



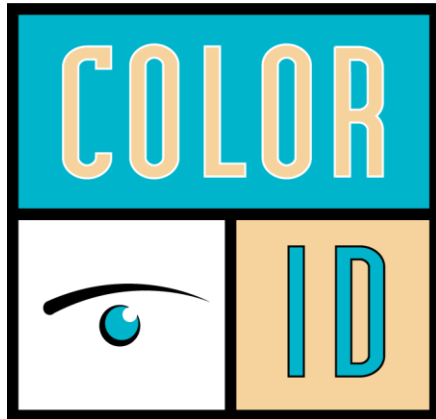
The Implications for HEIs: A Deep Dive into the Meaning Behind It All

**ECCA-Webinar:
Advancing Digital Identity in Higher Education
2026-02-25**

**Alexander Loechel
Referent IT-Projekte · IT-Services · LMU Munich**



Summarizing the presentations → Implications for HEIs



Mobile Identity

→ Virtual Campus Cards in the USA

Pavol Hrina (DIForum)

EUDI-Wallet and Digital Credentials



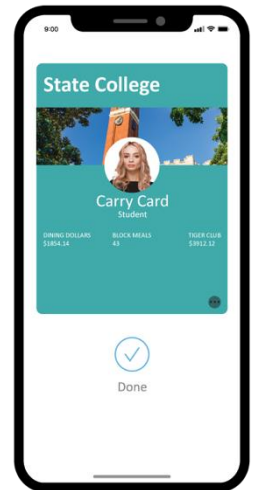
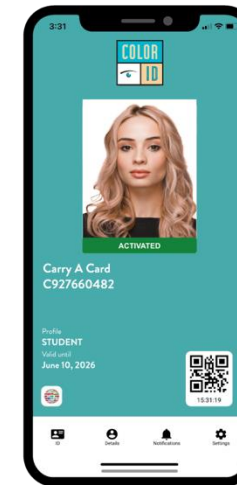
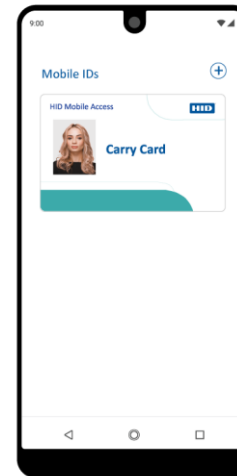
Focus: Campus Cards

Identity-Management and the Combination of Identity and Facility-Management

Mobile Identity in the U.S.

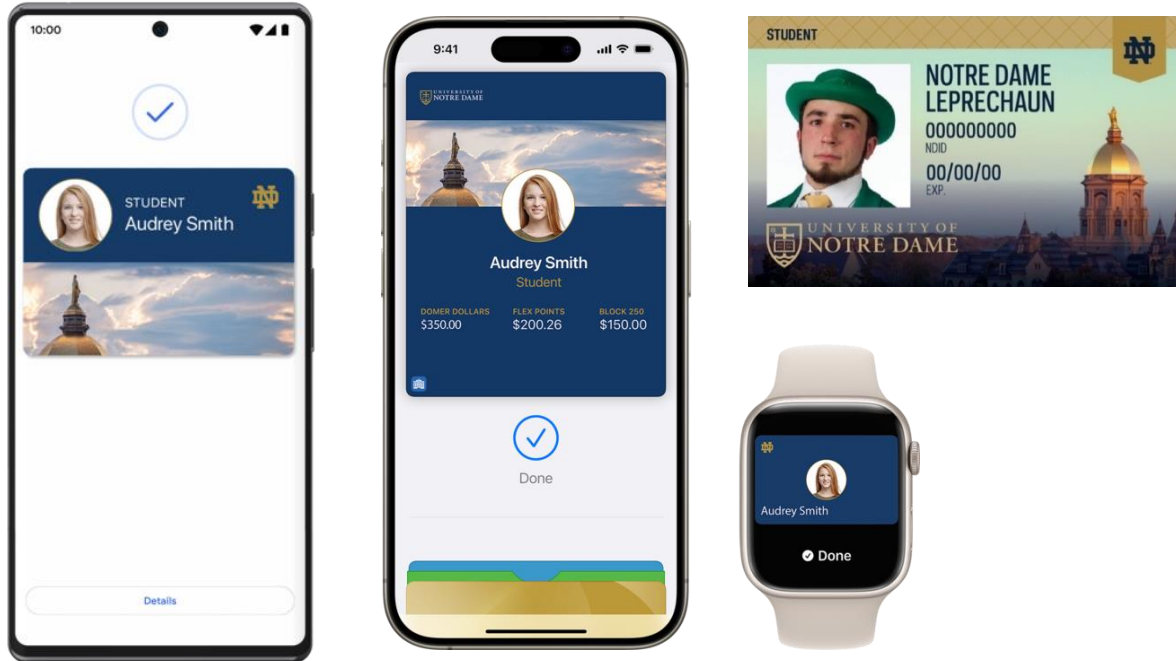
Key Takeaways:

- Mobile is **Operational**, Not Experimental!
- **Mobile First** and Multiple Credentials
- Mobile and Plastic Identity Cards must **coexist**



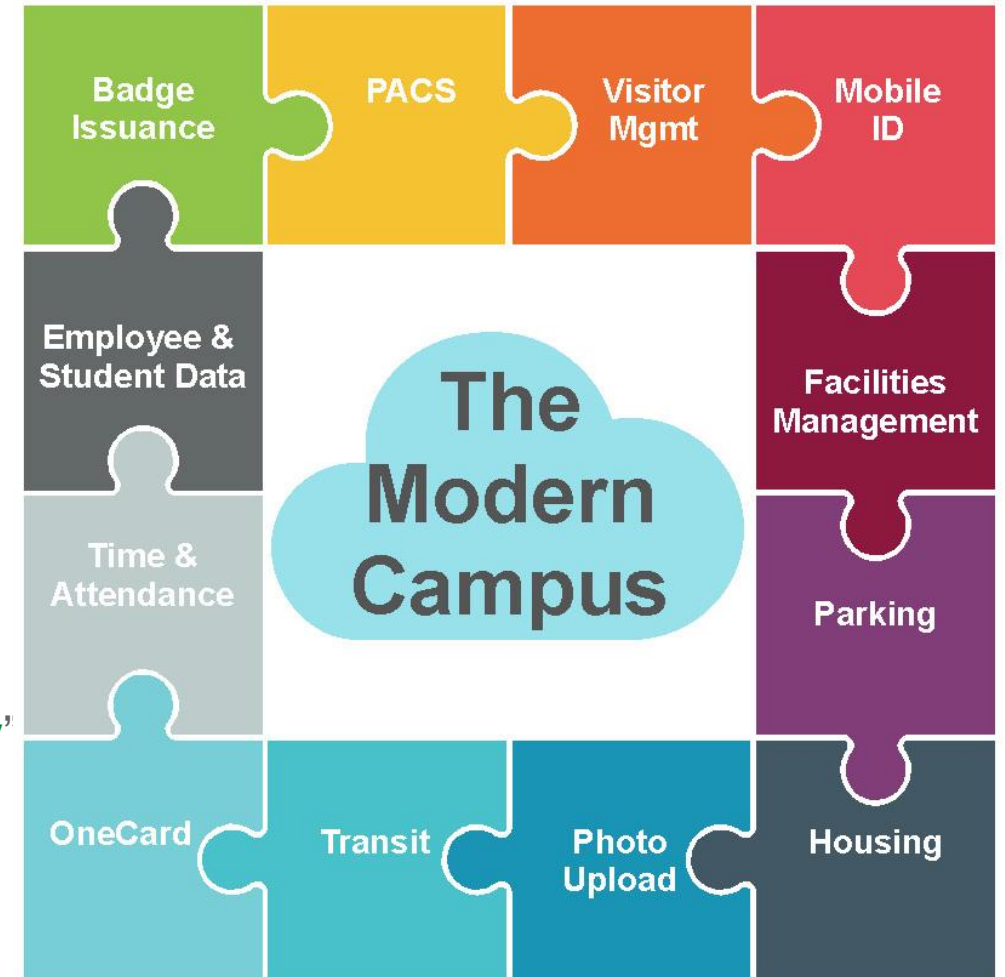
Mobile Identity in the U.S.

