

# Federated Identity Management for Libraries (FIM4L) – die zweite Seite der Medaille

74. DFN Betriebstagung,

**Peter Gietz**

DAASI International



**In Kooperation mit  
Gerrit Gragert**

Staatsbibliothek zu Berlin



**Staatsbibliothek  
zu Berlin**

Preußischer Kulturbesitz

**Teile der Folien geklaut von:**

**Jos Westerbeke**

Erasmus University

**Jiří Pavlík**

Moravian Library



# Die Bibliothek als ein sicherer Ort

---

Eine Bibliothek muss Nutzer\*innen:

- Privatsphäre bieten
- schützen
- deswegen auch Verantwortung für den Schutz ihrer persönlichen Daten übernehmen



Vertrauter sicherer Platz mit  
Privatsphäre

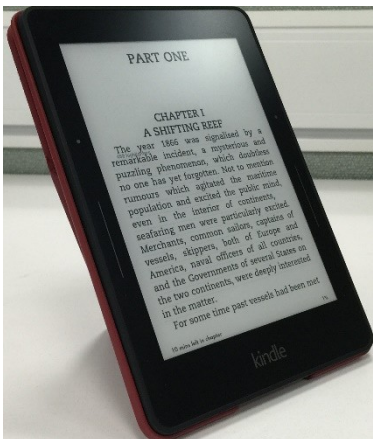
# Die Bibliothek als Versorger von digitalen Inhalten

---

Spätes 20. Jh. – frühes 21.Jh.

Print -> Digital -> Remote

Remote = jederzeit, von jedem Ort, auf jedem Gerät



Benötigt:

**authentifizierten und autorisierten Zugriff  
unter Wahrung des Datenschutzes**

# Von IP-basiertem Zugriff zu föderiertem Zugriff mit SSO



IP basierte Authentifizierung:

**ortsbasiert**

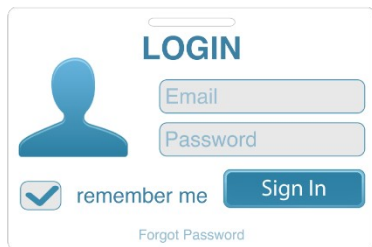
(Kann über VPN-Technologie erweitert werden)



SSO Authentifizierung:

**Personen-ID basiert**

(jederzeit, von jedem Ort, auf jedem Gerät)

