

eduTAP digitale Ausweise im Wallet

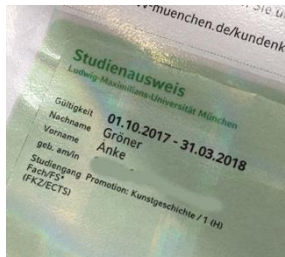
AK IdM 2026 @ Hochschule Kempten
2026-07-22

Alexander Loechel
Referent IT-Projekte · IT-Services · LMU München



Der Weg der Ausweise ins Smartphone-Wallet Der LMU-Studierendenausweis (im Zeitverlauf)

LMU
Student ID
bis 2019



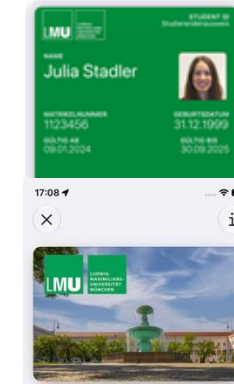
Dumb Campus
(konventionell,
analog, manuelle
Prozesse)

LMUcard
Student ID
2019-2025



Smart Campus
(vernetzt, IoT & Smartcards;
Datensilos, isolierte Systeme)

LMU
Student ID
2025/2026+



heute

Smarter Campus
(Interoperabilität, Personalisierung;
KI und Datenanalyse)

LMU
Student ID
2027+ ?



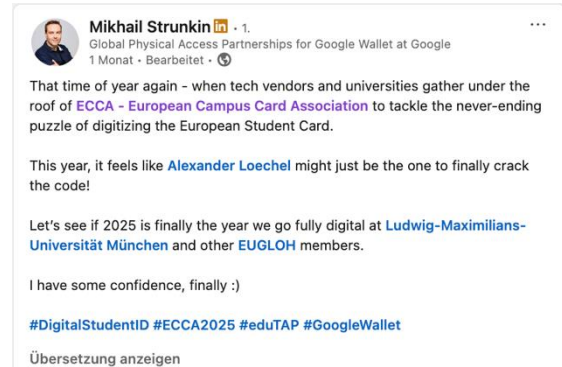
Hochschul-ID
(Studierende / Beschäftigte /
Affilierte)

- ✓ Verifiable Credentials
- ✓ Selective Disclosure
- ✓ Zero Knowledge Proofs
- ✓ Abbildung wichtiger Shibboleth-Attribute

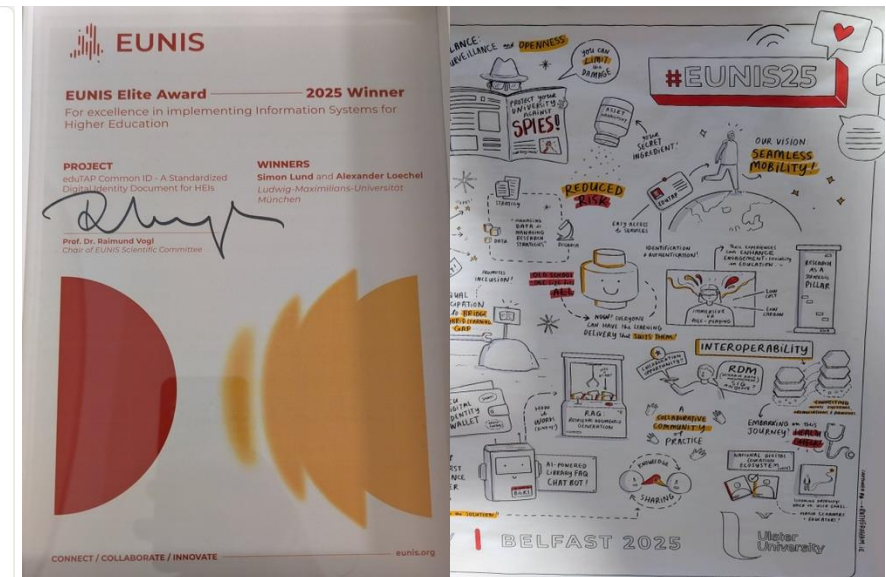
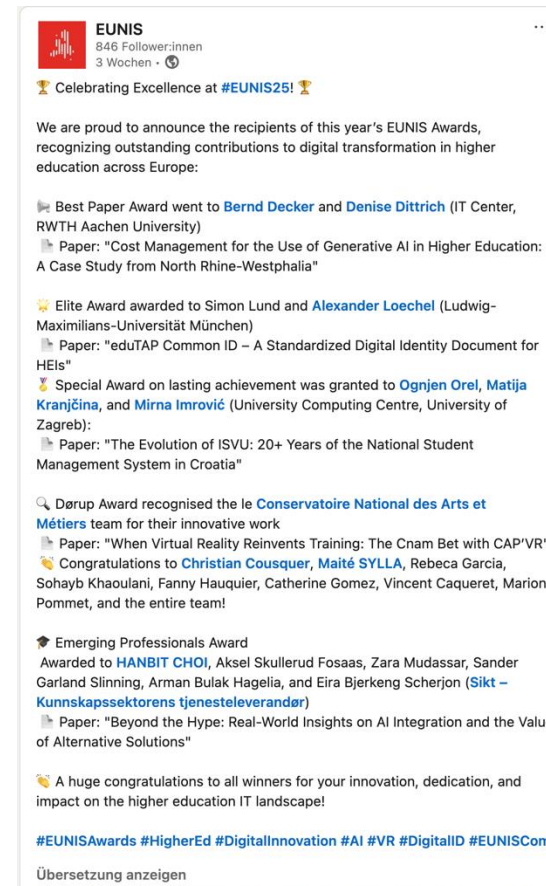
eduTAP & eduTAP@LMU

Referenzen & Auszeichnungen → eduTAP und digitale LMU-Ausweise als Beispiel

ECCA-Konferenz 2025 – LMU München



EUNIS-Konferenz 2025, Belfast (UK) → EUNIS Elite Award



Identity Management (IDM) / Identity and Access Management (IAM) VS eduTAP - Digitale Ausweise?

→ *Zugang zu Services*

Ausweise als Authentifizierungsfaktor für den Zugang zu Services

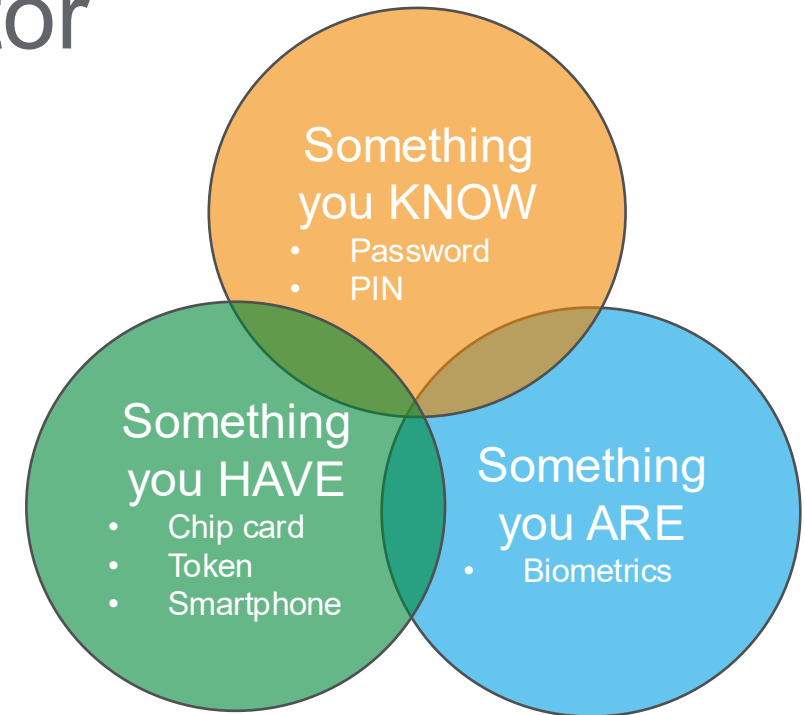
→ Triple-**A**-System

- (Identification)

- **Authentication**

- **Authorization**

- **Accounting**



Authentifizierungsfaktoren

Wieso eduTAP? Warum dieses Projekt

Wie es zu eduTAP kam – drei Rahmenbedingungen, die zusammen kamen:



LMUcard · 2015–2019

Die LMU führt die multifunktionale Campuskarte ein – eduTAP führt dieses Thema direkt fort.

+



EUGLOH · seit 2019

Die LMU wird Teil der European University Alliance: EUGLOH (European University Alliance for Global Health) – Die Allianz setzt Ziele für Zusammenarbeit.

+



Erasmus+

Erasmus+ · 2021–2027

Die 6. Programmgeneration der Erasmus-Verträge bringt mit der ECHE die Digitalisierungs-Verpflichtungen der ESCI:

- EWP, OLA und IIA
- ESC + ESI



LUDWIG-
MAXIMILIANS-
UNIVERSITÄT
MÜNCHEN

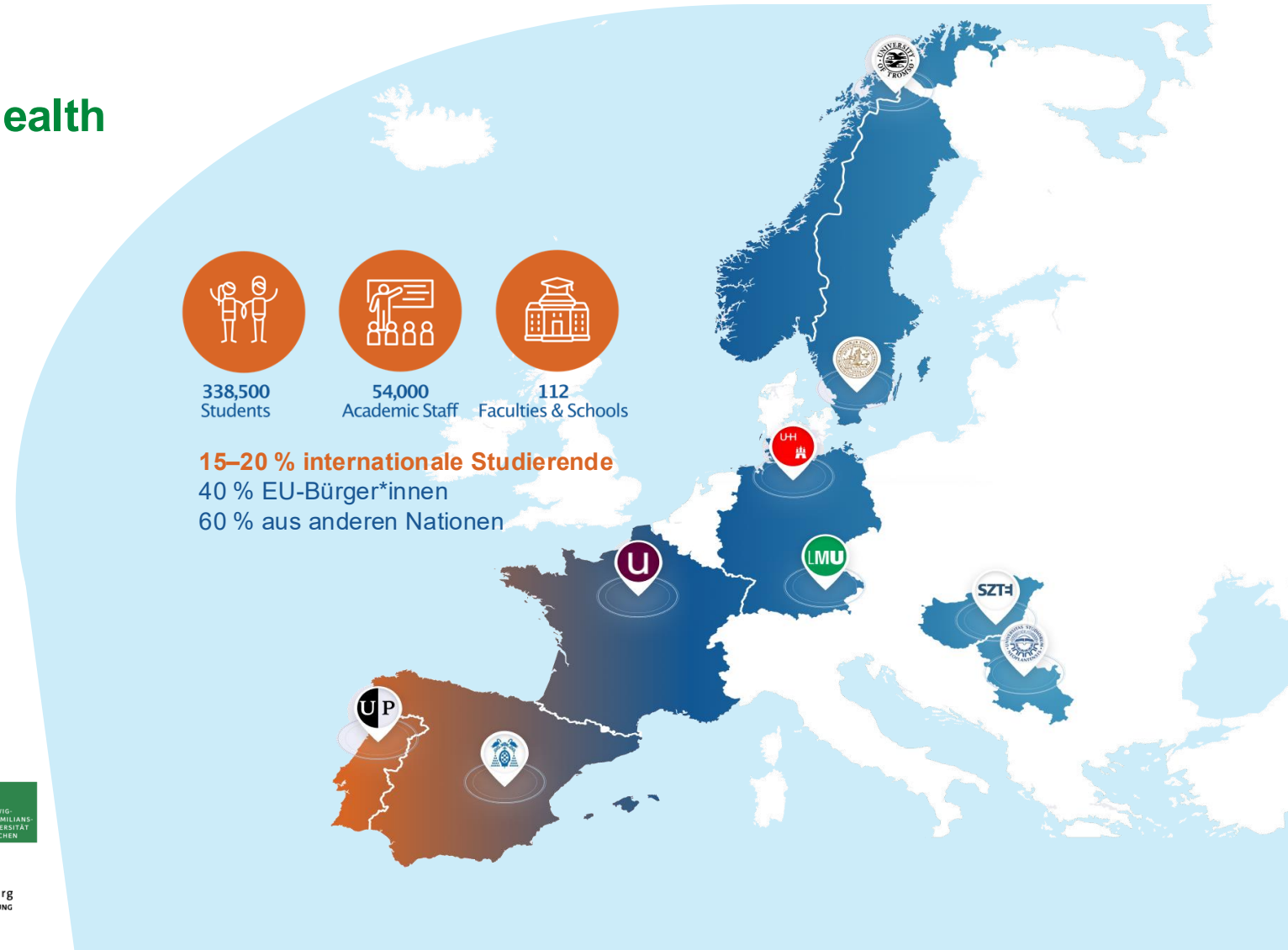
EUA: EUGLOH, Erasmus+ + ECHE & die European Student Card (ESC)



9 Universities, 1 Goal

Build Europe's Campus for Global Health

- ✓ Equip students and staff with the competencies for the future of Global Health
- ✓ Create a **seamless, inclusive European Campus** enabling **mobility**, shared learning opportunities and a **shared infrastructure**
- ✓ Tackle pressing health challenges through interdisciplinary, co-created education, research and innovation responsive to societal needs



Vision of the European Commission:

Towards a European Education Area Erasmus+

It is in the shared interest of all EU Member States to harness the full potential of education and culture as drivers for job creation, economic growth and improved social cohesion, as well as a means to experience European identity in all its diversity.

The Commission is developing initiatives to help work **towards a European Education Area**.
The vision contained within this policy is that, across the EU:

- ✓ **spending time abroad to study and learn should become the norm**
- ✓ school and higher education qualifications should be recognised across the EU
- ✓ knowing two languages in addition to one's mother tongue should be standard
- ✓ everyone should be able to access high-quality education, irrespective of their socio-economic background
- ✓ people should have a strong sense of their **identity as a European**, of **Europe's cultural heritage** and its diversity

Quelle: https://ec.europa.eu/education/education-in-the-eu/european-education-area_en

ESCI – die ECHE-Anforderungen an Hochschulen: „Implement the priorities of the Program:

- By undertaking the necessary steps to **implement digital mobility management** in line **with the technical standards of the European Student Card Initiative.**
- ...“

Quelle: https://ec.europa.eu/info/funding-tenders/opportunities/docs/cap/eplus2020/eche-fp-2020/1877638-charter-annotated-guidelines-feb2020_en.pdf

Timeline – European Student Card Initiative (ESCI)

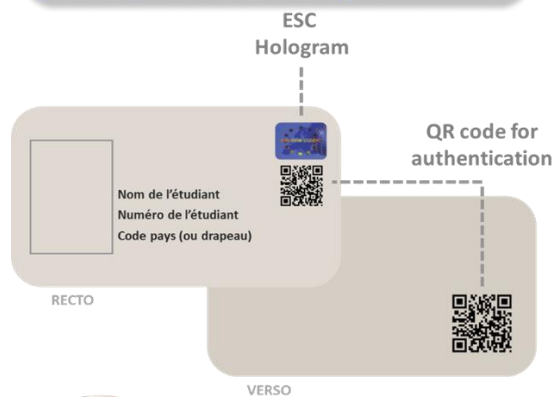
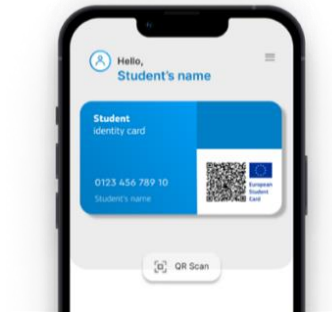
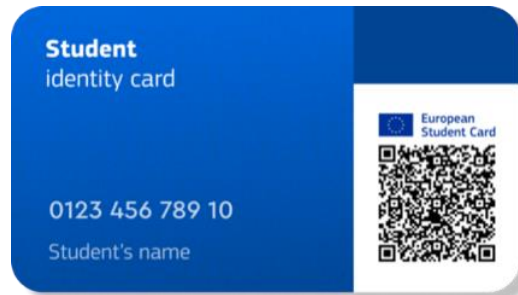
- Erasmus Without Papers (EWP)
 - 2021 – Online Learning Agreements (OLA)
 - 2022 – Inter-Institutional Agreements (IIAs)
 - 2023 – Exchange Student Nominations, Acceptances, Transcripts of Records
- MyAcademicID
 - 2022 – European Student Identifier (ESI)
- European Student Card Project (ESC)
 - **2025 – European Student Cards einführen und ausstellen** (*wird aber nicht sanktioniert*)

Mobile Identity → Digitale Identität

Der Mobility-Use-Case – Die European Student Card (ESC)

Die **European Student Card** – ein Projekt, das lokalen Studierendenausweisen eine **europäische Dimension** hinzufügt

✓ Studierendenstatus sicher validieren



European Student Card logo

Combines the European identity (text & flag) with the QR code. It facilitates the implementation and recognition of the ESCs

ESCN - European Student Card Number

Unique card identifier that serves to link a specific card to the specific higher education institution who produced it and to identify a card

ESI - European Student Identifier

Unique identifier that allows to link a given student to a specific ESC. It is not recommended to be printed on the card.



European
Student Card



Idee von →
Jean-Paul
Roumegas
(les Crouse)



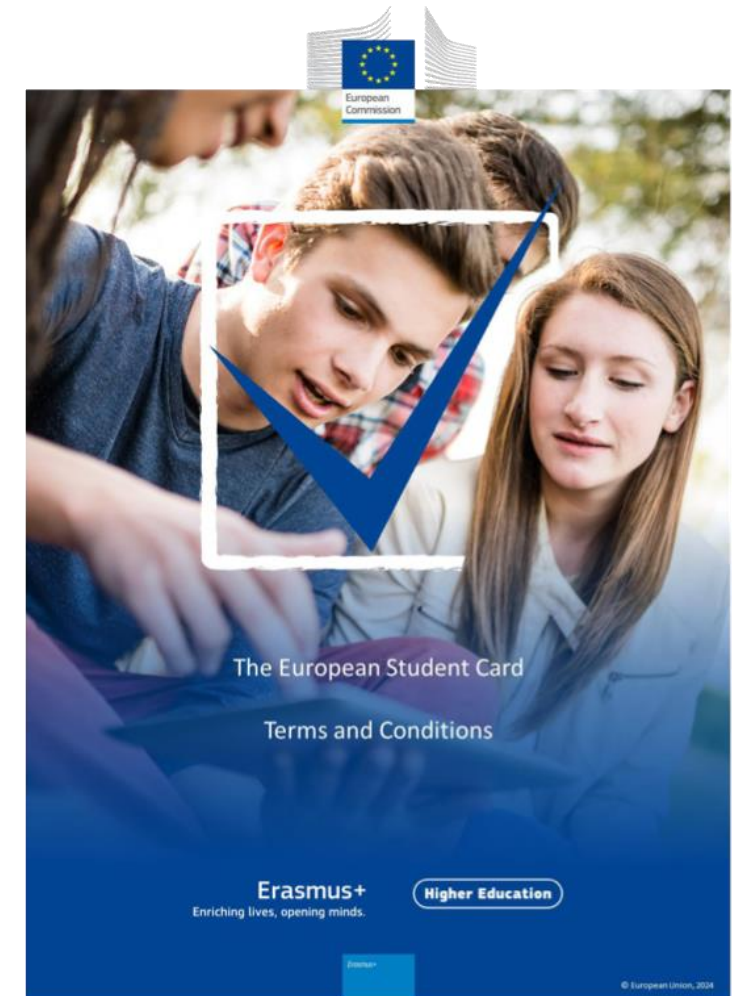
Eine großartige Vision

ESC Terms and Conditions

Reciprocity of recognition

All users agree to the **principle of reciprocity of recognition**, whereby they commit to recognising the European Student Cards issued by any other user and granting ESC holders enrolled in their institution participating in a student mobility programme, to the best of their ability, **access to the same services** and **quality of service** that they would grant to their own students.

This reciprocity of recognition supports students' seamless mobility and integration across the participating HEIs and throughout Europe.



A complex system that works is invariably found to have evolved from a simple system that worked. The inverse proposition also appears to be true:

***A complex system designed from scratch never works
and cannot be made to work.***

You have to start over, beginning with a working simple system.

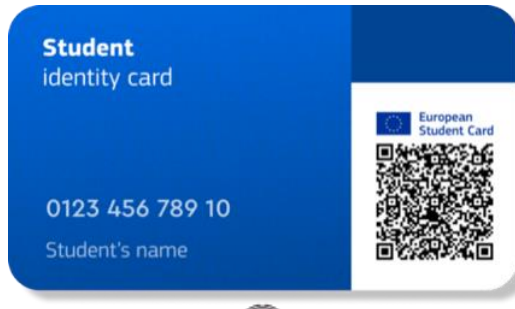
Source: "John Gall's law" - from "Systemantics: How Systems Really Work and How They Fail" – 1975

- Die Vision der European Student Card ist nicht top-down lösbar – nicht mit der aktuellen technischen Spezifikation und Implementierung
- Ein neuer Ansatz ist nötig – auf Basis existierender, bewährter Technologien

Die European Student Card (ESC)



European Student Card

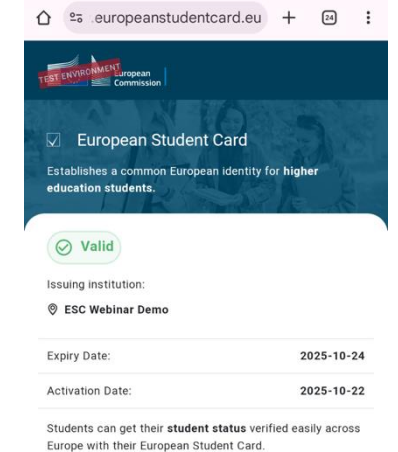


Nahtloser Zugang zu physischen und digitalen Services
während der Mobilität – z. B.
Bibliothek, ÖPNV, physischer Zutritt



One Credential to rule them all?
Per QR-Code oder als Verifiable Credential?

nicht realistisch



This is a test environment. The credentials displayed here are NOT valid.

EUGLOH & ESC – die gemeinsame Vision

Wir haben eine gemeinsame Vision: **seamless mobility & easy service access**

Aber eine ESC per QR-Code war für uns keine Option (DSGVO & IT-Sicherheit)



eine großartige Vision



EUGLOH möchte seine Services teilen – in der Allianz und darüber hinaus (wir alle haben weitere Partner)



Die IT-Leute von LMU, U.Porto und Lund kannten sich bereits, kennengelernt auf der ECCA 2019

- ✓ **verstehen die technologischen Möglichkeiten,**
- ✓ kennen und **verstehen** die Themen, haben Zugang zu den großen Technologieanbietern
- ✓ aber auch zu den Fähigkeiten des ESC-Projektteams

→ Wenn wir zeitnah eine gute und **interoperable Lösung** wollen, müssen wir einen funktionierenden Vorschlag vorlegen,

→ der unsere Anforderungen und Zielgruppen erfüllt (Studierende, Beschäftigte, Fachkräfte)

Mobile Identity → Digitale Identität Eine gemeinsame Vision

EUGLOH & die European Student Card haben eine **gemeinsame Vision**

✓ **seamless mobility**

✓ **easy service access**

Für:

- ✓ Studierende,
- ✓ Beschäftigte und
- ✓ Fachkräfte



EUGLOH ESC Working Group
gegründet Ende 2020:

Alle EUGLOH-Universitäten sollen die ESC einführen
und gemeinsame Services definieren (Lead: Paris-Saclay).