Who controls identity lifecycle?



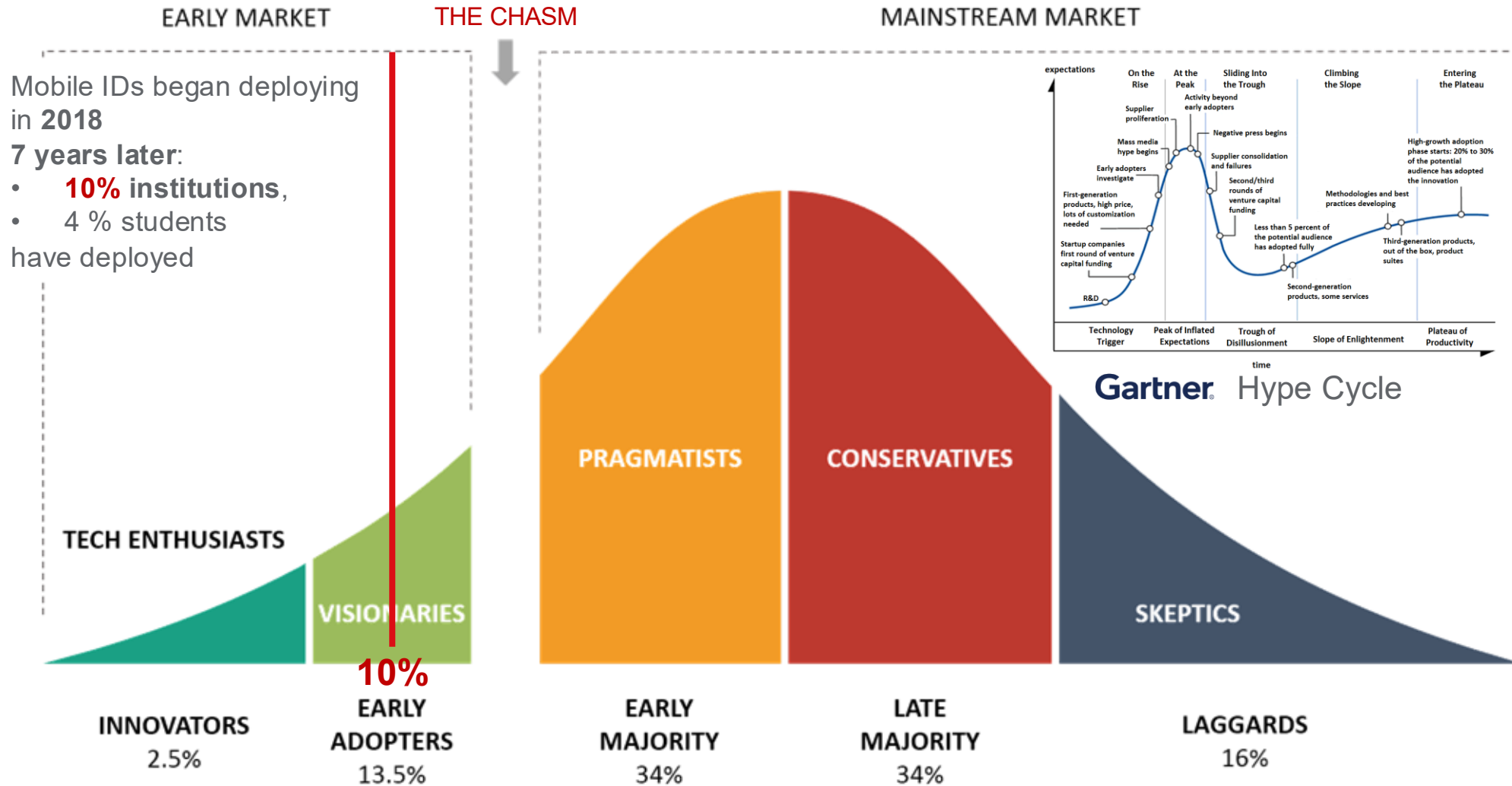
In the U.S. Apple and Google promote the “**ONE Pass strategy**”

- **One credential** that groups all services for **one campus**.
- Just like a plastic card, all relying parties must support the same credential type (e.g. HID Seos, or Mifare DESfire)

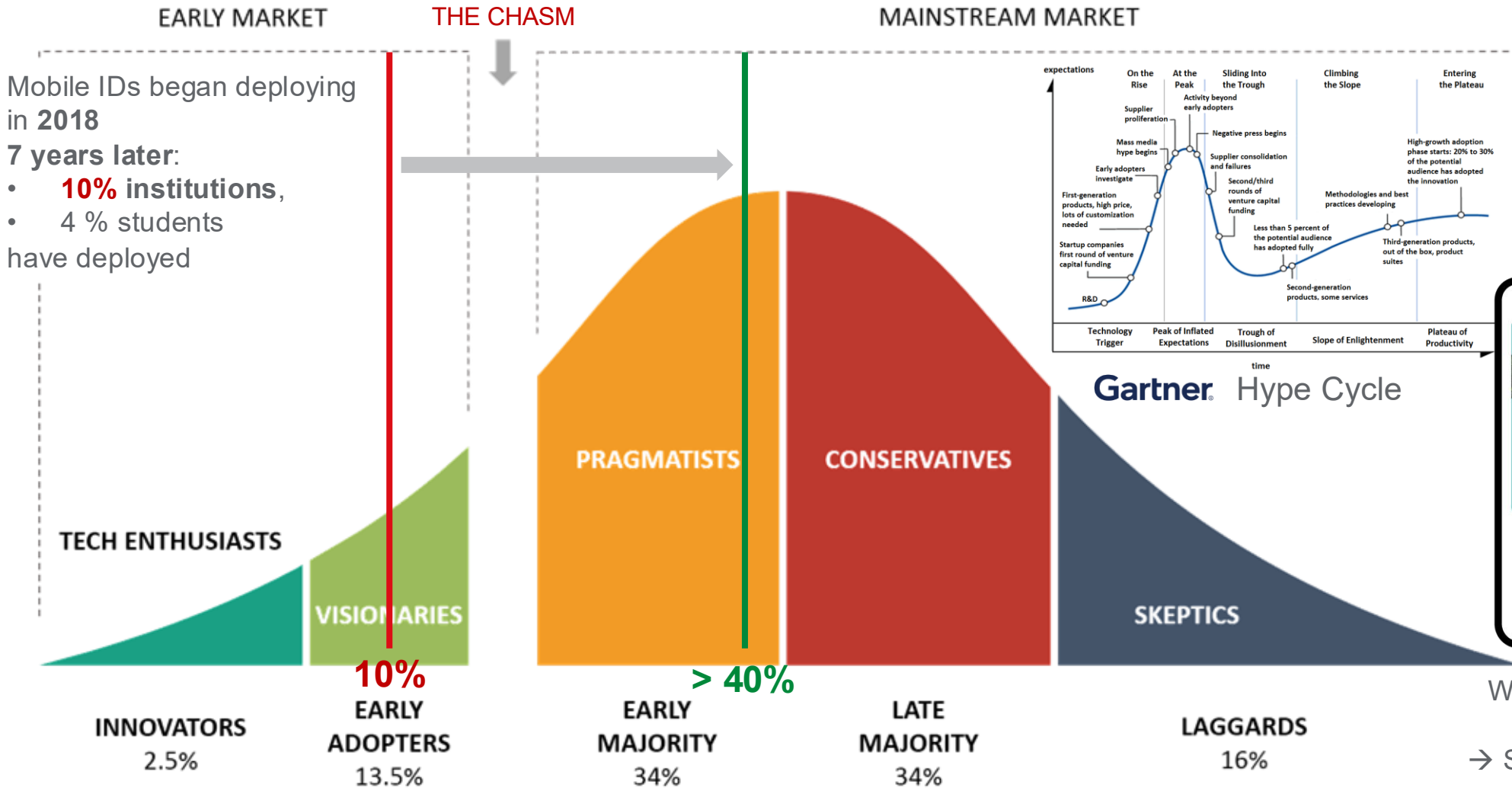


→ Multiple Credentials?

