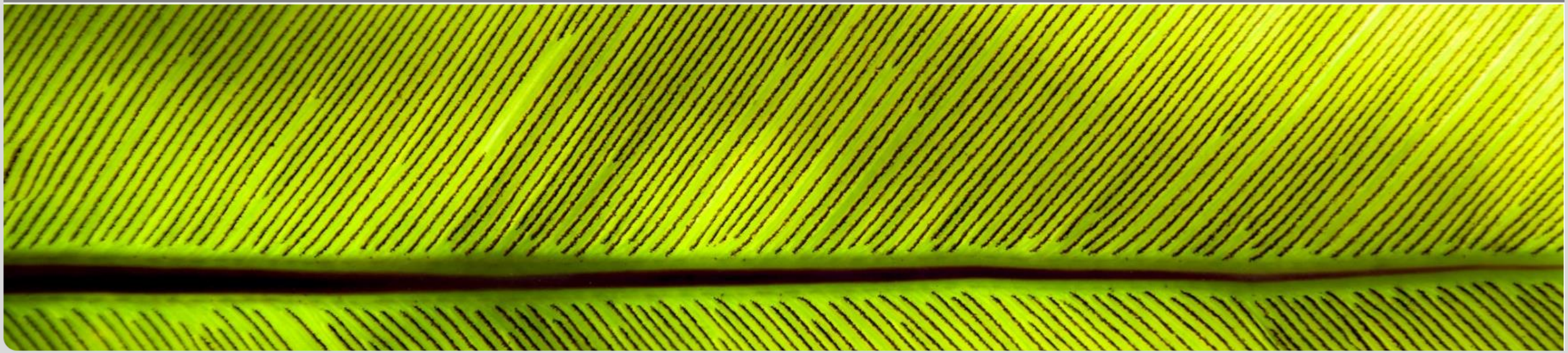
Karlsruher Institut für Technologie

HIFIS Workshop

Tag 1

Steinbuch Centre for Computing (SCC)



HIFIS Workshop Agenda

- 29. April 2019
  - 13:00 Ankommen, Snacks
  - 13:30 Begrüßung
  - 13:45 bwIDM: Technik, Policies, Entwurfsentscheidungen (inkl. Pause)
  - 17:00 bwDienste

- 30. April 2019
  - 9:00 Zusammenspiel HDF-AAI und bwIDM
  - 9:30 Diskussion (inkl. Pause)
  - 12:00 Snacks, Abschluss
  - 13:00 Ende

BEGRÜßUNG

PROJEKT BWIDM

Projekt bwIdm

- Laufzeit 2011-2013
- Finanziert vom MWK (Ministerium für Wissenschaft, Forschung und Kunst)
- Aus Folien „Arbeitssitzung: Organisation und IuK-Technik der Universitäten BW, 15.11.2011 (Martin Nussbaumer)“
  - Motivation: Beobachtbarer Trend zu verteilten Diensten in Baden-Württemberg
  - Ziel: bequemer Zugriff zu verteilten Diensten wie im lokalen Umfeld
  - Vision: Ein Forscher aus Baden-Württemberg kann verteilte BW-Dienste mit dem gewohnten lokalen Zugang nutzen
- 4 Kernteampartner, 5 Partner

Arbeitspakete

- AP1: Föderale Technologien
- AP2: Status Quo
- AP3: Interoperabilität mit bestehenden Föderationen
- AP4: Erweiterungsfähigkeit bwIDM
- AP5: Organisatorischer Rahmen
- AP6: Datenschutz und Sicherheit
- AP7: Schnittstellen und Datenmodell
- AP8: Integration lokaler IDMs in die Föderation
- AP9: Erstellen der Fachkonzepte

AP1: Föderale Technologien

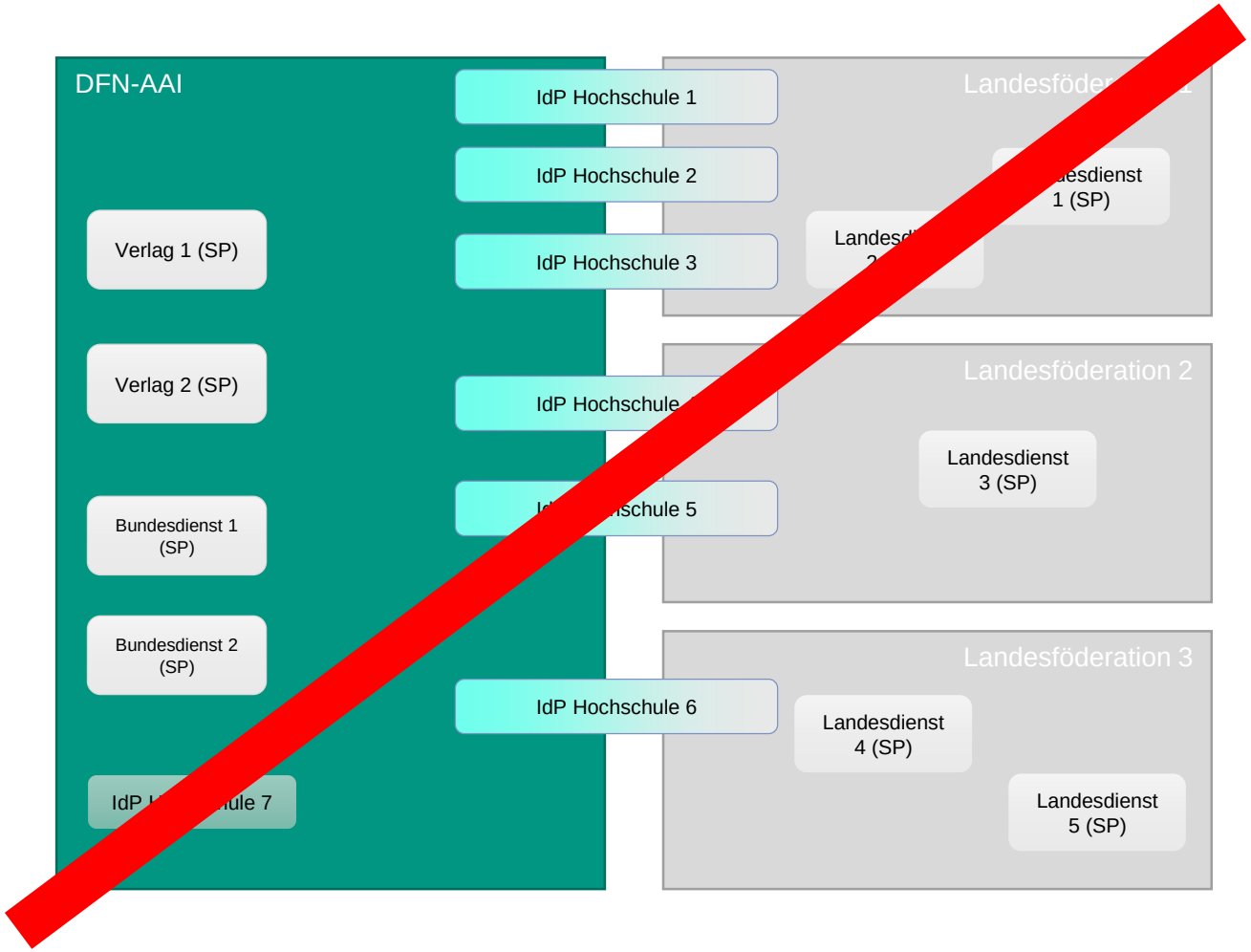
- Evaluation verschiedener Technologien, die einen föderierten Login ermöglichen
- Kerberos, Radius
  - Föderierter Login möglich
  - Keine Attributübertragung
  - Keine Föderationsverwaltung
- SAML/ Shibboleth
  - Proof of Concept SAML ECP als PAM Modul
  - Föderationsverwaltung bereits vorhanden: DFN-AAI
- Moonshot (Kombination aus Radius und SAML)
  - Während der Projektlaufzeit noch nicht einsatzbereit
  - Benötigte einen modifizierten SSH Client

AP2: Status Quo

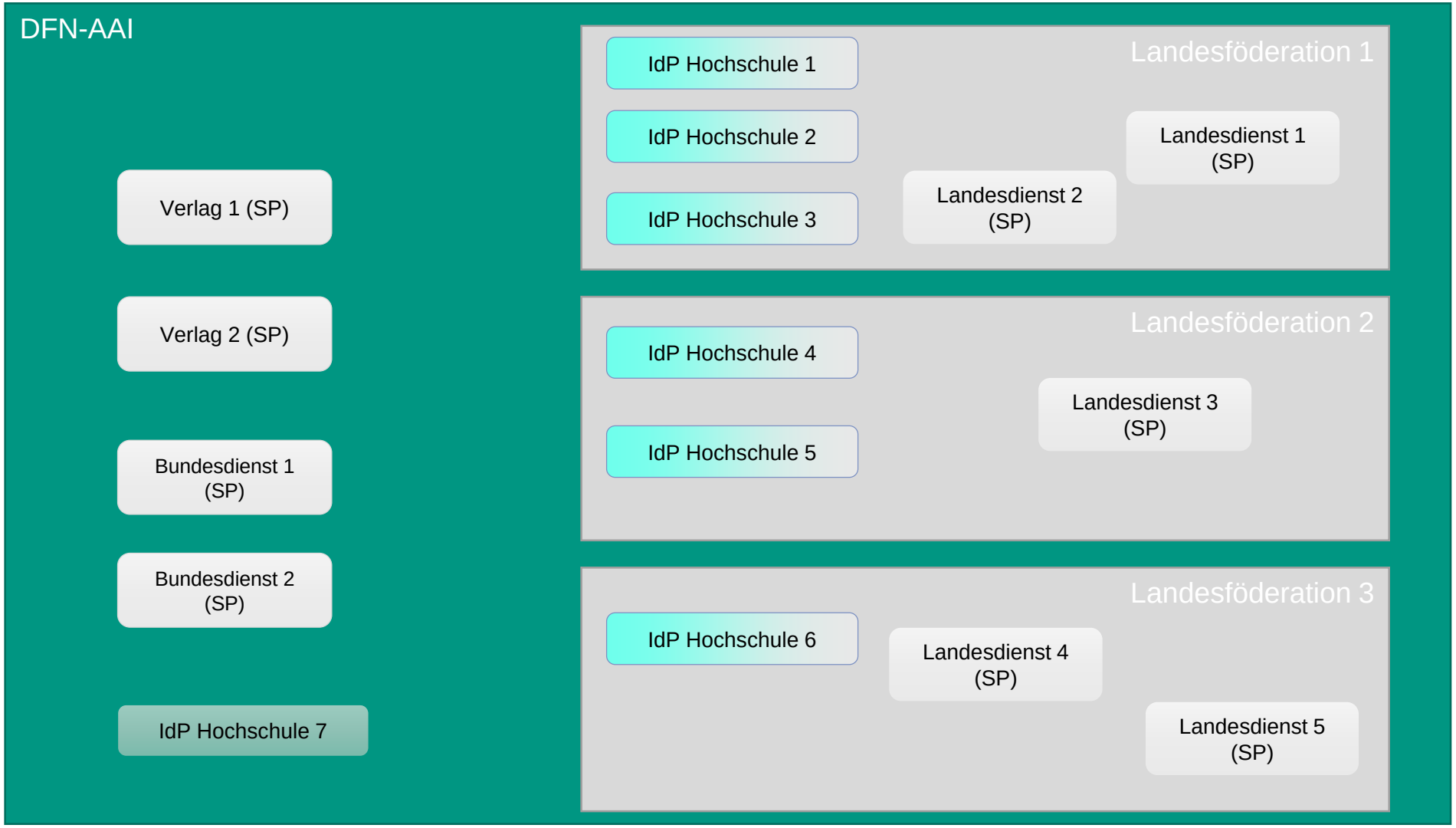
- Abfrage der vorhandenen Dienste
- Vorhandene Zugangsmechanismen
- Vorhandene IDMs, Identitätsdaten
- Wer darf aktuell welchen Dienst an welchem Standort nutzen?

