



European Digital Student Service Infrastructure - Level 2 EU Student eCard Stakeholders Forum

March 9-10, 2023
Venice

The sole responsibility of this publication lies with the project consortium. The European Union is not responsible for any use that may be made of the information contained therein.
CEF-TC-2020-3



**Co-funded by
the European Union**



EU Student eCard Stakeholders Forum

**Digitized Card Pilot for
European HEIs**

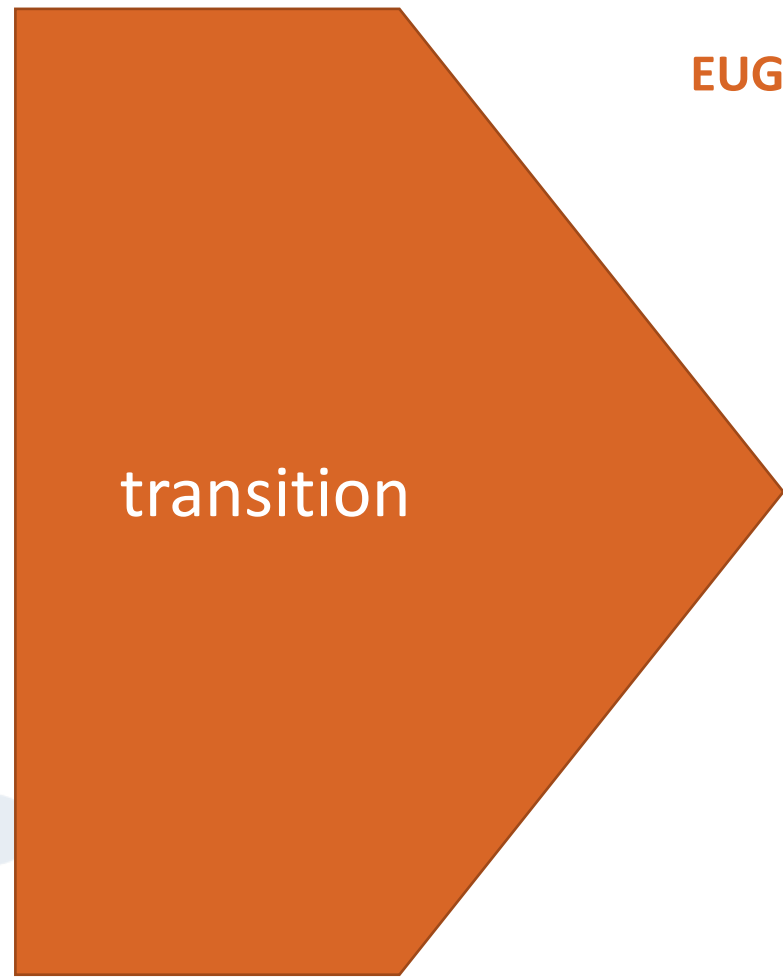
Alexander Loechel

IT Manager

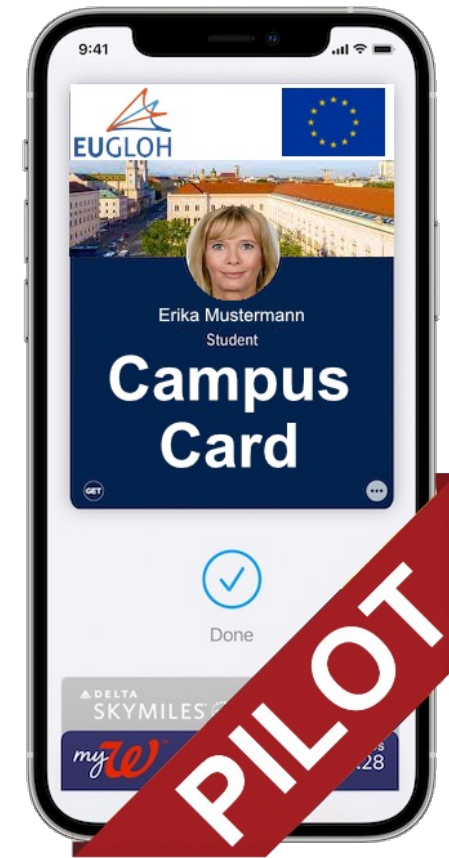
Ludwig Maximilian University
of Munich



The path to an interoperable European Campus Card



EUGLOH Digitized Campus Card Pilot



- ✓ Vision of the European Commission: Towards a European Education Area
- ✓ The European Student Card Initiative (ESCI)
- ✓ European Charter for Higher Education (ECHE) of the Erasmus+ Program



A great vision!

Common understanding

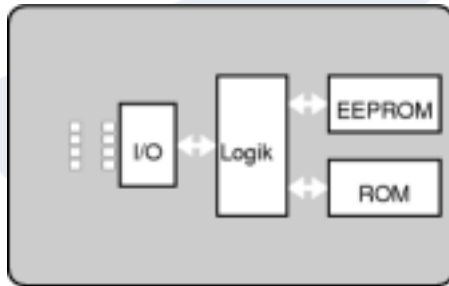
Terms and Definitions

Explain certain technical points

Terms and Definitions

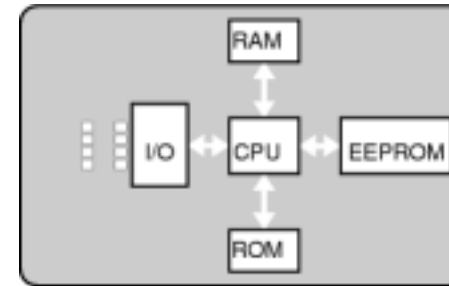
- **Smartcards**

→ processor cards ← computing capabilities



- **Chip cards**

→ memory cards ← stores data



Terms and Definitions

In context of this project:

- **Wallet**

A Digital Wallet is a smartphone application that acts as a container for passes. It is derived from the term wallet that describes a small case, often flat and made of leather, for keeping money, credit cards and identification documents

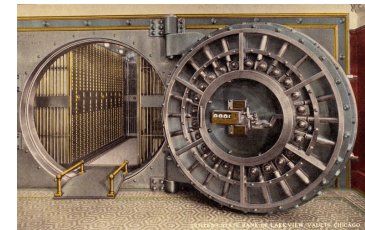


- **Pass**

A Wallet Pass is an application that contains a visual representation of a card + a data structure + a contact less readable data structure or program

- **Vault**

A Digital Vault is a large secure data store. It is derived from the term vault that describes a secure room or rooms in or below a bank used to store valuables. The related term safe or safe-deposit box, describing a box, usually made of metal, fireproof, in which personal valuables (e.g., credentials and documents, items of important possessions) can be locked for safekeeping.



Terms and Definitions

- **Short-term vs long-term mobility**



- **Identity**

the fact of being, or feeling that you are, a particular type of person, organization

- **Account**

an agreement allowing you to use a particular computer system, website, etc.

- **Role**

the position or purpose that someone or something has in a situation, organization, society

- **Service**

mean of **delivering value to customers** by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

Terms and Definitions

- **Credential**
documentary or electronic evidence that a person has certain status or privileges
- **Identification document**
documentary or electronic evidence of a person's identity
- **Service provider**
a company or institution that provides **services** to **customers**
- **Relying party**
an instance that checks a credential for certain data and validity
- **Certificate authority**
In cryptography, a certificate authority or certification authority (CA) is an entity that stores, signs, and issues digital certificates.
- **Credential Manager**
- **Credential Issuer / Pass Issuer**
entity that's responsible for credentials, owns the credentials, and issues them to their customers
- **Credential Holder / Pass holder**
individual to whom an identification document / pass is issued

Terms and Definitions

- **Interoperability**
Interoperability is a characteristic of a product or system to work with other products or systems.
- **Digital sovereignty**
In political discourse, the term digital sovereignty is used to describe the possibilities for the self-determined use and design of information technology by societies, states, companies and individuals. This includes both digital competence as expertise and competence in the sense of the authority to carry out activities independently.
- **Digital self sovereignty identity**
Self-sovereign identity (SSI) is an approach to digital identity that gives individuals control over the information they use to prove who they are to websites, services, and applications across the web.
- **AAI**
Federated Authentication and Authorization Infrastructure (AAI) - Identity and Access Management

Stages of Digitalization

Digitalization 1.0

- Digitization – create digital versions of analog documents

Digitalization 2.0

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

→ Digital transformation

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

Trust level / Assurance Level

- 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
 - check of a government issued photo-ID

high

- Authentication
-  **eIDAS** compliant
 - In eID of EU Citizen IDs
 - Provided by HEI for foreign Students
- Identity proofing:
- Officially confirmed
 - Identity document checked to be genuine and represent the claimed identity
- **Qualified signature**

- ✓ Vision of the European Commission: Towards a European Education Area
- ✓ The European Student Card Initiative (ESCI)
- ✓ European Charter for Higher Education (ECHE) of the Erasmus+ Program



A great vision!

Background

Vision of the European Commission: Towards a European Education Area

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

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

ECHE requirements for HEIs

„Implement the priorities of the Program:

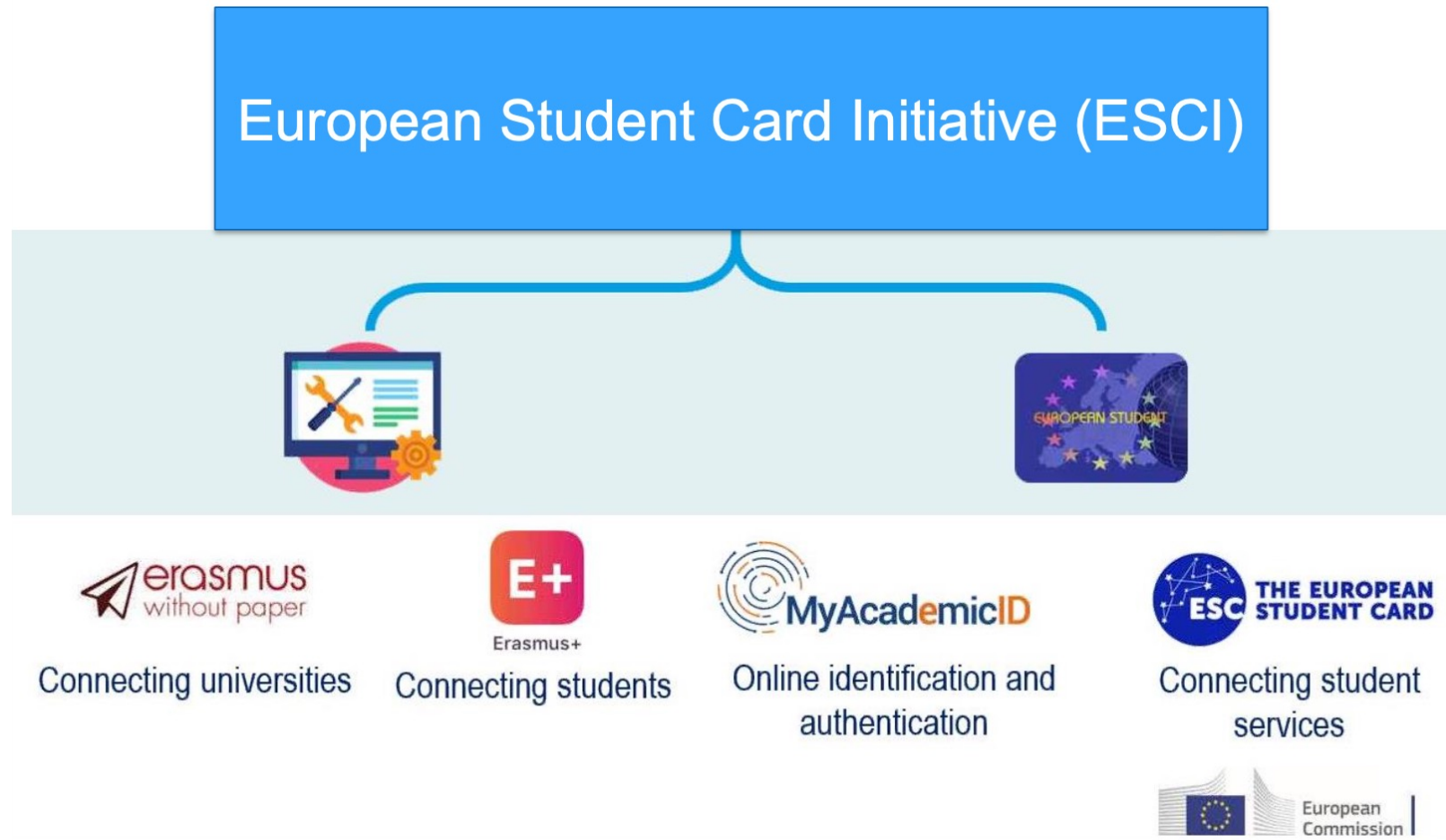
- By undertaking the necessary steps to **implement digital mobility management** in line **with the technical standards of the European Student Card Initiative.**
- ...“

Source: 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 – Implement and Issue European Student Cards**

The European Student Card Initiative (ESCI)



History of the European Student Card



Comité National
de la Carte Étudiant
et de ses Usages

2012 – 2013

- Signing of a protocol of Intent
- Bilateral Franco-Italian agreement between:
 - Fondazione ENDISU
 - ANDISU,
 - Cnous

November 2013

- Exchange between the Cnous and the CPU on European Student Card

2016

- Institutional structuring at European level
→ Erasmus+ Strategic Partnership

2016 – 2018 → European Student Card Project



2019 – 2020 → MyAcademicID Project

2025 - Goal

- All European / Erasmus+ Higher Education Institutions offer their students a European Student card



December 2015

- Memorandum of Understanding
- Student Unions of 4 countries:
 - France
 - Germany
 - Ireland,
 - Italy
- Exchange within ECStA

2020 – 2022

- European Digital Student Service Infrastructure Project
- ESC-Tension Project – European Student Card Extension and Adoption

→ sole focus: students



FONDAZIONE
ENDISU



1921–2021
100 JAHRE
DEUTSCHES
STUDENTENWERK
DAMIT STUDIEREN GELINGT

Benefits of the European Student Card Initiative


- **For students:**
 - Easy access to course materials prior to mobility, online course registration and automatic recognition of ECTS credits
 - **Immediate access to services at the host university, such as libraries, transport and accommodation**
 - **Discounts on cultural activities throughout the EU**
- **For Higher Education Institutions:**
 - Easy, online management of the entire mobility process – from student selection to the recognition of ECTS credits
 - Online identification of students, simplified and secure exchange of student data - including academic records - between Higher Education Institutions
 - Reduced administrative burden associated with student mobility

Source: https://ec.europa.eu/education/education-in-the-eu/european-student-card-initiative_en

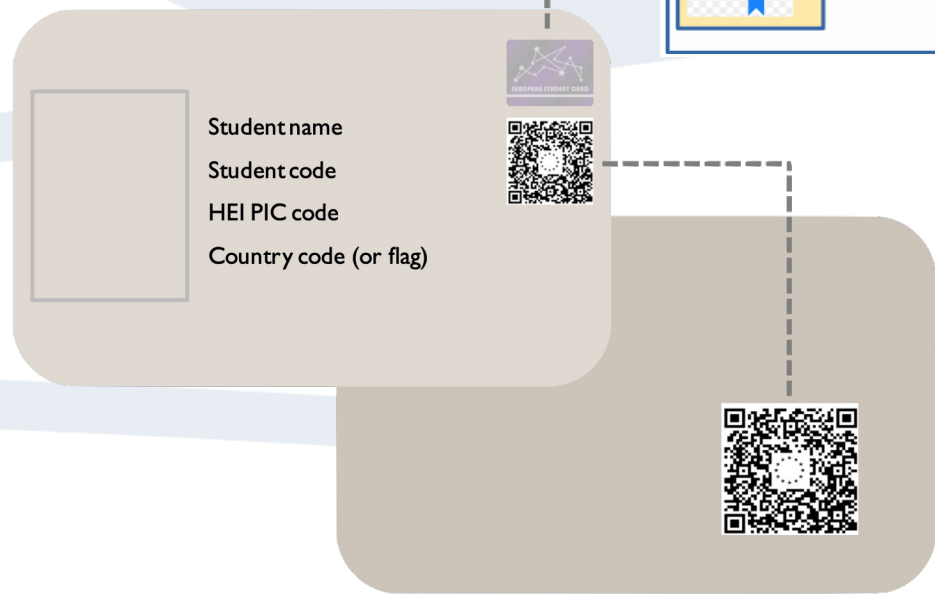
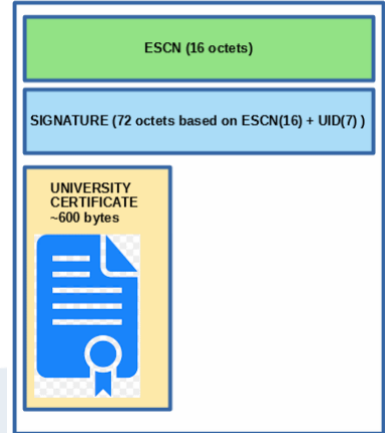
→ **European Student Card Project** as implementing instance

Services connected with the ESC

Higher Education Institutions should **provide services** to their **own (outgoing)** and **incoming students**

- ✓ **Identification and status verification / prove of entitlement**
- ✓ Electronic payment / cashless campus
 - ✓ canteen, cafeteria and vending machines
 - ✓ printer / scanner
- ✓ Library and learning spaces
- ✓ Access-Control
 - ✓ Areas / buildings / rooms → also special services for disabled persons
 - ✓ Single Sign On / 2FA / FIDO2
 - ✓ Attendance check (check-in for exams, attendance at courses)
- ✓ Public transport
- ✓ Accommodation
- ✓ **Electronic Signature** of legal documents (→ eIDAS) 
- ✓ *Discounts on cultural activities throughout the EU → Museums, theaters, cinemas, ...*

Expected Interoperability



		HEI			
		Available options for interoperability			
	Legend	Plain regular card	Card with QR code	Chip card with electronical control	Smart card
Potential impact on card production process					
Reading device available					
Possibility to add new services on demand					
Level of interoperability					

- ✓ Vision of the European Commission: Towards a European Education Area
- ✓ The European Student Card Initiative (ESCI)
- ✓ European Charter for Higher Education (ECHE) of the Erasmus+ Program



A great vision!
BUT

BUT (legal aspects & IT-Security aspects)

- The European Student Card Project specification is not transparent,
- Conflicts with GDPR requirements
 - → **Student IDs are not optional**; therefore, they could not be issued on consent (Article 7 - Conditions for consent, define when GDPR Art. 6 par. 1 lit. (a) did not apply)
 - Centralized Infrastructure conflicts with GDPR Article 24 & 25
- Conflicts with competition law and procurement law
 - Not vendor neutral
 - Holograms for example exclusive by one provider
- IT-Security
 - QR-codes are not considered secure
 - **NEVER EVER** code an URL into QR-Codes → communicate Trusted verification Apps or Websites
→ corona vaccination pass verification as best practice

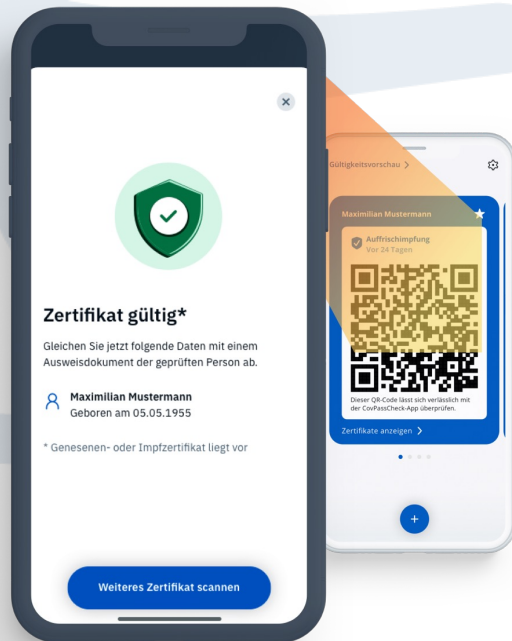


→ not a specification that could be implemented by all HEIs

QR-Code verification

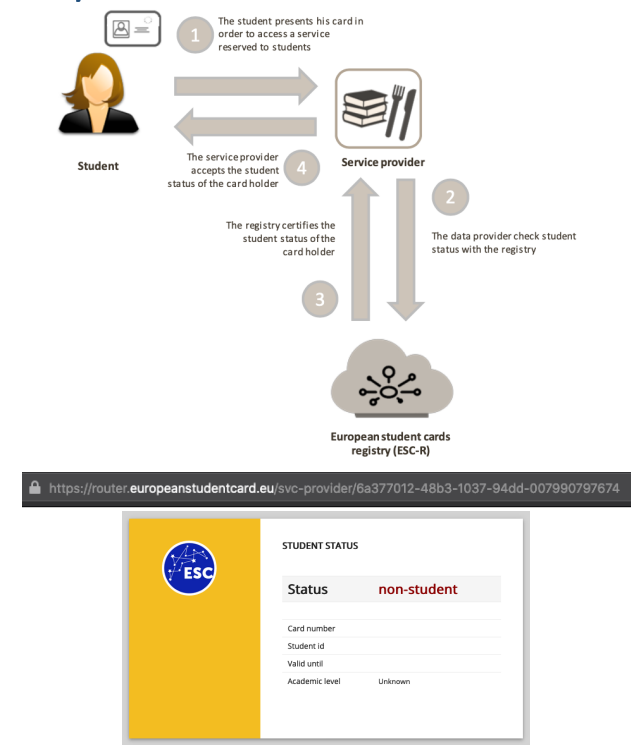
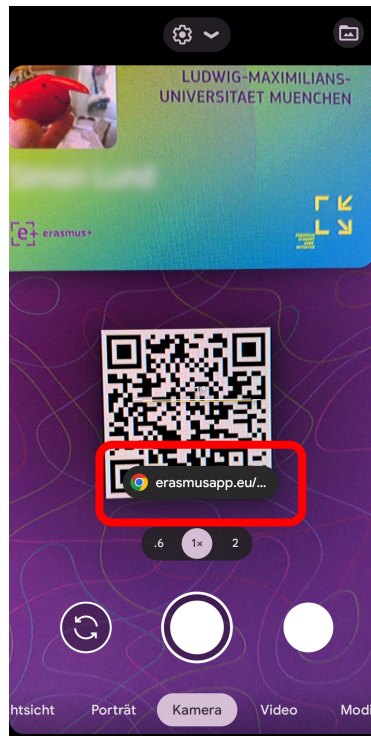
Done right – Example:
European Covid vaccine certificate and check app

