EPiC Series in Computing

Volume 107, 2025, Pages 282–292

Proceedings of EUNIS 2025 annual congress in Belfast

eduTAP Common ID
A Standardized Digital Identity Document for HEIs

Simon Lund[1] and Alexander Loechel[123]*
Simon.Lund@lmu.de, Alexander.Loechel@lmu.de

[1] Ludwig-Maximilians-Universität München, Germany
[2] European University Alliance for Global Health (EUGLOH)
[3] European Campus Card Association (ECCA)

Abstract

Universities increasingly seek to transition from physical campus cards to digital solutions like in-app implementations. However, these solutions typically operate as isolated local systems, lacking both interoperability across institutions and robust security measures. To address these issues, this paper proposes the eduTAP Common ID, a digital identity document for Higher Education Institutions (HEIs), aligning with ISO 18013-5 (mDoc) and eduGAIN schemas (eduPerson and SCHAC). By leveraging mobile wallets, we enable HEIs to move toward a standardized and secure digital identity that is interoperable not only across universities but also with external providers. Building on ISO 18013-5, the proposed HEI Common ID incorporates privacy-preserving mechanisms such as selective disclosure and informed consent, serving as a foundation for our long-term objective of establishing a standardized GDPR-compliant, trusted, and globally scalable digital student and staff credential for HEIs.

1 Introduction

Secure identity verification is fundamental to accessing the wide range of services and facilities offered by universities to students and staff. With increasing requirements against forgery and unauthorized access, the means of identity verification in higher education have undergone significant evolution. Over time, student and staff IDs evolved from paper-based identity documents to plastic cards embedded with security features. Today, the next step is the transition toward digital, on-device identity solutions.

Despite this shift, universities experimenting with digital IDs rely on non-standardized verification methods with weak security. For example, institutions implement simple graphical representations of campus cards in mobile apps, displaying holder information and photos for visual inspection.

Unlike physical cards with embedded security features such as holograms, these digital representations lack cryptographic safeguards and are easily replicated. Consequently, universities may need to introduce additional verification steps, for instance during exams.

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

Moreover, services beyond university campuses, such as museums, theaters, sports facilities, and retail stores, rely on student verification as well, e.g., for discounts. In Europe, student mobility further underscores this need, with discounts on Interrail passes and public transport often tied to student status. Yet, the lack of a standardized, verifiable format prevents interoperable and secure verification across different contexts. As a result, service providers may accept unverified IDs – weakening the chain of trust – or ultimately deny benefits altogether.

These issues highlight the need for a robust solution to digital IDs for higher education institutions (HEIs) – one that ensures secure authentication beyond simple visual representation by incorporating machine-readable formats with strong cryptographic safeguards. Such a solution should rely on future-proof signing algorithms, such as the Elliptic Curve Digital Signature Algorithm (ECDSA), to ensure strong cryptographic security and long-term resilience against attacks. In addition, it should leverage open trust infrastructure, such as a public key infrastructure (PKI) or digital ledgers (e.g., European Blockchain Services Infrastructure, EBSI [3]), to facilitate interoperability across service providers.

However, rather than designing a solution from the ground up, existing digital identity solutions can be adopted to fulfill these requirements. A suitable approach in this context are smartphone-based digital wallets which align with existing identity management solutions in the HEI space due to their decentralized architecture. For example, initiatives such as the European Digital Identity Wallet (EUDI-Wallet) [2], Google Wallet Identity [8], and Apple's Verify with Wallet [1] provide established frameworks that can be adapted to educational contexts.

Efforts to do so are bundled in the eduTAP project [13]. Building on existing mobile wallet technologies, eduTAP aims to establish a foundation for verifiable, secure, and interoperable credentials for proximity-based service access and identity verification in the context of HEIs.

This paper contributes to this effort by proposing a digital identity document design for HEIs that could serve as the foundation for a future standard: the eduTAP Common ID. Drawing on ISO 18013-5 [10], a widely adopted standard for mobile identity verification, and eduGAIN schemas (eduPerson and SCHAC) for academic identity interoperability, this proposed framework aims to address the aforementioned requirements as a secure, trusted, interoperable, and scalable solution for verification of all HEI members, supporting both on-campus and external use cases.

While eduTAP itself is not a standard and does not mandate standardized wallet passes in general, a common specification for the eduTAP Common ID is sensible given its global scope. As this digital identity document must be verifiable by any service provider regardless of which HEI issues it, standardization becomes critical for achieving interoperability across institutional boundaries by providing a common ground for participants to exchange data in mutually recognized, verifiable, and interoperable formats. Furthermore, formalizing this specification allows for the consolidation of expert knowledge, ensuring that proven security mechanisms for data protection and forgery prevention are incorporated, while facilitating compliance with regulatory frameworks.

2 Background and Related Work

2.1 Digital Identity in Higher Education

Identity management is a fundamental component of university IT infrastructure, enabling secure authentication for students and staff across digital and physical services.