AP3: Interoperabilität…

- Mit bestehenden Föderationen
- Evaluation möglicher Föderationsmodelle
  - Szenario Schwarzbuch
  - Szenario Föderation in Föderation
- Gespräche mit der DFN-AAI
  - DFN-AAI als Dach für die Länder
  - Definition der Protokolle durch die DFN-AAI
  - Empfehlung von Attributklassen und -werten
  - Pflege der Metadaten
- Zugehörigkeit über Entity Category



AP3: Föderation in Föderation

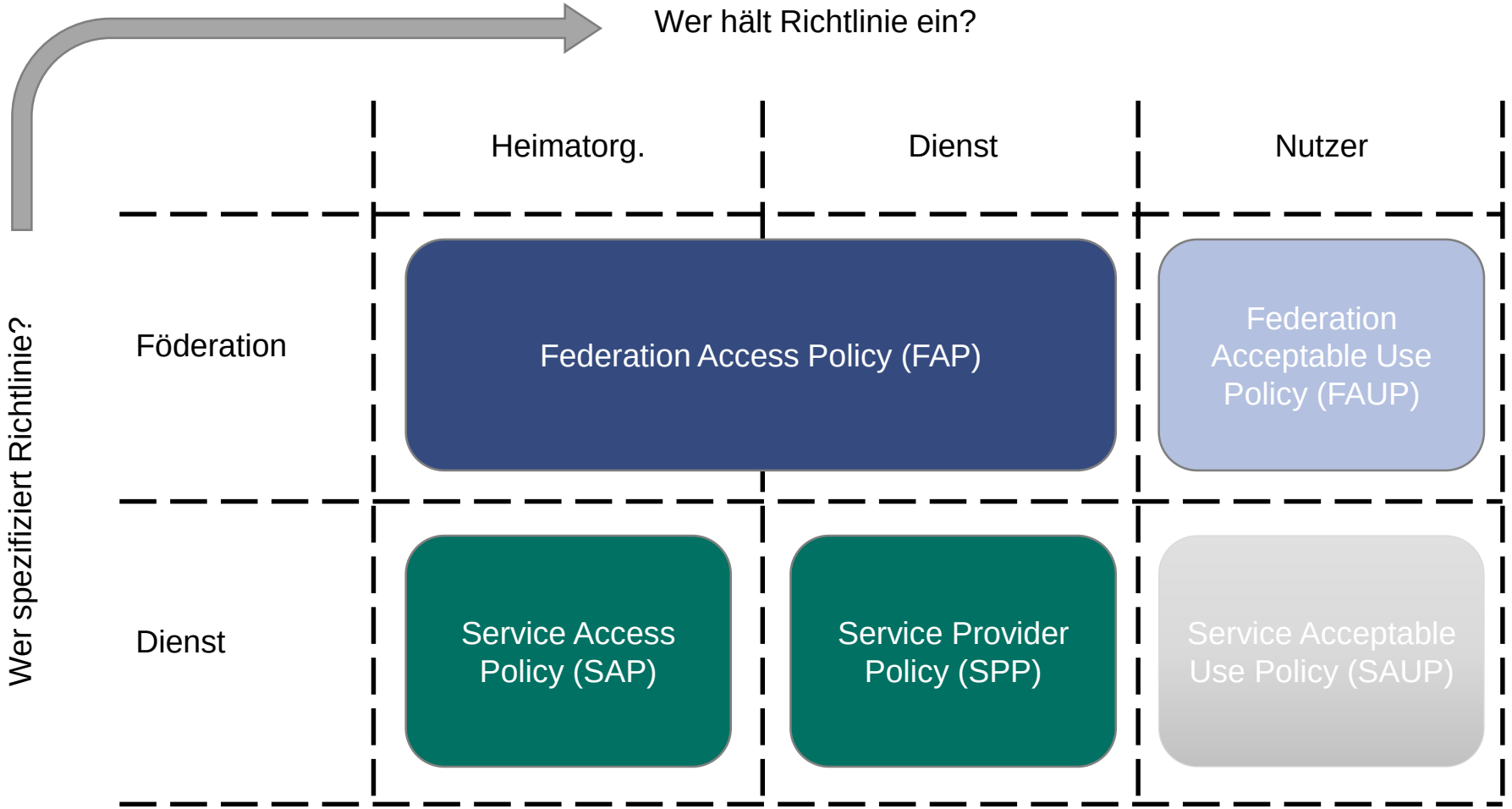


AP5: Organisatorischer Rahmen

- Rechtliche Grundlage
- Haushaltsrechtliche Regelungen
  - Wie wird untereinander verrechnet?
  - Wer bezahlt was?

- Nutzungsrechtliche Regelungen
  - Evaluation verschiedener Policymodelle

AP5: Policymodell



AP5: Organisatorischer Rahmen

- Ergebnisse
  - FAP: https://www.bwidm.de/wp-content/uploads/bwidm-fap-1.0.pdf
  - Aufnahmeantrag: https://www.bwidm.de/wp-content/uploads/bwidm-aufnahmeantrag-1.0a.pdf
  - SAP: https://www.bwidm.de/dienste/

- Governance
  - AK-IDM als operative Austauschplattform
  - ALWR als strategisches Gremium
  - bwIDM Geschäftsstelle

AP6: Datenschutz und Sicherheit

- Betrachtung Datenschutz durch die ZENDAS
  - Einsatz von uApprove bei den IDPs
  - Abgestimmter Text für die Freigabe zur Datenübermittlung
  - Verfahrensverzeichniseinträge an jedem Standort

- Evaluation der Sicherheit
  - SAML und ECP wurde als sichere Technologie evaluiert

AP7: Schnittstellen und Datenmodell

- Schnittstellen und Datenmodell großteils durch SAML und die DFN-AAI spezifiziert
- Definition weiterer Attribute
  - Definiertes Kürzel für die Heimateinrichtung
  - Primäre Gruppe
  - Sekundäre Gruppen
- https://www.bwidm.de/attribute/

AP8: Integration lokaler IDMs…

- In die Föderation

- Auftrag an die Heimatorganisationen
  - Anpassen des lokalen IDMs an die Erfordernisse von bwIDM
  - Etablieren einer SAML/ Shibboleth Infrastruktur
  - Teilnahme an der DFN-AAI Advanced

AP9: Erstellen der Fachkonzepte

- Gemeinsam mit den geplanten Diensten den Schulterschluss mit bwIDM planen
  - bwLSDF
  - bwSync&Share
  - bwUnicluster

Direkte Projektergebnisse

- Start der bwIDM Subföderation unter der DFN-AAI mit den neun Landesuniversitäten
- Policy und Governance Struktur etabliert
  - FAP, SAP, Geschäftsstelle, AK-IDM
  - Voraussetzungen zur Teilnahme an bwIDM
- Definition von notwendigen Attributen
- Dokumentation auf https://www.bwidm.de
- Erste Dienste bwSync&Share, bwFilestorage und bwUnicluster
  - Betrieb der reg-app

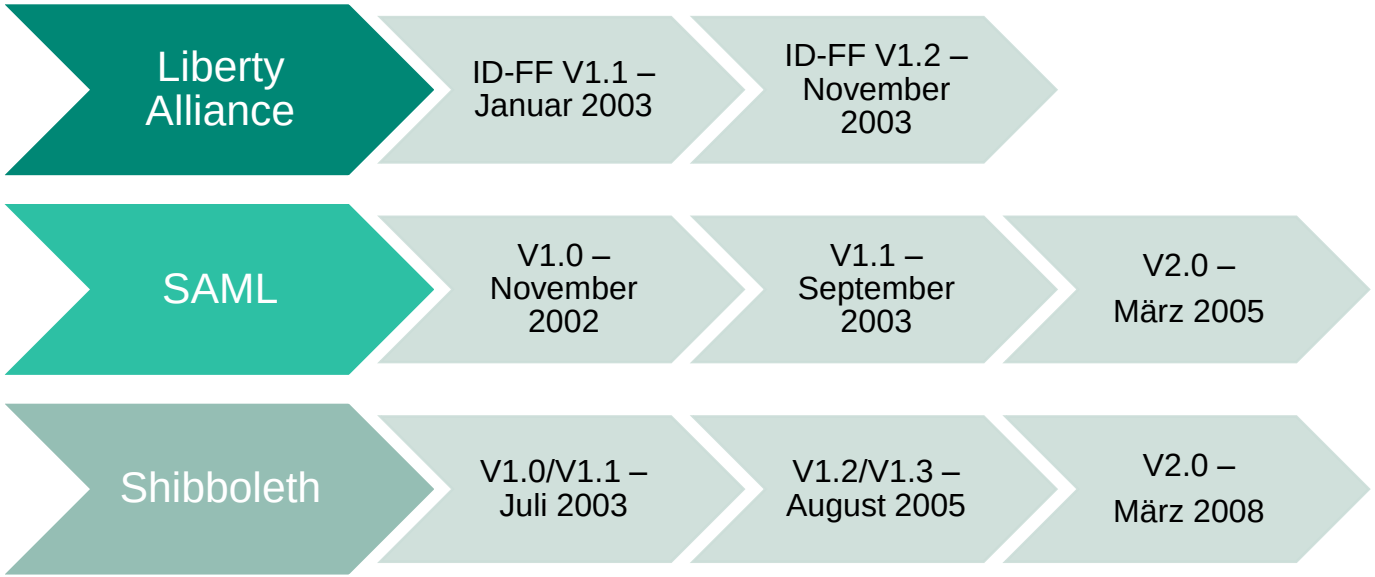
Nach Projektende

- Start der bwForcluster
  - Installation reg-app an den Forcluster Standorten
- Aufnahme weiterer Heimatorganisationen, die an das MWK angeschlossen sind
  - FHs, PHs,…
  - Inzwischen 48 Teilnehmer
- Weiterentwicklung reg-app
  - Anpassungen für Betrieb mit ZAS
  - Bugfixing
  - Verbesserungen

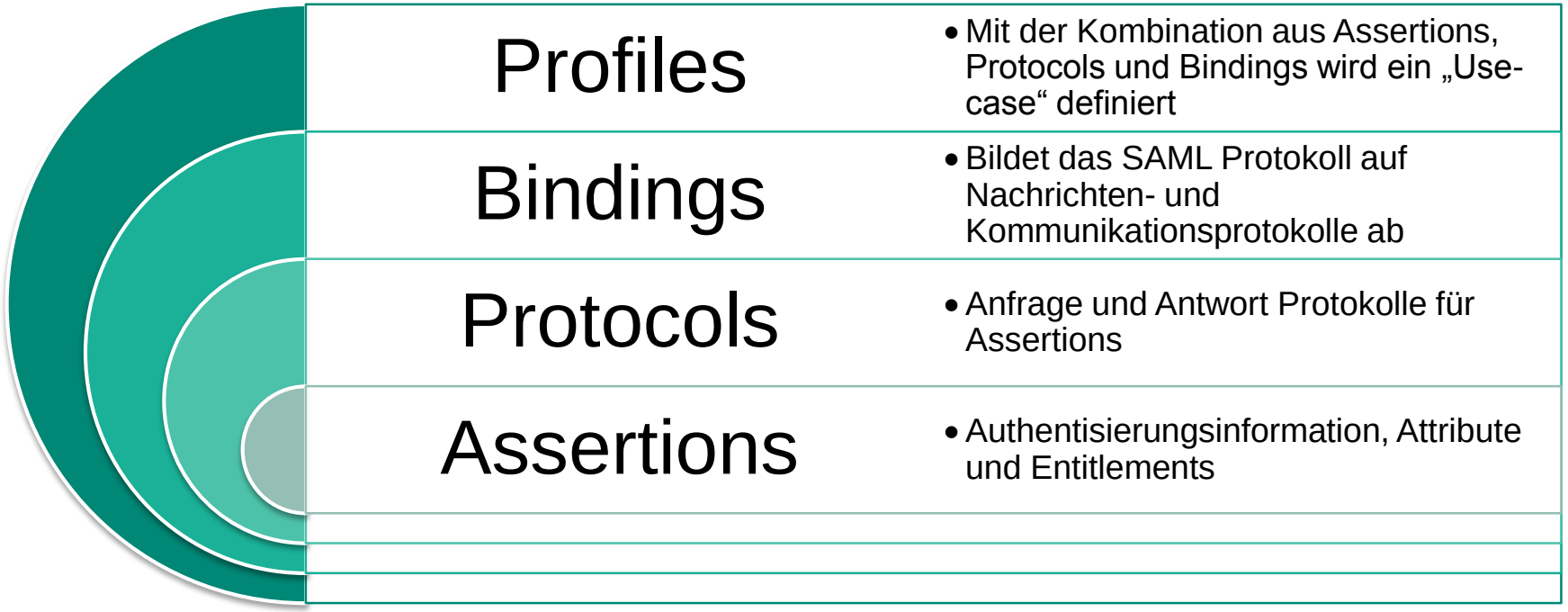
SAML/ SHIBBOLETH

SAML

- Security Assertion Markup Language
- XML-basiert
- OASIS (Organization for the Advancement of Structured Information Standards)
- Dient zum Austausch von Authentifizierungs- und Autorisierungsinformationen über institutionelle Grenzen hinweg
- Bietet Profile für einige Use-cases, ist aber zusätzlich erweiterbar



