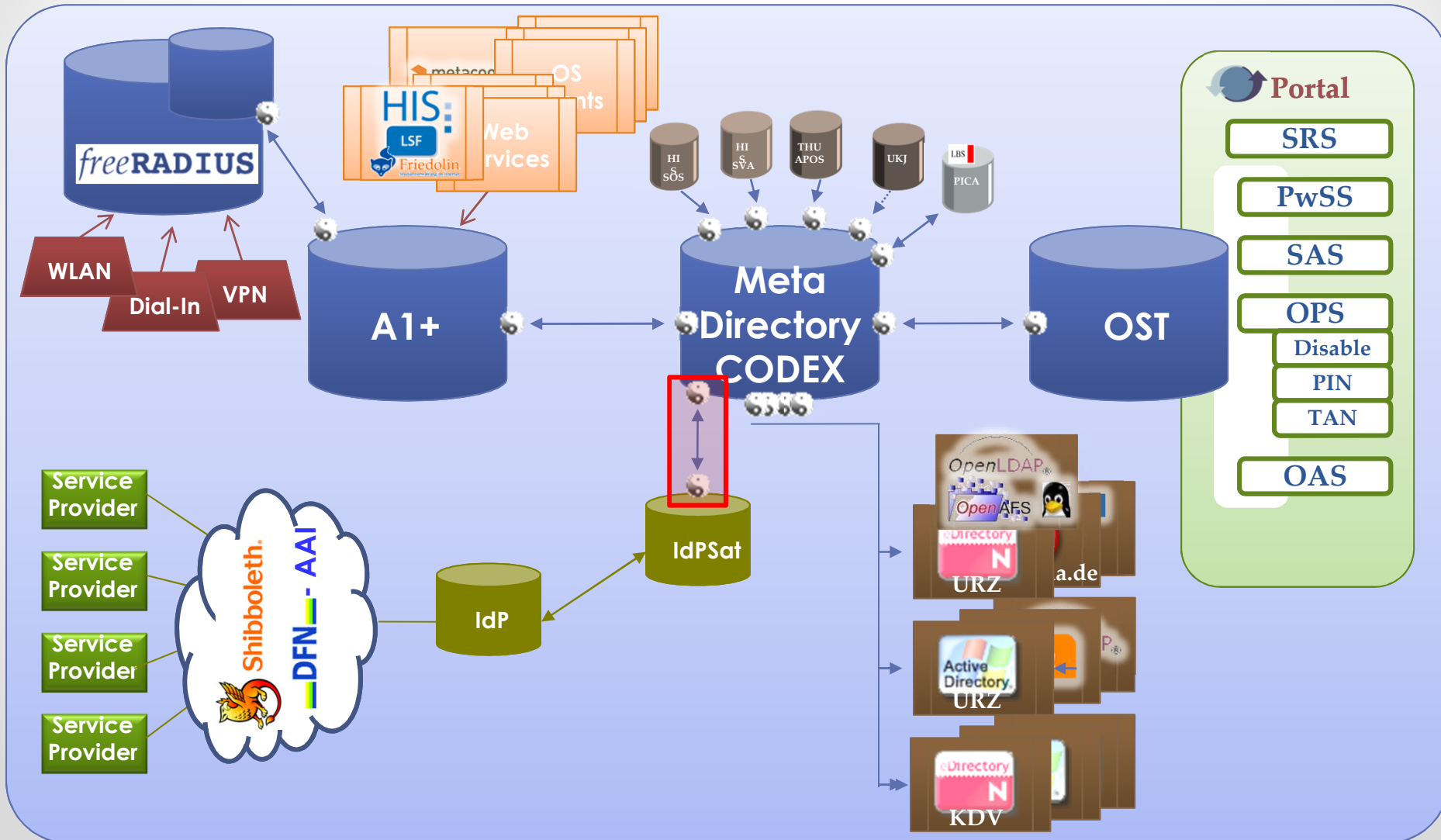


Thüringer Identity Management Projekt CODEX

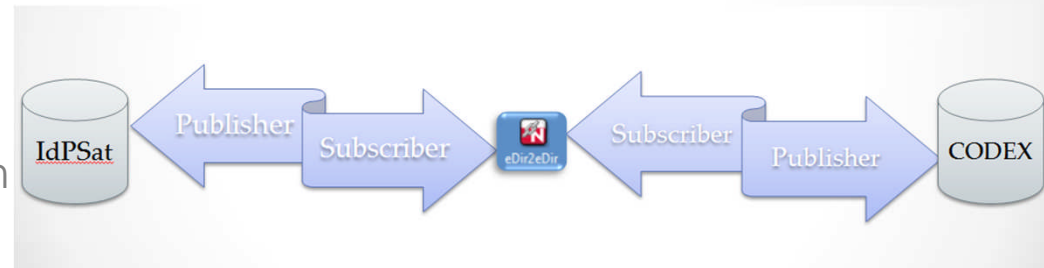
Konnektion des Shibboleth Identity
Providers

Einordnung in das Gesamtszenario



Umsetzung des Konnektors














- Novell
 - eDirectory 8.8 SP2
 - IDM 3.5.1
 - Designer 3.5
- eDir2eDir Konnektor
 - 1 Treiber je eDirectory Baum
 - Treiber des eines Baums kommuniziert mit dem des anderen Baums



- Generischer Ansatz
 - Einsatz an allen Thüringer Einrichtungen möglich
 - Globale Variablen und Mapping Tabellen
 - Möglichkeit mehrere Organisationen einer Einrichtung zu unterstützen (Bsp. Bauhaus Universität und Hochschule für Musik in Weimar)

Umsetzung des Konnektors

- Global Configuration Values:

Connected System or Driver Name	IdPSat-Codex	
domainName	uni-jena.de	
OrganisationNameDN	O=uni	 
OrganisationUnitNameDN	OU=user,O=uni	 
personContainer	uni\user	 
usingMultipleOrganisations	false	