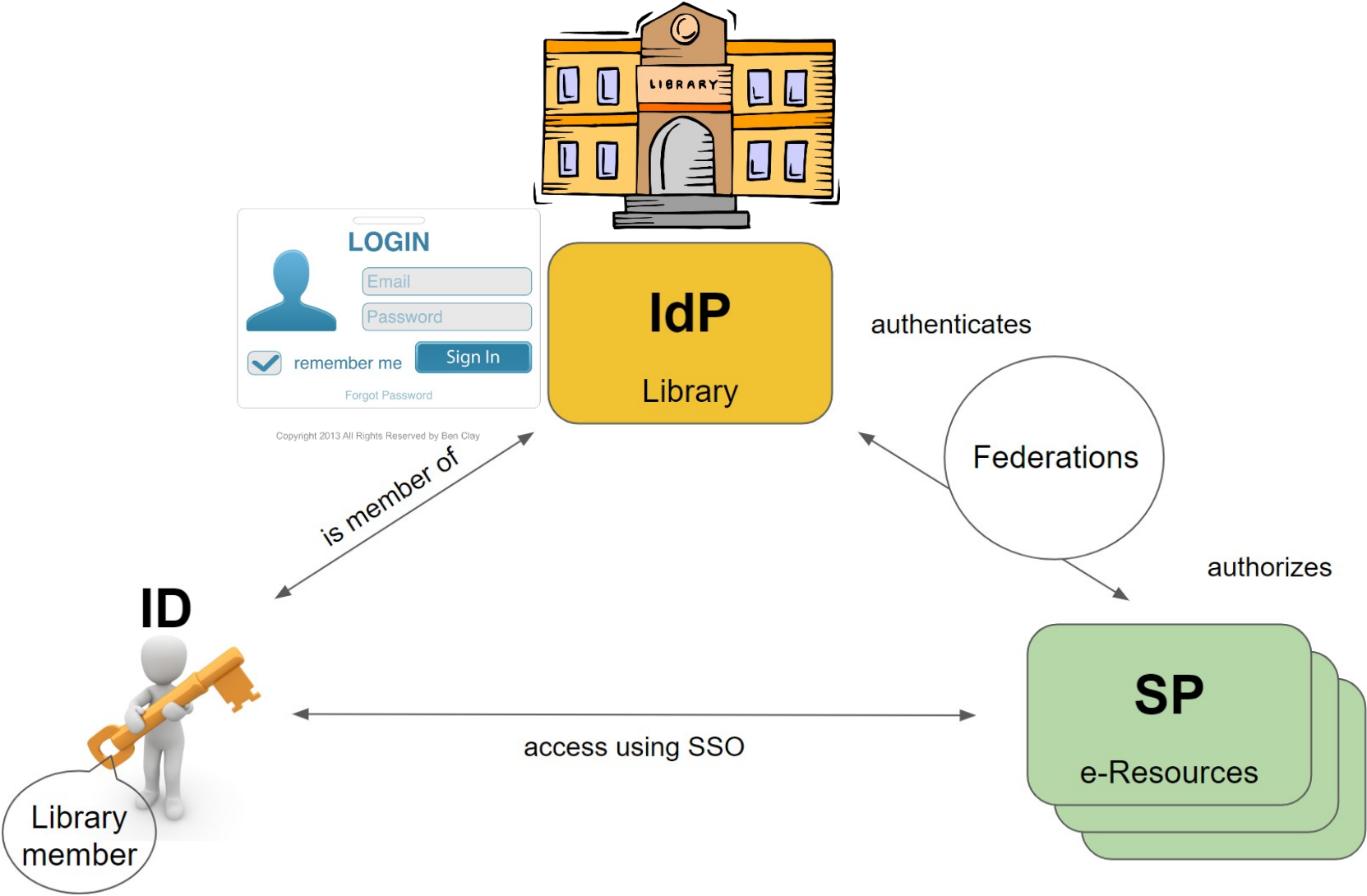


Copyright 2013 All Rights Reserved by Ben Clay

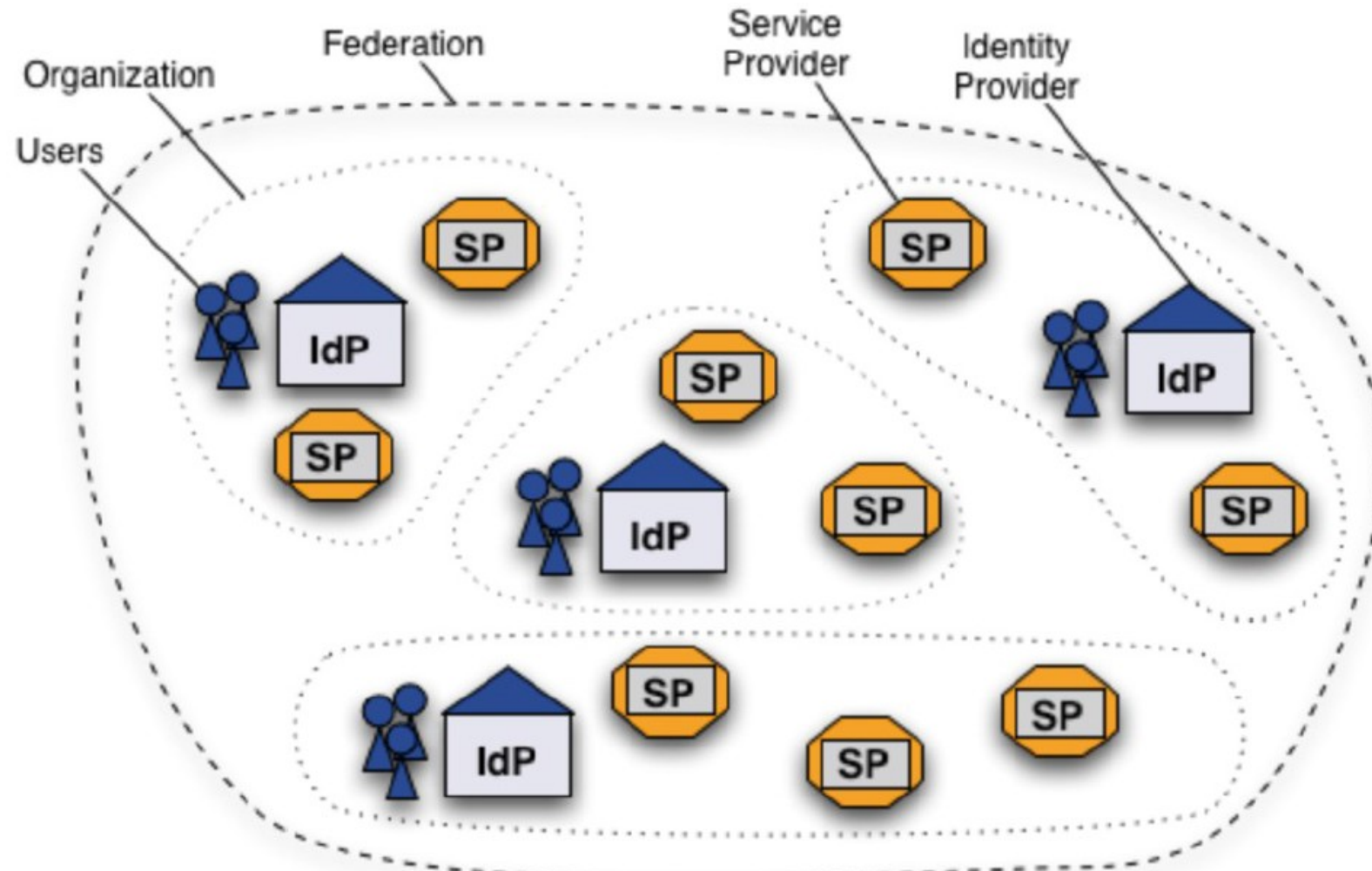
**SSO-Vorteile:**

- Zugeschnittene Verträge: z.B. Subscription nur für eine Fakultät (= *Einschränkung der Freiheit der Wissenschaften?*)
- Bei Missbrauch: Verlag muss nur eine Nutzer\*in aussperren und nicht den ganzen IP-Bereich, also alle
- Bessere Statistiken
- SSO

# Wie funktioniert SSO



# SAML-basierte nationale Föderation



# SAML basierte Inter-Föderation eduGAIN



# Entstehungsgeschichte von FIM4L (etwas verkürzt)

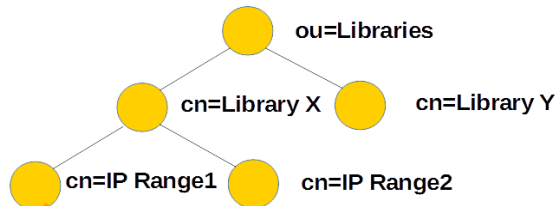
---

- Am Anfang war **FIM4R**
  - eine Workshop-Reihe von Forschungsinfrastrukturen aus den verschiedensten Fachdomänen (von CERN bis Digital Humanities) zu
    - Harmonisierung von AAI-Architekturen im Allgemeinen
    - Nachnutzungsmöglichkeiten durch eduGAIN im Besonderen
  - Erstes Dokument zu Anforderungen von Forschungsinfrastrukturen an eduGAIN, insbesondere zu notwendigen personenbezogenen Daten
- Die **EU** hat u.a. auf dieses Paper reagiert mit einem INFRA-Call zu AAI, welcher von AARC gewonnen wurde
- **AARC: Authentication and Authorization for Research Collaborations**
  - **AARC I** hatte ein Work Package zu Bibliotheken und AAI (vgl. <https://aarc-project.eu/libraries/>):
    - Mehrere Pilotanwendungen für Bibliotheken
    - Workshop bei LIBER Conference
  - Aus dieser Initiative bei der nächsten LIBER Conference hat sich **FIM4L** gegründet



