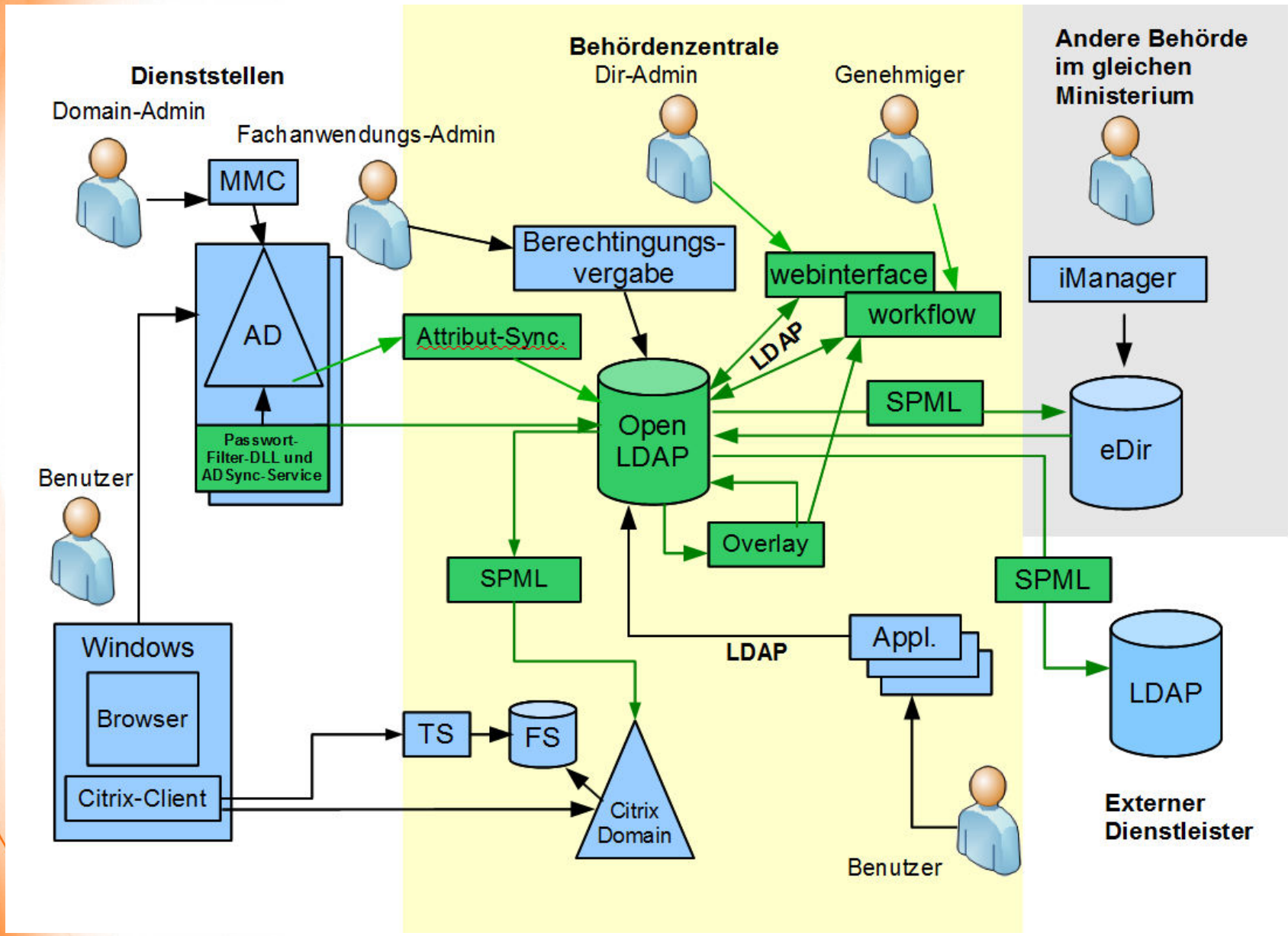
Auftraggeber ist eine größere Bundesbehörde mit im gesamten Bundesgebiet verteilten Dienststellen