personContainerPathForMultipleOrganisations	user	
adminMailAddress	maike.lorenz@uni-jena.de	
delayTimeForExpiryDate	14	
ignoreLoginDisabledValue	false	

Umsetzung des Konnektors

- Bildung des Attributes eduPersonAffiliation

eduPersonAffiliation Mapping.IdPSat-Codex.DirXML Driver Set.IdPSat (

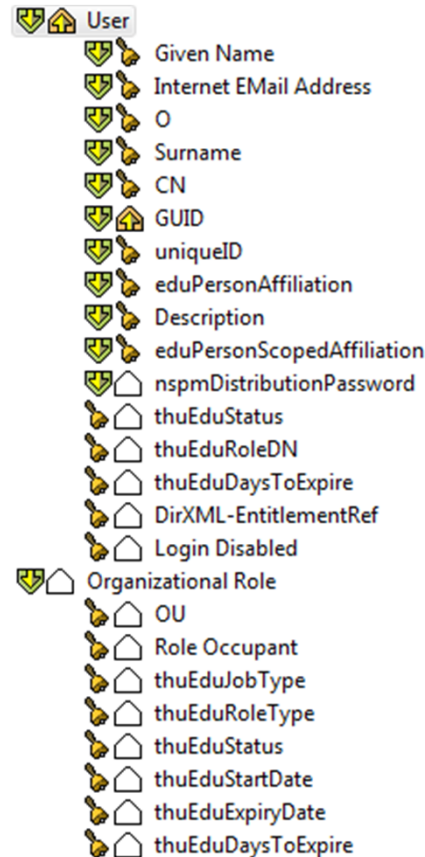
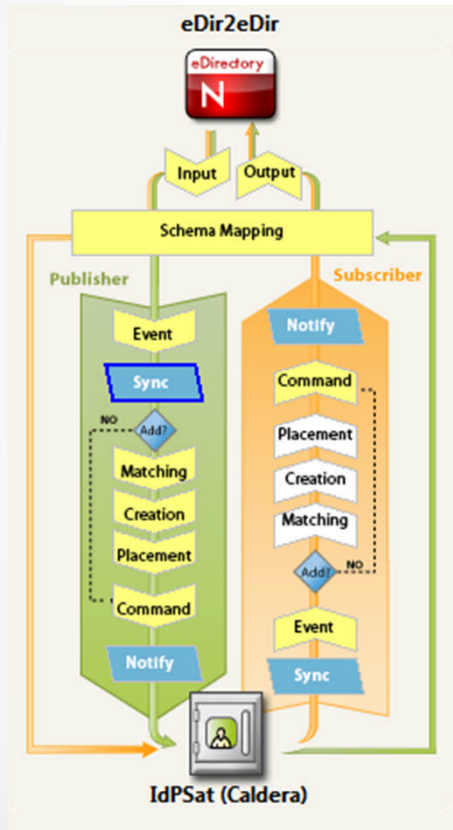
	eduPersonAffiliation CODEX Case Sensitive	eduPersonAffiliation IdPSat Case Sensitive
1	Student	member;student
2	Lehrbeauftragter	member;employee;faculty
3	Prof.im Ruhestand	member;employee;staff
4	Zeitstudent	affiliate
5	Praktikant	affiliate
6	UKJ	affiliate
7	Kooperationspartner	affiliate
8	Gastwissenschaftler	affiliate
9	Student anderer Hochschule	member;student
10	Weiterbildungsstudent	affiliate
11	Bibliotheksbenutzer	X
12	Mailnutzer	X
13	Servicekraft extern	X
14	Mitarbeiter im Ruhestand	X
15	Studentenwerk	X
16	Funktioneller Account	X
17	Mitarbeiter	X

