eduTAP

https://eduTAP.eu

A Concept and System of Digital Identity Credentials for proximity on-site service access

Modern Campus ID (Student ID / Staff ID) for universities in Europe & the world

Alexander Loechel – FOREU-IT topical group on interoperability – 04.12.2025 - online

EUGLOH

European University Alliance for Global Health

www.eugloh.eu

Definition of Interoperability

Interoperability

Noun

- The ability of computer systems or software **to exchange** and **make use of information**.

<div align="right">Definition as of Oxford Languages</div>

Digital Credentials for Higher Education

Two Digital Credential Verticals, one Wallet Environment

| **Long-Term Digital Credentials** | **European Digital Identity Wallet (EUDI-Wallet)** | **Short-Term Digital Credential** |

- Diplomas / Diploma Supplements
- Transcript of Records
- Micro-Credentials

- Container for Credentials
- Web-Wallet

- Student IDs
- Library-IDs
- Event-Tickets

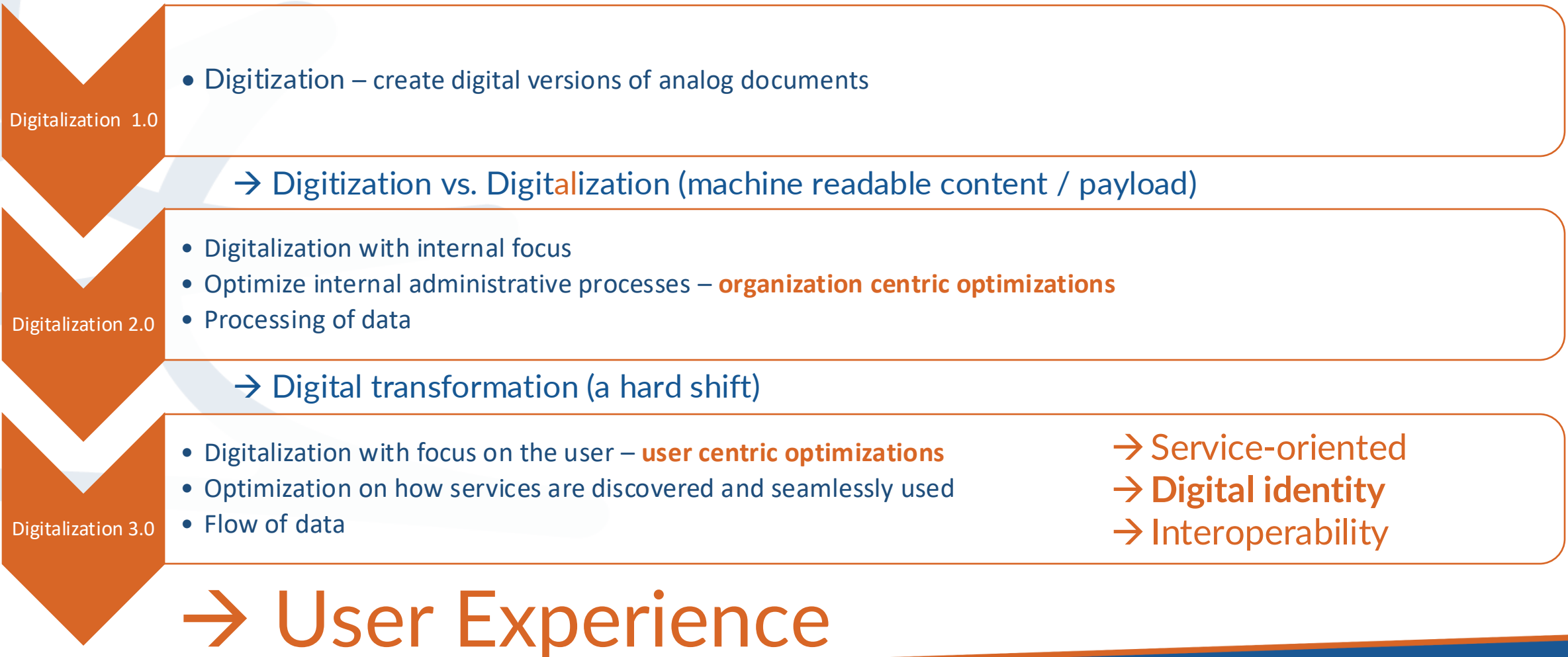→ *Digitization of Academic Proofs of Achievement*

→ *Digitize, **digitalize** and simplify administrative processes*

→ *Digitalization of Service Access*

→ DC4EU / EBSI / EDEH Interoperability Framework

→ European Student Card / **eduTAP**

Stages of Digitalization – Period of Digital transformation

Digitalization 1.0

- Digitization – create digital versions of analog documents

→ Digitization vs. Digit**al**ization (machine readable content / payload)

Digitalization 2.0

- Digitalization with internal focus
- Optimize internal administrative processes – **organization centric optimizations**
- Processing of data

→ Digital transformation (a hard shift)

Digitalization 3.0

- Digitalization with focus on the user – **user centric optimizations**
- Optimization on how services are discovered and seamlessly used
- Flow of data

→ Service-oriented
→ **Digital identity**
→ Interoperability

→ User Experience

Trust level / Assurance Level

→ Very important for **IDENTIFICATION & AUTHENTICATION**
→ Quality of identity (personal) data
→ Type of authentication & consequences for identification medium

no trust

normal

Authentication:
• username / email + password

Identity proofing:
→ self-asserted
→ verified e-mail address

substantial / medium

Authentication
• certificate based
• FIDO2
• Smart ID

Identity proofing:
→ officially confirmed
→ manual check of a government issued photo-ID

high

Authentication
• eID.AS compliant
  → eID of EU Citizen IDs
  → provided by HEI for foreign Students

Identity proofing:
→ officially confirmed
→ Identity document automated and technically checked to be genuine and represent the claimed identity

Recognition of eduTAP @ Conferences

ECCA Conference 2025 LMU Munich, Germany   EUNIS Conference 2025 Belfast, UK → Elite Award
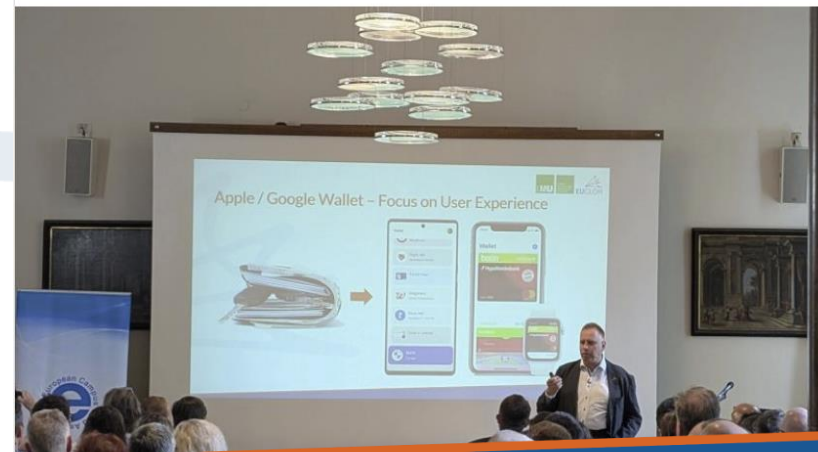
EUGLOH

European University Alliance for Global Health

edu**TAP**

https://eduTAP.eu

Modern Campus ID (Student ID / Staff ID)
for universities in Europe & the world

Concept of eduTAP
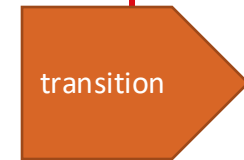
The LMU Student ID (over time)

LMU Student ID till 2019

transition

LMUcard Student ID 2019-2025

transition

today

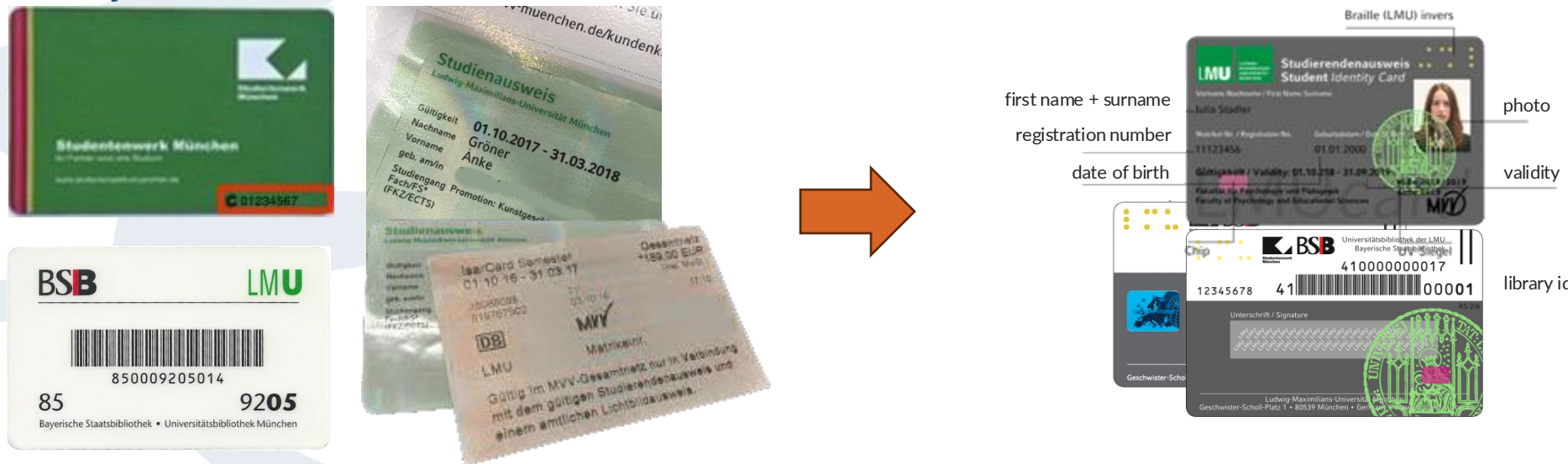LMU Student ID 2025+

transition

LMU Student ID 2027+ ?

eduTAP & eduTAP@LMU

LMUcard – LMU Student ID

The transition of LMU Student IDs from paper to plastic cards (LEGIC CTC4096-MM410)

→ A Project 2015 – 2019

Goal: *A modern integrated, contactless card for all services at LMU* ← Better User Experience
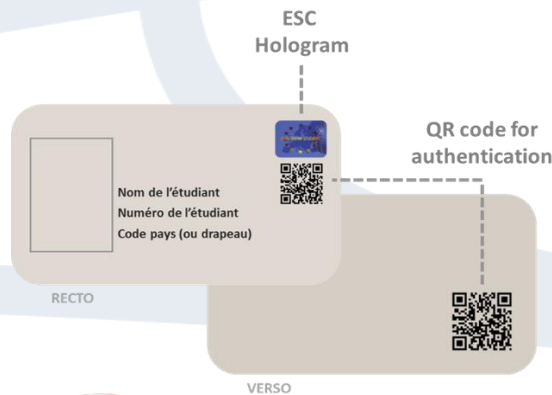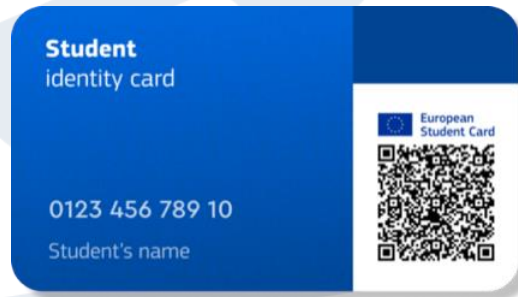
✓ Visual Student ID – contactless readable registration number

✓ Payment at mensa / canteens, cafeterias and vending-machines, copiers

✓ Library ID ✓ Public Transport Ticket (MVV Semesterticket)

It was a hard project with a lot of stakeholders

The European Student Card (ESC)

The **European Student Card** – a project to add a **European dimension** to local Student IDs

✓ Securely **validate** the **student status**

ESC Hologram

QR code for authentication

Nom de l'étudiant
Numéro de l'étudiant
Code pays (ou drapeau)

RECTO

VERSO

Idea by →
Jean-Paul Roumegas
(les Crouse)

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.

