EPiC Series in Computing

Volume 107, 2025, Pages 175–185

Proceedings of EUNIS 2025 annual congress in Belfast

eduTAP – a Concept and System of Digital Identities for proximity on-site service access

Alexander Loechel[1,4,5,6], Simon Lund[1], José Filipe Alves[2,4,5] and Morgan Persson[3,4,5]

[1]Ludwig-Maximilians-Universität München, GERMANY
[2]Universidade do Porto, PORTUGAL
[3]Lunds universitet, SWEDEN
[4]European University Alliance for Global Health (EUGLOH)
[5]European Campus Card Association (ECCA)
Alexander.Loechel@lmu.de, Simon.Lund@lmu.de,
JoseAlves@uporto.pt, Morgan.Persson@lth.lu.se

Abstract

Universities offer a variety of services to students, staff, and affiliates, traditionally managed through physical campus cards. However, increasing mobility requirements and the need for secure, interoperable digital identity solutions call for a modernized approach to service access.

This paper introduces eduTAP, an open-source concept and software framework that builds on top of digital wallets and provides service access in Higher Education Institutions (HEIs) based on wallet passes. eduTAP leverages existing mobile wallet standards (Apple Wallet, Google Wallet, and the European Digital Identity Wallet) to enable secure authentication, service access, and identity verification.

By replacing traditional campus cards with dedicated digital service passes for local services and a harmonized digital identity document, eduTAP enhances scalability, privacy, and interoperability. The proposed harmonized identity document aligns with eduGAIN schemas and attribute definitions, ensuring global usability while enabling easy service access for students, staff, researchers, and affiliates at home and host universities while on mobility.

[6] Alexander Loechel, ORCID: https://orcid.org/0009-0003-9132-646X

1 Campus Cards and Services

Many universities have a long history, some spanning centuries—such as LMU Munich, founded in 1472; Lund University, in 1666; and the University of Porto, in 1911. As centre's of research and teaching, they provide various facilities and services to support communication and collaboration among their members. To manage access to these services, they employ identity management systems that operate both online and offline, enabling proximity-based use cases relying on a physical medium for authentication. Historically, universities relied on paper-based identity documents, later transitioning to integrated 'all-in-one' campus cards, which are now gradually being replaced by digital alternatives enabled by recent technological advancements. These include dedicated university or service provider applications on smartphones, as well as digital wallet passes.

1.1 Services Domains

Universities provide a diverse range of services for their members (students, staff, and affiliates), categorized into the following domains:

- **Identification and Authentication:** Verification of student and staff identity, proof of entitlements, secure multi factor authentication, attendance tracking and time recording
- **Electronic Payments / Cashless Campus:** Payments at canteens, vending machines, and printing services
- **Physical Access Control:** Entry to buildings, dormitories, and labs; role-based access for research and faculty spaces as well as athletic facilities
- **Library Services:** Borrowing books and accessing digital resources
- **Transportation:** University shuttle access and public transportation ticketing
- **Discounts and Promotions:** Student discounts in museums, theatres, and retail

From these service domains, two key characteristics can be identified.

1. **Two Levels of Service Access:**
    - Local services (e.g., payments, physical access, library services, and transportation) depend on institutional or national infrastructure and are often tied to legacy systems.
    - Global services (e.g., identification, discounts, and promotions) require interoperability across institutions, necessitating a unified identity dataset while maintaining privacy and security standards.
2. **Role-Inclusive Access:** Service access is not restricted to students. All university members – including staff, researchers, and affiliates – should have access to services with differentiated privileges rather than rigid role-based restrictions.

Recognizing these characteristics is crucial for designing a scalable, interoperable, and privacy-compliant service infrastructure that aligns with institutional, political, and market requirements while ensuring equitable access for all users.

