SPML-basierte Provisionierung im Identity Management

28. DV-Treffen der Max-Planck-Institute

22. September 2011

Gustav-Stresemann-Institut

Bonn

Peter Gietz,
DAASI International GmbH

DAASI International GmbH

- Spezialisiert auf Verzeichnisdienste, digitale Signatur, (Federated) Identity Management, Grid-Computing und eHumanities (einschl. anwendernaher Programmierung)
- Spin-Off der Universität Tübingen
  - seit 2000 auf dem Markt
  - 7 Mitarbeiter (Tendenz steigend)
- Hauptkundenzielgruppe: Hochschulen, Behörden, Forschungseinrichtungen, Bibliotheken und Verwaltungen
- Forschungsorientiert:
  - BMBF-Projekte zu Grid-Computing (IVOM, GapSLC) und eHumanities (TextGrid, DARIAH-DE)
- Konzentriert auf Open-Source, Aktiv in Standardisierung (IETF, OGF, TERENA, DFN, ...)
- Mehr unter: www.daasi.de

DAASI International GmbH

Agenda

1. Grundlegendes zu Identity Management
2. Prinzip von AD-Konnektoren
3. Einführung in SPML
4. Beschreibung des SPML Lösungsansatzes
5. Praktische Erfahrungen

DAASI International GmbH

Grundlegendes zu Identity Management

Definition des Begriffs Identity Management

- 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

DAASI International GmbH

Was war neu bei Identity Management?

- Benutzerverwaltungen gibt es seit den Anfängen der EDV
  - etc/passwd in Unix ist auch Benutzerverwaltung!
  - Die Probleme sind die alten
- Identity Management Systeme sorgen dafür dass
  - man ein Gesamtkonzept der IT-Landschaft entwickelt
  - Daten aus autoritativen Datenquellen kommen und nicht überall neu eingetippt werden müssen
  - die Benutzerverwaltung automatisiert wird
- Automatisierte Prozesse bewirken, dass
  - Berechtigungen gleich nach der Einstellung zur Verfügung stehen
  - aber auch gleich nach dem Austritt aus der Organisation entzogen werden können