Mobile Identity in the U.S. Adoption rates after 7 years



Mobile Identity in the U.S. Adoption rates after 7 years



→ ONE credential to rule them all **does NOT work**

Mobile Identity → Credentials (digital and physical) Campus Cards are about Accessing Services → Access and Identity Credentials

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

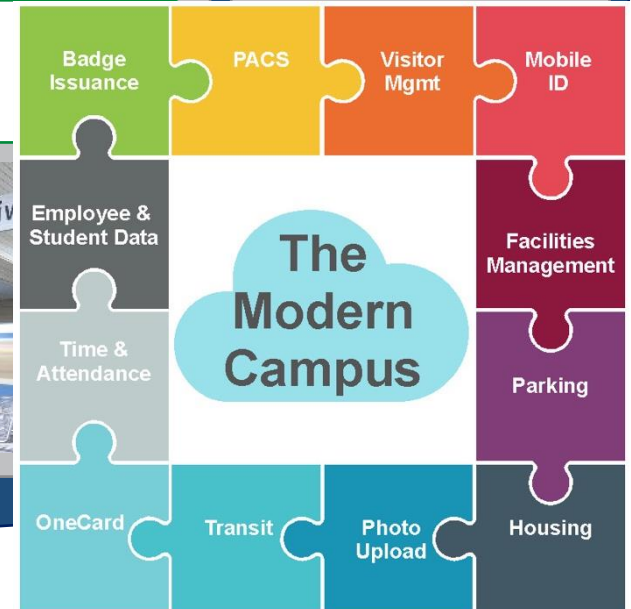
Transport

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

Discount and promotions

- **Discounts** on cultural activities
 - Museums
 - theaters
 - cinemas
- Shops
- Restaurants

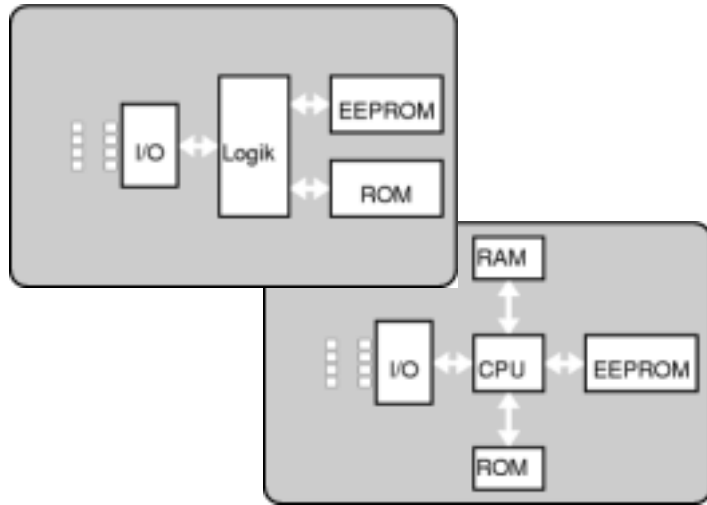
On- & Off-Campus → On-Site Usage / Proximity Use-Cases + Online Services



providing service → create benefits

Mobile Identity → Credentials (digital and physical)

Physical cards
(chip cards and smart cards)



Data Applications in the Credential

vs.

Smartphone



vs.

dedicated Credentials

→ Shift to **Wallets** (Container for multiple Credentials)

Mobile Identity → Digital Identity Definitions

The term Wallet is vague; let's define the relevant terms:

Wallet *(Noun)*

A **wallet** is a container that stores and manages credentials.

- In the physical world: a wallet holds cards (ID card, driver's license, bank card).
- In the digital world: a wallet is a software container that securely stores and presents digital credentials.

In the context of the **EU Digital Identity Wallet (EUDI Wallet)**, a wallet is defined as a tool that allows users to store **identity data** and **electronic attestations of attributes** and to present them securely to relying parties.



Credential *(Noun)*

- a qualification, achievement, quality, or aspect of a person's background, especially when used to indicate their **suitability** for something.
- a document proving a person's identity or qualifications.

Definition as of Oxford Languages

Examples:

- Digital National Identity Document → PID (Personal Identification Data)
- A School / University degree
- A Transcript of Record
- A course micro-credential
- Employee badge
- Student ID badge (→ PID)
- Age verification token
- Payment Card
- Access Key Token

Long-Term vs Short-Term Credentials

Long-Term Credentials

Characteristics:

- Issued once
- Intended to remain valid for a long period
- Represent stable attributes

Examples:

- Birth registration
- Marriage certificate
- **University degree**

They should:

- Be immutable (original statement never changes)
- *Support revocation mechanisms if necessary*

Short-Term Credentials

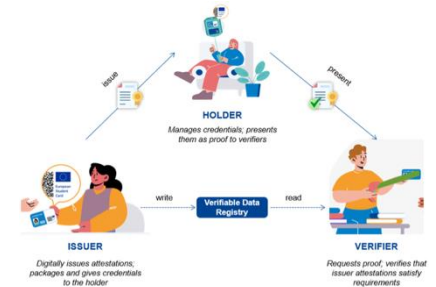
Characteristics:

- Limited validity period (minutes to years)
- Designed for temporary use
- Often revocable or refreshable

Examples:

- National ID Document (PID)
- Driving Licence
- Student ID / Employee Badge
- Access credential / Event ticket

Short-term credentials reduce privacy risks and improve security by limiting exposure.



Mobile Identity → Digital Identity

When you are more interested in Long-term Credentials for Higher Education

→ European Higher Education Interoperability Framework

(<https://education.ec.europa.eu/focus-topics/digital-education/digital-education-hub/workshops-and-working-groups/interoperability-framework>)



- Discover
- **Apply and get recognition**
- Access tools
- Manage educational resources
- Generate data
- **Earn a credential**
- User Identity
- Institutional Identity



Mobile Identity → Digital Identity Definitions

Issuer

- An entity that creates (and cryptographically signs) credentials.

Examples:

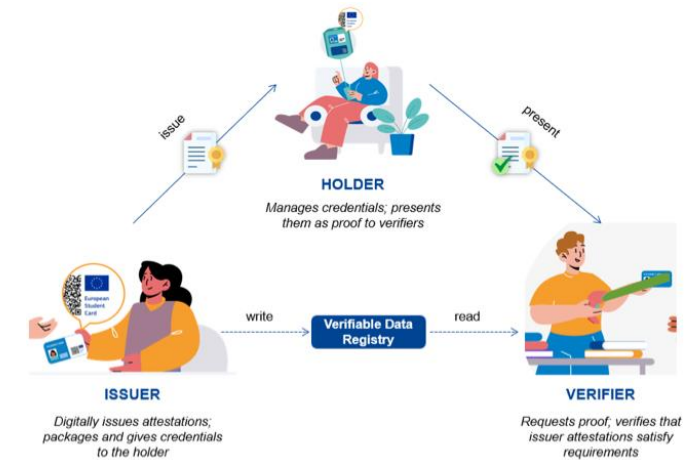
- Government issuing a digital ID
- **University** issuing a diploma credential, a Student ID, and enrollment credential
- Bank issuing a payment credential

Holder

- The person (or organization) who receives and controls the credential in their wallet.
- The holder decides when and to whom a credential is presented.