1.2 Service Access

While online services still mostly rely on knowledge-based authentication (e.g., username and password) or credential-based authentication (e.g. certificates, passkeys), on- site services predominantly use possession-based authentication, typically through physical media such as student ID cards or tokens. Dedicated service cards and integrated campus cards come in various physical forms, ranging from one- or two-dimensional barcodes on paper or plastic to magnetic stripe cards, chip cards (which store data on a microchip), and smart cards (which include a CPU and operating system, typically JCOP). These cards can be used either to identify the card to a reader based on its UID or to transmit application data through the reader to a controller.

A significant constraint of such cards is their limited interoperability due to disparate, incompatible standards of transponder technology, particularly at the data access layer. In Europe, campus cards primarily rely on NXP's Mifare and Legic, whereas in North America and Asia, technologies such as HID, Sony Felica, and Calypso are dominant. The majority of integrated campus cards prioritize on-card data for basic local identification, library access, and cashless transactions, yet they frequently lack contemporary requirements for secure authentication (FIDO2-based) or digital signature capabilities. Moreover, their constrained memory and reliance on proprietary technology prevent scalable integration across universities. While smart cards could support these advanced requirements, they remain costly and are not widely adopted.

As technology advances, smartphone apps and digital wallets have emerged as viable alternatives. Early digital card implementations used barcodes (e.g., public transport tickets, library cards) due to NFC and BLE restrictions imposed by smartphone manufacturers. However, smartphone-based wallet ecosystems now provide direct access to these communication protocols, enabling emulation of proprietary data layers like Mifare DESFire and Legic NEOS, as well as supporting FIDO2, Verifiable Credentials, and digital signatures. Google Wallet and Apple Wallet use standardized communication protocols (ISO 14443, NFC, BLE) to ensure interoperability with generic readers.

Ultimately, the authentication medium is merely a facilitator – whether via visual, contact-based, or contactless methods, the core process remains the same: presenting an identifier for service access.

2 Political Visions and Technical Standards for Identity Management and Mobility Processes

The university community thrives on teaching, research, and knowledge transfer through publications, patents, and entrepreneurship. Communication and exchange are fundamental to research and education, enabling scholars to build on prior work, collaborate globally, and engage in academic mobility through study abroad programs, workshops, and conferences.

The European Commission's vision for a European Education Area aims to normalize student and researcher mobility. Expanding opportunities beyond top talents fosters inclusivity and academic engagement. However, higher education institutions (HEIs) operate globally, extending beyond continents and political federations. Therefore, Erasmus+ and European policy programs should be seen as starting points for a globally integrated higher education network.

Accordingly, academic mobility must be globally supported, ensuring interoperable service access upon arrival and throughout a stay, particularly for short-term mobility. A best-practice example is eduroam, which enables HEI members to seamlessly access university wireless networks worldwide using their institutional credentials.

2.1 The Vision of the European Commission Towards a European Education Area

The European Commission’s vision for the European Education Area (EEA) aims to establish a unified and inclusive educational landscape across the European Union. This initiative focuses on enhancing the quality and inclusivity of education and training systems, facilitating seamless cross-border learning, and promoting lifelong learning opportunities for all citizens. Key objectives include reducing disparities in educational outcomes, supporting the professional development of educators, and fostering digital and green transitions within educational contexts. The EEA also emphasizes the importance of mutual recognition of diplomas and study periods abroad, thereby encouraging mobility among students, researchers, and teachers (see EEA et. al.).

The European Commission, through the Erasmus+ program, has defined three building blocks within the digital priorities of the Erasmus Charter for Higher Education to support the European Education Area (EEA) and its mobility efforts: the European Student Card, the Erasmus+ App, and Erasmus Without Paper. Grouped under the European Student Card Initiative (ESCI), these initiatives aim to streamline and digitalize administrative processes for Erasmus+ students and HEIs, enhancing mobility across Europe. (see ESCI et al.).