Anforderungen

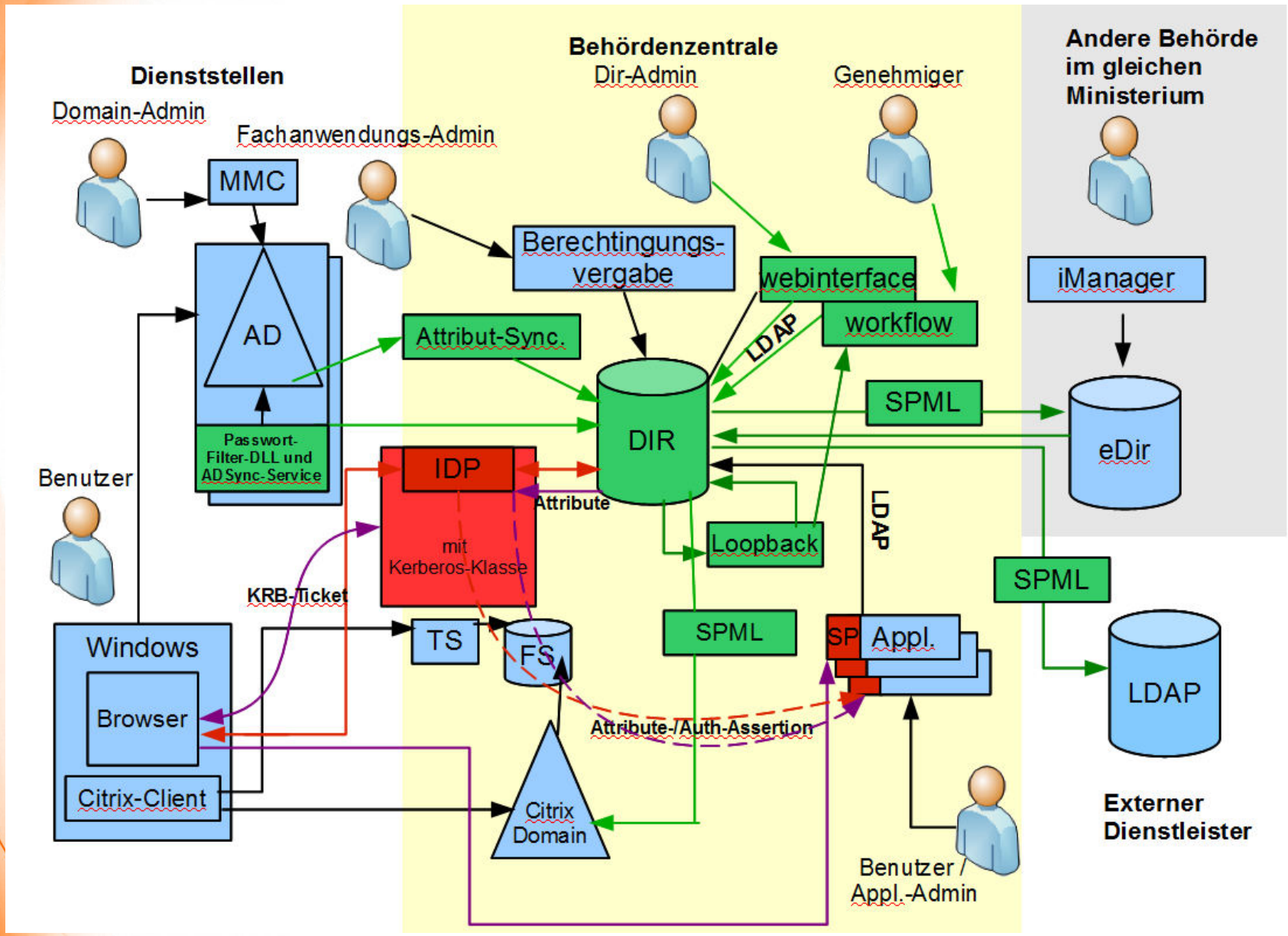
- Eine existierende auf proprietäte Software basierende Identity-Management-Lösung sollte mit Open-Source-Software nachgebaut werden
  - komplexe Synchronisierungsmechanismen
  - komplexe Berechtigungsattributvergabe
- Zusätzlich sollte WebSSO mithilfe von Shibboleth realisiert werden
  - ein IdP, der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