2022 übernahm die LMU den Technical Lead

Aber: unterschiedliche Zielgruppen und Ausgangslagen

Technische Anforderungen → echte **technische Interoperabilität**



EUGLOH campus cards state and connected services

→ Vision:

All university members should be able to use services of host university while on visit → easy and contactless



→ Interoperability



Status of four core members (IT wise - 2020)

Ludwig-Maximilians-Universität München

- Legic CTC Cards (Legic Advant + Prime)
- Payment (Studierendenwerk München)
- Cloud-Printing and Scanning (Secure-Printing and Payment)
- Library
- Ticket for Public Transport System

Université Paris-Saclay

- NXP Mifare DESfire Cards
- Payment (izly – les Crous)
- Library
- Physical Access Control

Lunds universitet

- NXP Mifare Classic Cards
- Physical Access Control (online and offline)
- Login at copiers (for copy/print/scan)
- Library
- Several other services, but not any payment services

Universidade do Porto

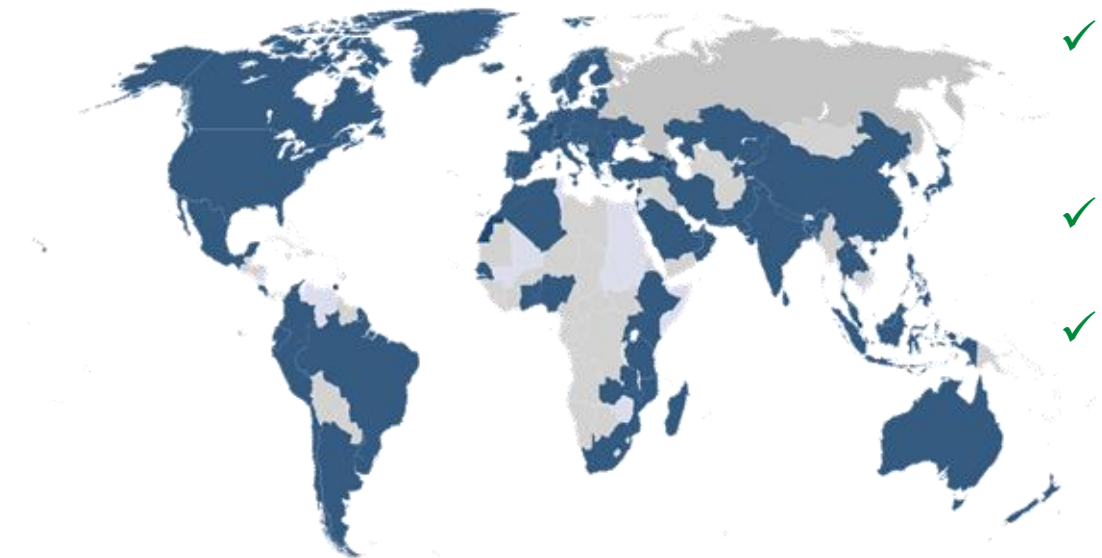
- NXP Mifare Classic Cards / Java Cards with Mifare Classic emulation
- Library
- Physical Access Control
- Canteen & cafeterias
- Printing Service
- Attendance

All contactless, but
Not compatible technologies

Egal ob an der Heimathochschule, der Partnerhochschule in Europa oder weltweit: Du kommst an, nimmst Smartphone oder Laptop heraus – und bist mit eduroam verbunden.



- ✓ Der Login der Heimathochschule funktioniert global – eine föderierte Kennung, keine lokalen Konten
- ✓ Du bist Mitglied der weltweiten Hochschulgemeinde, also hast du Zugang zu eduroam
- ✓ Zugang zum Service, im Moment der Ankunft
- ✓ Kein Antrag, keine lokale WLAN-Kennung, es funktioniert einfach



eduroam weltweit – über 100 Länder

**✓ eduroam ist die Messlatte für jeden neuen Service:
ganz simpel, funktioniert einfach – für jeden Nutzer.**

Welches Problem lösen wir?

Ein Smart / Smarter Campus soll **Services bereitstellen**

*“A **service** is a means of delivering **value to customers** by facilitating **outcomes** that **customers want to achieve** without the ownership of specific **costs** and **risks**.”*

ITIL Practitioner Guidance

- Meist fokussieren wir das Angebot, nicht den Service
- Wir haben die Ausweise smarter gemacht — aber die Services besser?

Mobile Identity → Digitale Identität EAM-Scope → Business Motivation & Capabilities

Kerngeschäft einer Hochschule:

- Lehre und Studium
- Forschung
- Transfer

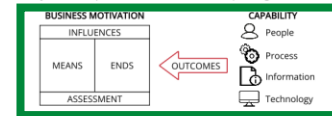
Die Services eines Smart Campus sind unterstützende Capabilities

- ✓ Zutritt zu Räumen / Arealen
- ✓ Essensausgabe in Mensen und Cafeterien
- ✓ Zugang zu Bibliotheksressourcen
- ✓ Kopieren & Drucken
- ✓ Anwesenheitserfassung
- ✓ Mobilität



DESCRIPTION
The Higher Education Business Capability Model describes a standard set of Business Architecture elements relevant to Higher Education. It can be used as a reference for Business Stakeholders, Enterprise Architects, and Technology Strategists to engage in discussion regarding business effectiveness, needs, and challenges. Standing alongside the accompanying Business Model Canvas, the Business Capability Model elaborates the core value chains for higher education and their underlying business capabilities.

UNDERSTANDING BUSINESS CAPABILITIES
A Business Capability is a particular logical combination of People, Process, Information, and Technology necessary to deliver a discrete required outcome to achieve a specific business objective. The business capabilities support the realisation of an institution's strategies. This model supports the development of strategies by viewing an institution as a collection of business capabilities that can be adjusted in response to the demands of the operating environment.



USAGE
The Business Capability Model serves as an anchor for assessing perspectives such as strategic importance, maturity, business operational pain points, capital investment, and organisational structure. It presents a view of the organisation with traceability from business objectives through to the information, technology, and other resources required to support them.

MAJOR CONCEPTS
Typically an **ORGANISATIONAL STRUCTURE** would be included to provide context for the scope of the model.

VALUE CHAINS capture how the institution generates value through Learning & Teaching and Research.

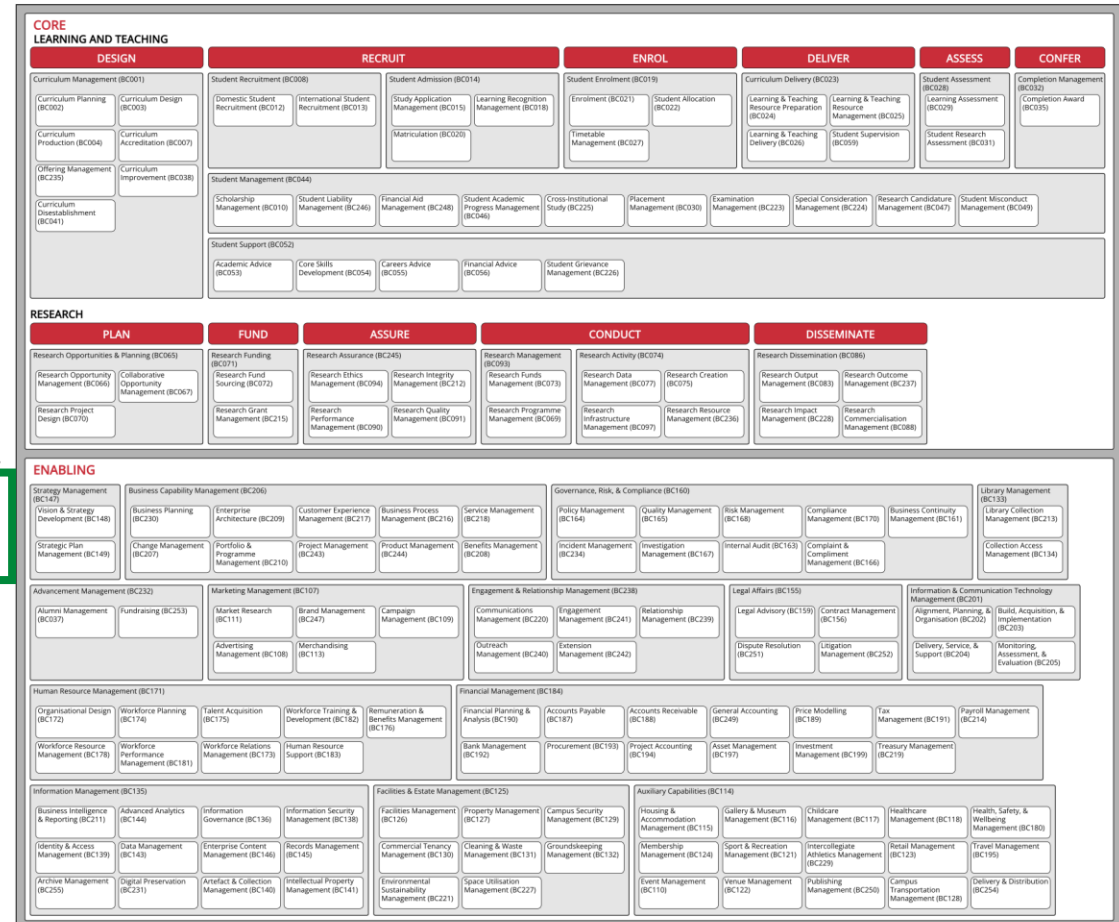
CORE business capabilities directly support the Value Chains are organised under the relevant Value Chain Segment.

ENABLING business capabilities support the core capabilities across the value chains and keep the institution running.

FURTHER INFORMATION
Definitions of each model element are provided in the accompanying Business Reference Model Catalogue, and supporting commentary is provided in the accompanying Business Reference Model Explainer.



HIGHER EDUCATION BUSINESS REFERENCE MODEL



Version 3.2.0, © 2025 CAUDIT; The HERM, the Higher Education Reference Models, is a collaborative community effort curated by the CAUDIT Enterprise Architecture group in active partnership with EUNIS, UCISA, and EDUCAUSE peer groups. The HERM is offered under the Creative Commons 4.0 CC BY-NC-SA license: you are free to use and adapt it, provided you do not use it for commercial gain. We encourage and require that any extensions or adaptations be shared back to benefit the global community. CAUDIT acknowledges the generous contributions of FromHereOn Pty Ltd. Please visit <https://caudit.edu.au/> for more information, and email herm-feedback@googlegroups.com with any feedback, suggestions, questions, and share-alike submissions.

Mobile Identity → Ausweise (digital & physisch) Campuskarten = Zugang zu Services → Smart Campus

Identifikation

- **Identifikation**
- **Statusnachweis**
- **Berechtigungsnachweis**
- Single Sign-on / 2FA / FIDO2
- Anwesenheitskontrollen
 - Check-in bei Prüfungen
 - Anwesenheit in Lehrveranstaltungen
 - Zeiterfassung
- Elektronische Signatur (rechtsverbindlicher Dokumente)

Elektronisches

- Bezahlen / Cashless Campus
- Mensen & Cafeterien
- Automaten
- Drucken / Scannen (Secure- & Follow-me-Printing)
- Ticketing (Veranstaltungen und Konferenzen)

Physische Zutrittskontrolle

- Areale (Campus, Parkplatz)
- Gebäude
- Räume
 - Seminarräume
 - Labore
 - Computerräume
 - Lernräume
 - Büros
 - Wohnanlagen (z. B. Wohnheime)

Bibliotheksservices

- Zugang / Ausleihe
 - Physische Medien (Bücher, Audio- und Videomedien)
 - E-Medien (E-Books, Audio- und Videomedien)
- Lernräume

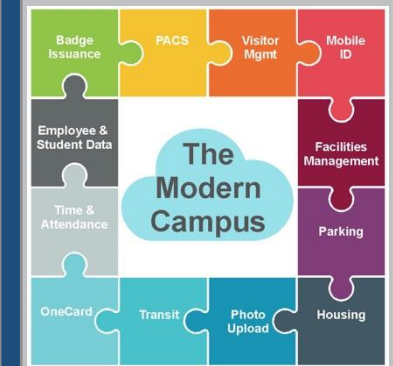
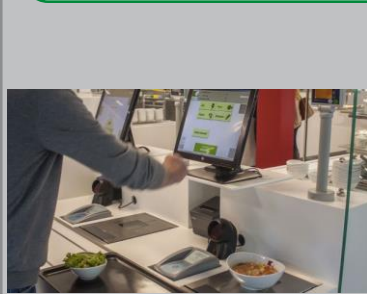
Mobilität

- Campus-Services (Uni-Shuttle)
- ÖPNV-Tickets & -Rabatte

Rabatte und Aktionen

- **Rabatte** auf Kulturangebote
 - Museen
 - Theater
 - Kinos
- Geschäfte
- Restaurants

On- & Off-Campus → **Vor-Ort-Nutzung / Proximity-Use-Cases**
+ Online-Services



Schlüssel zu allen Services → Identifikation / Authentifizierung

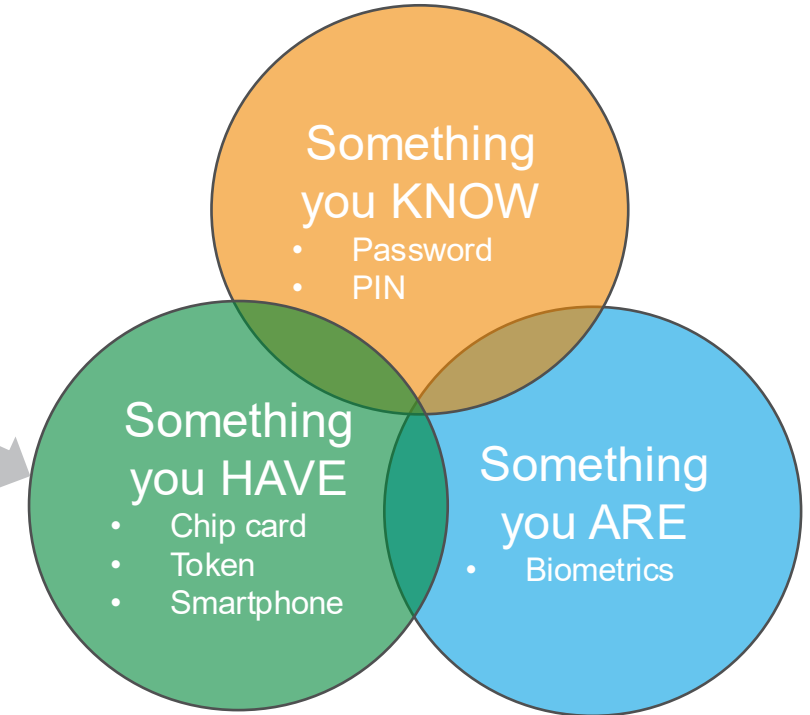
Zugang zu Services

→ Triple-A-System

- (Identifikation)
- **Authentifizierung**
- **Autorisierung**
- **Accounting**
- **Zugang zu Vor-Ort-Services** bedeutet:
Berechtigungen und Identität nachweisen ← IAM
- „*something you know*“ als Authentifizierungsmethode für den Vor-Ort-Zugang ist wenig **effizient**,
beste Kombination: „***something we have***“ + „***something we are***“
→ **Medium**: Smartphone-**Wallet-Passes** + Authentifizierung per Biometrie



Authentication Factors



Zugang zu den Services der Gasthochschule **bei Mobilität** – ab der ersten Minute
Campus Cards & eduTAP bedeuten **Servicezugang** vor Ort (auf und außerhalb des Campus)

- Für Mitglieder der eigenen Hochschule
- Für **Incoming-Mitglieder** anderer Hochschulen / Partner ← Mobilität (kurz- und langfristig)



Erasmus+

Für the Person **User Experience** ist entscheidend – so einfach wie möglich

Benchmarks:



WLAN-Zugang



Login zu Online-Services



Authentifizierung an physischen
(Vor-Ort-)Services

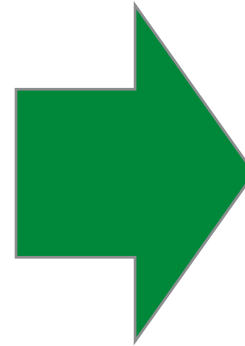
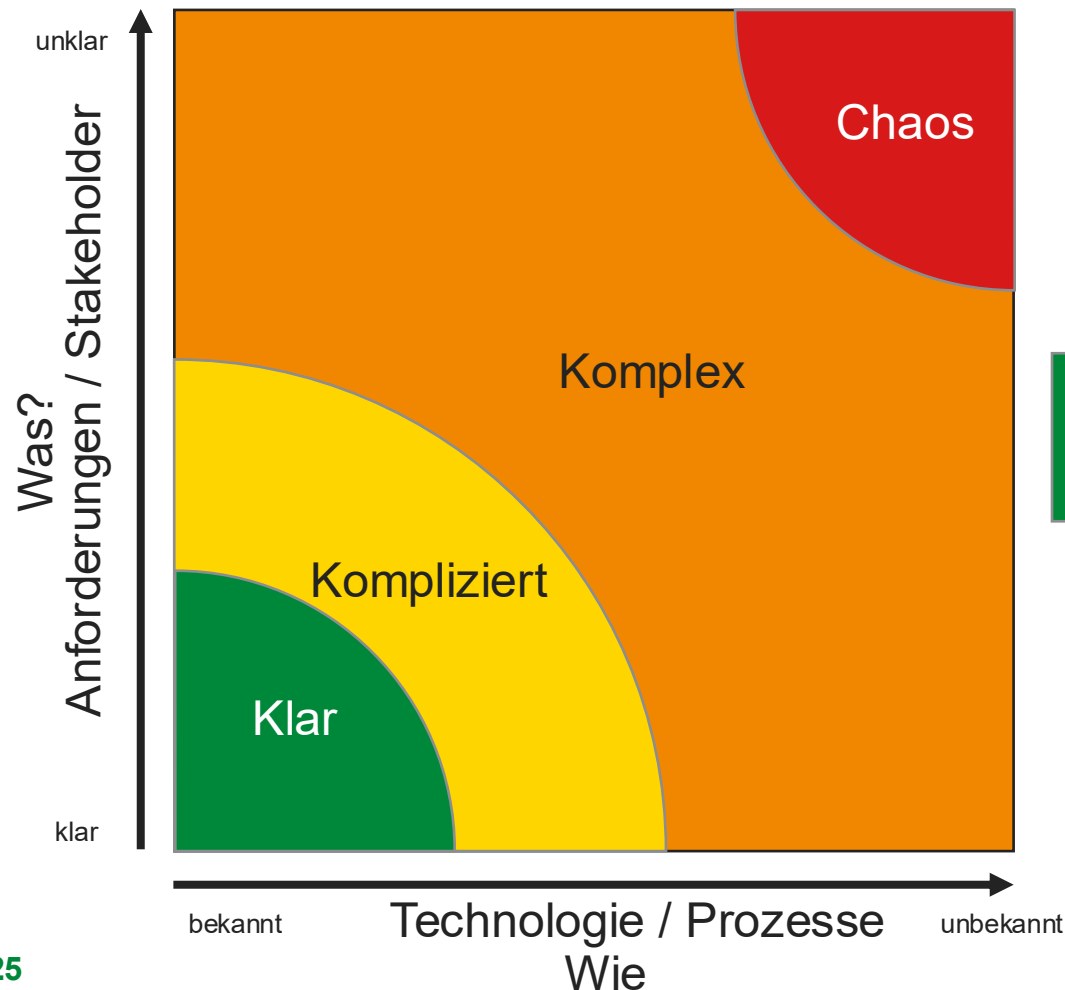
→ Servicezugang vor Ort sollte so **einfach** sein wie WLAN mit *eduroam*

- ✓ **Interoperabilität passiert auf der Leserseite** kontaktlose Kommunikationsprotokolle sind besser als visuelle Codes
- ✓ Fast alle Leser am Markt können **mehr als einen Standard lesen** (ggf. ist ein Firmware-Upgrade nötig)
- ✓ QR-Codes gelten **nicht als sicheres** Identifikationsmerkmal (besonders mit einer URL als Inhalt)

→ Am Ende zählt die **User Experience**



→ Komplexität managen – Stacey-Matrix & Cynefin-Framework



KISS als Leitlinie: Keep it Simple, Stupid

Digitalisierung 1.0

- Digitization – digitale Versionen analoger Dokumente erzeugen

→ Digitization vs. Digitalization (maschinenlesbarer Inhalt / Payload)

Digitalisierung 2.0

- Digitalisierung mit internem Fokus
- Interne Verwaltungsprozesse optimieren – **organisationszentrierte Optimierung**
- Datenverarbeitung

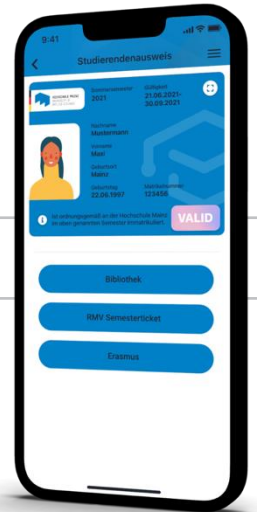
→ Digitale Transformation (ein harter Umbruch)

Digitalisierung 3.0

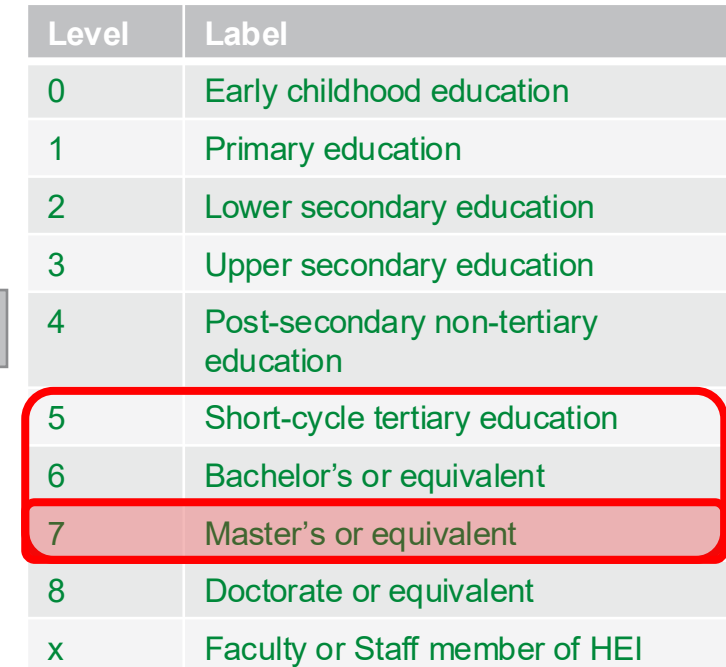
- Digitalisierung mit Fokus auf die Nutzer – **nutzerzentrierte Optimierung**
- Optimieren, wie Services gefunden und nahtlos genutzt werden
- Datenfluss

