bwIDM:
Föderieren auch nicht-webbasierter Dienste auf Basis von SAML

5. DFN Forum

22.5.2012

Michael Simon, Sven Schober, Saher Semaan,
Marcel Waldvogel, Martin Nussbaumer

bwIDM – Vision

- **Motivation**: Beobachtbarer Trend zu verteilten Diensten
  - **zunehmende Spezialisierung von IT-Diensten**: inspiriert durch Ansätze wie Utility Computing, Cloud Konzepte, Gridansätze, usw.
  - Anwendungsfall Baden-Württemberg: Hochleistungsrechnen auf Compute Cluster, bwGRID, Large Scale Data Facility (LSDF), landesweites integriertes Bibliothekssystem

- **Ziel:** bequemer Zugriff zu verteilten Diensten wie im lokalen Umfeld
  - Vergabe von Autorisierungskriterien bleiben „lokale Angelegenheit“
  - Koordinierte Richtlinien für die Autorisierung bei Diensten (Föderationsregeln)
  - Client Zugriff: verteilter Zugriff auf BW-Dienste über lokalen Zugang

- **Vision**: **Ein Forscher aus Baden-Württemberg kann *verteilte* BW-Dienste mit dem gewohnten *lokalen* Zugang nutzen**

Agenda

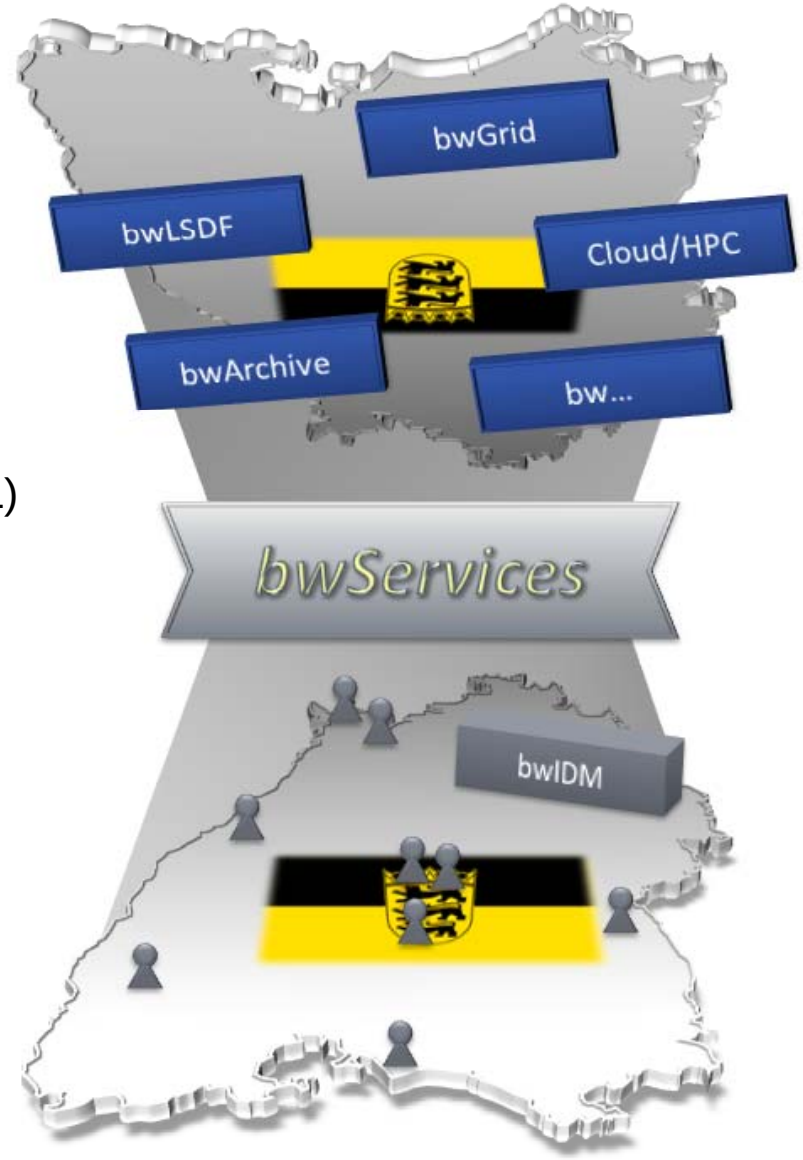
- Fakten, Aufgaben und Ziele zum bwIDM-Projekt
- Kriterienkatalog und Anforderungsanalyse
- Föderative Verfahren
  - Moonshot-Projekt
  - bwIDM-Ansatz über PAM/ECP mit notwendigen Erweiterungen
- Ausblick und Zusammenfassung

bwIDM - Projekt

- Beteiligte Einrichtungen
  - Die Universitäten des Landes Baden-Württemberg
  - Kern-Team
    - Universität Freiburg
    - Karlsruher Institut für Technologie (PL)
    - Universität Konstanz
    - Universität Ulm

- Unterstützt durch das Ministerium für Wissenschaft, Forschung und Kunst Baden-Württemberg (MWK)

- Laufzeit: 1.7.2011-31.12.2013



bwIDM - Alleinstellungsmerkmale

- bwIDM verwendet SAML und die Shibboleth Implementierung
  - Hoher Verbreitungsgrad an Universitäten und Bibliotheken
  - gut erprobt, stark wachsender Einsatz für webbasierte Dienste beobachtbar