✓ A great vision

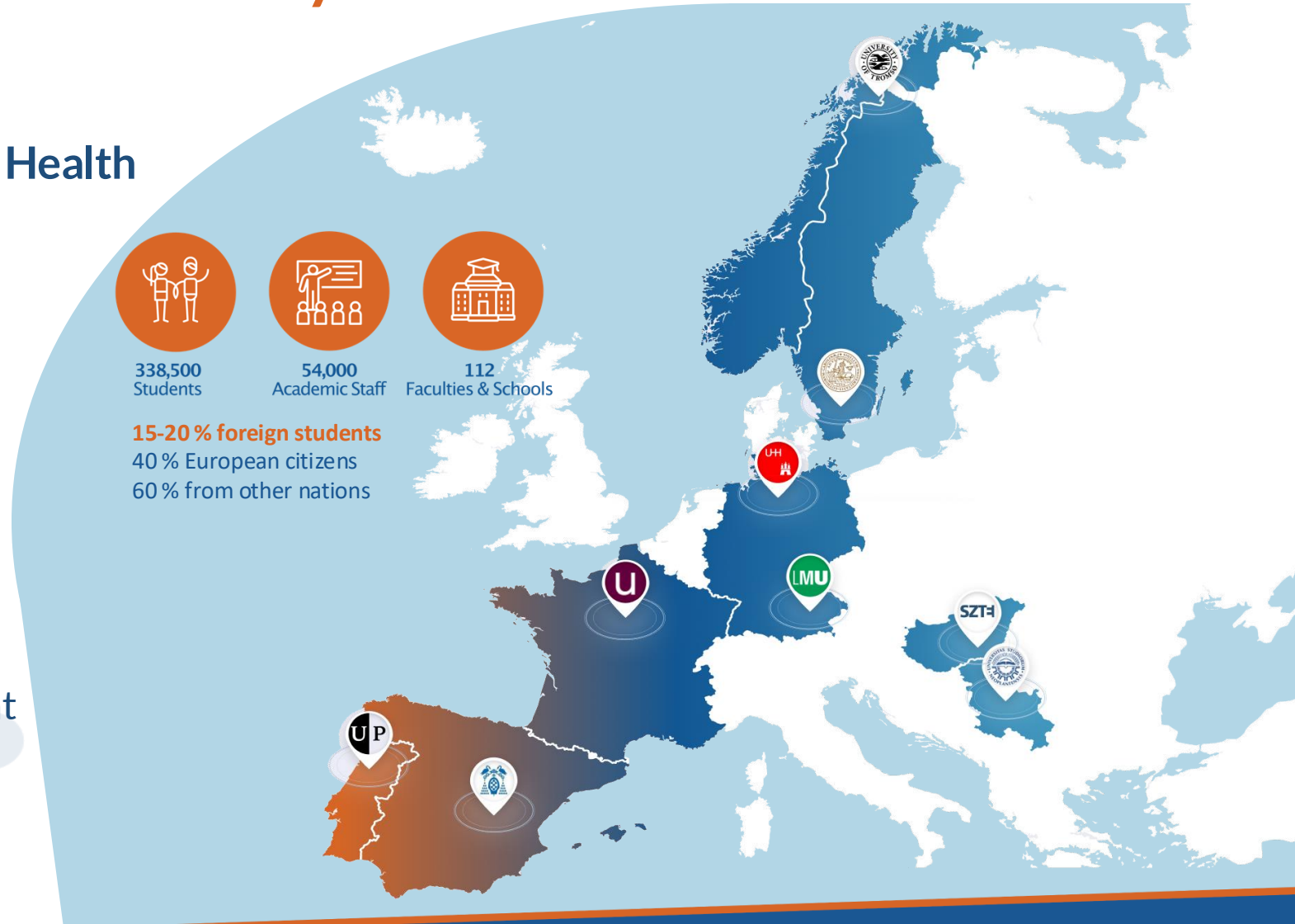# EUGLOH - The European University Alliance for Global Health

9 Universities, 1 Goal

Building Europe's Campus for Global Health

- Equipping students and staff with the skills needed to shape the future of global health

- Creating a **seamless, inclusive European campus** that enables **mobility**, joint learning opportunities, and **shared infrastructure**

- Addressing pressing health issues through interdisciplinary, co-created education, research and innovation that engages with social needs

338,500 Students

54,000 Academic Staff

112 Faculties & Schools

15-20 % foreign students
40 % European citizens
60 % from other nations

LMUcard + European Student Card (ESC)
LMU as an international university
International Partners and the European University Alliance

Strategic partnerships

- LMU-Bordeaux Research Cooperation Program
- Cambridge LMU Strategic Partnership
- LMU-China Academic Network (LMU-ChAN)
- LMU-NYU Research Cooperation Program
- LMU-TAU Research Cooperation Program
- LMU-Todai Cooperation in the Sciences
- LMU-UCB Research in the Humanities

Global collaborations

- LMU - China Scholarship Council (CSC) Program
- LMU-Harvard Young Scientists' Forum
- LMU's Latin America Network
- Venice International University

International alliances

- League of European Research Universities (LERU)
- European University Association (EUA)
- Europaeum

EU projects – The European University Alliances

European University Alliance for Global Health (EUGLOH)

Infinity partners → infinity stakeholders → infinity systems

A shared vision – seamless mobility

EUGLOH & the European Student Card have a shared vision

✓ **Seamless mobility**

✓ **Easy service access**

For:
✓ students,
✓ staff and
✓ professionals

EUGLOH ESC Working Group
formed end of 2020:

All EUGLOH universities should adopt ESC and define services to share (Lead Paris-Saclay).

2022 LMU took over the technical lead

But differ in the audience and baseline technical requirements → real **technical interoperability**

The European Student Card (2020)

Basic concepts

The European Student Card (ESC) is a new standard created by European Higher Education Institution (HEI) **to promote student mobility within Europe** (EHEA zone).

→ The long-term objective is **to give all European Students the same rights as a local student** when travelling abroad.

So, the idea is to **create a card that can be accepted anywhere within Europe**. This card **gives access to an unlimited number of services** that students use in their daily life, such as borrowing book from university library, accessing student cafeteria with discounted prices, accessing university premises, using public transportation etc.

Short- and long-term perspectives

The first basic service to be set up is **student status authentication**. This service offers the possibility for any organization (private business, public administration, association, HEI...) to confirm whether a card holder is a student or not. **This service is a necessity because student status authentication is usually a prerequisite to give access to other services that are restricted to students**.

- **Other services will become available afterward**, such as:
  - The possibility to use the card as an **electronic wallet** for day-to-day expenses
  - The possibility to write new information on the card after it has been delivered, granting access to a wide range of new services for the student
  - The possibility of using the card as a **key** to allow **exchange of data between HEIs**, to facilitate administrative procedures during student mobility
- **Dematerialisation of the card itself**, using a smartphone

→ Interoperability

Source: ESC Handbook for institution: Users's Guide to connect to the Platform
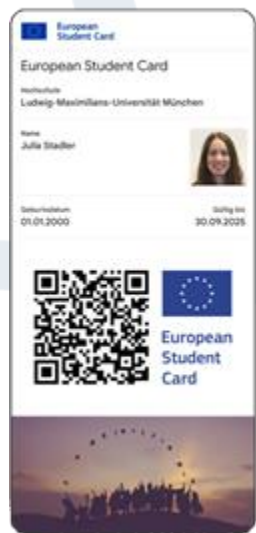(http://europeanstudentcard.eu/wp-content/uploads/2017/02/ESC-User-Guide-def.pdf)

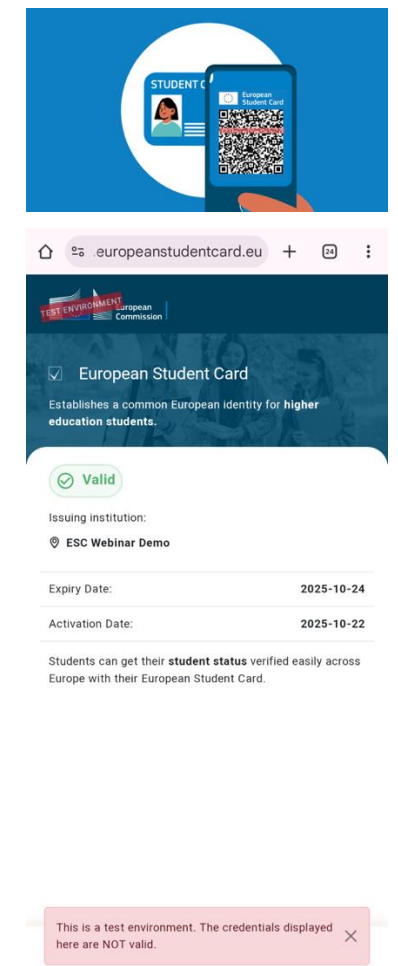# The European Student Card

Seamless access to physical and digital services
while on mobility, e.g. Library, Public Transport, Physical Access

One Credential to rule them all?

With a QR-Code or a verifiable credential?

→ not realistic

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

EUGLOH & ESC – a shared vision and ambitions

We have a shared vision: seamless mobility & easy service access

But an ESC QR-Code was no option for us (GDPR & IT-Security wise), the long-term perspective a digital smartphone pass looked fascinating

→ a great vision

EUGLOH wanted to share their services across the alliance, and beyond (as we all have more partners)

The IT-Persons from LMU, U.Porto and Lund already knew each other → we met at ECCA 2019
- ✓ **understand the technological possibilities**,
- ✓ knew and **understand** the topics, have access to major technology providers
- ✓ but also, the capabilities of the ESC Project team

→ *If we want a good and **interoperable solution** in the near future, we must come up with a working proposal*

→ *That meets our requirements and audience (students, staff and professionals)*

Campus Cards are about Accessing Services

Identification
- **Identification**
- **Status verification**
- **Proof of entitlement**
- Single Sign On / 2FA / FIDO2
- Attendance check
  - *Check-in for exams*
  - *attendance at courses*
  - *Time recording*
- Electronic Signature
  (*of legal documents*)

Electronic payment / cashless campus
- Canteen & cafeterias
- Vending machines
- Printing / scanning
  (*secure & follow me printing*)
- Ticketing
  (*events and conferences*)

Physical Access Control
- Areas (*campus, parking lot*)
- Buildings
- Rooms
  - Classrooms
  - Labs
  - Computer rooms
  - Learning spaces
  - Offices
  - Accommodation facilities (*i.e., dorms*)
- Athletic facilities

Library services
- Access to / borrow
  - Physical media (book, audio and video media)
  - E-media (book, audio and video media)
- Learning spaces

Transport
- On campus services
  (*university shuttle service*)
- Public transport tickets & discounts

Discount and promotions
- **Discounts**
  on cultural activities
  - Museums
  - theaters
  - cinemas
- Shops
- Restaurants

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

eID.AS

providing service → create benefits

Campus Cards from a User Experience Point of View

Campus Cards (Student IDs / Staff IDs / Affiliate IDs) function as:

- **Official** (visual) **Identity Documents** and for university branding

- Primary medium for **Service Access** on-site → **proximity use-cases**

- Service Domains:
  - On-Campus
    - **Identification** and attendance tracking (courses, internships, exams)
    - **Payment** (open loop or closed loop payment) and discounts eligibility
    - **Physical Access Control** (buildings, labs, dorms)
    - **Library Services**
    - on-campus & public **Transport** integration (regional semester ticket models)
  - Off-Campus (Museums, theaters, shops, restaurants, ...)
    - **Status-based Identification** for third-party services
    - **Eligibility Verification** (e.g., student status, age-based discounts)

Campus Cards are about Accessing Services

The Service Domains

- Payment / Cashless Campus,

- Physical Access Control ,

- Library services,

- Transport

are "**local**" services, which only needs to be solved on a local level

✓ Separate service passes can choose best fitting technology

✓ Services are provided to ALL persons (not only one role, e.g., students)

Educational role system (from eduPerson)

→ Student IDs / Staff IDs are **legally limited** to enrolled / employed members of a Higher Education Institution (HEI)

→ Dedicated service passes can be legally issued to not enrolled / employed persons ← Users of the service
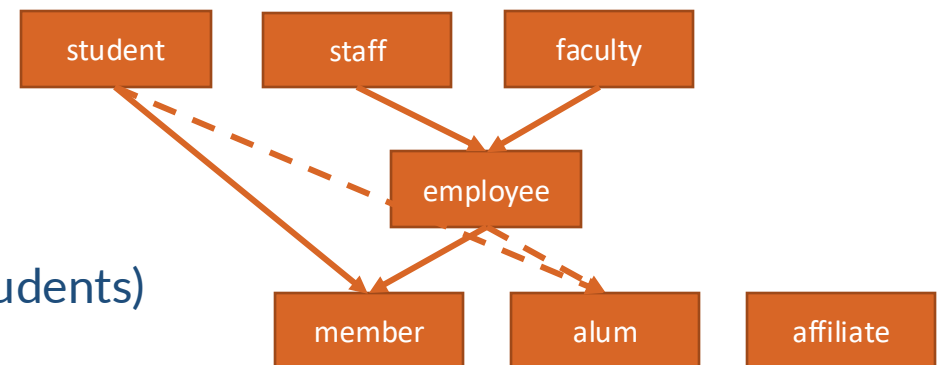
Key to all Services → Identification / Authentication

- Triple-A-System
  - (Identification)
  - # Authentication
  - **Authorization**
  - **Accounting**

- **On-site services access** is about proving your entitlements and identity

- "*something you know*" as an authentication method for on-site service access is not very efficient, best a combination of "*something we have*" + "*something we are*" → Smartphone Wallet passes + authentication via biometrics

- We already have a powerful IDM System for **online-services → Shibboleth → eduGAIN-AAI**

Authentication Factors

Something you KNOW
- Password
- PIN

Something you HAVE
- Chip card
- Token
- Smartphone

Something you ARE
- Biometrics

Trust level / Assurance Level

→ Very important for **IDENTIFICATION & AUTHENTICATION**
→ Quality of identity (personal) data
→ Type of authentication & consequences for identification medium

high

substantial / medium

normal

no trust

Authentication:
• username / email + password

Identity proofing:
→ self-asserted
→ verified e-mail address

Authentication
• certificate based
• FIDO2
• Smart ID

Identity proofing:
→ officially confirmed
→ manual check of a government issued photo-ID

Authentication
• eID.AS compliant
  → eID of EU Citizen IDs
  → provided by HEI for foreign Students

Identity proofing:
→ officially confirmed
→ Identity document automated and technically checked to be genuine and represent the claimed identity

DRY: do not re-invent the wheel

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

→ Digitalization Projects are complex enough,
  don't try to build everything from scratch

*If I have seen further it is by standing
on the shoulders of Giants.*

Source: "Sir Isaac Newton letter to Robert Hooke dated 5 February 1675"

Success factors – Understand the complexity

→ Complexity management and possibilities to act – Stacey Matrix & Cynefin-Framework

Left diagram (Stacey Matrix):
- Y-axis: What? Requirements / Stakeholders (from "clear" to "unclear")
- X-axis: Technology / Processes How (from "known" to "unknown")
- Regions: Clear, Complicated, Complex, Chaos

Right diagram (Cynefin Framework):

Complex	Complicated
Probe > Sense > Respond → Emergent Practice	Sense > Analyse > Respond → Good Practice
Chaos	Clear
Act > Sense > Respond → Novel Practice	Sense > Categorise > Respond → Best Practice