→ Serviceorientiert
→ **Digitale Identität**
→ Interoperabilität

→ **User Experience**



- ISCED:2011 Level



UNESCO ISCED:2011:
International Standard Classification of Education

eIDAS-Login für Credential-Antrag / Self-Service-Issuing
 → Zentral für **IDENTIFIKATION & AUTHENTIFIZIERUNG**
 → Qualität der Identitätsdaten
 → Art der Authentifizierung & Konsequenzen für das Identifikationsmedium

eduPersonAssurance:

<https://refeds.org/assurance>
<https://refeds.org/assurance/ATP/ePA-1m>
<https://refeds.org/assurance/ID/eppn-unique-no-reassign>
<https://refeds.org/assurance/IAP/low>
<https://refeds.org/assurance/IAP/medium>
<https://refeds.org/assurance/profile/cappuccino>
<https://refeds.org/assurance/ID/unique>

→

<https://refeds.org/assurance/IAP/high>

kein
Vertrauen

normal

Authentifizierung:
 • Nutzernamen/E-Mail Smart ID + Passwort

Identitätsprüfung:
 → selbst behauptet
 → verifizierte E-Mail-Adresse

substanziell
/ mittel

Authentifizierung:
 • zertifikatsbasiert
 • FIDO2

Identitätsprüfung:
 → amtlich bestätigt
 → manuelle Prüfung amtlicher Foto-ID

hoch

Authentifizierung

-  **eID.AS** konform
 → eID der EU-Bürger ausweise
 → von der Hochschule für internationale Studierende

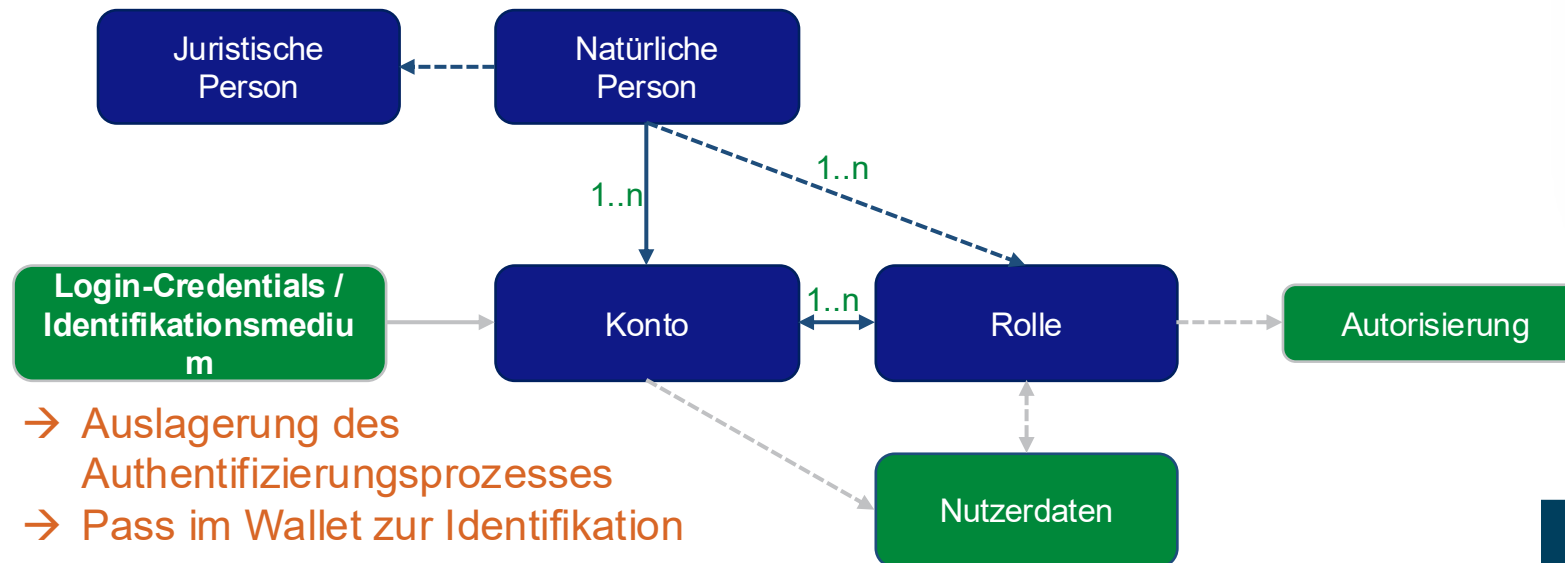
Identitätsprüfung:

- amtlich bestätigt
 → Ausweisdokument automatisiert geprüft: echt, gehört zur Identität

Identity Linking → von eduGAIN zu eduTAP

Nutzung der dezentralen / föderierten Authentifizierungs- und Autorisierungs-Infrastruktur

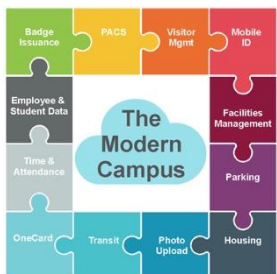
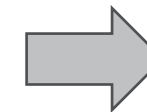
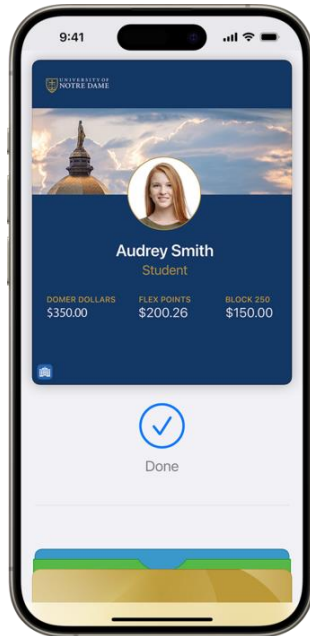
- Online – weniger einzelne Login-Credentials → höhere Assurance Level
- Brücke von der **Online-Identität** zu **Mobile Credentials** für verlässlichen, vertrauenswürdigen **Vor-Ort-Servicezugang** → serviceorientiert + interoperabilitätsorientiert
- Fokus auf den Datenfluss
- Das Medium **Wallet Pass** als Verlängerung einer **Digitalen Identität**



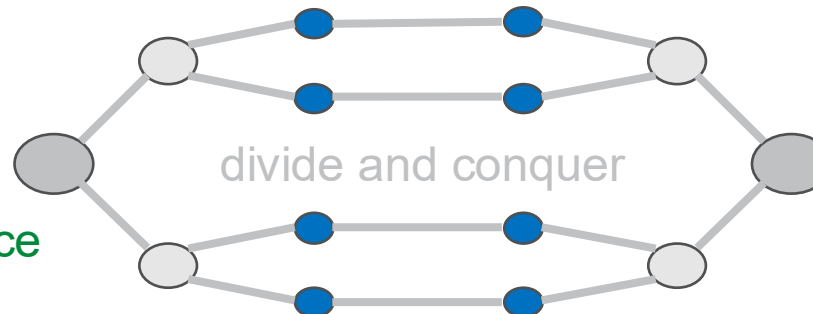
Co-financed by the Connecting Europe Facility of the European Union

This project has been co-funded by the European Commission. The content of the service reflects the views only of the authors and the European Commission cannot be held responsible for any use which may be made of the information contained therein.

Mobile Identität → Digitale Identität → Übergang der Ausweise (digital und physisch)



- Mehrere Credentials
- Micro Credentials
- Ein Credential pro Service



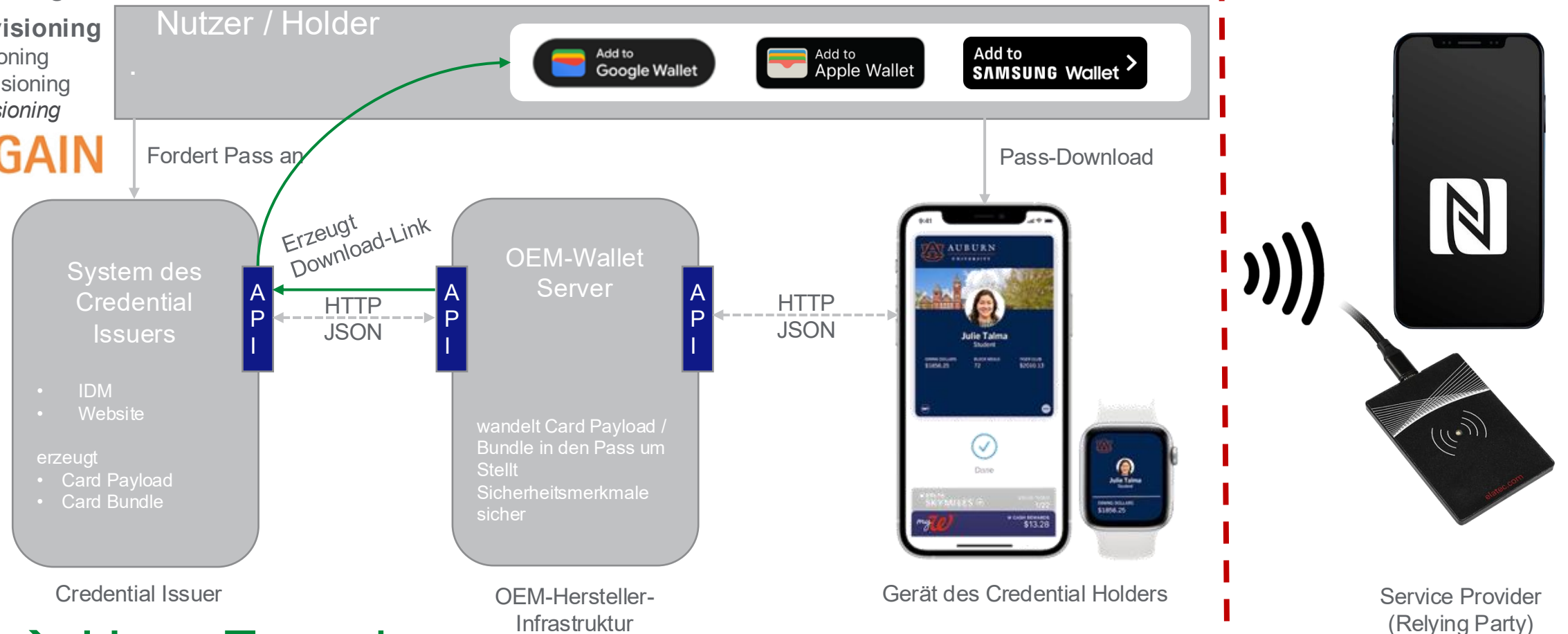
Mobile Identity – Digitale Identität

Ausstellungs-Prozess von Wallet-Pässen

Ausstellungs-Prozess von Wallet-Passes

→ Wichtig für die Nutzer – immer derselbe, konsistente Prozess

- Web-Provisioning
- App-Provisioning
- Wallet-Provisioning
- Push-Provisioning



→ User Experience

Mobile Identity → Digitale Identität Der Mobility-Use-Case

- ✓ Ausweise online ausstellen
- ✓ Niemand muss mehr im Kartenbüro erscheinen
oder auf den Postversand warten
→ der Ausweis ist in Sekunden verfügbar
- ✓ Karte beantragen = Pass erhalten
→ Login per eduGAIN und Pass herunterladen
- ✓ Entlastetes Personal vor Ort kann sich anderen
Services widmen, die Studierenden echten
Mehrwert bieten



Mobile Identity → Ausweise (digital & physisch) Campuskarten = Zugang zu Services → Zutritts- & Identitäts-Credentials

Identifikation

- **Identifikation**
- **Statusnachweis**
- **Berechtigungsnachweis**
- Single Sign On / 2FA / FIDO2
- Anwesenheitskontrollen
 - Check-in bei Prüfungen
 - Anwesenheit in Lehrveranstaltungen
 - Zeiterfassung
- Elektronische Signatur (rechtsverbindliche Dokumente)

Electronic Payment / Cashless Campus

- Mensa & Cafeterien
- Automaten
- Drucken (Secure- & Printing)
- Ticketing (Veranstaltungen, Konferenzen)

Physische Zutrittskontrolle

- Zutrittskontrolle
- Areale (Campus, Gebäude)

Bibliotheksservices

- Zugang / Ausleihe
- Physische Medien (Bücher, Audio, Video)
- Videomedien

Mobilität / Transport

- Campus-Services (Uni-Shuttle)
- Rabatte

Rabatte und Aktionen

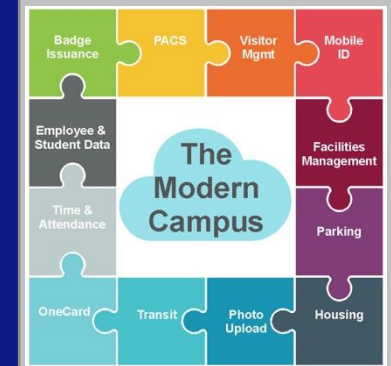
- **Rabatte** auf Kulturangebote
 - Museen
 - Theater
 - Kinos
- Geschäfte
- Restaurants

Separate Service-Pässe

- Lokale Services
- Jeder Service hat seinen eigenen Pass
- Anbieter wählen die passende Technologie je Pass

→ Funktionierende Lösungen der Anbieter

A gemeinsamer ID-Pass für alle Hochschulen (basierend auf ISO/IEC 18013-5)
→ **Identity Pass**



Der Weg der Ausweise ins Smartphone-Wallet Der LMU-Studierendenausweis (im Zeitverlauf)

LMU
Student ID
bis 2019



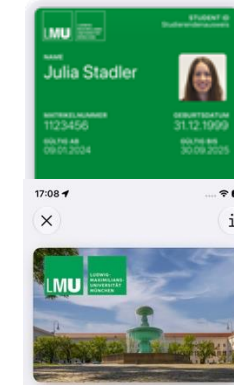
Dumb Campus
(konventionell,
analog, manuelle
Prozesse)

LMUcard
Student ID
2019-2025



Smart Campus
(vernetzt, IoT & Smartcards;
Datensilos, isolierte Systeme)

LMU
Student ID
2025/2026+



heute

Smarter Campus
(Interoperabilität, Personalisierung;
KI und Datenanalyse)

LMU
Student ID
2027+ ?



Hochschul-ID
(Studierende / Beschäftigte /
Affilierte)

- ✓ Verifiable Credentials
- ✓ Selective Disclosure
- ✓ Zero Knowledge Proofs
- ✓ Abbildung wichtiger Shibboleth-Attribute

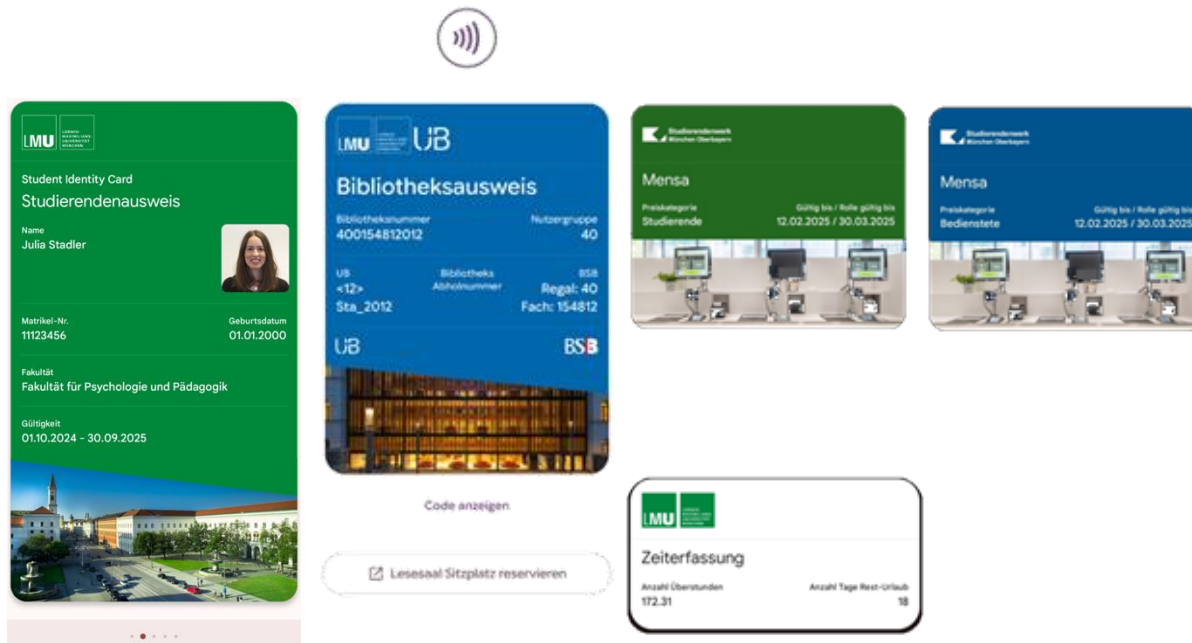
eduTAP & eduTAP@LMU

Mobile Identity → Digitale Identität

Der Weg der Ausweise ins Smartphone-Wallet

eduTAP-Beispiele @ LMU München

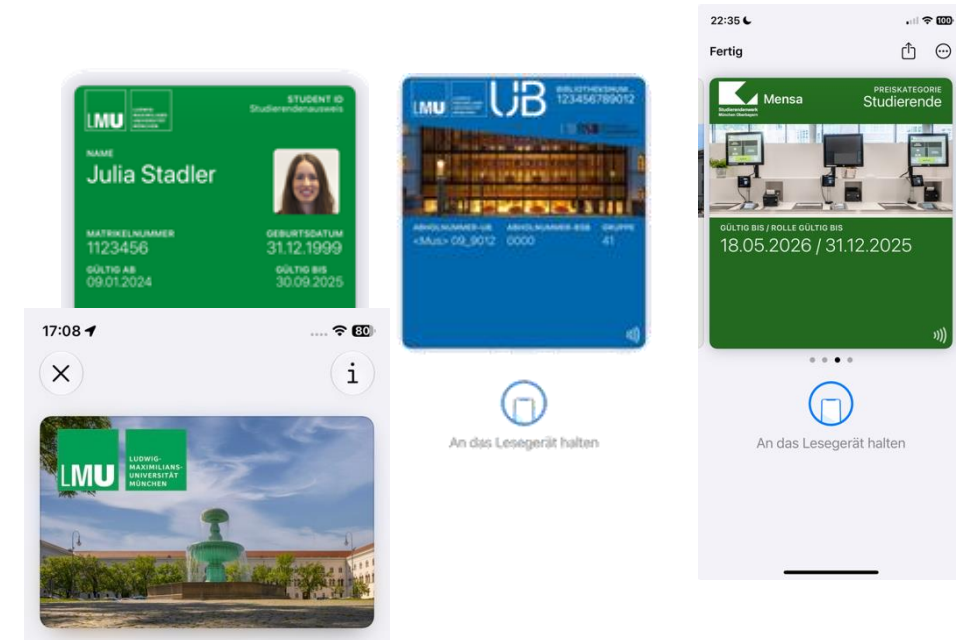
Google Wallet



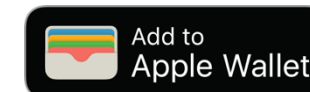
→ alle **NFC-fähig**



Apple Wallet



→ **NFC-fähig** wo erlaubt

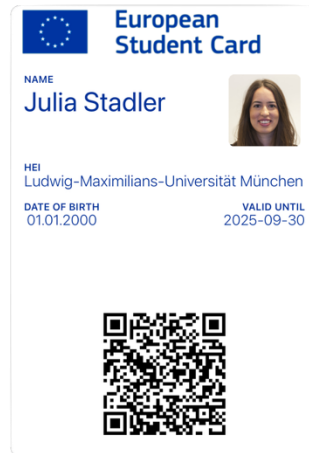


Mobile Identity → Digitale Identität Beispiel: Die European Student Card

Die European Student Card (v1.1, neues ESC-Design) (v1.5)