- Föderieren *nicht*-webbasierter Zugänge
  - Shibboleth für webbasierte Dienste
  - SAML sieht auch nicht-webbasierte Dienste vor
  - bwIDM: Shibboleth-basiertes Zugangsverfahren für nicht-webbasierte Dienste

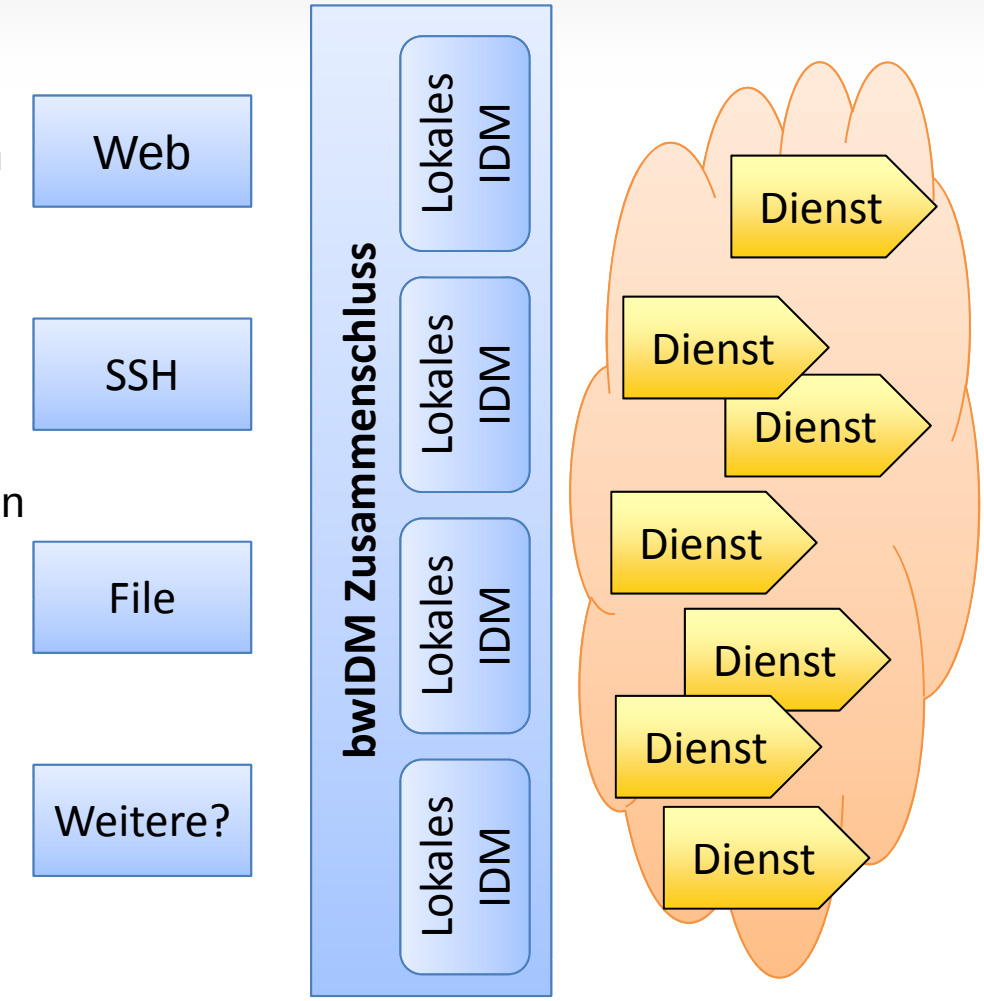
- Provisionierungsunterstützung, Identitätsmanagementunterstützung
  - Dienst-lokale Nutzerkonten: Verfahren für stark gekoppelte Dienste
  - Datenschutzkonforme Provisionierung Dienst-lokaler Konten*
  - Datenschutzkonforme Deprovisionierung Dienst-lokaler Konten*

***Dienst-lokale Konten**: Systemspezifische Informationen über Nutzer, die für den Betrieb des Dienstes unabhängig vom Authentifizierungsvorgang bereitgestellt werden müssen (bspw. UID, GID)

bwIDM - Kernaufgaben

bwIDM kümmert sich um

1. ... Zugriff
   - Dienstnutzung im technischen Sinn
   - Zusammenarbeit mit anzu-schließenden Diensten
2. ... „Identitätsmanagement“
   - Lebenszyklus von Personen, Attributen, Autorisierungsmerkmalen
   - Gewährleistung von Verlässlichkeit
3. ... einen Zusammenschluss
   - zu einem übergreifenden Ganzen
   - Eigenständigkeit lokaler IDMs



Anforderungsanalyse

- Kriterienkatalog zur Bewertung föderativer Verfahren (FV)