- Offline verification
- Chain of trust
- Data not a URL / executable command



Done wrong – Example:
European Student Card / Erasmus+ App Card

- Pure Online verification + centralized structure
- QR-Code contains a URL / executable command



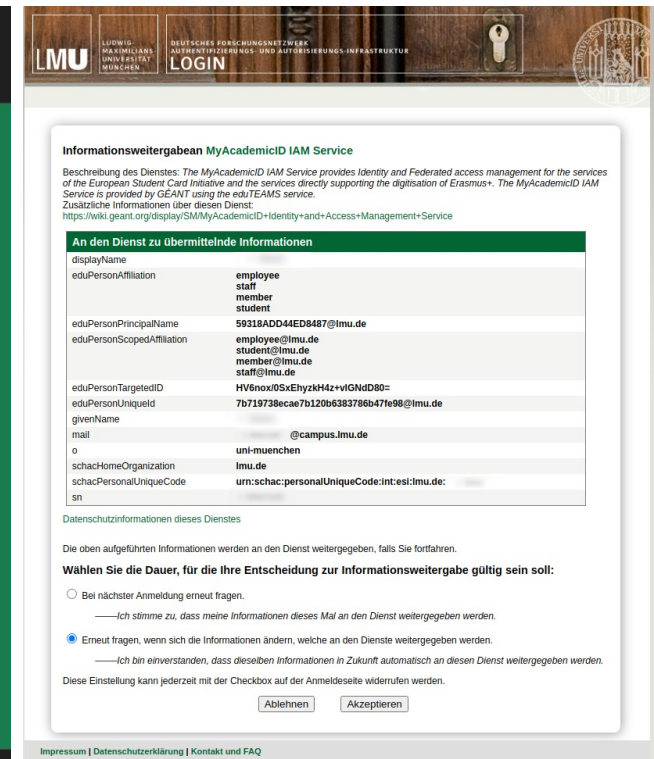
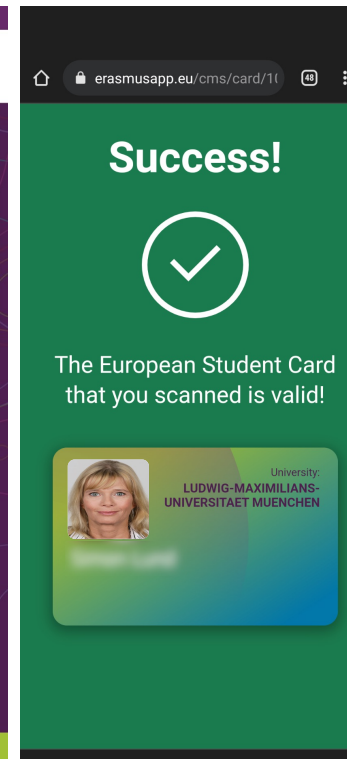
BUT (existing implementations)

European Student Card Integration within the **Erasmus+ App** (<https://erasmusapp.eu/card>)

- Very simple for HEI, only the following LDAP-Attributes have to be passed on the IDM:
 - schacHomeOrganization
 - schacPersonalUniqueCode → **ESI**
- Simple for students, no interaction with HEI necessary

BUT

- It is an absolute NO-GO
- Framework of trust → non-existing
 - Ignores all IT-Security best practices
 - QR-Code is not secure
 - Embedded URL → Phishing like attacks
 - No status verification with the HEI or Student Data
 - No security against screenshot sharing
- Issues for HEIs
 - No Branding of the HEI
 - Information propagation
 - No person or image verification
 - Issuing of virtual ID cards on behalf of the HEI without their consent



This Implementation should be revised!

- ✓ Vision of the European Commission: Towards a European Education Area
- ✓ The European Student Card Initiative (ESCI)
- ✓ European Charter for Higher Education (ECHE) of the Erasmus+ Program



**A great vision!
That does not work,
but is worth to be fulfilled**



European University Alliance for Global Health

9 Universities, 1 Goal: Building Europe's Campus for Global Health



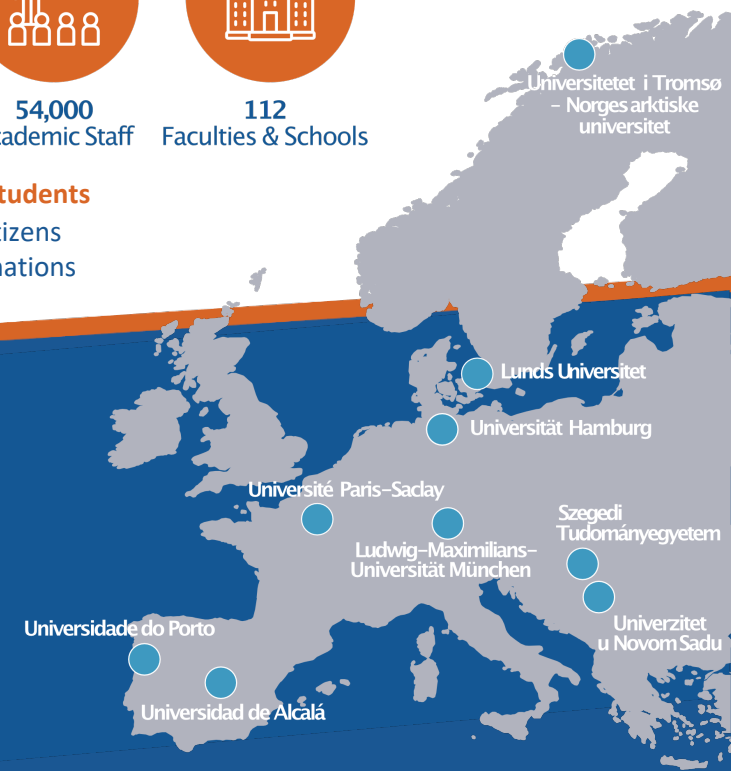
EUGLOH 2.0 Consortium Partners



→ UNS & UiT are from non-member states of the European Union



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



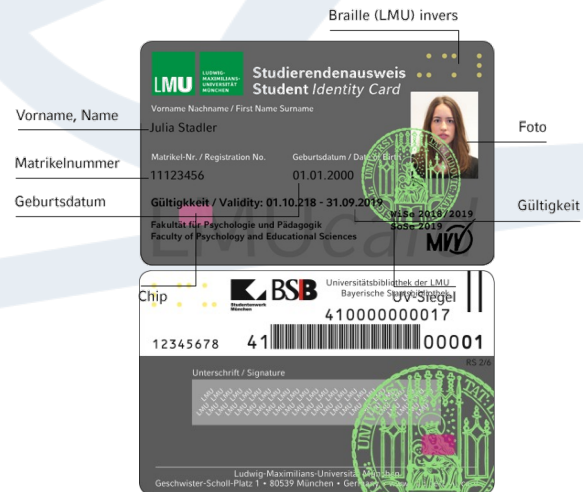
Key Goals

- Interdisciplinary Global Health programmes across universities – striving towards a joint European degree.
- **A vibrant, multicultural and inclusive inter-university campus.**
- **Seamless mobility** for students, staff and professionals – physical and virtual. } Interoperable services and identification → passes & service cards
- Strong links between higher education, research and local socio-economic ecosystems to prepare young people for the jobs of tomorrow.
- Empowering future generations to find solutions for Global Health challenges.

EUGLOH campus cards current state and connected services

→ Vision:

All university members should be able to use services of host university while on visit



Ludwig-Maximilians-Universität München

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

Université Paris-Saclay

- NXP Mifare DESfire Cards
- Payment (izly – les Crous)
- Library user number
- 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
- Library
- Physical Access Control
- Canteen & cafeterias
- Printing Service
- Attendance



European University Alliance for Global Health

9 Universities, 1 Goal: Building Europe's Campus for Global Health

*A vibrant, multicultural and inclusive inter-university campus.
Seamless mobility for students, staff and professionals – physical and virtual.*

- ✓ Vision of the European Commission: Towards a European Education Area
- ✓ The European Student Card Initiative (ESCI)
- ✓ European Charter for Higher Education (ECHE) of the Erasmus+ Program



**A great vision!
That does not work,
but is worth to be fulfilled**

Why does it not work?

*What is necessary to
make it happen?*

Another approach for the objectives

Understand the problems / the requirements

Understand the critical points

- **Stakeholder**
 - Users
 - Higher Education Institutions
 - Service Providers (*on and off campus + online*)
- **Provided Services**
 - Which services
 - Requirements for service provision
 - Requirements for identity or entitlement verification
 - Security Requirements
- Involved Technology and Technology Providers

Services

Higher Education Institutions should **provide services** to their **own (outgoing)** and **incoming students**

- ✓ **Identification and status verification / prove of entitlement**
- ✓ Electronic payment / cashless campus
 - ✓ canteen, cafeteria and vending machines
 - ✓ printer / scanner
- ✓ Library and learning spaces
- ✓ Access-Control
 - ✓ Areas / buildings / rooms → also special services for disabled persons
 - ✓ Single Sign On / 2FA / FIDO2
 - ✓ Attendance check (check-in for exams, attendance at courses)
- ✓ Public transport
- ✓ Accommodation
- ✓ **Electronic Signature** of legal documents (→ eIDAS)
- ✓ *Discounts on cultural activities throughout the EU → Museums, theaters, cinemas, ...*

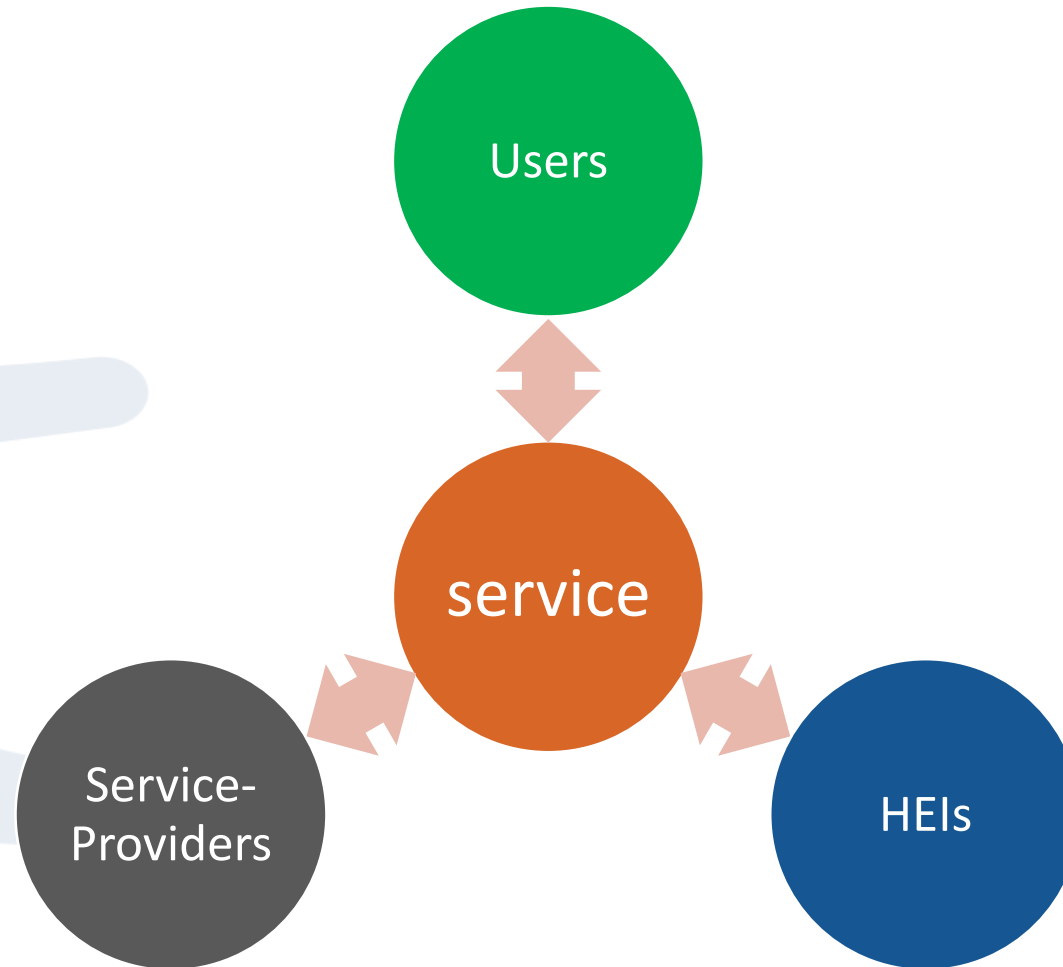


Are Students the only service consumers?

→ **Analyze Users**

→ **Analyze and cluster Services**

Stakeholders

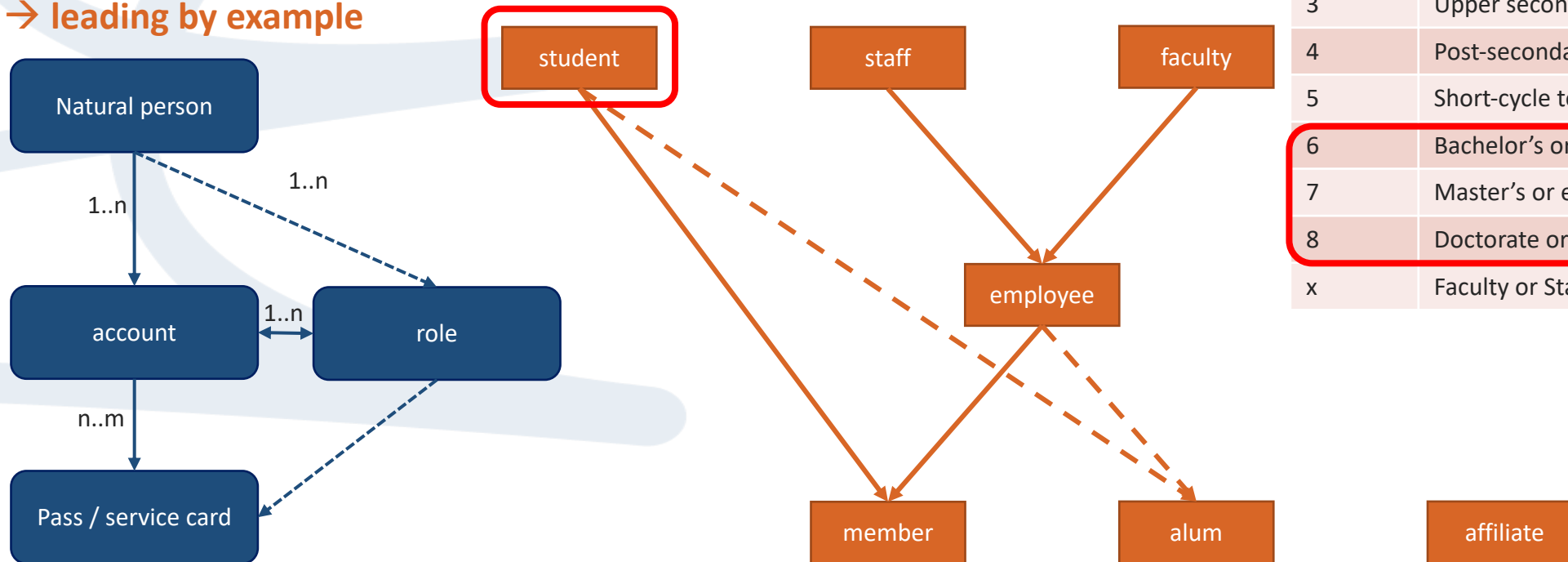


Stakeholder → User Scope

- Why focus on students and ISCED:2011 Level 6-8?
- It is about **providing services**
 - For users of the (home or host) institution
 - User incoming for a short-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



Services

Higher Education Institutions should **provide services** to their **own (outgoing)** and **incoming students**

- ✓ **Identification and status verification / prove of entitlement**
- ✓ Electronic payment / cashless campus
 - ✓ canteen, cafeteria and vending machines
 - ✓ printer / scanner
- ✓ Library and learning spaces
- ✓ Access-Control
 - ✓ Areas / buildings / rooms → also special services for disabled persons
 - ✓ Single Sign On / 2FA / FIDO2
 - ✓ Attendance check (check-in for exams, attendance at courses)
- ✓ Public transport
- ✓ Accommodation
- ✓ **Electronic Signature** of legal documents (→ eIDAS)
- ✓ *Discounts on cultural activities throughout the EU → Museums, theaters, cinemas, ...*

**Analyze and cluster
Services**



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 (secure & follow me printing)



Physical Access Control

- Areas (campus, parking lot)
- Buildings
- Rooms
 - Classrooms
 - Labs
 - Computer rooms
 - Learning spaces
 - Offices
 - Accommodation facilities (i.e., dorms)
- Sports 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
online services

providing service → create benefits



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 (secure & follow me printing)



Physical Access Control

- Areas (campus, parking lot)
- Buildings
- Rooms
 - Classrooms
 - Labs
 - Computer rooms
 - Learning spaces
 - Offices
 - Accommodation facilities (i.e., dorms)
- Sports facilities



Library services

- Access to / borrow
 - Physical media (book, audio and video media)
 - E-media (book, audio and video media)
- Special case of "Proof of entitlement"
- Learning spaces
- Special case of "PAC"



Transport

- On campus services (university shuttle service)
- Special case of "Proof of entitlement"
- Public transport tickets & discounts
- Special case of "Payment" / "discount"



Discount and promotions

- Discounts on cultural activities
 - Museums
 - theaters
 - cinemas
- Shops
- Restaurants
- Special case of "Identification" / "Status verification" / "Proof of entitlement"

on- & off-campus → on-site usage
online services

providing service → create benefits



Out of Scope – Services and Credentials / documents / processes

- Transcripts of Record (Document, transfer / transmission)
- Diplomas
- Testimonials
- Attendance certificates

Involved Technology and Technology Providers

- Required interoperability (definition: interoperability is a characteristic of a product or system to work with other products or systems.)
- It is about providing services

*All the projects and talks are about Cards / eCards / Passes, but does a card provide a service or does it just **provide access to the service provision***

Does cards / passes need to be interoperable?

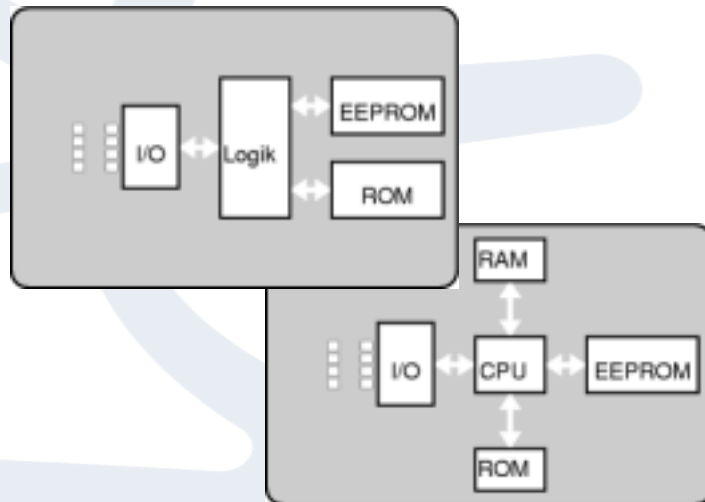
→ *Data cards (contactless or contact-based) are interoperable by definition, they work together with a reader*

→ *But should an **identifier / identification medium** be **shared** by different systems or generally **reused**?*

GDPR / Self-sovereign-identity → NO

Involved Technology and Technology Providers

Physical cards



vs.