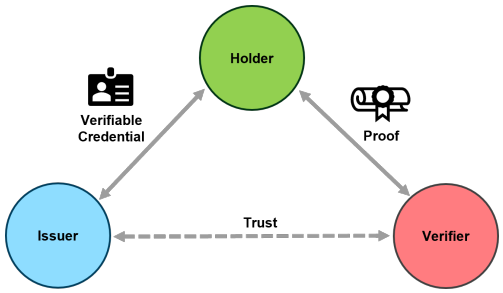

Figure 1: The Triangle of Trust in the context of verifiable credentials illustrates the key actors and their interactions (cf. [19, Figure 1]).

eduGAIN: Enabling worldwide access to educational resources. Operated by the GÉANT community, eduGAIN [4] connects national federations worldwide, facilitating federated authentication via Identity Providers (IdPs) and Service Providers (SPs) through standardized schemas such as eduPerson [17] and SCHAC [18]. By establishing a framework for cross-institutional identity management, eduGAIN enables users to access online services using credentials issued by their home institutions [4]. While eduGAIN has become a widely adopted infrastructure for federated authentication, its scope is limited to online services, such as web-based applications and infrastructure-level access like eduroam. It does not extend to proximity-based authentication scenarios typically encountered on campus, where traditional campus card systems are still used for identity verification.

eduTAP: Extending eduGAIN for Mobile Identity. To address this gap in federated identity infrastructure, eduTAP introduces a digital solution to on-site service access through mobile identity. Its core innovation lies in unbundling the traditional integrated campus card into multiple individual service passes, each represented as a credential in the user's mobile wallet, as further explored in "eduTAP – A Concept and System of Digital Identities for Proximity On-Site Service Access" (EUNIS 2025) [13]. eduTAP leverages existing mobile wallet functionalities – such as Auto-Presentment on Apple devices and Smart-Select or Quick-Select on Google platforms – in combination with established security technologies, including MIFARE DESFire, HID Seos, and LEGIC NEON.

Its goal is to establish an interoperable and flexible solution that, similar to eduGAIN, allows members of HEIs to access services they are eligible for via their mobile wallet, while also enabling HEIs to issue wallet-based passes for local services without imposing vendor lock-in or specific requirements for data formats. For example, while the underlying transport protocols are standardized through mobile wallet platforms, the structure of the credential data itself can remain institution-specific – i.e., a university library pass only needs to be interpretable by the library's scanners.

2.2 Verifiable Credentials and Standards

Verifiable Credentials (VCs) offer a decentralized approach to digital identity, enabling individuals to control their credentials without relying on centralized infrastructure. Here, a credential refers to a set of claims or attributes about a subject (e.g., name, birthdate, or more complex information such as ownership relationships) [10, 19, 21].

Aligned with the principles of self-sovereign identity (SSI) [15], the VC architecture is built on the so-called "triangle of trust" (see Figure 1), which defines three core roles:

- **Issuer**: The entity that *attests to specific attributes* about a subject and issues verifiable credentials. For example, a university that issues a digital diploma.
- **Holder**: The entity (typically an individual) that *receives, stores, and manages credentials* securely, often using a digital wallet.
- **Verifier**: The entity that *requests and validates credentials* in order to verify claims before providing a service. For example, an employer verifying a diploma.

Notably, the verifier does not require access to the full credential; instead, the holder selectively discloses only the relevant attributes, adhering to the principle of data minimization [10, 21]. This approach ensures that only strictly necessary information is shared, thereby preventing unnecessary data exposure.

ISO/IEC 18013-5:2021 Personal identification – ISO-compliant driving licence Part 5: Mobile driving licence (mDL) application. This standard defines a VC framework for mobile identity documents (mDocs), specifying a structured transaction and data model (see Figure 2) that enables standardized mobile identity verification [10]. Initially designed for mobile driver's licenses, ISO 18013-5 has since been adopted for other identity use cases, including TSA-approved digital identity documents in the USA and the EUDI-Wallet, in which the European Digital Identity Document "`eu.europa.ec.eudi.pid.1`" conforms to this standard [16, 2]. The standard supports contactless verification for on-site authentication using Bluetooth Low Energy (BLE) and Near Field Communication (NFC), as well as remote verification through online authentication workflows [10]. Major wallet providers, including Apple Wallet and Google Wallet, have already implemented support for this standard, making it a practical reference for mobile identity solutions [16].

The ISO 18013-5 data model follows a hierarchical structure. Each mDoc is identified by a unique document type, such as "`org.iso.18013.5.1.mDL`". Attributes within a document are organized into namespaces, enabling a single mDoc to support multiple schemas. To ensure authenticity and integrity, the issuer cryptographically signs these attributes and stores the corresponding signatures in the Mobile Security Object (MSO), which is transmitted alongside the data during a verification request.

Building on this, selective disclosure is achieved through a bidirectional transaction model, in which the verifier specifies the required attributes during a transaction. The holder is then presented with this request and, following an informed consent mechanism, decides whether to disclose the requested data. Only if the holder agrees is the information transmitted [10].