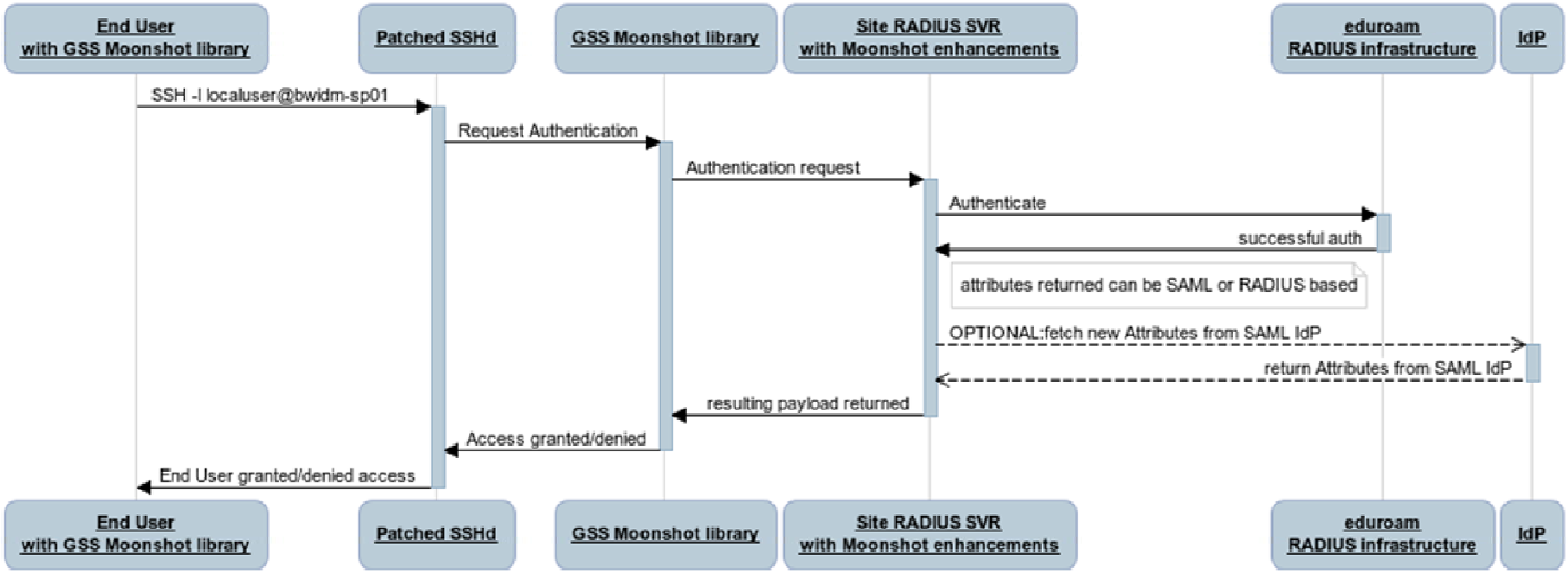
Personenmerkmale	• Übermittlung personenbezogener Attribute • Datensparsame Übermittlung • Einverständnis durch Nutzer bei Übertragung an Dritte
Datenbereitstellung	• Übermittlung von Autorisierungsmerkmalen • Dienst-lokale Aktualität von Autorisierungsmerkmalen
Betriebsfähigkeit	• Aufwand (initial, dauerhaft) • Zukunftssicherheit des Föderativen Verfahrens (FV) • Integrationsfähigkeit in bestehende Föderationen (DFN-AAI)

Agenda

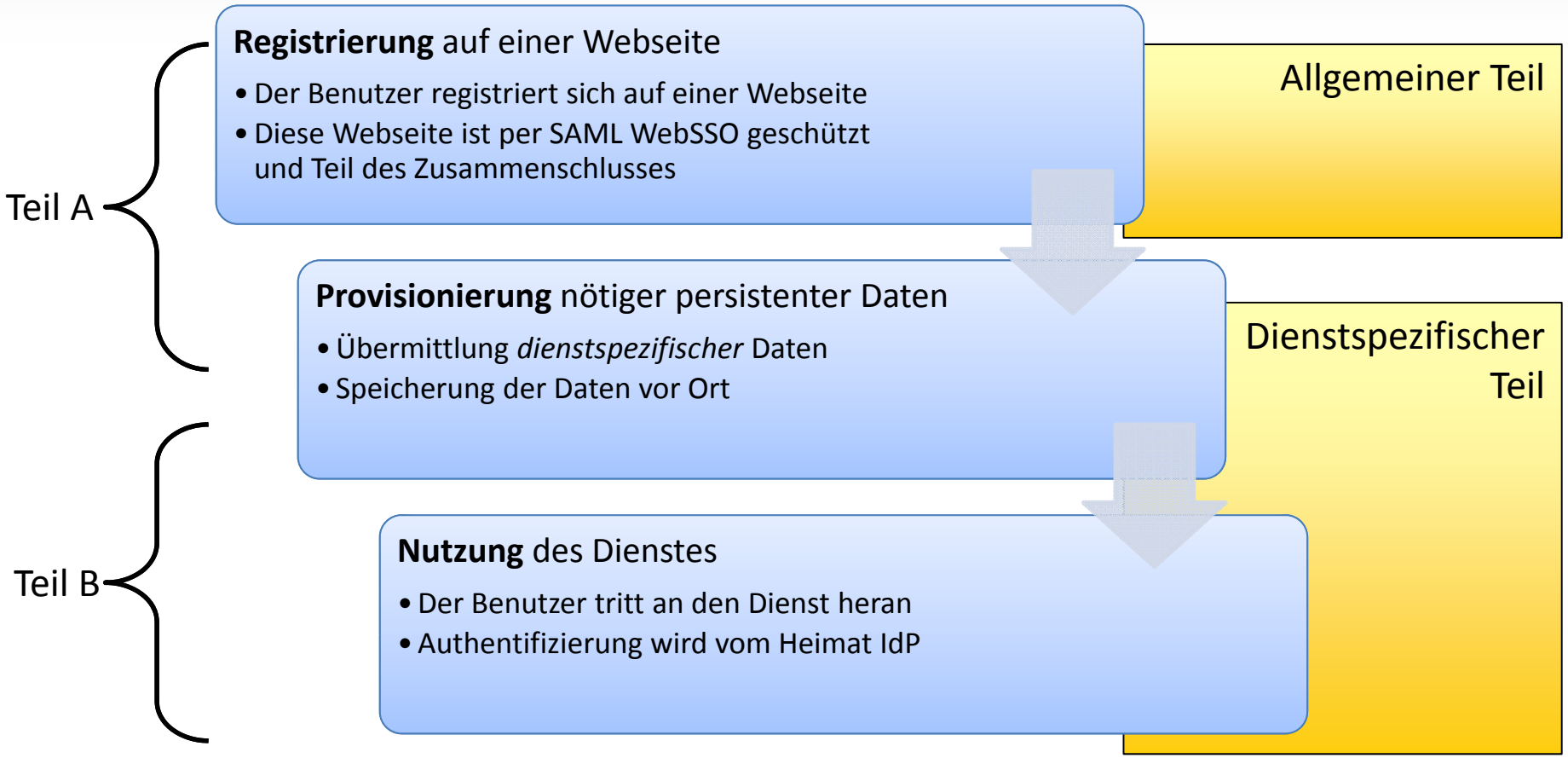
- Fakten, Aufgaben und Ziele zum bwIDM-Projekt
- Anforderungsanalyse
- Föderative Verfahren
  - Moonshot-Projekt
  - bwIDM-Ansatz über PAM/ECP mit notwendigen Erweiterungen
- Ausblick und Zusammenfassung