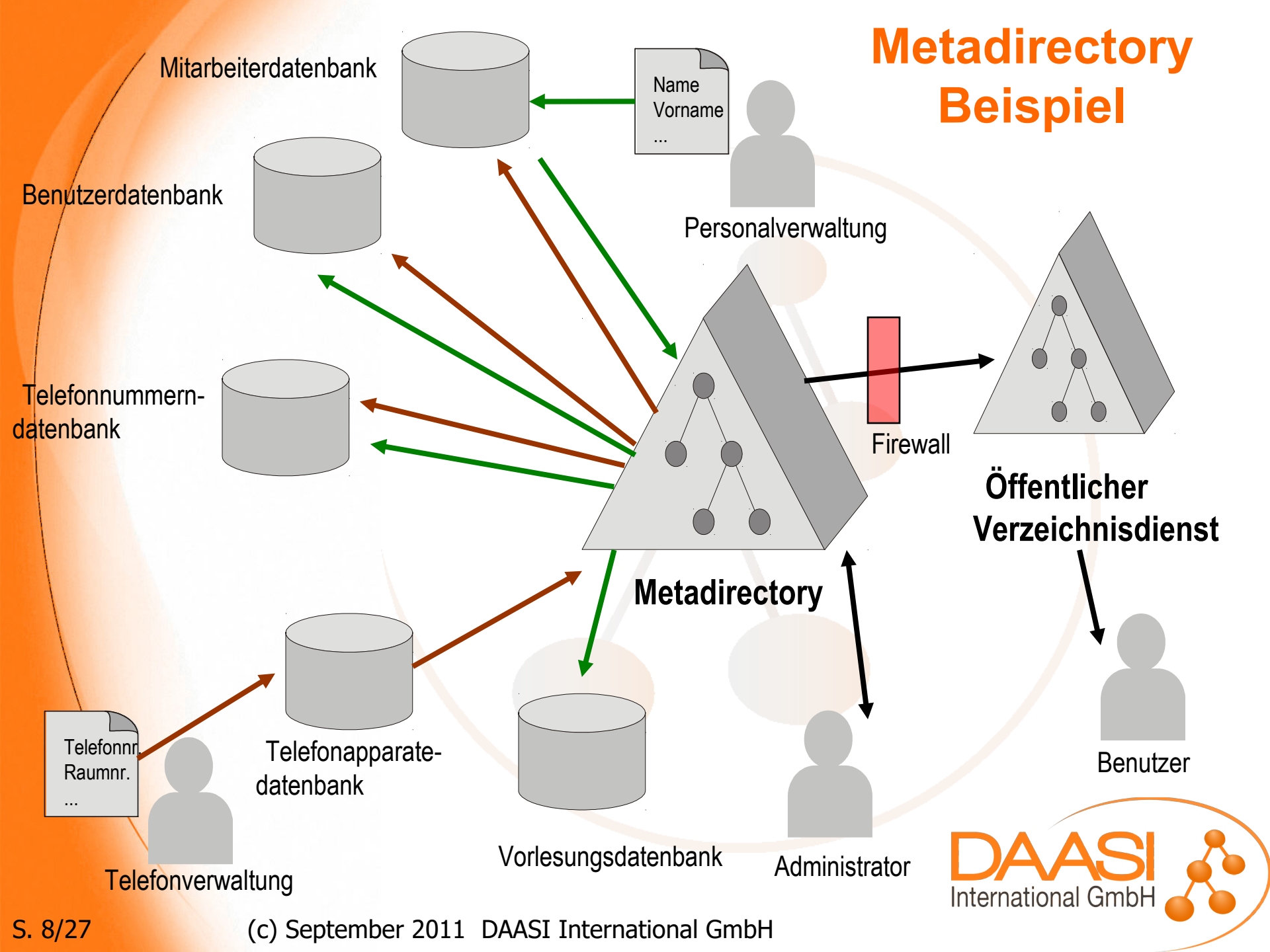
DAASI International GmbH

Wichtigste Komponenten von Identity Management Systemen

- Quelldatenbanken
  - authoritative Datenquellen und Anwendungen
- Zielsysteme
  - Konsumenten dieser authoritativen Daten
- Verzeichnisdienste sind zentrale Bestandteile
  - speichern Identitätsinformation, Passwörtern, Zertifikate, Rollen und Berechtigungen, Policy
  - Standards: X.500, LDAP
  - Implementierungen: OpenLDAP, Novell eDirectory, MS Active Directory
- Metadirectories dienen zur
  - Synchronisierung verschiedener Datenspeicher
  - Vermeidung von Inkonsistenzen
  - Passwort-Verwaltung und –Synchronisierung
- Konnektoren verbinden
  - Datenquellen mit Metadirectory
  - Metadirectory mit Zielsystemen (= Provisioning)

DAASI International GmbH

Metadirectory Beispiel



Prinzip von AD-Konnektoren

Prinzip von AD-Konnektoren

- Grundsätzlich kann ein AD über Standard-LDAP-Befehle angesprochen werden
  - Allerdings nicht 100%ge Unterstützung des LDAP-Standards …
  - Nur LDAPS kein START_TLS
- Zusätzlich gibt es das proprietäre Protokoll ADSI
- Bei Provisionierung von AD müssen einige Besonderheiten berücksichtigt werden:
  - SID Generierung
  - Kompliziertes Anlegen eines neuen Eintrags:
    - 1.) Eintrag anlegen mit den Daten und als gesperrt markieren
    - 2.) Passwort anlegen
    - 3.) Eintrag entsperren

Kurze Einführung in SPML

Glossar: DSML = Directory Service Markup Language.
XML-Format zur Abbildung von LDAP-Daten und -Operationen

Der SPML-Gedanke

- SPML v2 (Service Provisioning Markup Language) ist OASIS Standard vom April 2006
- SPML spezifiziert ein XML-Format zur Provisionierung
- Soll unabhängig von der Art des Quell- und der Zielsysteme für Provisionierung verwendet werden können.
- Definiert Grundoperationen „add“, „modify“, „delete“ und „lookup“, sowie Erweiterungen wie z.B. „search“.
  - Jede Operation besteht aus einem Request und einem Response
  - Operationsmodell ist flexibel erweiterbar
- Offen für verschiedene Datenformate (SPML „Envelope“, flexible „payload“)
- Vordefiniertes Datenschema z.B. „SPMLv2 - DSMLv2 Profile“:
  - Datenänderungsanweisungen im DSMLv2-Format
  - Transportiert im SPML-Dokument

