Die bwIDM Föderation

Compliance und Spielregeln

Universität Ulm

Daniel Baur

11.12.2013

Inhaltsverzeichnis

Policy Framework

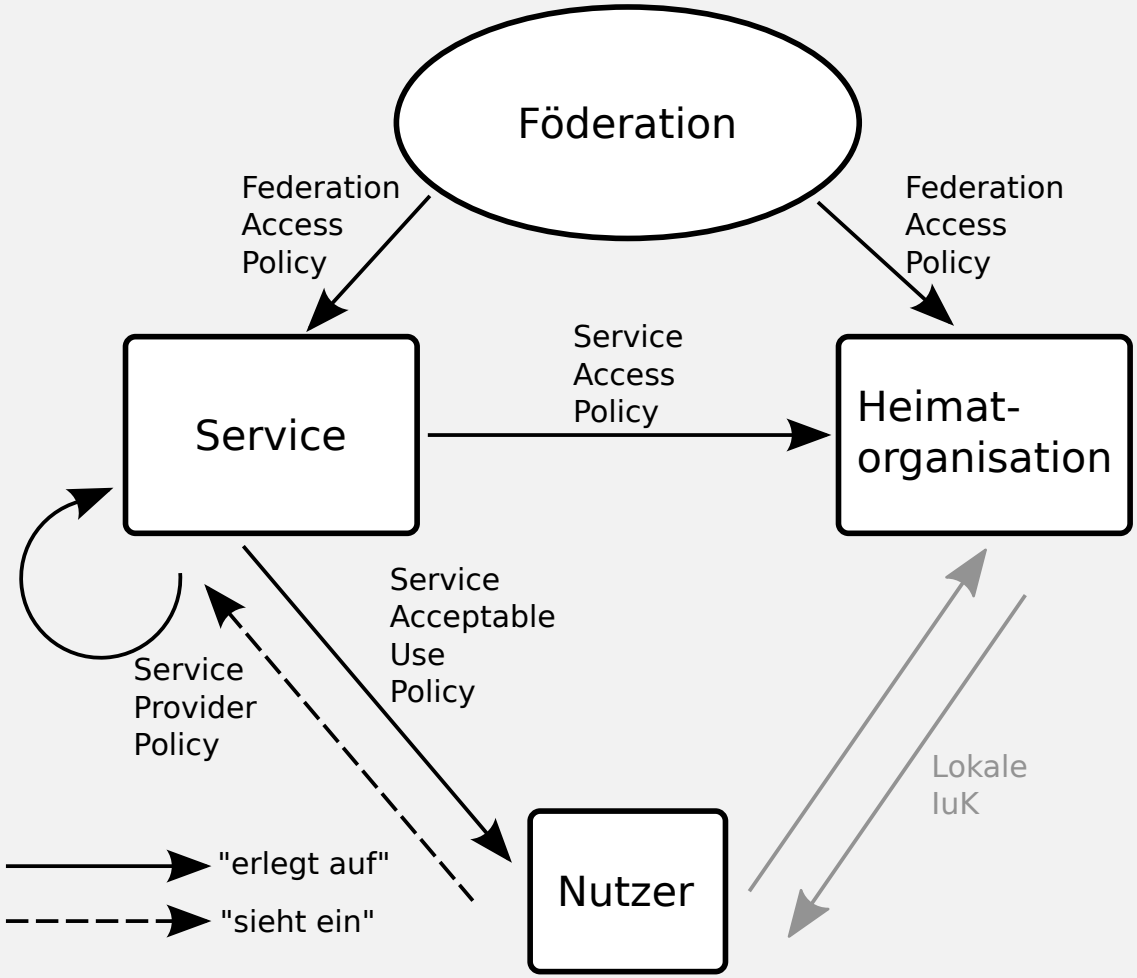
Warum eine Policy?