Das „Moonshot“-Projekt

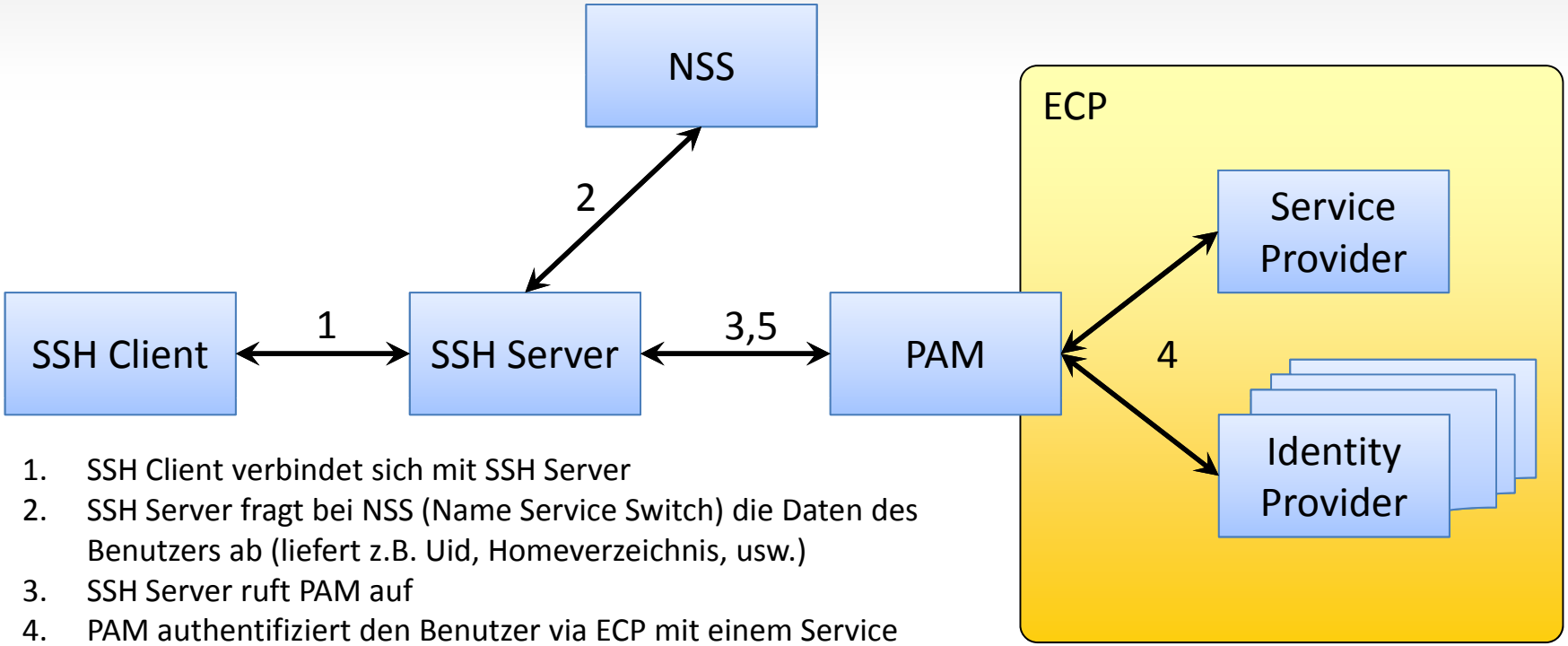
- Moonshot Ansatz: „Federating Everything“
  - Föderativer Authentifizierungs- und Autorisierungsmechanismus für jegliche Anwendung oder Dienste (web/non-web)
  - Eine Infrastruktur als Brücke zwischen Organisationen und deren Anwendungen/Dienste
  - Vision: Aufbau eines „Common Global Access Management System“



