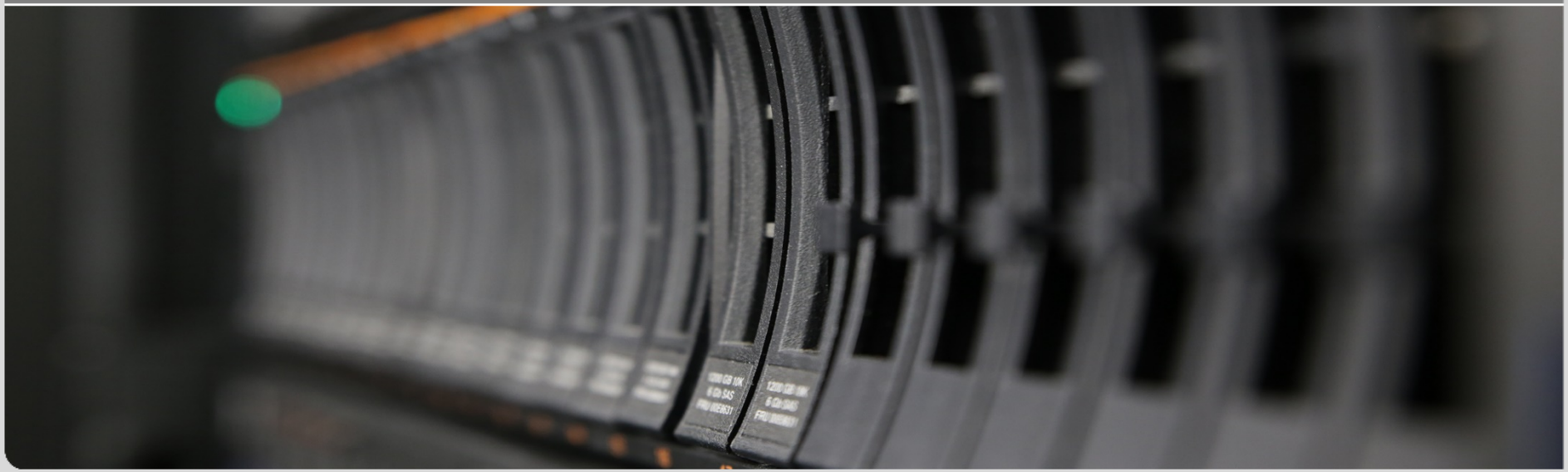
Karlsruhe Institute of Technology

Steinbuch Centre for Computing

Technische Einschätzung RA21

Wer soll künftig die digitale Identität unserer Mitglieder kontrollieren?

Martin Nußbaumer, Steinbuch Centre for Computing (SCC), KIT



Agenda

- Beobachtungen zu Authentifizierungsverfahren SAML / IP
- SAML Basics und Einordnung von RA21 in die SAML-Welt
- Einordnung der „Empfehlungen zu Authentifizierungsmethoden für den Zugriff auf elektronische Ressourcen“ (Erarbeitung im DFG-Rundgespräch 01/2019) in die SAML/RA21-Architektur

Agenda

- Beobachtungen zu Authentifizierungsverfahren SAML / IP
- SAML Basics und Einordnung RA21 in die SAML-Welt
- Einordnung der „Empfehlungen zu Authentifizierungsmethoden für den Zugriff auf elektronische Ressourcen“ (Erarbeitung im DFG-Rundgespräch 01/2019) in die SAML/RA21-Architektur

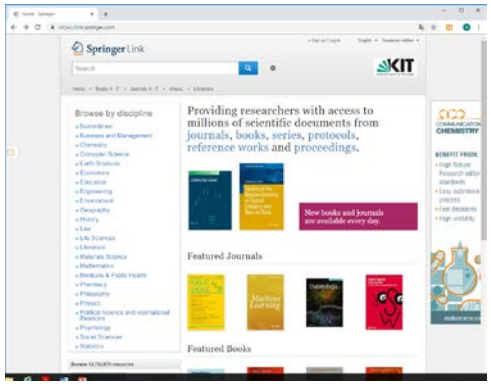
Beobachtung 1: IP-Auth verursacht wenig Aufwand für Zugreifende

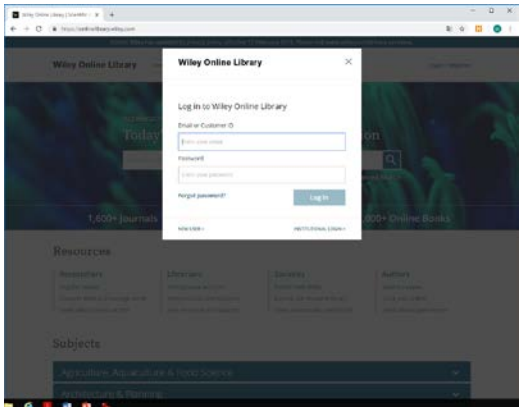
- IP-basierter Zugriff ist sehr einfach und funktioniert
  - … wenn sich der Zugreifende innerhalb des Netzwerks befindet
  - … und besonders gut, wenn Zugreifende am Heimatstandort sind
- eigentlicher Vorgang der Authentifizierung ist für Zugreifende „gefühlt“ nicht (mehr) vorhanden, transparent
  - Gute user experience für Zugreifende, da „nahtlos“ (Authentifizierung)
  - Personalisierte Mehrwertdienste nicht möglich

- Mit zunehmender Personen-Mobilität (off-campus) rücken Maßnahmen zur *virtuellen* Rückverlagerung der Person an den Standort in den Vordergrund (VPNs)
- Trotzdem: zunehmender Wunsch nach personalisierten Diensten mit IP/VPN praktisch nicht umsetzbar

Beobachtung 2: Personen-Auth (SAML) verursacht (aktuell) mehr Aufwand als IP-Auth

- Auch wenn der eigentliche SAML-Login wenig Aufwand verursacht, im Vergleich zu IP-Auth ist es mehr
- Deutliche Optimierungspotenziale beim „Weg zum IDP“
  - Link zur Anmeldung auf Verlagsseiten meist uneinheitlich platziert
  - Ebenso die Wahl der Heimatorganisation (manchmal mehrstufig: Welt → EU → Nation → KIT, viele Klicks!)
  - da wenig genutzt, kein Lerneffekt: jedes Mal hoher Suchaufwand → Frustration → Wahrnehmung: IP+VPN deutlich besser