Verifier / Relying Party

- An entity that checks the data and validity of a credential.
- A **Relying Party** is a service that relies on verified information to provide a service.
- The verifier (with Verifiable Credentials):
 - Validates cryptographic signatures
 - Checks revocation status
 - Evaluates trust anchors



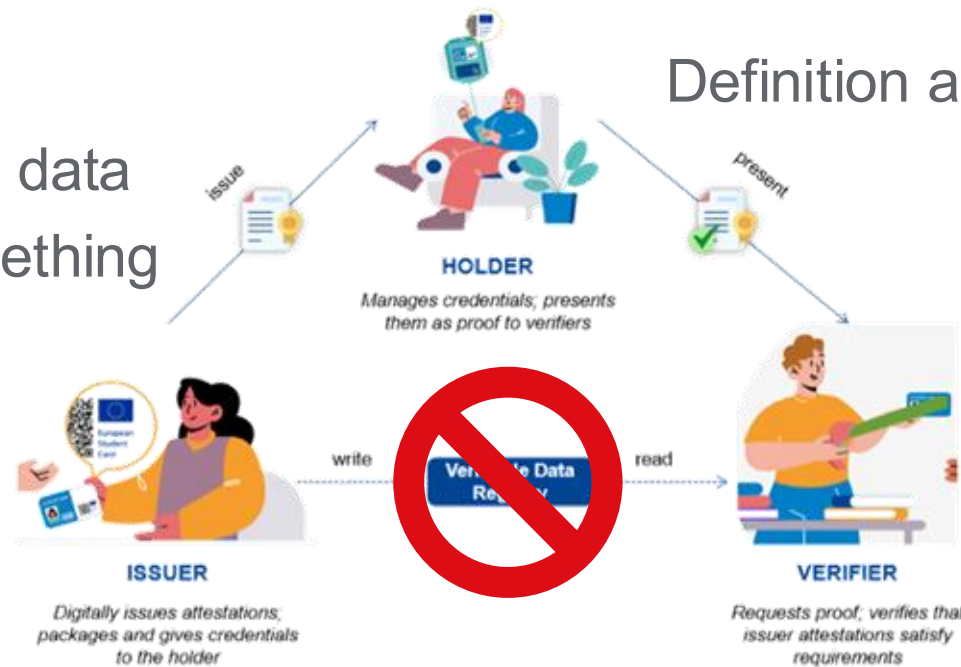
Interoperability *(Noun)*

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



- Understand the transmitted data
- can use the data to do something

Definition as of Oxford Languages



Campus Card use-case:
Access to on-campus services

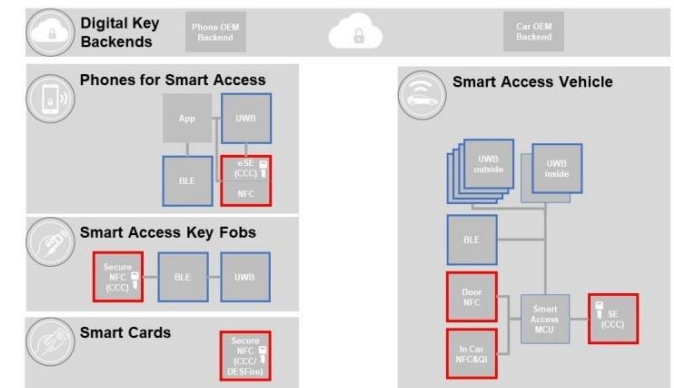
Secure Element

A **Secure Element (SE)** is a tamper-resistant hardware component designed to:

- Store sensitive credentials
- Perform cryptographic operations
- Protect against extraction attacks

Used in:

- Payment credentials (EMV)
- Mobile ID implementations
- Some digital identity wallets



Example: NXP Secure Elements

<https://www.nxp.com/company/about-nxp/smarter-world-blog/BL-HOW-SECURE-ELEMENTS-ENHANCE-DIGITAL-KEYS>



Types of Wallets (informal, conceptual/didactic):

- Mobile-App Wallets

Examples: Apple Wallet, Google Wallet, Samsung Wallet, national EUDI Wallet apps.

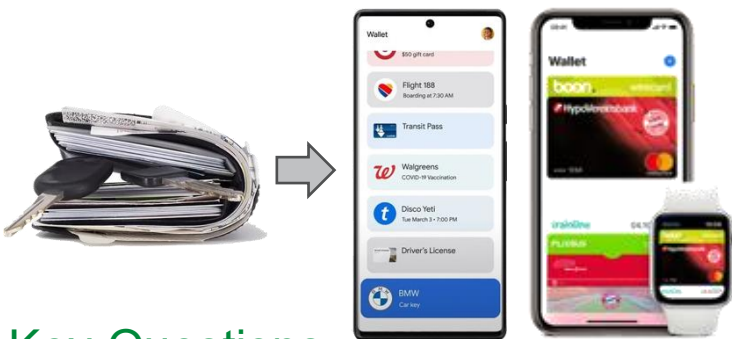
Characteristics:

- Installed as a native mobile app
- Credentials are typically protected by:
 - Secure Element (hardware chip), or
 - Trusted Execution Environment (TEE), or
 - OS-level secure key store
- Often support cloud backup or device migration

- Web-Wallets

Credentials are protected by a cloud-based Secure Element
→ Only online usable

- Vaults (Term normally not used in Digital identity context, but common in ITC → Stores secrets)
An even more protected storage of credentials



Key-Questions:

which credentials do you always carry around?

Mobile Identity → Digital Identity

Common Verifiable Credential Formats / Protocols for Digital Identities

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

Issuing and Redemption Protocols

- OID4VC (OID4VCI and OID4VP)

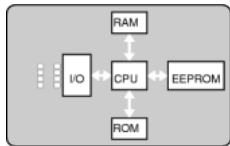
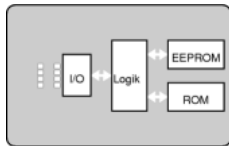


For **proximity** use-cases
NFC / BLE transmission is crucial

Mobile Identity → Digital Identity

Understand the use-cases and the technical requirements

→ Use-cases defines the required data and data format



→ We tend to try to solve all problems with the tool we have / like

→ But we have a toolbox of technologies available in the wallets

EU Digital Identity Wallet



→ Each credential can define its own data technology / data model

→ A Wallet can hold multiple credentials with multiple technologies

→ Auto-Presentation is the User-Experience enabler

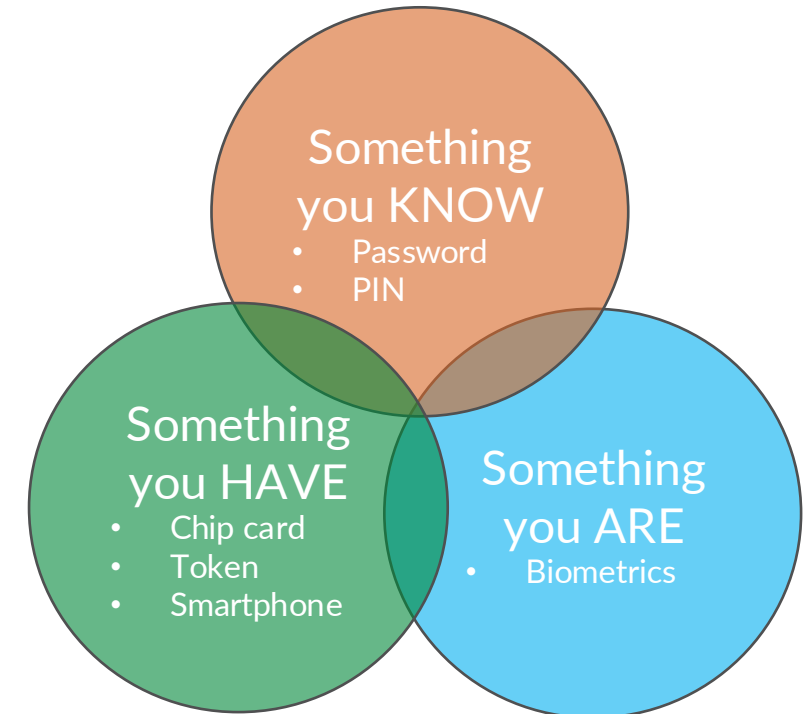


Mobile Identity → Digital Identity

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 combination: “*something we have*” + “*something we are*” → **Medium**: Smartphone **Wallet Passes** + authentication via biometrics