Der bwIDM-Ansatz: PAM/ECP mit Erweiterungen



PAM/ECP - Nutzung des Dienstes (Teil B)



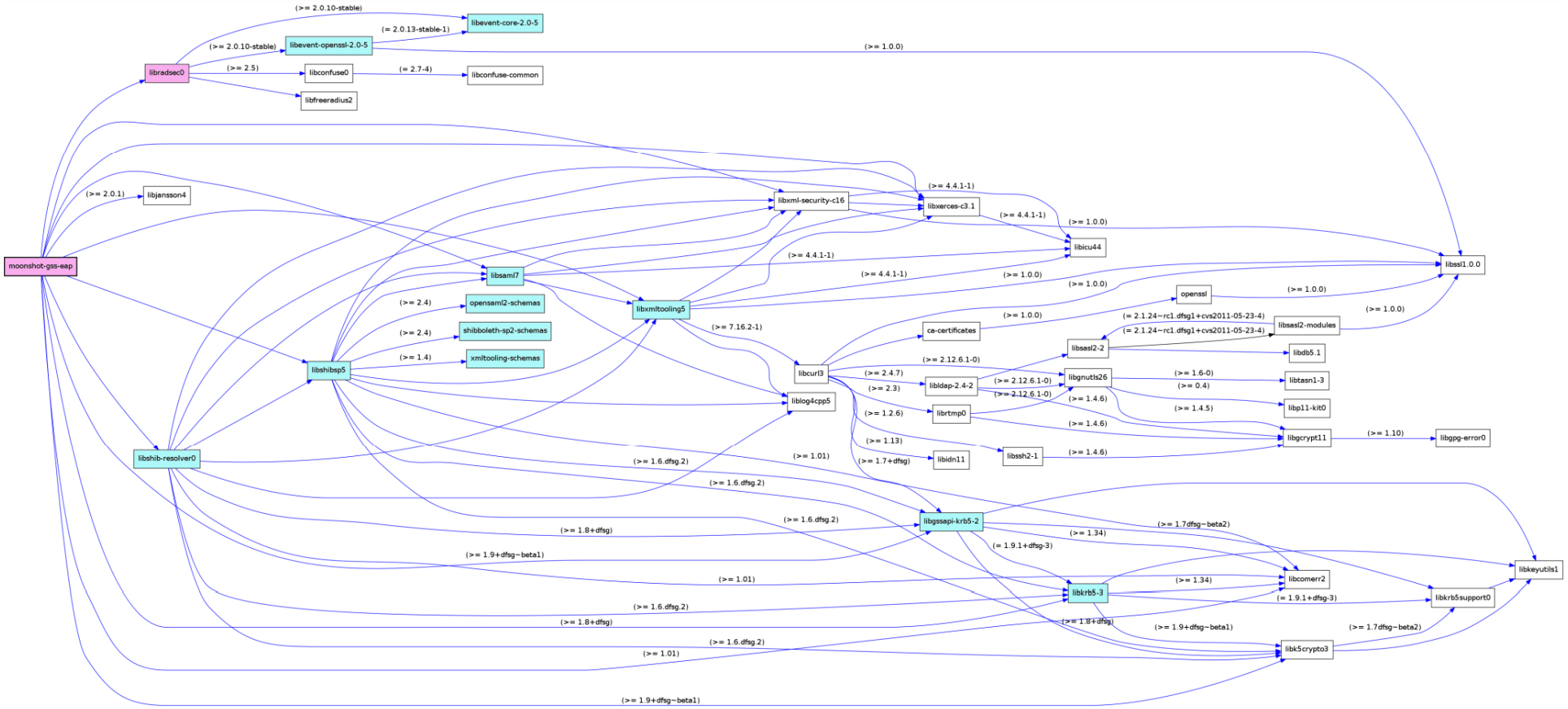
1. SSH Client verbindet sich mit SSH Server
2. SSH Server fragt bei NSS (Name Service Switch) die Daten des Benutzers ab (liefert z.B. Uid, Homeverzeichnis, usw.)
3. SSH Server ruft PAM auf
4. PAM authentifiziert den Benutzer via ECP mit einem Service Provider und dem Identity Provider der Heimatorganisation des Benutzers. Dabei bekommt der SP Autorisierungsdaten in der Assertion mitgeliefert und stellt diese Daten dem PAM Modul zur Verfügung.
5. PAM entscheidet dann, ob die Authentifizierung erfolgreich war.

