



OpenCAST in der AAI
Harald Strack | Berlin | 19.03.2019



Agenda

- 1 **Vorstellung**
- 2 **Digitalisierung**
- 3 **OpenCAST**
- 4 **AAI Integration**
- 5 **IDM und LMS**
- 6 **Nächste Schritte**



Firmengeschichte

Gegründet im Jahr 2003 verfügt ssystems über mehr als 15 Jahre Erfahrung in der Zusammenarbeit mit Personen, Gruppen, Teams in Hochschulen, die sich mit Campus-IT beschäftigen.

ssystems mit seinen Sitzen in **München** und **Berlin** ist derzeit eines der wenigen Unternehmen in Deutschland, die mit den Herausforderungen von Campus-IT auch im Kontext großer Hochschulen vertraut sind und bei dem das konzeptionelle und technische Fachwissen existiert, um ihre Projekt kompetent begleiten zu können.

Wir sind groß genug, um komplexe Lösungen realisieren zu können und dabei menschlich präsent und organisatorisch flexibel sind.



Über uns

Umfassende, professionelle IT-Serviceleistungen

Identity und Access Management

- Beratung, Konzeption und Umsetzung
- Prozessberatung und IDM Flows
- Verwaltung und Betrieb
- Verzeichnisdienste
- SSO, Shibboleth und AAI
- Erweiterung und Integration

Server und Infrastruktur

- Campus Management
- Mail, Web, Storage
- (Managed) Hosting, IaaS
- UNIX, Linux und Netzwerke
- Virtualisierung
- Datenschutz

 **CAMPUSSPEICHER**
Hosting mit Geist.

E-Learning, E-Prüfung

- Moodle, Blackboard, CLIX, OpenCAST
- Social Learning, E-Portfolios, Mahara
- Online Klausuren – E-Assessment
- CMS: TYPO3, Drupal, Firstspirit, WordPress

undkonsorten

Anwendungsentwicklung

- CMS und LMS Erweiterungen
- Systemprogrammierung, Backends
- Customized Frontends
- JAVA, Spring, GWT, BPM
- Python, Perl, PHP, Shell, uvm.

Referenzen

Nachhaltige Dienstleistungen



Ein Leitgedanke

Digitalisierung als Werkzeug in Bildungs- und Verwaltungsprozessen

Automatisierung von Verfahren
Grundlage des digitalen Aufbruchs an
Hochschulen



Vernetzte Interaktion
Digitale Formen der
Zusammenarbeit und
Verwaltung

Veranschaulichung
Komplexe Sachverhalte
eingänglich vermitteln



Individualisierung
unabhängig von Ort und Zeit
flexibel agieren

Bildungschancen
Begabtenförderung,
Vereinbarkeit von Familie und
Ausbildung, Inklusion



Bildung im Breitbandzeitalter

„Catching the Generation YouTube“

Chancen für die Lehre:

- Autom. Workflows für optimale Usability (Branding, Texterkennung, Transcriptions, etc.)
- Autorisierung von Inhalten, Schutz von Rechten
- Vorlesungsaufzeichnung: Inklusion, Barrierefreiheit und Flexibilisierung

Chancen für Verwaltung:

- Manuals und Howtos und Supportvideos
- Workorders und Changemanagement
- Videobotschaften

Grundpfeiler Kooperation bei Streaming

Ressourcen gemeinsam nutzen

- **Bedarf** an mehreren Hochschulen
- **Hochschulübergreifende** Entwicklung und Nutzung
- **Inhalte produzieren lassen**
- Angebot **kann Studierenden** unentgeltlich zur Verfügung gestellt werden

➔ Zeitgemäße Vermittlung von Inhalten (Out-of-Home Medien)