Zwischenfazit Aufwandsbeobachtung

- These: Loginaufwand für SAML (am IDP) wird perspektivisch für Nutzer immer geringer, da „SAMLifizierung“ von Diensten in letzten Jahren stark zugenommen (am KIT: nahezu jeder zweite Login SSO)

- Das zu lösende Aufwandsproblem liegt dann im „Weg zum IDP“
  - Ein großer Aufwand entsteht bei der Suche nach dem Login-Link und der Wahl des eigenen IDP (Durchklicken und IDP suchen)
  - Nebenbemerkung: das aufwandsminimale IP-Auth nimmt mit zunehmender Mobilität zu (virtuelle Verlagerung des Standorts)

- **Ziel von RA21: Minimierung des „Wegs zum IDP“**

- Anmerkung: Aufwandsbewertung aus Nutzersicht, betriebliche Aspekte vernachlässigt:
  - Sperren von ganzen Netzsegmenten bei Missbrauch (IP) vs. Einzelperson gesperrt (SAML)
  - Management von Netzsegmenten (IP) vs. Identity Management (SAML)
  - Verfügbarkeit VPN (IP) vs. Betrieb eines IDP (SAML)

Beobachtung 3: Wunsch nach personalisierbaren Diensten steigt (Nutzer, Verlage)

- Ausgangspunkt
  - Mit IP-Adressen treffen wir Aussagen zum Netz-Standort einer Person
  - Mit SAML treffen wir über Attribute Aussagen (*assertions*) zur Person

- **These**: Wer die Identität kontrolliert, (be)hält Einfluss auf personalisierbare Dienste

> Ein Gedankenexperiment: „ein Dienstanbieter (etwa ein Verlag) möchte personalisierte Dienste (Nutzerwunsch) legitimierten Zugreifenden bereitstellen.“

- Dienstanbieter legitimiert über IP-Auth (Einrichtung) und personalisiert mit einem (dritten) ID-Anbieter (etwa Google CASA)
  - Der Zugreifende zeigt über Verlag gegenüber Google CASA, dass Legitimation existiert, ab dann kann über Google-ID zugegriffen werden
  - Verlag nimmt Einbußen an die Qualität der Legitimation zu Gunsten der Personalisierung in Kauf
- Dienstanbieter stellt Personalisierung über den SAML-IDP der Einrichtung bereit
  - Der Dienst nutzt SAML-basierte Authentifizierung und erbittet notwendige Attribute und Nutzereinwilligung (DSGVO)
  - ein SAML-IDP kann dies datenschutzkonform liefern

Zwischenfazit Personalisierte Dienste

- Wer soll künftig die digitale Identität unserer Mitglieder kontrollieren, also Aussagen (Assertions) über unsere Mitglieder treffen?
- Wir, mit SAML?
- Oder Dritte, wie Google über einen Googleaccount?

Agenda

- Beobachtungen zu Authentifizierungsverfahren SAML / IP
- SAML Basics und Einordnung RA21 in die SAML-Welt
- Einordnung der „Empfehlungen zu Authentifizierungsmethoden für den Zugriff auf elektronische Ressourcen“ (Erarbeitung im DFG-Rundgespräch 01/2019) in die SAML/RA21-Architektur

Identity – Trust – Access

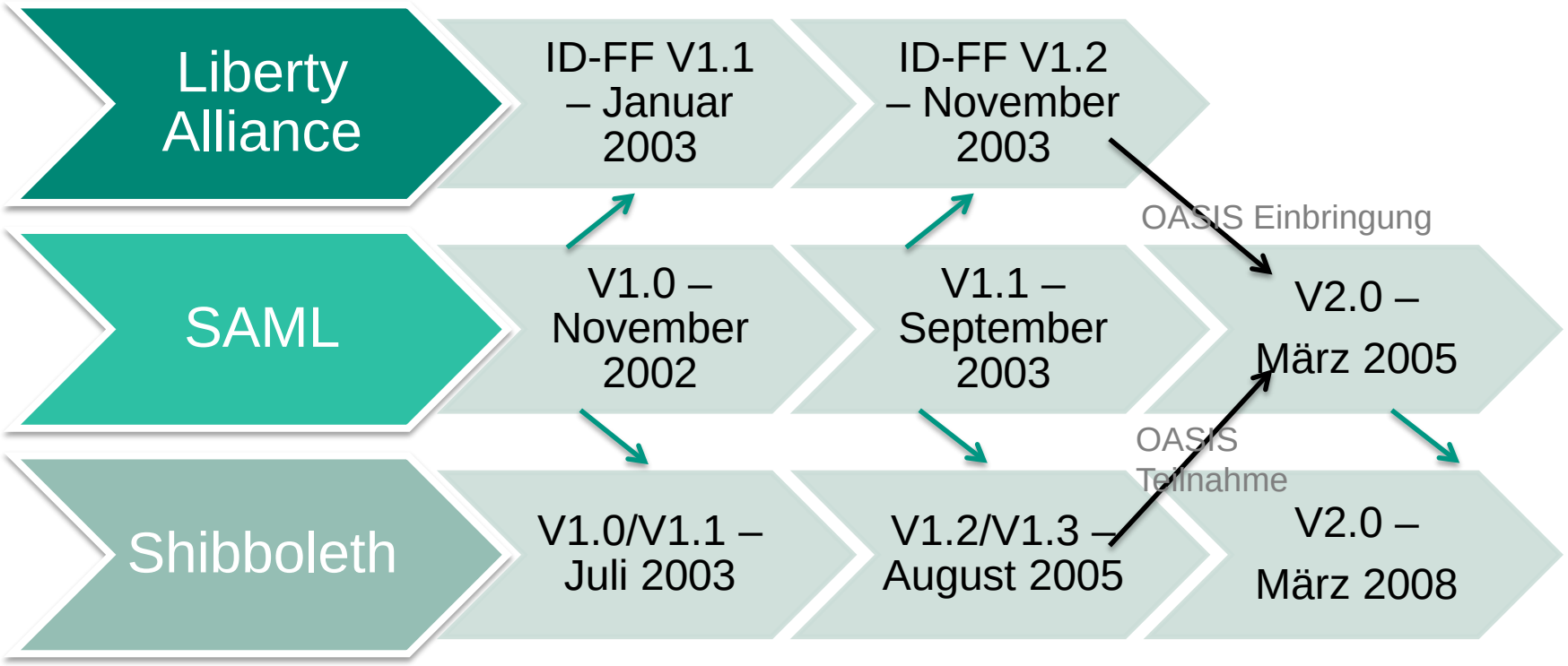
Folie von Klaas Wierenga (GEANT), DFG-Rundgespräch 01/2019