# Bibliotheksgerichtete Aktivitäten von AARC I

- Beispiel für AARC I Bibliotheks-Piloten:
  - Libraries walk-in-user pilot für eine einfache Migration zu FIM
    - Integration von IP-basierter Authentifizierung in Shibboleth mit Möglichkeit der webbasierten Verwaltung der IP-Ranges und deren Berechtigungen
    - Mandantenfähige Implementierung für Bibliotheksverbünde
    - (vgl. <https://wiki.geant.org/display/AARC/Libraries+walk-in-user+pilot>)



IP-Range-Start: 203.0.113.115  
IP-Range-End: 203.0.113.118  
Entitlement: <view database X>  
Affiliation: library-walk-in@libraryX  
Description: Frontdesk Kioskes

## AARC Library IP Ranges Management



Home Trusted IP Ranges Logout

AARC Scenario 23 Portal / Trusted IP ranges Toggle help texts

### Manage trusted IP ranges

The following trusted IP ranges could be found

Search

<input type="checkbox"/>	Begin	End	Affiliation	Entitlement	Description	
<input type="checkbox"/>	203.0.113.115	203.0.113.115	library-walk-in@uni-one.demo.university		Front Desk Kiosk	<input type="button" value="edit"/>
<input type="checkbox"/>	203.0.113.233	203.0.113.233	library-walk-in@uni-one.demo.university		Kiosk One	<input type="button" value="edit"/>
<input type="checkbox"/>	203.0.113.245	203.0.113.245	library-walk-in@uni-one.demo.university		Kiosk Two	<input type="button" value="edit"/>

Showing 1 to 3 of 3 rows

© DAASI International

## FIM4L Mitglieder

---

- Obwohl FIM4L von Bibliotheken getrieben ist, haben sich weitere Organisationen engagiert, da FIM ein Prozess ist, an dem verschiedene Stakeholder beteiligt sind:
  - **Bibliotheken**, Dachorganisationen von Bibliotheken und Bibliotheks-Vereinigungen, z.B:
    - LIBER, Erasmus University Rotterdam, Moravian Library Brno, Staatsbibliothek Berlin
  - **Föderationsinfrastrukturbetreiber**: NRNs, NRN Associations, Rechenzentren, z.B.:
    - GEANT, DFN, SURFnet, Eko-Konnect, UbuntuNet Alliance
  - **IT-Dienstleister**:
    - OCLC, Spherical Cow Consulting, DAASI International
  - **Verlage** nur:
    - Elsevier

Vollständige Liste: [https://www.fim4l.org/?page\\_id=346](https://www.fim4l.org/?page_id=346)

# FIM4L Arbeitsgruppen

---

- **FIM4L** (International) war zunächst eine internationale Aktivität mit Beteiligung aus Europa, Afrika und den USA (vgl. <https://fim4l.org>),
  - Charter: <https://www.fim4l.org/wp-content/uploads/2020/09/FIM4L-charter-public-version.pdf>
  - Mailingliste (mit mittlerweile 68 Mitgliedern):
  - Erste Version der Guidelines and recommendations
- **FIM4L LIBER Working group**
  - LIBER (Ligue des Bibliothèques Européennes de Recherche) ist die Europäische Vereinigung von Forschungsbibliotheken (<https://libereurope.eu/>)
  - Um die Nachhaltigkeit der Aktivität zu sichern, wurde von europäischen Mitgliedern von FIM4L.org ein Antrag gestellt für eine offizielle LIBER-Arbeitsgruppe, der bewilligt wurde.
  - Die FIM4L Working Group ist nun Teil von LIBER's Strategic Direction on Research Infrastructure, welche wiederum eine Säule der LIBER 2018-2022 Strategy ist.
    - Vgl. <https://libereurope.eu/strategy/research-infrastructures/fim4l/>
- Die internationale Gruppe existiert aber weiterhin und bleibt die „mother of all FIM4L activities“
  - **IFLA** (International Federation of Library Associations and Institutions, vgl. <https://www.ifla.org/>) ist eine internationale Vereinigung von Bibliotheken, verschiedenster Art
  - Es finden gerade Gespräche statt, um eine IFLA WG als internationale Repräsentanz zu gründen