➔ Flexibilisierung durch Breitbandausbau

➔ Prozessdokumentation und Kommunikation



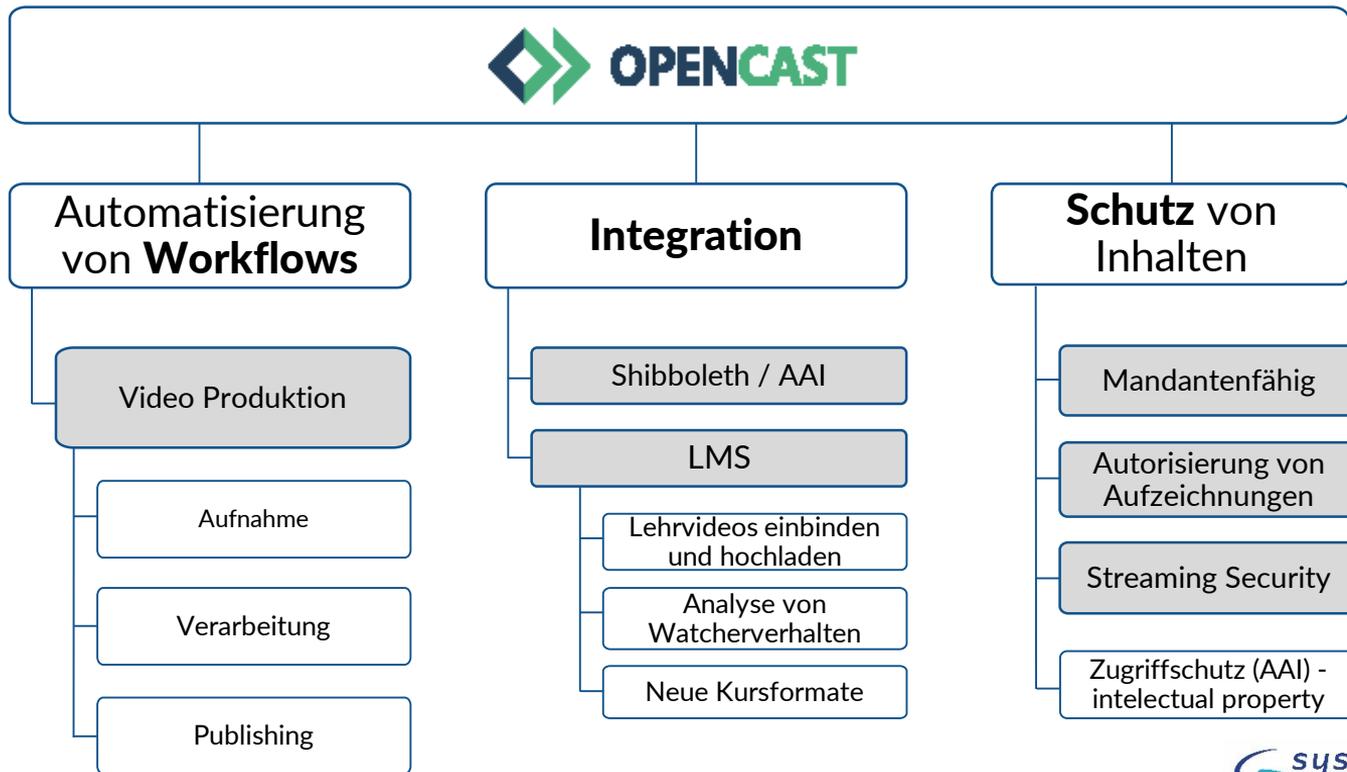
Digitalisierungsmaßnahmen

Entwicklung und Einsatz netzgestützter Lehre und Verwaltung



Video Produktion und Publikation

Mobile Streamingflatrates seit 2017 verfügbar



Video Produktion mit OpenCAST

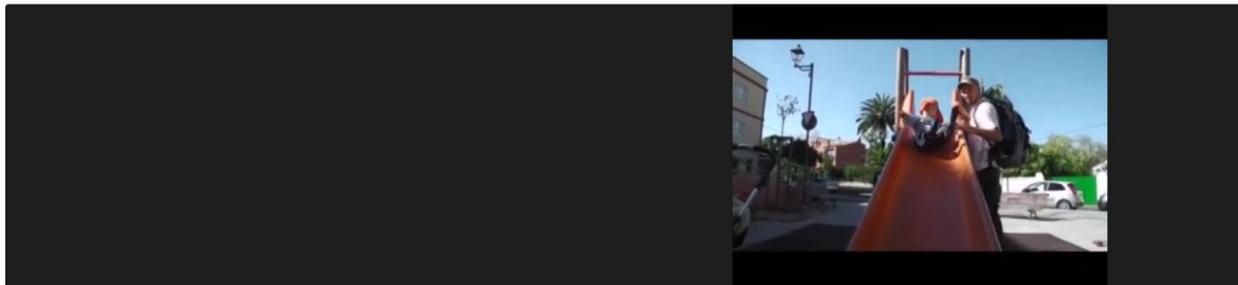
Ausgewählte Workflow Operationen



Online Schneiden

Manuelle Interaktion in Workflows

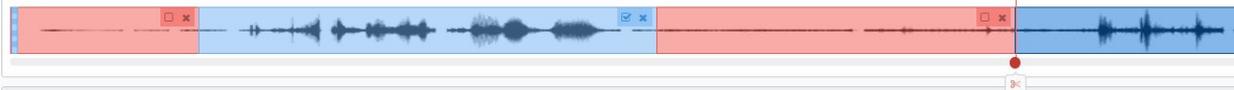
test12344
3/11/19 - Vorlesung Z



Timeline

00:00:00.000
00:00:00

Presenter



Segments Metadata Thumbnail Tracks Comments

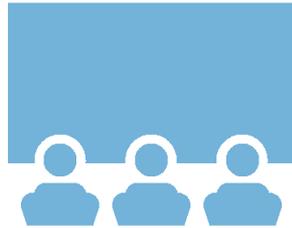


A default thumbnail used to visually represent the event is generated automatically. In case you want to use a different thumbnail, you can extract a thumbnail from the video at the current playback po

The current thumbnail has been extracted from the video.