Identity – Trust – Access (cont)

Folie von Klaas Wierenga (GEANT), DFG-Rundgespräch 01/2019

Zeitleiste SAML und Shibboleth

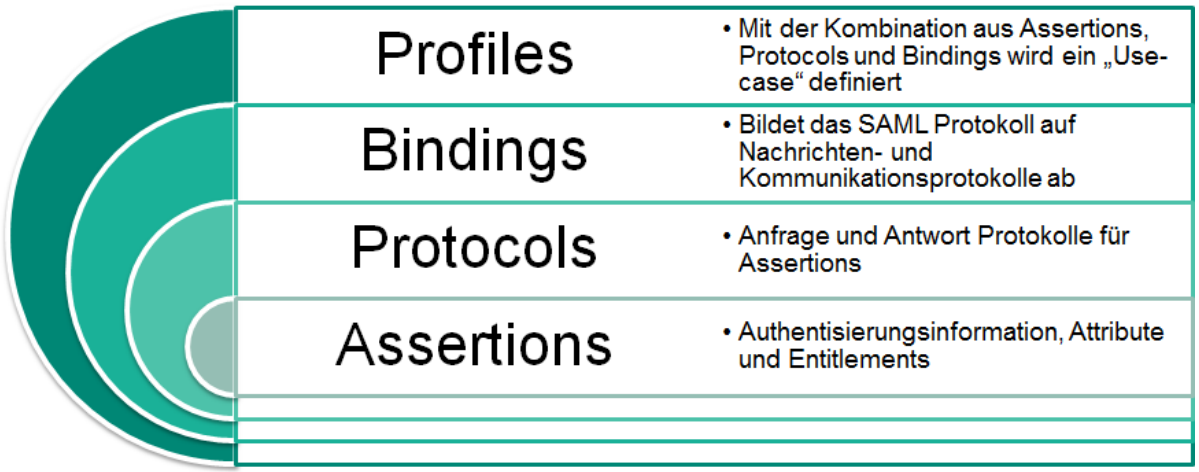
Fazit: stabile, reife und zukunftssichere Technologie