# Ausgangslagen

---

- Es gibt unterschiedliche Ausgangslagen:
  - Bibliotheken
    - haben die Befürchtung, dass der Einsatz neuer Technologien, dazu führt, dass mehr personenbezogene Daten Preis gegeben werden
    - wollen ihren Nutzer\*innen nutzer\*innenfreundliche Dienste anbieten
    - manche haben wenig Ressourcen für IT-Infrastrukturumstellungen
    - manche verfügen über zu wenig Geld für die Lizenzen aller von den Nutzer\*innen benötigten digitalen Ressourcen für alle Nutzer\*innen
  - Verlage
    - sehen in FIM die Möglichkeit personifizierte Dienste anzubieten
    - haben auch von Hochschulenn getrieben in die neue FIM-Technologie investiert und wollen sie nutzen
    - wollen ohne Mehraufwand flexiblere Möglichkeiten für Vertragsgestaltung haben
    - sehen einen Vorteil, mehr personenbezogene, bereits geprüfte Daten über die Nutzer\*innen zu haben
    - sehen einen Vorteil, mehr individuelle Verhaltensdaten zu haben
    - haben manchmal leider nur rudimentäre Implementierungen von SAML

## FIM4L Charter:

---

- Sammlung der **Bibliotheksanforderungen** an FIM und Vermittlung der Anforderungen an relevante Gruppen wie FIM4R, REFEDS, the eduGAIN community, STM und RA21.
- Erstellen von **Guidelines and Recommendations** über Attributfreigabe unter Wahrung des Datenschutzes
- Zusammenbringen von **relevanten Stakeholdern**, die den Einsatz von FIM anstelle IP-basierter Authentifizierung in Bibliotheken (alle Arten von Bibliotheken) fördern wollen
- **Vertretung der Bibliotheken** bei der Diskussion der RA21-Empfehlungen
- **Förderung der Adaption** von datenschutzkonformer Nutzung von FIM