DAASI International GmbH

SPML-Komponenten

- Provisioning System Object (PSO):
  - Einzelnes Datenobjekt in einem Daten-Container, also z.B. ein AD-Eintrag
- Provisioning Service Target (PST):
  - Ist Container (Zielsystem) für Objekte (z.B. AD)
- Provisioning Service Provider (PSP):
  - Nimmt SPML-Dokumente für ein oder mehrere PSTs entgegen
  - Führt Änderungen auf PSOs des PSTs durch (also: ändert Einträge im AD)
- Requesting Authority (RA):
  - Erzeugt SPML-Dokumente die der PSP konsumiert
  - Wird am Quellsystem angeschlossen

DAASI International GmbH

Vor- und Nachteile

- Vorteile:
  - SPML kann leicht von XML-Parsern eingelesen werden
  - Erweiterbares Format
  - Es werden nur Änderungen provisioniert (im Gegensatz zu einem Gesamtabgleich), diese finden zeitnah, z.B. jede Minute statt
  - Klar strukturiertes generisch einsetzbares Provisionierungsmodell
  - Standardisierte möglichkeit, auch Gruppeninformationen zu provisionieren
- Nachteile:
  - SPML geht davon aus, dass Datenänderungen am Zielsystem nur über die Provisionierung erfolgt
  - Recovery eines Zielsystems über SPML nicht durch Standardoperationen möglich
  - Typischer XML-Overhead

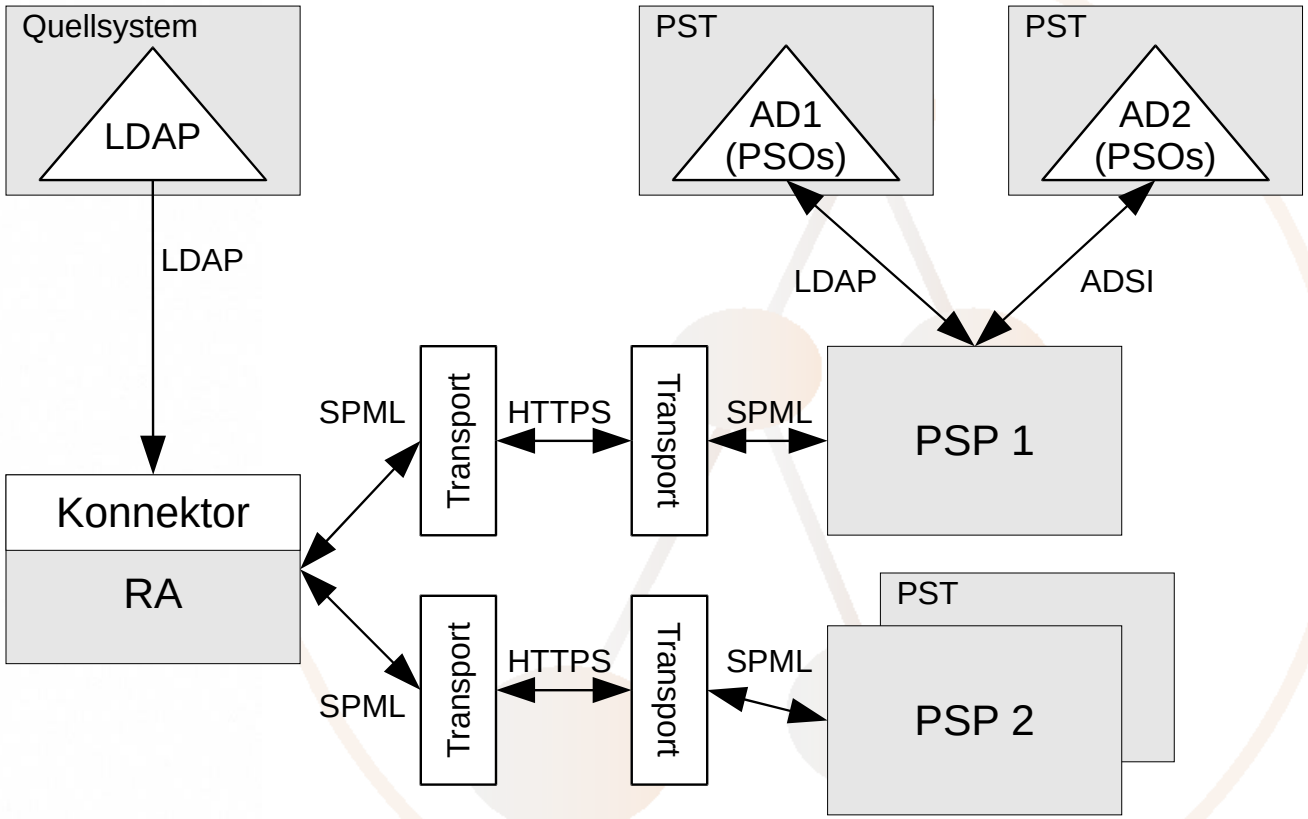
Beschreibung der SPML-Implementierung von DAASI