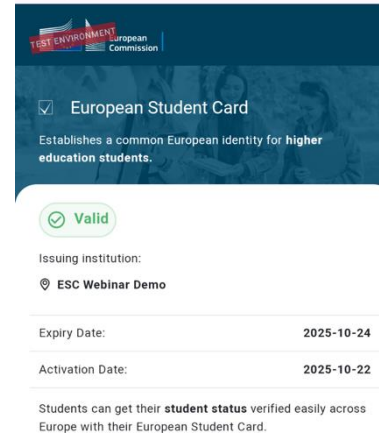


Google



Apple

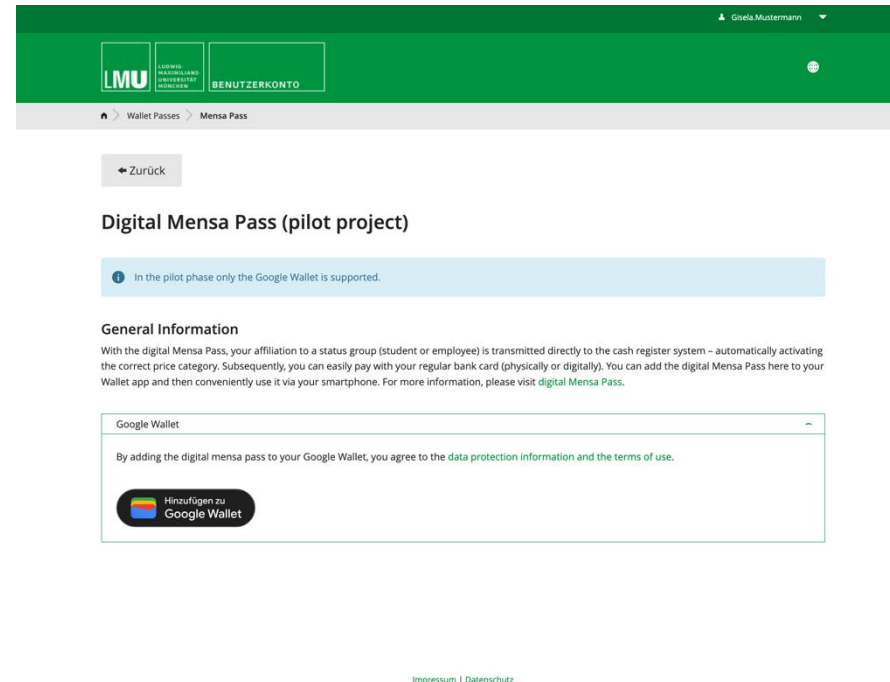
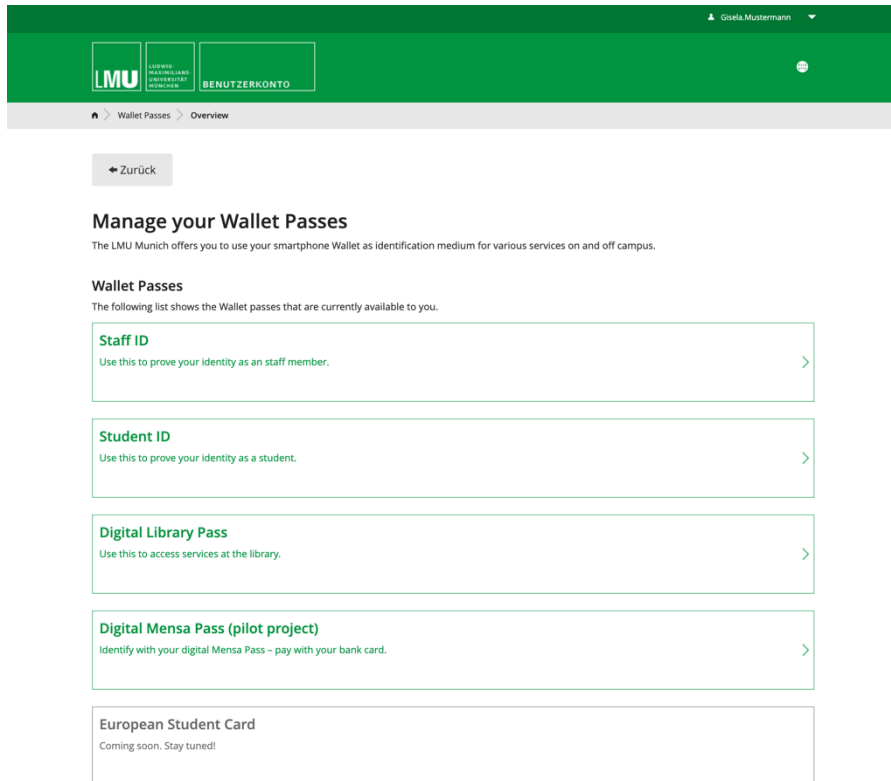
- ✓ Rabatte außerhalb des Campus
- ✓ Europäische Dimension → Erasmus+-Marketing
- ✓ Online-Statusprüfung



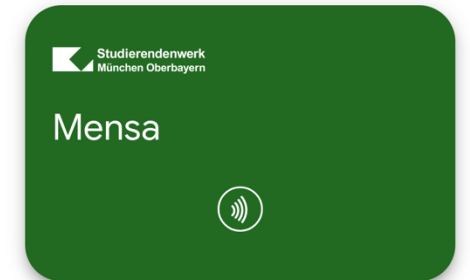
01-01-2000

Der Weg der Ausweise ins Smartphone-Wallet

Beispiele: LMU München Benutzerkonto – Pass Portal



Add loyalty
card



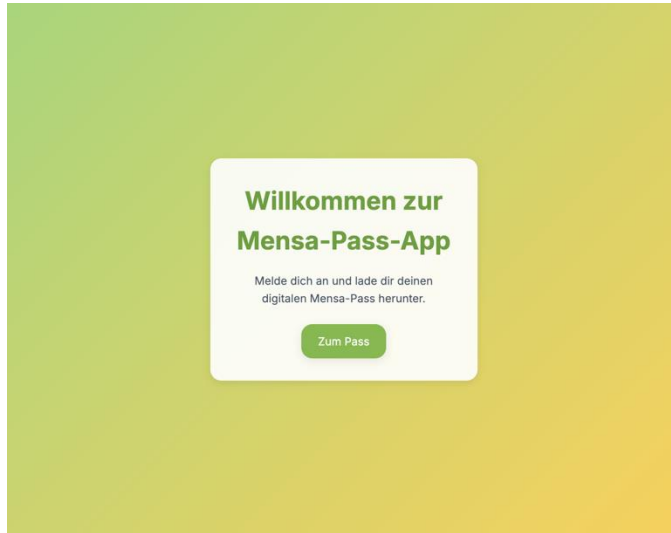
After adding your loyalty card to Wallet, you'll see your point balance and loyalty benefits in places like Maps, Shopping, and more. You can turn this off in [Google Wallet passes data](#) or on an individual pass in the Google Wallet app.

Pass providers can automatically add related passes, promotions, offers and more to your existing passes which can be controlled on your device in Wallet settings.

[Terms and Privacy Policy](#)

Add

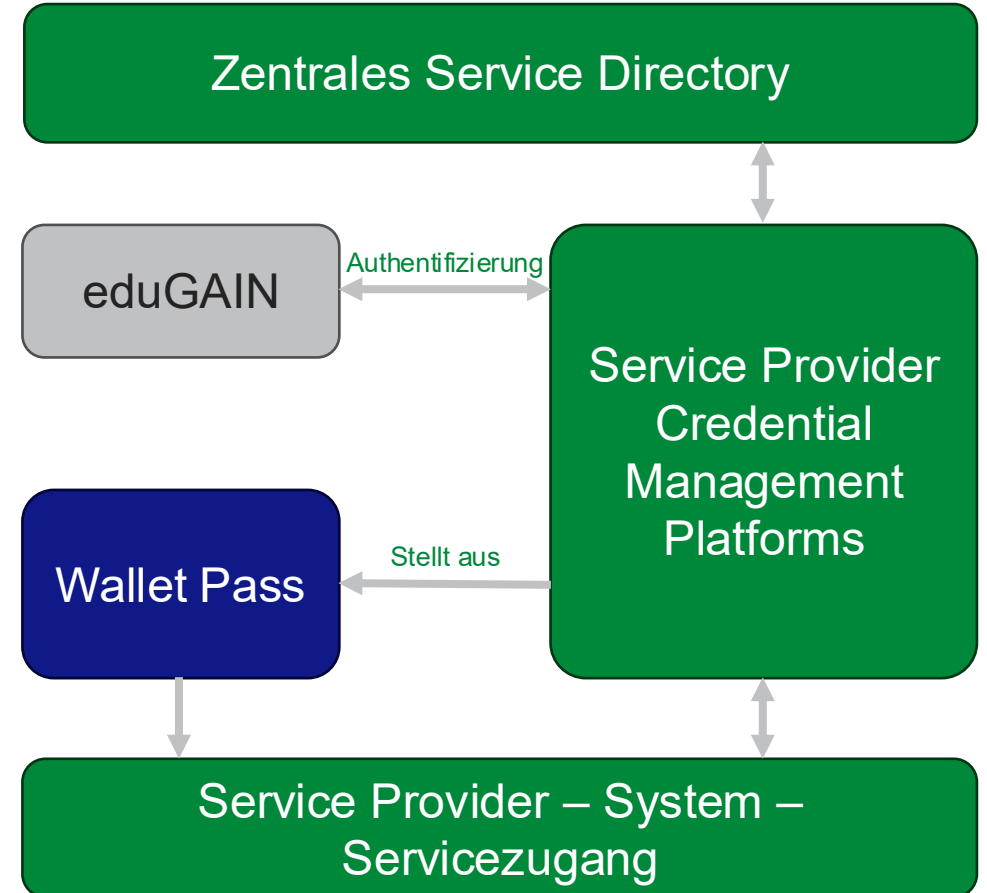
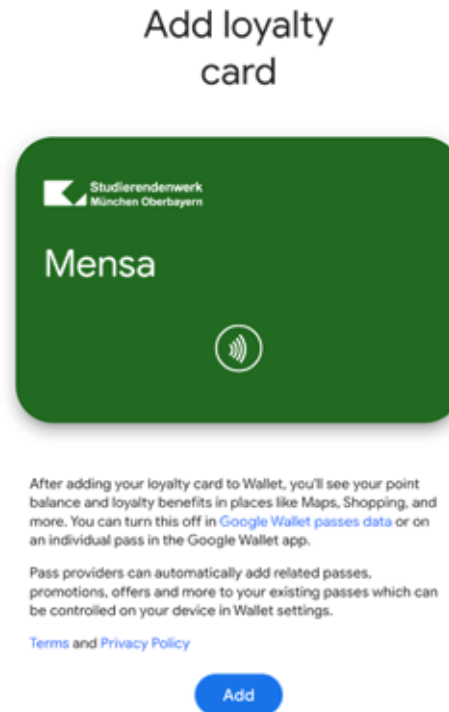
Der Weg der Ausweise ins Smartphone-Wallet Dedizierte Pass-Portale mit Login via eduGAIN



<https://mensapass.stwm.de/>

*Derzeit nur für Münchner
Hochschulen offen,
Gäste erhalten keine Rabatte,
können aber direkt zahlen via
Open-Loop-Payment*

*→ Rabatte für Allianz-Mitglieder
werden politisch diskutiert und sind in
Vorbereitung*



Mobile Identity → Digital Identity

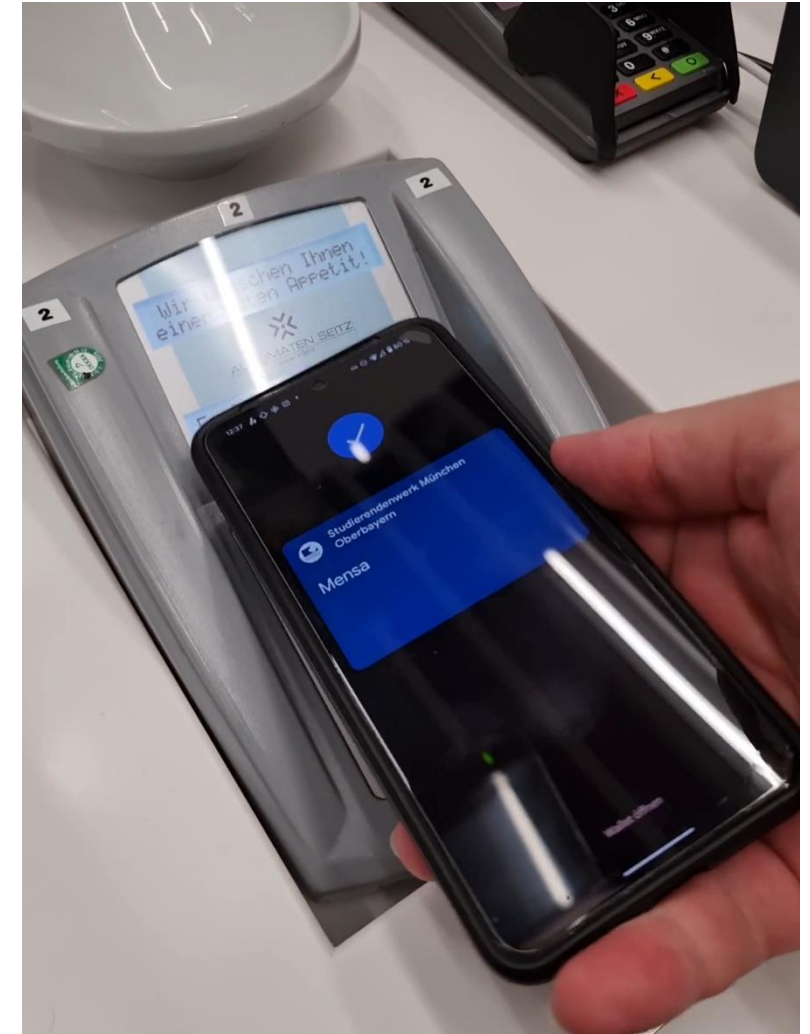
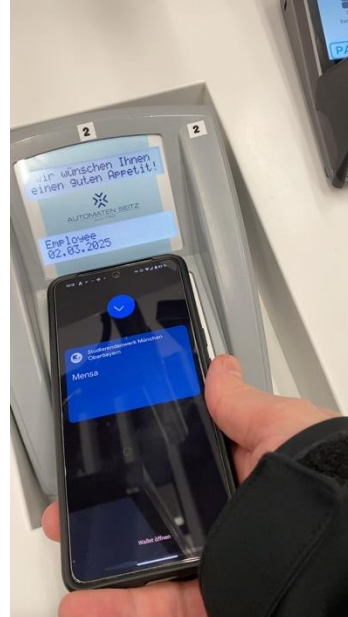
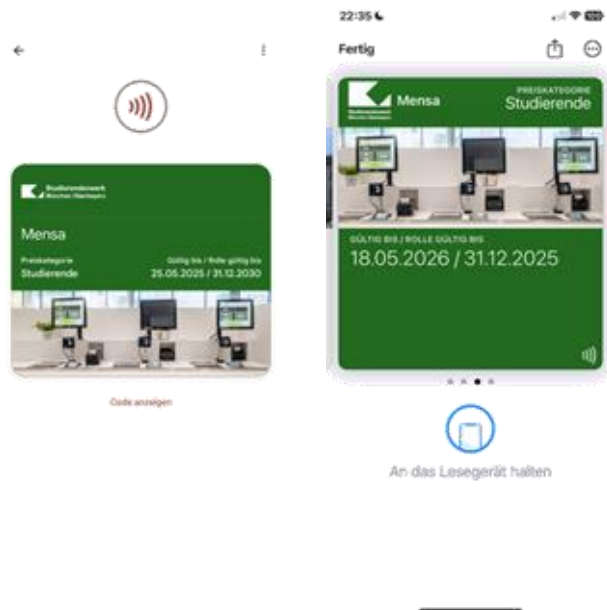
Beispiel: Tap to Pay - Rabatt-Pass für Mensen

Bezahlvorgang in der Mensa



Double Tap:

1. Berechtigungsprüfung der Statusgruppe (Studierende, Beschäftigte, Gäste)
→ Rabatt wird angewendet
2. Bezahlen mit Open-Loop-Bank-/Kreditkarte



Mobile Identity → Digital Identity

Beispiel: Tap to open a door

Physical Access Control – Zutrittskontrolle / Schließsysteme

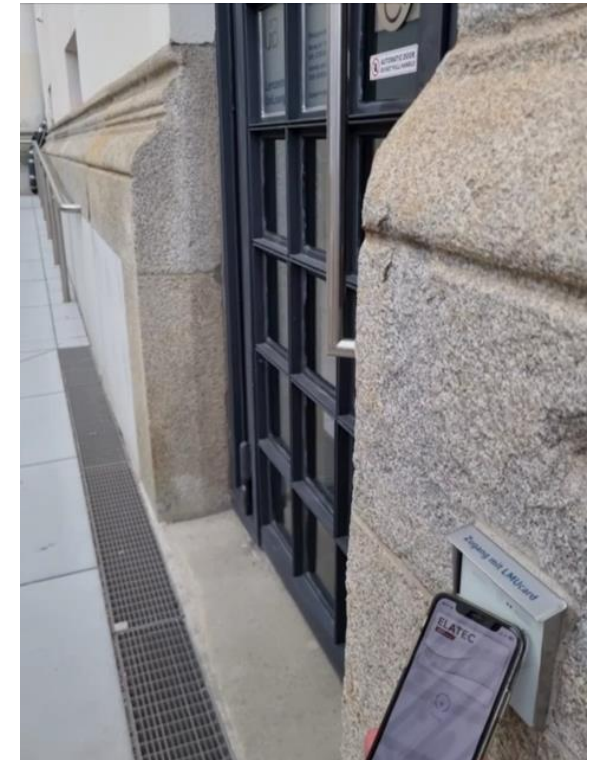
Physischer Zutritt zu den Lernräumen



LMUcard



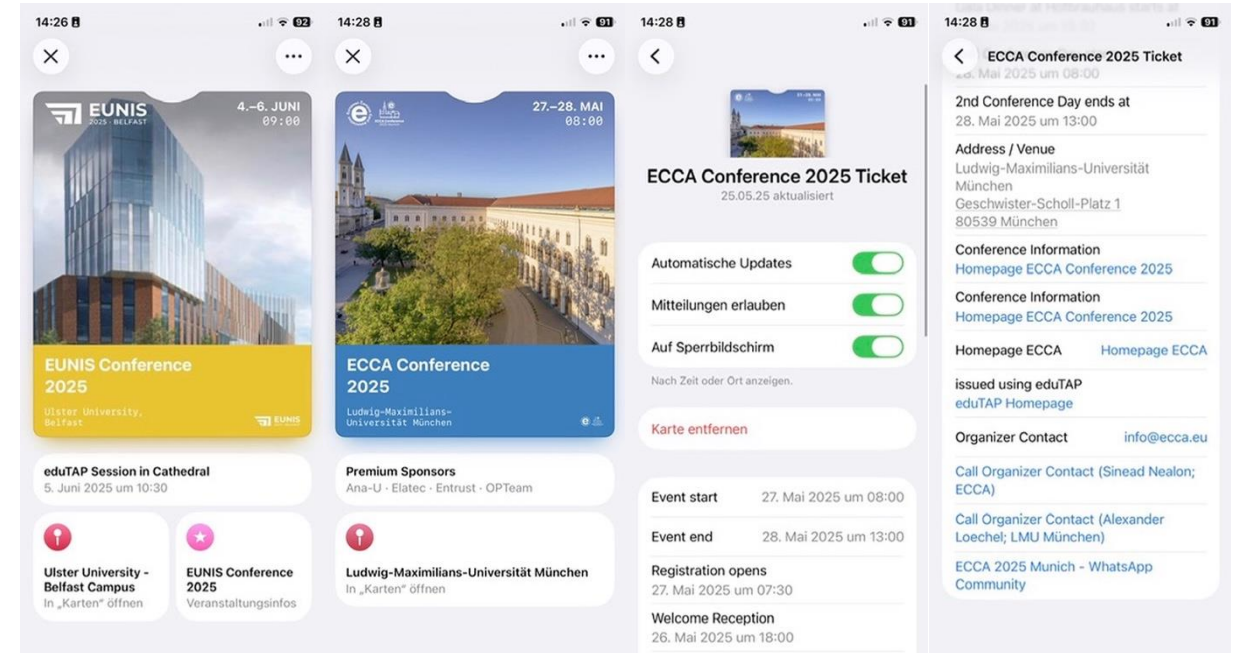
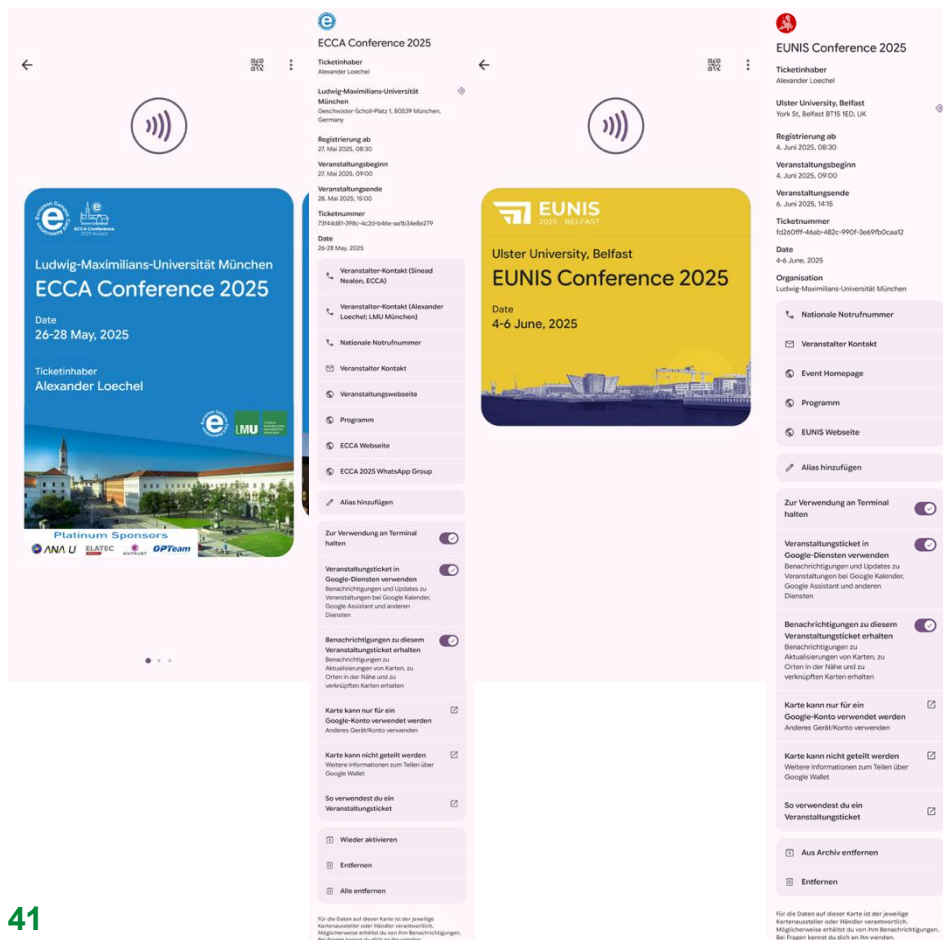
Google Smart Tap



Apple Access

Mobile Identity → Ausweise Mit den Inhabern kommunizieren

- Wallet-Passes sind aktualisierbar, widerrufbar und haben Kommunikationskanäle
- Sie haben zudem interaktive Elemente



- Nachrichten an einen Pass senden
- Pop-ups bei Zeit- oder Orts-Ereignissen
- Geofencing von Passes

tap to ...

- ✓ dich ausweisen,
- ✓ deinen Status nachweisen,
- ✓ deine Berechtigungen zeigen,
- ✓ Rabatte einlösen,

tap to ... einen Service direkt vor Ort nutzen:

- ✓ tap to pay – bezahlen
(Open- und Closed-Loop Payments),
- ✓ tap to open a door – Türen öffnen,
- ✓ tap to lend a book – Bücher ausleihen,
- ✓ tap to ride – Campus-Shuttle nutzen.

TAP TO PAY



no App, just tap!