How to KISS: Keep it Simple, Stupid

Identification / Authentication for Service Access

- ✓ **Interoperability happens on the reader side** → contactless communication protocols are better than visual codes
- ✓ Almost all readers in the market could **read more than one standard** (*maybe a firmware upgrade necessary*)
- ✓ QR-Codes are not considered a secure identification element (especially with an URL as content)

→ It is all about User Experience

Think outside the card: Medium → Services

Identification	Electronic Payment / cashless campus	Physical Access Control	Library services	Transport	Discount and promotions

• Identification
• Status verification
• Proof of entitlement
• Single Sign On / 2FA / FIDO2
• Attendance check
  • *Check-in for exams*
  • *attendance at courses*
  • *Time recording*
• Electronic Signature
(of legal documents)
	Canteen & cafeterias
	Vending machines
	Printing / *(secure & fo...)*
	Ticketing *(secure & fo...)*
		Areas *(campus, parking lot)*
		Buildings
		Rooms
		Clearance
			Access to / borrow
			• Physical media (book,
			• E-media (book, audio and
				On campus services *(university shuttle service)*
				Special case of "Proof of entitlement"
				...port tickets
				...of "discount"
					• Discounts on cultural activities
					  • Museums
					  • theaters
					  • cinemas
					• Shops
					• Restaurants
					→ Special case of "Identification" / "Status verification" / "Proof of entitlement"

Separate Service Passes

- Local Services
- Each service is associated with a distinct pass
- Providers can choose appropriate technology per pass

→ Working solutions by solutions providers

eID.AS

A **Common ID** pass
for all HEIs
(ISO/IEC 18013-5 based)
→ **Identity Pass**

providing service → create benefits

Campus Cards are about Accessing Services

Almost all services are **SHARED** services

- ✓ University library ← Can be used by members of all universities in town / metropol area, in a university alliance or are open to the public

- ✓ Transport (semester ticket) ← Are just discounted and time limited public transport tickets (valid for 6 month)

- ✓ Canteens, cafés and vending machines on campus ← Can be used by all roles and members of all universities

- ✓ Physical Access Control (PAC) ← For all roles in a university / university alliance

Services are provided by **different** Service Providers (European universities are not business focused)

- ✓ Canteens, cafes and vending machines are operated by Student Affairs Unions

- ✓ Transport services are operated by local transport companies

- ✓ University Buildings (PAC) are university or state owned

→ Each Service Provider can issue their **own pass**, matching their needs and security requirements

Munich campus as an Example of SHARED Services

Most European Universities do not have a clearly demarcated campus area. They are just in the city.

The university is not even the main service provider for student life.

Typical Service-Providers:
- [Studierendenwerk München Oberbayern logo] (=Student Affair Union)
  - Canteen & cafeterias
  - Vending machines
  - Student housing / dorms
  → Responsible for all universities in Munich (LMU, TUM, HM, …)
- Libraries are dedicated (almost independent) units at LMU we have two libraries: University Library and
  [UB logo] [BSB Bayerische StaatsBibliothek — Information in erster Linie]
  Bavarian State Library
- Transport → Public Transport System
  [MVV logo]
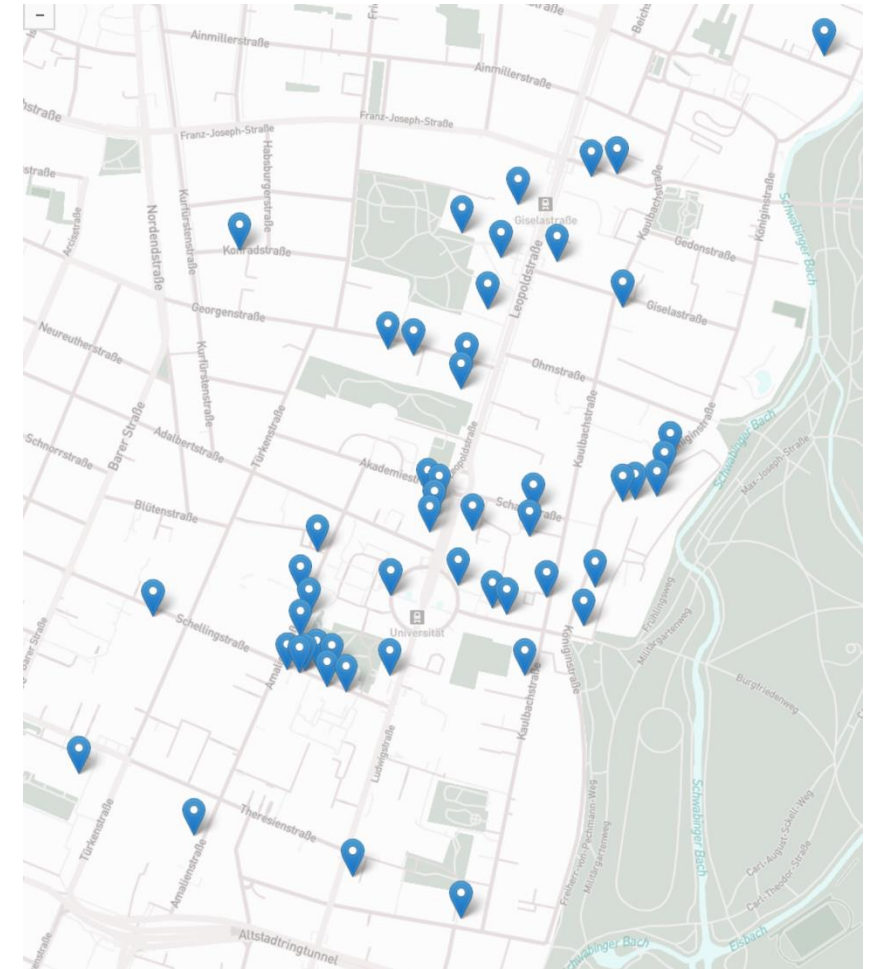
The LMU Student ID (over time)

LMU Student ID till 2019

→ transition →

LMUcard Student ID 2019-2025

→ transition →

today

LMU Student ID 2025+

→ transition →

LMU Student ID 2027+ ?

University Identity Student ID

eduTAP & eduTAP@LMU

Transition of credentials into the Smartphone Wallets
Examples: Active and potential IDs for LMU Munich

Google Wallet

Apple Wallet

→ all **NFC enabled**
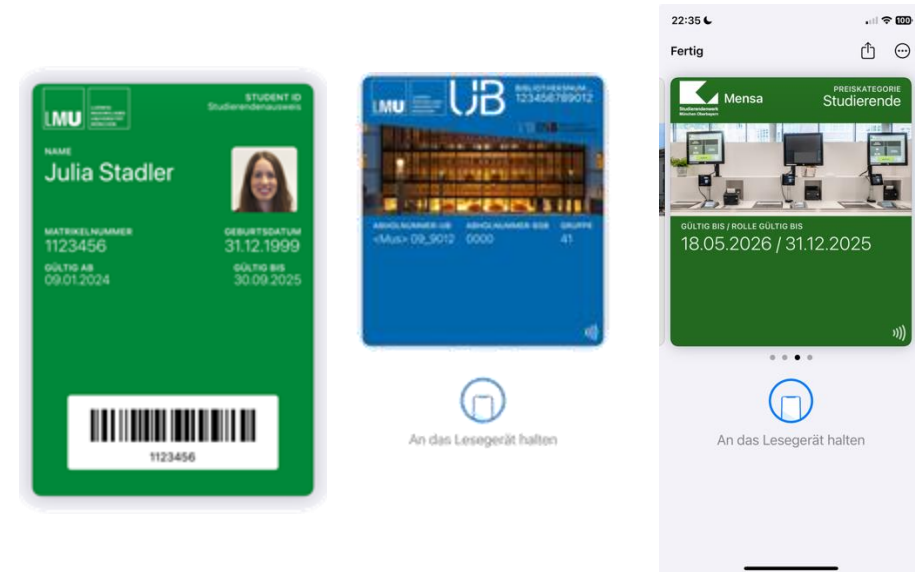
→ **NFC enabled** where possible
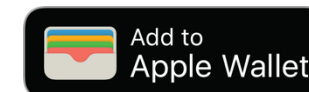
Transition of credentials into the Smartphone Wallets
Examples: LMU Munich Benutzerkonto – Pass Portal
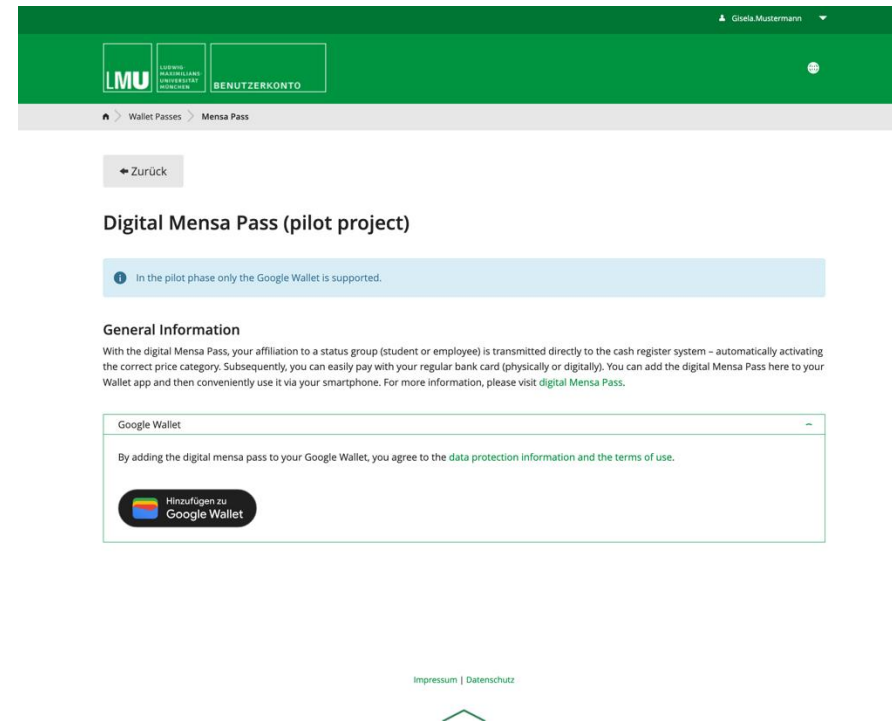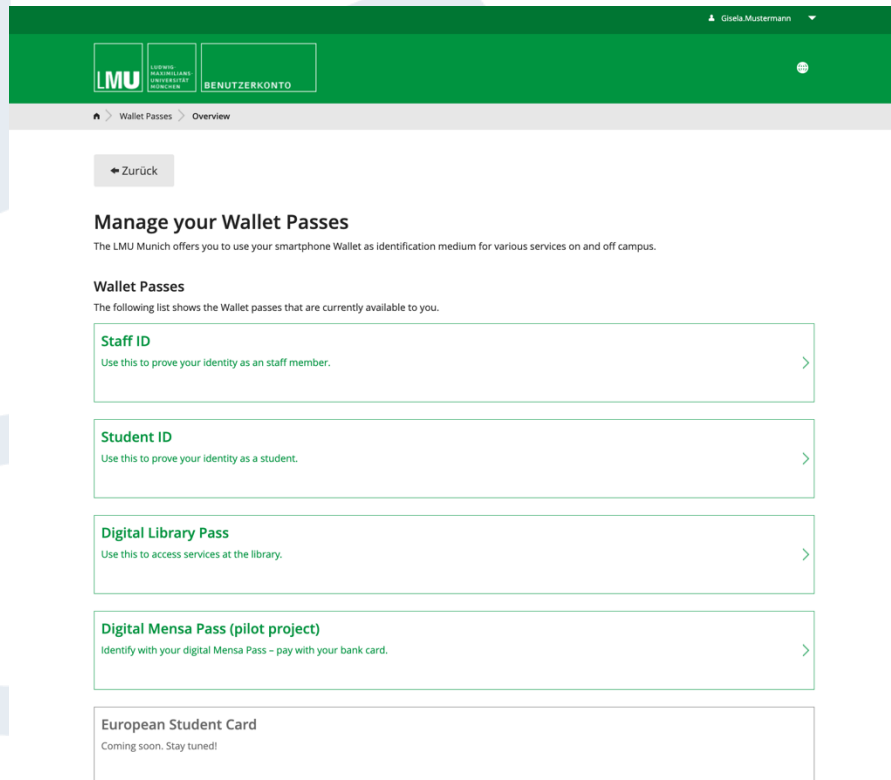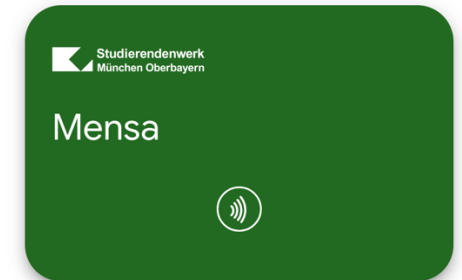
→ Plan to have all pass types online at LMU in the summer semester 2025 mostly design questions and information on the back are discussed

Transition of credentials into the Smartphone Wallets
LMU Student ID

The new **LMU Student ID** in the Wallet

- ✓ will come operational in summer semester 2025 (optional to LMUcard)

- ✓ for summer semester 2027 either physical LMUcard or wallet ID

Google   Apple   more wallets to come

Transition of credentials into the Smartphone Wallets
The European Student Card

The European Student Card (v1.1 new ESC Design)   (v1.5)
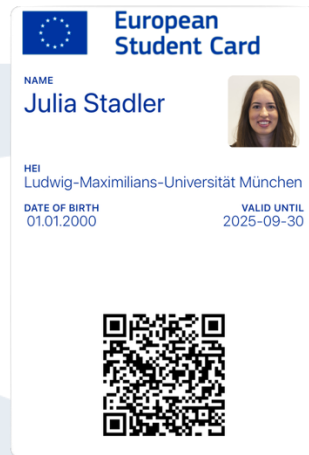
Google   Apple