Beteiligte Komponenten

- Quellsystem OpenLDAP
  - mit Overlay „accesslog“ durch das alle Änderungs-Operationen in einem Teilbaum des Servers gespeichert werden können
- RA
  - mit Konnektor für „accesslog“, der sehr zeitnah Änderungen wahrnimmt.
  - Transport über REST (HTTPS)
  - verwaltet eine Queue für jeden PSP
- Active Directory als eins der möglichen Zielsysteme
- PSP für Active Directory
  - Änderungen der Objekte (PSOs) über LDAP
  - oder über ADSI

DAASI International GmbH

Aufbau einer SPML-Umgebung

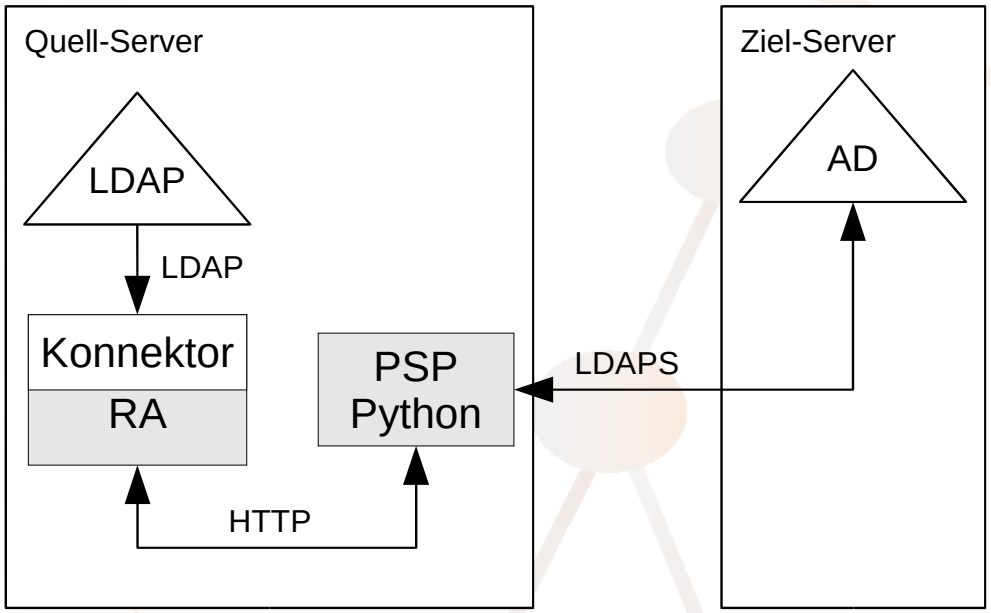


Ablauf

- Änderung im OpenLDAP wird über Overlay protokolliert
- Periodische Abfrage der protokollierten Änderungen werden ausgelesen
- Ausgelesene Änderungen werden in DSMLv2 transformiert
- DSMLv2-Dokumente werden für jeden PSP in SPML-Dokumente „verpackt“
- SPML-Request wird an PSP gesendet, dort:
  - SPML-Request wird „ausgepackt“ -> DSMLv2-Request
  - DSMLv2 wird in LDAP- oder ADSI-Anweisungen für PST transformiert
  - Ergebnis der Anweisung wird in DSMLv2 transformiert
  - DSMLv2-Dokumente werden für RA in SPML-Dokumente „verpackt“
- SPML-Response wird an RA gesendet
  - wenn Fehler auftritt bleibt das Dokument in der Queue