SAML Komponenten



Authentication Context

- Definiert Art und Weise der Authentifizierung

Metadata

- Konfigurationsdaten für Service- und Identityprovider

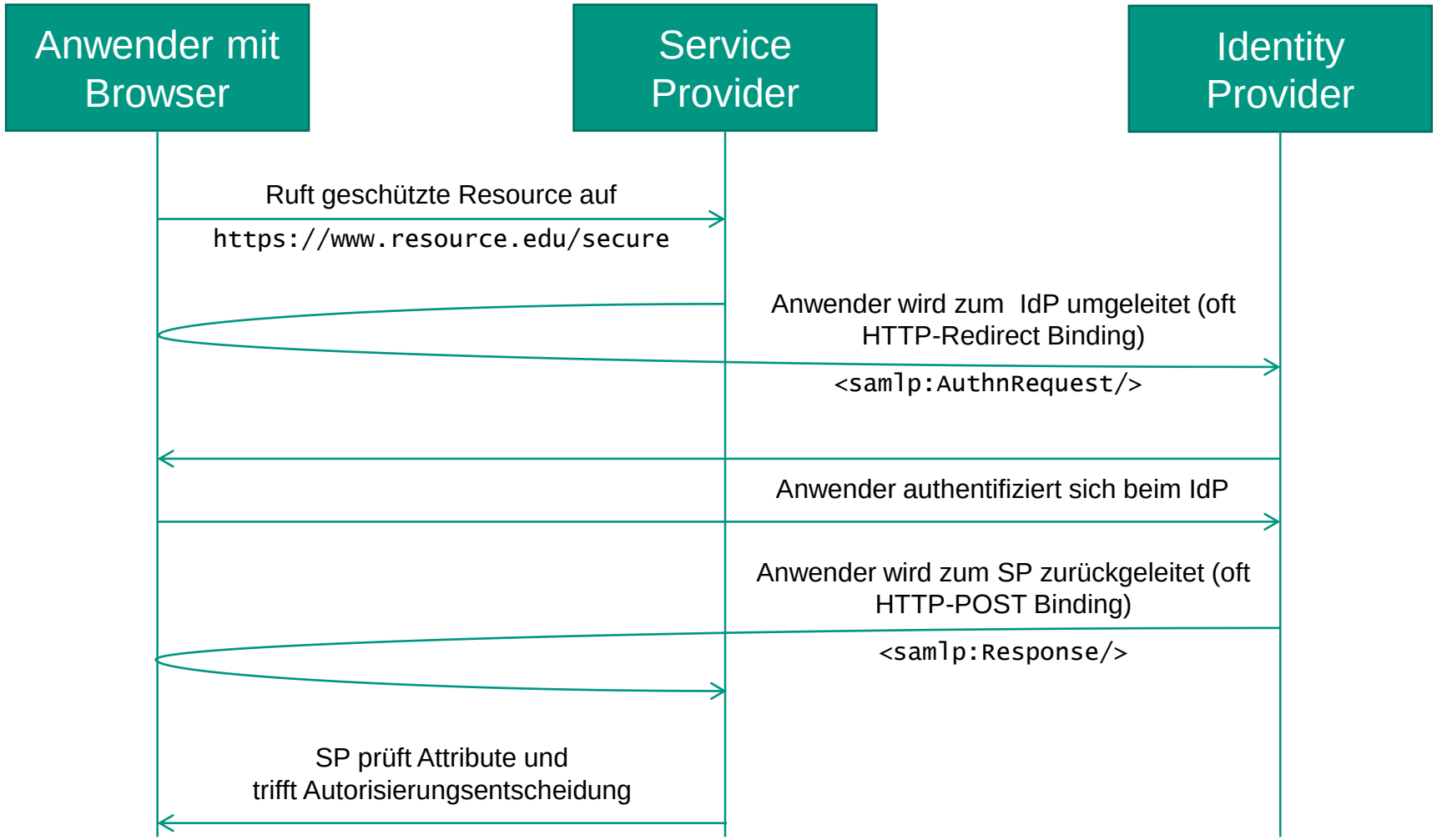
SAML Begriffe

- Asserting Party/ Identity Provider (IdP)
  - Generiert und verwaltet identitätsbezogene Daten und Assertions
  - Bietet Authentisierung von Principals ggü. Service Providern
- Relying Party/ Service Provider (SP)
  - Bietet z.B. Zugriff auf geschützte Ressourcen bzw. Services
  - Braucht identitätsbezogene Informationen für Autorisierungsentscheidungen
- Metadaten
  - Beschreibende Daten über die Parteien
  - Z.B. Zertifikate, Kontakte, Namen, Protokolle, Endpunkte, …

SAML Profile - WebSSO

- Bietet Single Sign On für browserbasierende Webapplikationen
- Benutzer mit Browser will auf eine geschützte Resource beim Service Provider zugreifen
- Er wird an einen Discovery Service weitergeleitet, dort wählt er seinen IdP
- Er wird zum IdP weitergeleitet
- Der IdP authentisiert ihn
- Er wird wieder zum Service Provider weitergeleitet
- Dabei kommen folgende Kombinationen zum Einsatz:
  - Protocol: Authentication Request Protocol
  - Binding: HTTP Redirect, HTTP POST, HTTP Artifact

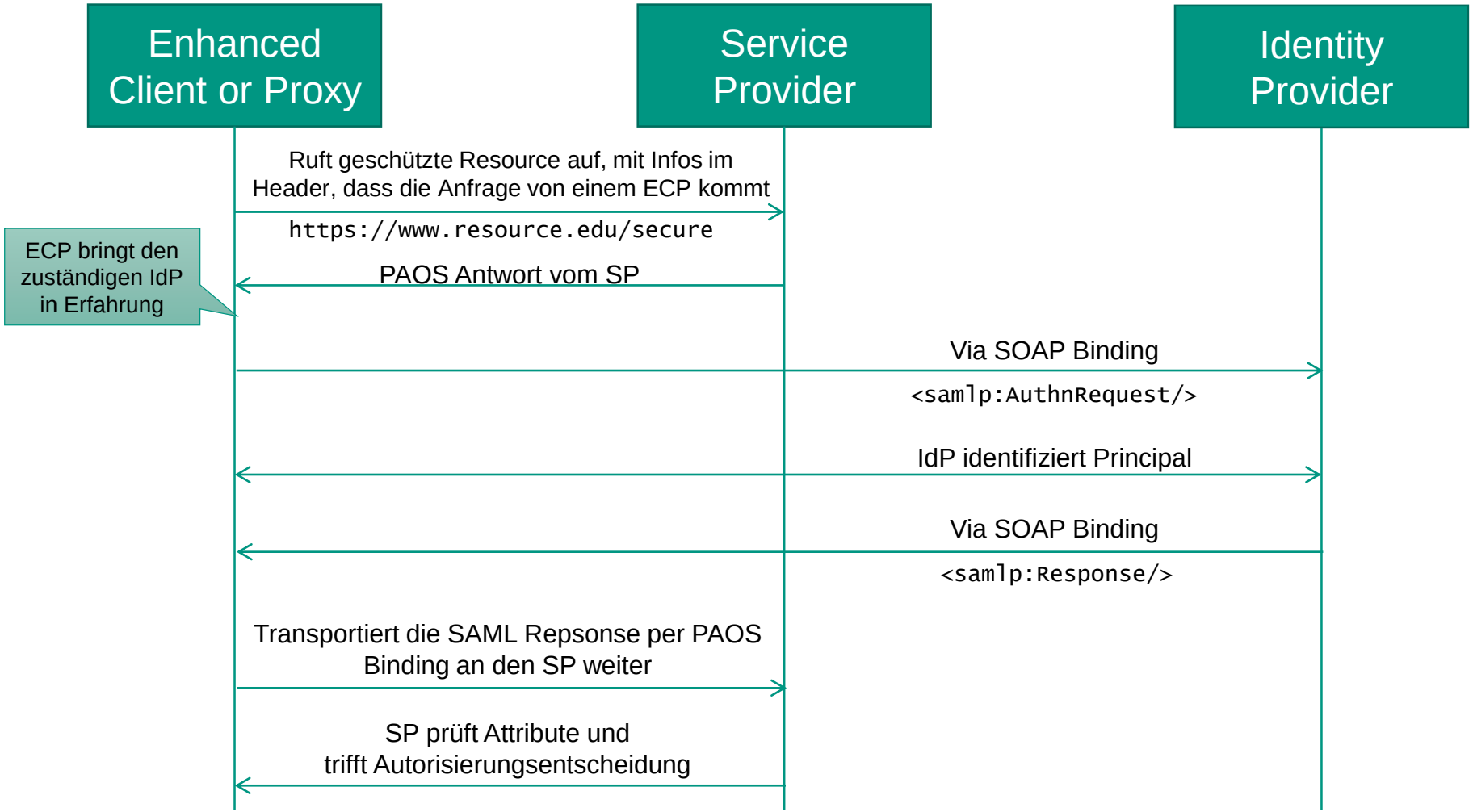
SAML Profile – WebSSO: Ablauf



SAML Profile - ECP

- Enhanced Client or Proxy Profile
- Als Enhanced Client wird ein User-Agent bezeichnet, der Funktionalität des Profils direkt unterstützt
- Ein Enhanced Proxy simuliert einen Enhanced Client, falls ein User-Agent das Profil nicht unterstützt oder unterstützen kann
- Ist für Anwendungen gedacht, die nicht browserbasiert sind und deswegen nicht das WebSSO Profil verwenden können

SAML Profile – ECP: Ablauf



SAML Profile - Assertion Query/Request Profile

- In diesem Profil sind einige Anfragen zusammengefasst
  - Am häufigsten verwendet: samlp:AttributeQuery
- Mit einer AttributeQuery kann man Benutzerdaten abfragen
  - Mit einer persistentID und einem StoredPersistentIdGenerator im IDP
  - Dokumentation DFN AAI Wiki

BWIDM BEISPIELE

Zugang bwHPC (bwUnicluster)