SAML Komponenten

Take away: SAML ist mehr als WebSSO

SAML Komponenten



Authentication Context

- Definiert Art und Weise der Authentifizierung

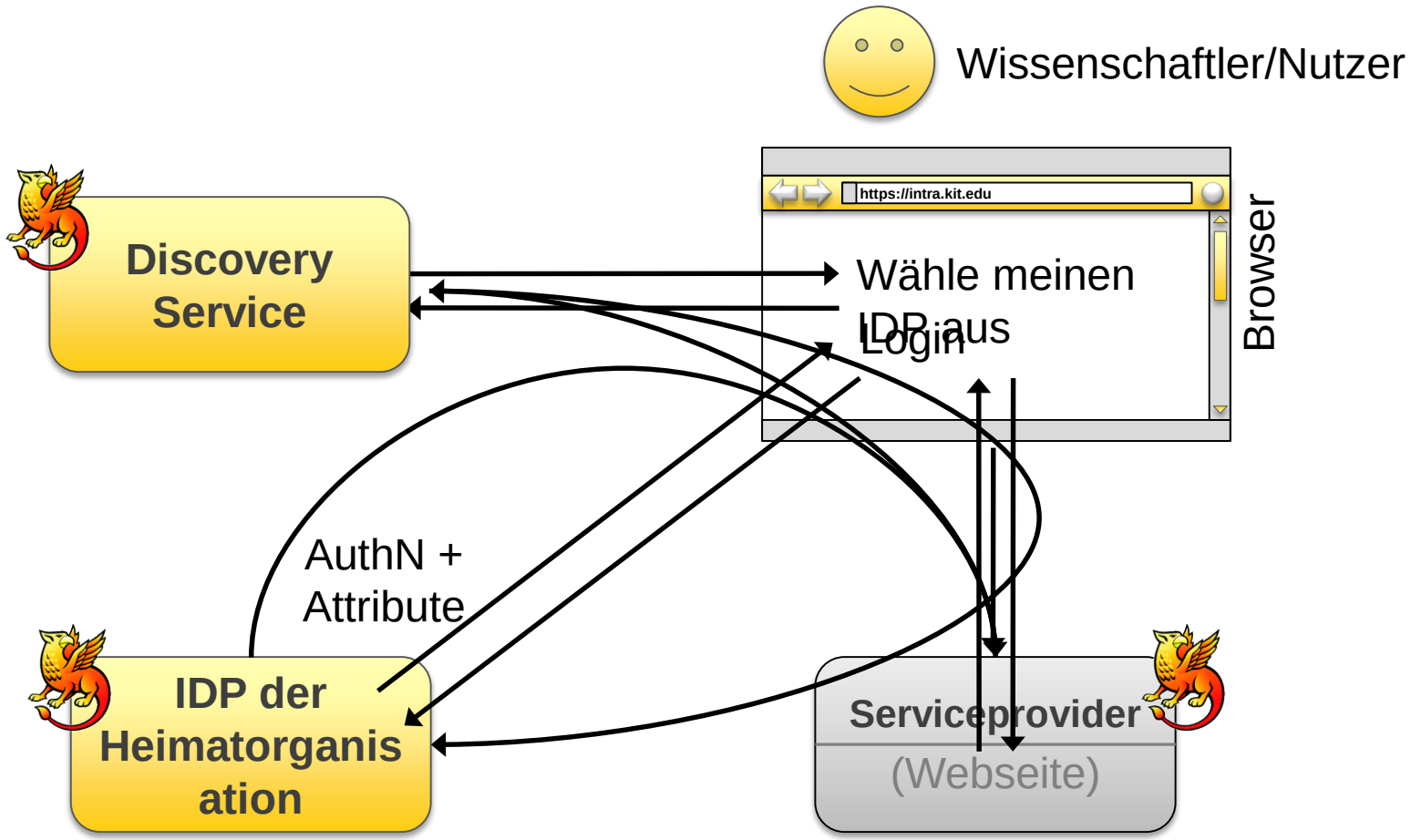
Metadata

- Konfigurationsdaten für Service- und Identityprovider

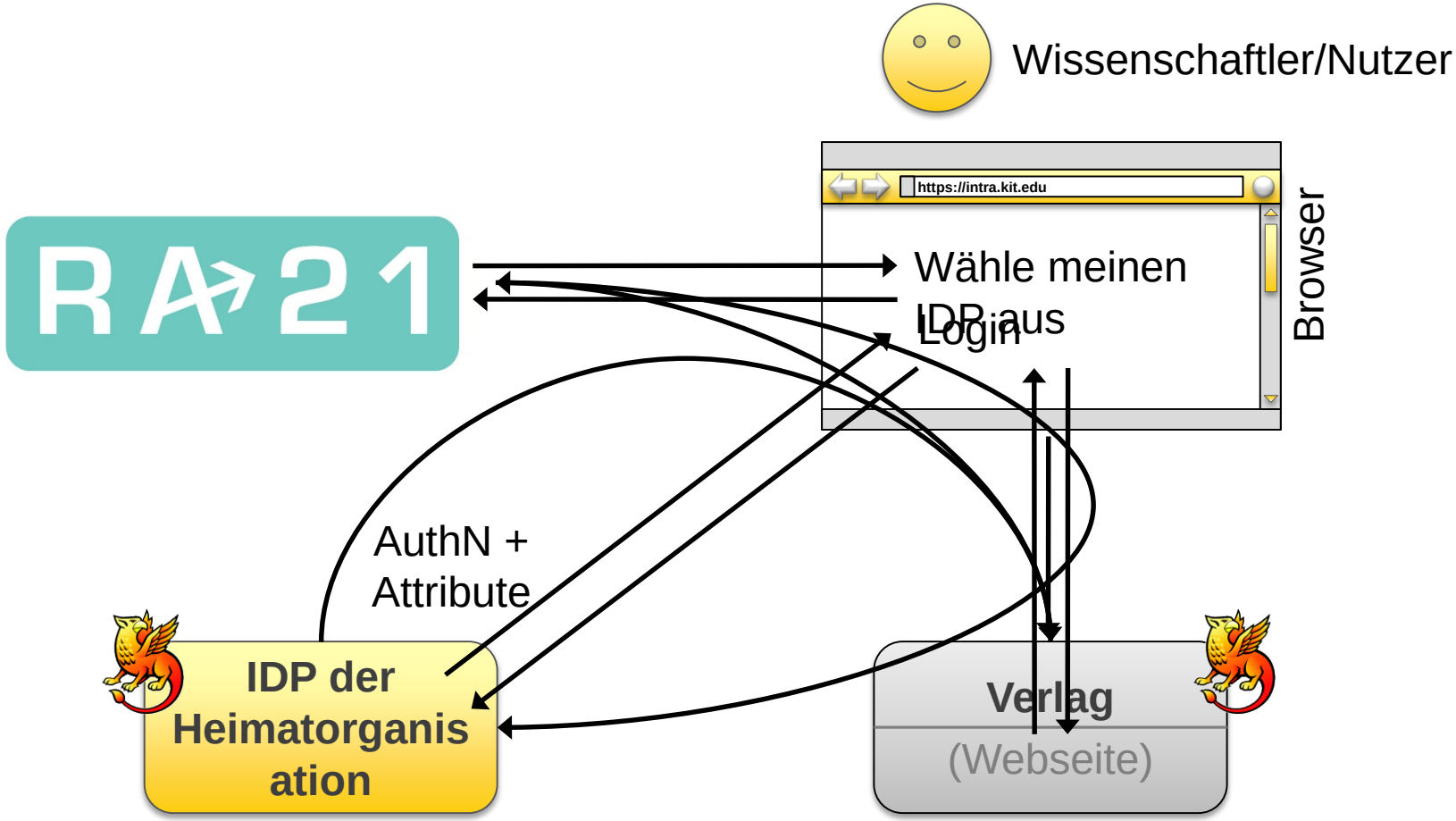
Im Hinblick Verlagszugriff ist hauptsächlich WebSSO interessant

Mit Blick auf **Forschungsdaten-Repositories** und **Zugriff auf Datenspeicher** sind aber Erweiterungen wie ECP von Interesse