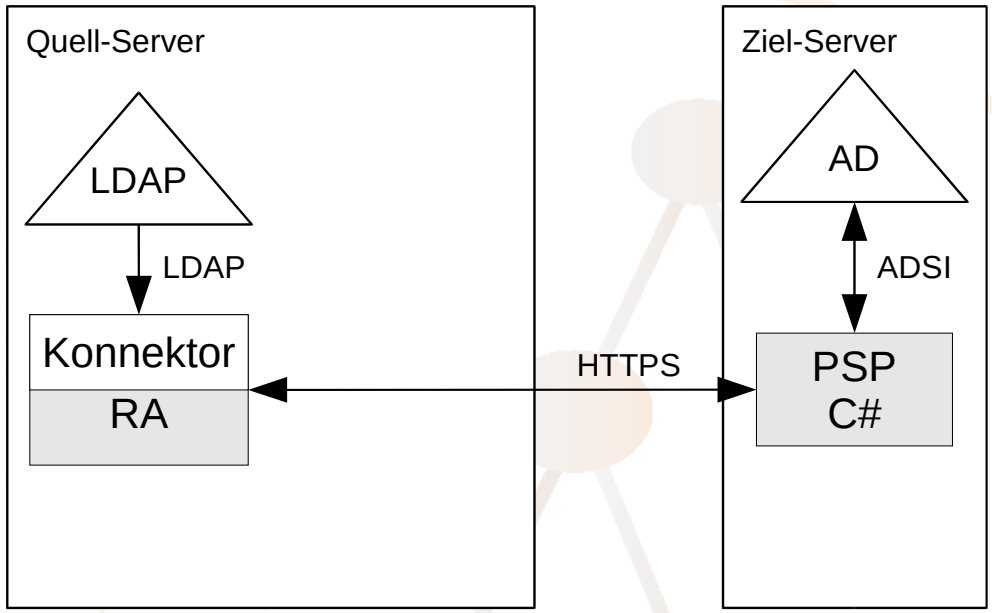
DAASI International GmbH

Aufteilung der Komponenten (1/2)



- Keine Einwirkungen auf das AD-System
- Production ready

Aufteilung der Komponenten (2/2)



- Mehr Möglichkeiten durch ADSI (Group-Policies, etc.)
- PSP muss auf dem AD installiert werden
- Auf unserer Roadmap

Erfahrungen

Lessons learnt

- Vorteil gegenüber täglichem Gesamtabgleich, da Änderungen zeitnah provisioniert werden
- Für Recovery und Synchronisierung wurden zwei zusätzliche SPML-Capabilities von DAASI spezifiziert und entwickelt (für Selbstheilung von Fehlern):
  - Identify-Capability:
    - Versucht ein Objekt anhand dessen Daten zu identifizieren
    - z.B. für den Fall, dass im AD manuell ein Eintrag gelöscht und wieder angelegt wurde, also sich die ObjectID geändert hat
  - Sync-Capability:
    - Erhält Daten von RA und aktualisiert Daten des PST auf gleichen Stand
    - Also ein Gesamtabgleich