- Benutzer registriert sich für den Dienst auf https://bwidm.scc.kit.edu
  - SAML WebSSO
- Benutzer kann sich auf dem Unicluster einloggen
  - Mit seinem Heimatpasswort via ECP (Enahnced Proxy)
  - Mit einem gesetzten Dienstpasswort
  - In Zukunft mit hinterlegtem SSH Pubkey?
  - Bei Dienstpasswort oder SSH Pubkey erfolgt AttributeQuery
- Benutzer muss innerhalb 14 Tage die Umfrage bei der ZAS ausfüllen
  - ZAS verwendet SAML WebSSO

Zugang bwHPC (Forcluster)

- Benutzer beantragt Vorhaben auf der ZAS Webseite
  - Einloggen via SAML WebSSO
- Nach Genehmigung registriert sich der Benutzer bei der reg-app am passenden Forcluster Standort
  - SAML WebSSO
- Im Hintergrund wird das Projekt von der ZAS abgefragt und der Benutzer in die passende Gruppe eingefügt
- Benutzer kann sich einloggen (wie Unicluster)

Zugang bwSync&Share

- Benutzer registriert sich auf https://bwidm.scc.kit.edu für bwSync&Share
  - SAML WebSSO
- Danach Nutzung
  - Über Webinterface https://bwsyncandshare.kit.edu mit SAML Web SSO
  - Über den Client mit SAML ECP (Enhanced Client)

Für nicht SAML ECP fähige Dienste

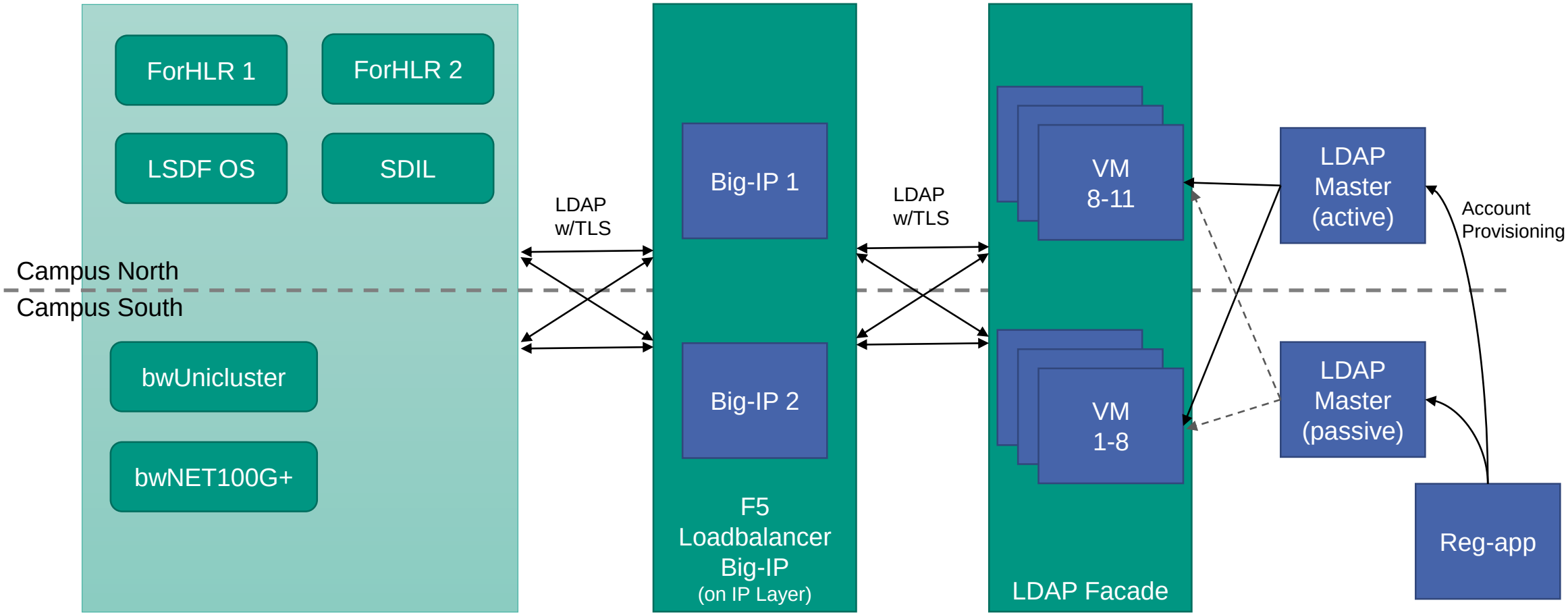
LDAP FACADE

Aufteilung der Komponenten

Teil B: Nutzung des Dienstes

- Dienst spricht selbst kein SAML ECP
- Erste Version war ein PAM Modul in Python
  - Modul mit ECP Funktionalität
  - Skepsis ggü. PAM Modul auf HPC Betreiber Seite
  - Autorisierung muss komplett nachgebildet werden
- Lösung: LDAP Facade
  - Bietet HPC-seitig eine LDAP Schnittstelle
    - Leicht zu nutzen mit pam_ldap und nss_ldap
  - Implementiert nicht selbst SAML ECP
  - Fragt die reg-app
    - Komplette SAML Konfiguration dort bereits vorhanden
    - Autorisierungsregeln ebenfalls

Betrieb LDAP Facade am KIT



Karlsruher Institut für Technologie

Software für föderiertes Identitätsmanagement

TECHNIK REG-APP

Funktionalität reg-app

- Reg-app ist eine Art Identitätsmanagement System
  - Im Gegensatz zu den meisten IDM Systemen nicht aktiv
  - Benutzer bringt initial seine Daten via SAML Web SSO
  - Durch einen persistenten Identifier kann der Benutzer dann aktualisiert werden
- Anbindung mehrerer Dienste möglich
  - Erweiterbar durch modulare Dienstprovisionierung
- Sichtbarkeit der Dienste über Regeln
- Autorisierung der Dienste über Regeln
- Rollen
- Gruppen
- Anbindung externer Datenquellen

Verwendete Technik

- Java Enterprise (jee6)
- OpenJDK 8
  - Andere Versionen sollten funktionieren
- Application Server Wildfly 8
  - In kommender Version sind Abhängigkeiten minimiert
  - Sollte dann auch auf anderen Appservern laufen
- Verwendete Features
  - EJB 3.0
  - JPA, JTA (Persistence und Transaction API)
  - JMS (Messaging Service)
  - Timer API

Eingebundene Bibliotheken

- Drools - https://www.drools.org/
  - Als Regelengine
- Ldaptive - http://www.ldaptive.org/
  - Zur LDAP Kommunikation
- OpenSAML
  - SAML Kommunikation/Validierung
- Velocity
  - Templates
- Bouncy Castle
- Jsch

SAML Unterstützung

- Metadaten Download von URL
- Ein Metadaten Download repräsentiert eine Föderation
- Filtern der Metadaten
  - anhand einer Entity Category (bspw. bwIdm)
  - anhand einer Regel
- Cronjob für den Download über einen Zeitplan
- Dokumentation

- Unterstützte Protokolle (OpenSAML)
  - WebSSO, ECP, AttributeQuery
  - Persistent NameIDs (Encrypted und Plain)
  - Zukünftig: Abfrage und Bereitstellung einer Attibute Authority

Provisionierungsworkflows

- LDAP
  - Ohne/mit Dienstpasswort
  - Ohne/mit Gruppen
  - LDAP Werte mit Velocity Templating
  - Für komplexere Szenarien: Auflösung der LDAP Werte mittels Javascript (z.B. setzen der primären Gruppe mit bestimmtem Namensschema)
- PowerFolder
- OpenStack
- Zukünftig Nextcloud
- Dokumentation
- Interface

Gruppen

- Heimatorg Gruppen
  - Primäre Gruppe
  - Sekundäre Gruppen
- Lokale Gruppe
  - Lokale Gruppen sind an einen Dienst gebunden
  - Können mit zusätzlichen Diensten verknüpft werden (Kein Webinterface)
  - Können von einem Gruppenadmin Rolle des jeweiligen Dienstes verwaltet werden
- Gruppen aus externen Datenquellen
  - Wenn ein „group_key“ bei der Datenquelle konfiguriert ist
- Gruppen können bei Diensten gefiltert werden

Externe Datenquellen

- Nur eine Art von externer Datenquelle bis jetzt
  - HttpUrlSingleAttributeSource
  - Schickt ein HTTP Get Request an URL
  - Ergebnis muss JSON sein
  - Und in eine Map<String, String> passen
- Weitere Datenquellen möglich
  - Geplant ist AttributeQuery an weitere Attribute Authorities
- Fehlende Implementierungen
  - Verknüpfung Datenquelle mit Service per Admin Interface
  - Benutzerdatenquellen
- Interface

Deprovisionierung

- Thema auch DFN-AAI weit
- Bisher pragmatische Lösung
  - Ein IDP meldet den SAML Status Unknown Principal bei einer AttributeQuery
  - Die reg-app versteht das als Status „ON_HOLD“ für den Benutzer
  - Dieser Status wird auch an die gebuchten Dienste propagiert
  - Nach einer bestimmten Zeitdauer können die Dienste dann automatisch deregistriert werden
- IDP Konfiguration ist in diesem Fall einfach
  - In der Standardkonfiguration bei einem StoredIDConnector bereits implementiert
  - In der „pid“ Datenbanktabelle muss in die Spalte „deactivationDate“ ein Wert gesetzt werden
  - Wert selbst ist egal. Sobald ein Wert drin steht, meldet der IDP „Unknown Principal“
- Wird zukünftig erweitert um die schacUserStatus Lösung die DFN-AAI weit empfohlen wird

Karlsruher Institut für Technologie

HIFIS-Workshop: bwSync&Share

Klaus Scheibenberger, 29./30.04.2019

STEINBUCH CENTRE FOR COMPUTING – SCC

Prämissen für den Aufbau des Dienstes

- Der Dienst (Start 2014) unterliegt den europäschen/deutschen Datenschutzgesetzen
  - Vor Ort im KIT betrieben, Datenspeicherung im zentralen KIT-Fileservice

- Eingebunden in das Baden-Württemberg-weite föderierte Identitätsmanagement *bwIDM* (AAI, www.bwidm.de)
  - Dieses ist ein Subset der DFN-AAI
  - Einrichtungen gewähren ihren Nutzern die Dienstnutzung (durch Zuordnung von Entitlements)
  - Nutzer authentifizieren sich mit ihrem lokalen Account ihrer Heimateinrichtung (Identity Provider (IdP))

- Ausprägung
  - Standard-Speichervolumen (Quota) aktuell 25 GB
  - Externe Nutzer können eingeladen werden (keine eigene Quota)
  - Derzeit ca. 40.000 Nutzer

Erweiterung des Dienstspektrums

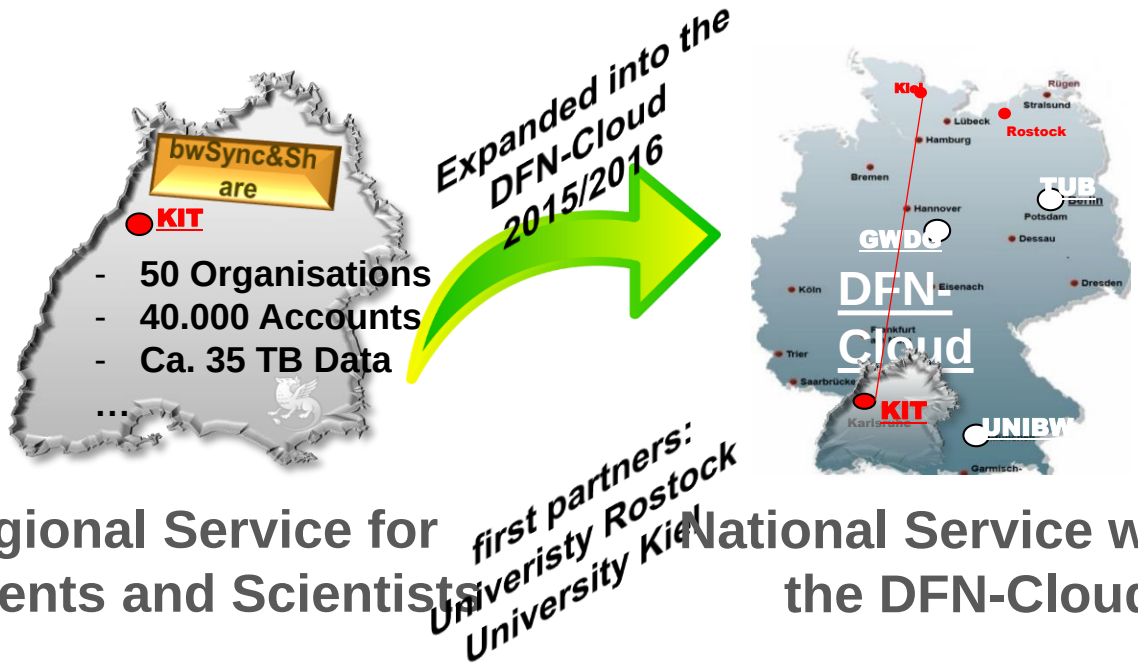
- Seit 2017: Integration von Onlv Office als Webediting-Tool zur kollaborativen Zusammenarbeit 