- Commitment für den Regelbetrieb
- Vertrauensbasis der Föderation
- Regeln (und Konsequenzen)
- Handbuch (Verfahrensleitfaden)
- Standardisierung

Entstehungsprozess

- Best-Practice-Ansatz
- Rahmenwerk DFN-AAI
- Iterativer Abstimmungsprozess Kernteam <-> Partnerforum
- Juristische Überpüfung
- Verabschiedung auf dem Partnerforum

Policy Framework



Federation Access Policy

- Organisation der Föderation
- Mitgliedschaft
- Regeln der DFN-AAI Advanced
- Gebühren
- Verpflichtungen der Föderation
- Verpflichtungen der Mitglieder
- Verpflichtungen eines Identity Providers
- Verpflichtungen eines Service Providers
- Haftung und Datenschutz
- Änderungen
- Sonstiges

Service Access Policy

Anforderungen des Service Anbieters an die Heimatorganisation, damit deren Endnutzer die angebotenen Services benutzen können.

- benötigte Attribute (Kernsatz)
- Definition servicespezifischer Attribute (Erweiterungssatz)
- besondere Nutzungsvorrausetzungen
  - z.B. Vertrag
  - z.B. Entgelt

Service Provider & Acceptable Use Policy

Informationen und Vorrausetzungen für die Dienstnutzung durch den Endnutzer.

Service Provider Policy

- optional
- Nutzungsvorrausetzungen
- Lifecycle der Dienstnutzung
- erweiterte Erläuterungen zur Verwendung der Nutzerdaten

Service Acceptable Use Policy

- optional
- Nutzungsbedingungen

Beispiel bwFileStorage

Nutzungsbedingungen bwFileStorage - bwFileStorage Version 1.1

Leistungen und Nutzerkreis
Der Dienst bwFileStorage bietet den Nutzern der Rechenzentren der Universitäten und Hochschulen im Land Baden-Württemberg filesystembasierten Zugriff auf den LSDF Datenspeicher, der am Karlsruher Institut für Technologie (KIT) installiert ist. Der Zugriff auf die Daten wird über die Protokolle SCP, SFTP und HTTPS gewährleistet.
Der Dienst ist nicht geeignet zur Speicherung personenbezogener Daten.

Datenschutz
Bei der Registrierung für den bwFileStorage-Dienst werden die folgenden Nutzerinformationen von der Heimateinrichtung an den Dienstbetreiber KIT verschlüsselt übermittelt und dort gespeichert:
- Vor- und Nachname
- E-Mailadresse
- Heimateinrichtung
- Eindeutige Nutzerkennung (EPPN & persistent ID)
- Status des Nutzers (Student, Mitarbeiter, Gast)

Die Vorschriften des Landesdatenschutzgesetzes (LDSG) und bereichsspezifische Datenschutzvorschriften (insbesondere TKG, TMG) in den jeweils geltenden Fassungen werden beachtet.
Es gelten die Regeln der 'Ordnung für die digitale Informationsverarbeitung und Kommunikation' (IuK) am Karlsruher Institut für Technologie (abzurufen unter http://www.kit.edu/downloads/AmtlicheBekanntmachungen/2013_AB_036.pdf).

Speicherplatz
Die Größe des Speicherplatzes, über den ein Nutzer verfügen kann, ist beschränkt.

Datensicherheit
Die Kommunikation zwischen den Endgeräten des Nutzers und der Dienstinfrastruktur des KIT erfolgt verschlüsselt.
Die abgespeicherten Daten werden unverschlüsselt auf Speichersystemen des KIT abgelegt. Der Datenzugriff ist beschränkt auf:
- Denjenigen Nutzer, der die Daten initial abgespeichert hat.
- Weitere Nutzer, die der Datenbesitzer durch Vergabe von entsprechenden Zugriffsrechten autorisiert hat.

Alle Daten werden regelmäßig auf Band gesichert, um im Notfall ein Disaster-Recovery zu ermöglichen. Nutzer haben keinen direkten Zugriff auf diese Kopie. Es werden jedoch in Form von Snapshots mehrere Versionen der Dateien vorgehalten, wodurch Benutzer ältere Dateiversionen wieder herstellen können.

Verfügbarkeit
Die Systeme der Dienstinfrastruktur laufen im Regelbetrieb rund um die Uhr. Während der Servicezeit (werktags von 09.00 bis 17.00 Uhr) beträgt die Reaktionszeit vier Stunden. Das KIT strebt generell eine möglichst hohe Dienstverfügbarkeit an.
Geplante Dienstunterbrechungen (z.B. für Wartungsarbeiten) werden im Voraus mit einer Frist von fünf Tagen angekündigt.

☐ I have read and accepted the terms of use.