Vergleich der Ansätze

Kriterien	Moonshot	bwIDM-PAM/ECP
Personenmerkmale		
Übermittlung personenbezogener Attribute	Unklar	Ja
Datensparsame Übermittlung	Nein	Ja
Einverständnis durch Nutzer bei Übertragung an Dritte	Nein	Ja
Datenbereitstellung		
Übermittlung von Autorisierungsmerkmalen	Nein	Ja
Dienst-lokale Aktualität von Autorisierungsmerkmalen	Nein	Ja
Betriebsfähigkeit		
Aufwand	hoch	gering
Zukunftssicherheit des Föderativen Verfahrens (FV)	Zukünftiger Standard?	Exist. Standards
Integrationsfähigkeit in bestehende Föderationen (DFN-AAI)	k.A.	Ja

Vergleich „Invasivität“ der Ansätze: Moonshot

Abhängigkeitsgraph involvierter Bibliotheken/Pakete



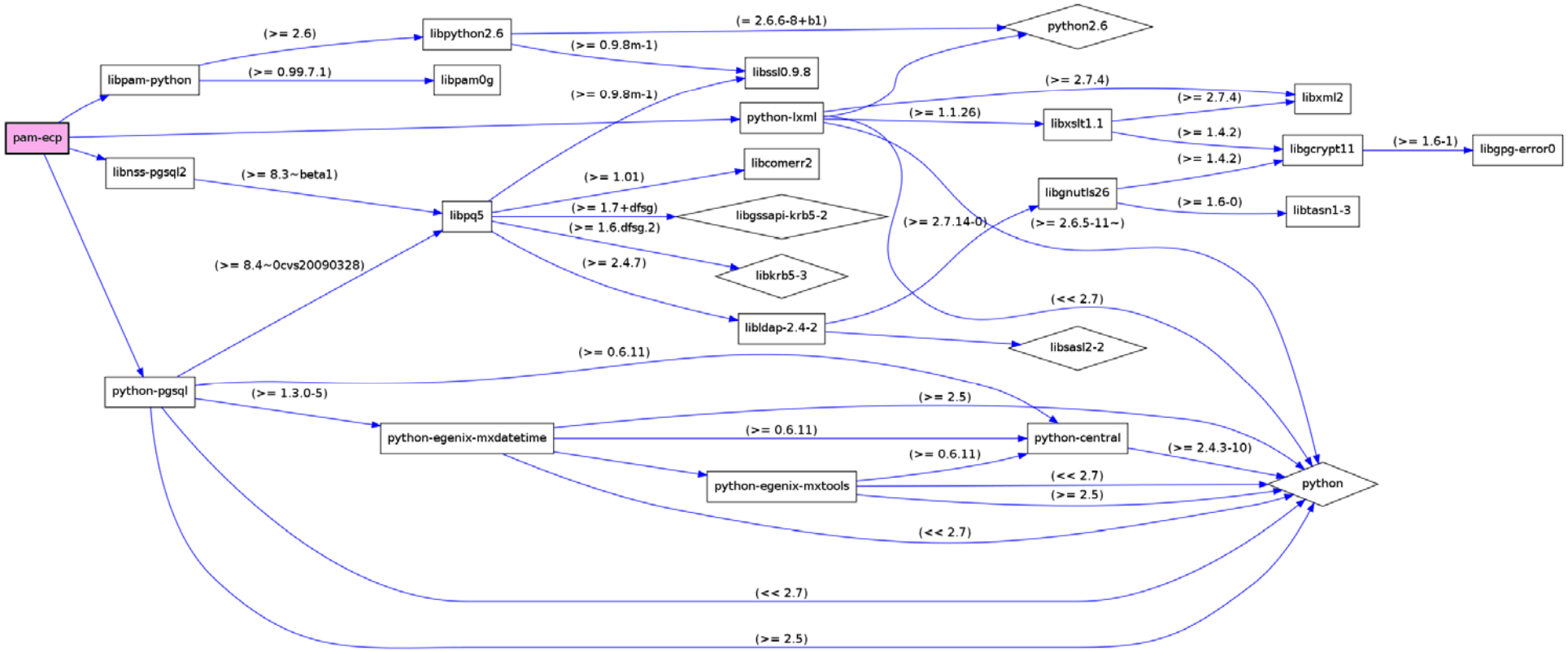