2.2 The European Student Card

As a key component of the European Student Card Initiative (ESCI), the European Student Card (ESC) is designed to establish a unified European student identity and enable seamless student status verification across Europe. However, the ESC is not a standalone card but rather an extension of existing student IDs, incorporating the ESC logo and QR code (Figure 1: A European Student Card (physical and virtual in an app)￼).

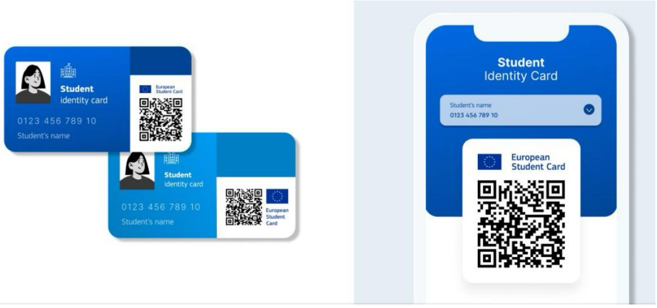


Figure 1: A European Student Card (physical and virtual in an app) [7]

Key Features of the European Student Card[8]

- European Student Card Number (ESCN) – a unique identifier based on RFC-4122
- European Student Identifier (ESI)
- ESC Logo & QR Code (URL containing the ESCN)

Since it is integrated into existing student IDs, most ESCs also include a photo, name, university branding, and matriculation number, alongside validity and birth date details.

Origins and Development

The ESC originated from student affairs organizations in France (Les CROUS) and Italy (Fondazione ENDISU, ANDISU) and later expanded to Ireland and Germany (DSW). The European Commission endorsed the initiative, funding the first ESC project in 2016 and subsequent ESC Tension projects. From 2021 to 2027, the ESC has been embedded in the digital agenda for education in Europe.

Technical Implementation

- The ESCN is embedded in a QR code linking to a centralized ESC Router database.
- The ESCN follows a scoped UID format, combining an Erasmus Participant Identification Code (PIC) and a server-generated counter.
- Unlike modern digital identity solutions, the ESC does not leverage chip card applications for contactless retrieval.

The ESC Router stores student data, accessible via web lookup. Anonymous queries return status information, while authorized access provides: Full Name, European Student Identifier (ESI), ESC Number (ESCN), Academic Level (Bachelor, Master, Doctorate), Email Address, and Expiry Date

[7] Source: https://erasmus-plus.ec.europa.eu/news/new-european-student-card-logo-a-fresh-look-for-improved-access-to-student-services

[8] Source: https://erasmus-plus.ec.europa.eu/european-student-card-initiative/card/how-it-works

Challenges and Limitations

Although further developments toward verifiable credentials are under discussion, ESC v1 primarily functions as a free alternative to the International Student Identity Card (ISIC) for off-campus discounts. On-campus service integration often requires additional registration due to legacy system dependencies.

For short-term mobility, the ESC offers limited benefits, as universities still require local campus cards for integration. Long-term mobility students are typically issued a campus card upon arrival.

Conclusion

While the vision of the European Student Card aligns with EU Digital Identity goals, its limited interoperability and exclusive focus on students restrict its practical usability. Broader support for all members of the higher education community, including faculty and staff, is essential to achieving a truly integrated digital identity framework.

2.3 GÈANT Trust and Identity Services

The GÉANT Association is a non-profit collaboration of European National Research and Education Networks (NRENs), providing IT infrastructure and identity services for Higher Education Institutions (HEIs). Among its core offerings, GÉANT Trust & Identity Services support authentication and authorization across universities, ensuring a standardized approach to identity management.

A key service is eduGAIN, an inter-federation of identity federations that enables HEI members to authenticate with a single institutional account across multiple services. As an Authentication and Authorization Infrastructure (AAI), eduGAIN relies on:

- Shibboleth, SAML2, and OIDC for authentication and access control.
- common LDAP schema (eduPerson, SCHAC) to standardize identity attributes and roles across institutions.