- ✓ Discounts off-campus
- ✓ European dimension → Erasmus+ marketing
- ✓ Online status verification
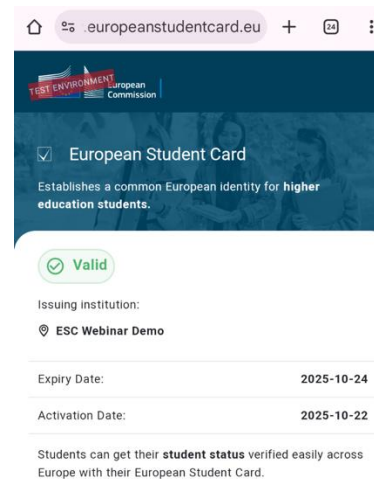
Transition of credentials into the Smartphone Wallets
Library ID

NFC enabled by default

Google

Apple

An das Lesegerät halten

Discount-Pass for Mensa
Studierendenwerk München Oberbayern

Eligibility verification for discounts with the Apple / Google Wallet via NFC, payment with an Open-Loop Bank / Credit-Card

Google Wallet
Since Feb. 2025
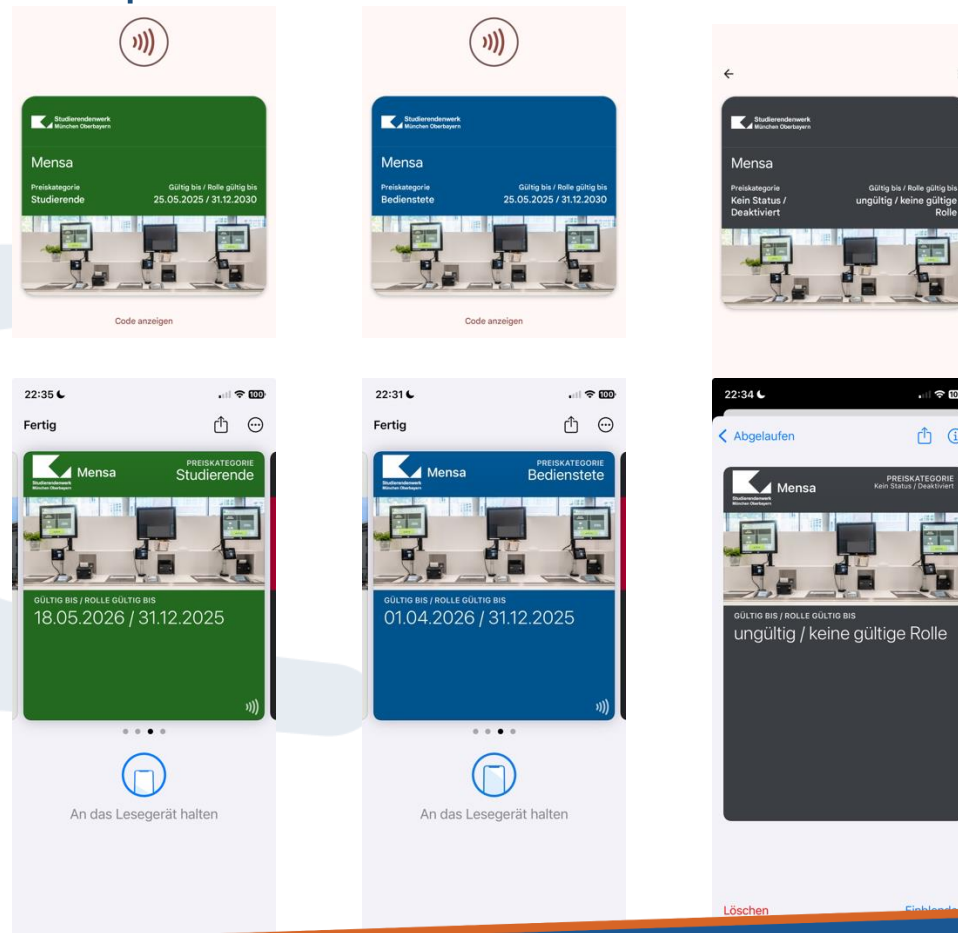
Apple Wallet

Discount-Pass for Mensa
Studierendenwerk München Oberbayern

Payment Process in the Mensa

Double Tap:

1. Eligibility verification of status group (Student, Employee, Guest)
   → Discount will be applied

2. Pay with an Open-Loop Bank / Credit-Card
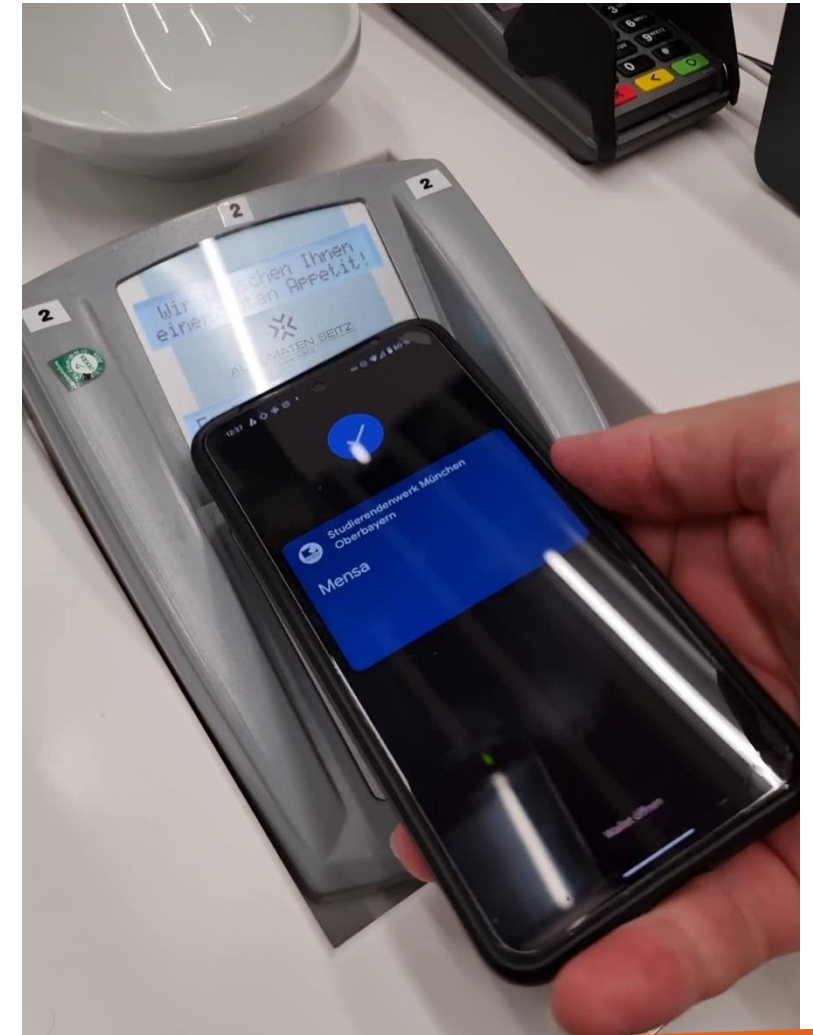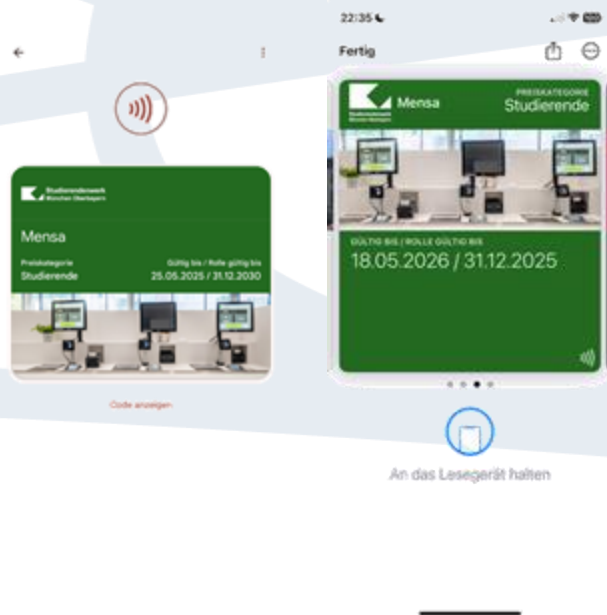
Transition of credentials into the Smartphone Wallets
Use Case: Physical Access Control (Access to learning spaces)

Physical access to the learning spaces (provided by the library)

LMUcard
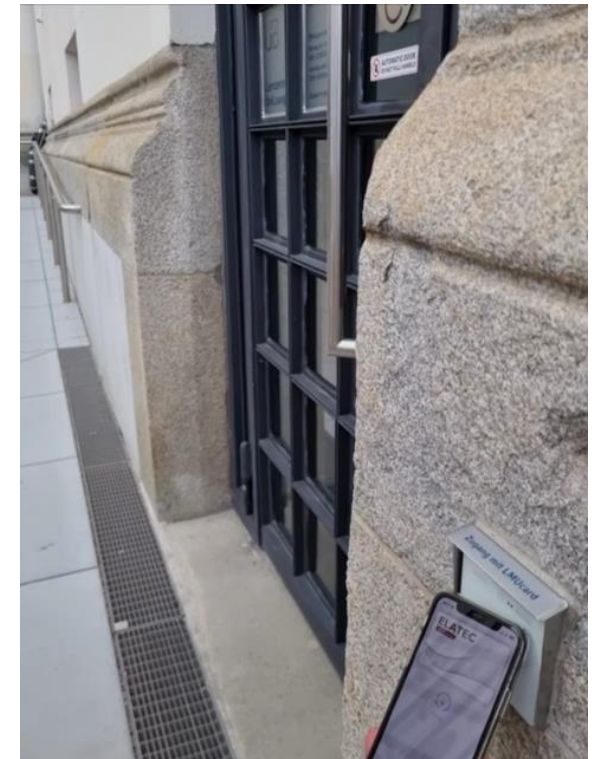
Google Smart Tap

Apple

Access

Apple / Google Wallet – Focus on User Experience
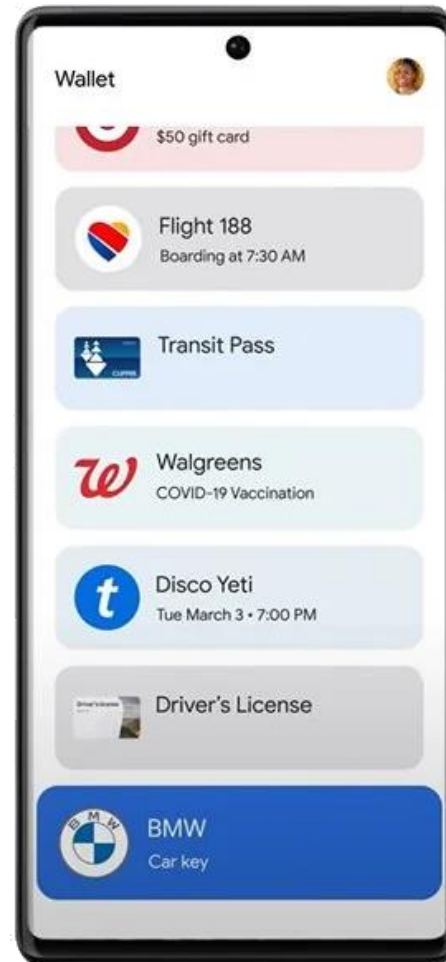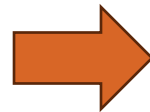
Campus Cards from a User Experience Point of View

User preferences for **Physical Wallets**:

✓ Less cards are better

✓ **Contactless** cards are better

Identity
Discounts
Access
Library
...