OpenCAST Access Control

Benutzer, Rollen und Access Policies



Video Authentifizierung und Autorisierung

16

Im Hochschulumfeld

Zwei Herausforderungen

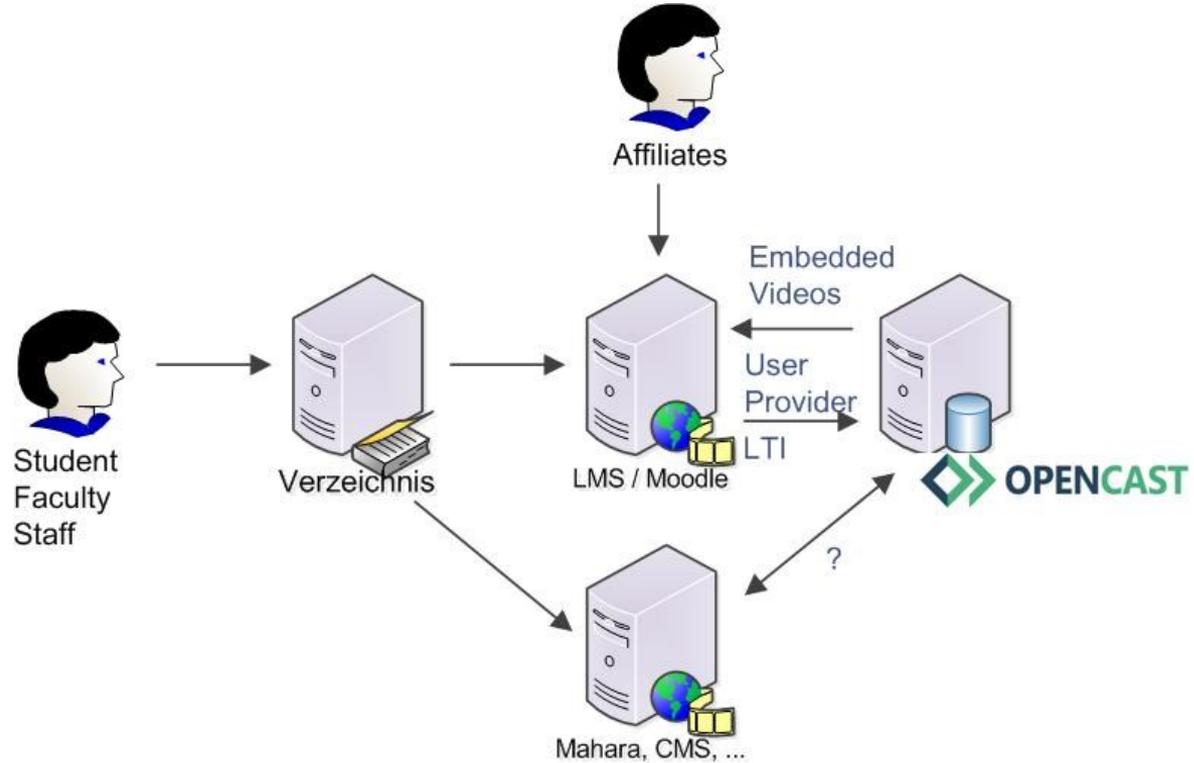
- Ver- und Bearbeiten von Videos authentifizieren und autorisieren (OpenCAST Admin UI)
- Videos im Player autorisieren (WWW-Anwendungen)

! AAI und non-AAI Strategien möglich

- ➔ User abbilden
- ➔ Rechte abbilden
- ➔ Embedding Codes „on the fly“ autorisieren

Autorisierung via LMS

Integrierte Provisionierung



Kursbezogene Autorisierung

Kopplung von LMS mit OpenCAST

Eigenschaften:

- Berechtigungen auf Kursebene einfach abbildbar
- Unabhängig von zentralen Diensten umsetzbar
- Auch externe LMS-Nutzgruppen können berechtigt werden

! Reine LMS-Lösung

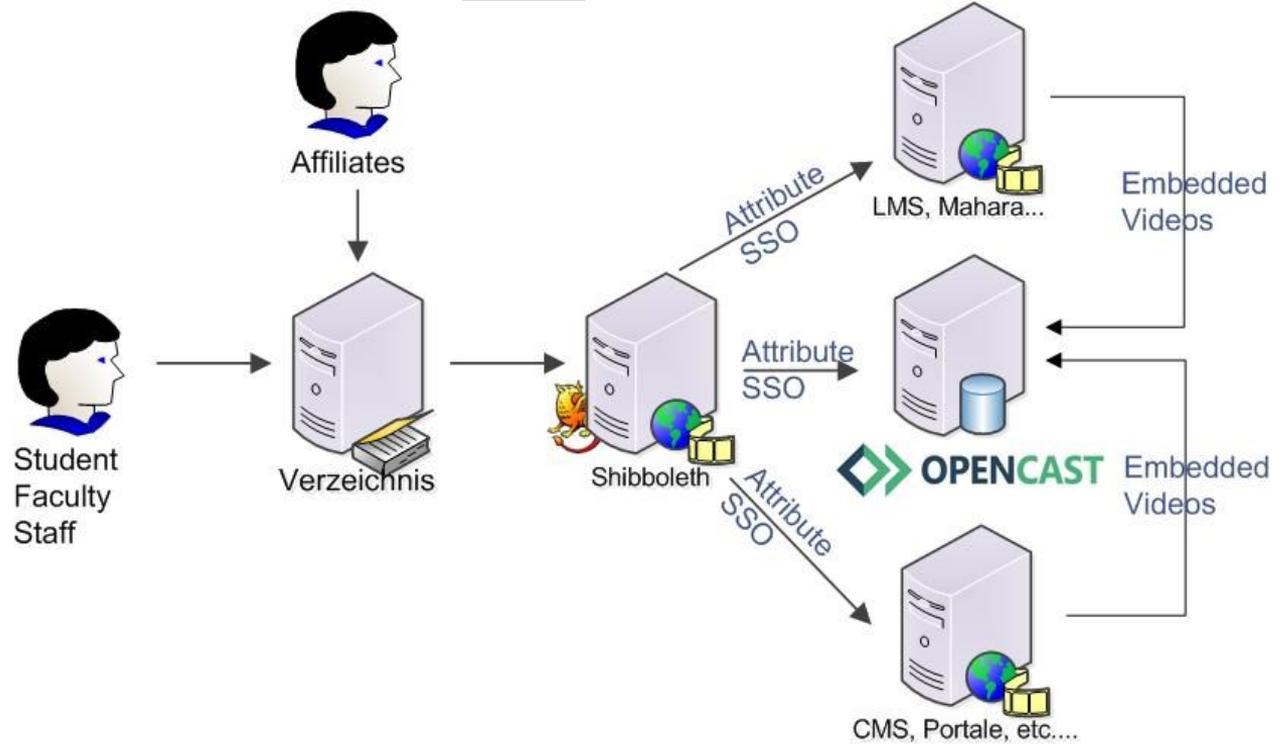
➔ Direkte Kopplung von Diensten

➔ LMS Prozesse als Basis für OpenCAST

➔ Lifecycle via LTI

Autorisierung via AAI

Entkoppelung aller Workflows



studieren

shift

Personenbezogene Autorisierung

Datenhaltung und Prozesse zur Pflege der Identitäten

Vorteile:

- Managed Lifecycle
- Auch Nicht-LMS-Nutzer können berechtigt werden
- Jede SSO-Angebundene Plattform kann Videozugriff autorisieren

! Strategie bei vielen Diensten ähnlich

➔ Technische Entkopplung via Shibboleth

➔ Anwendungskopplung von Diensten via SSO

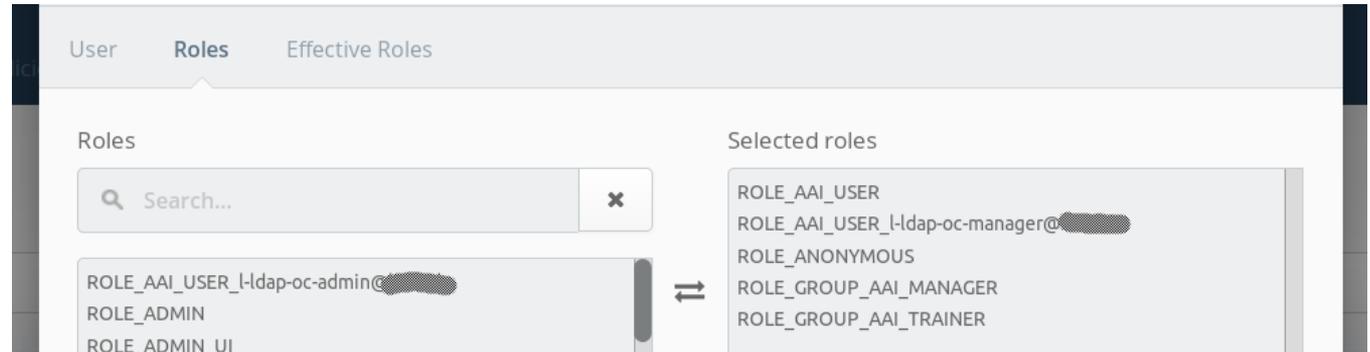
➔ Nicht invasiv

Benutzer Rollen

Spring Security Roles

Everything is a role:

- n Rollen für jeden Benutzer
- Role-Based visibility
- Gruppenrechte ebenfalls als Rolle von Rollen abbildbar



The screenshot shows a user management interface with three tabs: "User", "Roles", and "Effective Roles". The "Roles" tab is active. It features a search bar with a magnifying glass icon and a close button (x). Below the search bar, a list of roles is displayed, including "ROLE_AAI_USER", "ROLE_AAI_USER_ldap-oc-admin@...", "ROLE_ADMIN", and "ROLE ADMIN UI". To the right of this list is a double-headed arrow icon. Further right, a "Selected roles" list is shown, containing "ROLE_AAI_USER", "ROLE_AAI_USER_ldap-oc-manager@...", "ROLE_ANONYMOUS", "ROLE_GROUP_AAI_MANAGER", and "ROLE_GROUP_AAI_TRAINER".

Ressource Policies

Policy = Role mit ACL

Effektive Permissions:

- n Policies an jeder Ressource (Video)
- Je eine Rolle mit Permission Read (anschauen) und/oder Write (verwalten)
- Anonyme Rolle für öffentlichen Zugriff

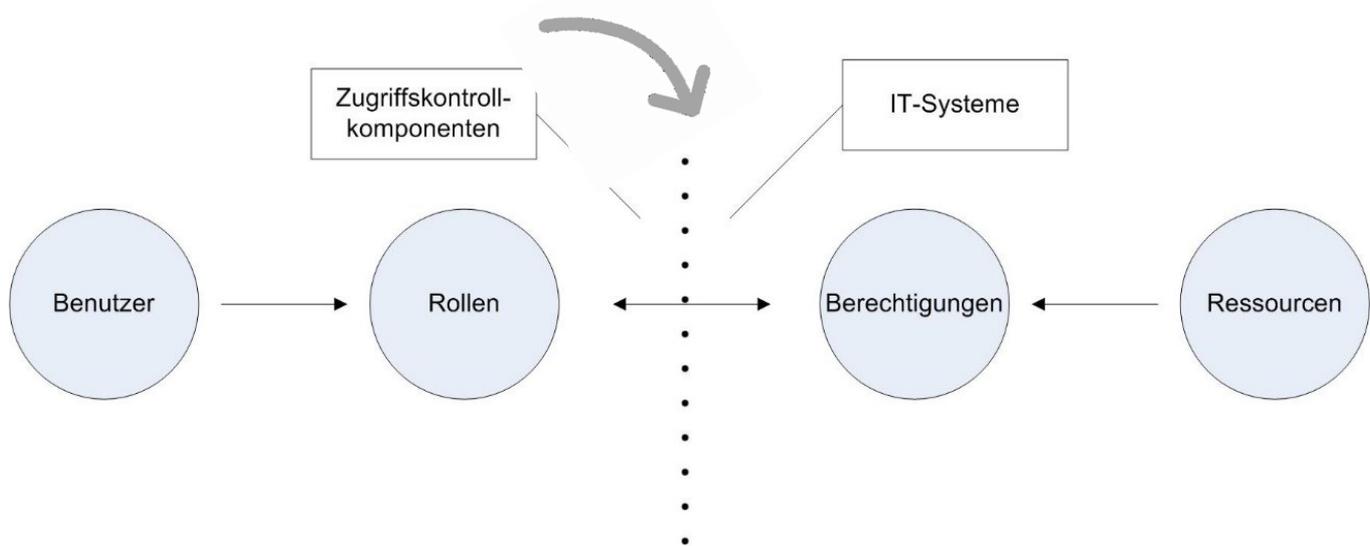
Details			
Role	Read	Write	Actions
ROLE_USER_L_VHBTEST2_	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ROLE_ADMIN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
ROLE_AAI_USER	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
ROLE_GROUP_AAI_MANAGER	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
+ New policy			