Eigenentwicklung

nicht in Standarddistribution verfügbar

http://collab-maint.alioth.debian.org/debtree/

Vergleich „Invasivität“ der Ansätze: bwIDM-PAM/ECP

Abhängigkeitsgraph involvierter Bibliotheken/Pakete



Eigenentwicklung

nicht in Standarddistribution verfügbar

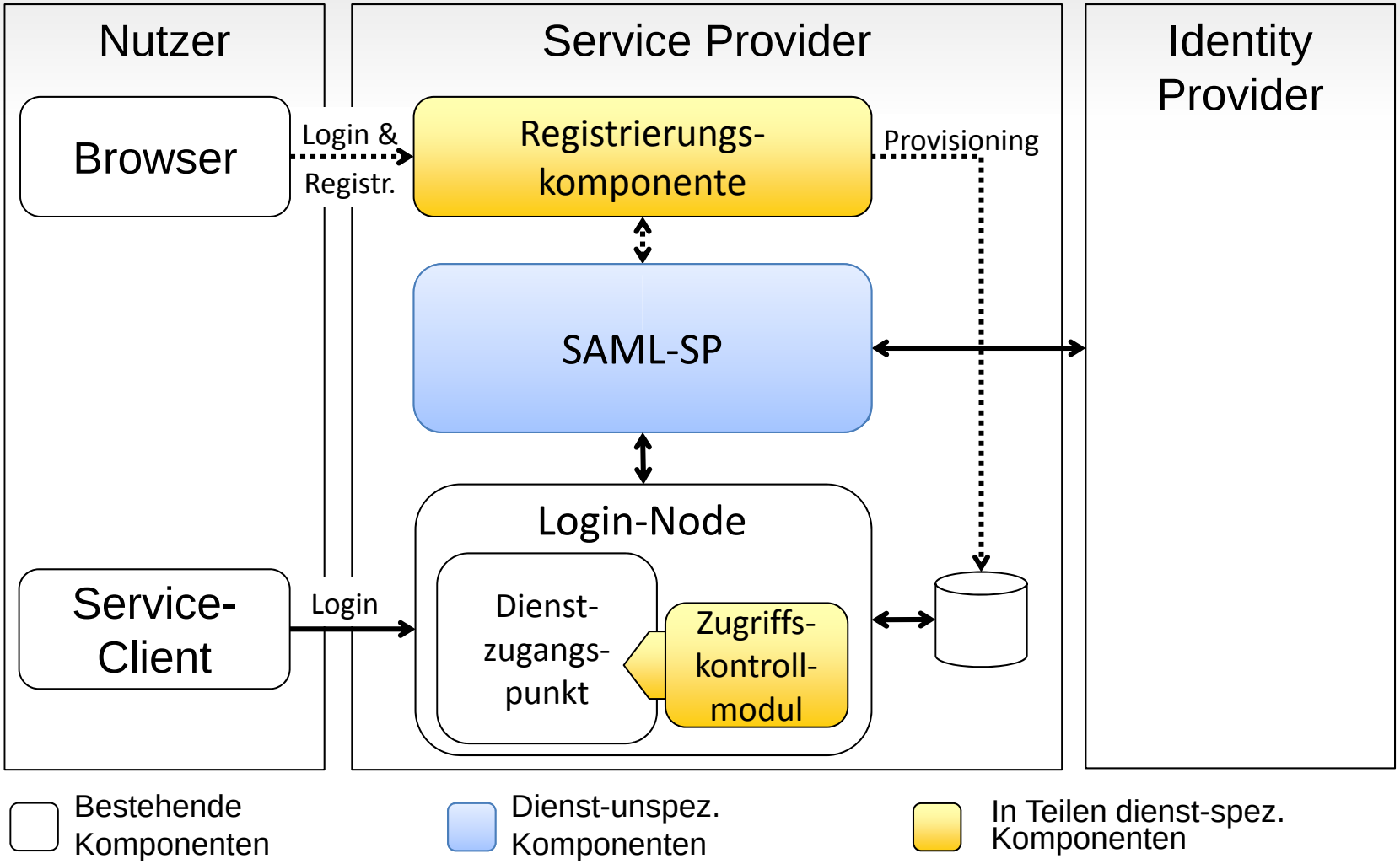
http://collab-maint.alioth.debian.org/debtree/

Agenda

- Fakten, Aufgaben und Ziele zum bwIDM-Projekt
- Anforderungsanalyse
- Föderative Verfahren
  - Moonshot-Projekt
  - bwIDM-Ansatz über PAM/ECP mit notwendigen Erweiterungen
- Ausblick und Zusammenfassung

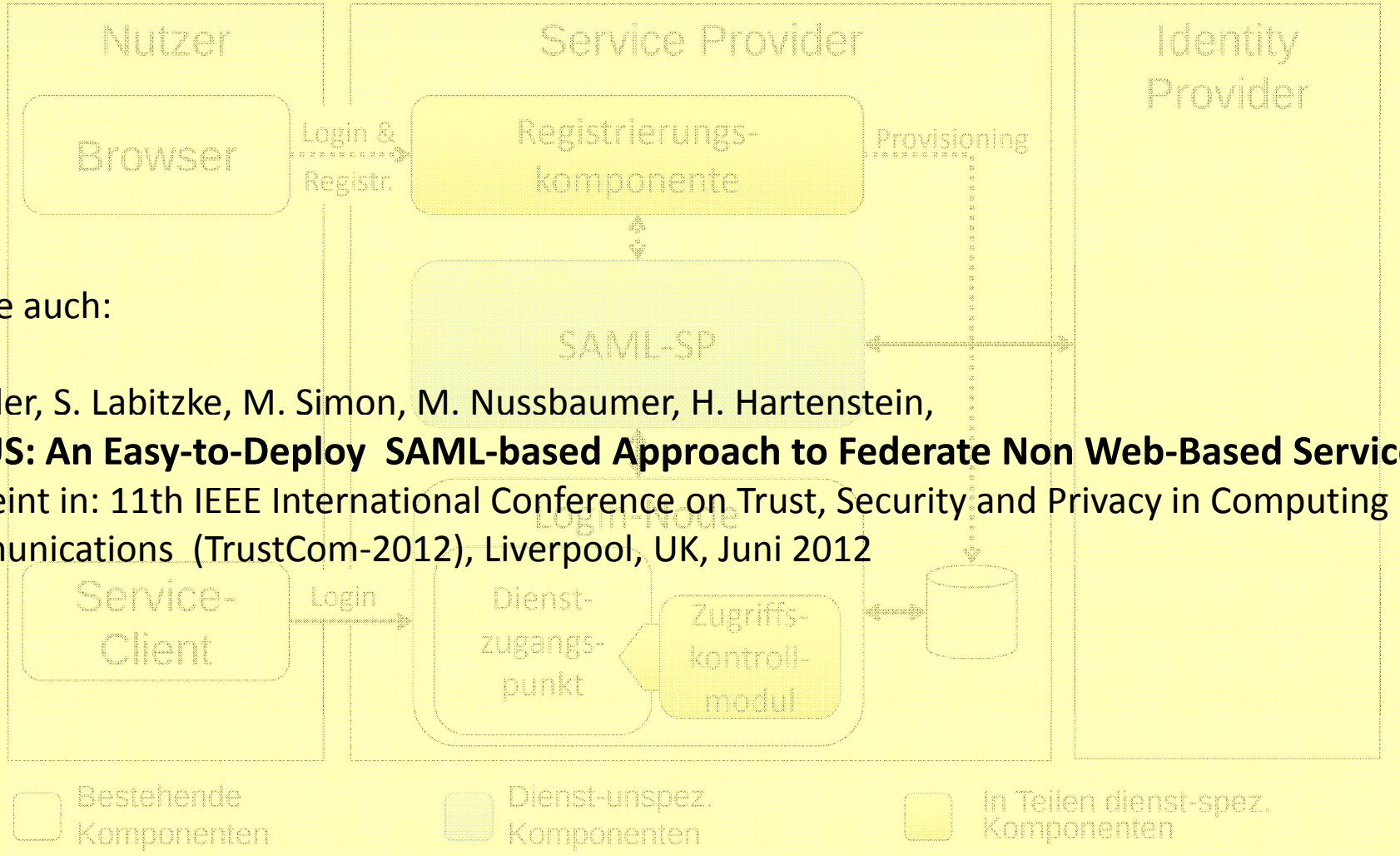
Ausblick – Verallgemeinerung des Konzepts