Integrated Campus Card

- Identity
- Discounts
- Access
- Library
- ...
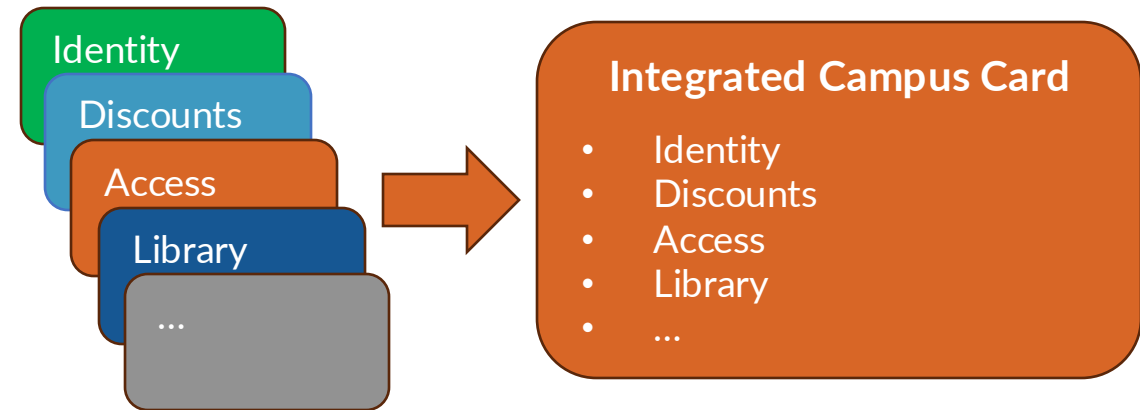
Example LMU 2015 – Transition from multiple cards into **ONE** integrated Campus Card

first name + surname

enrollment number

date of birth

photo

validity

library id
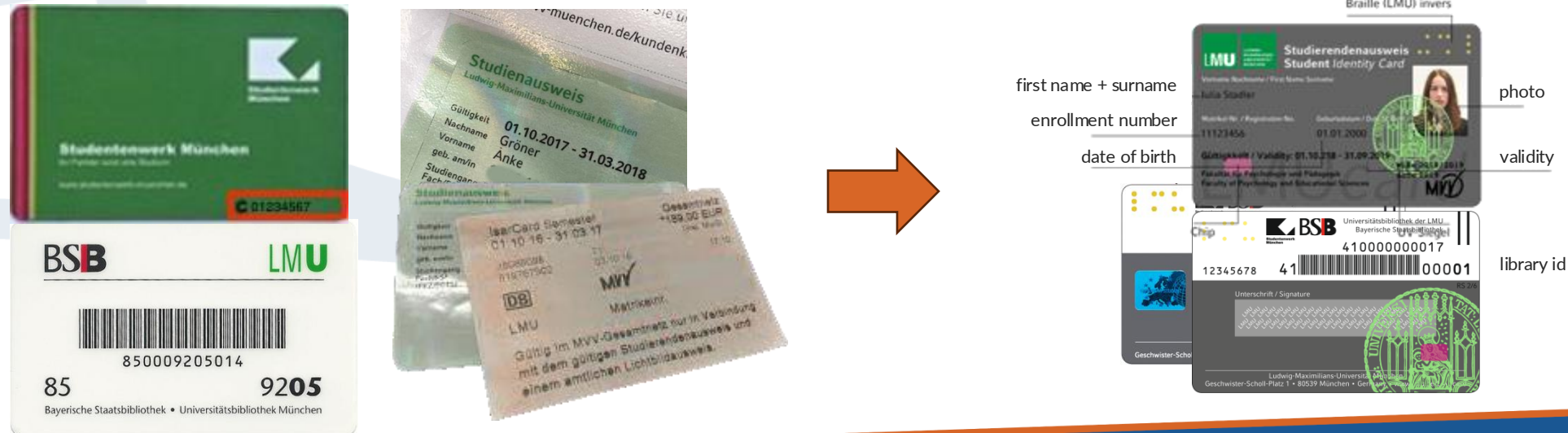
Campus Cards from a User Experience Point of View

User preferences for **Smartphone Wallets:**

✓ NFC / Contactless passes are better than scanning visual codes

✓ **One pass per service** is better

➤ User control over which services to use

➤ Auto-Presentment of pass needed

➤ Clear contextual communication
(additional information on pass
specific for the service,
specific branding of service)

Integrated Campus Card

- Identity
- Discounts
- Access
- Library
- ...

divide and conquer
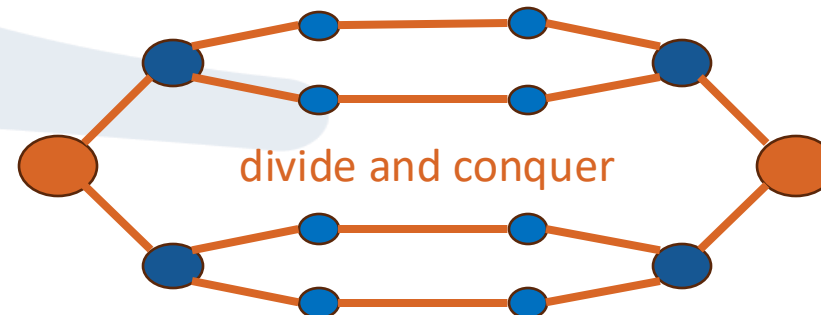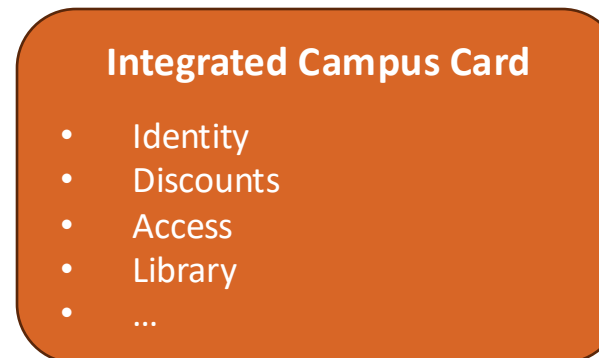
Digitizing cards **vs.** Leveraging the possibilities of smart devices → Stages of Digitalization – Period of Digital transformation

Digitalization 1.0

- Digitization – create digital versions of analog documents

→ Digitization vs. Digit**al**ization (machine readable content / payload)

Digitalization 2.0

- Digitalization with internal focus
- Optimize internal administrative processes – **organization centric optimizations**
- Processing of data

→ Digital transformation (a hard shift)

Digitalization 3.0

- Digitalization with focus on the user – **user centric optimizations**
- Optimization on how services are discovered and seamlessly used
- Flow of data

→ Service-oriented
→ **Digital identity**
→ Interoperability

→ User Experience

eduTAP – educational tapping

TAP TO PAY

tap to …

- ✓ identify yourself,
- ✓ verify your status,
- ✓ proof your entitlement,
- ✓ claim a discount,

tap to access a service on-site directly:

- ✓ tap to pay (open and close loop-payments),
- ✓ tap to open a door,
- ✓ tap to lend a book,
- ✓ tap to take a campus shuttle.

no app, just tap!

https://eduTAP.eu

eduTAP – educational tapping – What is eduTAP?

- eduTAP the concept
  - Splitting integrated campus cards into **dedicated service passes** and a **harmonized identity pass**
  - Leveraging the full potential of digital wallets
  - **Use existing**, secure and proven contactless **standards** – do not invent new standards

→ Focus on **User Experience** and **interoperability**

- eduTAP the software – to enable HEIs and Service Providers to:
  - create, issue, and manage passes within the smart device wallet
  - interact with wallet passes to give access to services, identify,
    and verify the status of students and staff members

→ **eduTAP** helps to fulfill the
great vision of the European Student Card
and enables interoperability and a better user experience

Services and Service Consumers

- ✓ It is all about **providing services → edu**TAP **is for anyone**
  - ✓ For users of the (home or host) institution
  - ✓ User incoming for a short-term or long-term mobility
- ✓ Staff / faculty members are more likely on short-term mobility than students
  → leading by example
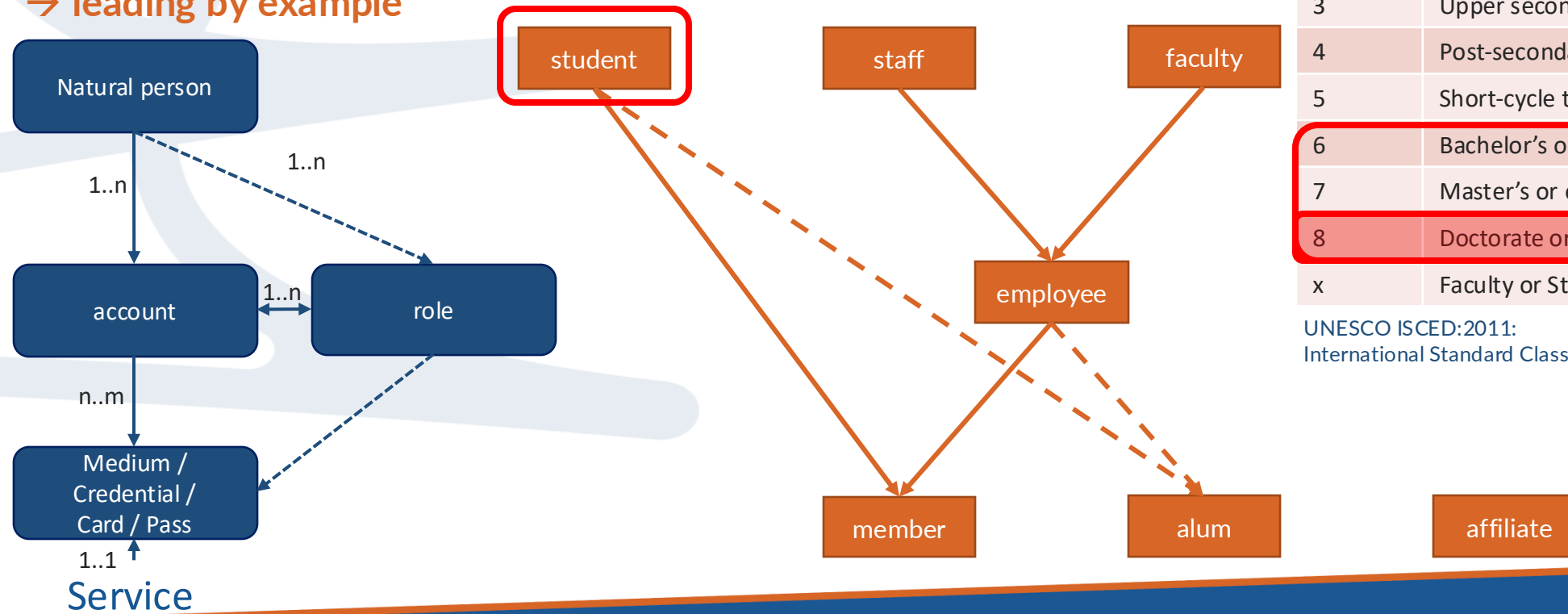
ISCED:2011 Level

Level	Label
0	Early childhood education
1	Primary education
2	Lower secondary education
3	Upper secondary education
4	Post-secondary non-tertiary education
5	Short-cycle tertiary education
6	Bachelor's or equivalent
7	Master's or equivalent
8	Doctorate or equivalent
x	Faculty or Staff member of HEI

UNESCO ISCED:2011:
International Standard Classification of Education

Natural person — account — role — Medium / Credential / Card / Pass — Service

student — staff — faculty — employee — member — alum — affiliate

1..n 1..n n..m 1..1

eduTAP – educational tapping – for the users

eduTAP passes enable using smart devices to perform transactions with a

simple tap

making everyday interactions **easier** and more secure both on campus and beyond.

→ User Experience

Our mission is to provide an **interoperable solution** that works for everyone
- for users of the (home or visiting) institution
- for user incoming for a short-term or long-term mobility
- staff / faculty members are more likely to be on short-term mobility than students

Technical details and features of Wallets / Passes

The wallet is a **container for multiple passes**

Technical features:

- **Auto-Presentment / Smart Select** ← **reader selects the specific pass to interact with** (if available)

- Selectable Authentication requirements ← **security features**

- Express-mode (Apple)

- Battery reserve (pass is still usable if phone has powered off; important for keys, transit tickets, payment)

- Groupable

- Validity dates

- Remote updateable / revokable

- Offline usable (→ non traceable)

- *Host Card Emulation possible*
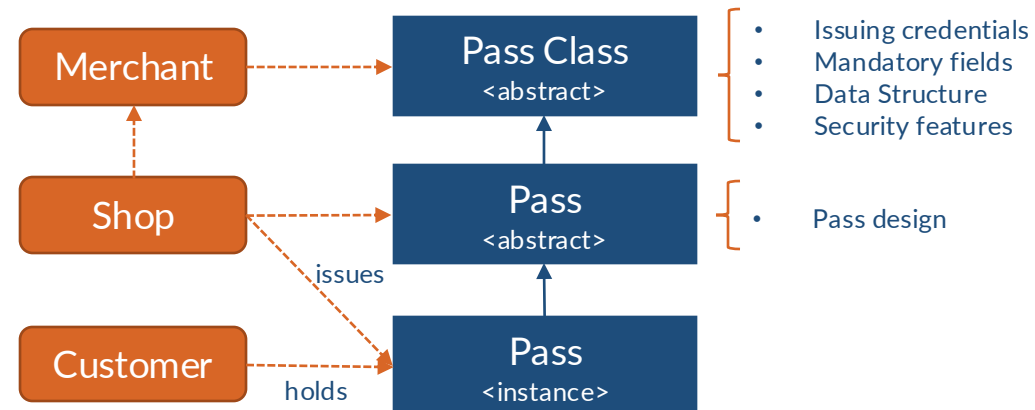
Technical details and features of Wallets / Passes

Auto-Presentment / Smart Select of an NFC enabled Pass in the Wallet
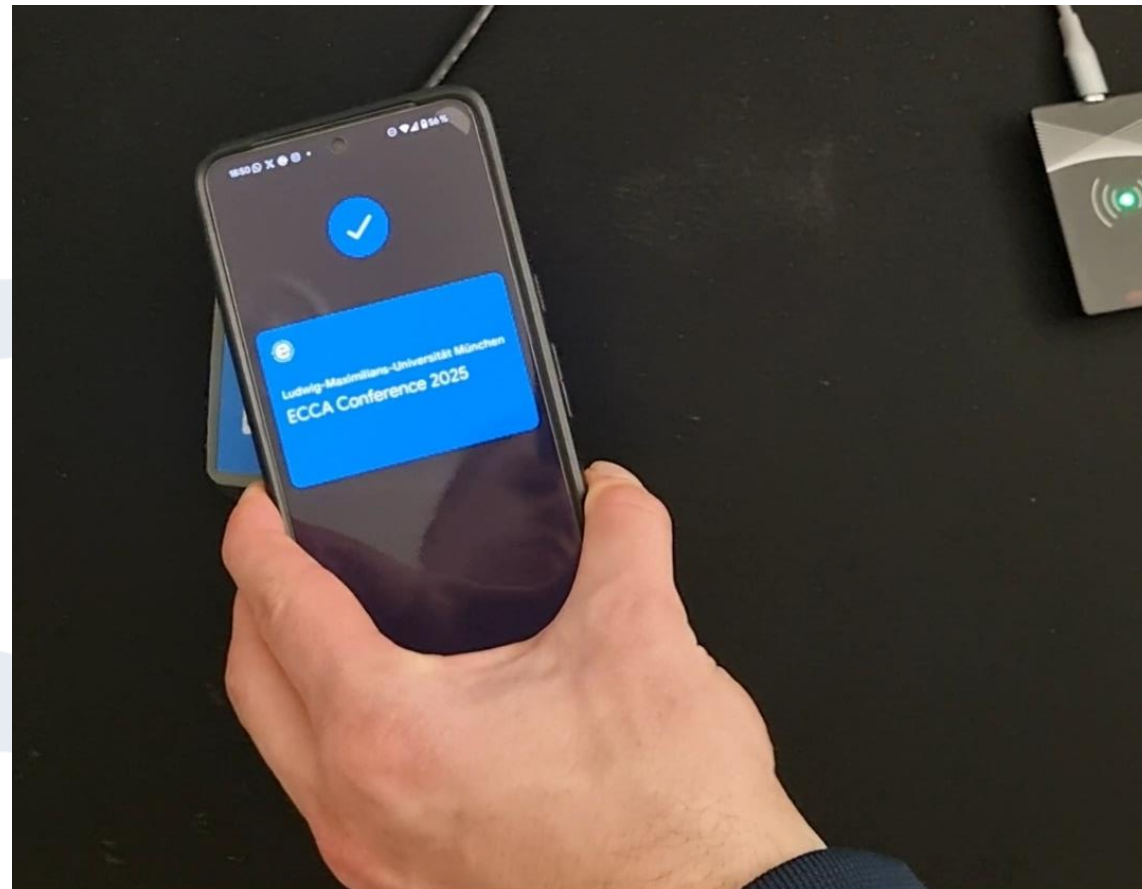
Technical details and features of Wallets / Passes