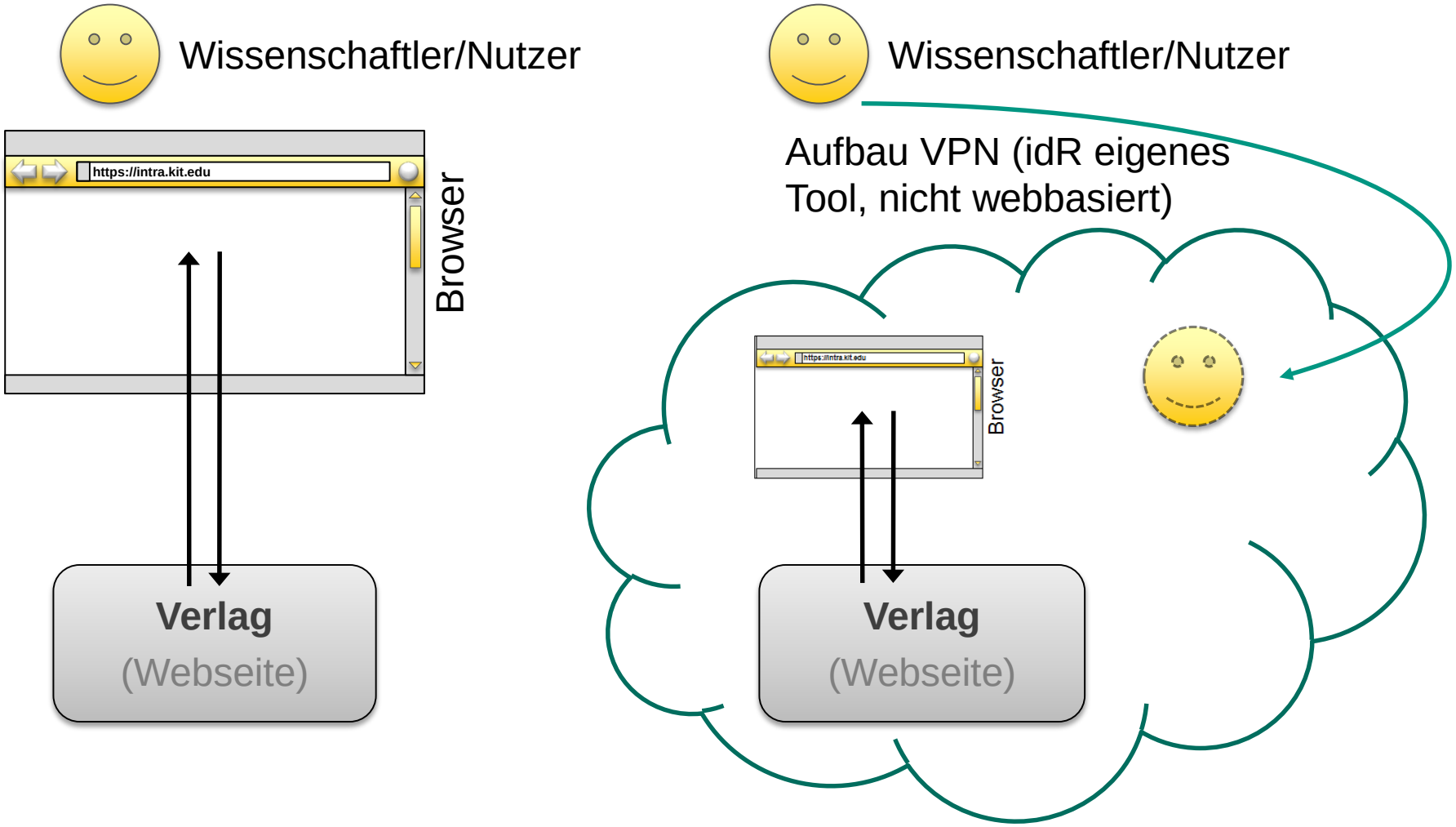
SAML-Welt im Überblick



SAML-Welt am Beispiel Verlage und RA21



Zum Vergleich: IP-Auth



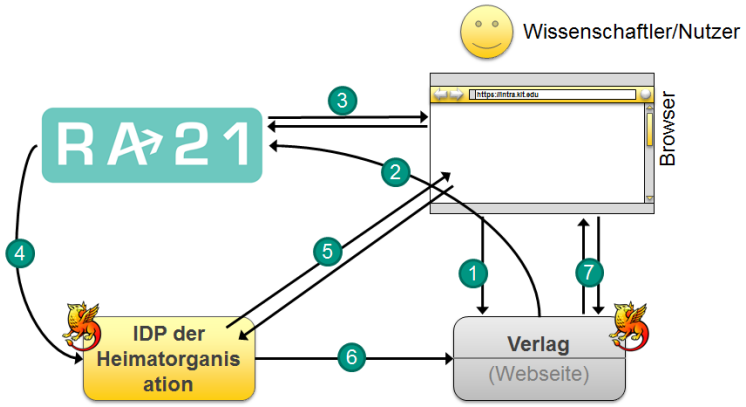
Agenda

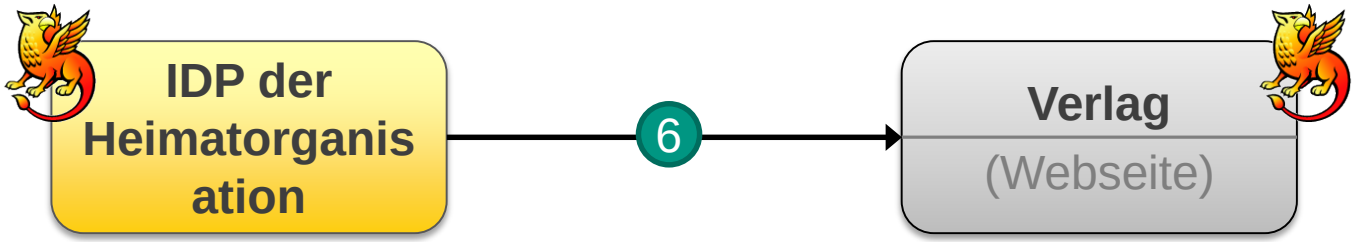
- Beobachtungen zu Authentifizierungsverfahren SAML / IP
- SAML Basics und Einordnung RA21 in die SAML-Welt
- Einordnung der „Empfehlungen zu Authentifizierungsmethoden für den Zugriff auf elektronische Ressourcen“ (Erarbeitung im DFG-Rundgespräch 01/2019) in die SAML/RA21-Architektur

Im DFG Rundgespräch 01/2019 wurde eine Empfehlung erarbeitet, die u.a. 7 Empfehlungen vorsieht