Abbildung von AAI Attributen

Funktionsrollen zu Applikationsrollen

OpenCAST Autorisierungen abbilden:

- AAI Entitlements, Affiliations Attribute auf OpenCAST-Rollen abbilden



Attribute Mapper

Abbildung von Attributen auf Rollen

Spring Expressions:

- Dynamische Ausdrücke zur Abbildung Attributen auf Rollen

Beispiel:

```
<util:list id="roleMapping" value-type="java.lang.String">  
  <!-- Statische Rolle -->  
  <value>'ROLE_AAI_USER'</value>  
  <!-- User Rolle -->  
  <value>'ROLE_AAI_USER_' + ['eduPersonPrincipalName']</value>
```

Attribute Mapper

Abbildung von Attributen auf Rollen

Spring Expressions:

- Organisationen und Abteilungen abbilden: oft schon ausreichend

Beispiel:

```
<!-- Organisations Rolle -->  
<value>['homeOrganization'] != null ? 'ROLE_AAI_ORG_' + ['homeOrganization'] +  
'_MEMBER' : null</value>  
<!-- Abteilungs Rolle f. Serien-Recht abbilden -->  
<value>['department'] != null ? 'ROLE_AAI_DEPARTMENT_' + ['department'] +  
'_MEMBER' : null</value>>
```

Attribute Mapper

Abbildung von Attributen auf Rollen

Spring Expression Language:

- Manager und einzelne Serie berechtigen

Beispiel:

```
<!-- Manager Rolle auf Basis von entitlement -->  
<value>['eduPersonEntitlement'].contains('urn:mace:...:opencast:manager') ?  
'ROLE_GROUP_AAI_MANAGER' : null</value>  
<!-- Zugriff auf Serie auf Basis von entitlement -->  
<value>['eduPersonEntitlement'].contains('urn:mace:...:opencast_dev') ?  
'ROLE_SERIES_OPENCAST_DEV' : null</value>
```

Attribute Mapper

Abbildung von Attributen auf Rollen

Role Based Visibility:

- UI Elemente Aus- und Einblenden

Beispiel:

```
<!-- Manager bekommt ACL Details angezeigt -->  
<value>['eduPersonEntitlement'].contains('urn:mace:...:opencast:manager') ?  
'ROLE_UI_EVENTS_DETAILS_ACL_VIEW' : null</value>  
<!-- Zugriff auf Systemstatus fuer RZ Mitglieder -->  
<value>['department'].equals('RZ') ? 'ROLE_UI_NAV_SYSTEMS_VIEW' : null</value>
```

Attribute Mapper

Abbildung von Attributen auf Rollen

Spring Expression Language:

- Granulare Rechte statisch oder dynamisch abbilden

Beispiel:

`<!-- Kursentitlement abbilden statisch -->`

```
<value>['eduPersonPrincipalName'].contains('urn:mace:...:student:BUB:BUB01') ?  
'ROLE_SERIES_BBUB_BBUB01' : null</value>
```

```
<value>['eduPersonPrincipalName'].contains('urn:mace:...:student:BUB:BUB02') ?  
'ROLE_SERIES_BBUB_BBUB02' : null</value>
```

Scripting Interface

Analog Attribute Resolver Scripts auf IdP

Komplexe Attributabbildungen:

- Dynamische Generierung von Rollen aus Attributen

Beispiel:

```
function extractRoles (aaiRoles,request) {  
  ...  
  en = request.getHeaderNames();  
  while (en.hasMoreElements()) {  
    headerKey = en.nextElement();  
    value = request.getHeader(headerKey);  
    logger.debug ("Header '{}' => '{}'", headerKey, value);  
    //compute roles from Shibboleth...  
  }  
  return aaiRoles;  
}
```

Scripting Interface

UI Customizing

Personalisierte Dialoge:

- Auf Rollen basierte Auswahl von Serie, Lizenz, etc.

Beispiel: `m = metadataCollection....get(DublinCore.PROPERTY_PUBLISHER....());`
`m.setValue(user.getName());`

```
m = metadataCollection....().get(...PROPERTY_LANGUAGE....());  
m.setValue("deu");
```

```
m = metadataCollection.getOutputFields().get("license");  
m.setValue("ALLRIGHTS");
```

```
m = metadataCollection.getOutputFields().get("isPartOf");  
for (Role r : user.getRoles()) {  
    //set series
```

Scripting Interface

UI Personalisierung

Aufzeichnung erstellen ✕

Metadaten
Quelle
Anlagen Hochladen
Verarbeitung
Zugriffsrichtlinie
Zusammenfassung

Metadaten

Titel *	Meine Vorlesung	<input checked="" type="checkbox"/>
Betreff *	Mein Thema	<input checked="" type="checkbox"/>
Beschreibung	Alle Schlagwoerter, unter denen das hier gefunden werden soll	<input checked="" type="checkbox"/>
Sprache	Deutsch	<input checked="" type="checkbox"/>
Rechte		<input checked="" type="checkbox"/>
Lizenz	Alle Rechte vorbehalten	<input checked="" type="checkbox"/>
Serie *	Vorlesungsreihe XY	<input type="checkbox"/>
Vortragende(r)		<input checked="" type="checkbox"/>
Mitwirkende	VHB Testuser givenName Testuser SN	<input checked="" type="checkbox"/>
Ich akzeptiere die Terms of Use *	Bitte auswählen...	<input checked="" type="checkbox"/>