Battery Reserve Mode – Use the Wallet even if it's powered of

- for Keys (Dorm-Rooms, Class-Rooms, Building Access, Cars)
- for Payment
- for Transport Tickets

Up to 7 Days after shutdown of the smartphone

Technical details and features of Wallets / Passes

- ✓ Technical details and features of wallets / passes → Path to an **interoperable** campus card
- ✓ If each pass (technology) can be individually selected and leveraged, and the pass in the wallet can be selected by the reader (**Smart Select / Auto-Presentment**)

→ One pass per service

Pass
- Smart Select / Express Mode Selector
- Design – visual presentation
- Data-Slot → Smart Tap / VAS / Mifare / mDoc (ISO/INC 18013-5)

Wallet-App	Wallet-App	Wallet-App	Wallet-App
• Account-binding • Presentation • …			

Operating System Layer (OS) | **OS Wallet API**
- API for …

Hardware-Layer (access to)
- NFC / BLE / UWB
- Secure Element / Security Chip
- Subscriber Identity Module SIM/eSIM

Pass
→ Card bundle
- Visual design of a pass (images)
- Presentation data
- Data-structure

(OEM-specific default:
Google Smart Tap
Apple VAS / ECP 2.0)

low security level

Pass
→ Card bundle
- Visual design of a pass (images)
- Presentation data
- Host Card Emulation
  - Mifare DESFire
  - HID Seos
  - Legic NEON
  - …
- Data-structure in HCE

Technical details and features of Wallets / Passes

- For contact less communication is NFC the protocol
- Communication via ISO 14443
- Data Formats (File System access)
  - Google Smart Tap
  - Apple VAS (Value Added Services)
  - NFC ECP 2.0 (Enhanced Contactless Polling)
  - Host Card Emulation (HCE: of proprietary Protocols)
    - Mifare DESfire (via Mifare2GO / NXP secure element)
    - Legic NEON / Advant (via Legic Connect)
    - HID Seos
    - → Internal the Secure Module acts as a JCOP smart card
  - ISO 18013-5 Personal Identification
    → NFC handover to BLE or WiFi
    Core functionality in Android and iOS OS API
- Security consideration required by **use case**

Security Level
Chip / Smartcard

Security Level
Smartphone

high

high

Legic NEON   ISO 18013-5   ECP 2.0
Legic Advant
Mifare DESfire
HID Seos

Smart Tap

VAS

low

Mifare Classic /
Card UID

Technical details and features of Wallets / Passes

Detail view on the Wallet

Pass			
• Smart Select / Express Mode Selector • Design – visual presentation • Data-Slot → Smart Tap / VAS / Mifare / mDoc (ISO/INC 18013-5)			
Wallet-App • Account-binding • Presentation • …	**Wallet-App**	**Wallet-App**	**Wallet-App**
Operating System Layer (OS) • API for …	OS Wallet API		
Hardware-Layer (access to) • NFC / BLE / UWB • Secure Element / Security Chip • Subscriber Identity Module SIM/eSIM			

EU Digital Identity Wallet

EWC

OpenWallet FOUNDATION

Necessary to issue passes to **all relevant wallets**

→ The eduTAP solution is wallet **agnostic**, not bound to a specific wallet provider or company

→ eduTAP just enables HEI and Service Providers to easily **create** and **issue** wallet passes

Issuing process of wallet passes reedeming

→ important for redeeming on-device and cross-device scenarios

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

user / holder

Add to Google Wallet · Add to Apple Wallet · Add to SAMSUNG Wallet

Requests pass

Download of pass

Generates Download-Link

System of Credential Issuer

- IDM
- Website

generates
- Card Payload
- Card Bundle

API | HTTP JSON | API

OEM-Wallet Server

converts card payload / bundle into pass
Ensures security features

API | HTTP JSON

Credential issuer

OEM-Manufacturer Infrastructure

Device of credential holder

Service Provider (relying party)

→ User Experience

EUGLOH

European University Alliance for Global Health

eduTAP

https://eduTAP.eu

The Credential Management Platform in Detail

Credential Management Platform and eduTAP Components

→ Architecture of the delivery system
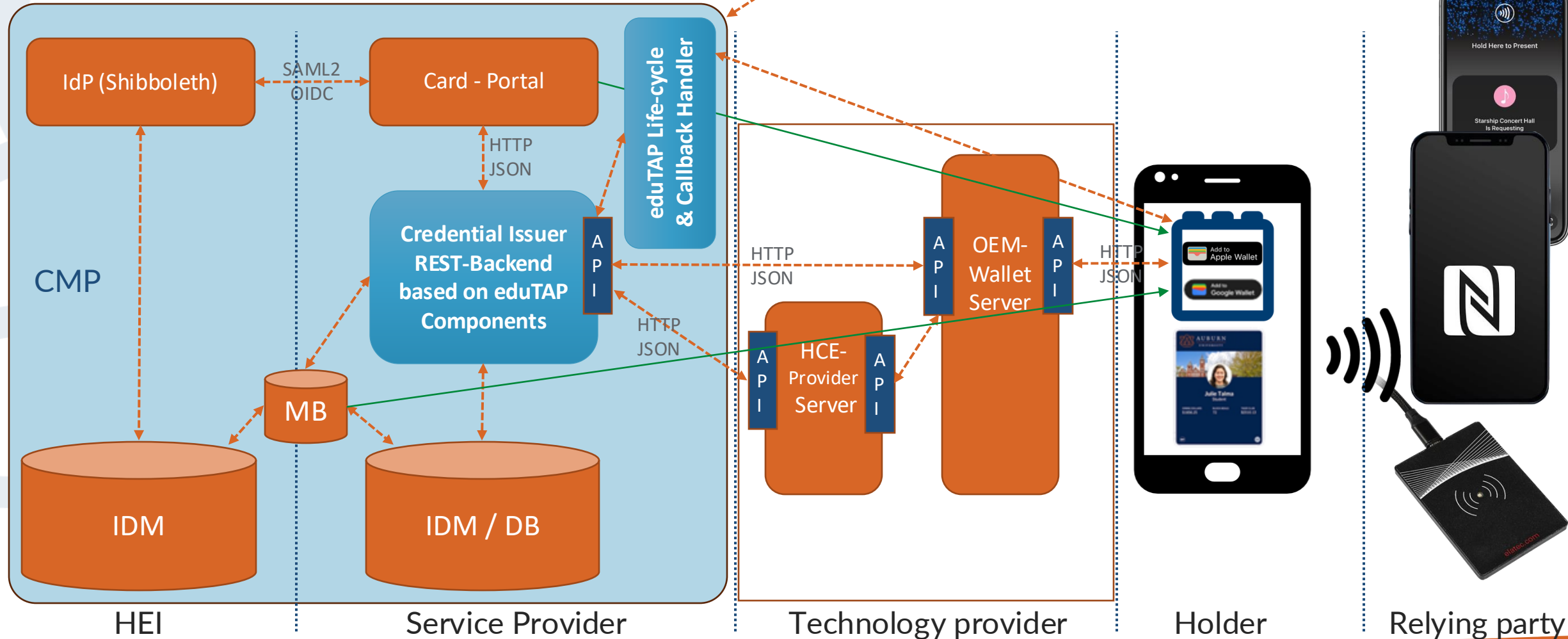
eduTAP Service Directory

HTTP JSON

IdP (Shibboleth) — SAML2 OIDC — **Card - Portal**

eduTAP Life-cycle & Callback Handler

HTTP JSON

CMP

Credential Issuer REST-Backend based on eduTAP Components — API

HTTP JSON

MB

HTTP JSON

API **HCE-Provider Server** API

API **OEM-Wallet Server** API

HTTP JSON

IDM

IDM / DB

Add to Apple Wallet

Add to Google Wallet

Hold Here to Present

Starship Concert Hall Is Requesting

HEI · Service Provider · Technology provider · Holder · Relying party

Credential Management Platform and eduTAP Components
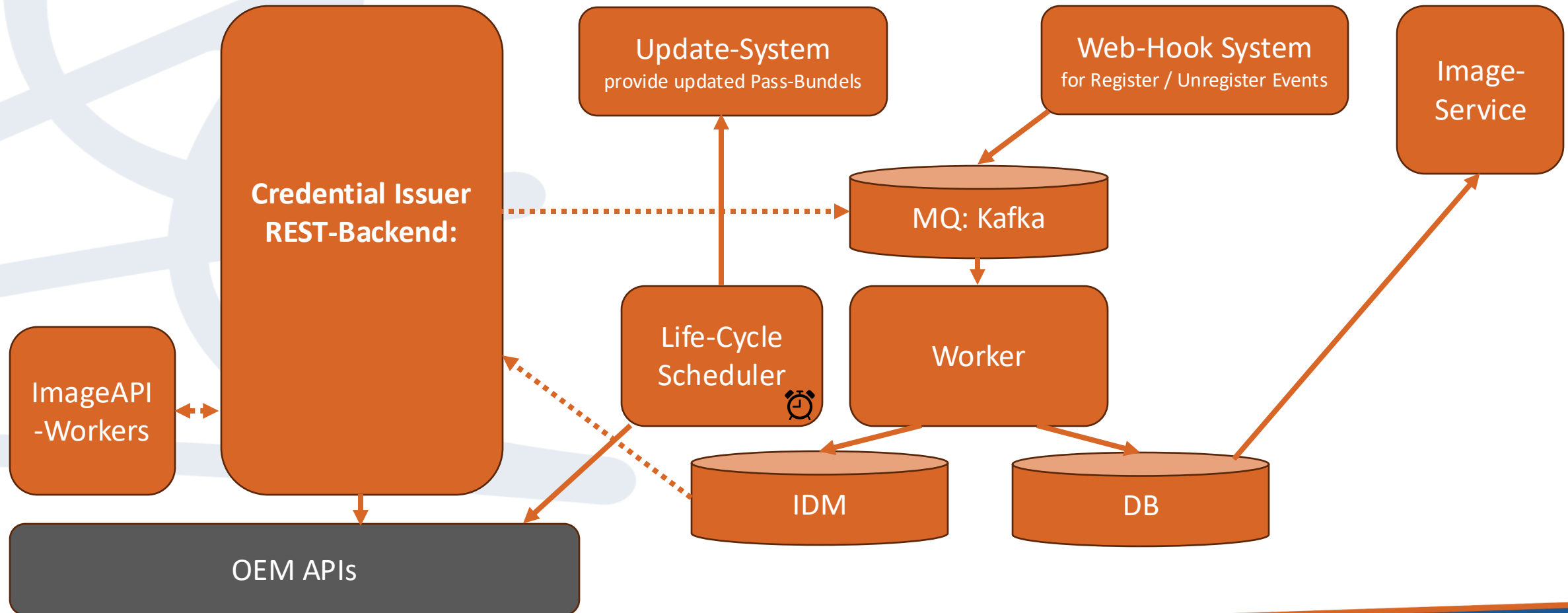
Credential Management Platform and eduTAP Components

→ eduTAP Components to the Frontend and to the Wallet APIs

Credential Issuer REST-Backend:

- To the Frontend
  - ✓ Authentication with SAML2 / OIDC / eIDAS
  - ✓ Identity-Linking with Apple, Google, Samsung, …
- To the Wallets
  - ✓ edutap.wallet_google
  - ✓ edutap.wallet_apple
  - ✓ edutap.wallet_Samsung
  - ✓ OID4VCI

Credential Management Platform and eduTAP Components

Example of a simplified API with hardening and model validation: edutap.wallet_google

API Functions

Most tasks are done by import and using the sole `api` module:

```
from edutap.wallet_google import api
```

To tell the API functions what kind of item to deal with, the first parameter is the registered name of the model (except for `save_link`). Models can be the different top-level wallet-classes or -objects, but also issuers, permissions and such (see section models below).

`create` (data)	Creates a Google Wallet items.
`read` (name, resource_id)	Reads a Google Wallet Class or Object.
`update` (data, *[, partial])	Updates a Google Wallet Class or Object.
`message` (name, resource_id, message)	Sends a message to a Google Wallet Class or Object.
`listing` (name, *[, resource_id, issuer_id, ...])	Lists wallet related resources.
`save_link` (models, *[, origins, iat, exp])	Creates a link to save a Google Wallet Object to the wallet on the device.