Attributspezifikation

Attributspezifikation

- Standardattribute für Austausch zwischen IdP und SP
- (meist) etablierter Standard: *eduPerson*.
- “kompatibel” mit DFN-AAI
- 2 Arten von Attributen:
  - Kernsatz
    - Attributspezifikation
    - Verpflichtend für jeden IdP
  - optionale Attribute
    - Spezifikation durch Service Anbieter
    - Nur für diesen Service benötigt
- Vorteile:
  - geringere Einstiegshürde
  - erhöhte Flexibilität

Kernsatz

eduPersonPrincipalName *bxp27@uni-ulm.de*	eindeutiger Identifikator für die Person mit Scope
mail *daniel.baur@uni-ulm.de*	Mailadresse der Person
givenName *Daniel*	Vorname der Person
sn *Baur*	Nachname der Person
eduPersonScopedAffiliation *staff@uni-ulm.de*	Art der Zugehörigkeit einer Person zu einer Institution

Kernsatz

eduPersonEntitlement *http://bwidm.de/entitlement/bwGRiD*	Berechtigung für eine Ressource
uid *bxp27*	Login-Name
http://bwidm.de/bwidmOrgId *ul*	eindeutiges Organisationskürzel
(persistentId) *hEmsRYfZqHWExkD73L...*	persistenter Identifikator

optionale Attribute

o *Universitaet Ulm*	Name der Organisation (Freitext)
http://bwidm.de/bwidmCC *kizinfsy*	Ordnungskriterium
http://bwidm.de/bwidmMemberOf *kizinfsy*	Gruppenzugehörigkeit(en)

bwIDM Attribute

http://bwidm.de/bwidmOrgId

- Eindeutiges Kürzel für jede Organisation innerhalb von bwIDM
- Ersatz/Alternative für den Scope
- kann z.B. in Kombination mit uid den EPPN ersetzen

http://bwidm.de/bwidmCC

- Ordnungskriterium einer Person innerhalb der Organisation
- Einteilung von Benutzern in Untergruppen

http://bwidm.de/bwidmMemberOf

- Gruppenzugehörigkeit(en) der Identität
- Einteilung von Benutzern in Untergruppen

Datenschutz und Sicherheit

Erinnerung: Ziele des Arbeitspakets

Gewährleistung der Durchsetzung

- einschlägiger Auflagen des Datenschutzes sowohl im
  - landesweiten als auch im
  - hochschulinternen Rahmen sowie
- bestehender Anforderungen der IT-Sicherheit, definiert beispielsweise durch
  - hochschulinterne Sicherheitsrichtlinien oder
  - dienstspezifische Bedürfnisse.

Datenschutz

- Grundsätzliche Feststellung: Standorte bleiben für die Einhaltung der datenschutzrechtlichen Bestimmungen in ihren Bereichen verantwortlich.
- Bewertung der vorgeschlagenen Zugangsverfahren in Zusammenarbeit mit ZENDAS: Mit den von ZENDAS vorgeschlagenen Änderungen sind die ausgewählten Verfahren »sauber«.
- »Abfallprodukte«, die bwIDM (nur) am Rande berühren:
  - Rechtswirksamkeit von uApprove geklärt sowie Musterformulierung von ZENDAS erarbeitet.
  - Beispiel für Verfahrensverzeichniseintrag eines IdP durch Uni Hohenheim und ZENDAS erarbeitet.
  - Beide Vorlagen stehen kosten- und lizenzfrei zur Verfügung.

Sicherheit

- Grundsätzliche Policy-Entscheidungen:
  - Standorte bleiben autonom in ihren Erwägungen und Maßnahmen.
  - Bei Vorfällen besteht aber eine Pflicht zur Zusammenarbeit.
  - Einschlägige Kontaktpersonen sind hierfür zu benennen.
- Bewertung der vorgeschlagenen Zugangsverfahren: Aus Sicherheitssicht sind die ausgewählten Verfahren ebenfalls »sauber«.

Fazit

- Aufgaben für die Föderation sind damit erfüllt,
- ebenso die Betrachtung der vorgeschlagenen Zugangsverfahren.
- Aber die einzelnen Dienste müssen zuverlässig und rechtskonform betrieben werden (nicht Teil des bwIDM-Projekts!).
- Möglicherweise wünschenswert: Eine einheitliche Strategie für bw-Dienste.