DAASI International GmbH

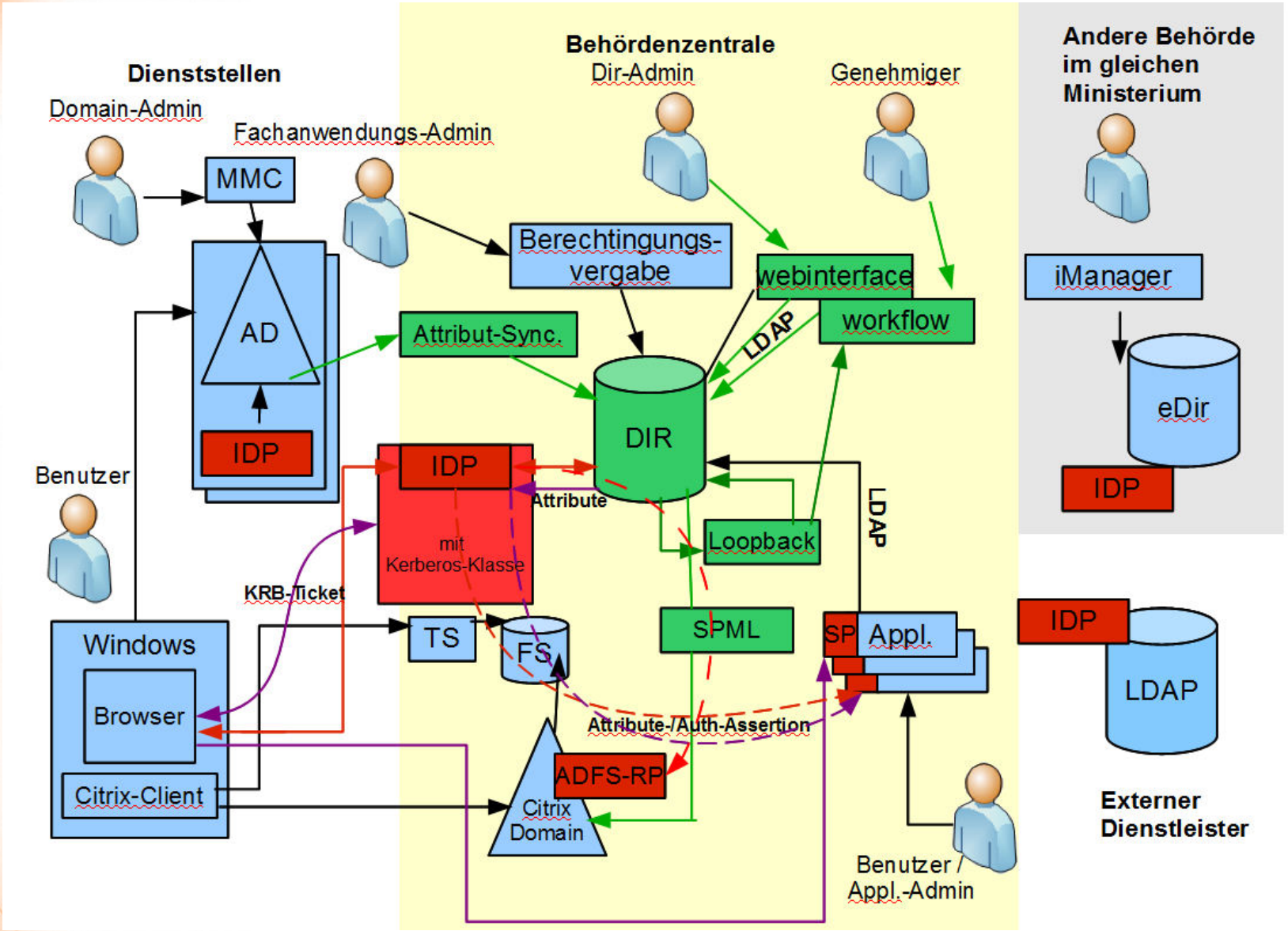
Migration der jetzigen Lösung



Integration von WebSSO und Kerberos



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

DAASI International GmbH