DAASI International GmbH

Lessons learnt

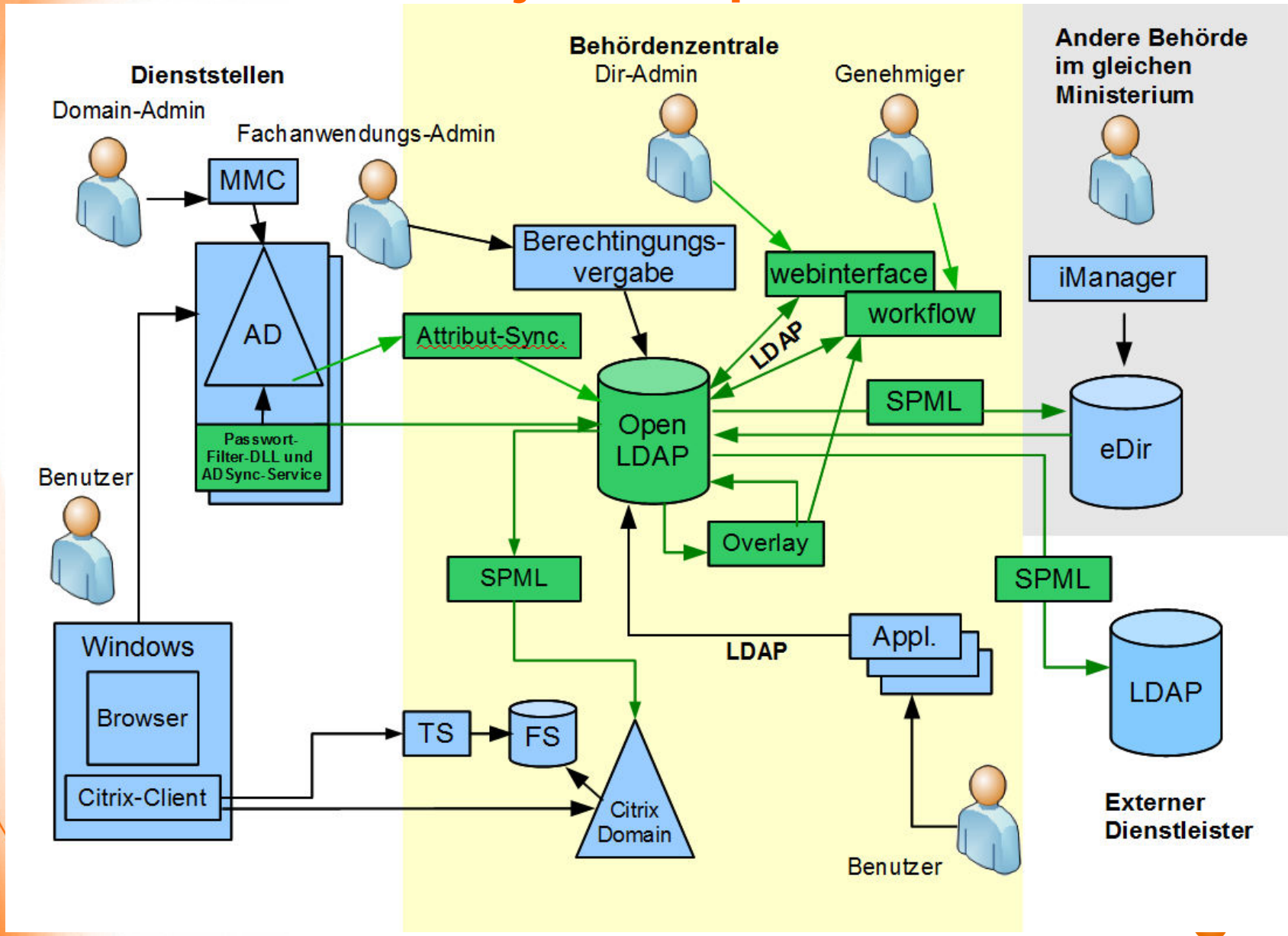
- XSL-Transformationen vor Senden der Daten bei RA und vor Empfang an PSP haben sich bewährt z.B. für
  - Attribut-Mappings
  - Ignorieren spezieller Einträge
  - Hinzufügen von konstanten Daten