Embedding

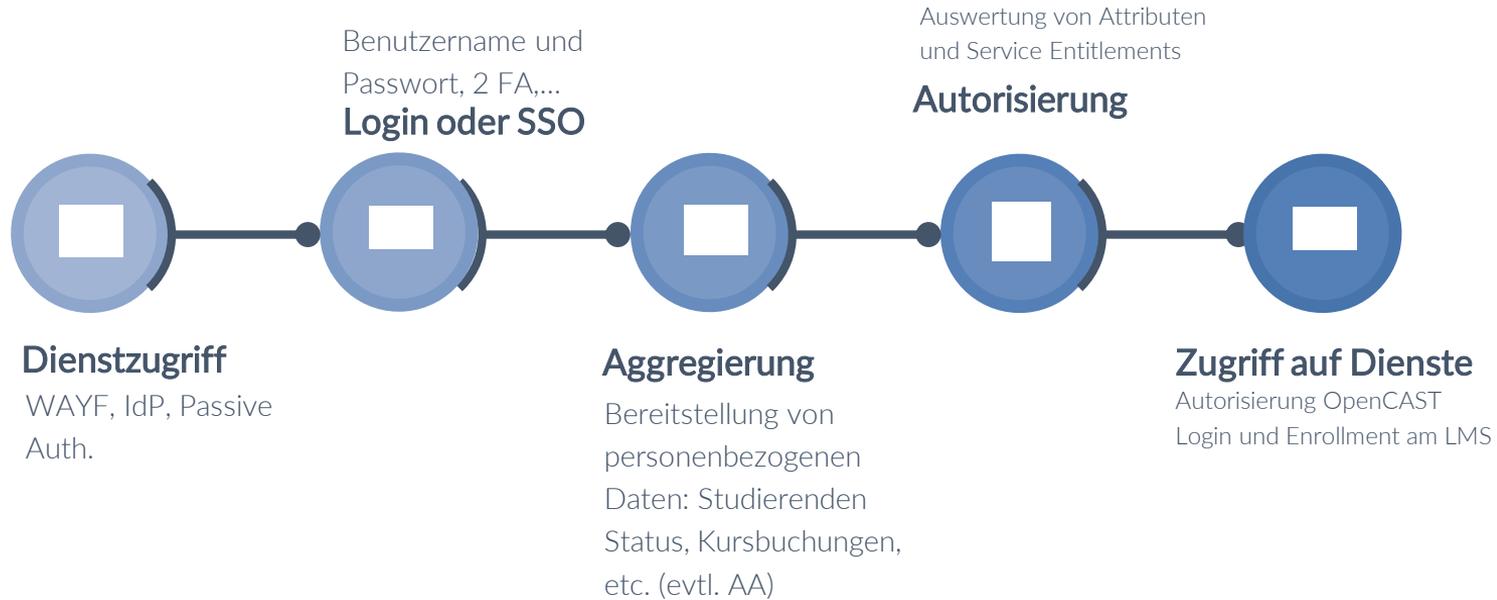
Autorisierung im SSO Kontext

The screenshot displays a web application interface. At the top, there is a navigation bar with links: Home, Dashboard, Events, Meine Kurse, Dieser Kurs, Hilfe, and Kurse. Below this is a breadcrumb trail: < Kurse. On the left side, there is a settings menu titled 'Einstellungen' with a gear icon. The menu is expanded to show 'Textseite-Administration' with sub-items: Einstellungen, Lokale Rollen zuweisen, Rechte ändern, Rechte prüfen, Filter, Logdaten, Sicherung, and Wiederherstellen. Below this are 'Kurs-Administration' and 'Website-Administration' sections, each with a search input field and a 'Suchen' button. At the bottom of the settings menu is a 'Navigation' section with a plus icon. On the right side, there is a video player. The video title is 'Technische Mechanik: Beispiel 4.1 - Berechnung der Einzelast'. The video player shows a play button and a thumbnail of two people looking at a tablet. Below the video player, there is a timestamp: 'Zuletzt geändert: Saturday, 22. December'.



Exkurs: AAI-Autorisierung

Aggregation und Autorisierung am SP



Embedding Code

Iframe oder Nativ

Autorisierung im SSO-Kontext:

- Ressourcen von OpenCAST (SP) redirecten zu Shibboleth IdP (SSO)

Embedding code

620x349 540x304 460x259 380x214 300x169

```
<iframe allowfullscreen src="<SERVER_URL>/paella/ui/watch.html?id=5af27df7-dd43-4fcc-b005-e4ba935c6ca9" style="border:0px #FFFFFF none;" name="Paella Player" scrolling="no" frameborder="0" marginheight="0px" marginwidth="0px" width="460" height="259"></iframe>
```

Copy to clipboard

Embedding: Moodle Repository

Videos in LMS einbinden

Anbindung an OpenCAST über External API

Backchannel Autorisierung (non-AAI)

- Moodle Rolle berechtigt Zugriff auf Repository
- OpenCAST berechtigt Zugriff auf Videos