Authentication Factors

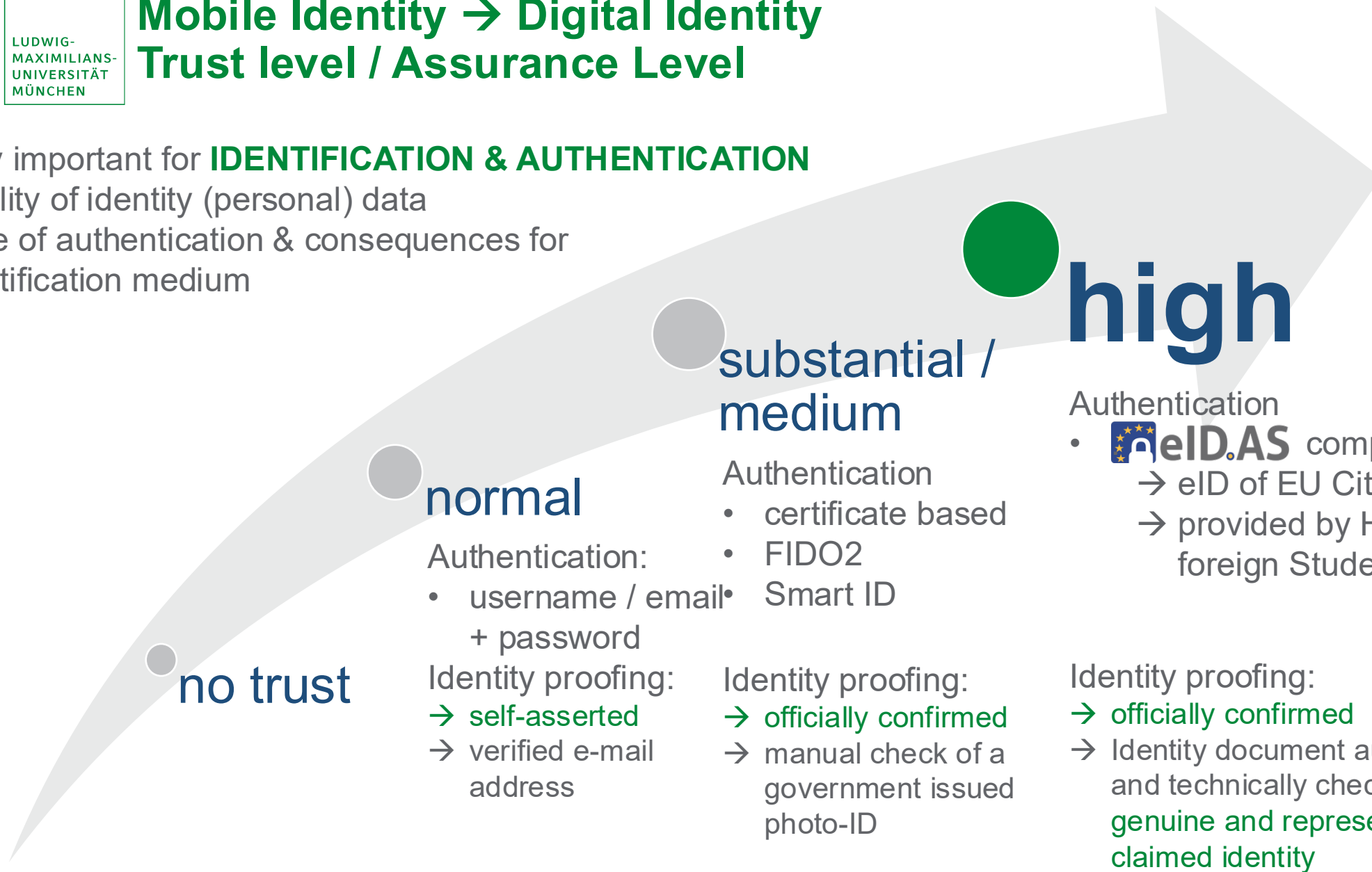


→ We already have a powerful IDM System for **online-services** → **Shibboleth** → **eduGAIN-AAI**

Mobile Identity → Digital Identity

Trust level / Assurance Level

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



no trust

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

Authentication:
 • username / email
 + password

normal

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

Smart ID

Authentication
 • certificate based
 • FIDO2

substantial / medium

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

Authentication

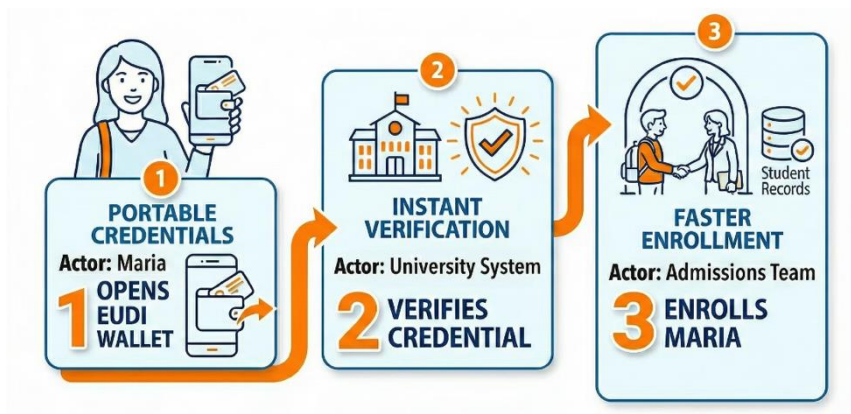
-  **eID.AS** compliant
 - eID of EU Citizen IDs
 - provided by HEI for foreign Students

high

Mobile Identity → Digital Identity

Who is the relying party / verifier?

- Cross-organisation verification ← EUDI-Wallet is exactly designed for this process



- Use-Case for the European Student Card

- Within an organisation / a dedicated service-provider issuer relation

→ Campus Cards use-cases

- Library ID
- Canteen Discounts
- Physical Access Control

Mobile Identity → Digital Identity

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>

Mobile Identity → Digital Identity

European Student Card Verifiable Credential Pilot Report

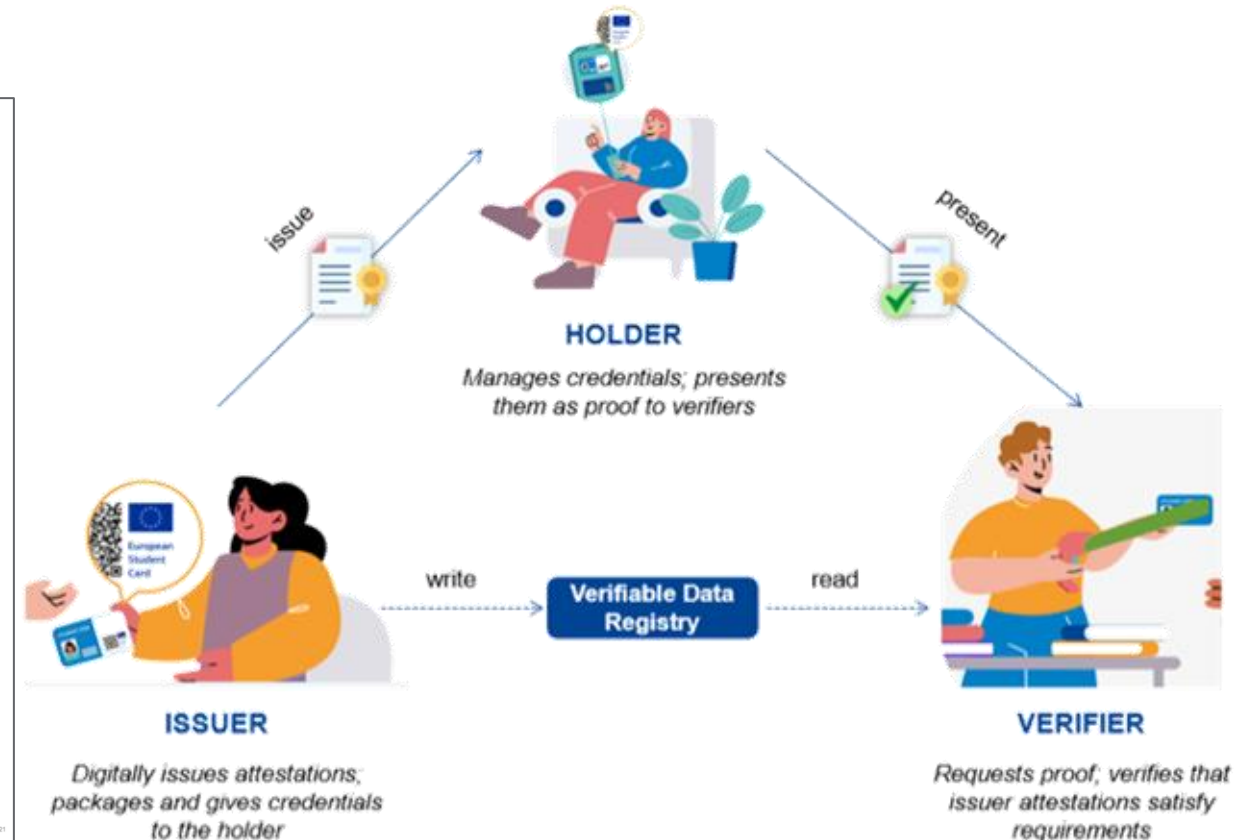
- W3C Verifiable Credential Data Model v1
- ELM (European Learning Model) Based Data Model – Attribute Structure
- Revocation / Update Process required