By defining a shared attribute set and ensuring mutual trust among federations, eduGAIN enhances interoperability, allowing universities to securely exchange authentication and authorization information at a pan-European and global scale.

Beyond eduGAIN, GÉANT offers additional trust and identity services that either leverage eduGAIN or complement its authentication framework:

- eduroam – A global Wi-Fi roaming service providing seamless and secure network access for the academic community.
- eduTEAMS – A service enabling federated identity and access management for research collaborations.
- MyAcademicID – A European Commission-backed initiative for student authentication in Erasmus+ and mobility programs. Also defining body of the European Student Identifier (ESI)
- MyAccessID – A service supporting researcher identity verification for trusted access to academic resources.

Currently, GÉANT Trust and Identity Services focus primarily on online identity management. However, on-site proximity-based authentication (e.g., physical access control, payments, and campus services) remains a critical gap. This paper introduces eduTAP as a solution to bridge this gap, extending federated identity principles to physical service access, ensuring secure, scalable, and privacy-compliant authentication in both online and on-campus environments.

2.4 The eduTAP Concept

Identity management and on-site service access have long relied on integrated campus cards, which consolidate multiple services into a single physical medium. However, with increasing mobility requirements and the shift toward digital services, traditional chip- and smart-card-based solutions are reaching their technical limits. The emergence of smartphone-based wallets (e.g., Apple Wallet, Google Wallet, and the European Digital Identity Wallet) presents a viable alternative.

The primary motivation behind integrated campus cards was to reduce the number of physical cards someone needed to carry. While physical wallets have a natural limit, smartphone wallets can store hundreds of digital passes. More importantly, the auto-presentment feature allows the reader to request an appropriate pass dynamically, making smartphone wallets function as a multi-application smart card.

eduTAP embraces this technology to modernize campus service access. The name "eduTAP" stems from "educational tapping," inspired by Apple's "tap to pay" concept. The approach follows two key principles:

1. Service-Specific Passes: Instead of a single integrated campus card, services are divided into separate passes within the wallet, allowing each to leverage the most suitable technology (e.g., EMA for payments, access control protocols for physical entry). This follows the divide-and-conquer approach to reducing complexity in complex systems.
2. Leveraging Existing Standards: Rather than introducing new proprietary standards, eduTAP relies on the built-in capabilities of smartphone wallets, ensuring compatibility and scalability.

eduTAP aligns with the European Union's vision for digital identity and academic mobility. It prioritizes user-centric design, advocating for native wallet applications over university-specific apps to enhance accessibility and interoperability. Like eduroam, services should be available across institutions, with discoverability facilitated through a centralized service directory integrated with eduGAIN/Shibboleth authentication.

Crucially, eduTAP is designed for all members of the higher education ecosystem—not just students but also employees, affiliates, and potentially alumni or the public (e.g., for library or cafeteria access). The decentralized nature of eduTAP enhances data privacy by storing service-specific credentials locally, eliminating the need for centralized databases such as ESC-Router or ISIC. Users retain control over their personal data, sharing only the necessary information for accessing specific services, fostering digital self-sovereignty.

By shifting from physical campus cards to a smartphone wallet-based approach, eduTAP modernizes campus authentication, enhances mobility, and strengthens privacy while ensuring broad accessibility and interoperability.

2.5 Smartphone Wallets and Features

To understand eduTAP and its benefits, it is essential to grasp the concept of digital wallets and their capabilities. A digital wallet is a software-based container for storing, managing, and presenting digital assets such as payment credentials, identification documents, physical access credentials (e.g., door or car keys), and tickets for transport and events.

There are two primary types of wallets:

- Smartphone-based wallets (e.g., Apple Wallet, Google Wallet, Samsung Wallet) focus on day-to-day transactions and proximity use cases, such as payments, access control, transit tickets, and event passes.
- Edge / Cloud-based wallets store a broader range of digital credentials, including diplomas, birth certificates, and student mobility records. Some wallets (like the EUDI-Wallet) also support proximity use cases, such as eIDs and mobile driving licenses.