  - Sehr “nahe” an Microsoft Office Produkten (doc(x), xls(x), ppt(x)) aber auch odp, odt, ods, epub, csv
  - Permanente Synchronisierung von Änderungen in bwSync&Share

- Da bwIDM ein Subset der DFN-AAI ist, konnte der Dienst in 2015/16 problemlos auf Einrichtungen, die Mitglieder der DFN-AAI sind, erweitert werden. (“bwSync&Share in der DFN-Cloud”, s. www.dfn.de/dfn-cloud/syncshare-dienste/bwsyncshare/)

bwSync&Share in der DFN-Cloud

- Im Kontext von „bwSync&Share in der DFN-Cloud“ wurde ein Forschungs- und ein Erprobungsrahmenvertrag mit dem DFN geschlossen.
- Nutzende Einrichtungen schließen eine Erprobungsvereinbarung mit dem KIT.
- Anschließend erfolgt die technische Einbindung des IdP der Einrichtung in den Dienst.



www.dfn.de/dfn-cloud/bwsyncshare-in-der-dfn-cloud/

bwSync&Share in der DFN-Cloud

Nutzungsvertrag

Vor Beauftragung dieses Cloud-Dienstes muss mit dem DFN-Verein ein Rahmenvertrag zur Nutzung von föderierten Cloud-Diensten abgeschlossen werden.

Verantwortliche Einrichtung

Karlsruher Institut für Technologie (KIT) / Steinbuch Centre for Computing (SCC)

Kurzbeschreibung

Das KIT / SCC entwickelt mit „bwSync&Share in der DFN-Cloud" eine für die Zwecke von Forschung und Lehre maßgeschneiderte externe Storage-Cloud mit Diensten zur Dateiablage und -synchronisation über verschiedene Endgeräte. Der Dienst basiert auf der Anwendung PowerFolder der Firma dal33t GmbH.

Durch die Integration von OnlyOffice können über die Webschnittstelle auch ohne Installation einer Office-Suite auf dem Endgerät Office-Dokumente bearbeitet werden. Über das Synchronisieren und Teilen von Dateien hinaus ist damit auch ein gemeinsames, gleichzeitiges Bearbeiten von Office-Dateien möglich.

Nach Schaffung der im Dienstprofil beschriebenen Voraussetzungen seitens des Erprobungspartners erfolgt die Bereitstellung des Dienstes innerhalb eines Monats.

Dienstprofil

Weitere Informationen zu diesem Dienst stellt das KIT / SCC bereit: Dienstprofil bwSync&Share in der DFN-Cloud.

Kostenumlage ....

Aktuelles

- Personenbezogene Daten
  - Gemeinsam mit der KIT-Rechtsabteilung und dem Datenschutz-Team wurde ein **Nutzungsvertrag** und eine **AV-Vertragsvorlage** für den Dienst **bwSync&Share für die Einrichtungen im Land** entwickelt.
  - Der Abschluss eines AVV (getriggert von) einer Einrichtung mit dem Dienstbetreiber (KIT) ist notwendig, wenn in einem Verfahren (dieser Einrichtung) der Dienst zur Speicherung personenbezogener Daten genutzt werden soll. (Zur Vereinfachung stellen wir nun eine entsprechende Vorlage zur Verfügung.)
  - Teil des AVV sind u.a. die technischen und organisatorischen Maßnahmen (TOM)
- Ziel: „Selbsttragender“ Landesdienst (ab 2020)
  - D.h. Übergang zu einem Dienst, der nicht mehr als ein vom Ministerium für Wissenschaft und Kunst gefördertes Projekt, sondern eigenständig durch die Einrichtungen im Land finanziert wird („Pauschalmodell“).
- Nextcloud-Evaluierung

Details zu Nextcloud-Evaluierung

- Nextcloud unterstützt seit Mitte 2018 auch „Multiple IdPs“
  - Anbindung an bwIDM kann geprüft werden.
  - Weitere interessante Features:
    - Ende-zu-Ende Verschlüsselung (Zukunft; geteilte Ordner)
    - alternative S3-Speicheranbindung
    - Föderation zwischen Nextcloud Instanzen (Open Cloud Mesh)
- Aktuelle Testinstallation:
  - 3 Nextcloud- Server
  - 3 Redis-Server für Caching
  - 3 SQL-Server
  - 1 Splunk-Server für Monitoring
  - 1 ClamAV-Server für Antivirus
- Bisherige Erfahrungen
  - Stabiler Testbetrieb (bislang wenige Benutzer)
  - Sowohl Web als auch Clients funktionieren
  - Basiert auf PHP (nicht JAVA)
  - Ende- zu- Ende- Verschlüsselung noch nicht produktionsreif

Karlsruher Institut für Technologie

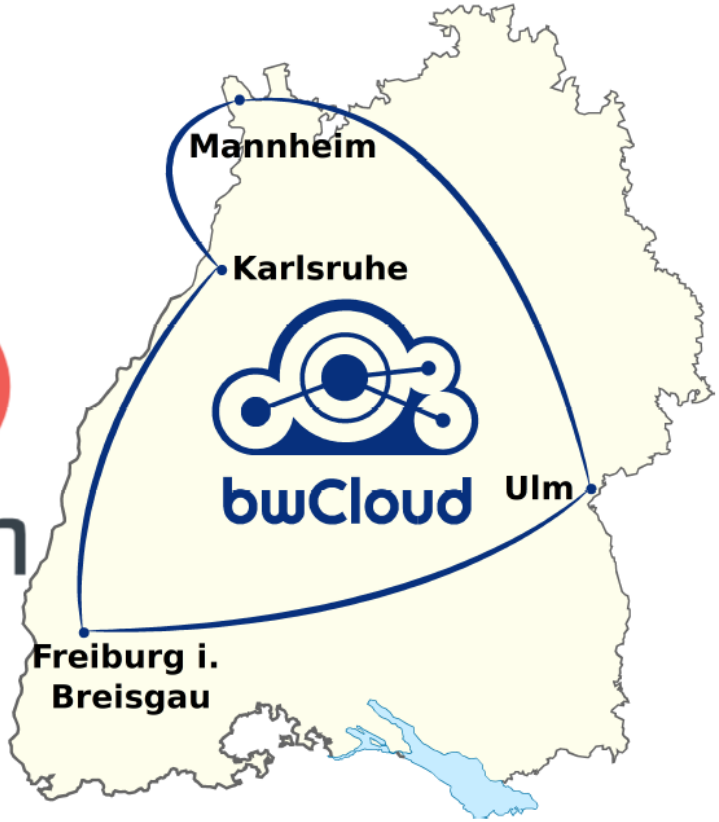
HIFIS-Workshop: bwCloud SCOPE

Klaus Scheibenberger, 29./30.04.2019

STEINBUCH CENTRE FOR COMPUTING – SCC

Die bwCloud – IaaS-Dienst für Hochschulen und Universitäten (s. bw-cloud.org)

- Betrieben von vier verschiedenen Betriebsstandorten und einer landesweiten Betriebsgruppe
- Technische Grundlage: CentOS (Red Hat), OpenStack, Ceph
- Vernetzt durch das Landes-hochschulnetz BelWü
- Angebunden an das föderierte Identitäts-management bwIDM



Auszug aus einem Foliensatz von
Janne Schulz (Projektleiter) für:
ZKI, AK „Zentrale Systeme“
Jahrestagung vom 6.-9. März 2018 in Göttingen

Openstack-Regions

- Das OpenStack Konzept der „Regionen“:
  - Vollständig eigene logische Umgebung mit eigenen Quotas für NutzerInnen, eigenen Netzen, Datenbanken usw.
- Jede Region betreibt eigene Dienste:
  - Compute, Netzwerk, Storage
- Gemeinsam genutzt:
  - Authentifizierung (Keystone)
  - Dashboard (Horizon)
  - Images (Glance)
    - wird von Freiburg aus regelmäßig via Cron gesynct

Auszug aus einem Foliensatz von
Janne Schulz (Projektleiter) für:
ZKI, AK „Zentrale Systeme“
Jahrestagung vom 6.-9. März 2018 in Göttingen

Nutzerkontexte, Use-Cases, Ziele

SCOPE

Science

- VMs für Forschungsprojekte und WissenschaftlerInnen
- Compute intensive Nutzung, z.B. für:
  → Pre- oder Post-processing von HPC Jobs
  → Ideal für Projekte & Kooperationen
- → große & sehr große Flavors

- **Aufräumen der „Neben-RZs“**
- **Verhindern Kauf/Miete teurer Cloud-Ressourcen**
- **Aufbauen von Expertise**

Operations (RZs)

- Keine Quota Limitierung
- Keine Limitierung der Nutzung (z.B. bei Aufbau eigener virtueller Netzwerkstrukturen)
- Exklusive Nutzung der Knoten (wenn verlangt / notwendig)

- **Reduktion von Lizenzzahlungen durch Migration in Cloud-Umgebung (bsp. Webserver?!)**
- **Beschleunigung von Dev- & Eval-Prozessen**
  → Aufbau echter DevOps Gruppe(n)