Smartphone



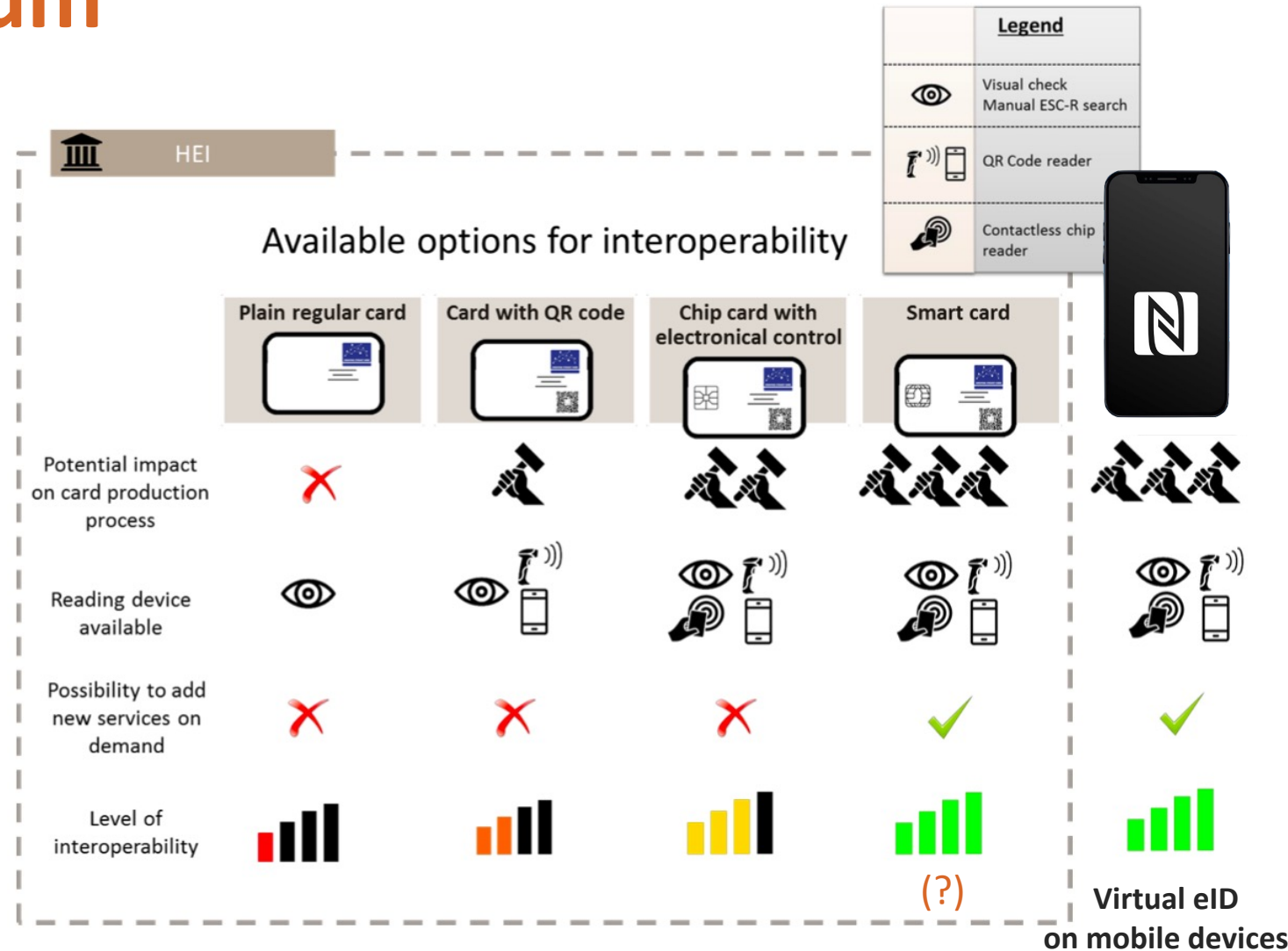
Question of the medium

Possible technological implementations:

1. Plain Card with Hologram
2. Plain Card with Hologram + QR-Code
3. Chip card (with Hologram + QR-Code)
 1. Chip card technology neutral
 2. Mifare DESfire chip card with App
 3. Multi-technology chip card with App
4. Smart card (with Hologram + QR-Code + App)
5. Virtual eID (Smartphone) ✓

→ Costs are an essential point for decisions

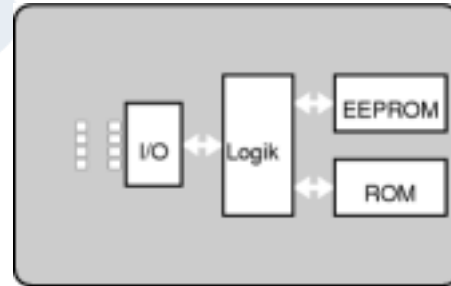
→ Smartphones are cheap for HEIs



Physical card side?

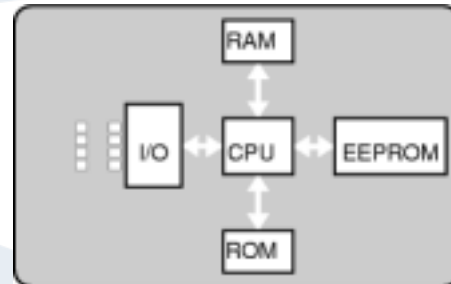
Chip cards → bind to one certain technology

- NXP Mifare DESfire
- Legic Advant
- HID iClass
- ...



Smartcards → expensive

- JCOP



→ Plastic cards are not the solution, so...

- ✓ Sustainability
 - ✓ Interoperability
- } Responsibility

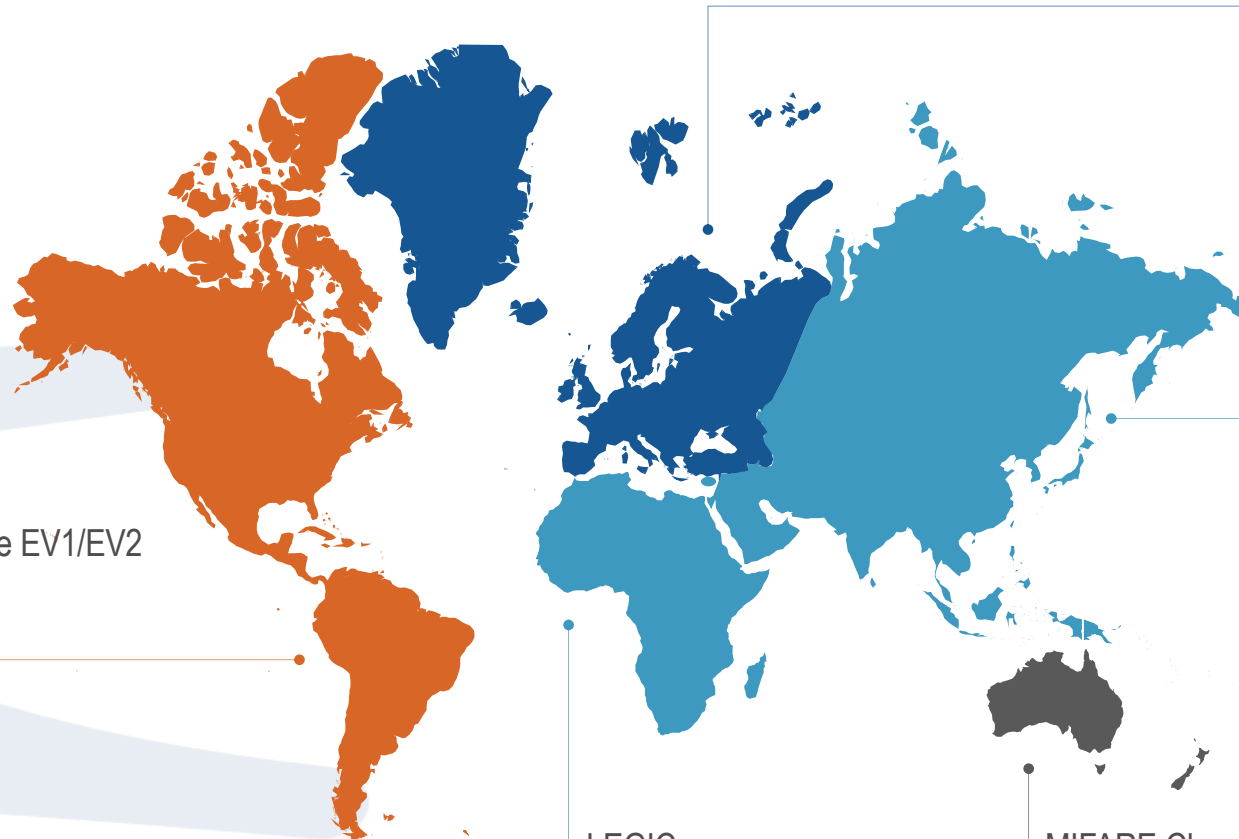
Cards – Communication Protokolls and Data / File Systems

Different standards of Transponder technologies – “standards” – not Compatible to each other

MIFARE Classic
 MIFARE DESFire EV1/EV2
 HID iCLASS
 HID Prox
 Indala
 ioProx
 AWID
 Keri
 CASI-RUSCO

MIFARE Classic
 MIFARE DESFire EV1/EV2
 HID Prox
 EM4102

ISO 14443A ECM-340
 ISO 14443B ECMA-352
 ISO 15693 ISO 11784
 ISO 18000 ISO 11785
 ISO 18092 NFC Tag Types 1-5



MIFARE Classic
 MIFARE DESFire EV1/EV2
 LEGIC
 Calypso
 Moneo
 Oyster
 HID Prox
 EM4102

LEGIC
 MIFARE Classic
 MIFARE DESFire EV1/EV2
 SONY Felica
 TIRIS
 CEPAS
 Octopus
 EM4102

LEGIC
 MIFARE Classic
 MIFARE DESFire EV1/EV2
 EM4102

MIFARE Classic
 MIFARE DESFire EV1/EV2
 HITAG
 HID Prox

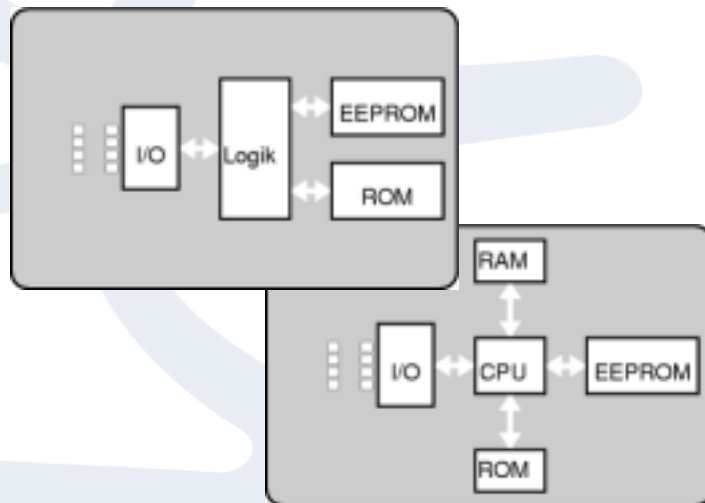
Card Interoperability happens on the reader side

- 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



Involved Technology and Technology Providers

Physical cards



Limited memory / computing capabilities

vs.

Smartphone



→ Card Emulation

Technology wise

→ **Clear winner**

vs

almost unlimited memory / computing capabilities

Medium → 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 (secure & follow me printing)



Physical Access Control

- Areas (campus, parking lot)
- Buildings
- Rooms
 - Classrooms
 - Labs
 - Computer rooms
 - Learning spaces
 - Offices
 - Accommodation facilities (i.e., dorms)
- Sports facilities



Library services

- Access to / borrow
 - Physical media (book, audio and video media)
 - E-media (book, audio and video media)
- Special case of “Proof of entitlement”
- Learning spaces
- Special case of “PAC”



Transport

- On campus services (university shuttle service)
- Special case of “Proof of entitlement”
- Public transport tickets & discounts
- Special case of “Payment” / “discount”



Discount and promotions

- Discounts on cultural activities
 - Museums
 - theaters
 - cinemas
- Shops
- Restaurants
- Special case of “Identification” / “Status verification” / “Proof of entitlement”

on- & off-campus → on-site usage
online-services



providing service → create benefits

Medium → 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 (secure & follow me printing)



Physical Access Control

- Areas (campus, parking lot)
- Buildings
- Rooms
 - Classrooms
 - Labs
 - Computer rooms
 - Learning spaces
 - Offices
 - Accommodation facilities (i.e., dorms)
- Sports facilities



Library services

- Access to / borrow
 - Physical media (book, audio and video media)
 - E-media (book, audio and video media)
- Special case of "Proof of entitlement"
- Learning spaces
- Special case of "PAC"



Transport

- On campus services (university shuttle service)
- Special case of "Proof of entitlement"
- Public transport tickets & discounts
- Special case of "Payment" / "discount"



Discount and promotions

- Discounts on cultural activities
 - Museums
 - theaters
 - cinemas
- Shops
- Restaurants
- Special case of "Identification" / "Status verification" / "Proof of entitlement"

on- & off-campus → on-site usage
online-services



providing service → create benefits

Medium → 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 (secure & follow me)

Physical Access Control

- Areas (campus, parking lot)
- Buildings
- Rooms
 - Classrooms
 - Labs

Library services

- Access to / borrow
 - Physical media (book, audio and video media)
 - E-media (book, audio and video media)
- Special case of

Transport

- On campus services (university shuttle service)
- Special case of "Proof of entitlement"
- transport tickets
- of "discount"

Discount and promotions

- Discounts on cultural activities
 - Museums
 - theaters
 - cinemas
- Shops
- Restaurants
- Special case of "Identification" / "Status verification" / "Proof of entitlement"

Legacy problem

→ Not easy / quick to replace

Legacy systems

- Legacy identifiers
- Technical limitations
- Specific solutions

→ Working solutions by solutions providers



Benchmark – Student IDs

The ISIC+ITIC Cards (International Student / Teacher Identity Card)

Both

- ✓ physical medium (card)
- ✓ virtual medium (native Smartphone App) available

Provided Data:

- Higher Education Institution (Name)
- Name
- Photo
- Date of birth
- Signature (back)
- Validity

Accepted by third party service providers for **discount and promotions**

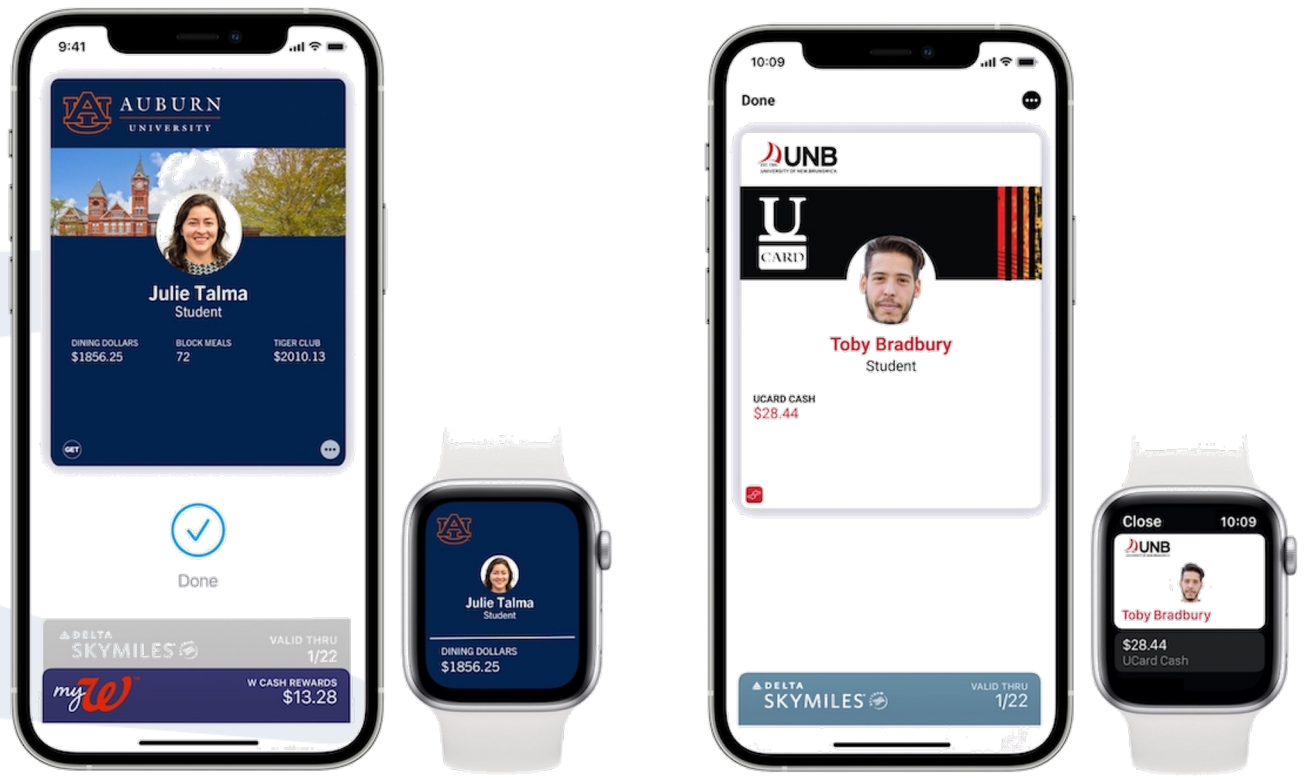


Benchmark – Users Expectations

- Don't stick to old technology if your user expects something modern
 - Integration and Interoperability
 - **Smartphone** is the essential working tool for younger generations
 - Higher Education Institutions should provide credentials in modern ways
 - **Student IDs / Campus IDs should be recognized and accepted anywhere**
-
- ✓ Be compliant
 - ✓ Be Secure → implement IT-Security best practices
 - ✓ Respect privacy
 - ✓ Respect self sovereignty and decisions of users

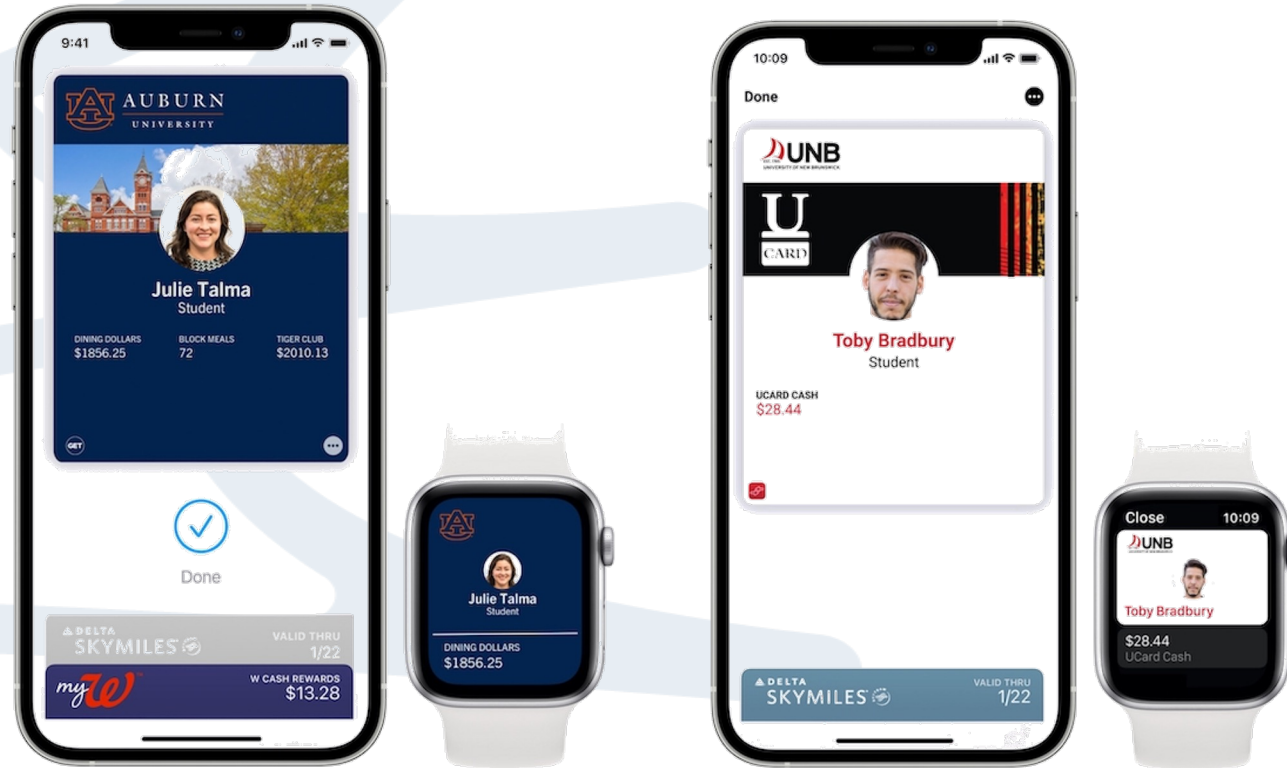


Enhanced Benchmark – Student IDs



Student IDs – Enhanced Benchmark

- ✓ Sustainable & Interoperable Virtual eID on Mobile Devices in USA
- ✓ Fulfil User Expectations