Since this paper focuses on proximity-based, on-site, and offline use cases, smartphone wallets and the relevant proximity features of the EUDI-wallets and its credentials are particularly relevant. The term pass refers to a single instance of a digitized card, credential, or document stored in a wallet.

Key Features of Smartphone Wallets

1. Auto-Presentment / Smart Selection & Contactless Communication
   The smart selection feature allows a reader to request a specific pass via NFC or BLE, enabling seamless access to multiple passes without manual selection.

2. Remote Management & Security
    - Issuers can update, revoke, or void passes remotely
    - Security mechanisms that bind a pass to a specific user account or device, flags for sharing options and screenshots, preventing unauthorized copying or sharing.
    - Validity periods ensure automatic expiration unless renewed by the issuer.
3. Offline Functionality & Enhanced Security
    - Passes are locally stored and can be used even when the device or reader is offline.
    - Additional security features, such as biometric authentication, provide stronger protection than physical cards.
    - Some smartphones offer battery reserve mode, allowing access to specific passes (e.g., transit tickets or keys) even when the device has no remaining charge.

By leveraging these features, smartphone wallets provide a scalable and secure alternative to traditional physical campus cards, improving user convenience and institutional flexibility.

2.6 Dedicated Service Passes for Local Services

The majority of services are confined to a specific geographical area or technical domain, and they possess distinct technical prerequisites. Common local services include:

- Access to the library is permitted for the purpose of borrowing books or utilizing library facilities, including learning spaces.
- a secure follow me printing and payment
- physical access control systems for parking lots, buildings, classrooms and labs, or offices
- access to athletic facilities
- discount and closed loop payment in canteens, cafeterias and vending machines
- local on-campus transport or public transport
- time and attendance recording for staff members

A thorough examination of these examples reveals a substantial variation in complexity. The majority of libraries mandate only a "library ID," typically a multi-digit number that reflects the user account and its associated rights within the library system. Conversely, electronic payment systems (Closed Loop-Payment) and physical access control mechanisms (Online and Offline-Systems) are characterized by significantly elevated security requirements. Public transportation tickets serve as a prime illustration of a medium-security system, reliant upon cryptographically signed data presented in the form of a two-dimensional bar code (see Deutschlandticket).

The provision of all local services is the responsibility of either a single service provider or a group of service providers who collaborate with a network that has agreed to common standards and technologies. Consequently, a dedicated service pass for such a service can select the most suitable technology from wallet pass implementations that aligns with its specific use case.

2.7 A Harmonized Digital Identity Document

Service providers and institutions often require specific personal data, entitlements, or affiliation details for identity verification. This is particularly relevant in mobility scenarios, European University Alliances, and student authentication for exams or attendance checks. Traditionally, students present both a university-issued ID (e.g., student card) and a government-issued document (e.g., passport, national ID). However, this approach is inefficient and lacks standardization.

The eIDAS Regulation provides a framework for secure electronic identification, aligning with technical implementations such as SD-JWT-based Verifiable Credentials (VCs)[9] and ISO 18013-5-

[9] Source https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/

based mobile documents (mDocs). Both enable verifiable credentials with selective disclosure and zero-knowledge proofs, ensuring data integrity.

The ISO/IEC 18013-5 standard, originally designed for mobile driving licenses (mDL), has been adopted for various identity use cases, including TSA documents in the USA and the European Digital Identity Document (`eu.europa.ec.eudi.pid.1`) within the EUDI-Wallet.