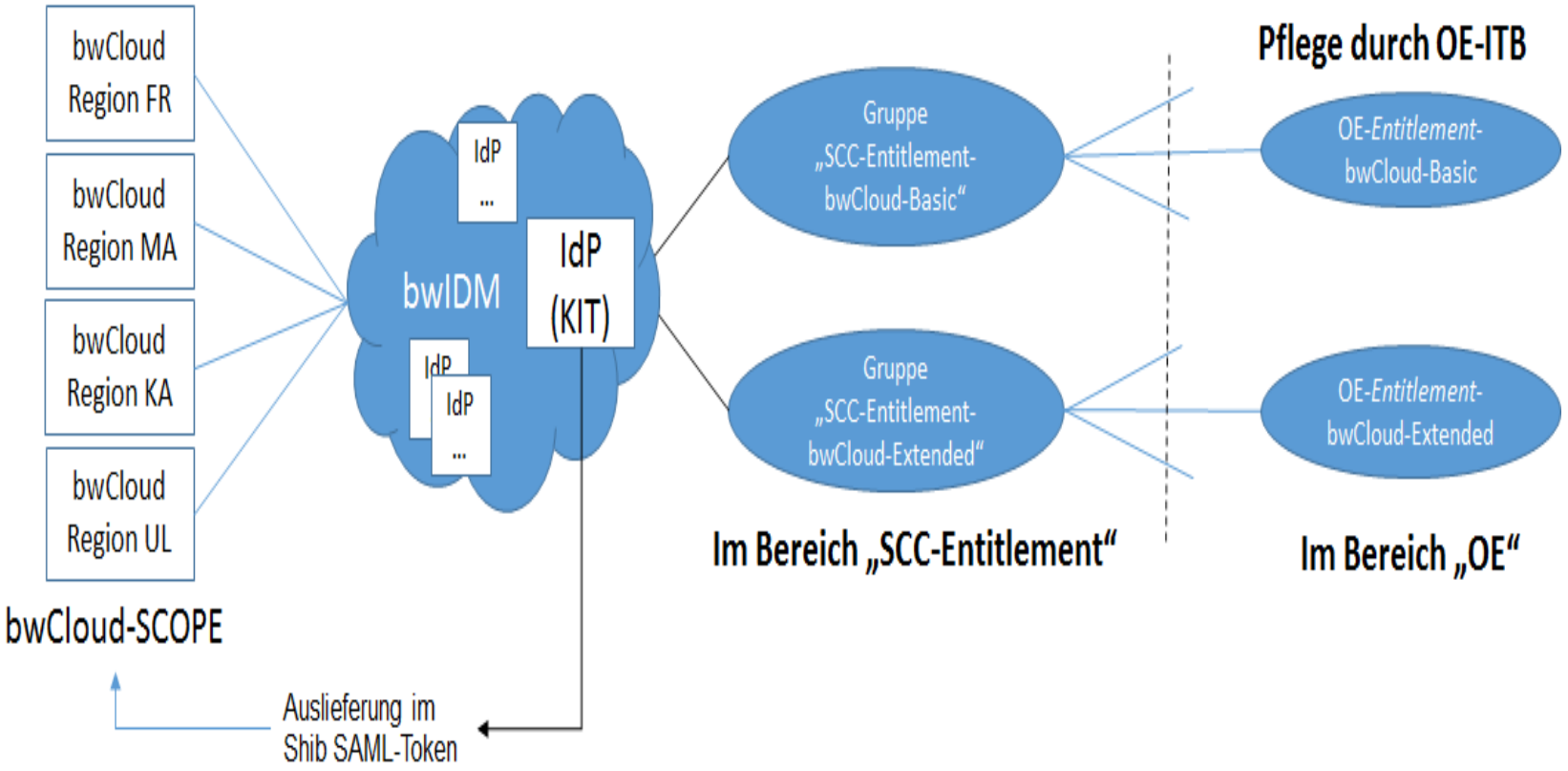
Education

- „Kleine“ VMs für Studis
  → Limitiertes Quota
  → Geteilte („shared“) Nutzung der physischen Hardware
- Gruppenprojekte für Lehr-/Lernsituationen

Auszug aus einem Foliensatz von Janne Schulz (Projektleiter) für:
ZKI, AK „Zentrale Systeme“
Jahrestagung vom 6.-9. März 2018 in Göttingen

bwCloud

Beispiel: Entitlement-Vergabe am KIT

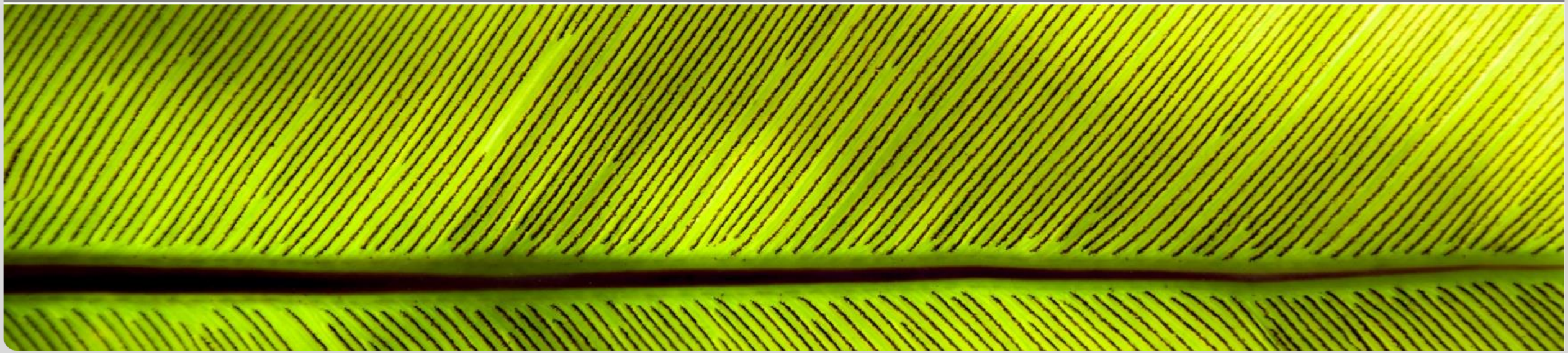


Karlsruher Institut für Technologie

HIFIS Workshop

Tag 2

Steinbuch Centre for Computing (SCC)

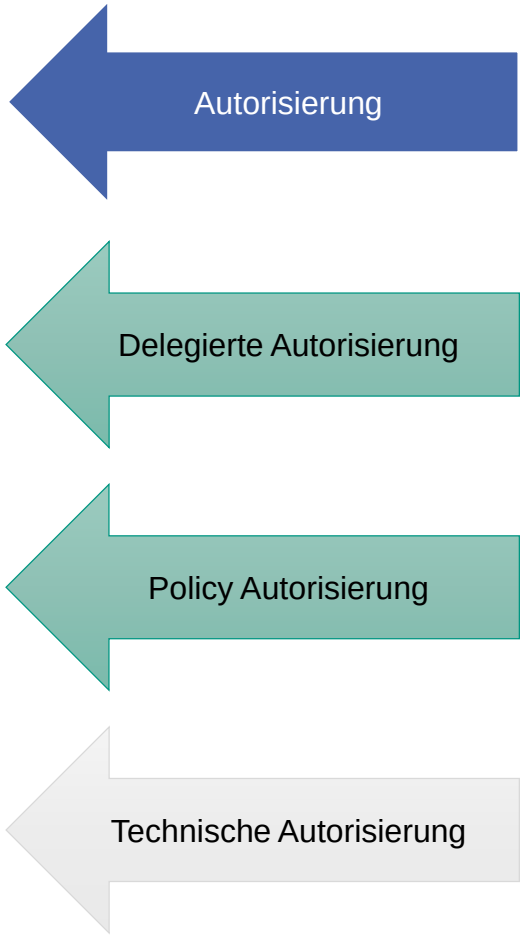


HIFIS Workshop Agenda

- 29. April 2019
  - 13:00 Ankommen, Snacks
  - 13:30 Begrüßung
  - 13:45 bwIDM: Technik, Policies, Entwurfsentscheidungen (inkl. Pause)
  - 17:00 bwDienste

- 30. April 2019
  - 9:00 Zusammenspiel HDF-AAI und bwIDM
  - 9:30 Diskussion (inkl. Pause)
  - 12:00 Snacks, Abschluss
  - 13:00 Ende

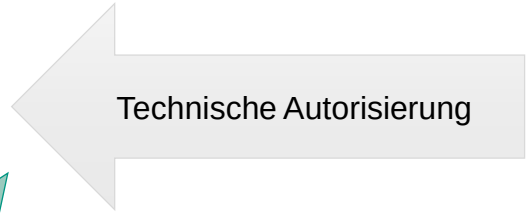
HDF-AAI UND BWIDM



- Autorisierung
  - Formale Richtlinien/ Förderkriterien
  - Verrechnung
- Delegierte Autorisierung
  - Community Verwaltung
  - Verwaltung von Projektmitgliedern durch delegierte Person (z.B. PI)
- Policy Autorisierung
  - z.B. Anerkennen lokaler Policies
  - IuK-/ Benutzerordnung, Dienst AGBs, SAUP, …
- Passwort Policy
  - Technische Autorisierung
  - Zugangsprüfung durch übermitteltes Attribut

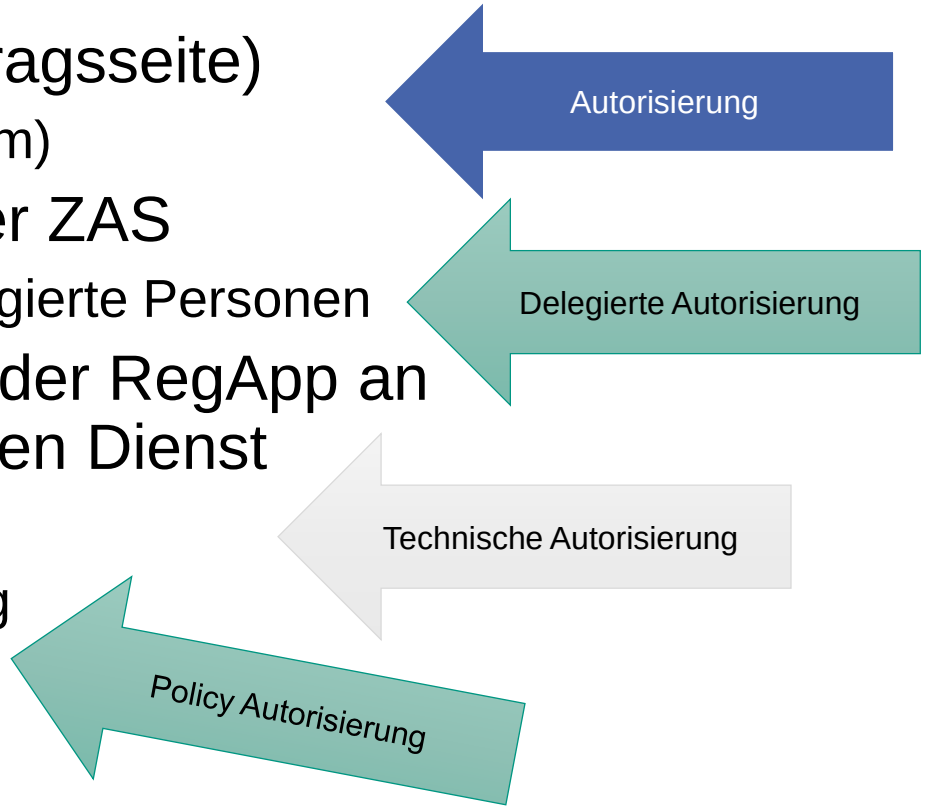
bwIdm Flächendienste

- Flächendienste: Dienste mit höheren Nutzerzahlen
  - z.B. bwSync&Share
- Autorisierung für Flächendienste an der Heimatorganisation
  - Kriterien legt der Dienst fest
  - z.B. Mitarbeiter und Studenten, keine Gäste
- Übertragung als Attribut (entitlement)
- Benutzer registriert sich bei der RegApp am KIT für bwSync&Share
  - Attributprüfung in der reg-app
  - Anerkennen der lokalen Benutzerordnung



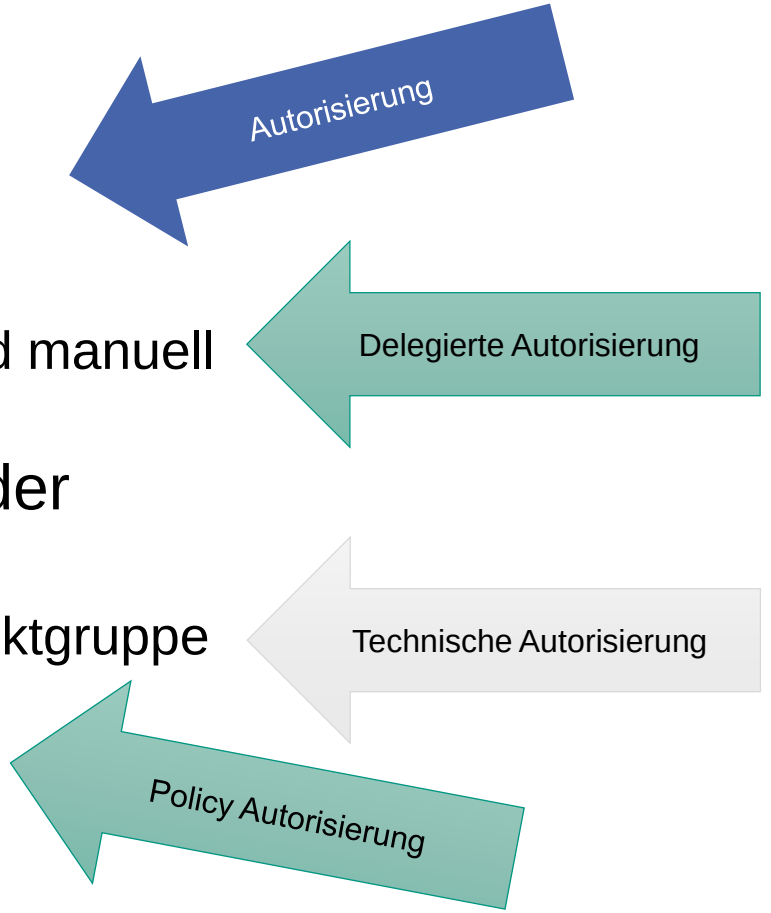
bwIdm HPC (Forcluster)