Empfehlung #1

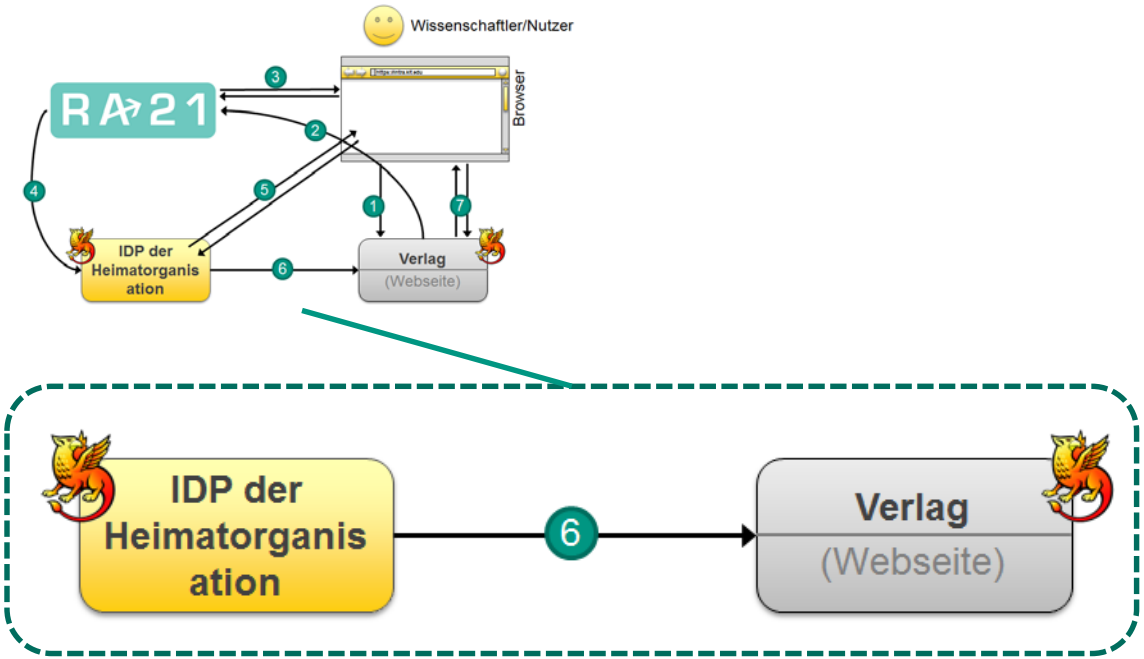
Die Entscheidung und Verantwortung darüber, welche Daten (Attribute) an Anbieter (Service Provider) übergeben werden, sollte ausschließlich bei den Informationsinfrastruktureinrichtungen (Identity Provider) liegen. Diese Einrichtungen sind aufgerufen, die Verantwortung kritisch wahrzunehmen.





Empfehlung #2

Generell sollten nur die Daten vom Identity Provider an den Service Provider übermittelt werden, die für den jeweils genutzten Dienst oder Inhalt notwendig sind. Single-Sign-On-Lösungen erfordern für die Zugangsautorisierung keine personenbezogenen Attribute. Ausreichend sind die schon eingesetzten Attribute **eduPersonEntitlement** und eduPersonScopedAffiliation.

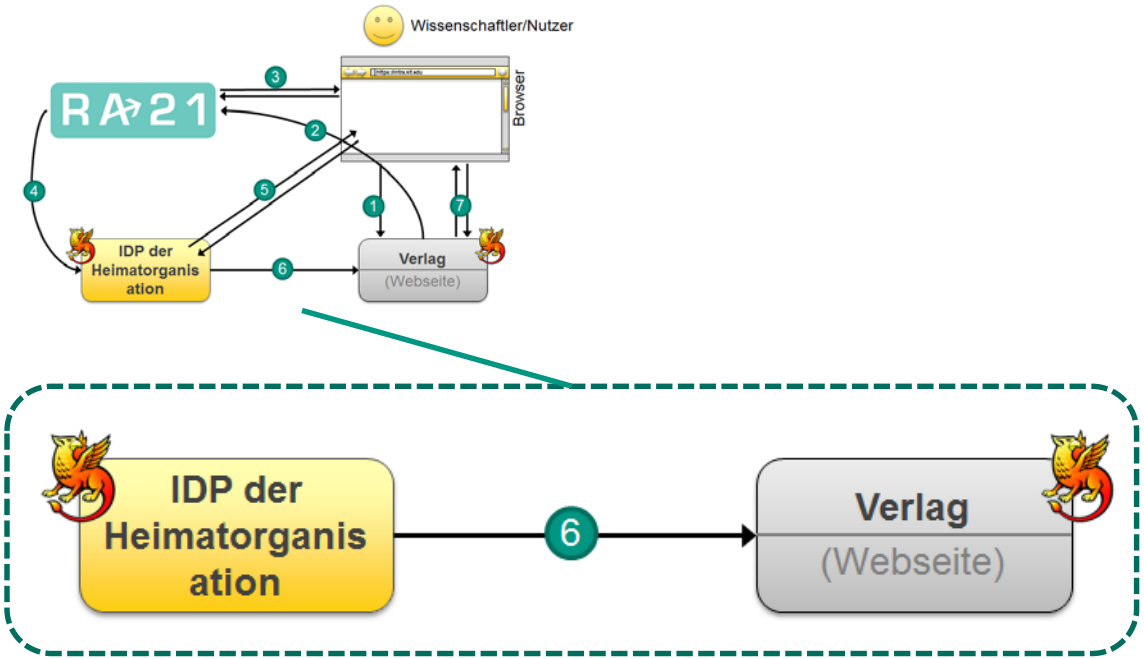


RA21 tritt zum 31.1.19 dem GEANT Data Protection Code of Conduct bei.
Auszug aus RA21-Announcement (15.3.19): "[..] Specifically, the service provider should only ask for **eduPersonEntitlement** and, optionally, a pseudonymous pairwise user identifier (e.g., eduPersonTargetedID). [..]"

https://ra21.org/index.php/2019/02/28/ra21-adopts-refeds-data-protection-code-of-conduct/

Empfehlung #3

Für Dienste, die eine Personalisierung erfordern, sollte eine *nationale* und *internationale* Verständigung zur datenschutzkonformen Attributfreigabe angestrebt werden. Eine Regelung der Weitergabe von Attributen sollte transparent und servicegruppenspezifisch erfolgen.

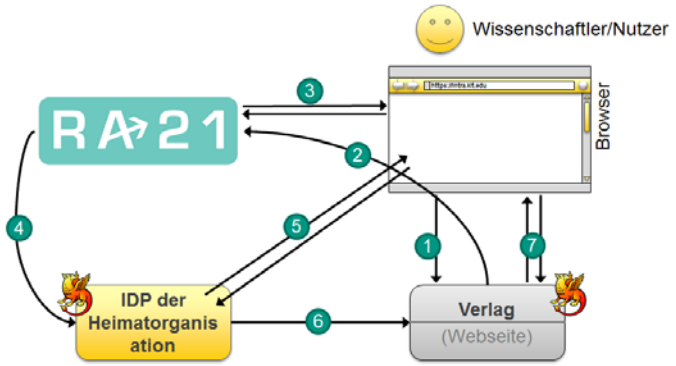


RA21 tritt zum 31.1.19 dem GEANT Data Protection Code of Conduct bei. Auszug aus RA21-Announcement (15.3.19): "[..] Specifically, the service provider should only ask for eduPersonEntitlement and, optionally, a pseudonymous pairwise user identifier (e.g., **eduPersonTargetedID**). [..]"