Our Proposal: eduTAP Common ID – a Standardized Higher Education Institution Digital Identity Document (Dedicated Paper for EUNIS 2025, by Lund and Loechel)

To harmonize identity verification in higher education, eduTAP proposes a standardized Digital Identity Document based on ISO/IEC 18013-5, aligned with the GÉANT Trust and Identity Service and complementing eduGAIN. The working draft identifier “`org.geant.edutap.pid.1`” has been developed for this purpose. This mDoc-based identity document would encapsulate the most relevant identity attributes, commonly used within Shibboleth, LDAP (eduPerson, SCHAC), and European Student Card standards.

3 eduTAP: From Concept to Implementation

While eduTAP is primarily a concept, the eduTAP project provides software libraries, pass templates, and support for integrating digital wallet passes into existing university infrastructures, a reference implementation. It also addresses how reader infrastructure can be upgraded to support these passes during a migration period.

Software Libraries & Wallet Support Modules

At the core of eduTAP’s technical offering are wallet support modules tailored for different wallet vendors. These modules simplify communication with OEM Wallet APIs, handling callbacks, webhooks, and real-time pass updates. The first two modules, developed for Apple Wallet and Google Wallet, are open-sourced, and available on PyPI, making them reusable for all interested institutions.

The developer team aims to integrate the project under GÉANT Trust and Identity Services, ensuring it remains fully open-source, like Shibboleth and gain larger adoptions and a border community. Today, eduTAP does not provide a full credential management platform but instead offers a lightweight boilerplate for a REST API backend for issuing wallet passes, which can be integrated into existing IDM and domain-specific applications by HEI IT teams or third-party integrators (compare Figure 2: Concept of the eduTAP Credentical Management Platform).

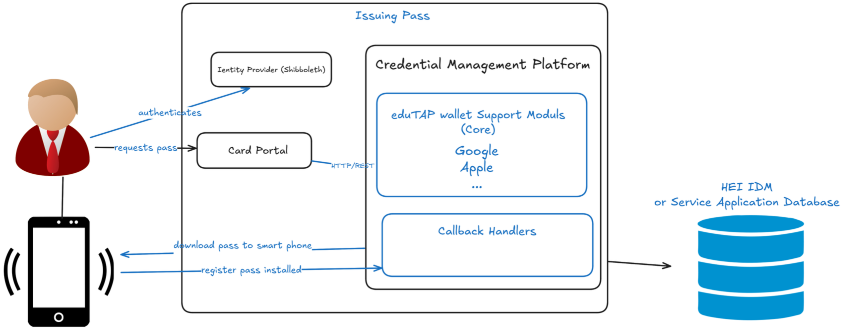

Issuing Pass
Ientity Provider (Shibboleth)
authenticates
requests pass
Card Portal
HTTP/REST
Credential Management Platform
eduTAP wallet Support Moduls (Core)
Google
Apple
...
Callback Handlers
download pass to smart phone
register pass installed
HEI IDM
or Service Application Database

Figure 2: Concept of the eduTAP Credentical Management Platform

Centralized Service Directory

A critical component in achieving seamless on-site service access, aligned with the ESC vision, is service discoverability. eduTAP proposes a centralized Service Directory, allowing universities and service providers to:

- List available services (e.g., libraries, canteens, lab access).

- Define access requirements, describe data privacy and terms of service, in the end provide links to local service portals where users can obtain wallet passes.
- Enable users to search for services at a university or location via a web interface or API.

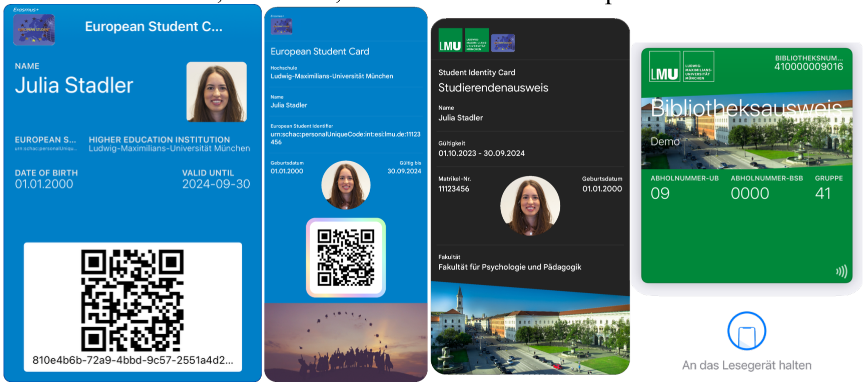
This web-based system will also support external applications, such as the Erasmus+ App, to enhance mobility service access for students and staff.