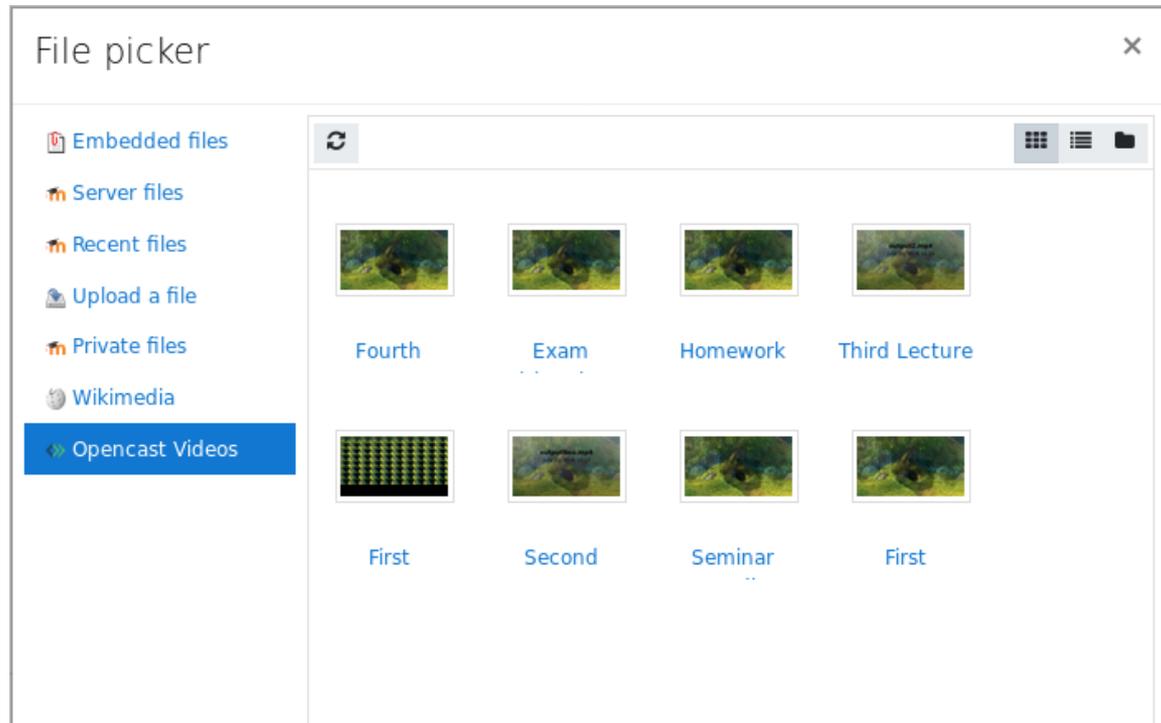
➔ Zugriff auf alle berechtigten Videos

➔ Zugriff auf eigene Videos

➔ Volltextsuche

Moodle Repository

Analog Attribute Resolver Scripts auf IdP



Zusammenfassung Entkopplung

Dienstübergreifende Autorisierung

Voraussetzung für Entkopplung

- Gemeinsame Benutzerdatenbasis in LMS, OpenCAST und weiteren Plattformen, SSO-Anbindung

! Ensure consistent, perpetual aggregation (same keys on the different sources) if user data is merged from different sources

➔ Multi-Platform

➔ Mandantenfähig

➔ Hochschulübergreifender Einsatz

Exkurs: LMS Enrollment via AAI

AAI Enrolement für Moodle

▼ Rollen Zuweisung **Trainer/in**

Rolle, in die degradiert werden soll ?

Attributwert ?

▼ Rollen Zuweisung **Trainer/in ohne Bearbeitungsrecht**

Rolle, in die degradiert werden soll ?

Attributwert ?

▼ Rollen Zuweisung **Teilnehmer/in**

Rolle, in die degradiert werden soll ?

Attributwert ?

Ebenen:

- Personendaten
- Ressourcen
- Auth.
- Autorisierung
- Lifecycle Mgmt.

studieren

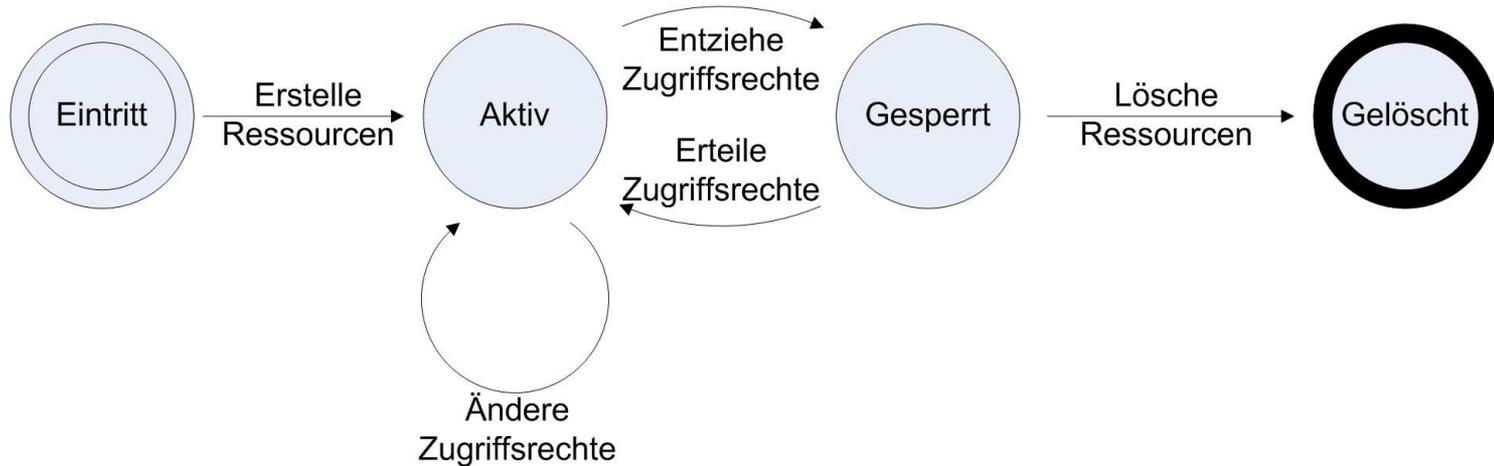
shift

Exkurs IDM: AAI Backends

Datenhaltung und Prozesse zur Pflege der Identitäten

Typischer Kontext:

- Affiliations und Entitlements als Grundlage für Zugriffsrechte
- Beliebige Attribute als Grundlage für Zugriffsrechte



(DFN-)AAI als Innovationsturbo

organisatorisch / technischer Rahmen für den Austausch von Nutzerinformationen

Digitalisierung

Nutzung von SSO/AAI Infrastruktur

- Rahmen für Entwicklung von digitalen Prozessen
- SOA, wohldefinierte Microservices, ESB, SB Federation (!)