Campus ID Solution by TRANSACT

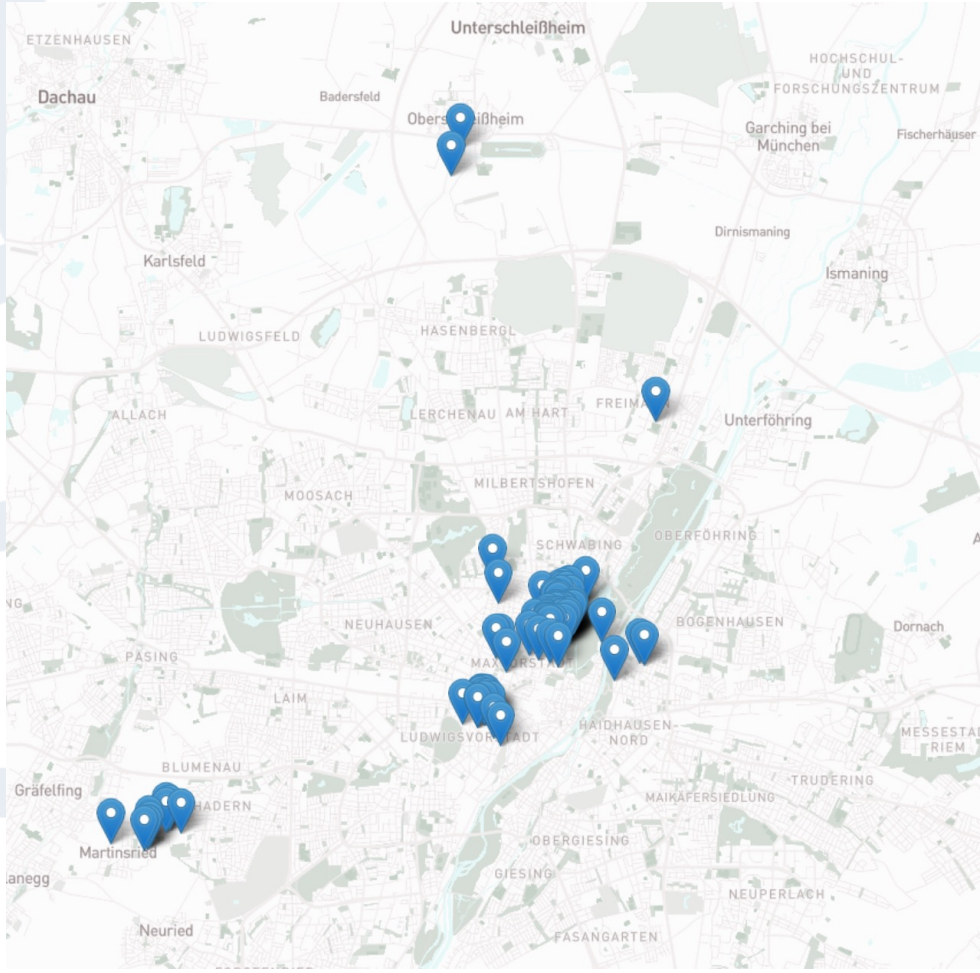
Features

- Physical Access Control
- Library
- Payment
- Printing and Copy, Vending, and Laundry
- On Campus Transport

→ The Difference:
Universities in the USA are campus universities, a clearly demarcated area, the universities act more commercially oriented as **full-service providers**



as Counter Example in Europe

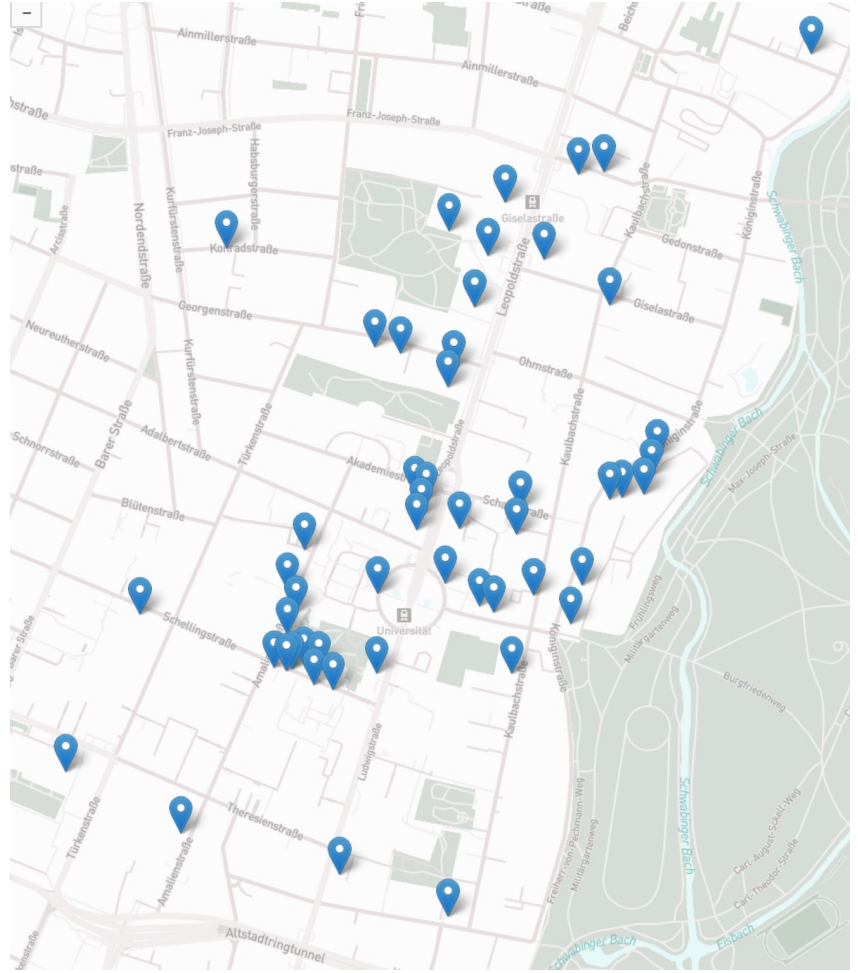


Most European Universities do not have a clearly demarcated campus area, they are just in the city.

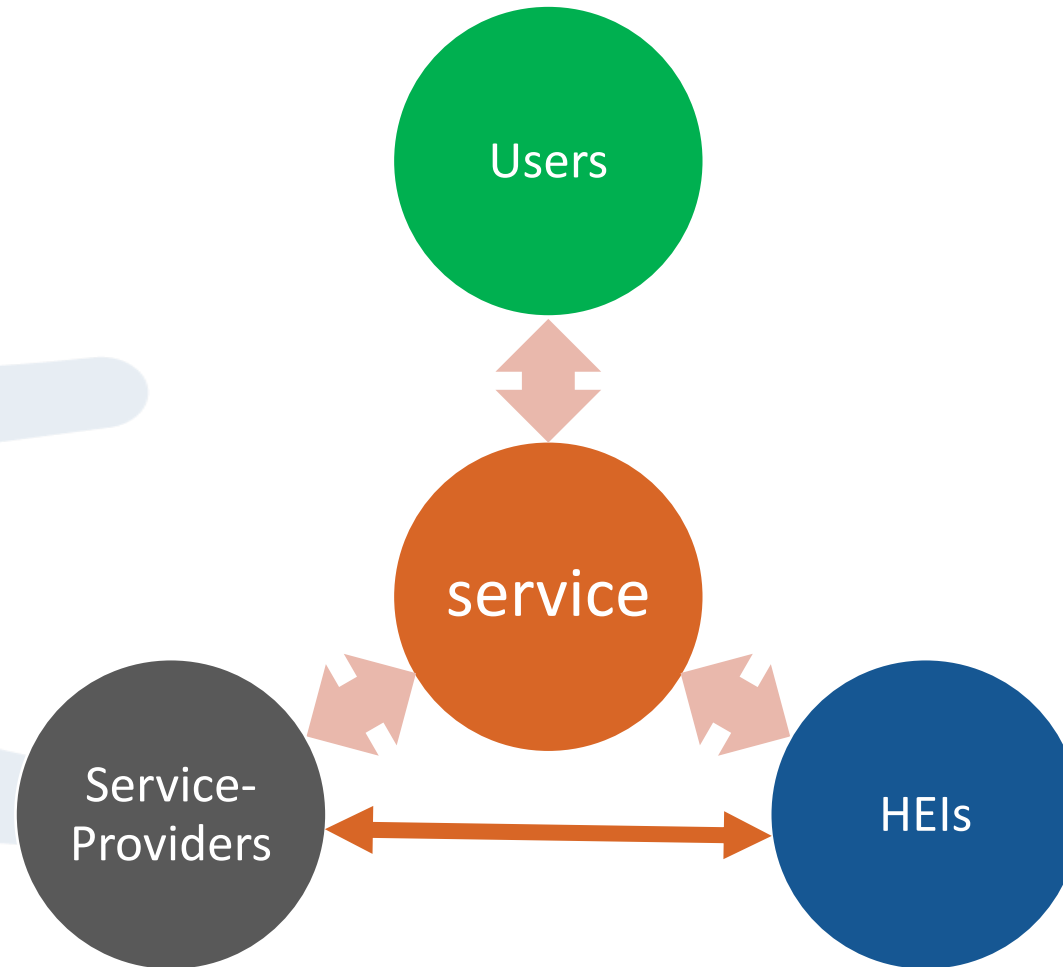
The University is not even the main service provider for student live.

Typical Service-Provider:

-  (=Student 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:
 -  **BSB** Bayerische Staatsbibliothek
Information in erster Linie
 - Bavarian State Library**
- Transport → Public Transport System



Stakeholders



Medium → Services ← Stakeholder Example

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

Service-Provider



(secure & follow me printing)

Physical Access Control

- Areas (campus, parking lot)

Service-Provider



- Offices
- Accommodation facilities

Library services

- Access to / borrow
- Physical media (book)

Service-Provider



- Learning spaces

Transport

Service-Provider



- Public transport tickets & discounts
- Special case of "Identification" / "discount"

Discount and promotions

- Discounts on cultural activities
 - Museums
 - theaters
 - cinemas
- Shops
- Restaurants
- Special case of "Identification" / "Status verification" / "Proof of entitlement"

Legacy problem

→ Not easy / quick to replace

Legacy systems

- Legacy identifiers
- Technical limitations
- Specific solutions

On integrated cards, the oldest service defines the technology baseline & options

→ Working solutions by solutions providers





European University Alliance for Global Health

9 Universities, 1 Goal: Building Europe's Campus for Global Health

*A vibrant, multicultural and inclusive inter-university campus.
Seamless mobility for students, staff and professionals – physical and virtual.*



LMU's International network

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

EU projects

European University Alliance for Global Health (EUGLOH)



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) 
- THE EUROPAEUM 

Infinity partners → infinity stakeholders → infinity systems

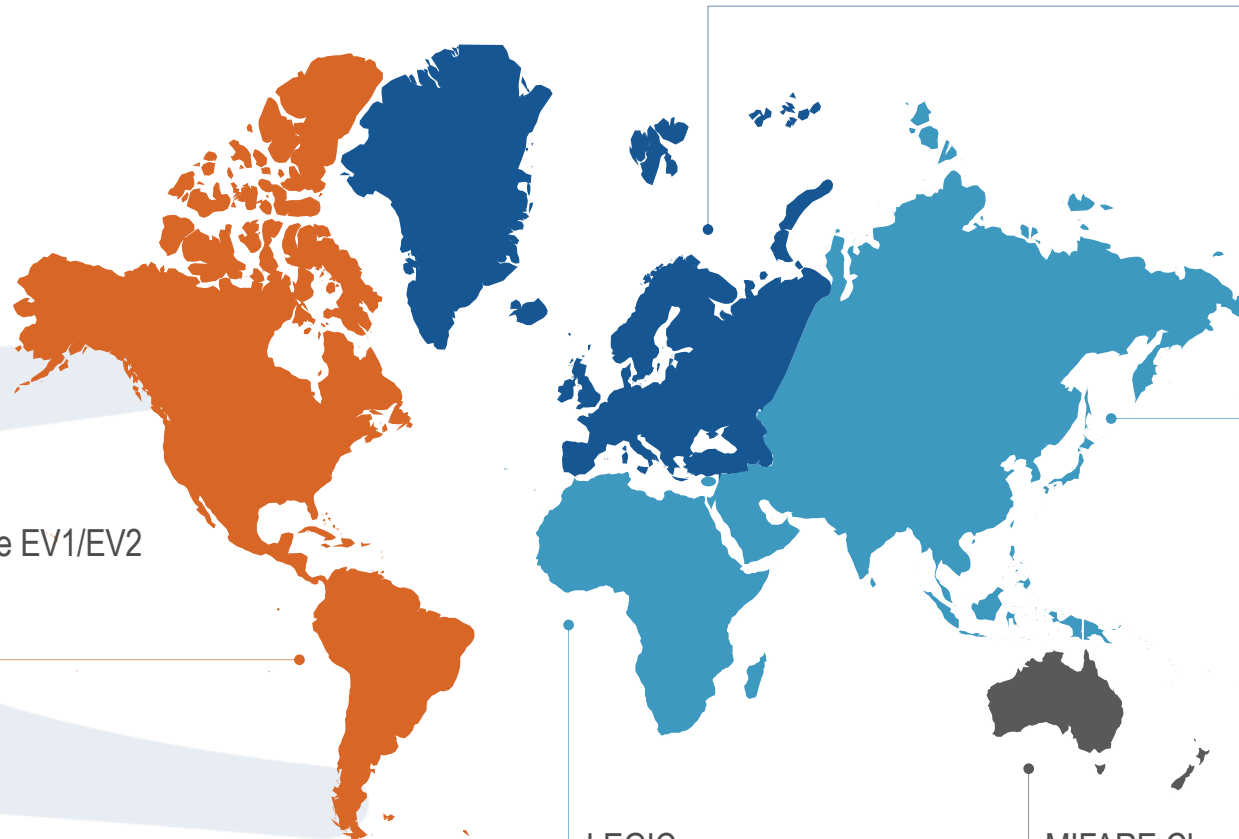
Cards – Communication Protokolls and Data / File Systems

Different standards of Transponder technologies – “standards” – not Compatible to each other

MIFARE Classic
 MIFARE DESFire EV1/EV2
 HID iCLASS
 HID Prox
 Indala
 ioProx
 AWID
 Keri
 CASI-RUSCO

MIFARE Classic
 MIFARE DESFire EV1/EV2
 HID Prox
 EM4102

ISO 14443A ECM-340
 ISO 14443B ECMA-352
 ISO 15693 ISO 11784
 ISO 18000 ISO 11785
 ISO 18092 NFC Tag Types 1-5



MIFARE Classic
 MIFARE DESFire EV1/EV2
 LEGIC
 Calypso
 Moneo
 Oyster
 HID Prox
 EM4102

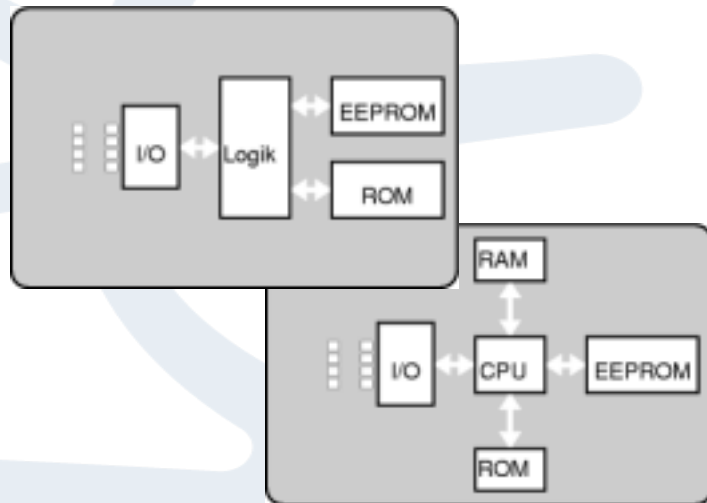
LEGIC
 MIFARE Classic
 MIFARE DESFire EV1/EV2
 SONY Felica
 TIRIS
 CEPAS
 Octopus
 EM4102

LEGIC
 MIFARE Classic
 MIFARE DESFire EV1/EV2
 EM4102

MIFARE Classic
 MIFARE DESFire EV1/EV2
 HITAG
 HID Prox

Involved Technology and Technology Providers

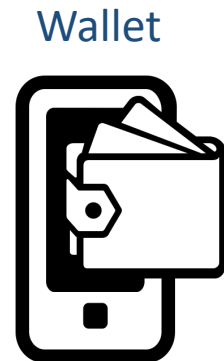
Physical cards



vs.

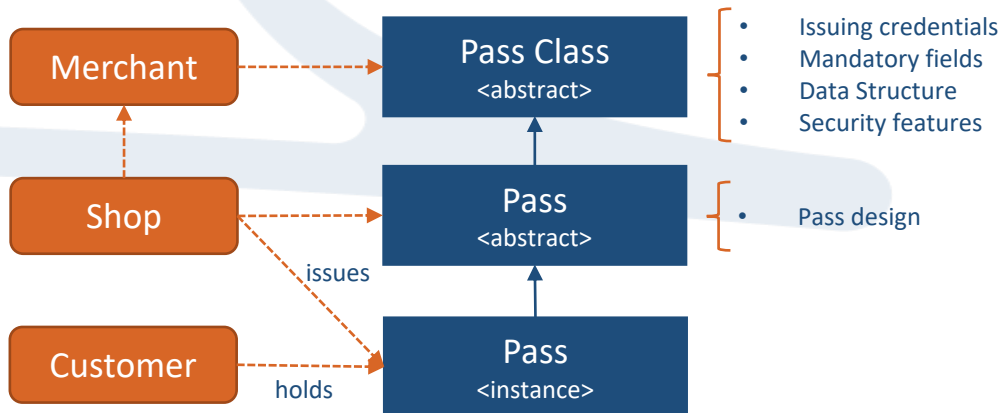
Smartphone

→ infinity systems ?



Technical details and features of Wallets / Passes

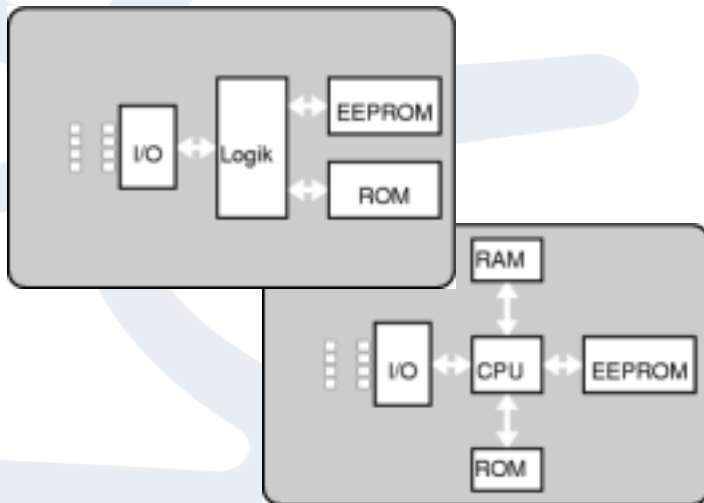
- **Smart / Quick Select option (Express-Mode)**
- Battery reserve
- Authentication requirements ← security features
- Groupable
- Validity dates
- Remote updateable / revokable
- Offline usable
- Host Card Emulation



Pass <ul style="list-style-type: none"> • Smart Select / Express Mode Selector • Design – visual presentation • Data-Slot → Smart Tap / VAS / Mifare / mDoc (ISO/INC 18013-5) 			
Wallet-App <ul style="list-style-type: none"> • Account-binding • Presentation • ... 	Wallet-App	Wallet-App	Wallet-App
Operating System Layer (OS) <ul style="list-style-type: none"> • API for 		OS Wallet API	
Hardware-Layer (access to) <ul style="list-style-type: none"> • NFC / BLE / UWB • Secure Element / Security Chip • Subscriber Identity Module SIM/eSIM 			

Involved Technology and Technology Providers

Physical cards



vs.

Smartphone

An own app / wallet-app would only be justifiable if the OEM-Wallets / EU-eID-Wallet would not be legally useable

→ infinity systems ?

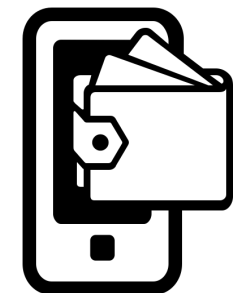
App is no solution that scales, otherwise it would be a wallet-app itself.