- Projektantrag über ZAS (Zentrale Antragsseite)
  - Prüfung durch CAT (Cluster Auswahl Team)
- Verwaltung der Projektmitglieder in der ZAS
  - Projektmanager (Antragssteller) und delegierte Personen
- Projektmitglieder registrieren sich bei der RegApp an den HPC Standorten für den passenden Dienst
  - Autorisierung durch Abfrage bei der ZAS
  - Anerkennen der lokalen Benutzerordnung



ForHLR

- Projektantrag
  - Prüfung durch HLRS Lenkungsausschuss
- Anlegen der Projektgruppen
  - Werden direkt in der RegApp angelegt und manuell verwaltet
- Projektmitglieder registrieren sich bei der RegApp am KIT für den ForHLR
  - Autorisierung durch Mitgliedschaft in Projektgruppe
  - Anerkennen der lokalen Benutzerordnung
-
- HDF Integration

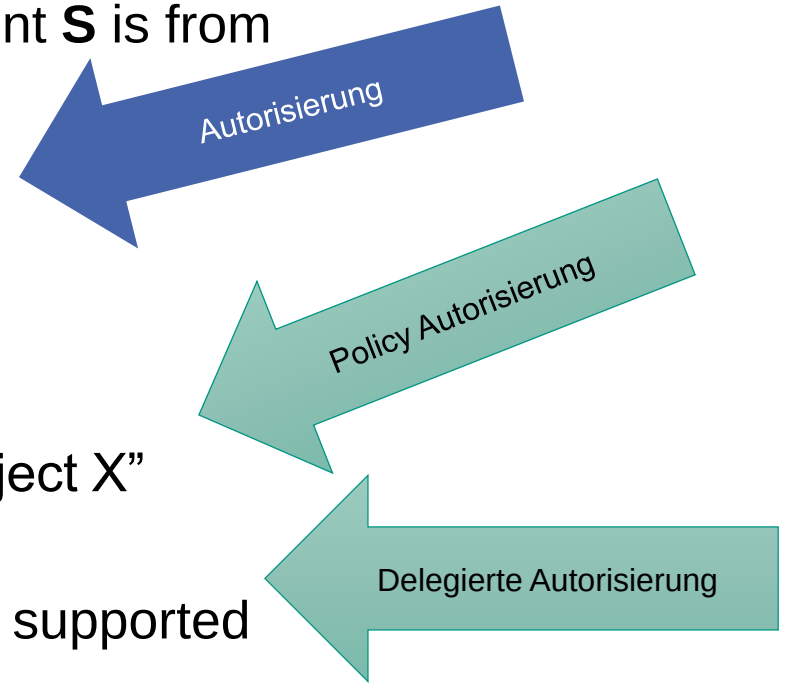


HDF-AAI

- Unterstützung von weltweiten Nutzern
  - Erfordert explizite Behandlung von "Assurance"
- Unterstützung von non-web Diensten
  - Erfordert Protokolle jenseits von SAML (z.B. via TTS oder Proxy)
- Abbildung von existierenden Prozessen (in HPC, Grid, Cloud)
  - Erfordert Integrationsarbeit (und gute Nerven :D)
  - Aktuell: Prototypische Integration von Produktionsdiensten am KIT
    - LSDF
    - ForHLR 2

HDF-Integration

- Principal investigator “PI” runs a scientific project (“project X”) with partners across multiple centres
  - *Analogy: Service in RegApp managed by PI*
  - Project is managed in the community proxy (e.g. unity)
  - E.g.: **PI** is from DKFZ, Postdoc **Doc** from DESY and Student **S** is from Uni Strasbourg
- PI writes proposals for resources at other centres
  - *Analogy: "ZAS" Antrag, HLRS Lenkungsausschuss*
  - => Obtains 10 MCPUh in Jülich + 100 TB at KIT
- PI authorises Doc and S
  - <=> adds him to his group => gives them the attribute “project X”
  - Sites typically support "project X" via authorization groups
  - Doc and S can access all resources **wherever** project X is supported



Unterschiede, Schwerpunkte

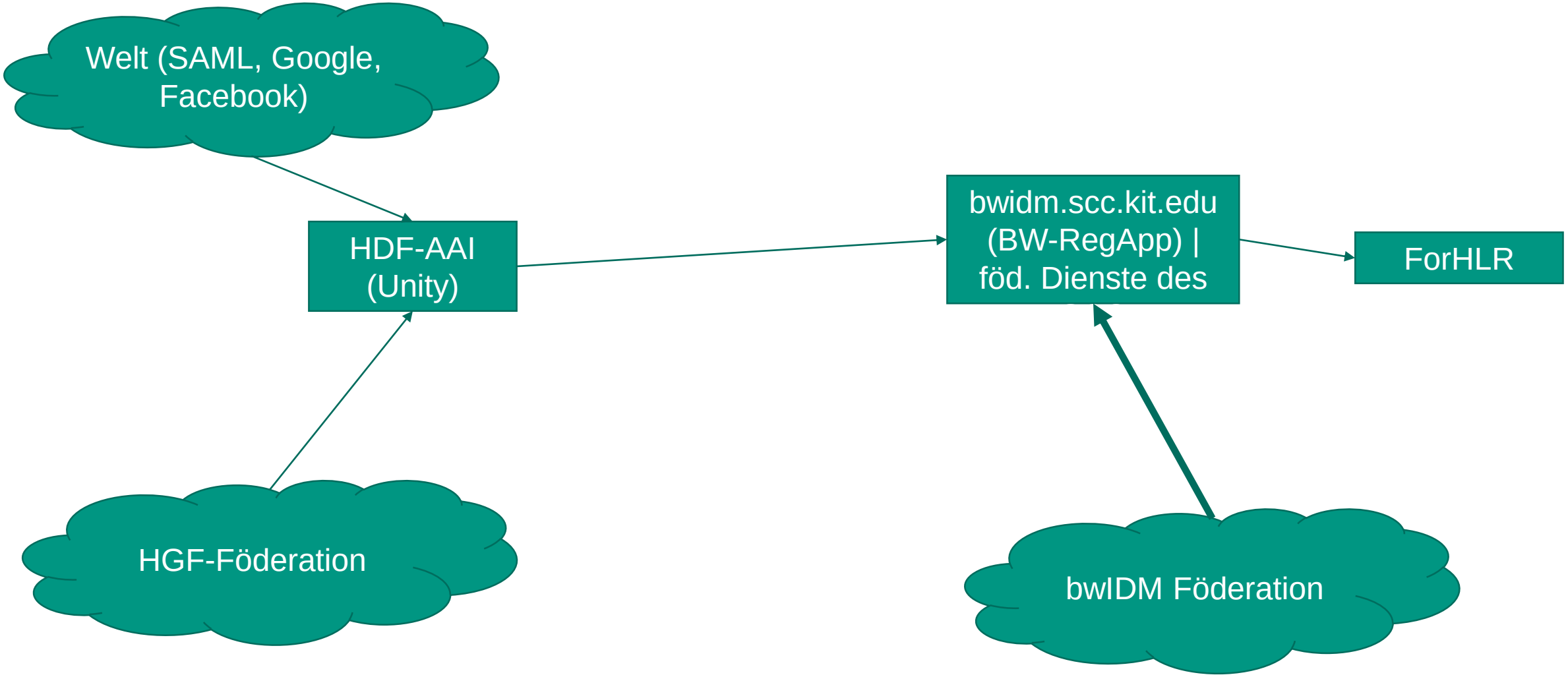
bwIdm

- Fokus auf Dienste
  - Nutzung für Flächendienste, durch Delegation der Autorisierung an den Heimatstandort des Nutzers
  - Nutzung von HPC Diensten Autorisierung durch zentrale Stelle

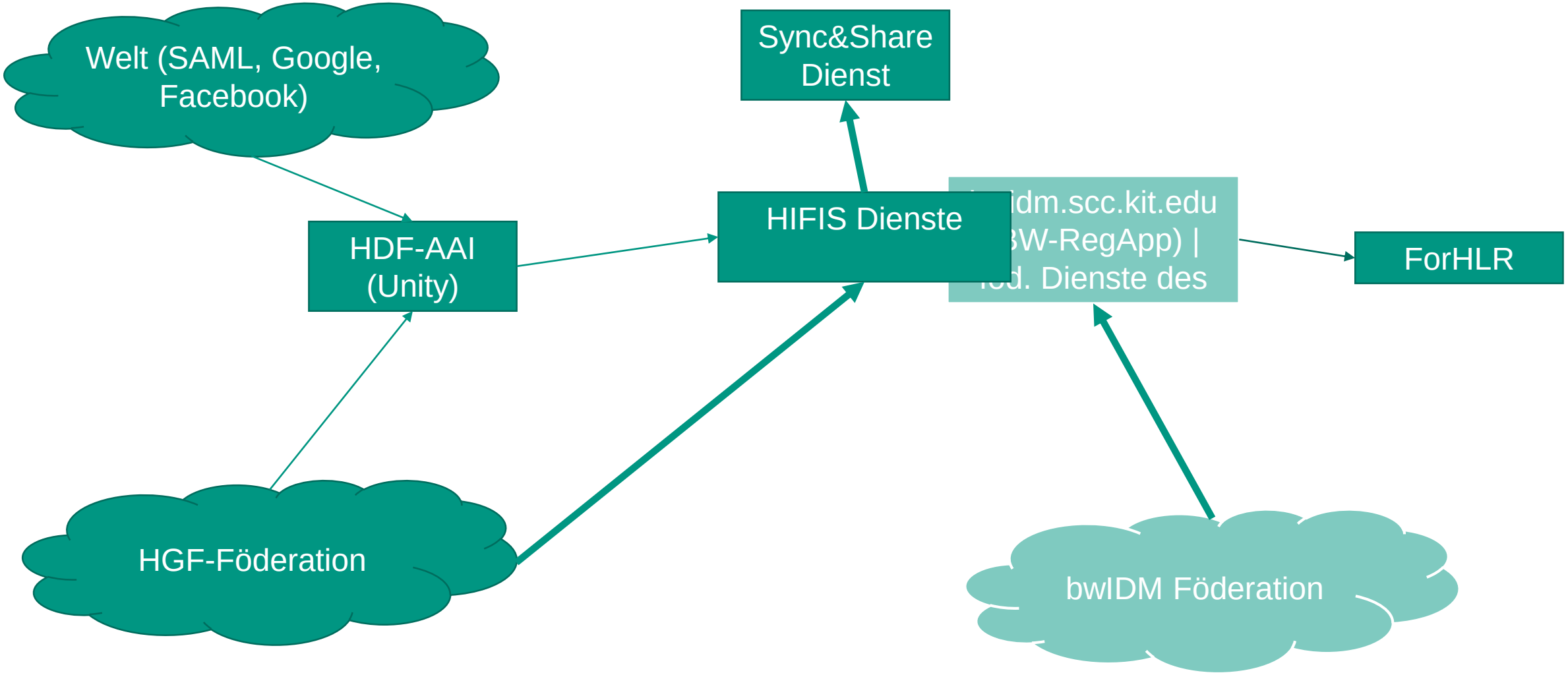
HDF-AAI

- Fokus auf Projektgruppen/ Community
  - Community mit delegierter Autorisierung durch Projektleiter (PI) nach Projektantrag (Proposal)
  - Dienstebündel
- Fokus auf Assurance
  - Unterscheidung DFN, Welt, Google
  - Assurance Elevation über PI