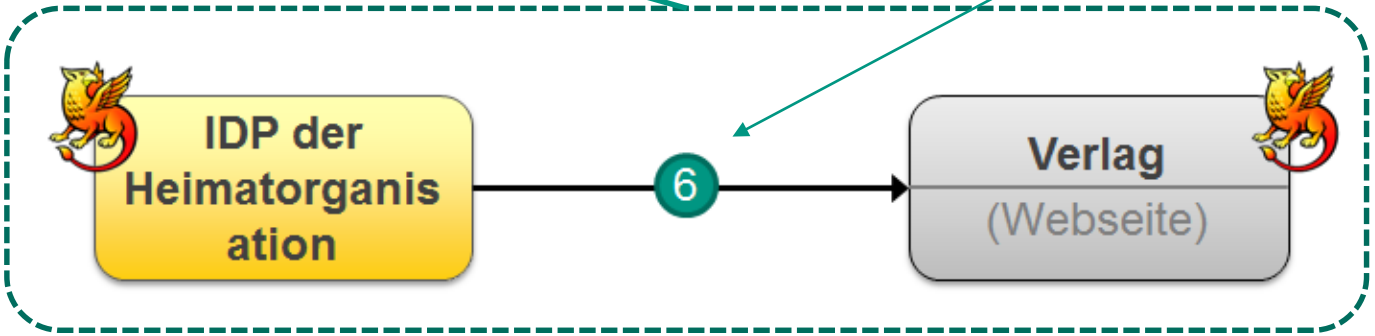
https://ra21.org/index.php/2019/02/28/ra21-adopts-refeds-data-protection-code-of-conduct/

Empfehlung #4

Zur inhaltlichen Ausgestaltung bei Übergabe von Attributen für Identity Provider sollten technische Empfehlungen erarbeitet werden. Bestehende Handlungsanleitungen wie der Code of Conduct (GEANT) sollten dabei Berücksichtigung finden.

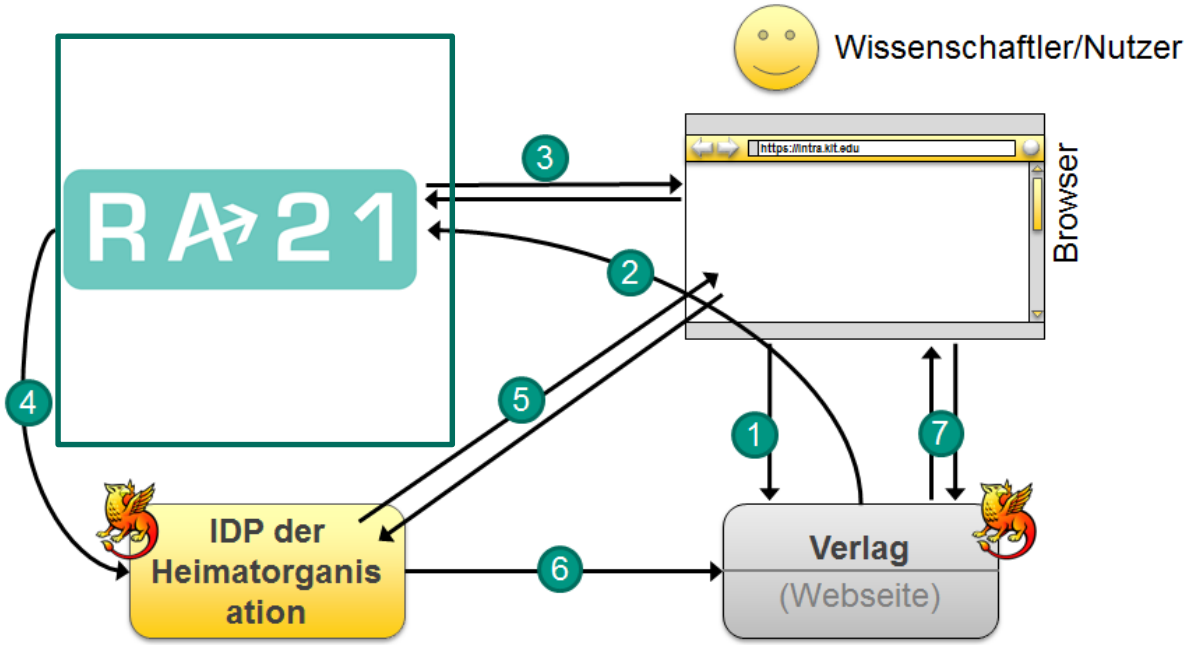


Weitergabe von Attributen definiert die Heimatorganisation. Vertrauensbildende Maßnahme in Hinblick auf personalisierte Dienste: **Verlage sollen dem GEANT Code of Conduct beitreten**



Empfehlung #5

Da auch der vermittelnde Discovery Service Daten sammeln und benutzerbezogene Daten verarbeiten kann, muss dieser in vertrauenswürdiger, neutraler und nicht kommerzieller Hand liegen.