4 eduTAP@LMU: An Example of an eduTAP implementation

Ludwig-Maximilians-Universität München (LMU) is the first eduTAP implementation within the EUGLOH alliance. The deployment at LMU demonstrates how eduTAP can be adapted to different institutional environments.

At LMU, services such as canteens and cafeterias are managed by Studierendenwerk München Oberbayern, which has opted to experiment with open-loop payment solutions. Additionally, the LMU does not have a physical access control system to provide access to rooms. As a result, the eduTAP implementation did not require high-security pass types within Apple Wallet, making the rollout straightforward.

The implementation consists of multiple dedicated wallet passes, each serving a specific purpose (as shown in Figure 3: Example of passes issued by LMU): A library pass, a status verification pass for role based discount at the Mensa, a Staff ID, a Student ID and a European Student Card v1



Erasmus+
European Student C...
NAME
Julia Stadler
EUROPEAN S...
urn:schac:personalUniqu...
HIGHER EDUCATION INSTITUTION
Ludwig-Maximilians-Universität München
DATE OF BIRTH
01.01.2000
VALID UNTIL
2024-09-30
810e4b6b-72a9-4bbd-9c57-2551a4d2...

European Student Card
Hochschule
Ludwig-Maximilians-Universität München
Name
Julia Stadler
European Student Identifier
urn:schac:personalUniqueCode:int:esi:lmu.de:11123456
Geburtsdatum
01.01.2000
Gültig bis
30.09.2024

Student Identity Card
Studierendenausweis
Name
Julia Stadler
Gültigkeit
01.10.2023 - 30.09.2024
Matrikel-Nr.
11123456
Geburtsdatum
01.01.2000
Fakultät
Fakultät für Psychologie und Pädagogik

BIBLIOTHEKSNUM...
410000009016
Bibliotheksausweis
Demo
ABHOLNUMMER-UB
09
ABHOLNUMMER-BSB
0000
GRUPPE
41

An das Lesegerät halten

Figure 3: Example of passes issued by LMU

5 References / Citations

Géant – MyAcademicID Identity and Access Management Service Wiki-Page, *MyAcademicID Identity and Access Management Service*, Retrieved Februaray 21, 2025, from https://wiki.geant.org/display/SM/MyAcademicID+Identity+and+Access+Management+Service

European Commission: Directorate-General for Education, Youth, Sport and Culture, *European student card – General specifications*, Publications Office of the European Union, 2024, https://data.europa.eu/doi/10.2766/8835223

European Commission: Directorate-General for Education, Youth, Sport and Culture, *European student card – Technical specifications*, Publications Office of the European Union, 2024, https://data.europa.eu/doi/10.2766/5229016

European Commission – European Student Card Initiative website (2025), *The European Student Card*, Retrieved February 24, 2025, from: https://erasmus-plus.ec.europa.eu/european-student-card-initiative/card

Alexander Loechel, José Filipe Alves, Morgan Persson (2024-06-07) *eduTAP - Bridging online identity to mobile credentials for reliable and trustworthy on-site service access (in the educational sector)* Location: Presentation at EUNIS Conference 2024 Athens, Greek Retrieved from https://edutap.eu/presentations/EUNIS2024.pdf

eduTAP website (2024). *eduTAP* . Retrieved February 24, 2025, from: https://edutap.eu/