<https://eduTAP.eu>

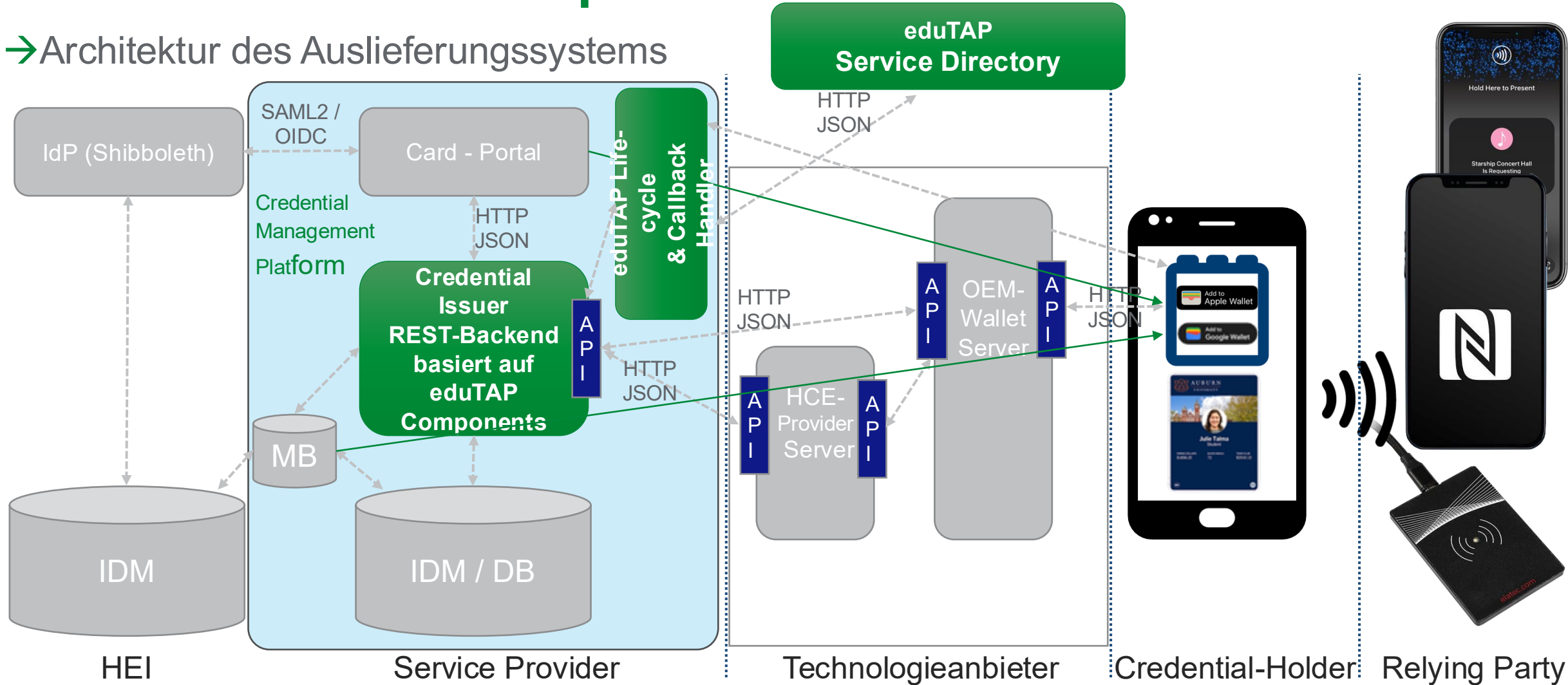
- **eduTAP** das Konzept
 - Integrierte Campuskarten aufteilen in **dedizierte Service-Pässe** und einen **harmonisierten Identity Pass**
 - Das volle Potenzial digitaler Wallets nutzen
 - **Bestehende**, sichere und bewährte kontaktlose **Standards nutzen**
→ keine neuen Standards erfinden

→ Fokus auf **User Experience** and **Interoperabilität**
- **eduTAP** die Software – damit Hochschulen und Service Provider:
 - Pässe im Smartphone-Wallet erstellen, ausstellen und verwalten
 - mit Wallet-Pässen Servicezugang gewähren, identifizieren und den Status von Studierenden und Beschäftigten prüfen können

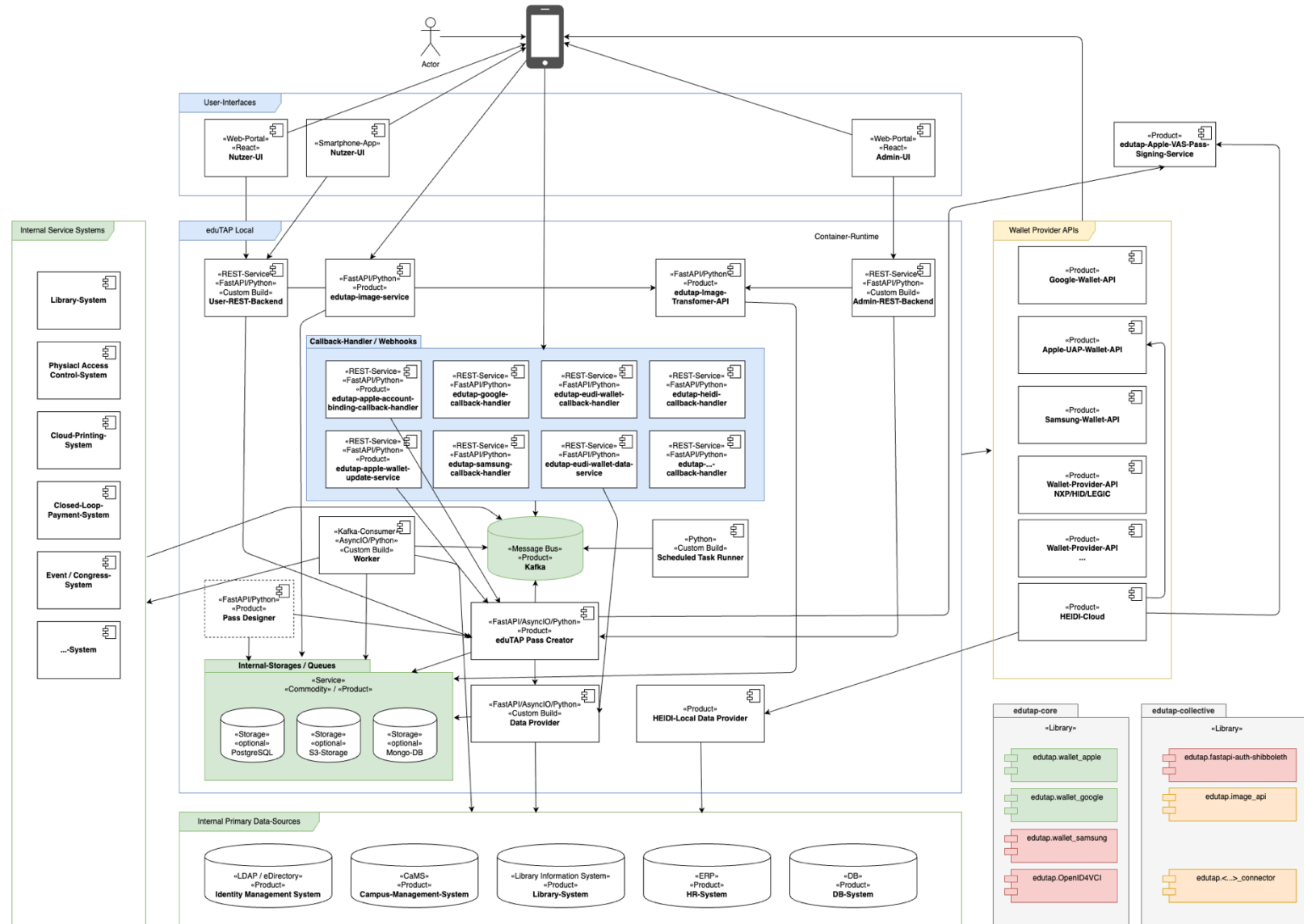
→ **eduTAP** hilft, die große Vision der European Student Card / des Mobility-Use-Case zu erfüllen and **ermöglicht Interoperabilität** und eine **bessere User Experience**

Die Credential Management Platform and eduTAP Components

→ Architektur des Auslieferungssystems



eduTAP@LMU Setup Architektur



eduTAP vs. Credential Management Platforms auf eduTAP-Basis

eduTAP → passt für große Hochschulen (Entwickler und Skills vorhanden)

- ✓ eduTAP ist Community Open Source
- ✓ eduTAP ist ein Satz von Bibliotheken und Beispiel-Implementierungen
- ✓ eduTAP liefert Vorlagen für Pass-Designs und die nötigen legal and technical documentation
- ✓ eduTAP liefert KEIN Frontend und keinen Pass-Designer

Commercial Credential Management Platforms (CMP) → Make or **buy**

e.g. [HEIDI \(Higher Education Institution Digital Identities\)](#) / [HELIX-PASS](#) Plattform ist eine kommerzielle Credential Management Plattform (CMP) auf Basis der eduTAP-Komponenten

- ✓ Liefert Adapter zu Fachanwendungen (z. B. Campus-Management-Systems, Library-Systems, ...)
- ✓ Liefert einen Pass-Designer
- ✓ Liefert eine Management-UI

Demo → Download eines eduTAP-Passes



<https://demo.edutap.eu/>

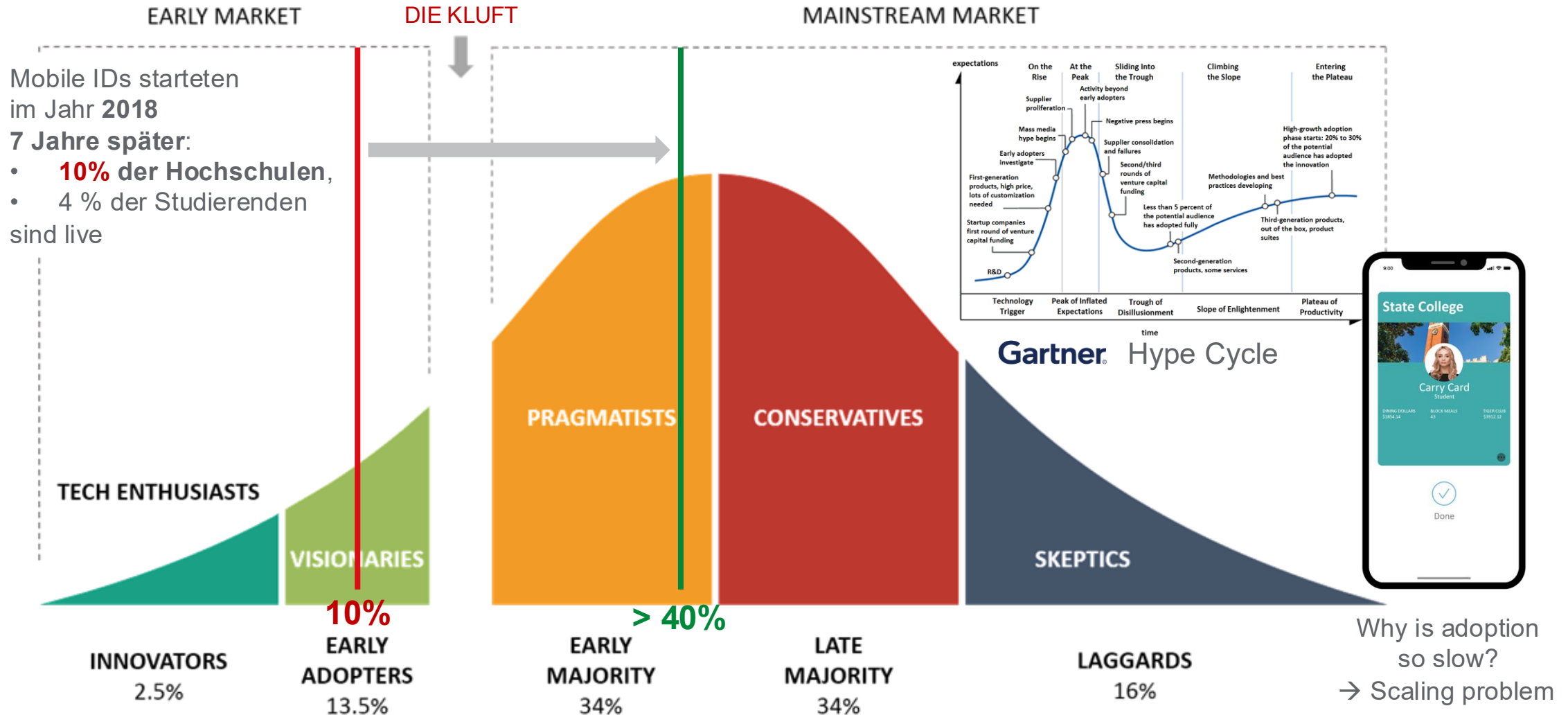


Add to Google Wallet



Add to Apple Wallet

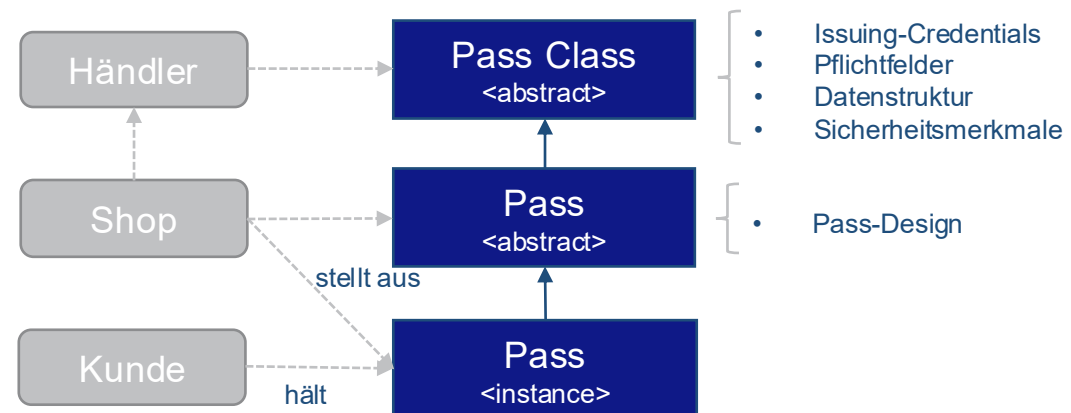
Mobile Identity in den USA Adoptionsraten nach 7 Jahren



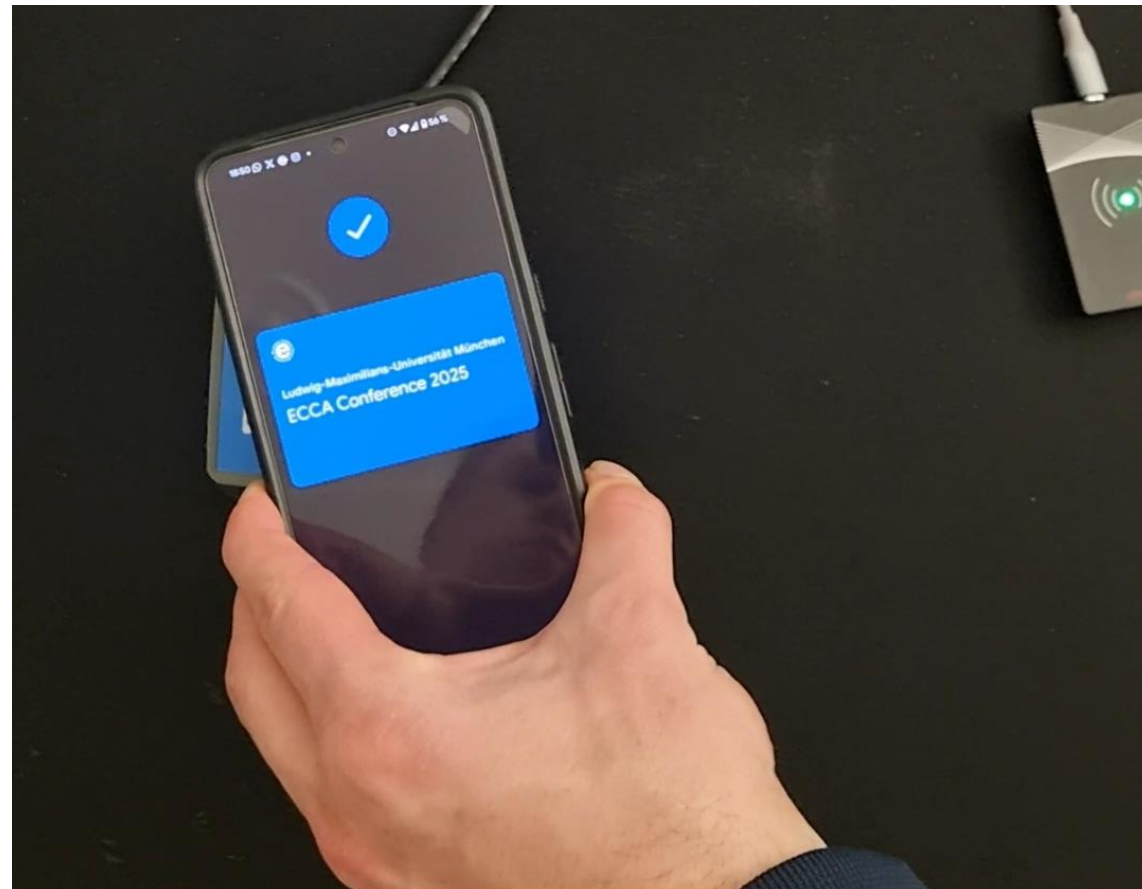
Das Wallet ist ein **Container für mehrere Pässe**

Technische Merkmale:

- **Auto-Presentment / Smart Select** ← Leser wählt den passenden Pass automatisch aus (falls vorhanden)
- Wählbare Authentifizierungs-Anforderungen ← **Sicherheitsmerkmale**
- Express-mode (Apple)
- **Batteriereserve** (Pass bleibt nutzbar, wenn das Handy ausgeht; wichtig für Schlüssel, Transit-Tickets, Payment)
- Gruppierbar
- Gültigkeitszeitraum
- Aus der Ferne aktualisier-/widerrufbar
- **Offline nutzbar** (→ nicht nachverfolgbar)



Auto-Presentment / Smart Select eines NFC-fähigen Passes im Wallet



Battery Reserve Mode – Wallet nutzen, selbst wenn das Gerät aus ist

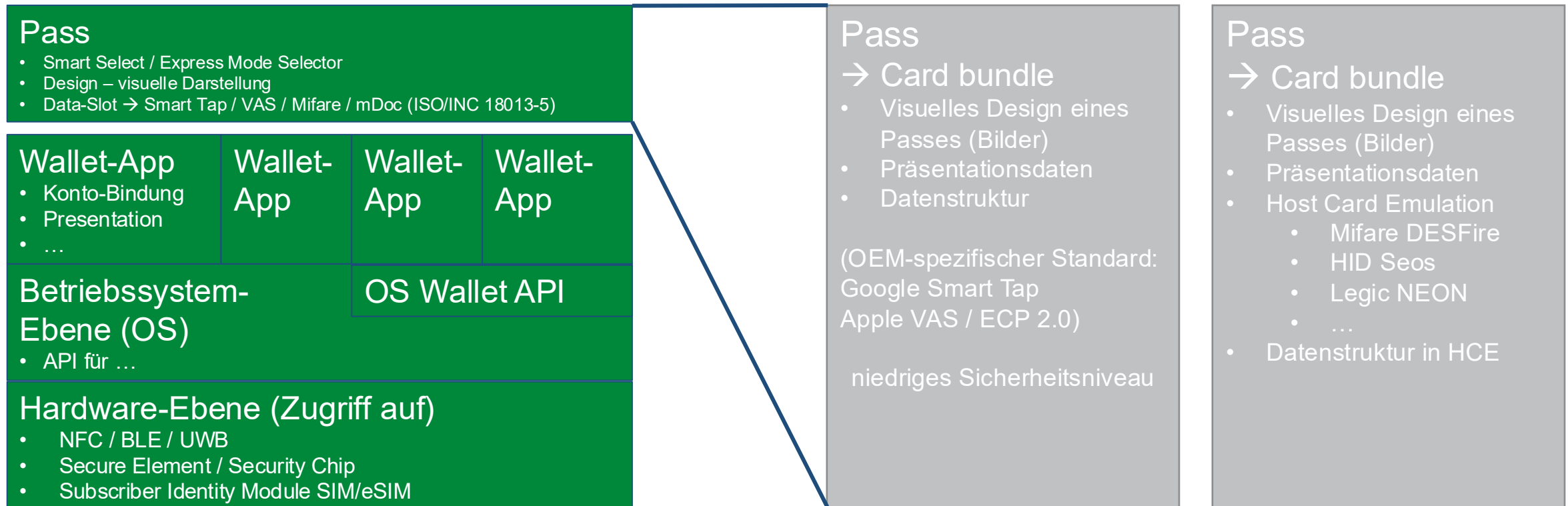
- für Schlüssel (Wohnheim, Seminarräume, Gebäudezutritt, Autos)
- fürs Bezahlen
- für ÖPNV-Tickets

Apple garantiert heute 5 Stunden, zuvor bis zu 7 Tage nach dem Ausschalten des Smartphones, wegen zu geringer Batterie



- ✓ Technische Details und Features von Wallets / Passes → Weg zur **interoperablen** Campuskarte
- ✓ Wenn jeder Pass (jede Technologie) einzeln ausgewählt und genutzt werden kann (und der Pass in der Wallet kann durch den Leser ausgewählt werden (**Smart Select / Auto-Presentment**))

→ Ein Pass pro Service



- Für kontaktlose Kommunikation ist NFC das Protokoll
- Kommunikation über ISO 14443
- Datenformate (Dateisystem-Zugriff)
 - Google Smart Tap
 - Apple VAS (Value Added Services)
 - NFC ECP 2.0 (Enhanced Contactless Polling)
 - Host Card Emulation (HCE: proprietäre Protokolle)
 - Mifare DESfire (via Mifare2GO / NXP secure element)
 - Legic NEON / Advant (via Legic Connect)
 - HID Seos
- Intern agiert das Secure Module als JCOP-Smartcard
- ISO 18013-5 Personal Identification
NFC-Handover zu BLE oder WiFi
Kernfunktionalität in der OS-API von Android und iOS