Voraussetzung:

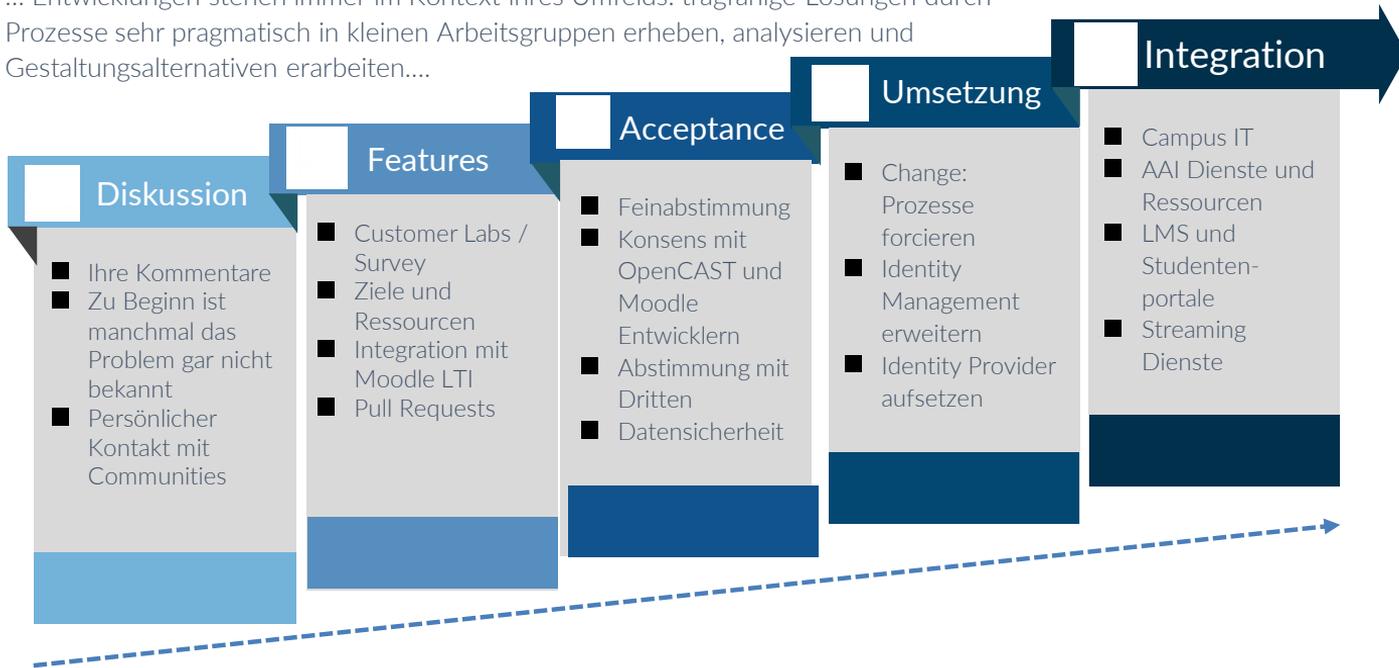
- ➔ Einführung von SSO-Systemen
- ➔ Teilnahme an DFN-AAI
- ➔ Anbindung v. Diensten: OpenCAST

Nächste Schritte

Wie aus guten Ideen Core Features werden

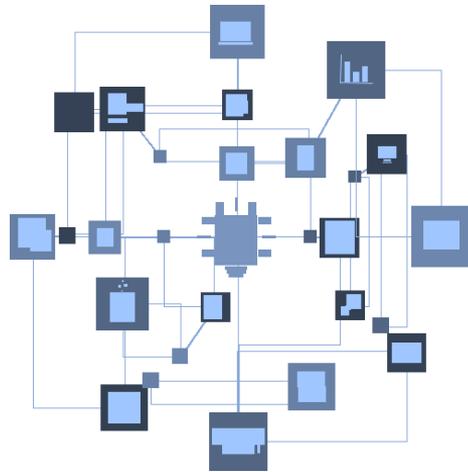
OpenSource Software Entwicklung...

... Entwicklungen stehen immer im Kontext ihres Umfelds: tragfähige Lösungen durch Prozesse sehr pragmatisch in kleinen Arbeitsgruppen erheben, analysieren und Gestaltungsalternativen erarbeiten....



Innovation

Entwicklung und Umsetzung einer Digitalisier



25%

Koordination und Strategie

Klare Richtung vorgeben, Initiativen passend zur Strategie wählen, konkrete Herausforderungen und Ziele definieren

25%

Lehre

Übergeordnete Idee des Kundenbedürfnisses: Was benötigt der Student von morgen? Oder heute schon? Wie lernen Studenten heute?

25%

Ressourcen

Wo werden Ressourcen eingesetzt? Externe Partner, Freelancer, Projektallianzen und interne Ressourcen. Macrobudgets und Minibudgets.

25%

Balance der Ressourcen

Das Erforschen von Neuem (Exploration) und das Verwerten von Bestehendem (Optimierung).

studieren

shift

ssystems Consulting

Ihr Partner für innovative Digitalisierung

online studieren

 info@ssystems.de

 030202360710

 www.ssystems.de