HDF-AAI mit bwIdm



HDF-AAI mit bwIdm



Karlsruhe Institute of Technology

Steinbuch Centre for Computing

Architecture and Policies from the European Perspective

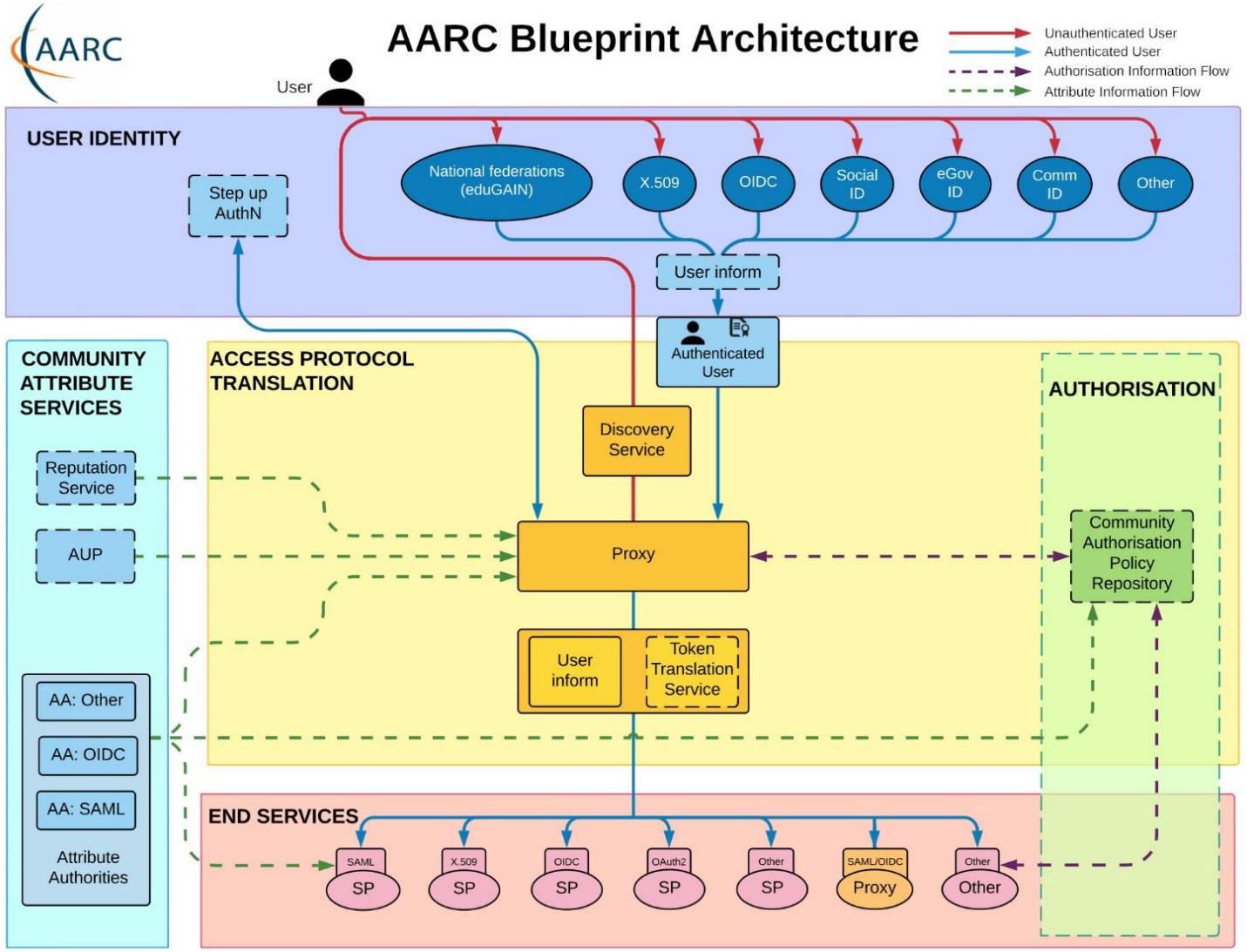
Authentication and Autorisation for Research Communities

- Two Major outputs:
  - Blueprint Architectures – https://aarc-project.eu/architecture
  - Policy Kit – https://aarc-project.eu/policies

AARC Blueprint Architecture 1/2

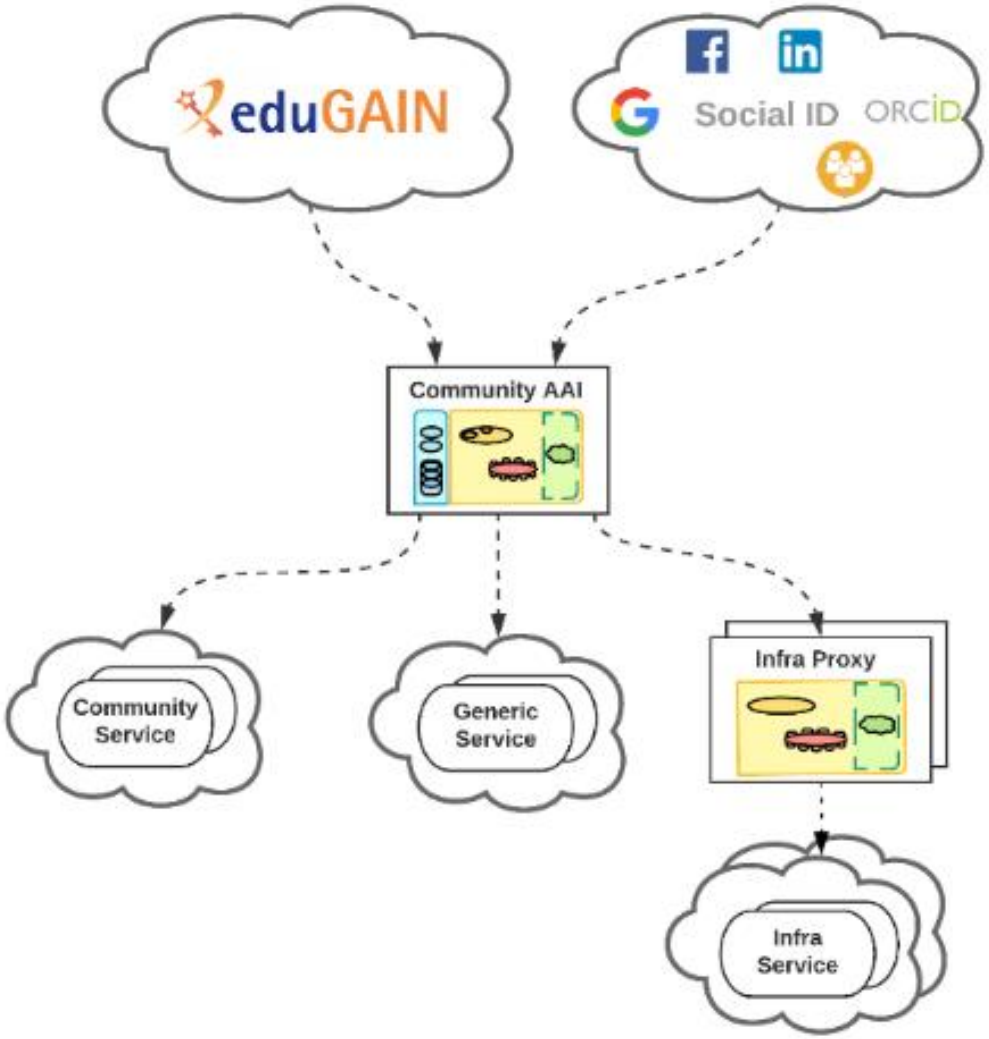
- The proxy model
- A technical approach to ...
  - ... describe the existing real-world scenarios
  - ... address difficulties such as attribute release

AARC Blueprint Architecture 1/2



AARC Blueprint Architecture 2/2

- Community First Approach
  - Add organisational structure to the proxy model
  - Again: Reflect reality



AARC Policy KIT

- Policies of bwIDM addressed the same things in a similar way
  - ...also much earlier than AARC did...
- Based on EGI and EUDAT
- Complex, but condensed to the max

AARC Policy KIT

		Management	Infrastructure Security Contact	User Community Management	Service Management	User
Top Level	Infrastructure Policy	Defines & Abides by	Abides by	Abides by	Abides by	Abides by
Data Protection	Privacy Statement	Defines			Defines	Views
Membership Management	Community Membership Management Policy	Defines		Abides by		
	Acceptable Use Policy	Defines		Defines		Abides by
	Acceptable Authentication Assurance	Defines		Abides by	Abides by	
Operational Security	Incident Response Procedure	Defines	Abides by		Abides by	

AARC Policy KIT

- https://aarc-project.eu/policies
  - Moodle Courses
  - Theoretical Background
  - Policy Templates
  - => HDF Baseline :)

Document	Who should complete the template?	Audience	Description	Link
Top Level Infrastructure Policy	Infrastructure Management	All Infrastructure Participants (abides by)	This policy template defines the roles of actors in the Research Infrastructure and binds the policy set together	Google Doc
Incident Response Procedure	Infrastructure Management & Security Contact	Infrastructure Security Contact, Services (abides by)	This template procedure provides a step-by-step breakdown of actions to take following a security incident.	Google Doc
Membership Management Policy	Infrastructure Management	Research Community (abides by)	This policy template defines how Research Communities should manage their members, including registration and expiration.	Google Doc
Acceptable Authentication Assurance	Infrastructure Management	Research Community, Services (abide by)	This is a placeholder for the Infrastructure to determine rules for the acceptable assurance profiles of user credentials.	Google Doc
Risk Assessment	Infrastructure Management, Services & Security Contact	Infrastructure Management (completes)	This table can be used as a starting point for identifying whether a full Data Protection Impact Assessment is required.	Google Doc
Policy on the Processing of Personal Data	Infrastructure Management & Data Protection Contact	Research Community, Services (abide by)	This document defines the obligations on Infrastructure Participants when processing personal data.	Google Doc
Privacy Policy	Infrastructure Management (for general policy) & Services (for service specific policies)	Users (view)	This can be used to document the data collected and processed by the Infrastructure and its participants. Each service in the infrastructure, as well as the infrastructure itself, should complete the template.	Google Doc
Service Operations Security Policy	Infrastructure Management	Services (abide by)	This policy defines requirements for running a service within the Infrastructure.	Google Doc
Acceptable Use Policy	Infrastructure Management (for baseline) & Research Communities (for community specific restrictions)	Users (abide by)	This is a template for the acceptable use policy that users must accept to use the Research Infrastructure. It should be augmented by the Research Community.	Google Doc

Practical Policy: The SP Perspective

- Central legal aspect: “**Erfüllung der Sorgfaltspflicht**”
- SP: “How can I be sure that I’m not guilty in case of illegal activity in my computer centre”

=> I must ensure that I know **reasonably well** the people on my resources

=> Assurance, Membership Management Policy, Acceptable Use Policy, ...

=> I must ensure that I can reach somebody who **will** reveal a persons identity in case of illegal activity

=> Operational Security, Incident Response, e.g. SIRTFI

=> I must ensure that I operate on legal grounds

=> GDPR, Privacy Policy

- As an IdP, I must be able to trust that the SP will operate on legal grounds

=> Data Protection Code of Conduct