ANNEX I: Participating organisations

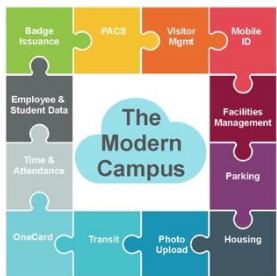
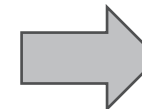
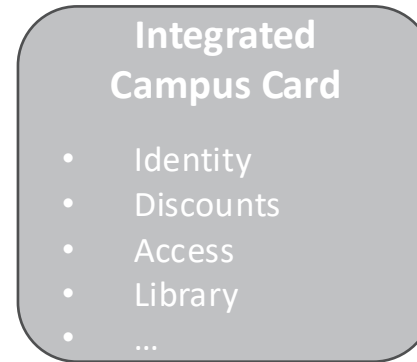
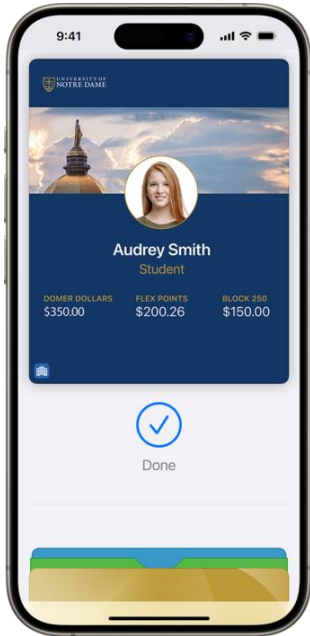
Participating organisations

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

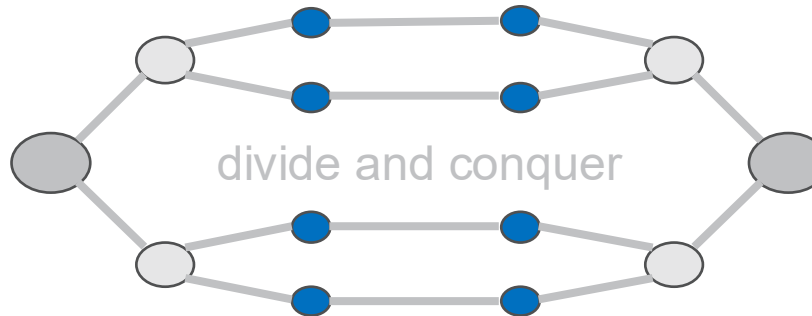


Mobile Identity → Digital Identity → Transition of Credentials (digital and physical)

Ownership?

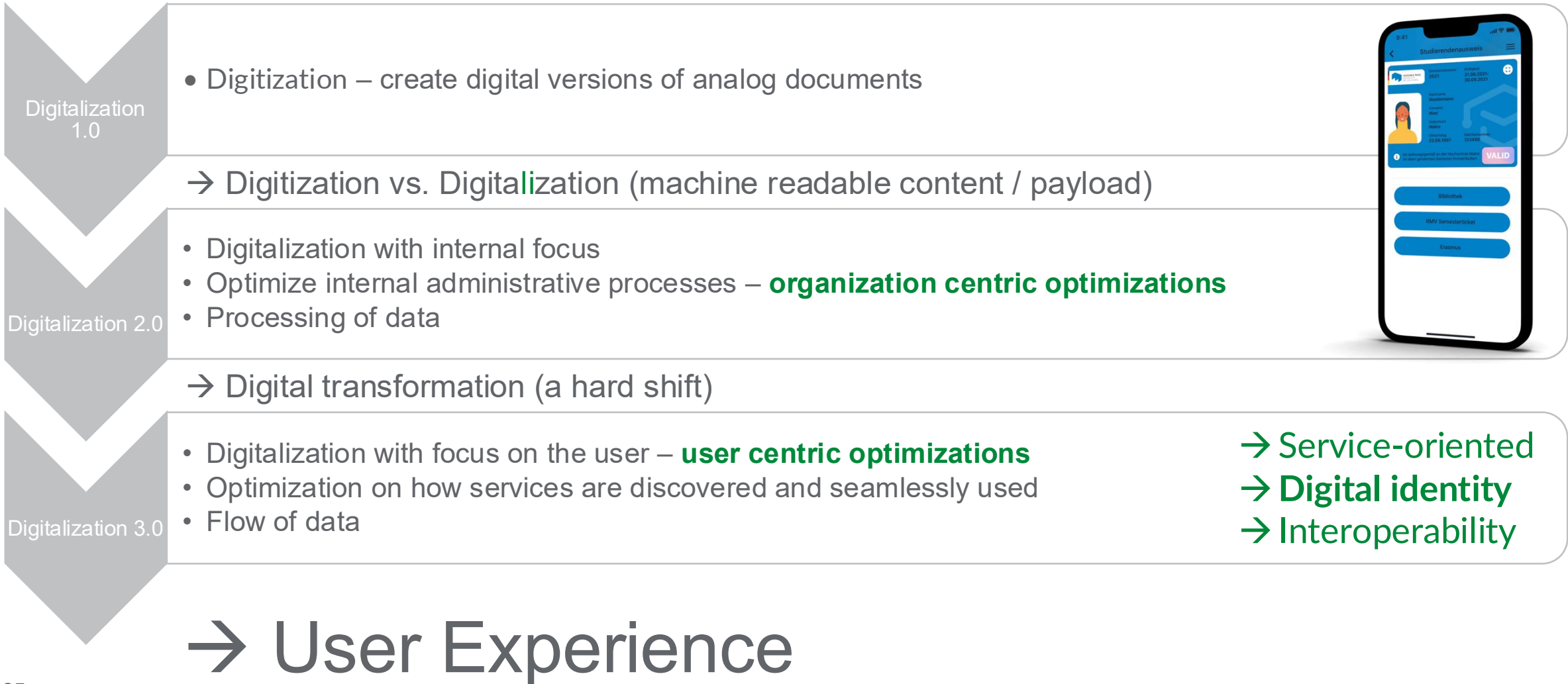


→ Multiple Credentials
→ Micro Credentials



Mobile Identity → Digital Identity

Stages of Digitalization – Period of Digital transformation



Mobile Identity → Digital Identity

Kano-Model – Systematic for User Experience & User Satisfaction

Adoption of a Technology depends on

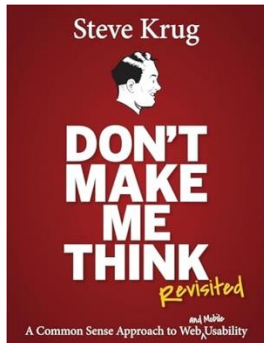
- Does it solve the users / customers needs
- Is the User Experience good enough

Every company gets about three innovation tokens.