	Jobtype Case Sensitive	eduPersonAffiliation IdPSat Case Sensitive
1	Arbeitsbeschaffungsmaßn.	employee
2	Aushilfe Drittmittel	employee
3	Aushilfe Haushalt	employee
4	Auszubildender	employee
5	Beamter	member;employee;faculty
6	Beschäftigter (SGB)	member;employee;faculty
7	Beschäftigter DM	member;employee;staff
8	EU/BU-Rentner	employee
9	Freiwilliges Jahr	employee
10	Hilfskraft	employee
11	Juniorprofessor (Bea)	member;employee;faculty
12	Lehrbeauftragter	X
13	Nichtwiss. Beschäftigte	member;employee;staff
14	Praktikant	employee
15	Prof.im Ruhestand	member;employee;faculty
16	Professor (Beamter)	member;employee;faculty
17	Professor (Beschäftigter)	member;employee;faculty
18	Volontär	employee
19	wiss. Hilfskraft DM	employee
20	wiss. Hilfskraft Haushalt	employee
21	Wissensch. Beschäftigter	member;employee;faculty

- Ableitung von Entitlement

Umsetzung des Konnektors

- Filterkonfiguration und Passwortsynchronisation



Umsetzung des Konnektors

- Schema Mapping
 - uniqueID = CN (common name)
- Matching
 - CN
- Lebenszyklus
 - Weicht vom Lebenszyklus des IdM Systems ab
 - Tagezähler Resttage der Gültigkeit (thuEduDaysToExpire)
 - Z.B.: 14 Tage Nachlaufzeit, gültig bis thuEduDaysToExpire = -14, wenn kleiner -14, dann löschen

Umsetzung des Konnektors

- Bei Sperrung, Löschung oder Ablauf der Gültigkeit im Quellsystem, wird Benutzerobjekt sofort aus IdPSat gelöscht
- Rollenevents
 - Müssen bearbeitet werden, z.B. Statusänderung an Rolle
 - Werden auf Seite des Quellsystems in Benutzerevent gewandelt, wodurch Benutzerobjekt inkl. zugehöriger Rollen neu verarbeitet wird
- Es werden keine Events in Richtung Quellsystem zugelassen
 - Außer entfernen der Assoziation, nachdem Benutzerobjekt aus IdPSat gelöscht wurde

Zusammenarbeit und Ausblick

- Konnektorentwicklung im Thüringer Projekt CODEX
 - Verantwortlichkeit für:
 - Entwicklung und Test
 - Dokumentation, inkl. Installationsanleitung
 - Ggf. Consulting in den anderen Einrichtungen
 - Wartung und Weiterentwicklung
- Ausblick:
 - Thüringenweite Schemaerweiterung 2011
 - Konnektor an dieses Schema anpassen
 - Z.B.: im Umgang mit neuen Kontaktdatenobjekten

Vielen Dank für Ihre Aufmerksamkeit

- Fragen?