Credential Management Platform and eduTAP Components

eduTAP Components are opinionated Software (*a Reference Implementation of the eduTAP Concept*)

✓ Pydantic   for all Pass-Models

✓   HTTPX   for API connections

✓ FastAPI   for web-services

✓ Container based setup for deployment
✓ High SLA requirements, distributed, redundant, …

✓ Reuses Concepts from the Zope / Plone (but with the modern Python possibilities)

→ Adapters and Multi-Adapters: Protocol and EntryPoints

```
1.  @router_callback.post("/callback")
2.  async def handle_callback(request: Request, callback_data: CallbackData):
3.      """FastAPI handler for the callback endpoint.
4.
5.      It is called by Google Wallet API when a user interacts with a pass.
6.      The callback is triggered on save and delete of a pass in the wallet.
7.      """
8.      # get the registered callback handlers
9.      try:
10.         handlers = get_callback_handlers()
11.     except NotImplementedError:
12.         raise HTTPException(
13.             status_code=500, detail="No callback handlers were registered."
14.         )
15.
16.     # extract and verify message (given verification is not disabled)
17.     callback_message = await verified_signed_message(callback_data)
18.     logger.debug(f"Got message {callback_message}")
```

```
1.  @runtime_checkable
2.  class CallbackHandler(Protocol):
3.
4.      async def handle(
5.          self,
6.          class_id: str,
7.          object_id: str,
8.          event_type: str,
9.          exp_time_millis: int,
10.         count: int,
11.         nonce: str,
12.     ) -> None:
13.         """
14.         :param class_id: ClassId
15.         :param object_id: ObjectId
16.         :param event_type: EventType
17.         :param exp_time_millis: Expiration time in milliseconds
18.         :param count: count retries
19.         :param nonce: nonce UID
20.
21.         :raises: ValueError
22.         """
```

→ Configurable Persistence Layers

Credential Management Platform and eduTAP Components

eduTAP vs Credential Management Platforms build on top of eduTAP

eduTAP → works for large Universities (Developers and Skills are available)

- ✓ eduTAP is Community Open Source
- ✓ eduTAP is a set of libraries and example implementations
- ✓ eduTAP does provide a set of templates for Pass Designs and necessary legal and technical documentation
- ✓ eduTAP does not provide a Fronted or Pass-Designer

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

e.g. HEIDI (Heigher Education Institution Digital Identities) Platform is a CMP on-top of eduTAP-Components

- ✓ Provide Adapters to Business Applications (e.g. Campus-Management Systems, Library-Systems, …)
- ✓ Provides a Pass-Designer
- ✓ Provides a Management-UI

eduTAP

*A **sneak peek** into the future of Student IDs*
→ More interoperability and less passes by Verifiable Credentials
***eduTAP** Common ID*

eduTAP and the current Apple / Google Student IDs

How about the native, current **Student IDs** in Apple Wallet & Google Wallet (Mifare or HID based)?
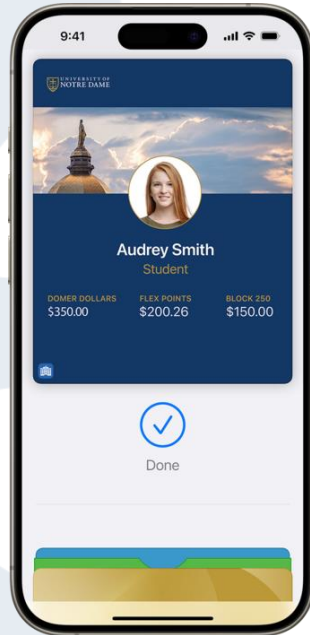
✓ Fantastic integrated cards (**one card** for all services, perfect for **corporate**)

✓ *Should be used for all university services* (Apple's intention)

→ University / organisation-centric optimization

→ Does not support the "seamless mobility" requirement

→ Shared services, how about other users than own students?

→ **LESS secure** (if following the ESC data zone approach)

→ Not the required User Experience, and does not meet the legal requirements

This is a dead-end solution, it will not help or bring benefit,
it actually provides a WORSE User Experience

It does NOT support **Selective Disclosure** and **Zero Knowledge Proof**

Apple and Google is aware of this and working on it!

Apple and Google Access Platform are good for PAC and Payment passes
→ NOT for Student or Staff IDs
→ GOOD dedicated service passes

Wallet Passes are about a great User Experience

A **great User Experience** is key to adoption and usage

✓ Non-NFC Passes are **NO GOOD** User Experience

✓ Unnecessary passes should be avoided ← NO dedicated pass for
simple eligibility verification (status, institution affiliation)

Is there a better solution?

transition

University Identity
Student ID
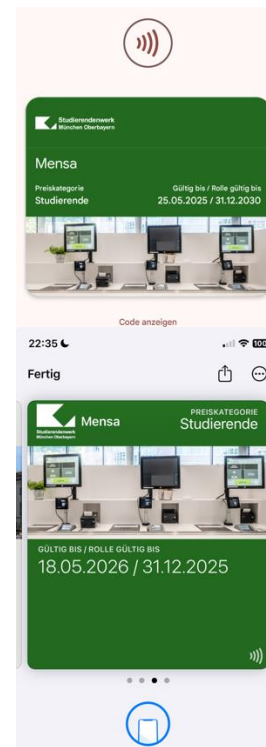
✓ **Verifiable Credentials**

✓ **Selective Disclosure**

✓ **Zero Knowledge Proofs**

Think outside the card: Medium → Services

Identification	Electronic Payment / cashless campus	Physical Access Control	Library services	Transport	Discount and promotions

• Identification
• Status verification
• Proof of entitlement
• Single Sign On / 2FA / FIDO2
• Attendance check
  • *Check-in for exams*
  • *attendance at courses*
  • *Time recording*
• Electronic Signature
(of legal documents)
	Canteen & cafeterias
	vending machines
	Printing / *(secure & fo*
	Ticketing *(secure & fo*
		Areas *(campus, parking lot)*
		Buildings
		Rooms
			Access to / borrow
			• Physical media (book,
			• E-media (book, audio and
				On campus services *(university shuttle service)*
				special case of "Proof of entitlement"
				port tickets
				of "discount"
					• Discounts on cultural activities
					  • Museums
					  • theaters
					  • cinemas
					• Shops
					• Restaurants
					→ Special case of "Identification" / "Status verification" / "Proof of entitlement"

Separate Service Passes

- Local Services
- Each service is associated with a distinct pass
- Providers can choose appropriate technology per pass

→ Working solutions by solutions providers

A **Common ID** Pass
for all HEIs
(ISO/IEC 18013-5 based)
→ **Identity Pass**

eID.AS

providing service → create benefits

Service Domains: Identity and Discount

From a legal point of view, Identity Documents of public universities are **official state photo IDs**

- ✓ Legal requirements
- ✓ Security considerations
- ✓ High assurance level

→ **International standards** for HEI Identities → eduGAIN (incl. eduPerson, SCHAC) e.g. European Student Identifier → routable information for course participation at other institutions (during mobility programmes)

Identity Documents (Student ID, Staff ID and Affiliate IDs) are used

On-Site (proximity use-cases)   Online

On-Campus

- ✓ Attendance at courses
- ✓ Check-in for exams
- ✓ Time recording
- ✓ Discounts in canteen & cafeterias
- ✓ Identification for university authorities (Student legal office and examination offices, campus security)

Off-Campus

- ✓ Identification for public authorities (e.g., police)
- ✓ Identification for third party (e.g., checkin at hostels)
- ✓ Eligibility verification for discounts and access (e.g., role-based, age-based, institution related)

- ✓ As authentification factor

A question of scale: Student IDs

European Union

- ~ **5,000** Higher Education Institutions (HEIs)
- ~ **18,800,000+** tertiary students (2022)

→ Organized in
National Research and Education Networks (NRENs)

Erasmus+ Countries

- Includes EU + Iceland, Liechtenstein, Norway, North Macedonia, Serbia, Turkey
- Significantly expands the European higher education landscape → ~ **20,000,000+** tertiary students

Worldwide

- ~ **18,000** recognized HEIs across 180+ countries
- ~ **200,000,000+** tertiary students globally

→ It should work everywhere: seamless mobility & easy service access

→ a GLOBAL Student ID ←

GÉANT – The IT provider for Higher Education in Europe

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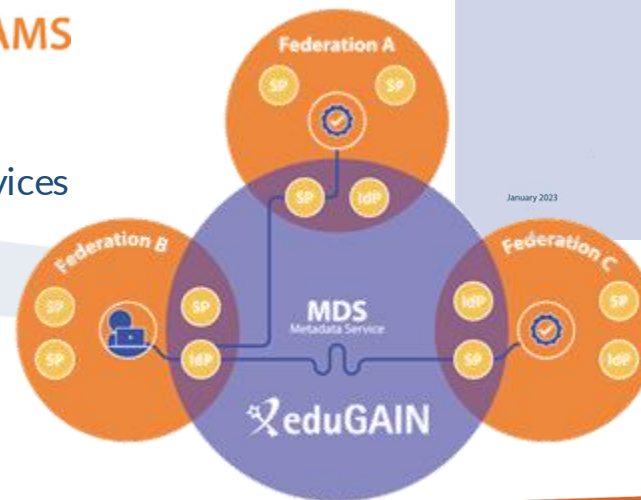
→ eduTAP is a perfect fit for
GÉANT Trust & Identity Services

Identity Pass: Reuse Shibboleth / eduGAIN data schema:
The common authentication method in the educational sector

✓ Shibboleth – local or in federation (national or multi-national) → eduGAIN-AAI → SAML2 or OIDC

Verifiable Credential for HEIs (Prototypes)

European Student Card as Verifiable Credential

DC4EU non-foundational Ids

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

Digital Identity in the Wallet

Common Verifiable Credential Formats / Protocols for Digital Identities

- SD JWT (EU)

- ISO/IEC 18013-5 (mDL)

- W3C Verifiable Credential Data Model

Issuing and Redemption Protocols

- OID4VC (OID4VCI and OID4VP)

- ISO/IEC 18013-5

For **proximity** use-cases **NFC / BLE transmission** is crucial

→ Our choice ISO/IEC 18013-5 (mDL) for Wallet credentials   DC4EU → SD JWT

Image Source: https://www.linkedin.com/feed/update/urn:li:activity:7333379048112361472/

A Common Identity Pass using the ISO/IEC 18013-5 model

- The "ISO/IEC 18013-5 Personal Identification" model is designed to support
  - A protocol for two devices to establish a secure wireless communication channel and exchange structured request and response message
  - **Identification** of the credential holder (user binding)
  - Selective release of data elements by the credential holder (data minimization / consent)
  - **Pre-consent** mechanism for frequently repeated processes (e.g., discount payment at Student Affairs Unions)
  - A protocol to retrieve credential data directly from the mobile device of the holder, purely offline, facilitating availability and non-traceability
  - An optional protocol to retrieve additional data from the issuing authority
  - A mechanism to establish **integrity** and **authenticity** of the credential data
  - A mechanism to confirm device binding (signing at transaction time)
  - Multi-document and multi namespace aware ← extendable for other use cases

- **Established governmental credential format that is already in use ← Following the ARF of EUDI-Wallet**
  → mobile driving licence / eu.europa.ec.eudiw.pid.1 (prototype of national eIDs in Europa)

- **Already supported** by the OEM-Smartphone-Manufactures (Apple and Google)
  → see: https://android-developers.googleblog.com/2020/11/privacy-preserving-features-in-mobile.html

EU Digital Identity Wallet

Identity Pass: ISO/IEC 18013-5 Data model
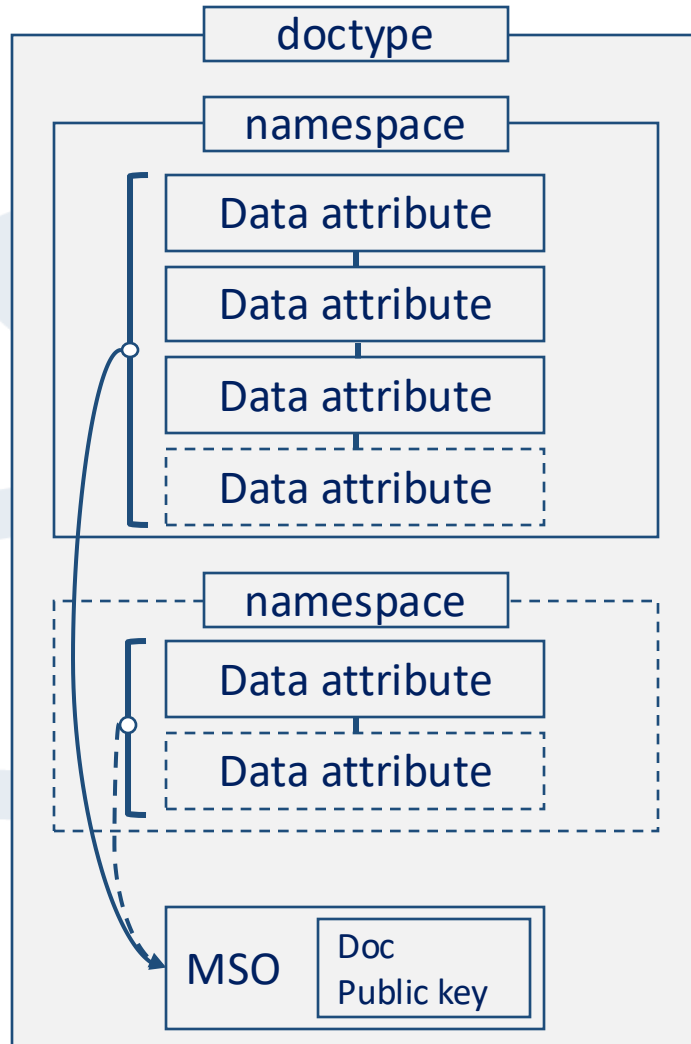
Reuse of directory data (common eduGAIN attributes)