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

“Boring” is a good thing - **“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

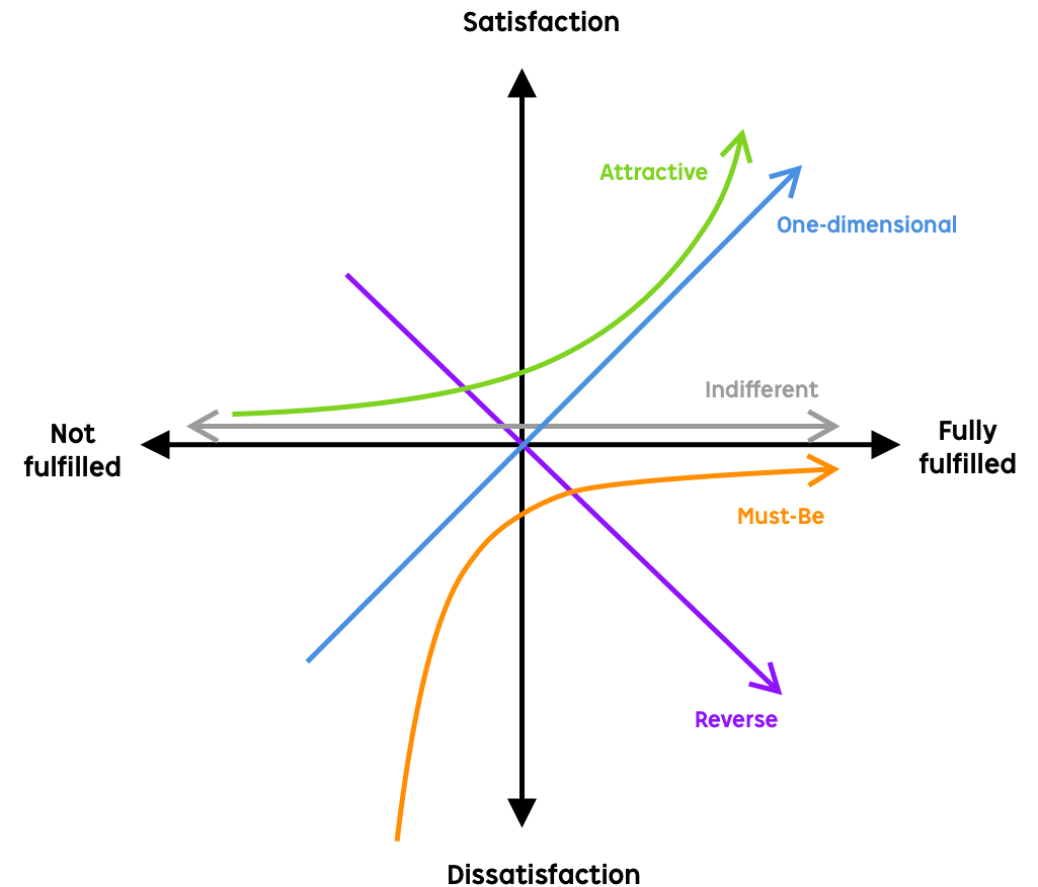


Don't make me Think

→ 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, ...)



Mobile Identity → Digital Identity Definition of Service (ITIL)

*“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

Mobile Identity → Digital Identity

Campus Cards & eduTAP are about **Service Access** on site (on and off campus)

- For Member of the Higher Education Institution
- For incoming members of other Higher Education Institutions / Partners ← Mobility (short- and long-term)

For the Person **User Experience** is key, it should be as easy and simple as possible

Benchmarks:



WLAN Access



Login to Online Services



Authentication to physical
(on-site) services

→ To access services on site it should be as easy as using the WLAN with *eduroam*



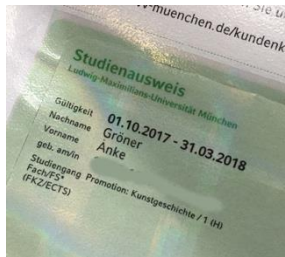
LUDWIG-
MAXIMILIANS-
UNIVERSITÄT
MÜNCHEN

Mobile Identity → Digital Identity

Transition of credentials into the Smartphone Wallets

The LMU Student ID (over time)

LMU
Student ID
till 2019



LMUcard
Student ID
2019-2025



LMU
Student ID
2025+



today



LMU
Student ID
2027+ ?



eduTAP & eduTAP@LMU

- University ID**
(Student / Staff / Affiliate ID)
- ✓ Verifiable Credentials
 - ✓ Selective Disclosure
 - ✓ Zero Knowledge Proofs
 - ✓ Reflection of important Shibboleth attributes

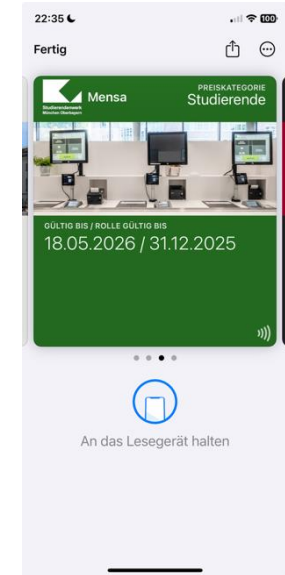
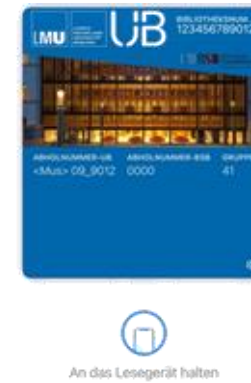
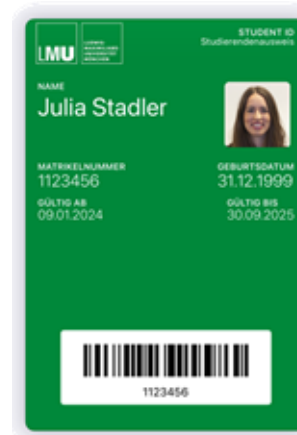


LUDWIG-
MAXIMILIANS-
UNIVERSITÄT
MÜNCHEN

Mobile Identity → Digital Identity Transition of credentials into the Smartphone Wallets eduTAP Examples @ LMU Munich

Google Wallet

Apple Wallet



→ all **NFC enabled**

→ **NFC enabled** where possible



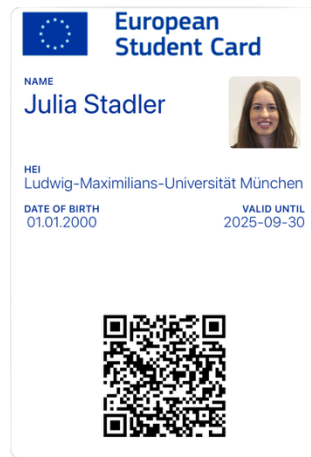
Mobile Identity → Digital Identity

Example: The European Student Card

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

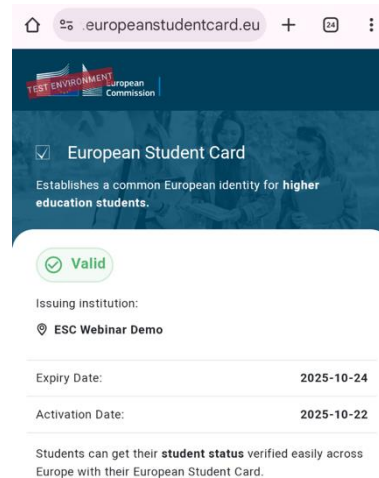


Google



Apple

- ✓ Discounts off-campus
- ✓ European dimension → Erasmus+ marketing
- ✓ Online status verification



(v1.5)