App

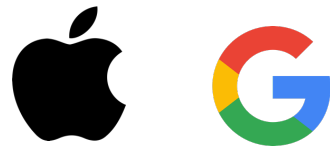


Wallet



EUGLOH - Working Group Partners

Technology Partners



RFID Systems



Not yet partners

Service Providers Partners



Solution Providers Partners



Medium → 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 & fast)
- Ticketing (secure & fast)

Physical Access Control

- Areas (campus, parking lot)
- Buildings
- ROOMS
- Classrooms

Library services

- Access to / borrow
 - Physical media (book, audio and video)
 - E-media (book, audio and video)

Transport

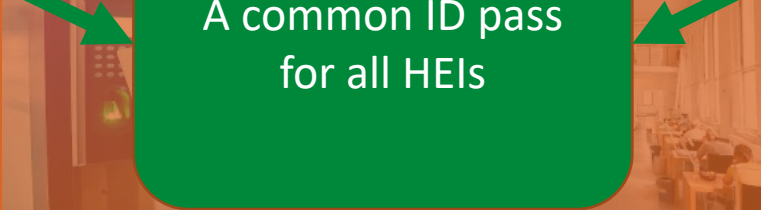
- On campus services (university shuttle service)
- "Proof of entitlement" for transport tickets
- Special case of "discount"

Discount and promotions

- Discounts on cultural activities
 - Museums
 - theaters
 - cinemas
- Shops
- Restaurants
- Special case of "Identification" / "Status verification" / "Proof of entitlement"

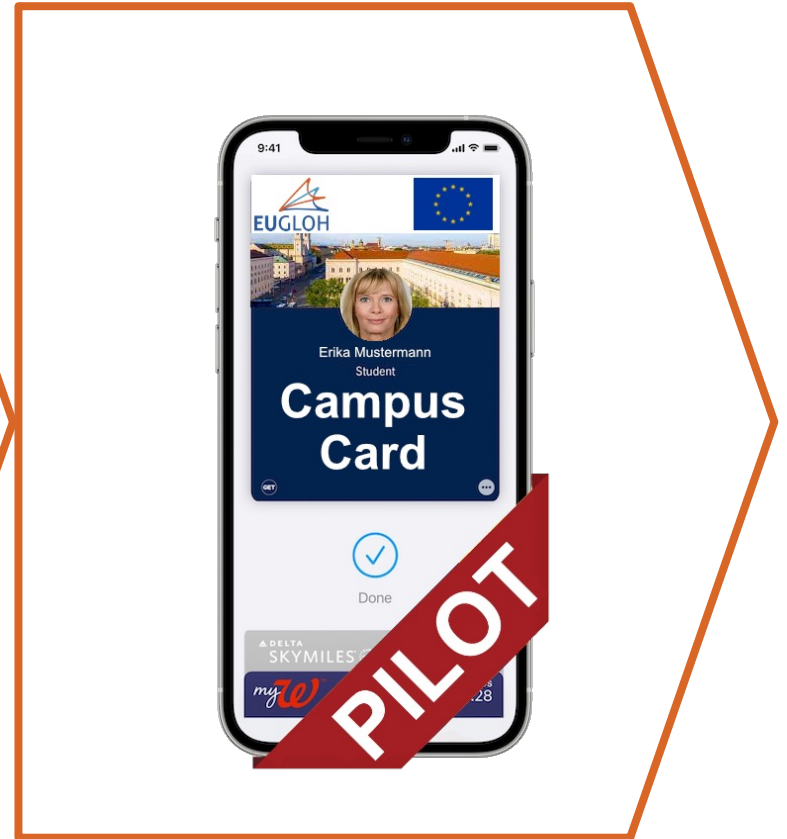
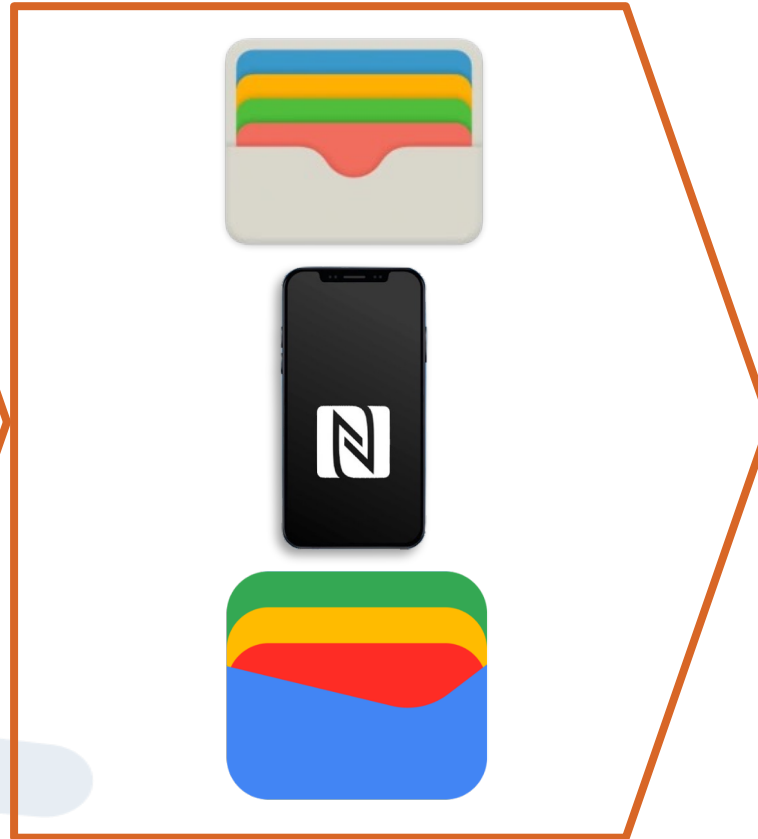
Working solutions by solutions providers
 → separate service pass (can chose appropriate technology)

A common ID pass for all HEIs



providing service → create benefits

The Future of ID & service cards – Wallet passes



Solving the issue

How to implement a scalable solution for Higher Education

→ Classical digitalization project

Disclaimer

NDA restricted – confidential - knowledge

Prototypes and Pilots

Not publicly available

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

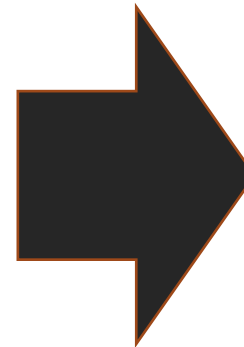
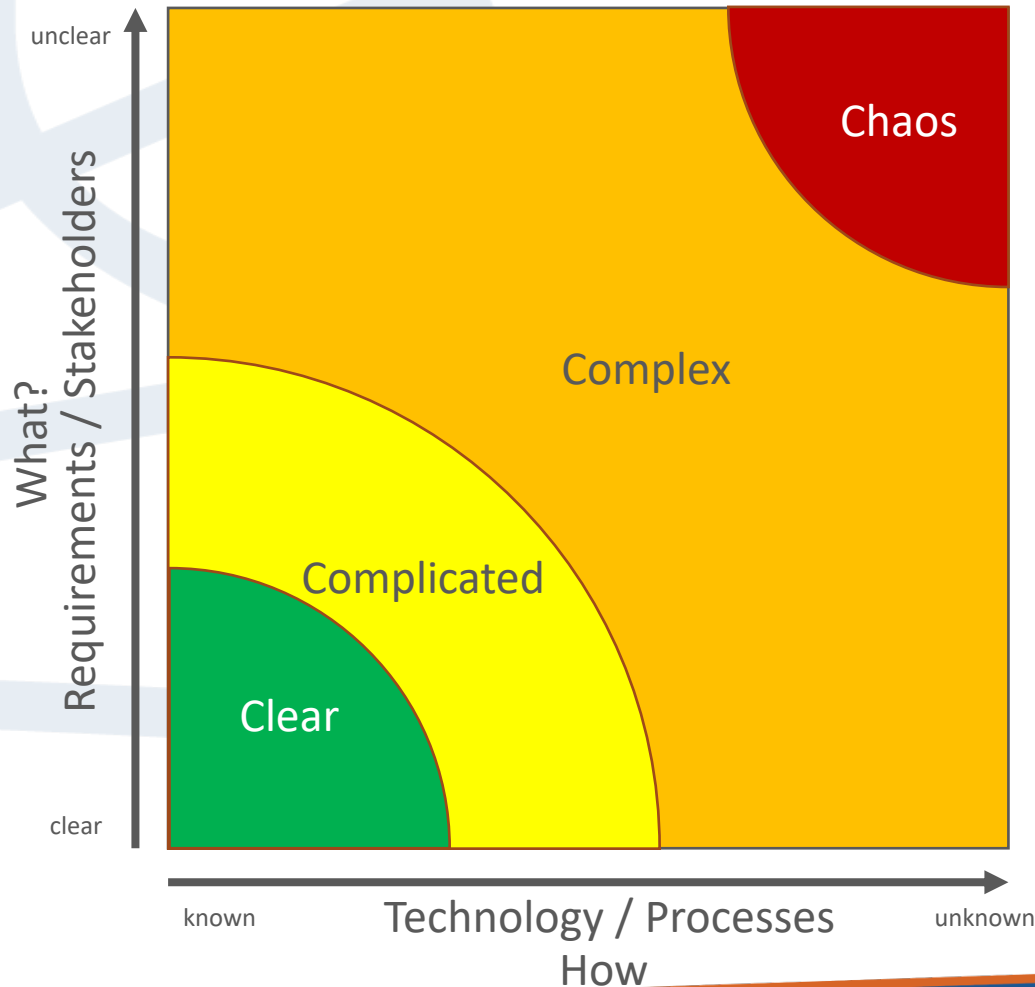
If I have seen further it is by standing on the shoulders of Giants.

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

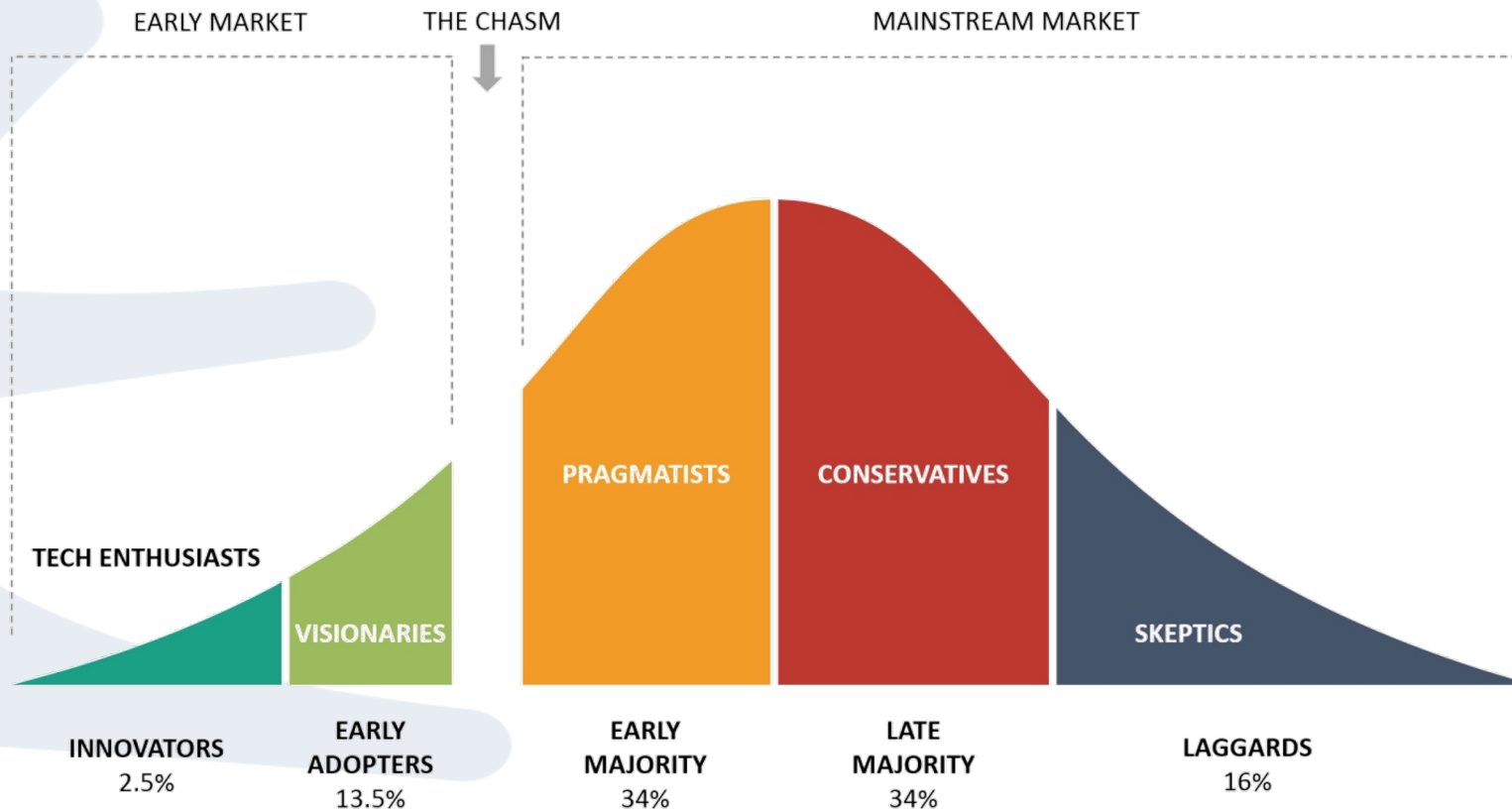


Success factors – Understand the complexity

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



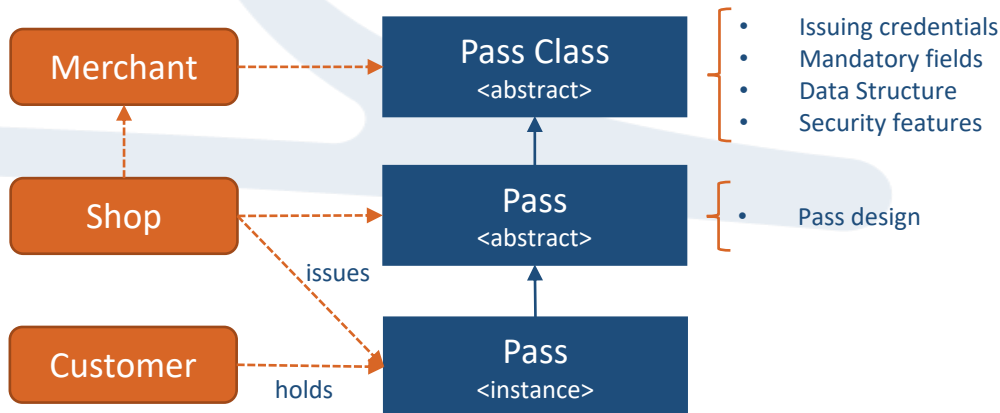
Technology



Source: <https://thinkinsights.net/strategy/crossing-the-chasm/>

Technical details and features of Wallets / Passes

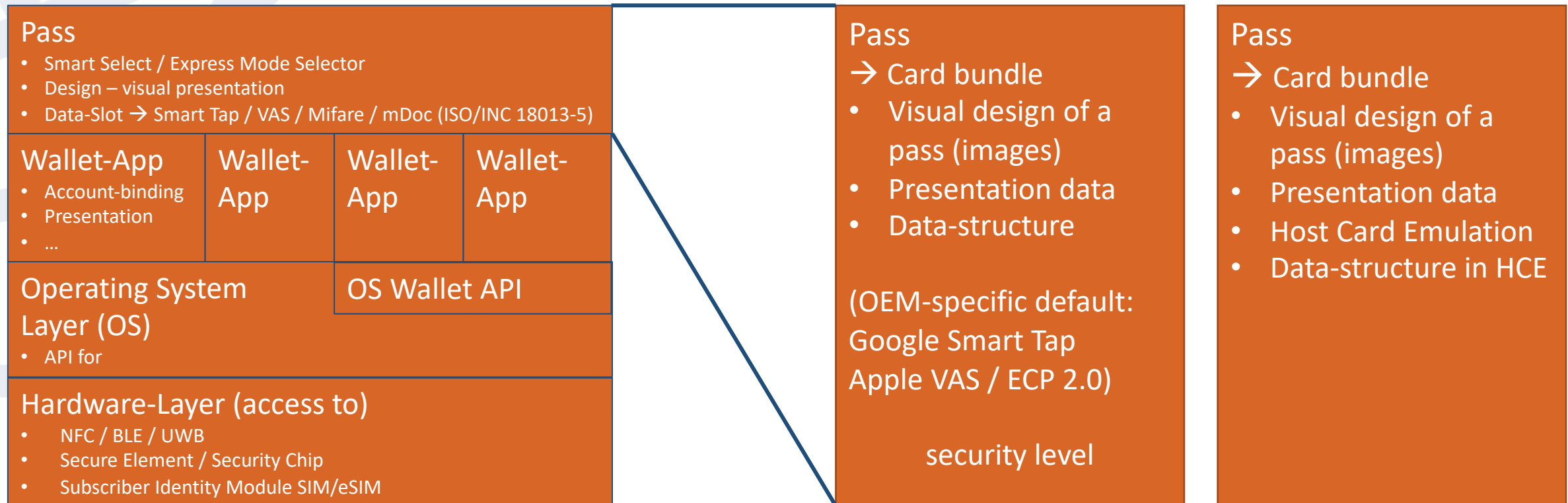
- **Smart / Quick Select option (Express-Mode)**
- Battery reserve
- Authentication requirements ← security features
- Groupable
- Validity dates
- Remote updateable / revokable
- Offline usable
- Host Card Emulation



Pass <ul style="list-style-type: none"> • Smart Select / Express Mode Selector • Design – visual presentation • Data-Slot → Smart Tap / VAS / Mifare / mDoc (ISO/INC 18013-5) 			
Wallet-App <ul style="list-style-type: none"> • Account-binding • Presentation • ... 	Wallet-App	Wallet-App	Wallet-App
Operating System Layer (OS) <ul style="list-style-type: none"> • API for 		OS Wallet API	
Hardware-Layer (access to) <ul style="list-style-type: none"> • NFC / BLE / UWB • Secure Element / Security Chip • Subscriber Identity Module SIM/eSIM 			

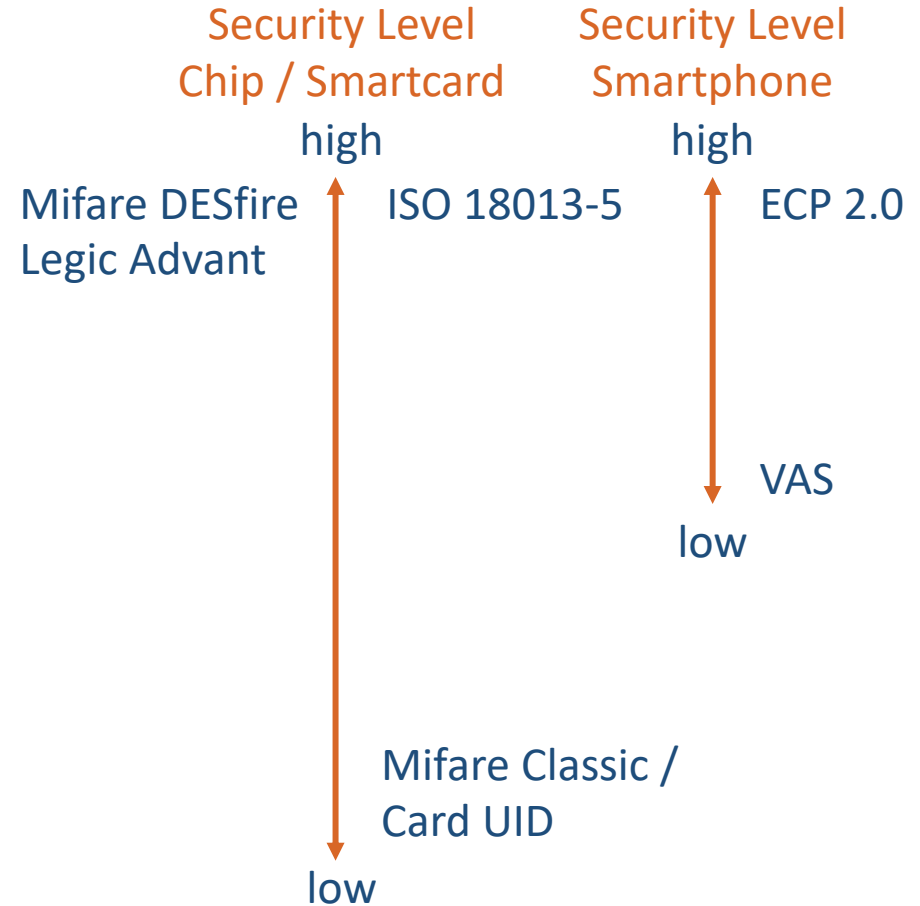
Technical details of Wallet passes

Detail view on the Pass

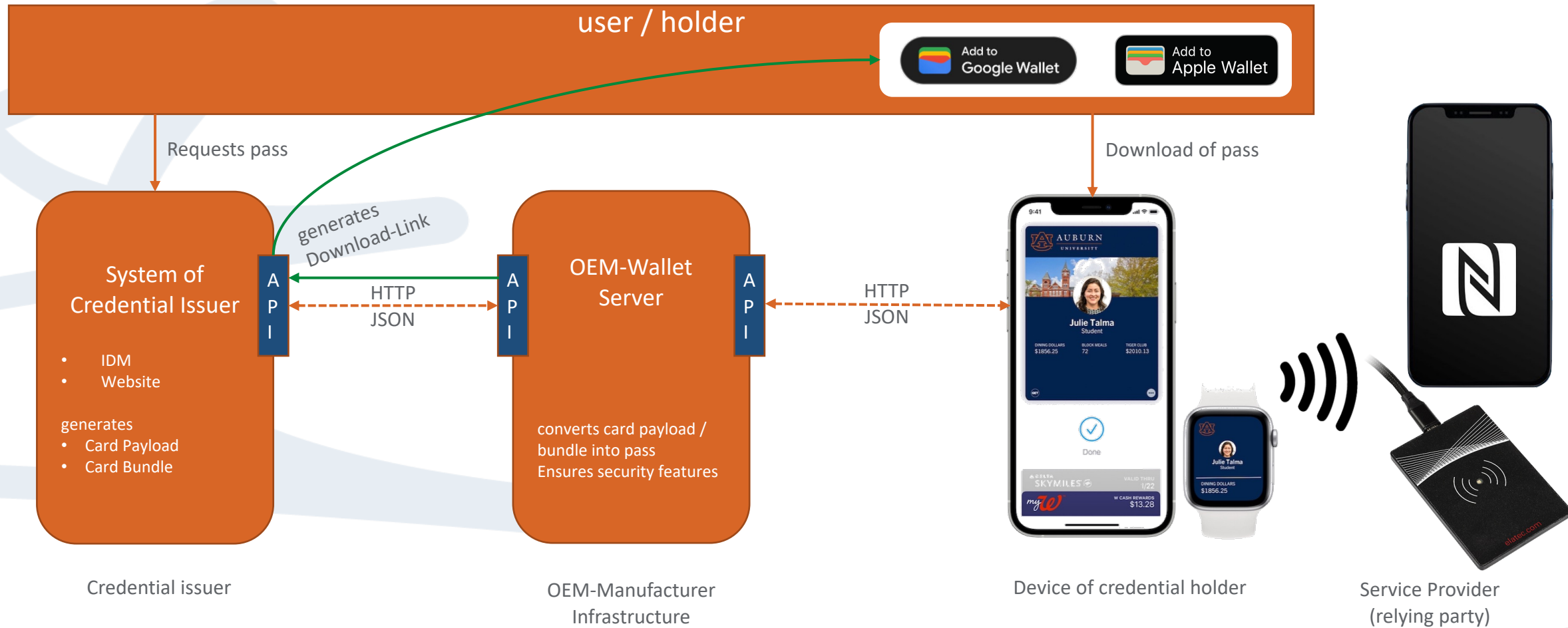


Technical details of Wallet passes

- 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)
 - Mifare DESfire (via Mifare2GO / NXP secure element)
- ISO 18013-5 Personal Identification
Core functionality in Android and iOS OS API
- Security consideration required by use case