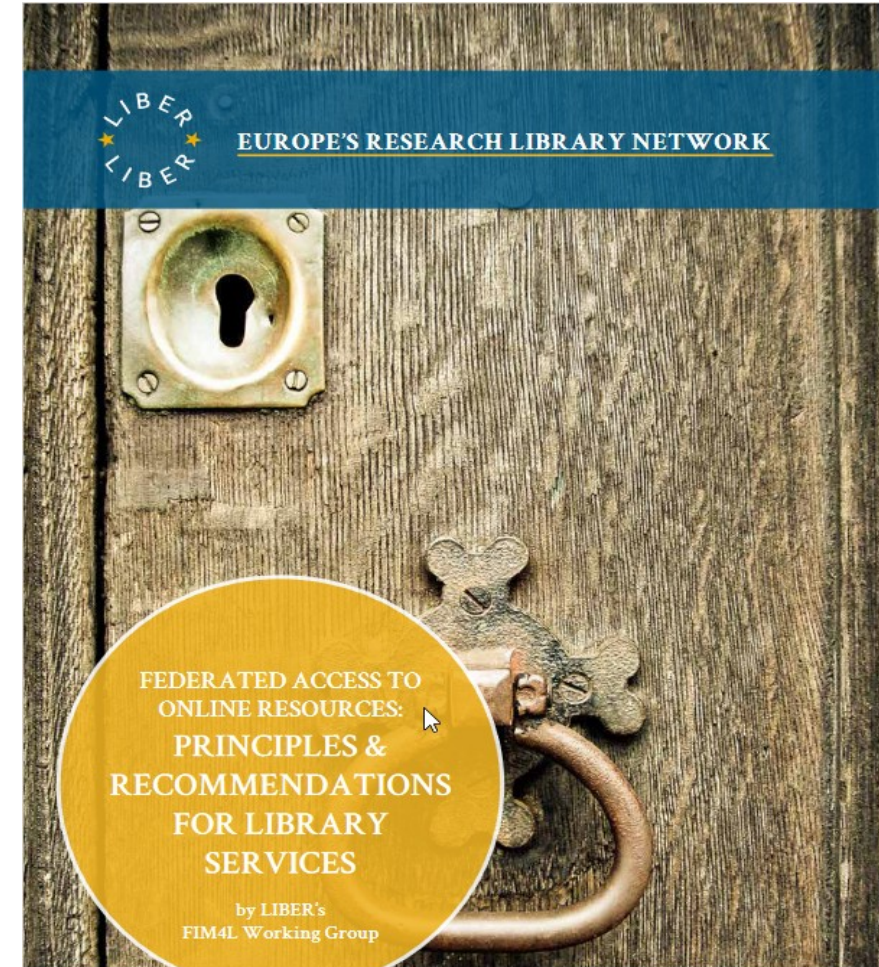
# FIM4L Guidelines and recommendations 4 zu Attributfreigabe

---

- Empfehlungen 4 (von insgesamt 10 Empfehlungen) zu Attributfreigabe im Sinne der Datensparsamkeit:
  - 4.a) Ein Verlag braucht ausschließlich eine Session-ID:
    - nur NameID zur semantikfreien Identifikation der Session freigeben
  - 4.b) Ein Verlag möchte Personalisierungsfeatures bieten
    - Pairwise Subject Identifier (Nachfolger von eduPersonTargetedID) freigeben
    - Also eine für einen Benutzer für einen Service Provider persistente ID (ein anderer SP bekommt eine andere ID)
  - 4.c) Nur ein Teil der eigenen Nutzer\*innen dürfen auf die Ressource
    - Folgende nichtpersonenbezogene Attribute können freigegeben werden:
      - eduPersonEntitlement mit dem spezifischen Wert urn:mace:dir:entitlement:common-lib-terms
      - eduPersonEntitlement, mit weiteren URN-Werten, die Gruppen- oder Rollenmitgliedschaften nach der entsprechenden AARC-Spezifikation (vgl. <https://aarc-project.eu/wp-content/uploads/2017/11/AARC-JRA1.4A-201710.pdf>)
      - eduPersonScopedAffiliation, mit der Zugehörigkeit, etwa student@ub.uni-xxx.de
      - SchacLocalReportingCode für IdP-Statistiken (wird wahrsch. durch das neue eduPersonAnalyticsID ersetzt)
  - Der Verlag will personenbezogene Daten: Er soll sie sich selber über ein Registrierungsformular holen
  - [eine Empfehlung für den Einsatz eines Consent-Tools, wie z.B. CAR wird gerade noch diskutiert.]

# Was können Bibliotheken in den nächsten Jahren erwarten?

- Verlage werden zunehmend FIM-basierte Verträge fordern und IP-basierte Authentifizierung ablehnen
- Nutzer\*innen werden bewusster im Umgang mit ihren personenbezogenen Daten
- Bibliotheks-Verbände werden entsprechende Empfehlungen abgeben
  - Siehe die auf FIM4L.org basierende LIBER-Empfehlung:
    - <https://libereurope.eu/wp-content/uploads/2020/12/LIBER-FIM4L-Recommendations-2020-v.01.pdf>



# Vielen Dank für die Aufmerksamkeit!

---

- Fragen?
- Kommentare?
- Ergänzungen?

Gerrit Gragert



Peter Gietz