Projektbeispiel

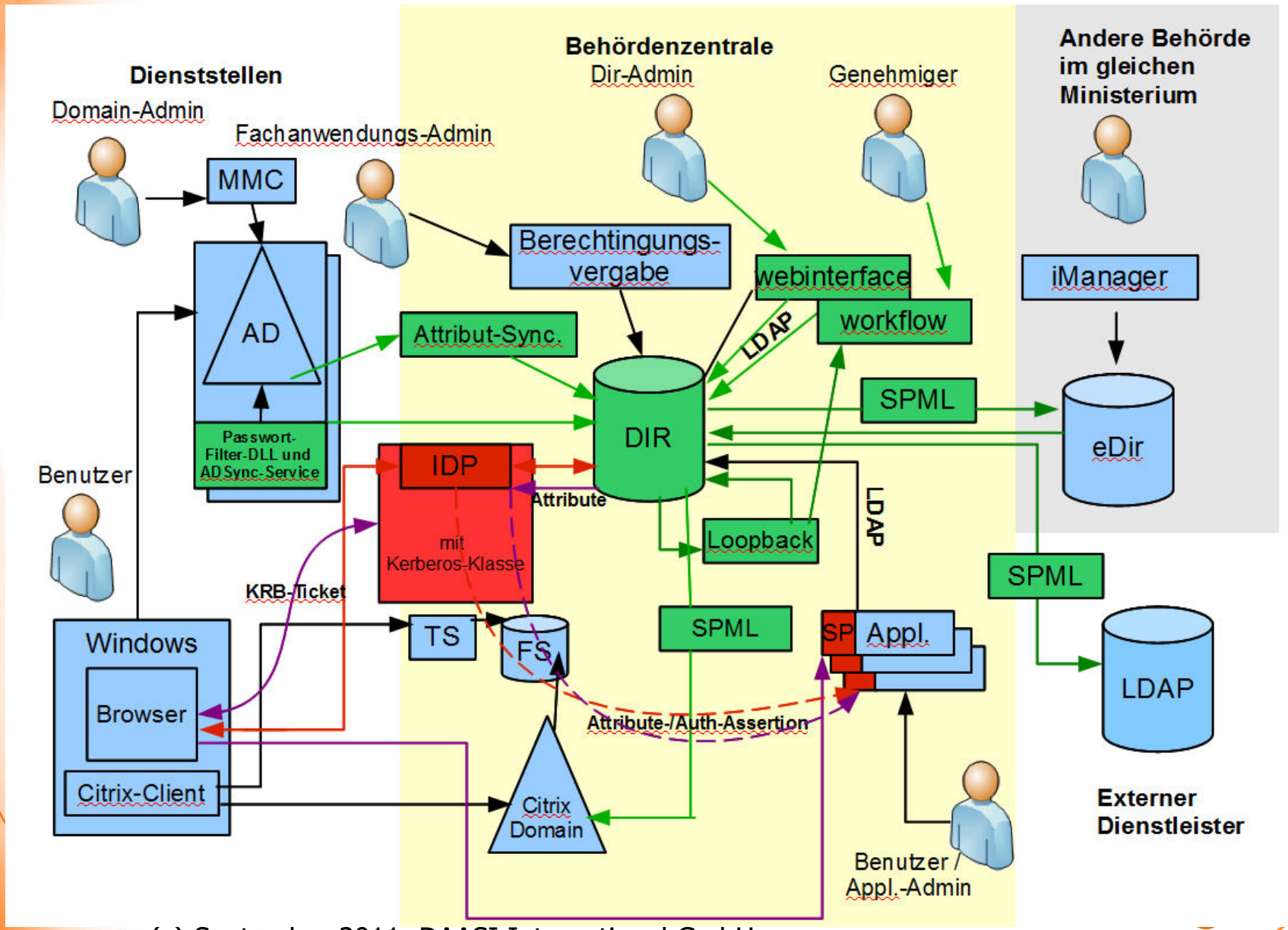
- Eine existierende auf proprietäte Software basierende Identity-Management-Lösung sollte mit Open-Source-Software nachgebaut werden
  - komplexe Synchronisierungsmechanismen
  - komplexe Berechtigungsattributvergabe
- Zusätzlich sollte WebSSO mithilfe von Shibboleth realisiert werden
  - ein IdP, der 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

Projektbeispiel



Projektbeispiel



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

- Meet LDAP-Experts @ LDAPCon 2011
  October 10-11, 2011 in Heidelberg

  www.ldapcon.org

DAASI International GmbH