Issuing process of wallet passes



Apple and Google have good ideas, but

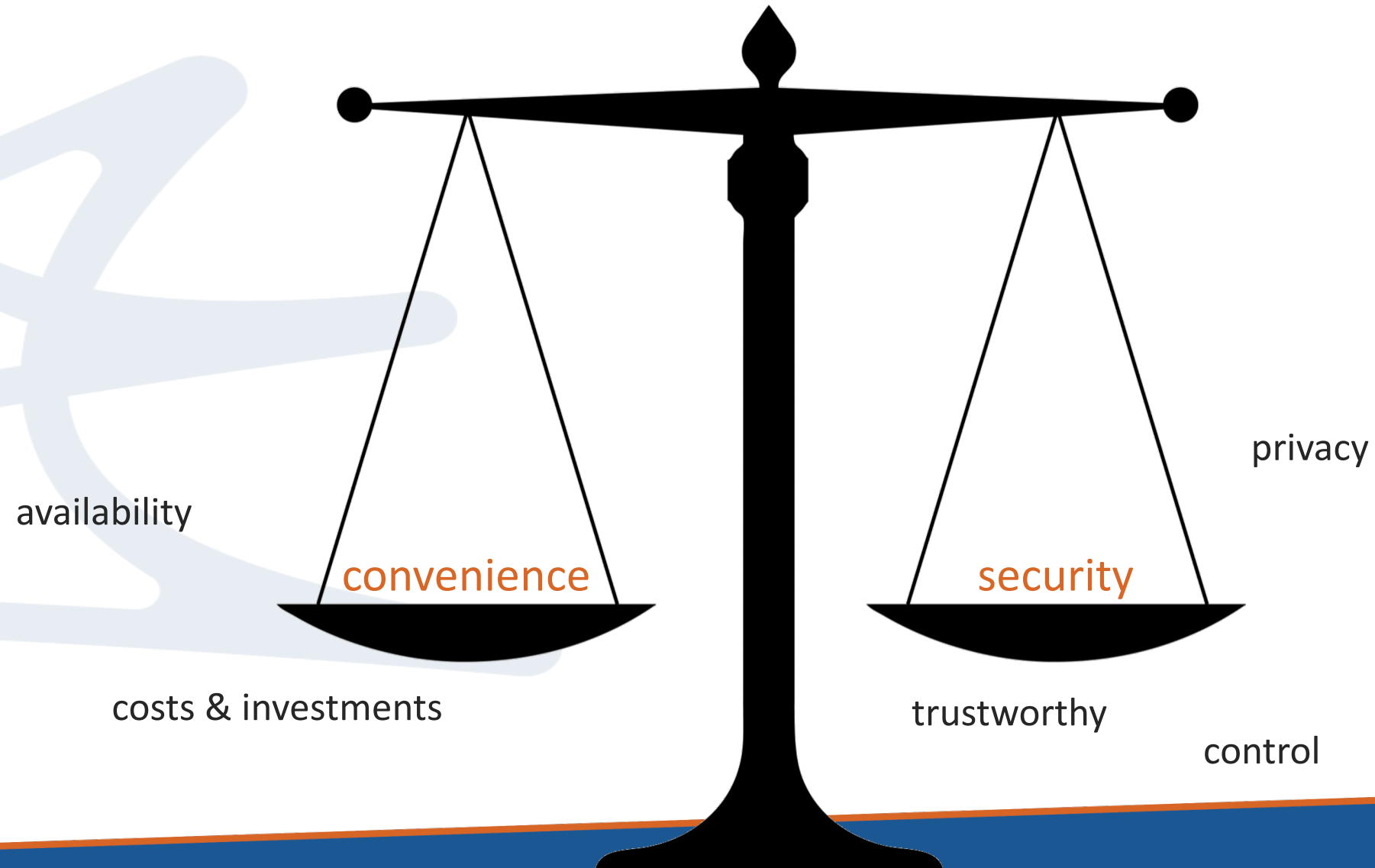
ONE SIZE DOES
NOT FIT ALL



One size
does **NOT**
fit all.



balance of objectives



Risk assessment
must be done by
service providers

Medium → 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 & fast)
- Ticketing (secure & fast)

Physical Access Control

- Areas (campus, parking lot)
- Buildings
- ROOMS
- Classrooms

Library services

- Access to / borrow
 - Physical media (book, audio and video)
 - E-media (book, audio and video)

Transport

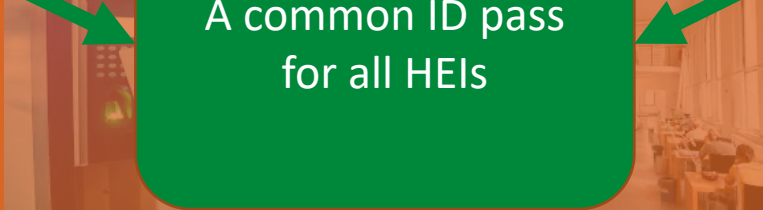
- On campus services (university shuttle service)
- Transport tickets
- "Proof of entitlement"
- "discount"

Discount and promotions

- Discounts on cultural activities
 - Museums
 - theaters
 - cinemas
- Shops
- Restaurants
- Special case of "Identification" / "Status verification" / "Proof of entitlement"

Working solutions by solutions providers
 → separate service pass (can chose appropriate technology)

A common ID pass for all HEIs



providing service → create benefits

Identity & Identification

Identification

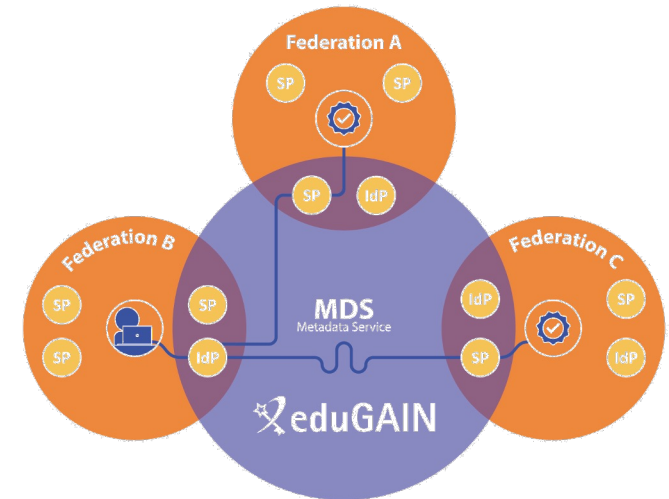
Status verification

Proof of entitlement

technology and information for Identification

User and Role bind services → Identity Management

- Existing technologies:
 - Directory Services → LDAP (Protocol and Schema definitions)
- LDAP-Schema for Higher Education
 - eduPerson (V4.3 from 30. November 2021; V1.0 from December 2007)
 - SCHAC – SCHEMA for ACademia (V1.6.0-proposed from 24. March 2022 / V1.5.0 from 15. April 2015; V1.0 from May 2006)
 - SAML – Security Assertion Markup Language
- Essential **LDAP-Schema Attributes**:
 - eduPersonAffiliation / eduPersonScopedAffiliation → Roles
 - eduPersonEntitlement → Mapped Entitlements ← **Services provided**
 - eduPersonAssurance → **Assurance Class / Level of Data**
 - schacHomeOrganization
 - schacPersonalUniqueCode → **European Student Identifier**
→ additional Identifiers necessary
 - Pairwise Id → Pseudonym
 - Subject Id → Unique Person Identifier



European Student Identifier (ESI)



The European Student Identifier (ESI) can take on one of two forms, depending on the qualifiers needed to make a given student code globally unique:

- ESI with **nation-wide (or region-wide) scope** student code

urn:schac:personalUniqueCode:int:esi:<country-code>:<code>

(for countries that support a national student identifier, e.g., France, Finland, Greece, Italy, Netherlands and Spain → University of Paris-Saclay case)

- ESI with **HEI-wide scope** student code

urn:schac:personalUniqueCode:int:esi:<shO>:<code>

(for most countries that have institution level student identifiers, e.g., Portuguese/Uporto case, German/LMU Munich + HU Berlin case)

Géant recommends NRENs to enforce the adoption of ESI

→ Additional schema scopes necessary for other roles

Attribute Release Test Service Provider

This page is intended for Identity Provider operators, who want to test the attribute release of their Identity Provider towards the MyAcademicID service.

Attribute Release Status for Students

Please find below a list of the [get:https://www.refeds.org/](https://www.refeds.org/) for the MyAcademicID service, marking any problems found with the attribute values that were received.

- The identifier of the user is released
- The name of the user is released
- The email of the user is released
- The student affiliation of the user is released
- The schacHomeOrganization of the user is released
- The European Student Identifier of the user is released

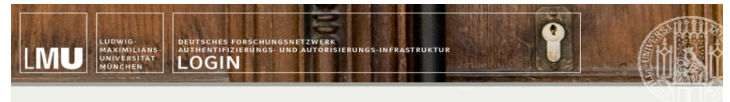
Attributes received:

Attribute	Value(s)
urn:oid:1.3.6.1.4.1.31921.1.1.1.10 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.11 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.12 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.13 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.14 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.15 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.16 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.17 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.18 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.19 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.20 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.21 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.22 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.23 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.24 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.25 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.26 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.27 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.28 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.29 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.30 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.31 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.32 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.33 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.34 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.35 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.36 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.37 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.38 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.39 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.40 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.41 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.42 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.43 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.44 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.45 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.46 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.47 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.48 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.49 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.50 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.51 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.52 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.53 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.54 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.55 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.56 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.57 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.58 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.59 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.60 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.61 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.62 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.63 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.64 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.65 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.66 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.67 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.68 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.69 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.70 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.71 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.72 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.73 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.74 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.75 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.76 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.77 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.78 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.79 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.80 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.81 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.82 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.83 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.84 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.85 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.86 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.87 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.88 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.89 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.90 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.91 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.92 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.93 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.94 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.95 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.96 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.97 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.98 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.99 [schacHomeOrganization]	• https://www.refeds.org/
urn:oid:1.3.6.1.4.1.31921.1.1.1.100 [schacHomeOrganization]	• https://www.refeds.org/

SAML Subject

NameID: https://www.refeds.org/

Format: urn:mace:namespaces:SAML2.0:nameid-format:persistent



Informationsweitergabe MyAcademicID IAM Service

Beschreibung des Dienstes: The MyAcademicID IAM Service provides Identity and Federated access management for the services of the European Student Card Initiative and the services directly supporting the digitisation of Erasmus+. The MyAcademicID IAM Service is provided by GEANT using the eduTEAMS service. Zusätzliche Informationen über diesen Dienst: <https://wiki.geant.org/display/SM/MyAcademicID+Identity+and+Access+Management+Service>

An den Dienst zu übermittelnde Informationen	
Anzeigename	student member staff employee
Zugehörigkeit	student member staff employee
Vertrauensgrad	https://refeds.org/assurance https://refeds.org/assurance/IAP/low https://refeds.org/assurance/ATP/ePA-1m https://refeds.org/assurance/ID/epm-unique-no-reassign https://refeds.org/assurance/ID/unique https://refeds.org/assurance/ATP/ePA-1d https://refeds.org/assurance/IAP/medium https://refeds.org/assurance/profile/cappuccino
Berechtigung	urn:mace:dir:entitlement:common-lib-terms
Personliche ID	@lmu.de
Zugehörigkeit	staff@lmu.de member@lmu.de student@lmu.de employee@lmu.de
eduPersonTargetedID	HV6nox/05xEhyzkH4z+vIGNdD80=
eduPersonUniqueID	7b719738ecae7b120b6383786b47fe98@lmu.de
Vorname	
E-Mail	@campus.lmu.de
o	uni-muenchen
schacHomeOrganization	lmu.de
schacPersonalUniqueCode	urn:schac:personalUniqueCode:int:esi:lmu.de:
Nachname	

Datenschutzinformationen dieses Dienstes

Die oben aufgeführten Informationen werden an den Dienst weitergegeben, falls Sie fortfahren.

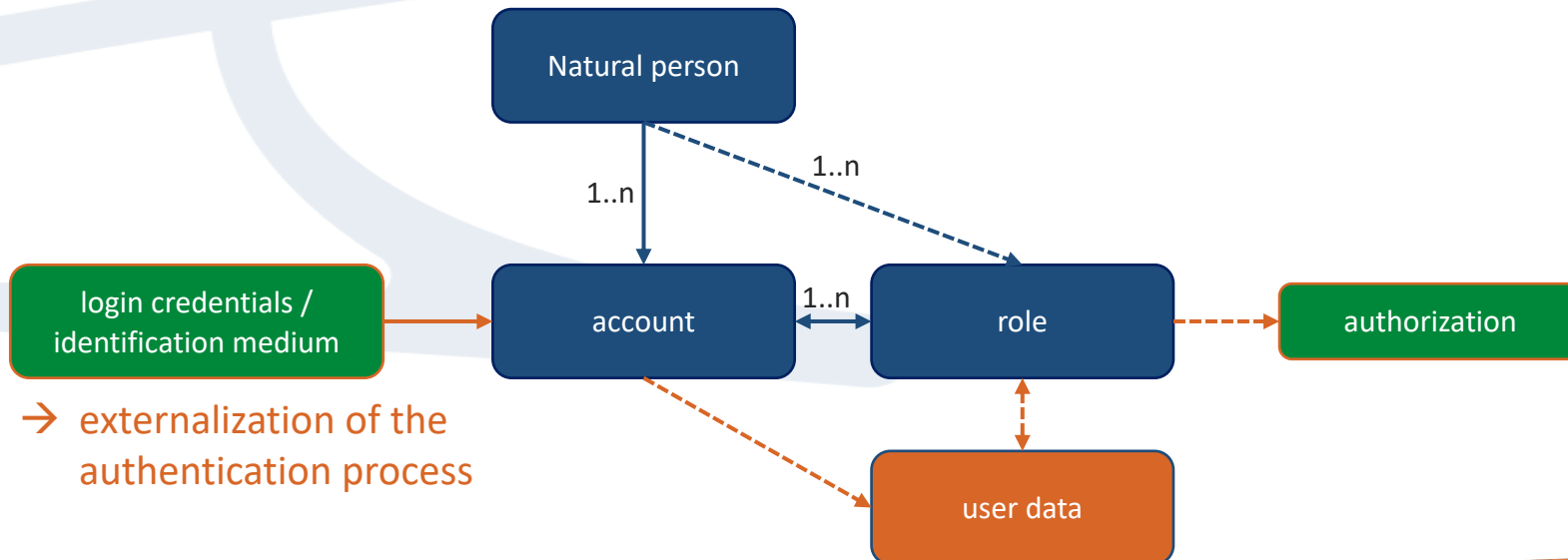
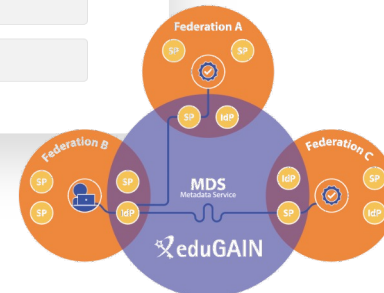
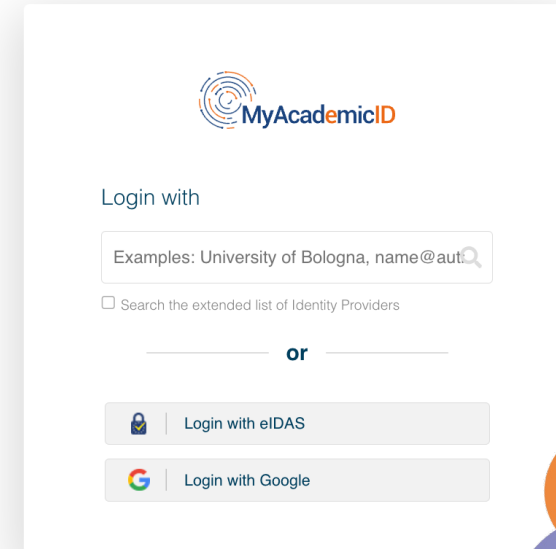
Wählen Sie die Dauer, für die Ihre Entscheidung zur Informationsweitergabe gültig sein soll:

- Bei nächster Anmeldung erneut fragen.
 - Ich stimme zu, dass meine Informationen dieses Mal an den Dienst weitergegeben werden.
- Erneut fragen, wenn sich die Informationen ändern, welche an den Dienst weitergegeben werden.
 - Ich bin einverstanden, dass dieselben Informationen in Zukunft automatisch an diesen Dienst weitergegeben werden.

Diese Einstellung kann jederzeit mit der Checkbox auf der Anmeldeseite widerrufen werden.

Identity Linking → reduced amount of logins

- Utilization of decentralized / federated Authentication and Authorization Infrastructure
 - Less login credentials – higher assurance levels
 - Data flow
- Example application fields (at LMU):
 - Initial account creation for application / enrollment process (SDG / OZG / BayEGovG)
 - Issuing of Library IDs (OZG)
 - Mobility and cooperation processes → Zweithörer Status (HIG)



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.

Federated Authentication and Authorization Infrastructure (AAI) Identity and Access Management

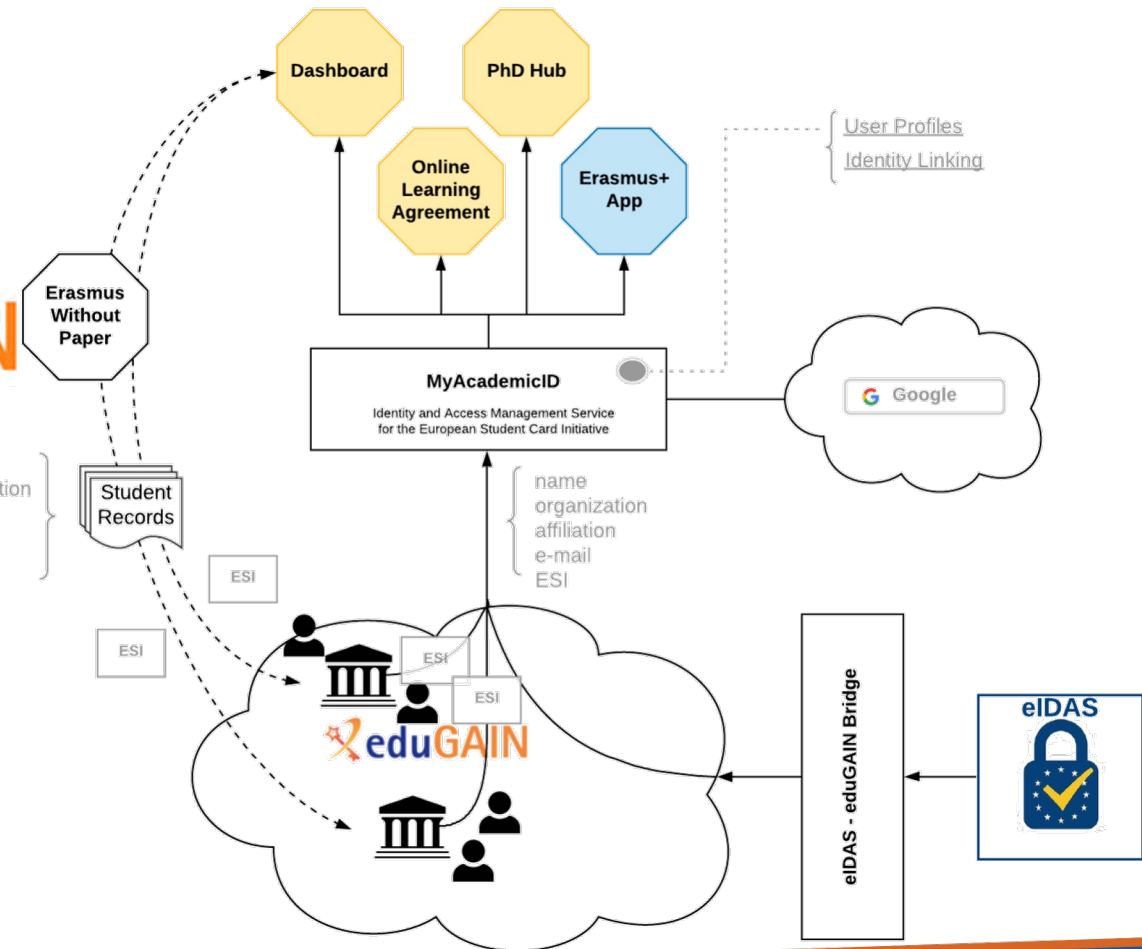
The MyAcademicID Identity and Access Management

- The MyAcademicID IAM Service is **provided by GÉANT** using the eduTEAMS service



- Provides Identity and Federated access management for the services of the European Student Card Initiative and the services directly supporting the digitization of Erasmus+
- Connected services: OLA, PHD Hub and Erasmus+ App, ...