- portrait (photo, *mandatory for identification documents*)
- givenNames
- sn (surname)
- email
- eduPersonAffiliation / eduPersonScopedAffiliation
- eduPersonEntitlement
- eduPersonAssurance
- schacHomeOrganization
- schacPersonalUniqueCode → European Student Identifier (ESI) - MyAcademicID
- schacDateOfBirth
- schacYearOfBirth
- schacPlaceOfBirth
- schacExpiryDate
- …

see also DC4EU education ID
(https://code.europa.eu/ebsi/json-schema/-/tree/main/schemas/vcdm1.1/education/verifiable-education-id)

works like a Shibboleth authentication on-site → trained processes

Diagram (left):
- doctype
  - namespace
    - Data attribute
    - Data attribute
    - Data attribute
    - Data attribute
  - namespace
    - Data attribute
    - Data attribute
  - MSO — Doc Public key

Identity Pass: Path to the best User Experience and Interoperability

Current Status Apple:

Identity Documents are required (photo ID, sensitive personal data) → Options in Apple Wallet

- ✓ Apple VAS Pass (Generic) with visual codes (e.g. QR-Code) **no NFC**
- ✓ Apple VAS Pass Passes (Generic) with NFC (currently not allowed)
- ✓ Student ID (Mifare DESFire) ← for inter-university usage **unencrypted** (not secure)
- ✓ **Identity Passes** (currently not allowed)

Not optimal
As possible data formats:
- • Plain text / JSON
- • Encrypted JWT or similar
- • Verifiable presentation not possible

→ All not optimal for GDPR

Optimal Solution: a Verifiable Credential / ISO 18013-5

- ✓ Works offline and untraceable
- ✓ All relevant data for identification and status verification
- ✓ **Interoperable** for identification and simple service access for inter-university usage
- ✓ A potential global solution
- ✓ Already implemented in Apple and Google Wallet
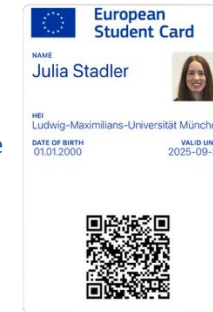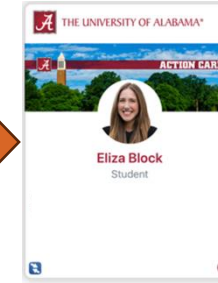
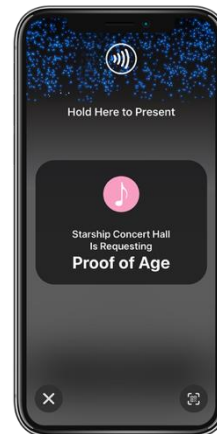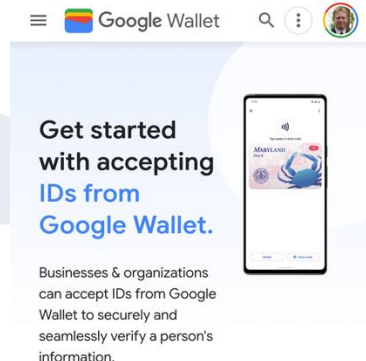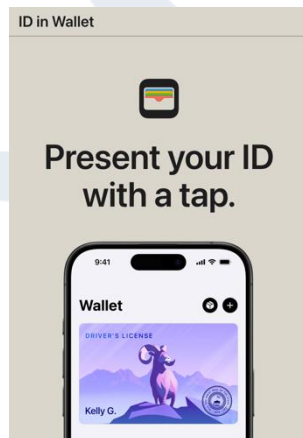
Phase 1
QR-Code
ESC

Phase 2
Apple Access Student ID with only
one Mifare AID unencrypted →
encrypted, signed JWT as payload
eduTAP simple ID

Long-term goal
Verifiable Credential
based on ISO 18013-5

→ Defined in ARF for European Digital Identity Wallet (EUDI-Wallet)

EU Digital Identity Wallet

→ **Identity passes would be the best solution for Student IDs, Staff IDs and Affiliate IDs**

Identity Pass: Path to the best User Experience and Interoperability

Current Status Google:

Identity Documents are required (photo ID, sensitive personal data) → Options in Google Wallet

✓ Google Smart Tap Passes (GenericObject) with visual codes(e.g. QR-Code) or NFC

✓ Google Smart Tap Passes (GenericPrivateObject) with NFC (no Image)

✓ Student ID (Mifare DESFire) ← for inter-university usage **unencrypted** (not secure)

✓ **Identity Passes** (currently not allowed)

Not optimal
As possible data formats:
- Plain text / JSON
- Encrypted JWT or similar
- Verifiable presentation not possible

→ All not optimal for GDPR

Optimal Solution: a Verifiable Credential / ISO 18013-5

✓ Works offline and untraceable

✓ All relevant data for identification and status verification

✓ **Interoperable** for identification and simple service access for inter-university usage

✓ A potential global solution

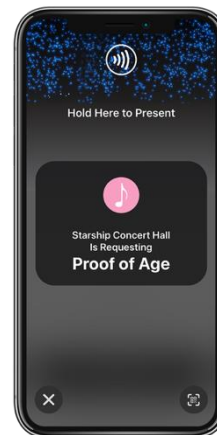✓ Already implemented in Apple and Google Wallet

Phase 1
QR-Code
ESC

Phase 2
NFC JWT
eduTAP simple ID

Long-term goal
Verifiable Credential
based on ISO 18013-5
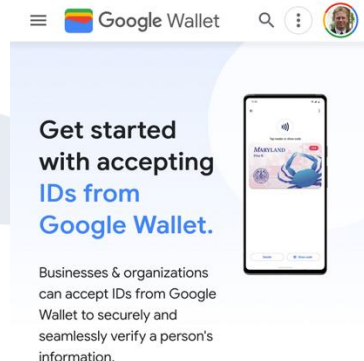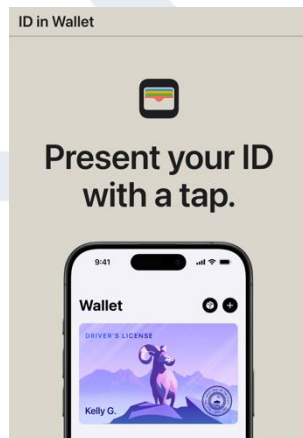
→ Defined in ARF for European Digital Identity Wallet (EUDI-Wallet)

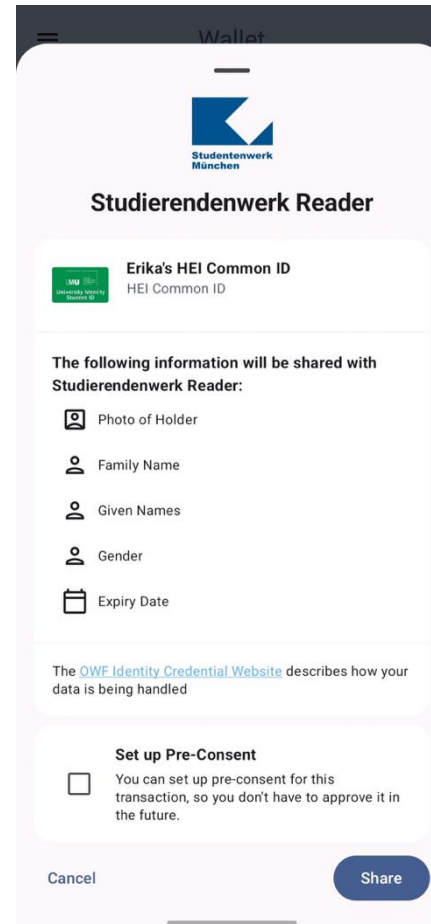**EU Digital Identity Wallet**

→ Identity passes would be the best solution for Student IDs, Staff IDs and Affiliate IDs

Identity Pass: Path to the best User Experience and Interoperability
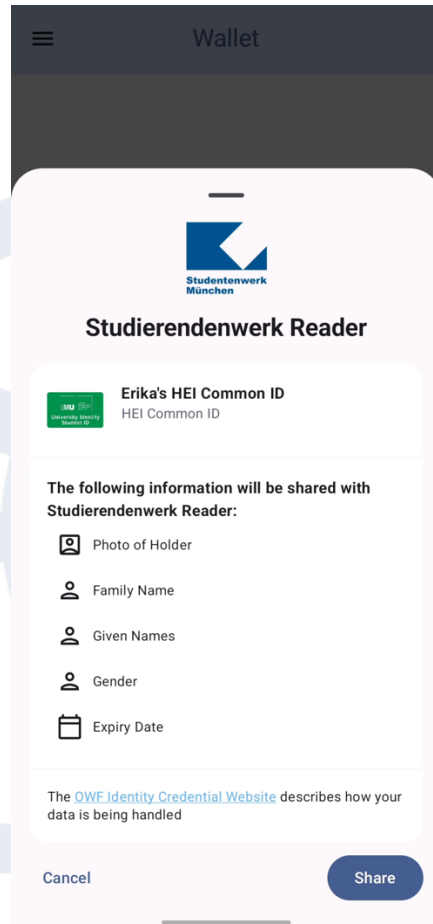
Informed Consent

Informed Consent
+ Pre-Consent
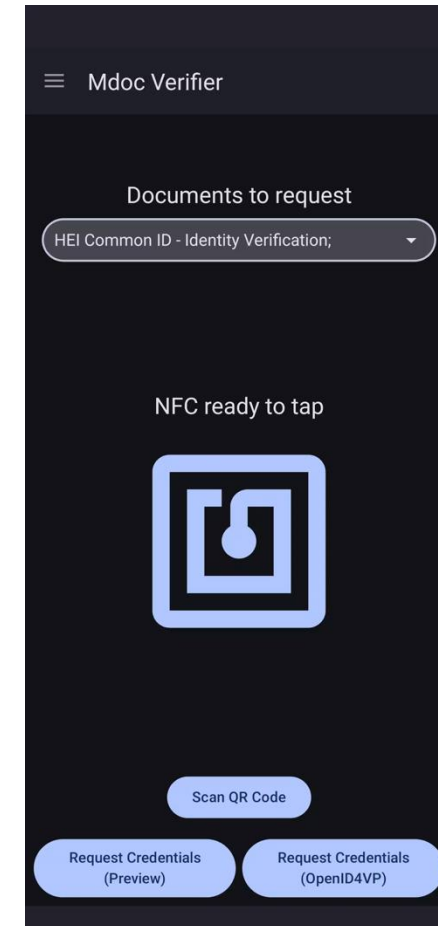
Verifier App

Campus Cards – Point of Views

Technology Experts vs. Consumers (Students, staff and professionals)
The Technology and issuing processes are not important to the consumers (card / pass holders)

The IDs and service passes should:

- ✓ **just work**
- ✓ be immediately available when needed
- ✓ be secure & GDPR compliant
- ✓ trustworthy
- ✓ **accepted everywhere**
- ✓ *be boring – no need for attention*

Students, teachers and researches should be able to focus on the important things,

→ their studies and research

→ enjoy student mobility (and do not need to wait weeks for a physical campus card)

"Boring" is a good thing

Every company gets about three innovation tokens.

Source: Dan McKinley, "Choose Boring Technology"
http://mcfunley.com/choose-boring-technology

"Boring" let you get things done

Same is true for people, if you **need to think** to get something done it costs effort, and energy for other more important things
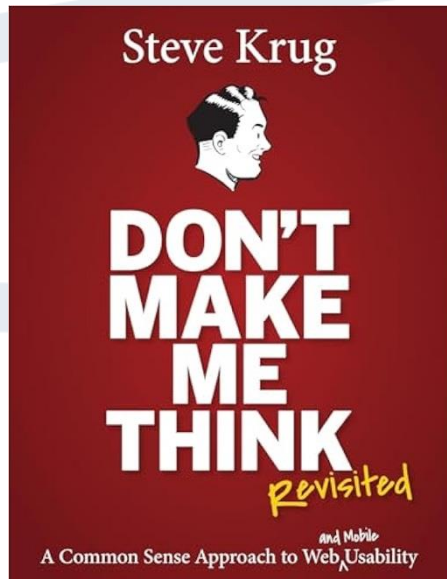
Don't make me Think

→ User Experience is important

You should **NOT** need to care about "boring" and "un-important" stuff

You should be able to
focus on the important things
(*studying, learning, researching, …*)

eduTAP

https://eduTAP.eu

*Modern Campus ID (Student ID / Staff ID)
for universities in Europe & the world*

Demo → Download an eduTAP created pass

https://demo.edutap.eu/

eduTAP – educational tapping

tap to ...

- ✓ identify yourself,
- ✓ verify your status,
- ✓ proof your entitlement,
- ✓ claim a discount,

tap to access a service on-site directly:

- ✓ tap to pay (open and close loop-payments),
- ✓ tap to open a door,
- ✓ tap to lend a book,
- ✓ tap to take a campus shuttle.

TAP TO PAY

no app, just tap!

https://eduTAP.eu

eduTAP – educational tapping – What is eduTAP?

- eduTAP the concept
  - Splitting integrated campus cards into **dedicated service passes** and a **harmonized identity pass**
  - Leveraging the full potential of digital wallets
  - **Use existing**, secure and proven contactless **standards** – do not invent new standards

  → Focus on **User Experience** and **interoperability**

- eduTAP the software – to enable HEIs and Service Providers to:
  - create, issue, and manage passes within the smart device wallet
  - interact with wallet passes to give access to services, identify,
    and verify the status of students and staff members

  → **eduTAP** helps to fulfill the
  great vision of the European Student Card
  and enables interoperability and a better user experience

We'd love to hear from you!

Get in touch:

eduTAP Project (https://eduTAP.eu/)

- Alexander Loechel (LMU Munich)
- Simon Lund (LMU Munich)
- José Filipe Alves (U.Porto)
- Morgan Persson (Lunds universitet)

Follow us on social media:

@eugloh19

@eugloh_network

@eugloh

@eugloh

www.eugloh.eu

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