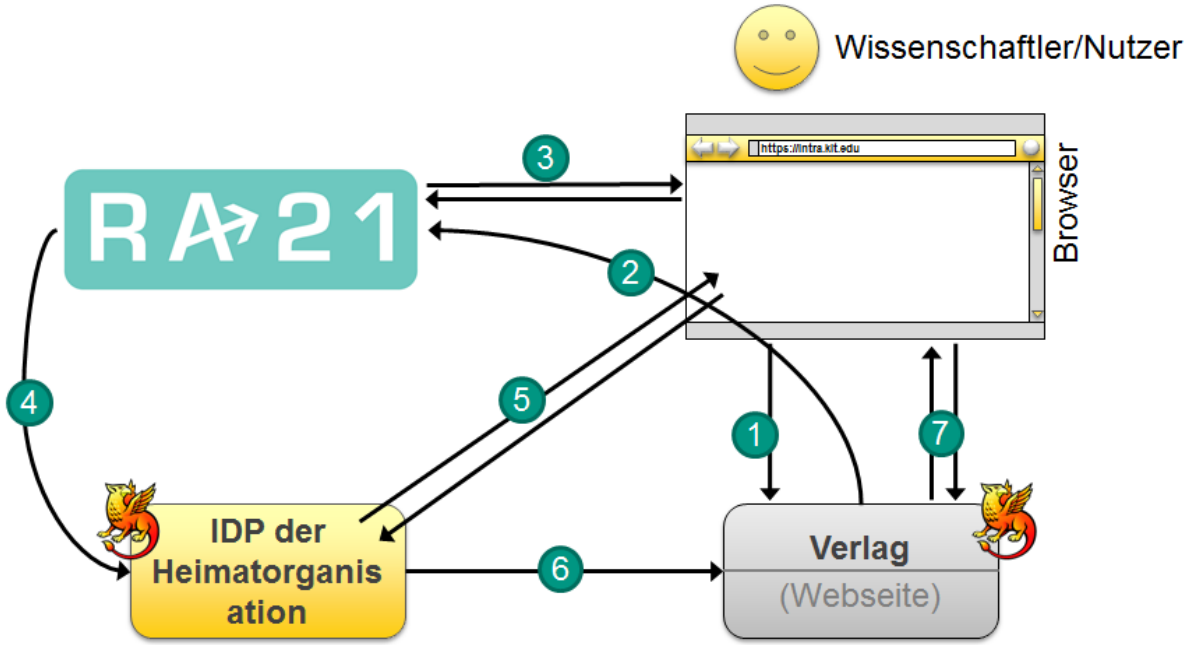


RA21 tritt zum 31.1.19 dem GEANT Data Protection Code of Conduct bei. Auszug aus RA21-Announcement (15.3.19): "[..] Specifically, the service provider should only ask for eduPersonEntitlement and, optionally, a pseudonymous pairwise user identifier (e.g., eduPersonTargetedID). [..]"

https://ra21.org/index.php/2019/02/28/ra21-adopts-refeds-data-protection-code-of-conduct/

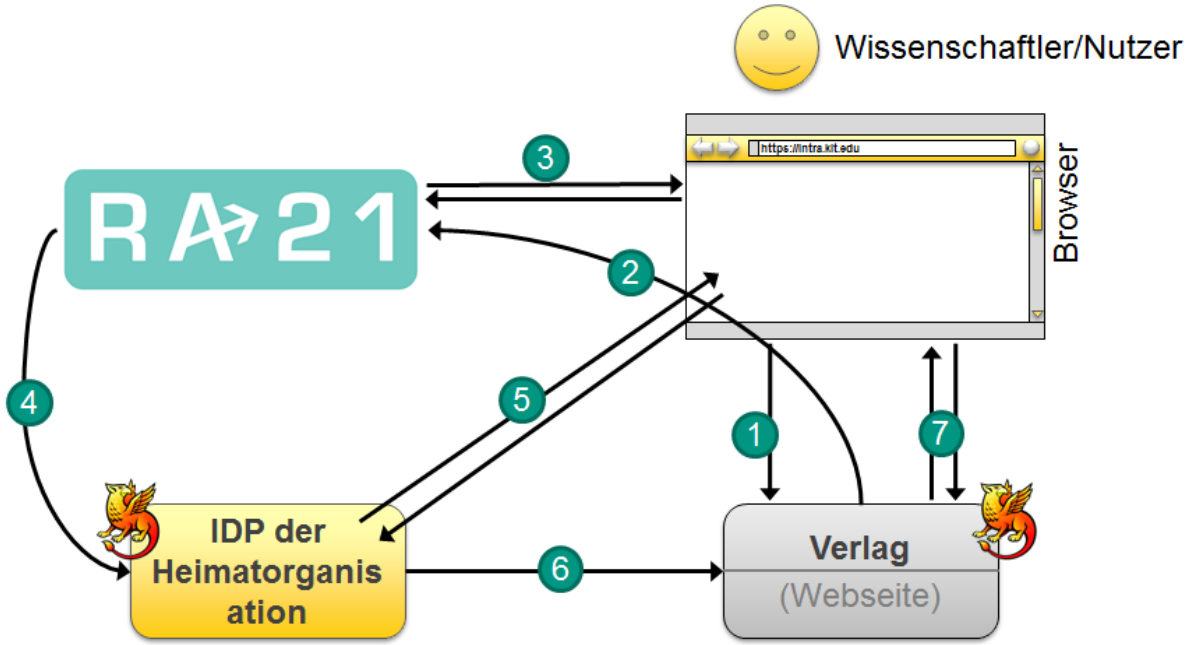
Empfehlung #6

In der lizenzrechtlichen Umsetzung sollte die ausschließliche Festlegung auf Single-Sign-On-Technologien für die Zugangssteuerung zu Inhalten und Diensten nicht akzeptiert werden. Die Möglichkeit zur Nutzung über etablierte alternative Verfahren - etwa über IP-Steuerung - sollte immer als zusätzliche Option gegeben sein.



Empfehlung #7

Grundsätzlich sollte die Open-Access-Transformation des wissenschaftlichen Publikationsmarktes prioritär verfolgt werden. Der offene Zugang zu wissenschaftlichen Inhalten ist am besten geeignet, Zugriffsprobleme zu lösen.



Fazit

- RA21 erfüllt als Discovery-Service aus technischer Sicht eine nützliche Aufgabe zur Verbreitung des Einsatzes von Personen-Auth („Weg zum IDP“)

- Im Rahmen fortschreitender Digitalisierung spielt integriertes Informationsmanagement eine zentrale Rolle
- dieses fußt auf funktionierendem Identity und Access Management
- eine wesentliche Komponente hinsichtlich organisationsübergreifender Dienste ist ein funktionierender IDP

- Die obigen Punkte gelten unabhängig der Verfügbarkeit von OpenAccess