Mobile Identity → Digital Identity

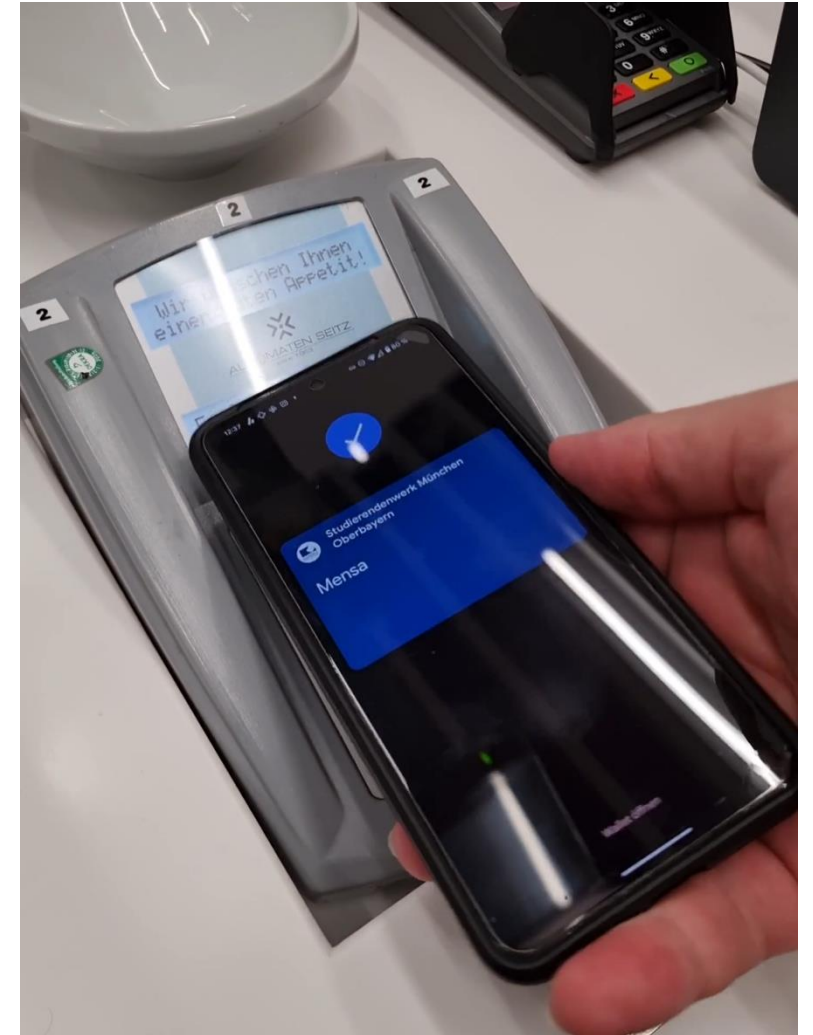
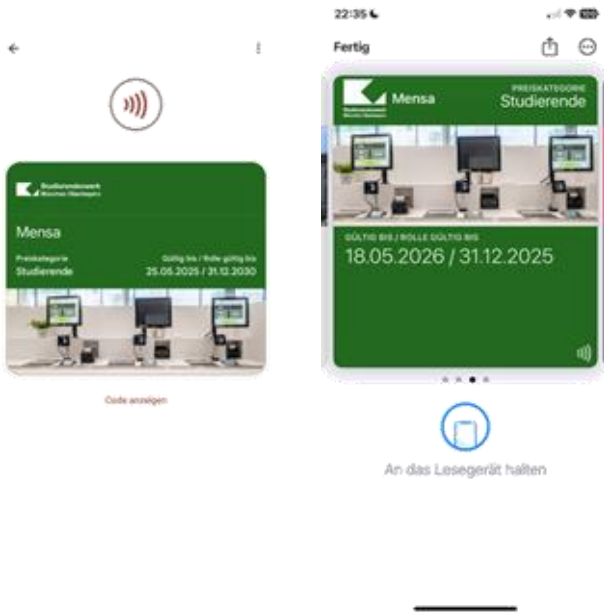
Example: Tap to Pay - Discount-Pass for Canteens

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



Mobile Identity → Digital Identity

Example: Tap to open a door (Physical Access Control)

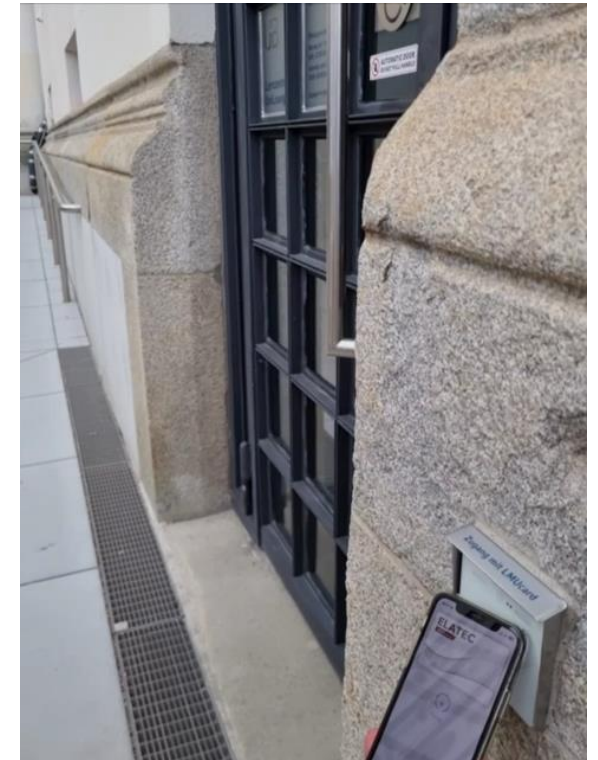
Physical access to the learning spaces



LMUcard



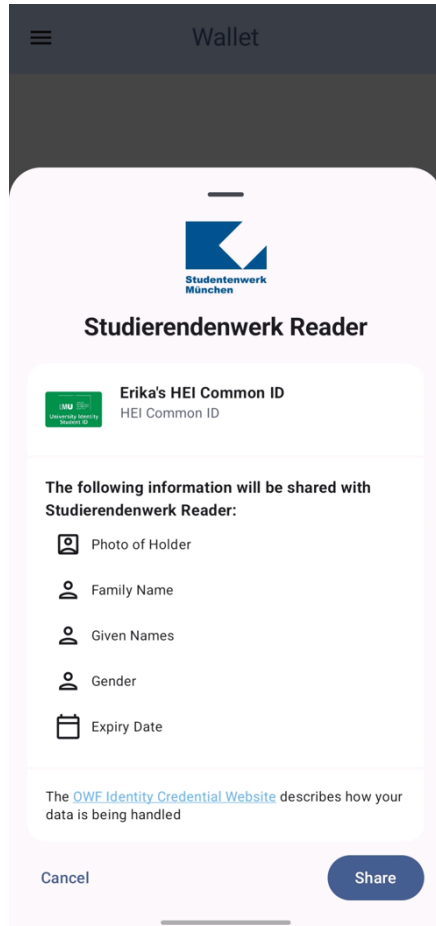
Google Smart Tap



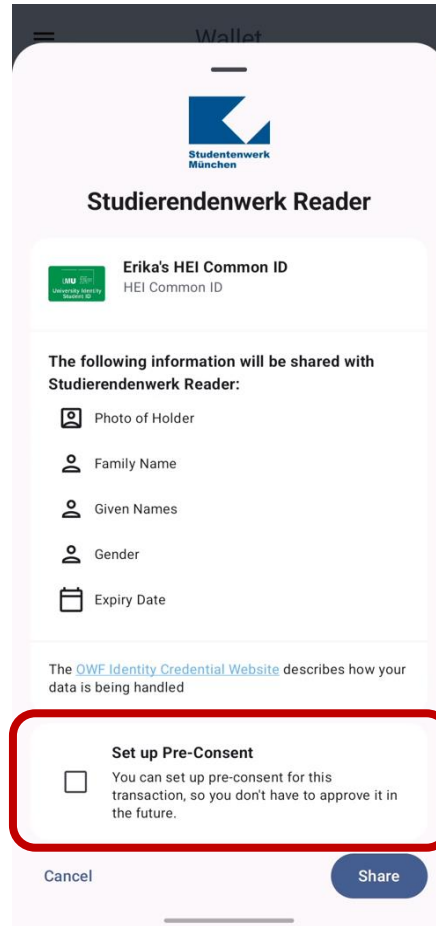
Apple Access

Mobile Identity → Digital Identity

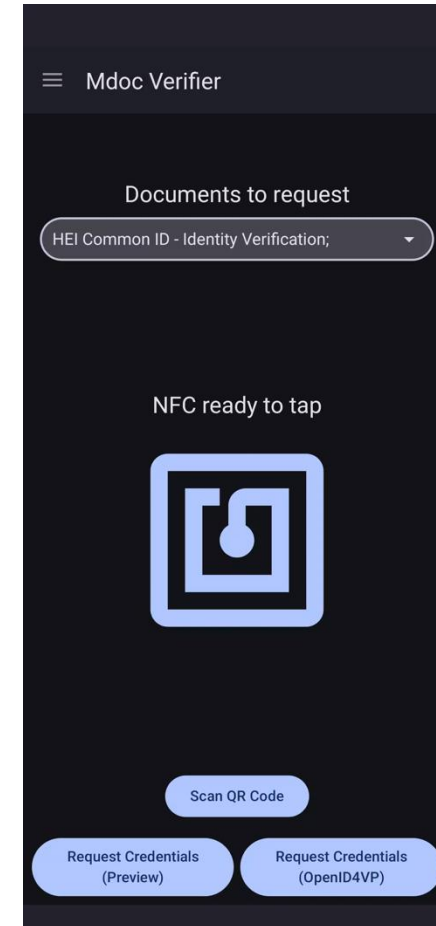
Identity Pass: Path to the best User Experience and Interoperability



Informed Consent



Informed Consent + Pre-Consent



Verifier App



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