Sicherheitsniveau
Chip / Smartcard

Sicherheitsniveau
Smartphone

hoch

hoch

Legic NEON
Legic Advant
Mifare DESfire
HID Seos

ISO 18013-5

ECP 2.0

Smart Tap

VAS

niedrig

Mifare Classic /
Card UID

niedrig

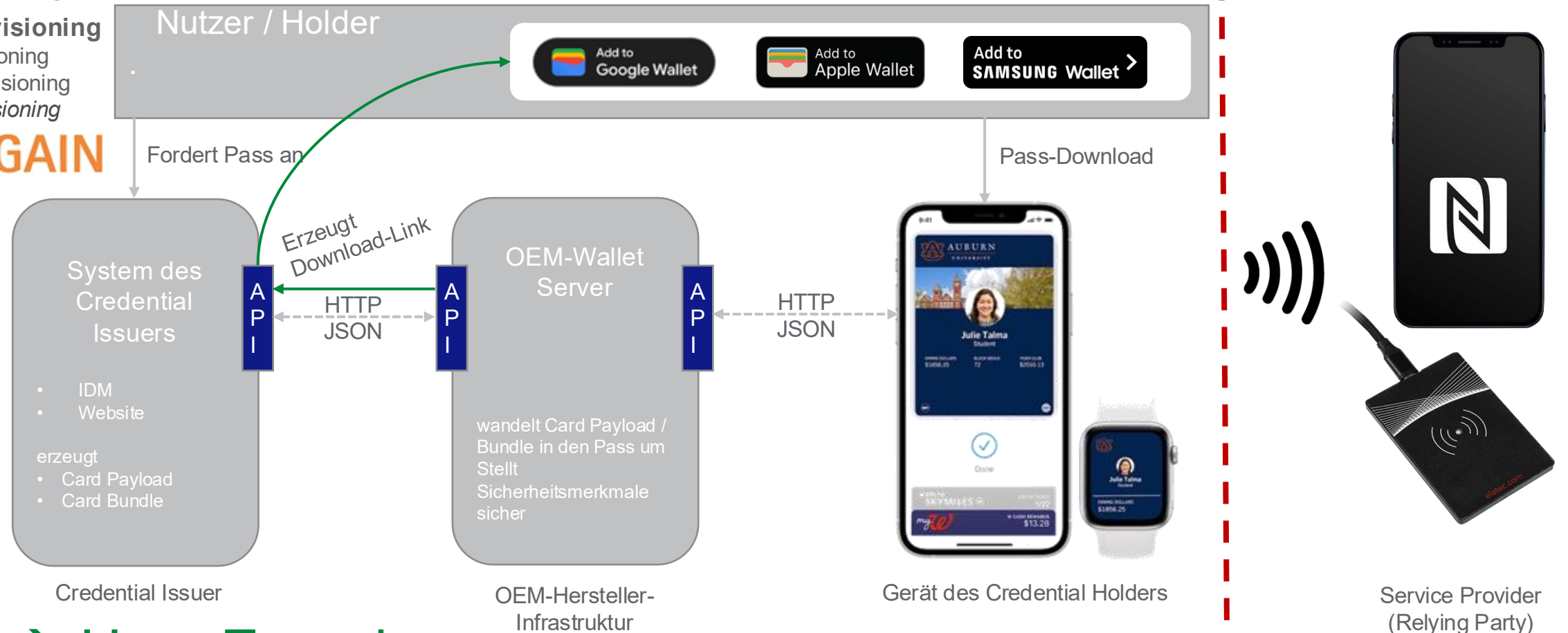
- Sicherheitsbetrachtung je nach **Use-Case**

Mobile Identity – Digitale Identität Ausstellungs-Prozess von Wallet-Pässen

Ausstellungs-Prozess von Wallet-Passes

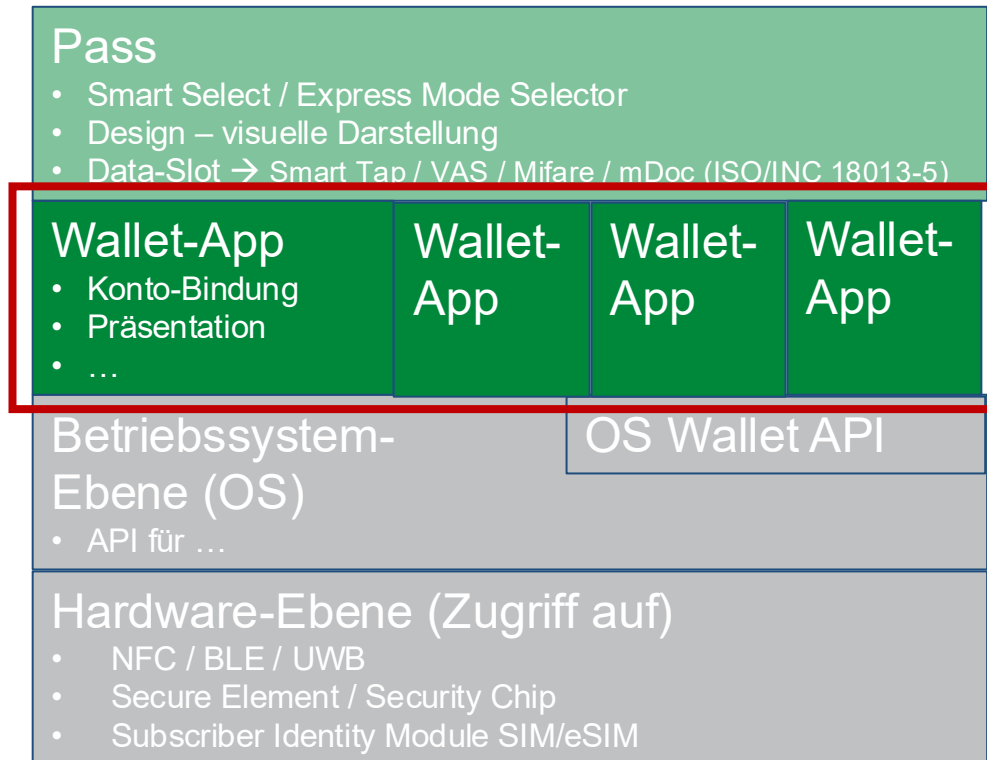
→ Wichtig für die Nutzer – immer derselbe, konsistente Prozess

- Web-Provisioning
- App-Provisioning
- Wallet-Provisioning
- Push-Provisioning



→ User Experience

Detailblick auf das Wallet



→ Die eduTAP-Lösung ist wallet-**agnostisch** – nicht an einen bestimmten Wallet-Anbieter gebunden

→ eduTAP befähigt Hochschulen und Service-Provider, Wallet-Passes einfach zu **erstellen** und **auszustellen**



European University Alliance for Global Health

eduTAP

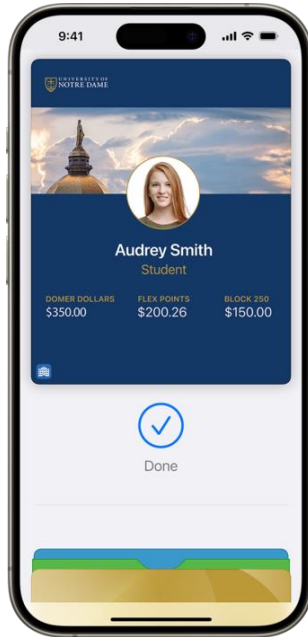
*A **sneak peek** into the future of Student IDs*

→ More interoperability and less passes by Verifiable Credentials

eduTAP Common ID



Was ist mit den nativen, heutigen **Student IDs** in Apple Wallet & Google Wallet (Mifare DESfire oder HID-basiert)?



- ✓ Großartige integrierte Karten (**eine Karte** für alle Services, perfekt für **Corporate**)
- ✓ *Sollen genutzt werden für alle Hochschul-Services* (Apples Intention)

- Universitäts-/organisationszentrierte Optimierung
- Erfüllt die Anforderung „nahtlose Mobilität“ nicht
- Shared Services: Was ist mit Nutzern, die keine eigenen Studierenden sind?
- **WENIGER sicher** (wenn man dem ESC-Data-Zone-Ansatz folgt)
- Nicht die geforderte User Experience, erfüllt rechtliche Anforderungen nicht.

Das ist eine **Sackgassen-Lösung** – sie hilft nicht und bringt keinen Nutzen, sie liefert sogar eine **SCHLECHTERE User Experience**

Sie unterstützt **KEIN Selective Disclosure and Zero Knowledge Proof**

Apple und Google wissen das und arbeiten daran!

Apple- und Google-Access-Plattformen sind gut für PAC- und Payment-Passes

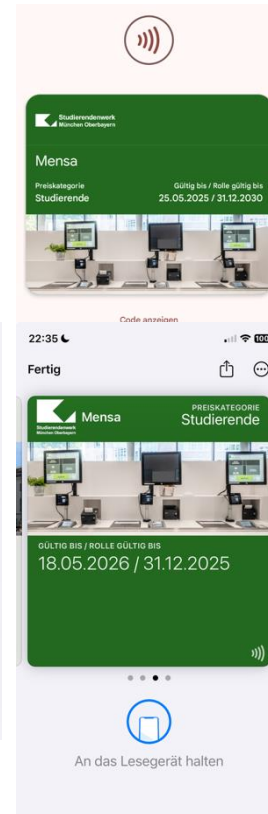
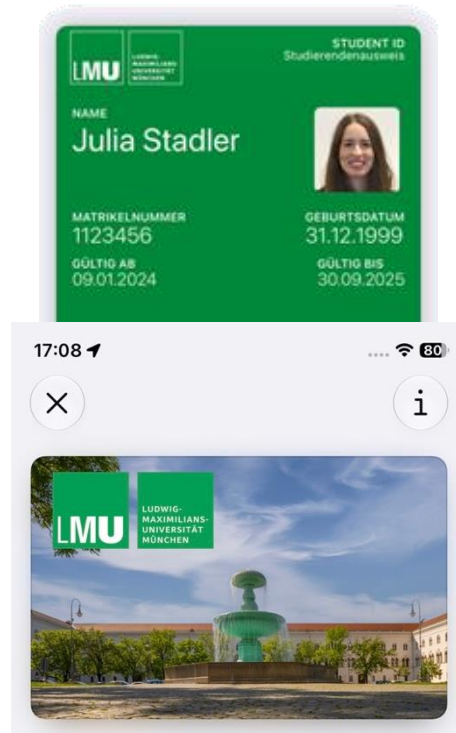
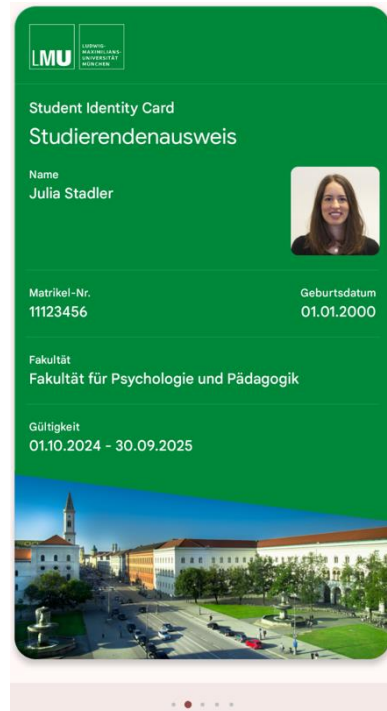
→ **NICHT** für Studierenden- oder Beschäftigten-IDs

→ **GUTE** dedizierte Service-Passes

Bei Wallet-Passes zählt die User Experience

Eine **großartige User Experience** ist der Schlüssel zu Akzeptanz und Nutzung

- ✓ Passes ohne NFC sind **KEINE gute** User Experience
- ✓ Unnötige Pässe vermeiden ← KEIN eigener Pass nur zur simple Berechtigungsprüfung (Status, Hochschulzugehörigkeit)



Übergang

Gibt es eine bessere Lösung?



- ✓ Verifiable Credential
- ✓ Selective Disclosure
- ✓ Zero Knowledge Proofs

Mobile Identity → Ausweise (digital & physisch) Campuskarten = Zugang zu Services → Zutritts- & Identitäts-Credentials

Identifikation

- **Identifikation**
- **Statusnachweis**
- **Berechtigungsnachweis**
- Single Sign On / 2FA / FIDO2
- Anwesenheitskontrollen
 - Check-in bei Prüfungen
 - Anwesenheit in Lehrveranstaltungen
 - Zeiterfassung
- Elektronische Signatur (rechtsverbindliche Dokumente)

Electronic Payment / Cashless Campus

- Mensa & Cafeterien
- Automaten
- Drucken (Secure- & Printing)
- Ticketing (Veranstaltungen, Konferenzen)

Physische Zutrittskontrolle

- Zutrittskontrolle
- Areale (Campus, Gebäude)
- Gebäude

Bibliotheksservices

- Zugang / Ausleihe
- Physische Medien (Bücher, Audio, Video)
- Videomedien

Mobilität / Transport

- Campus-Services (Uni-Shuttle)
- Rabatte

Rabatte und Aktionen

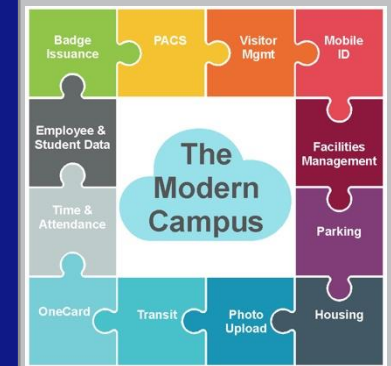
- **Rabatte** auf Kulturangebote
 - Museen
 - Theater
 - Kinos
- Geschäfte
- Restaurants

Separate Service-Pässe

- Lokale Services
- Jeder Service hat seinen eigenen Pass
- Anbieter wählen die passende Technologie je Pass

→ Funktionierende Lösungen der Anbieter

A gemeinsamer ID-Pass für alle Hochschulen (basierend auf ISO/IEC 18013-5)
→ **Identity Pass**



Aus rechtlicher Sicht sind Ausweisdokumente öffentlicher Hochschulen
amtliche Lichtbildausweise

- ✓ Rechtliche Anforderungen → **Internationale Standards** für HEI-Identitäten eduGAIN (inkl. eduPerson, SCHAC)
- ✓ Sicherheitsüberlegungen z. B. European Student Identifier routbar für Kurse an anderen Einrichtungen (bei Mobilitäten)
- ✓ Hohes Assurance Level

Ausweise (Studierende, Beschäftigte, Affiliates) werden genutzt

Vor Ort (Proximity Use-Cases)

Online

On-Campus

Off-Campus

- ✓ Anwesenheit in Lehrveranstaltungen
- ✓ Check-in bei Prüfungen
- ✓ Zeiterfassung
- ✓ Rabatte in Mensa & Cafeterien
- ✓ Identifikation gegenüber Hochschulstellen (Studierendenkanzlei und Prüfungsämter, Campus-Security)

- ✓ Identifikation gegenüber öffentlichen Behörden (z. B. Polizei)
- ✓ Identifikation gegenüber Dritten (z. B. Check-in im Hostel)
- ✓ Berechtigungsprüfung für Rabatte und Zutritt (z. B. rollenbasiert, altersbasiert, einrichtungsbezogen)

- ✓ Als Authentifizierungsfaktor

Mobile Identity Digitale Identität Verifiable Credentials für Hochschulen (Prototypen)

European Student Card als Verifiable Credential



DC4EU non-foundational

Table with available schemes for non-foundational IDs

Scope	Data model name	Brief explanation	Status/ Detailed explanation	Schema URL	Registry URL
Non-foundational identity	EducationalID	Identifies the natural person in the context of an educational organisation, including national extensions	Available	Schema	Verifiable Data Registry
Non-foundational identity	AllianceID	Identifies a student or staff member as affiliated with a European university alliance	Available	Schema	Verifiable Data Registry
Non-foundational identity	EuropeanStudentCard	European Student Card for student mobility, based on DG-EAC's service	Available	Schema	Verifiable Data Registry
Non-foundational identity	MyAcademicID	Identity credential for student mobility, based on MyAcademicID and eduGAIN infrastructure	Available	Schema	Verifiable Data Registry
Non-foundational identity	ProfessionalID	Identity credential for , based on	Available	Schema	Verifiable Data Registry
Non-foundational identity	DoctorID	Identity credential for , based on	Available	Schema	Verifiable Data Registry
Non-foundational identity	EngineerID	Identity credential for , based on	Available	Schema	Verifiable Data Registry

<https://github.com/dc4eu/educational-pilot/tree/main/sectorial-eaa-catalogue>

Mobile Identity → Digitale Identität

Pilotbericht: European Student Card als Verifiable Credential

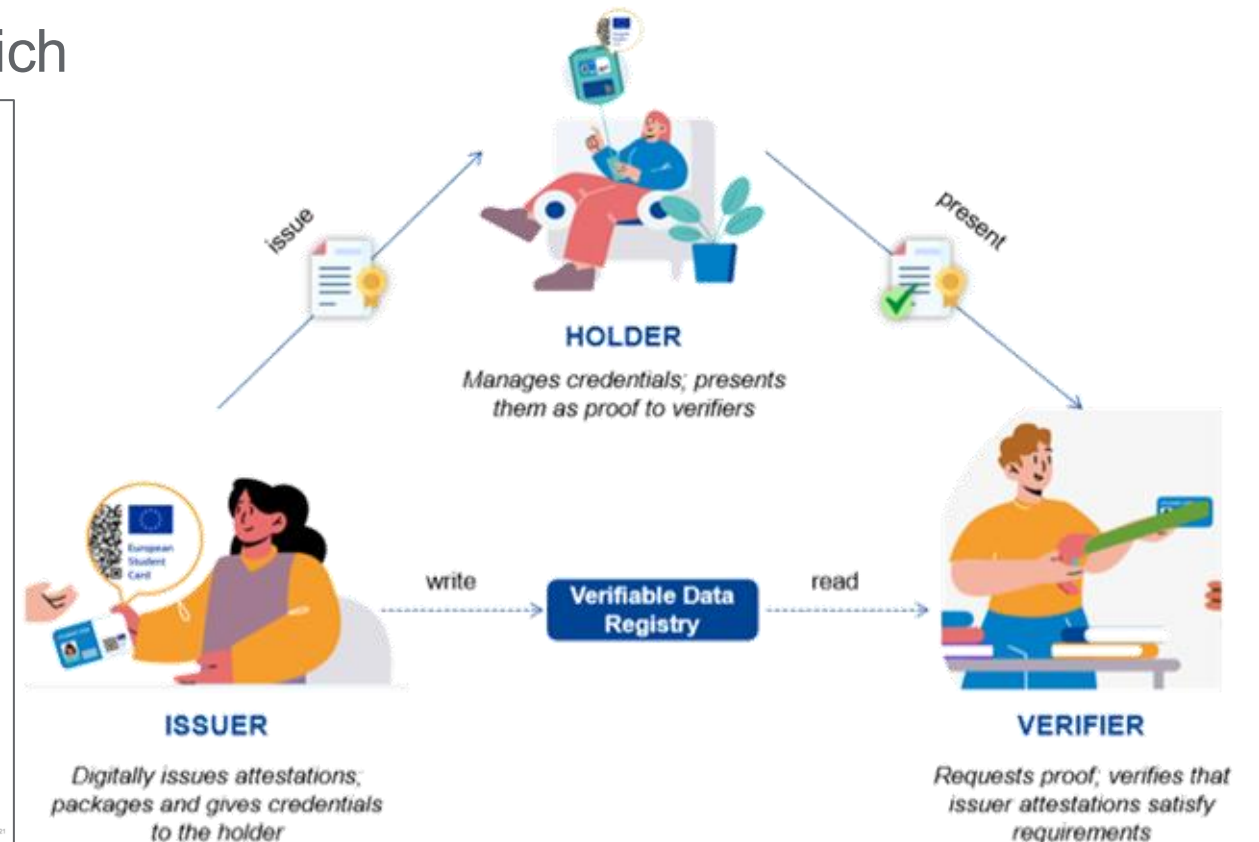
- W3C Verifiable Credential Data Model v1
- Datenmodell auf ELM-Basis (European Learning Model) – Attributstruktur
→ Revocation-/Update-Prozess erforderlich



ANNEX I: Participating organisations

Participating organisations

Organisation	Country
Aegean University	Greece
Aristotle University of Thessaloniki	Greece
Freie Universität Berlin (Una Europa alliance)	Germany
Katholieke Universiteit Leuven (Una Europa alliance)	Belgium
Ludwig-Maximilians-Universität München	Germany
National and Kapodistrian University of Athens	Greece
Politecnico di Milano	Italy
Sikt	Norway
Universidade de Beira Interior	Portugal
Università di Bologna (Una Europa alliance)	Italy
Università di Pavia	Italy
Universitat de Barcelona	Spain
Université de Strasbourg	France



Ein Common Identity Pass nach dem ISO/IEC-18013-5-Modell

Digitale Identität im Wallet

Gängige Verifiable-Credential-Formate / Protokolle für digitale Identitäten

- SD JWT (EU)
- ISO/IEC 18013-5 (mDL & mDoc)
- W3C Verifiable Credential Data Model

Issuing- und Presentation-Protokolle

- OID4VC (OID4VCI and OID4VP)
- ISO/IEC 18013-5



Für **Proximity**-Use-Cases ist **NFC-/BLE-Übertragung** entscheidend

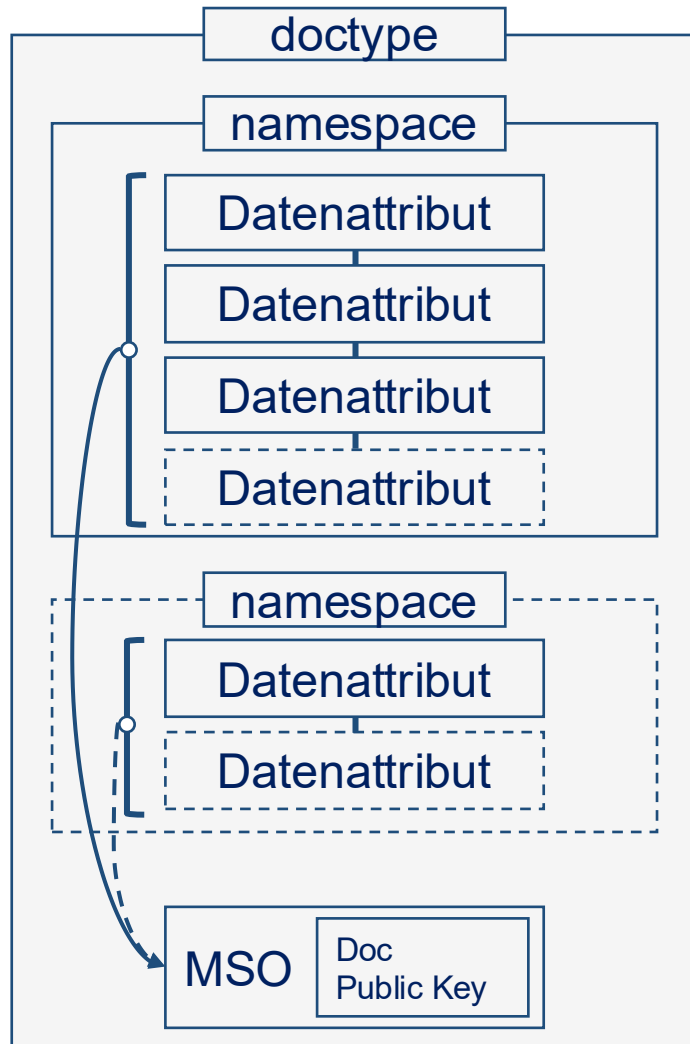
→ Unsere Wahl: ISO/IEC 18013-5 (mDoc) für Wallet-Credentials
DC4EU → SD JWT

Ein Common Identity Pass nach dem ISO/IEC-18013-5-Modell

- Das Modell „ISO/IEC 18013-5 Personal Identification“ ist ausgelegt für:
 - Ein Protokoll, mit dem zwei Geräte eine sichere drahtlose Verbindung aufbauen und strukturierte Request-/Response-Nachrichten austauschen
 - **Identifikation** des Credential-Inhabers (User Binding)
 - Selektive Freigabe von Datenelementen durch den Inhaber (Datenminimierung)
 - **Pre-consent** Mechanismus für häufig wiederholte Vorgänge (z. B. Rabatt-Zahlung in der Mensa)
 - Ein Protokoll, um Credential-Daten direkt vom Mobilgerät abzurufen – rein offline; sichert Verfügbarkeit und Nicht-Nachverfolgbarkeit
 - Ein optionales Protokoll, um Zusatzdaten von der ausstellenden Stelle abzurufen
 - Ein Mechanismus zur Sicherung von **Integrität** und **Authentizität** der Credential-Daten
 - Ein Mechanismus zur Bestätigung der Gerätebindung (Signatur zum Transaktionszeitpunkt)
 - Multi-Dokument- und Multi-Namespace-fähig erweiterbar für weitere Use-Cases
- **Etabliertes staatliches Credential-Format, bereits im Einsatz Folgt dem ARF of EUDI-Wallet**
 Mobiler Führerschein (mDL) / eu.europa.ec.eudiw.pid.1 (Prototyp nationaler eIDs in Europa)
- **Bereits unterstützt** von den OEM-Smartphone-Herstellern (Apple und Google)
 → siehe: <https://android-developers.googleblog.com/2020/11/privacy-preserving-features-in-mobile.html>



Ein Common Identity Pass nach dem ISO/IEC-18013-5-Modell



Wiederverwendung der Verzeichnisdaten (gängige eduGAIN-Attribute):

- portrait (photo, *verpflichtend für Ausweisdokumente*)
- givenNames
- sn (Nachname)
- email
- eduPersonAffiliation / eduPersonScopedAffiliation
- eduPersonEntitlement
- eduPersonAssurance
- schacHomeOrganization
- schacPersonalUniqueCode → European Student Identifier (ESI) - MyAcademicID
- schacDateOfBirth
- schacYearOfBirth
- schacPlaceOfBirth
- schacExpiryDate
- ...