- From a virtual Identity back to an Identification Document
- *quick* Affiliate / Entitlement validation *on site*
- HEI are about mass processes



Technical Details on the core eduCampusCard Pass

The European Campus Card / eduCampusCard Pass

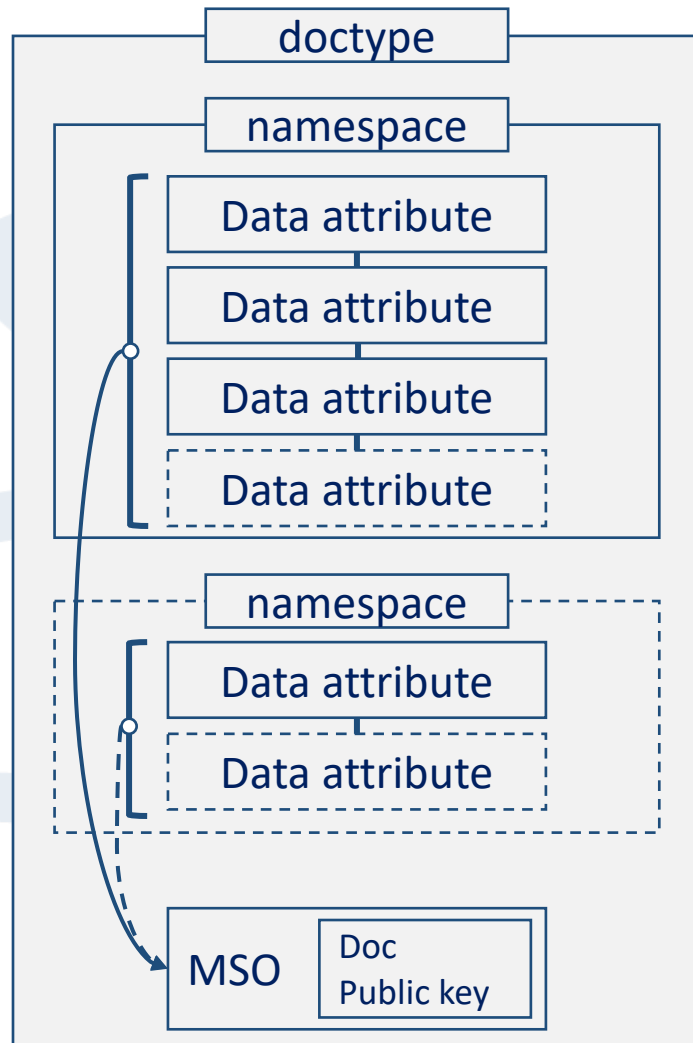
→ Identification Document for all members of a *Higher Education Institution*

- Identity-Document → ISO/IEC 18013-5 - Personal Identification – mDoc Application
- Backwards-Compatible → *maybe a Mifare DESFire Access for a UUID@schacHomeOrganisation*

Common Identification pass using 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**)
 - 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 → mobile driving licence
- Already supported by the OEM-Smartphone-Manufactures (Apple and Google (see: <https://android-developers.googleblog.com/2020/11/privacy-preserving-features-in-mobile.html>))
- No additional infrastructure costs

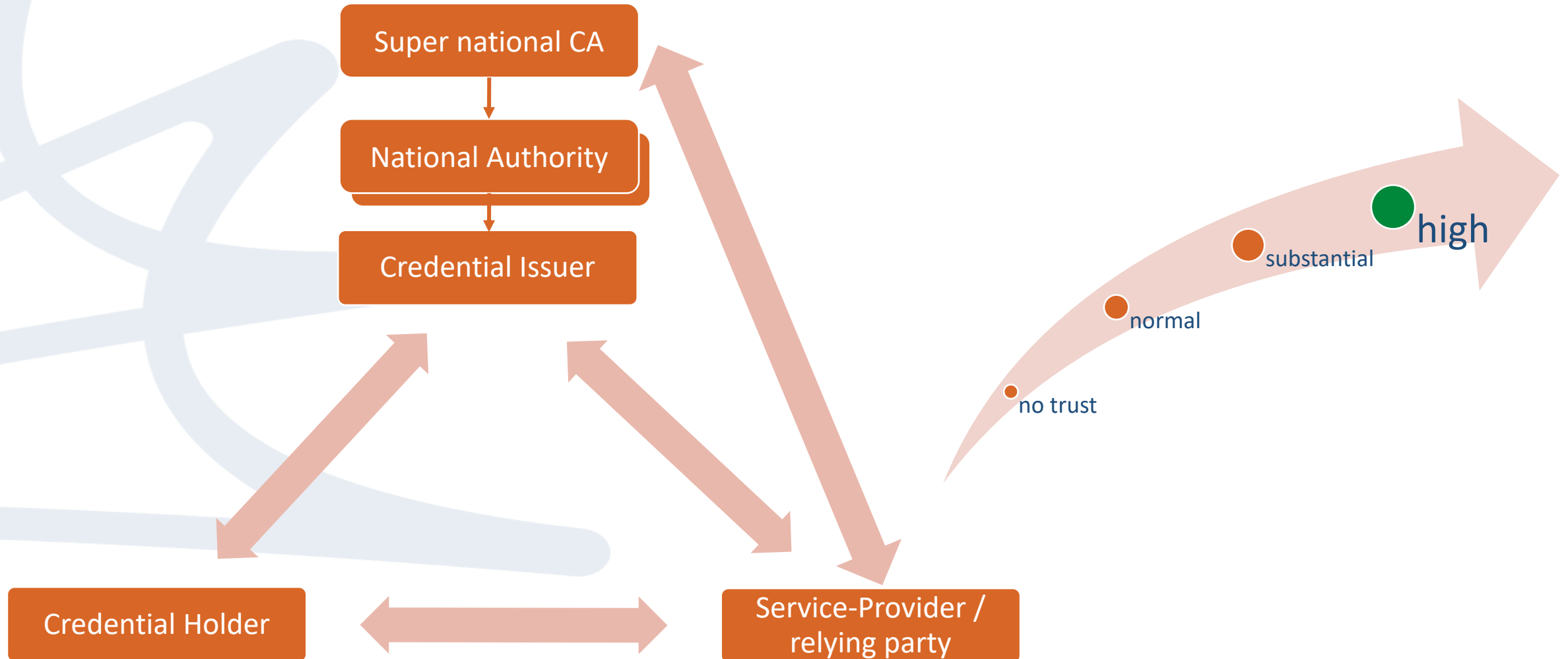
ISO/IEC 18013-5 Data model



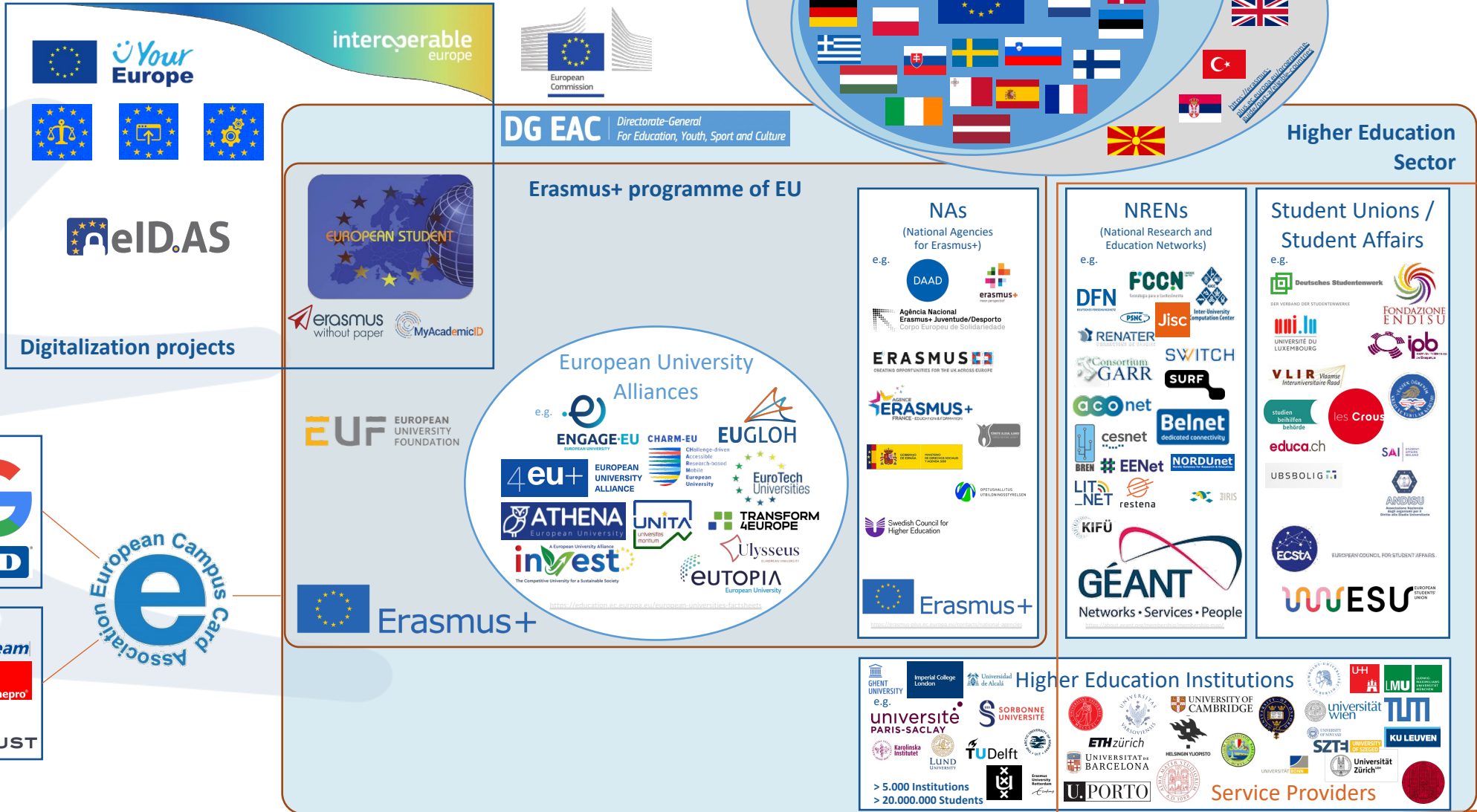
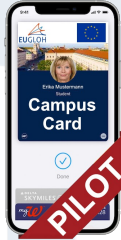
Reuse of directory Data:

- givenNames
- sn
- eduPersonAffiliation / eduPersonScopedAffiliation
- eduPersonEntitlement
- eduPersonAssurance
- schacHomeOrganization
- schacPersonalUniqueCode
- schacDateOfBirth
- schacYearOfBirth
- schacPlaceOfBirth
- schacExpiryDate

Chain of Trust & Trust level



The Stakeholder-Landscape



public transport providers. - cultural institutions (libraries, museums, theaters, cinemas). - shops



GÉANT – The IT provider for Higher Education in Europe

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

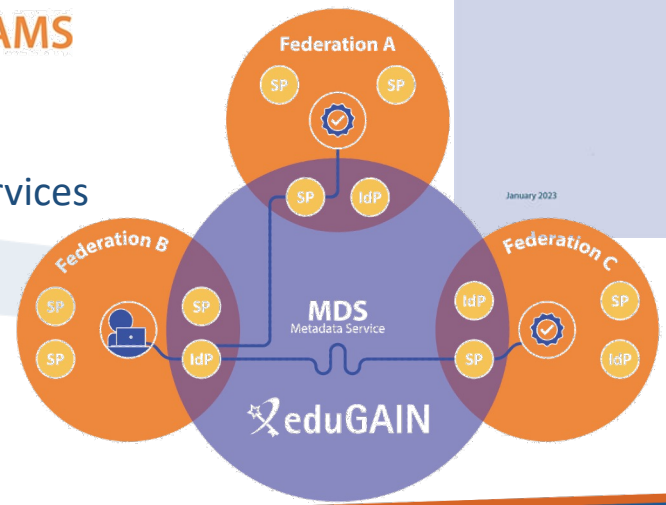
- Non-Profit Organization
- Service-Provider for IT / e-infrastructure services for the European Higher Education Sector

• Key Services:

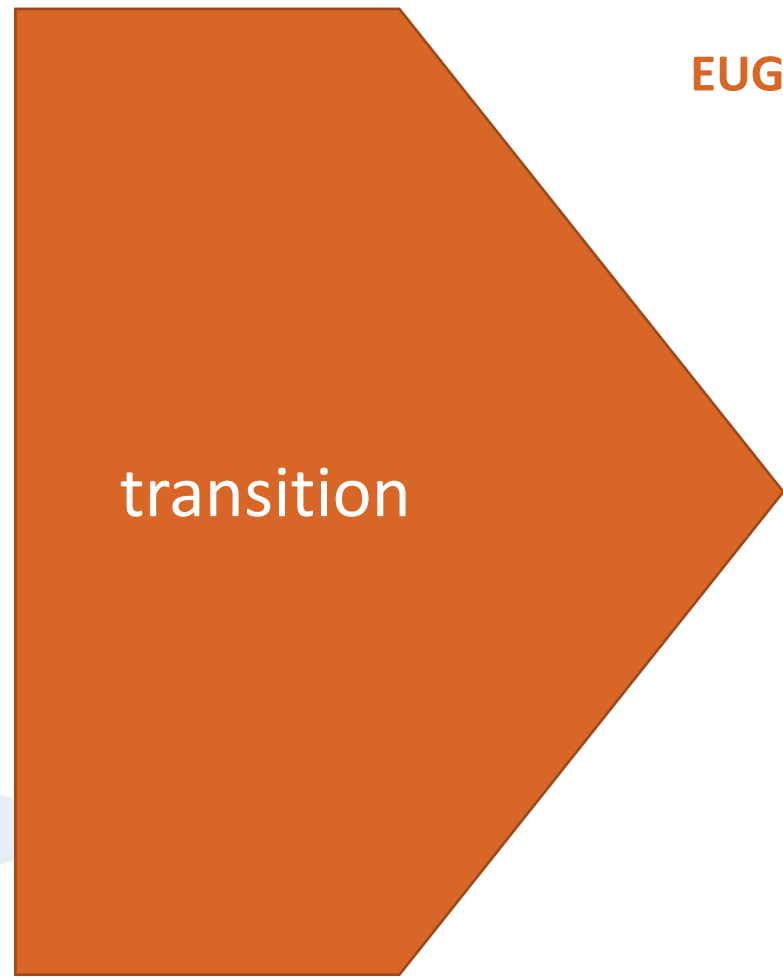
- GÉANT Trust & Identity Services



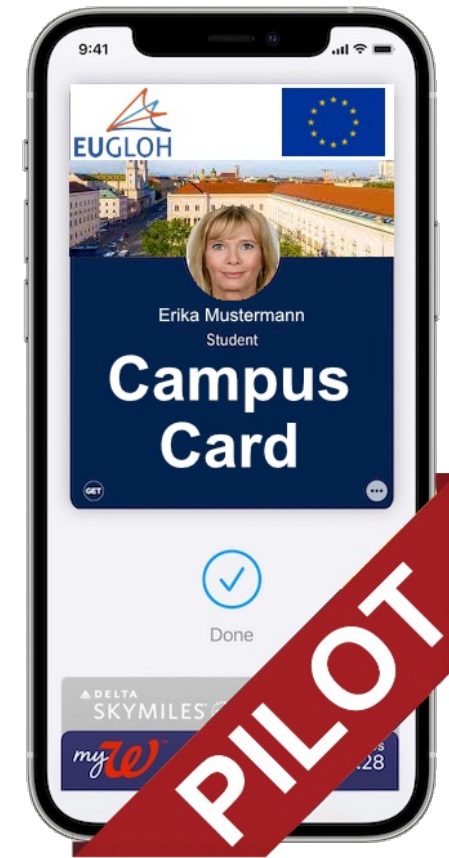
- GÉANT Network and Connectivity Services
- GÉANT Security Services
- GÉANT Cloud Services
- Procurement Agency for EU-HEIs



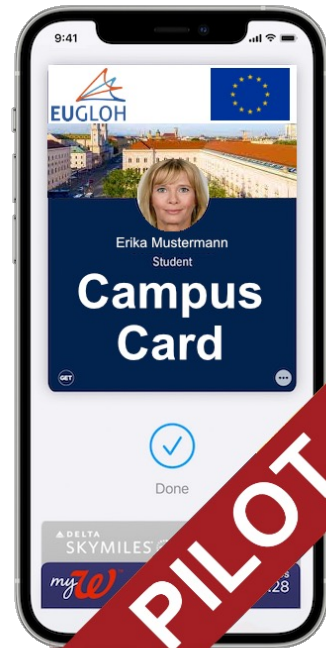
The path to an interoperable European Campus Card



EUGLOH Digitized Campus Card Pilot

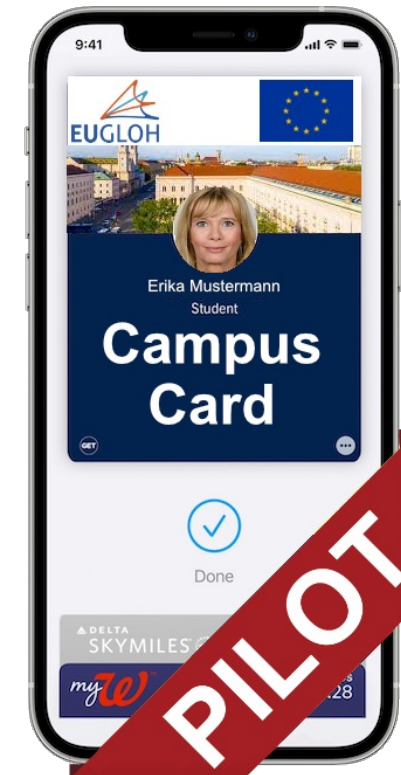
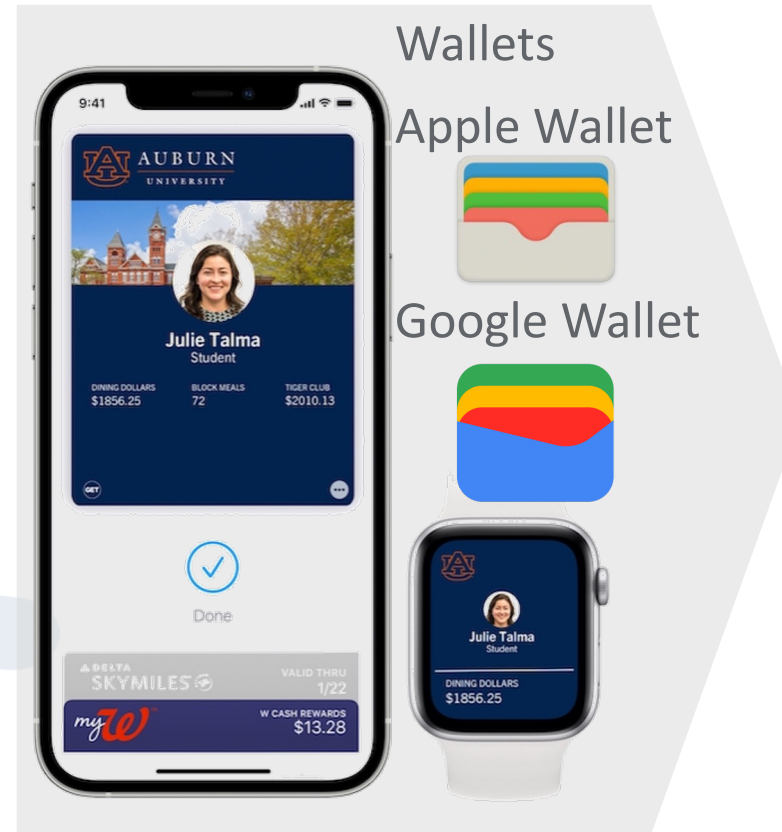


EUGLOH Digitized Campus Card Pilot – A digitized European Campus Card for interoperable Services



The Future of ID & service cards – Wallet passes

- ✓ Sustainable & Interoperable Virtual eID on Mobile Devices in Europe
- ✓ Online & Offline verification of data, and load additional core data from issuer
- ✓ Link data and applications



The future of passes in HEI context

Each HEI will have a „*European Campus Card Portal*“

For the user:

- Request / download European Campus Card
- Users can search for and book / download additional services
- Service listing with further information (including search) (also via Erasmus+ App)
 - Which university / which university location (e.g., Munich), category
 - What personal data is required → **Privacy information**
 - The user himself decides which services he would like to use and for this purpose, passes on his data → Self Sovereignty Identity (SSI)
- Listing of all linked services with the possibility of blocking / deleting them, and calling the account / information pages of the service provider.