FACIUS (**F**ederated **A**ccess **C**ontrol **I**ntegration for **U**niversal **S**ervices)



Ausblick – Verallgemeinerung des Konzepts

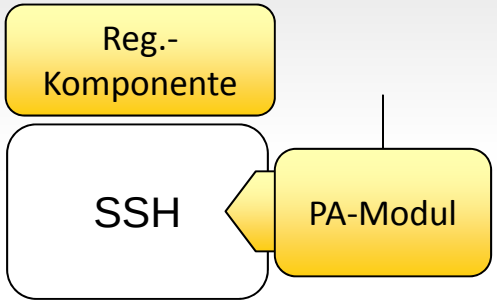
FACIUS (**F**ederated **A**ccess **C**ontrol **I**ntegration for **U**niversal **S**ervices)



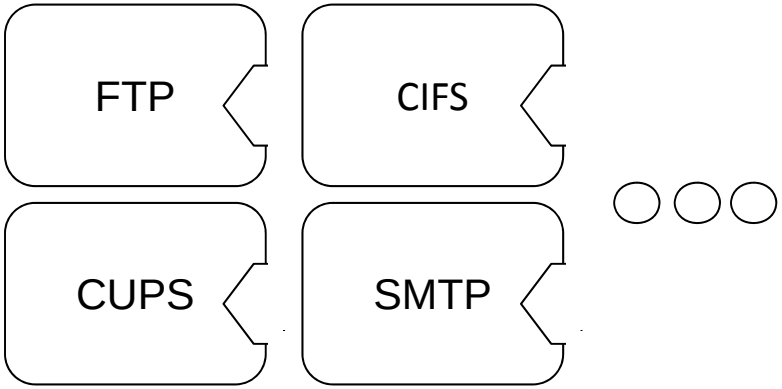
…siehe auch:

J. Köhler, S. Labitzke, M. Simon, M. Nussbaumer, H. Hartenstein,
FACIUS: An Easy-to-Deploy SAML-based Approach to Federate Non Web-Based Services,
Erscheint in: 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012), Liverpool, UK, Juni 2012

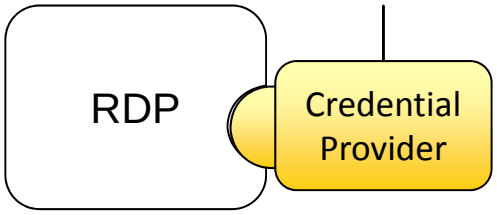
Ausblick – Übertragbarkeit auf weitere Dienste



- Reg.-Komponente und PA-Modul als Schnittstelle zum föderierten Dienst



- Föderieren von Diensten mit PAM-Unterstützung
  - PAM-Modul kann unverändert übernommen werden
  - Ggf. Anpassung der Reg.-Komponente nötig



- Föderieren von Diensten ohne PAM-Unterstützung
  - Verkapselung der Logik des PA-Moduls basierend auf weiteren Schnittstellen?

Zusammenfassung & Roadmap

- Zusammenfassung
  - Aufstellen eines Kriterienkatalogs für das bwIDM Projekt
  - Evaluation der föderativen Verfahren (FV) Moonshot und PAM/ECP+Erweiterungen entlang der Kriterien
  - Entwicklung und erfolgreiches Testen eines Proof-of-Concepts

- Roadmap
  - Finalisieren des FV und Einholen Datenschutz Gutachten (Zendas)
  - Zusammenschluss der BW-Landesuniversitäten mit ECP-fähigen Shibboleth IdP
  - Gespräche mit DFN über Zusammenarbeit in AAI
  - Bereitstellen erster ComputeCluster Dienste über PAM/ECP

Fragen und Diskussion

Herzlicher Dank an die weiteren Autoren:
T. Dussa und S. Labitzke (KIT),
H. Däubler und V. Nikolov (Univ. Ulm)
M. Klein (Univ. Freiburg)
J. Becker, M. Grandpre, M. Längle und D. Scharon (Univ. Konstanz),
H. Hartenstein (Projektverantwortung)