*funktioniert wie eine Shibboleth-Authentifizierung
vor Ort → eingespielte Prozesse*

siehe auch DC4EU Education ID

(<https://code.europa.eu/ebsi/json-schema/-/tree/main/schemas/vcdm1.1/education/verifiable-education-id>)

Authentifizierungs- und Autorisierungs-Infrastruktur (AAI) und AAI-Föderation

→ eduGAIN ist der Schlüssel zur Interoperabilität von Nutzeridentitäten

→ Interoperabilität hängt maßgeblich vom gemeinsamen Verständnis von Vokabular und Spezifikationen ab (LDAP-Schema)

✓ eduPerson

✓ SCHAC (Schema for Academia)

✓ SAML

✓ OIDC

→ Was ist MyAcademicID?

MyAcademicID ≠ European Student Identifier

1994]



English version

[Impressum](#) | [Datenschutzerklärung](#) | [Kontakt und FAQ](#)

Attributes received:

eduPerson

- 2.2.1. **eduPersonAffiliation**
- 2.2.2. eduPersonEntitlement
- 2.2.3. eduPersonNickname
- 2.2.4. eduPersonOrgDN
- 2.2.5. eduPersonOrgUnitDN
- 2.2.6. eduPersonPrimaryAffiliation
- 2.2.7. eduPersonPrimaryOrgUnitDN
- 2.2.8. eduPersonPrincipalName
- 2.2.9. eduPersonPrincipalNamePrior
- 2.2.10. **eduPersonScopedAffiliation**
- 2.2.11. eduPersonTargetedID
- 2.2.12. **eduPersonAssurance**
- 2.2.13. eduPersonUniqueid
- 2.2.14. eduPersonOrcid

Beispiel einer eduPersonScopedAffiliation:

student@lmu.de
student@up.pt
student@eugloh.eu

Beispiele:

schacHomeOrganization: lmu.de

schacPersonalUniqueCode: [ESI → urn:schac:personalUniqueCode:int:esi:lmu.de:1234567890]

SCHAC (Schema for Academia)

- Persönliche Merkmale
 - schacMotherTongue
 - schacDateOfBirth
 - schacYearOfBirth
 - schacPlaceOfBirth
 - schacCountryOfCitizenship
 - schacSn1
 - schacSn2
 - schacPersonalTitle
- Kontakt-/Ortsangaben
 - schacHomeOrganization
 - schacHomeOrganizationType
 - schacCountryOfResidence
 - schacUserPresenceID
- Studierenden-Informationen
- Beschäftigten-Informationen
 - schacPersonalPosition
- Verknüpfungs-IDs / Fremdschlüssel
 - schacPersonalUniqueCode
 - schacPersonalUniqueID
- Eintrags-Metadaten / Verwaltungsinformationen
 - **schacExpiryData**
- Vertraulichkeit / Attribute Release (Sichtbarkeit)
 - schacUserPrivateAttribute

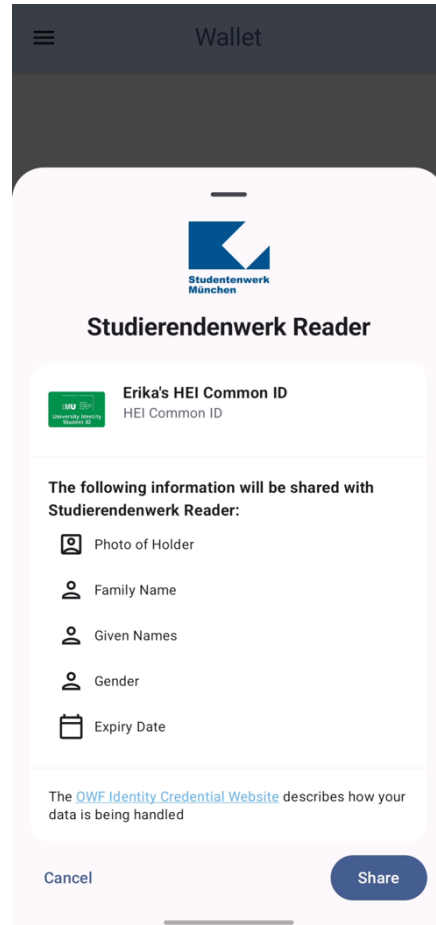
Basis-Schemata

- givenName
- sn (Nachname)
- displayName
- initials
- title
- jpegPhoto
- mail
- phone
- cn
- uid
- o
- ou
- preferredLanguage
- homePostalAddress
- postalAddress
- dfnEduPersonLibraryPatronId
- dfnEduPersonLibraryUsergroup
- dfnEduPersonFinalDegree
- dfnEduPersonTypeOfStudy

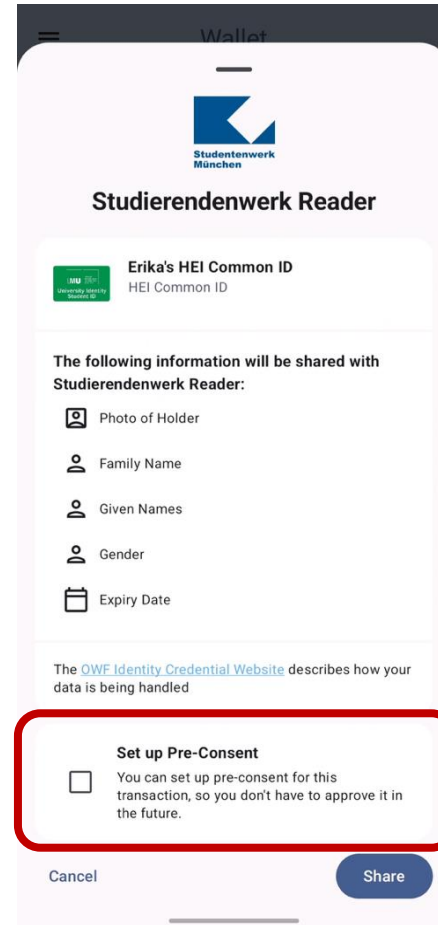
→ EDEH HEIF TF 3: User Identity

Mobile Identity → Digitale Identität

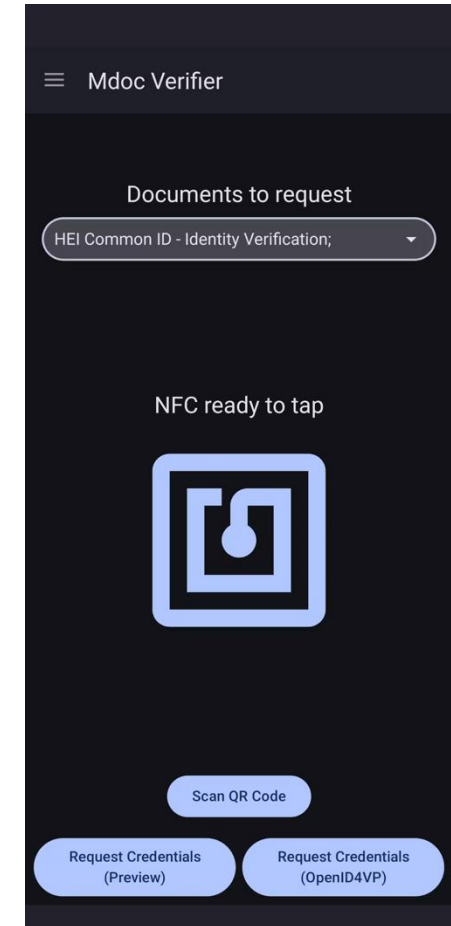
Identity Pass: Der Weg zur besten User Experience und Interoperabilität



Informed Consent



Informed
Consent
+ Pre-Consent



Verifier-
App

Identität steuert den Zugang zu Services eduGAIN (online Services) → eduTAP (physische Services)



WLAN weltweit mit der Heimat-
Kennung – seit 2003. So einfach muss
Servicezugang sein.



Online-Zugang

Föderierter Login & Attribute für alle
Online-Services – läuft heute.



Physischer Zugang

Vor-Ort-Zugang per Wallet-Pass: Tür,
Mensa, Bibliothek – die dritte Schicht.

eduGAIN liefert den Online-Zugang, eduTAP den physischen.

Eine Frage der Größenordnung: Student IDs

Europäische Union

- ~ **5,000** Hochschulen (HEIs)
- ~ **18,800,000+** Studierende (tertiär, 2022)

Erasmus+-Länder

- Umfasst EU + Island, Liechtenstein, Norwegen, Nordmazedonien, Serbien,
- Erweitert die europäische Hochschullandschaft deutlich → ~ **20,000,000+** Studierende (tertiär)
- **UK tritt dem Erasmus+-Programm wieder bei; wirksam ab 2027**

Weltweit

- ~ **18,000** anerkannte Hochschulen in 180+ Ländern
- ~ **200,000,000+** Studierende weltweit

→ Es soll überall funktionieren: **nahtlose Mobilität & einfacher Servicezugang**
→ eine **GLOBALE Student ID**



→ Organisiert in
National Research and Education Networks (NRENs)

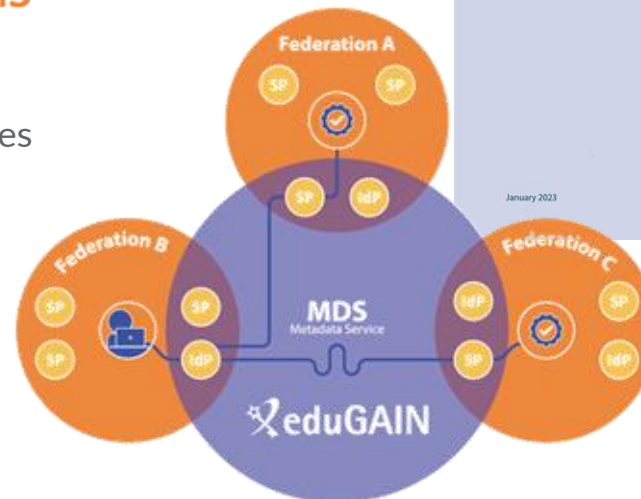
The GÉANT Association is the collaboration of European National Research and Education Networks (NRENs)

- Non-Profit Organization
- Service-Provider for IT / e-Infrastructure services for the European Higher Education Sector
- Pan European – Non-EU members
- Key Services:

- **GÉANT Trust & Identity Services**



- GÉANT Network and Connectivity Services
- GÉANT Security Services
- GÉANT Cloud Services
- Procurement Agency for EU-HEIs



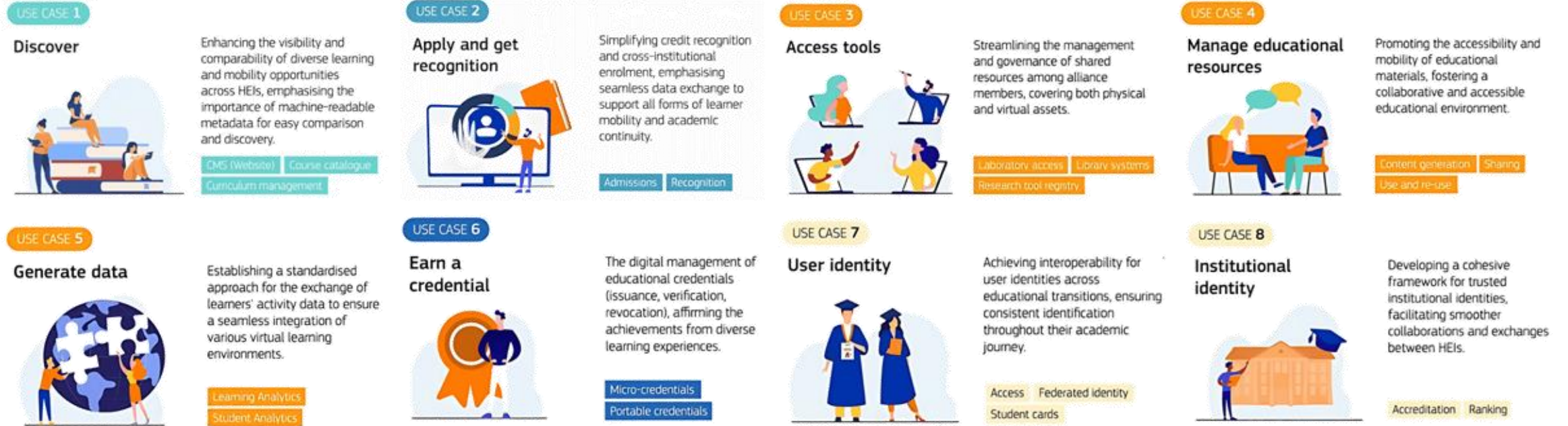
→ **eduTAP** is a perfect fit for GÉANT Trust & Identity Services

eduTAP als weitere Säule in GÉANTs Trust & Identity Services



ECCA Conference 2025, LMU München —
Alexander Loechel (LMU, Erfinder von eduTAP) und
Klass Wierenga (Chief Services Officer, GÉANT · Erfinder von eduroam)

The Higher Education Interoperability Framework



© European Digital Education Hub

The European Education Area focuses on the learner's journey, across institutions

Two Use-Cases are essential for a smooth and seamless mobility:

- ✓ User Identity
- ✓ Access Tools

Das Higher Education Interoperability Framework Team und die Task-Force 3: User Identity

- Der European Digital Education Hub – Working-Group on an Interoperability Framework
- Task-Force 1-3



Task-Force 3: User Identity



Webseiten:

- <https://eduTAP.eu/> Projekt-Homepage
- <https://eduTAP.eu/presentations> Vorträge zu eduTAP
- <https://docs.eduTAP.eu/> Dokumentation zu eduTAP
- <https://github.com/edutap-eu> GitHub-Organisation mit den Core-Bibliotheken
- <https://github.com/edutap-collective> GitHub-Organisation für Non-Core-Pakete der eduTAP-Komponenten – Beispiele

Paper:

- <https://easychair.org/publications/paper/Lvsf> - eduTAP – a Concept and System of Digital Identities for Proximity On-Site Service Access
- <https://easychair.org/publications/paper/ZpCzX> - eduTAP Common ID - A Standardized Digital Identity Document for HEIs

Standards:

- <https://www.iso.org/standard/69084.html> ISO/IEC 18013-5
- <https://www.iso.org/standard/76927.html> ISO/IEC 14443-4:2018
- <https://eudi.dev/3.0.0/main/> Architecture and Reference Framework – EUDI-Wallet



LUDWIG-
MAXIMILIANS-
UNIVERSITÄT
MÜNCHEN

Alexander Loechel
Referent IT-Projekte
IT-Services · Ludwig-Maximilians-Universität München
Martiusstraße 4 · 80802 München · Tel. +49 89 2180 9831
Alexander.Loechel@lmu.de · www.lmu.de



Mobile Identity → Digitale Identität

Gastgeber der letztjährigen ECCA-Konferenz – Connecting Technologies



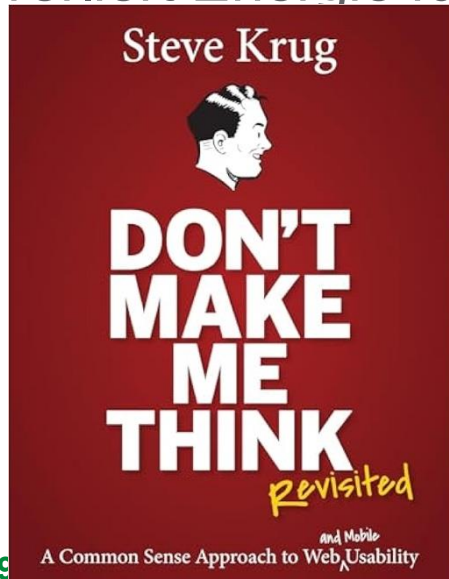
Every company gets about three innovation tokens.

Quelle: Dan McKinley, "Choose Boring Technology"

<http://mcfunley.com/choose-boring-technology>

„Boring“ heißt: Es funktioniert einfach

Für Menschen gilt dasselbe: Wer **nachdenken muss**, um et
verliert Energie für Wichtigeres



Don't make me think

→ User Experience ist entscheidend

Man sollte sich **NICHT** kümmern müssen
„langweiliges“ und „unwichtiges“ Drum

Man sollte sich be able to
Wesentliche konzentrieren können
(*Studieren, Lernen, Forschen, ...*)



Mobile Identity Digitale Identität

Kano-Modell – Systematik für User Experience & Nutzerzufriedenheit

Ob eine Technologie angenommen wird, hängt davon ab:

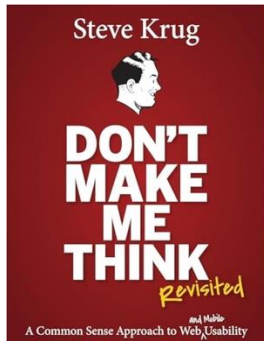
- Löst sie die Bedürfnisse der Nutzer/Kunden?
- Ist die User Experience gut genug?

Jedes Unternehmen hat etwa drei Innovation Tokens.

Quelle: Dan McKinley, „Choose Boring Technology“
<http://mcfunley.com/choose-boring-technology>

„Boring“ ist ein Vorteil – „langweilige“ Technik bringt Dinge zum Laufen

Dasselbe gilt für Menschen: Wer **nachdenken muss**, um etwas zu erledigen, verbraucht Energie, die für Wichtigeres fehlt

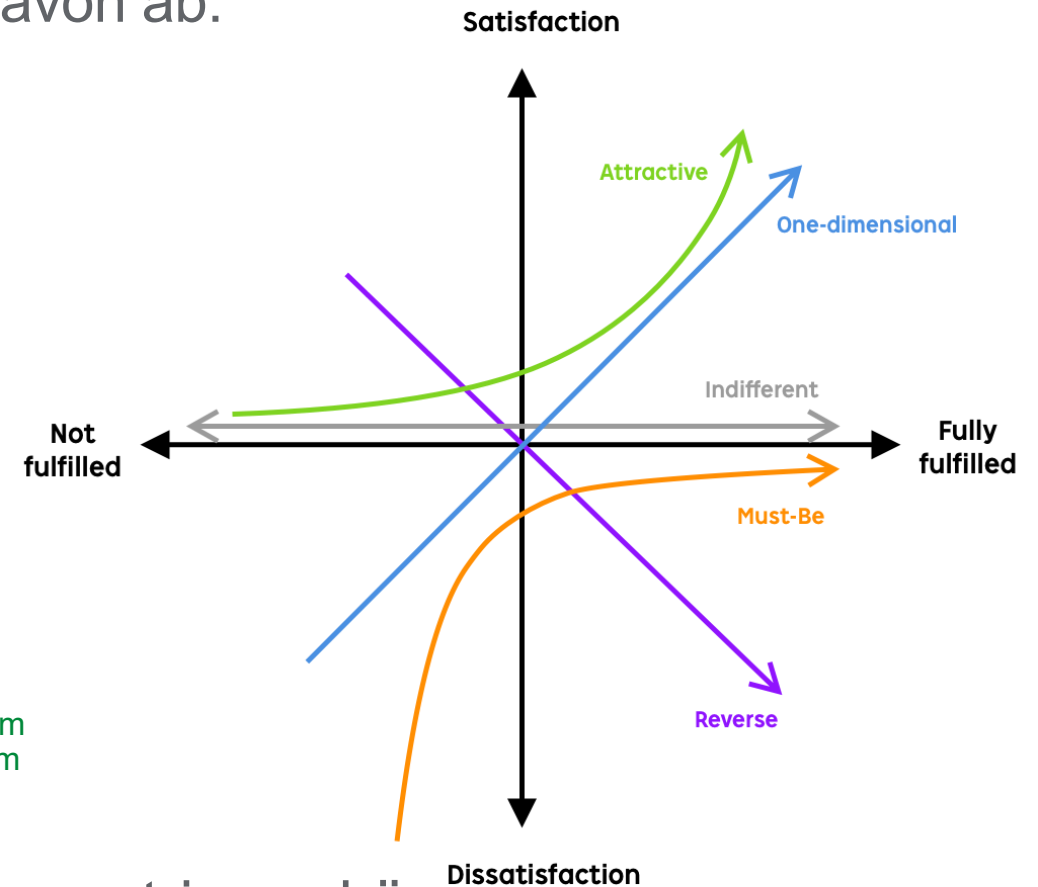


Don't make me think

→ User Experience ist entscheidend

Man sollte sich **NICHT** kümmern müssen um „langweiliges“ und „unwichtiges“ Drumherum

Man sollte sich **auf das Wichtige** konzentrieren können
(Studieren, Lernen, Forschen, Lehren, ...)



Business-Case-Test → Wirtschaftlichkeitshürde

Kosten eines Smart Campus vs. Kosten eines Smarter Campus?