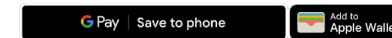
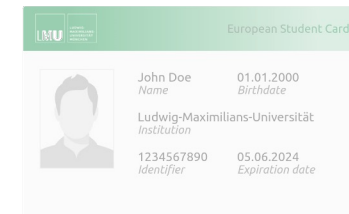
For the Service-Provider:

- Centralized service provider directory
- Data is transferred via identity linking through eduGAIN infrastructure
- Own passes or apps are made available via own website

[← Back](#)

European Student Card

Here you can manage your european student card and card services provided by the LMU and our partner universities.



Services

[Activated Cards](#)

Munich [Search](#)

Mensa Card Munich ⊖ +

Card for paying in all cafeterias operated by the Studentenwerk München.

food mensa pay

UB Card Munich ⊖ +

Grants access to the checkout system of the university library.

books library

StaBi Card Munich ⊖ -

Required for accessing the reading halls of the Staatsbibliothek Bayern.

books library

MVG Card Munich ⊖ +

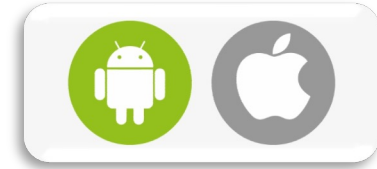
Transport ticket for students in Munich and surrounding counties.

transport subway bus

Cafeteria Berlin ⊖ -

Card for paying in all cafeterias operated by the Studentenwerk Berlin.

food mensa pay



The future of passes in HEI context

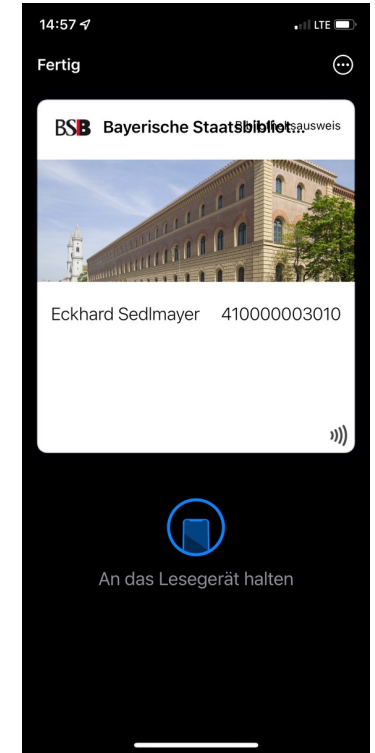
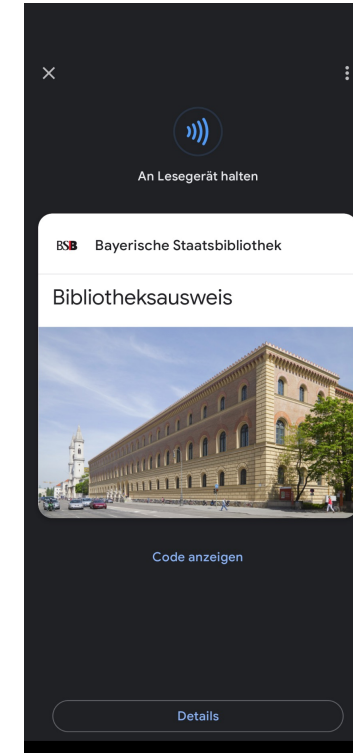
LMU / EUGLOH working on a cross-university pilot for wallet passes

- **Prototype** for a better solution to the ESCI vision → **concept phase**
- Not yet completed, but **first examples available**
 - Library cards for university library and Bavarian State Library as **Wallet Pass in iOS und Android**
- It is a migration to a new solution
 - Continuation of cooperation with service providers
 - Existing infrastructure and solutions will be considered
 - Most readers just need a firmware upgrade
 - Passes on plastic cards as fallback
- **ONE core pass** (European Campus Card / eduCampusCard) + any number of service cards (one pass per legacy service) or apps of the service provider

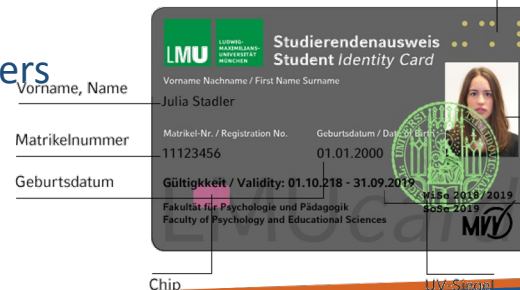
goal: starting 2023 issue ID passes in wallets for LMU members (students and staff)

→ first cards for services:

- Library



Braille (LMU) invers



Vorname, Name

Matrikelnummer

Geburtsdatum

Chip

Foto

Gültigkeit



Deliverables

- The EUGLOH Group wants to provide an ecosystem for a European Campus Card that quickly scales to all HEI in Europe or even world wide
- The EUGLOH Project did not receive any funds or grants for their work, all is financed out of our own budgets, so we do not have any project limits.
- We will provide:
 - Documentation
 - Help to generate a pass design
 - Infrastructure to issue service passes and the common identity pass
 - Infrastructure to manage, issue, update and revoke passes,
 - A service discovery portal and REST-API to include it in your own portals and Apps
 - We will provide example connectors to several common used IDM Backends and Databases
- BUT it will not be a full-service solution
- All our software will be open source and available free of charge



Public Money

Public Code

publiccode.eu

Deliverables

- Documentation is on GitHub
- Rendered Version: <https://ecc-pilot.github.io/documentation/>
- Disclaimer
- *Documentation is like our ideas and concepts not finalized*



European Campus Card Pilot Project

🔍 Search the docs ...

TABLE OF CONTENTS

- Project ✓
- Partners
- Requirements ✓

BACKLOG OF STILL UNSTRUCTURED CONTENT

- Data and presentation
- Deliverable's
- Security considerations
- Apple VAS
- Google SmartTap
- Transponder technologies ✓
- ISO/IEC 18013-5 Personal identification — ISO-compliant



Key Concepts

Identity Documents based on plastic cards are not a good base for interoperable service provision. Chip cards and smart cards, are limited. They have a limited memory, and storing data / applications on those cards differ by the providers. Also interoperability does not reside within the cards, as almost any technology provider has different internal standards to store and secure data on the card, *interoperability is done on the reader side.*

Modern smartphones have **Wallet** functions build into the operating system and could store almost an unlimited number of cards / passes and data. Also smartphones are the essential working tool for students and most university employees.

The approach of "Integrated Chip Cards", to store multiple service specific applications within one card is not valid anymore. Within Smartphone Wallets the approach of "**one card per service**" has more benefits.

Service provider on and off campus does have different needs and existing technologies, especially with legacy systems, so issuing one service card per service is a better approach.

Additionally most service providers does not provide their services to students exclusively. Multiple customer / consumer groups exists, that could uses those services. The European Campus Card does reflect this by opening the system to all roles.

A majority of service providers, especially off campus, do offer services and discounts to members of Higher Education Institutions. They often only need a affiliation status

☰ Contents

Background

Goals of this project - a "European Campus Card"

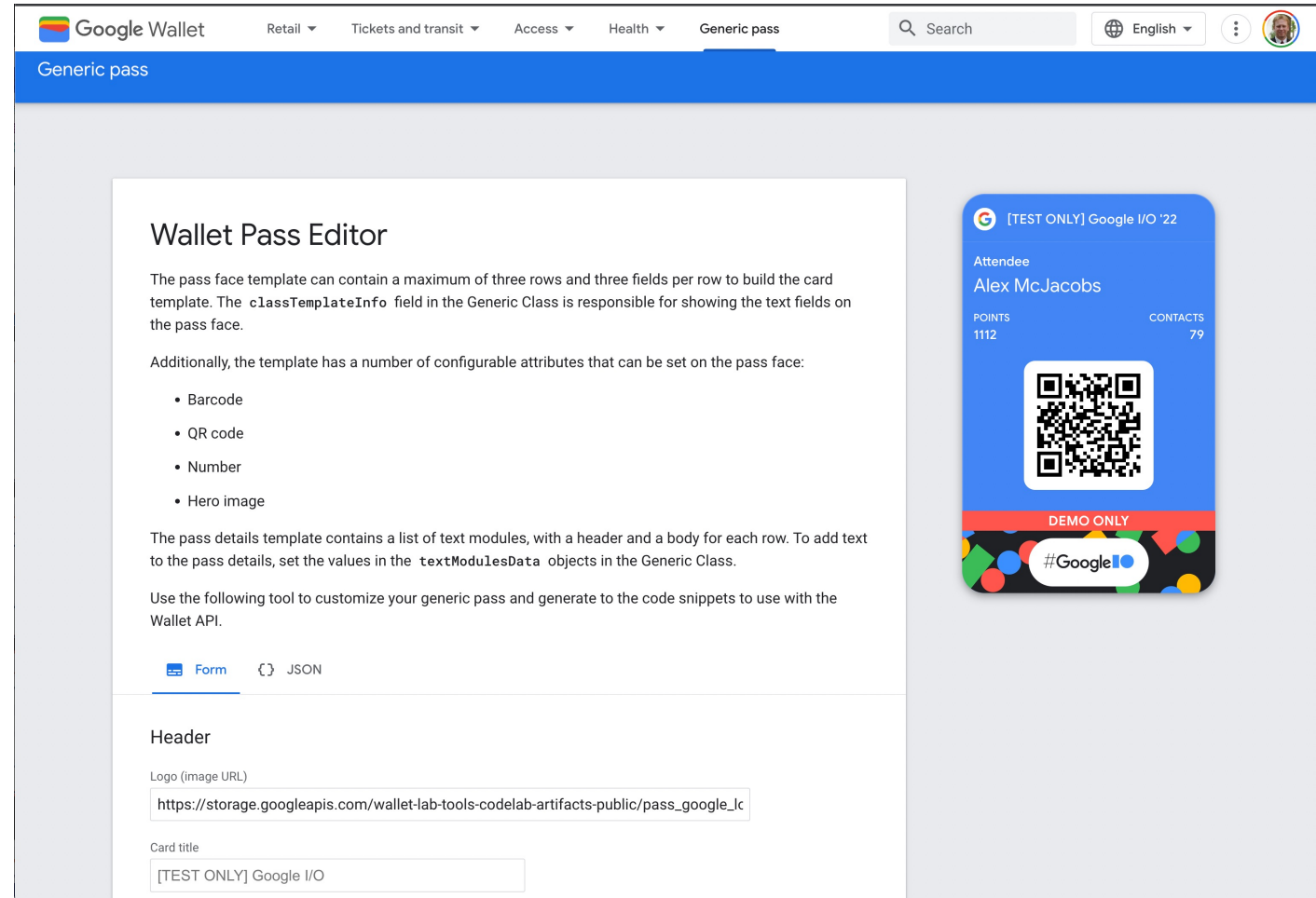
Key Concepts

Contents

Appendix

Deliverables

- Pass designs are JSON documents
- We will link to the tools of google and Apple in the beginning, but will also provide a portal to generate, validate or preview the designs in context of your portals

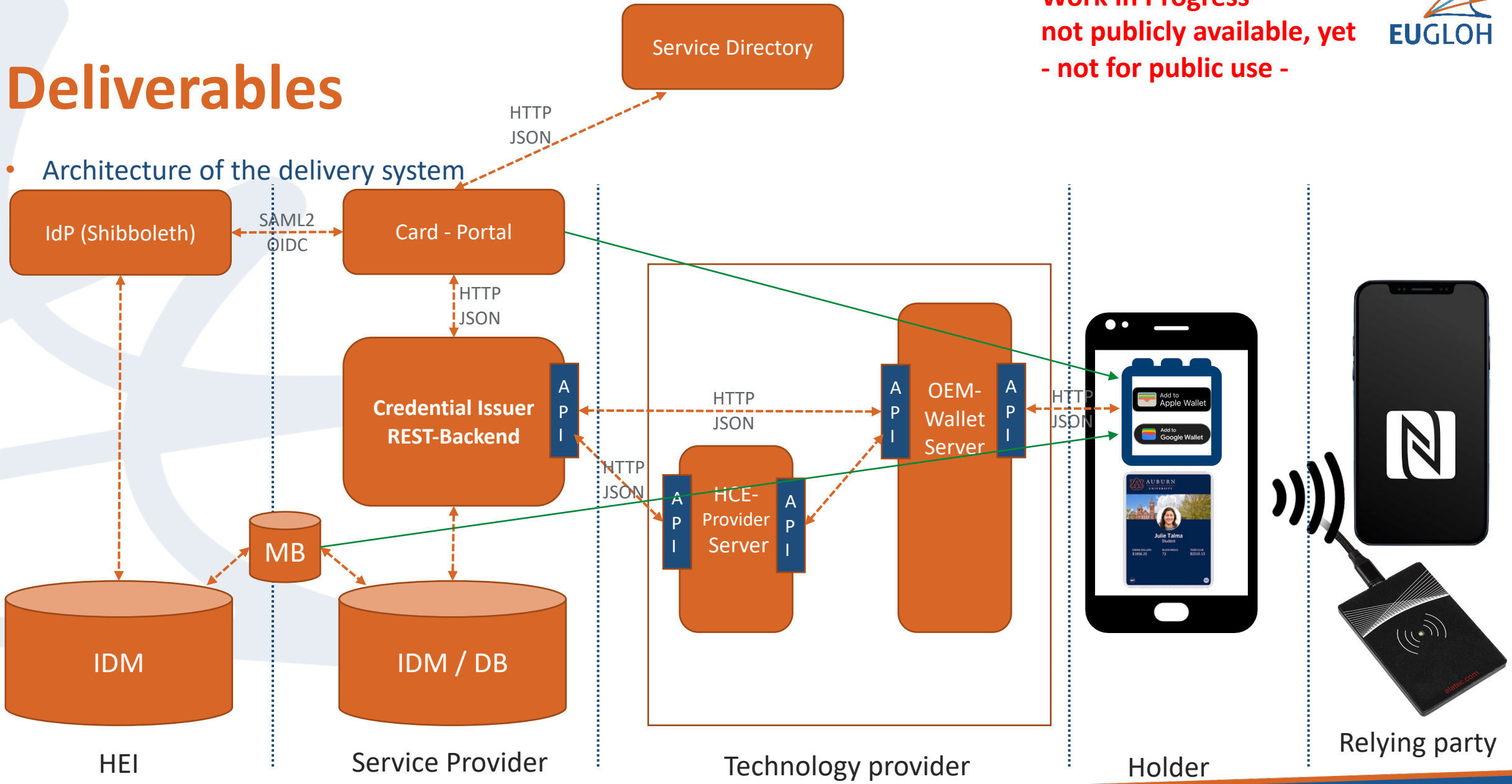


The screenshot shows the Google Wallet Generic Pass Editor interface. The top navigation bar includes the Google Wallet logo and menu items: Retail, Tickets and transit, Access, Health, and Generic pass. A search bar and language selector (English) are also present. The main content area is titled "Generic pass" and features a "Wallet Pass Editor" section. This section explains that the pass face template can contain up to three rows and three fields per row, and that the `classTemplateInfo` field in the Generic Class is responsible for showing text fields on the pass face. It also lists configurable attributes: Barcode, QR code, Number, and Hero image. Below this, it states that the pass details template contains a list of text modules with headers and bodies, and that values in the `textModulesData` objects in the Generic Class are used to add text. A note mentions using a tool to customize generic passes and generate code snippets for the Wallet API. At the bottom of the editor, there are tabs for "Form" and "JSON". The "Form" tab is active, showing a "Header" section with input fields for "Logo (image URL)" (containing `https://storage.googleapis.com/wallet-lab-tools-codelab-artifacts-public/pass_google_lc`) and "Card title" (containing "[TEST ONLY] Google I/O"). To the right of the editor, a preview of a blue pass card is shown. The card displays "[TEST ONLY] Google I/O '22", the name "Attendee Alex McJacobs", "POINTS 1112", and "CONTACTS 79". It features a QR code and a "#Google I/O" hashtag at the bottom. A red banner at the bottom of the card reads "DEMO ONLY".

Work in Progress
not publicly available, yet
- not for public use -

Deliverables

- Architecture of the delivery system



Wallet Solutions by technology providers

Specific solution for use cases:



Physical Access Control



Micro- / Closed Loop Payment

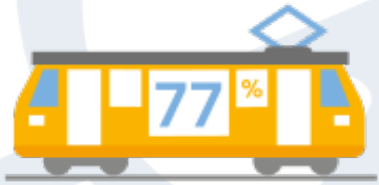
Solution for OEM Wallets of



NXP

LEGIC

MIFARE® THE WORLD LEADER IN CONTACTLESS ICS



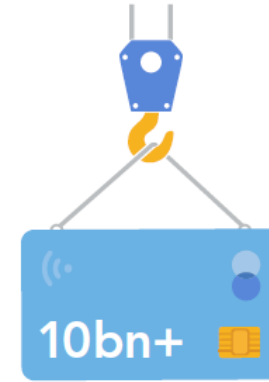
#1 in automatic fare collection, with 77% market share in transport ticketing



9 out of the 10 largest cities use MIFARE for their transport ticketing solutions



99 out of 100 contactless hotel doors support MIFARE



10 billion+ contactless and dual interface security controllers shipped



Used in more than 40 applications worldwide



1.2 billion people use MIFARE daily for uses including smart mobility, access, micropayment, loyalty

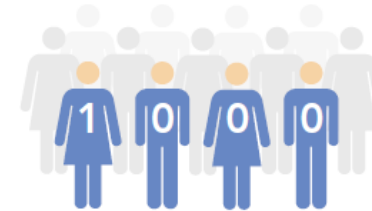
1500



Over 1500 campuses use MIFARE for access and micropayment



Running in over 750 cities worldwide



1,000+ partners within the MIFARE community



Highest level security certified products available

MIFARE

Leading brand for contactless smart paper tickets & multi-application smart cards.



Micropayment



Uni Access



Secure Access



Transportation



750 cities using MIFARE

1500 campuses use MIFARE for access and micropayment

NXP works with more than **1000** partners within the MIFARE community

1.2 Billion use MIFARE daily



digitalization

MIFARE

Leading brand connecting people to services, device manufacturers & cities.



LEGIC Partner on Apple Wallet



Example Wallet Solutions by LEGIC

end-customer
(credential issuer)

end-user
(credential holder)

end-customer
(service provider / relying party)

LEGIC Connect

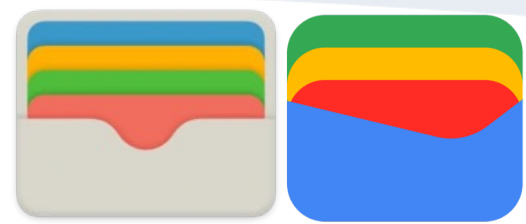
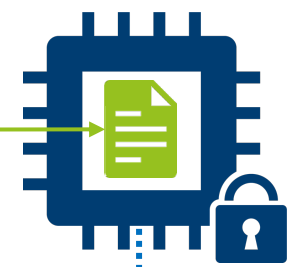
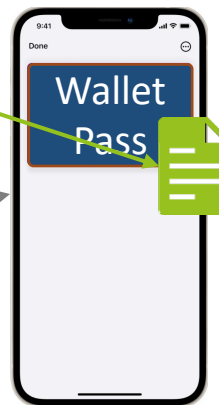
Hardware Security Module
Certified secure environment in data center

LEGIC Reader IC

Embedded Secure Module
Certified secure environment in reader chip

base concept

IDM Platform



Conclusion

- Wallet passes are the future for credential, not apps or cards
- cost-effective solutions are possible
- It is a long-term migration process

We'd love to hear from you!

Get in touch:

EUGLOH Work Package 5 – Campus Life

IT-Expert Working Group: heis.it.wp5.eugloh@up.pt

- Alexander Loechel (LMU Munich)
- José Filipe Alves (UPorto)
- Morgan Persson (LU)
- Pierre Gabrielle (Université Paris-Saclay)

Follow us on social media:



@eugloh19



@eugloh_network



@eugloh



@eugloh

www.eugloh.eu