Miolin, Kristina; Loechel, Alexander; Alves, Jose Filipe; Persson, Morgan; van Lent, Jeroen (2023-09-29) *One Europe, one mobile solution: Turning the European Student Card vision into reality*, Location: Presentation at EAIE Conference 2023 Rotterdam, The Netherlands; Retrieved from: https://edutap.eu/presentations/EAIE-2023.pdf

Alves, Jose Filipe; Persson, Morgan; Loechel, Alexander (2023-05-10) *Digitized Card Pilot for European HEIs – A European Campus Card for Interoperable Services –*, Location: Presentation at European Campus Card Association Conference 2023 at University of Warsaw, Poland, Retrieved from: https://edutap.eu/presentations/EUGLOH-ECCA-2023.pdf

Loechel, Alexander (2023-03-09) *Digitized Card Pilot for European HEIs*, Location: Presentation at EDSSI Level 2 – Stakeholder Forum, European Council of Student Affairs (ECStA) Palazzo Badoer, Vanice Italy, Retrieved February 27, 2025, from: https://edssi.eu/stakeholders-forum/ and https://edutap.eu/presentations/edssi2-digitized-card-pilot-for-eu-hei.pdf

6 Author biographies

Alexander Loechel, Referent IT-Projekte is a senior IT Manager at Ludwig-Maximilians-Universität München, Germany, responsible for strategic IT project management, digitalization, IT architecture, technology, and innovation management. Additionally, he is the IT representative of The European University Alliance for Global Health (EUGLOH) in FOREU4All, and the European Digital Education Hub – European Higher Education Interoperability Framework. He was the responsible manager for creating the integrated campus card "LMUcard" at LMU Munich and is the project lead of eduTAP.

Alexander graduated in Informatics and researched in Operations Research about managing complexity and situational awareness systems.

Alexander Loechel's profiles on the web, LinkedIn: https://www.linkedin.com/in/alexander-loechel-323a176b/ GitHub: https://github.com/loechel,

Simon Lund, is a software developer at Ludwig-Maximilians-Universität München, Germany, contributing to identity management projects. He is involved in the implementation of eduTAP@LMU and has previously worked on the "LMUcard" project. Simon completed his master's degree in computer science with a contribution to eduTAP by specifying and implementing a pre-consent mechanism in the context of digitizing university ID cards as verifiable credentials based on ISO/IEC 18013-5. Simon Lund's profiles on the web, LinkedIn: https://www.linkedin.com/in/simon-lund, GitHub: https://github.com/simon-lund

José Filipe Alves is an Information Security Officer of the University of Porto's CSIRT team. He is also a board member of the European Campus Card Association (ECCA) and a member of the eduTAP working group of the EUGLOH inter-university Alliance. He is involved with the University Smart Card Project, exploring smart card technologies, and leveraging its integration with internal and external systems. He is currently focused on the ongoing morphing of physical to digital identification, especially regarding eID credentials in Higher Education Institutions, namely trusted identification, student mobility, secure access, etc., i.e. everything that matters when interfacing intra and extra HEI services both across institutions and borders. Currently, he is involved in the DC4EU Large Scale Pilot.

José Filipe Alves's profiles on the web, LinkedIn: https://pt.linkedin.com/in/jose-filipe-alves

Morgan Persson, an IT Architect at the Faculty of Engineering at Lund University, Sweden, holds a Master of Science in Electrical Engineering with a focus on chip design. After working a few years at the Department of Information Technology, Morgan joined the Faculty IT Department in 2004. At Lund University, Morgan has been involved in developing most of the systems related to their campus card (LU-kortet), starting from its inception in 2005. Beyond LU-kortet. Having attended the European Campus Card (ECCA) conferences since 2005, Morgan joined the board of ECCA in 2009 and has presented at several conferences. Additionally, Morgan has been actively engaged in the eduTAP project.

Morgan Persson's profile on LinkedIn: https://www.linkedin.com/in/morganpersson