An der LMU haben wir:

- 15 Kartendrucker, 60 Validierungsdrucker
 - Kosten pro Leser: 150 – 350 € je nach Use-Case (Desktop-Leser vs. PAC-Leser)
 - Die Infrastrukturkosten des Smart Campus ändern sich nicht – unsere Leser sind von Haus aus voll kompatibel mit Wallet-Passes.
 - Die LMU besitzt alle Credentials und Smart-Campus-Geräte selbst – keine Abhängigkeit von einzelnen Herstellern
- ~ 840 Professor*innen
 - ~ 6.250 wissenschaftliches Personal (Faculty)
 - ~ 10.500 nichtwissenschaftliches Personal (Staff)
 - ~ 20.000 Klinikpersonal am Universitätsklinikum (Affiliates)
 - ~ 55.000 Studierende (Student)
 - ~ 70.000 aktive LMUcards (Student & Staff)
 - ~ 200.000 Bibliotheksnutzer*innen (separate Karte)

→ Der Kostenunterschied liegt beim Medium

Ausweisbezogene Kosten:

- ✓ LMUcard (LEGIC CTC4096-MM): ~13,50 € / ausgegebene Karte
(Haltbarkeit ~ 3–5 Jahre ~> 1–2 Karten pro Studierendem) ~ 20,00 € / Studierendem
- ✓ Digitale Credentials im Wallet: vs
 - ✓ Apple VAS / Google Smart Tap: 0,15 €
 - ✓ Apple Access Passes: ~ 2,00 € / Nutzer und Jahr ~ 10,00 € / Studierendem

→ Wallet-Passes sind günstiger,

aber im ersten Jahr gibt es keine voll digitalisierte Karten-/Pass-Nutzung

→ doppelte Kosten und Skalenverlust bei der Kartenbeschaffung;

→ Infrastruktur-Overhead pro Karte steigt.

→ Aber selbst wenn es günstiger ist: Hilft es den Studierenden?

→ Und die Reputation – die nicht-monetären Werte einer Hochschule?

1. **Smartere Technologie ≠ bessere Ergebnisse**
Smartere IT macht die Institution nicht besser.
Sie macht nur die Technologie moderner.
2. **Es gibt keinen Business Case ohne Service**
Wer Service und Ergebnis nicht klar definieren kann,
hat keinen Business Case – nur Technologie-Rollout.
3. **Der echte Business Case ist organisatorische Veränderung**
Smartere IT besteht den Business-Case-Test nur,
wenn sie verändert, wie die Institution arbeitet –
nicht nur, wie sie authentifiziert oder vernetzt.

Mobile Identity → Digitale Identität → Ausweise (digital & physisch)

Campuskarten = Zugang zu Services → Smart Campus → Zutritts- & Identitäts-Credentials

Identifikation

- **Identifikation**
- **Statusnachweis**
- **Berechtigungsnachweis**
- Single Sign On / 2FA / FIDO2
- Anwesenheitskontrollen
 - Check-in bei Prüfungen
 - Anwesenheit in Lehrveranstaltungen
 - Zeiterfassung
- Elektronische Signatur (of legal documents)

Elektronisches

- Bezahlen / Cashless Campus
- Mensa & Cafeterien
- Automaten
- Printing / scanning (secure & follow me printing)
- Ticketing (events and conferences)

Physische

- Zutrittskontrolle
- Areas (campus, parking lot)
- Gebäude
- Räume
 - Seminarräume
 - Labore
 - Computerräume
 - Lernräume
 - Büros
 - Accommodation facilities (i.e., dorms)

Bibliotheksservices

- Zugang / Ausleihe
 - Physische Medien (Bücher, Audio- und Videomedien)
 - E-Medien (E-Books, Audio- und Videomedien)
- Lernräume

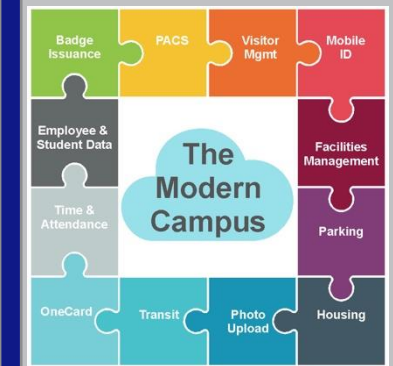
Mobilität

- On campus services (university shuttle service)
- ÖPNV-Tickets & -Rabatte

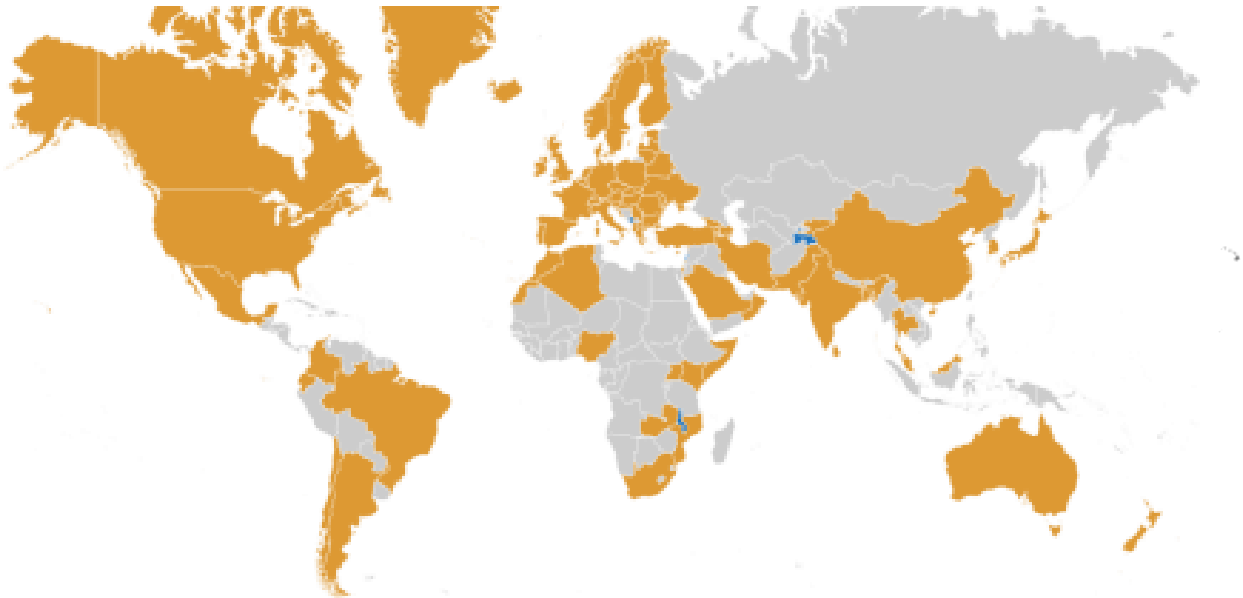
Rabatte und Aktionen

- **Rabatte** auf Kulturangebote
 - Museen
 - Theater
 - Kinos
- Geschäfte
- Restaurants

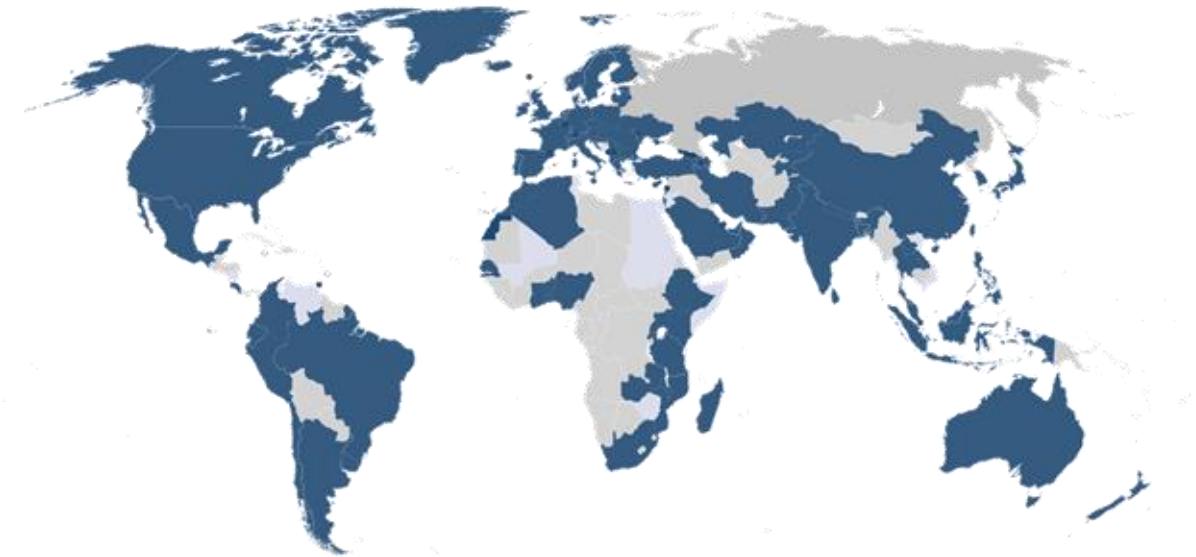
On- & Off-Campus → On-Site Usage / Proximity Use-Cases
+ Online Services



→ eduGAIN-Föderationsmitglieder



→ eduroam-Service-Provider



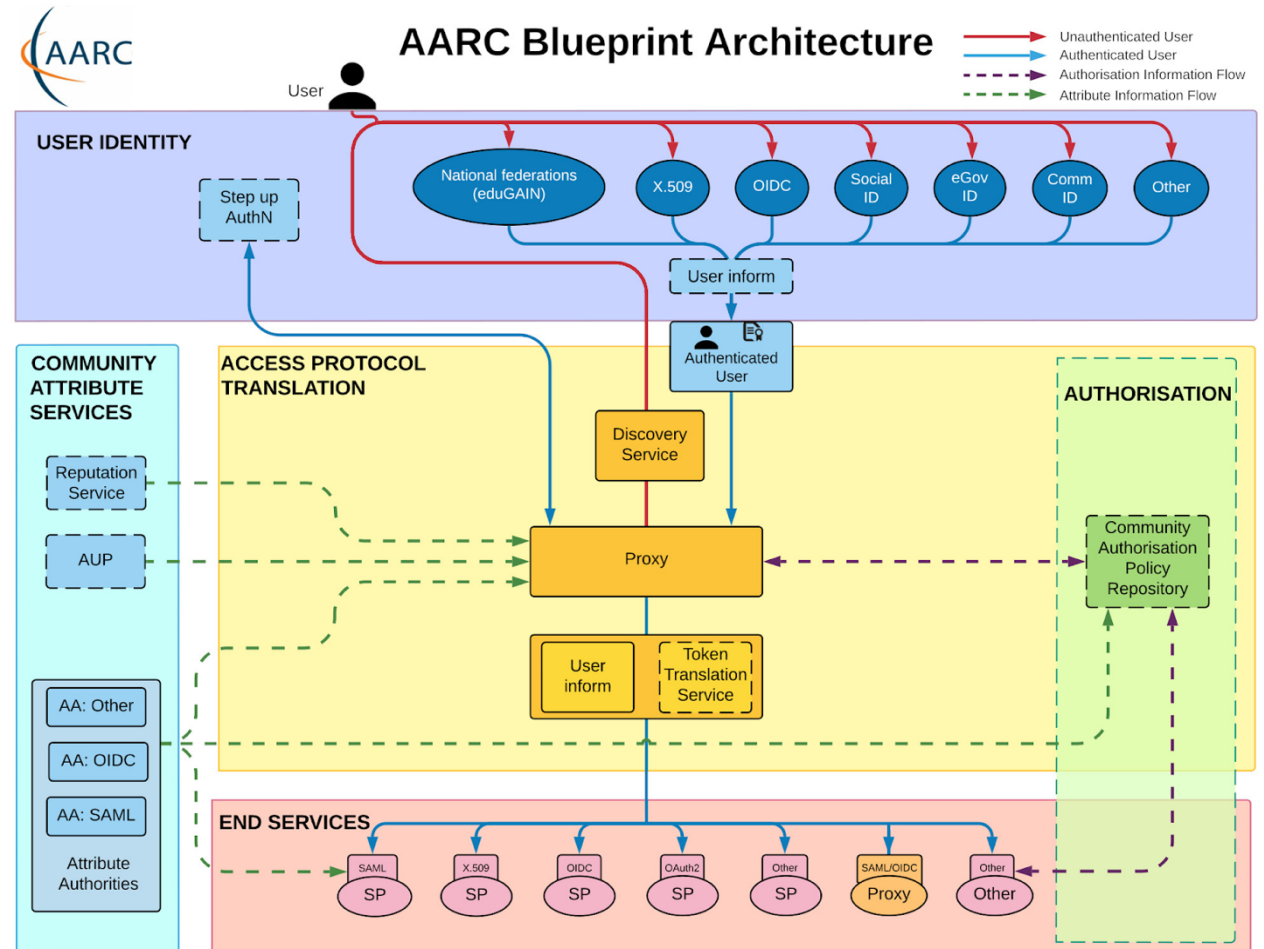
Die AAI/eduGAIN-Rückgrat: AARC-Architektur

Kernkomponenten der AAI (SAML-Begriffe):

- Identity Provider (IdP)
- Service Provider (SP)
- Discovery Service (DS) → WAYF

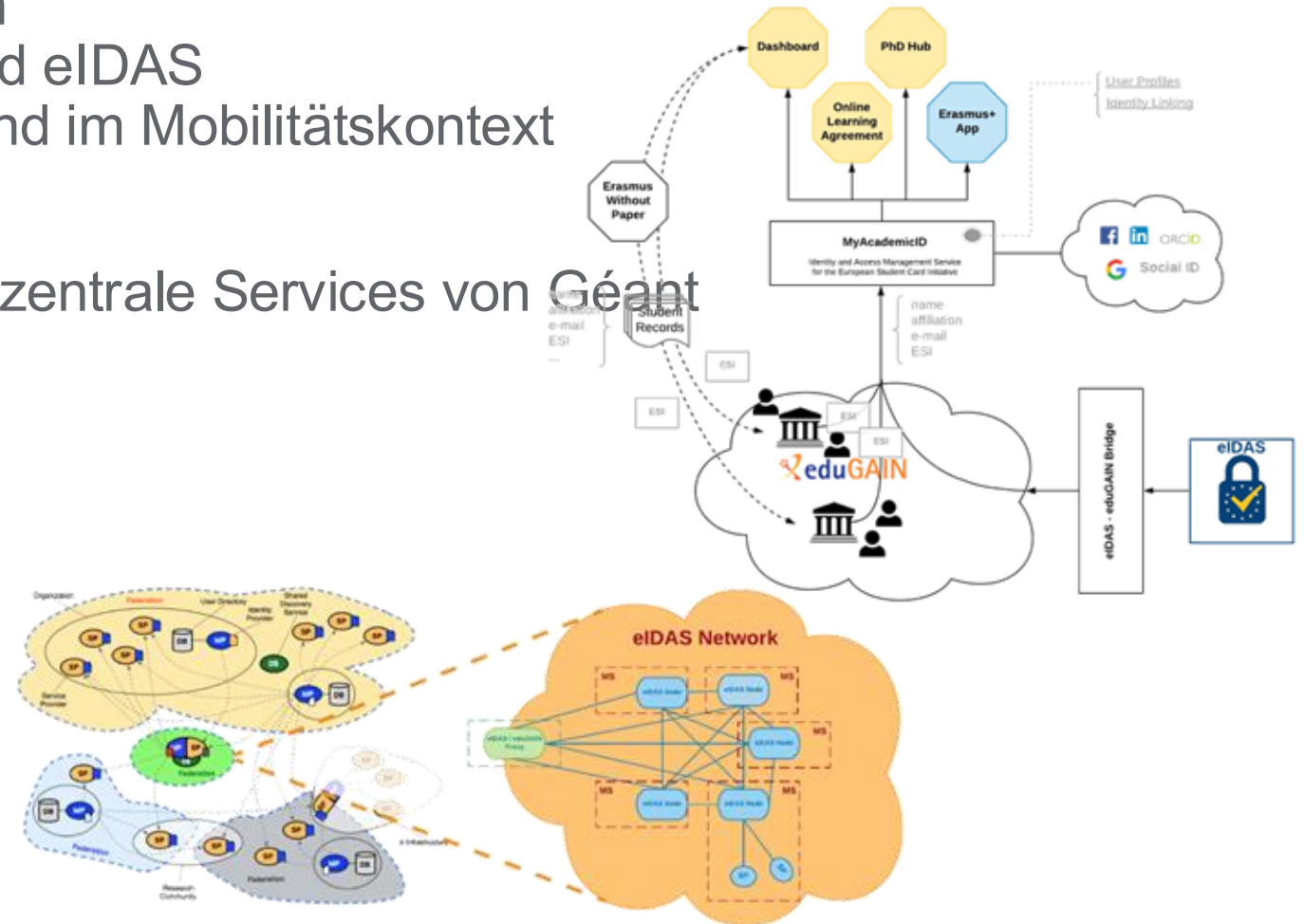
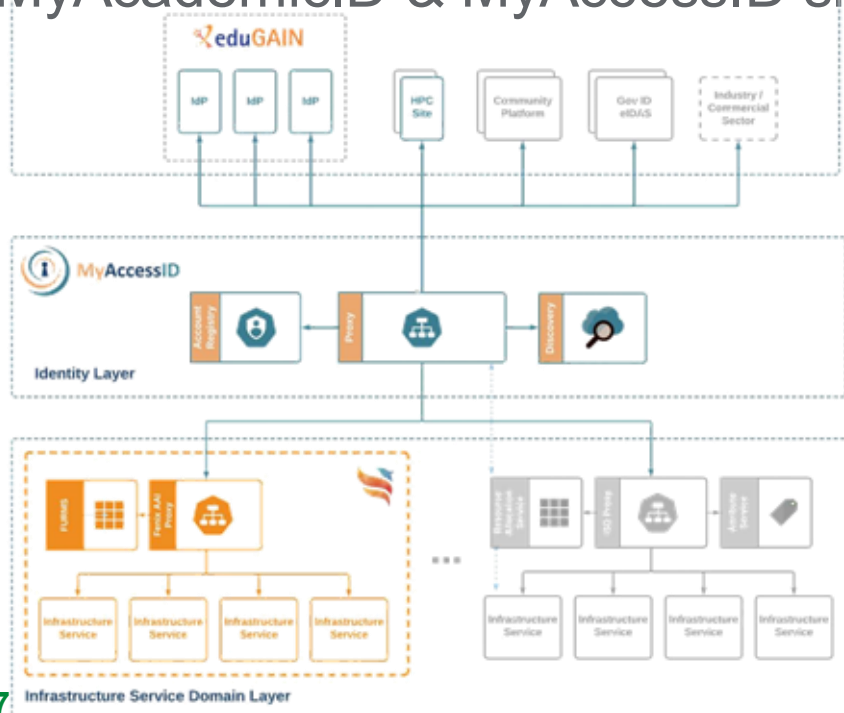
Weitere, heute noch seltene Elemente:

- Attribute Authorities
 - Metadata Aggregators
- MyAcademicID-Network



MyAcademicID als Brücke zwischen eduGAIN (AAI der Hochschulen) und eIDAS zu den Services der Hochschulen und im Mobilitätskontext

MyAcademicID & MyAccessID sind zentrale Services von Géant



Mobile Identity Digitale Identität EAM-Scope → Business-Motivation & Capabilities

Kerngeschäft einer Hochschule:

- Lehre und Studium
- Forschung
- Transfer

Services eines Smart Campus
sind unterstützende Fähigkeiten
(Enabling Capabilities)

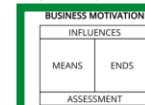
- ✓ Zugang zu Räumen / Campus
- ✓ Essensausgabe in Mensen und Cafeterien
- ✓ Zugang zu Bibliotheksressourcen
- ✓ Kopieren & Drucken
- 88 ✓ Anwesenheitserfassung
- ✓ Mobilität

HIGHER EDUCATION BUSINESS REFERENCE MODEL



DESCRIPTION
The Higher Education Business Capability Model describes a standard set of Business Architecture elements relevant to Higher Education. It can be used as a reference for Business Stakeholders, Enterprise Architects, and Technology Strategists to engage in discussion regarding business effectiveness, needs, and challenges. Standing alongside the accompanying Business Model Canvas, the Business Capability Model elaborates the core value chains for higher education and their underlying business capabilities.

UNDERSTANDING BUSINESS CAPABILITIES
A Business Capability is a particular logical combination of People, Process, Information, and Technology necessary to deliver a discrete required outcome to achieve a specific business objective. The business capabilities support the realisation of an institution's strategies. This model supports the development of strategies by viewing an institution as a collection of business capabilities that can be adjusted in response to the demands of the market.



The Business Capability Model provides perspectives such as strategic in business operational pain points, organisational structure. It provides traceability from business objectives, technology, and other resources.

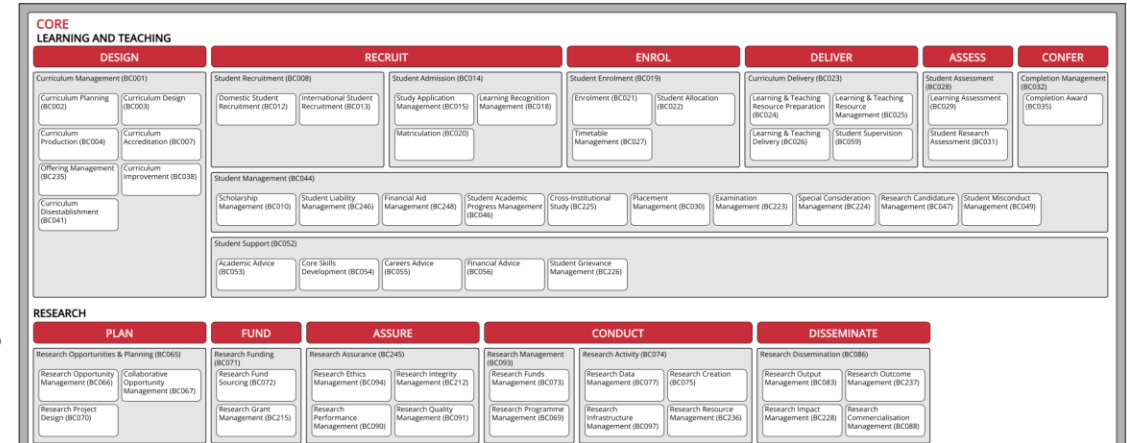
Typically an **ORGANISATIONAL** structure provides context for the scope of the model.

VALUE CHAINS capture how the Learning & Teaching and Research business capabilities are organised under the relevant Value Chains.

CORE business capabilities directly support the institution's mission and are organised under the relevant Value Chains.

ENABLING business capabilities support the core business capabilities and the value chains and keep the institution running.

FURTHER business capabilities are not directly related to the institution's mission but provide additional support.



Studierende & Beschäftigte interessieren die „Enabling Capabilities“ nicht – sie wollen sich auf ihr Kerngeschäft konzentrieren:

- ✓ Studierende wollen **lernen**
- ✓ Wissenschaftliches Personal will **forschen** and **lehren**

→ Serviceorientierung des Smart Campus