Other Standards: SD-JWT VC, W3C Verifiable Credentials, and OpenID4VCI. While ISO 18013-5 is a widely adopted standard for mobile identity documents, several other approaches to VCs exist. Selective Disclosure JSON Web Token for Verifiable Credentials (SD-JWT VC) defines a format that leverages SD-JWT [7] to represent VCs as JSON payloads [21]. Unlike traditional JWTs, SD-JWT enables selective disclosure of individual claims at the time of presentation.

Another standard is the W3C Verifiable Credentials Data Model, which "provides a standard way to express credentials on the Web in a format that is cryptographically secure, privacy-respecting, and machine-verifiable" [19]. A key difference is that, unlike ISO 18013-5, W3C

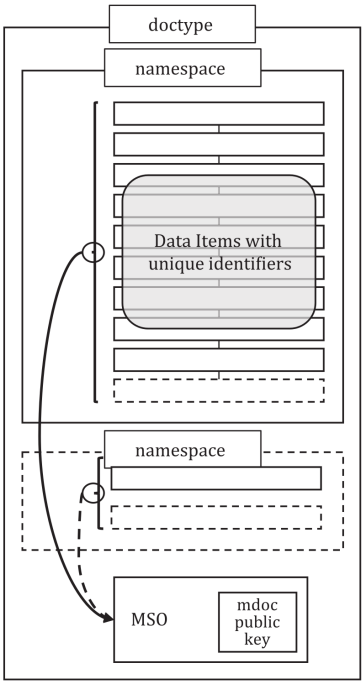

Figure 2: The mDoc data model with data elements organized into namespaces and the Mobile Secure Object (MSO) [10, Figure 2]

.

Verifiable Credentials are not inherently bound to a specific device [10, 19]. While SD-JWT VCs are generally portable, key binding can optionally be enforced [21].

To address interoperability challenges in VC ecosystems, two complementary protocols have been developed: OpenID for Verifiable Credential Issuance (OpenID4VCI) and OpenID for Verifiable Presentations (OpenID4VP) [12, 20]. Both build on OAuth 2.0 to provide standardized communication flows for issuing and presenting verifiable credentials.

OpenID4VCI enables wallets to authenticate with issuers and obtain credentials through an OAuth-based interaction, ensuring secure issuance [12]. OpenID4VP, in turn, defines a container format for remote presentation, allowing wallets to transmit credentials conforming to the aforementioned standards without requiring changes to the underlying communication protocol [20].

2.3 Data Protection and Privacy

The General Data Protection Regulation (GDPR) establishes strict requirements for processing personal data [5]. Among other principles, it mandates purpose limitation (Article 5(1)(b)), data minimization (Article 5(1)(c)), and lawfulness of processing (Article 6) to ensure that personal data is handled transparently and securely by the entity responsible for processing it. Identity attributes stored in VCs, including those of eduTAP Common ID, qualify as personal data under Article 4(1), and their processing requires explicit, informed consent as defined in Article 7 [5]. To ensure GDPR compliance, eduTAP Common ID relies exclusively on standards

that align with these principles. As described in the sections above, these standards incorporate privacy-preserving mechanisms such as selective disclosure to minimize data exposure, and cryptographic protections to prevent unauthorized access.

3 Key Considerations

The following considerations were taken into account in the design of the proposed eduTAP Common ID and in selecting suitable standards for its technical foundation:

1. **Interoperability:** To be suitable as a globally interoperable identity solution, the eduTAP Common ID must be based on open, well-documented standards. This ensures broad usability across HEIs and compatibility with external service providers.

2. **Proximity-Based Access:** The eduTAP framework extends eduGAIN to enable proximity-based authentication, which relies on physical service access. Hence, the eduTAP Common ID must support proximity-based authentication.

3. **Holder Binding:** As an identity document, the VC must be securely bound to the holder's device, ensuring that only the rightful user can present it.

4. **Data Protection:** The eduTAP Common ID must comply with data protection regulations, such as the GDPR. This includes ensuring user control over personal data and limiting data processing to what is necessary for the intended purpose.

5. **Security and Trust Infrastructure:** The credential must rely on state-of-the-art cryptographic security and be anchored in a trustworthy infrastructure to ensure integrity, authenticity, and resilience against forgery.

Design Rationale. The eduTAP Common ID is grounded in the verifiable credentials (VC) model, which provides a decentralized and privacy-preserving framework for representing identity information. VCs are designed to be interoperable across institutions, support selective disclosure, and offer strong cryptographic protections – making them well-suited for secure and user-controlled digital identity in the higher education context.

Among the available VC standards, ISO/IEC 18013-5 was selected as the technical foundation for the eduTAP Common ID. Its widespread adoption across major wallet ecosystems, including Apple Wallet and Google Wallet, ensures compatibility with existing mobile infrastructure. Moreover, its support for proximity-based authentication via NFC and BLE aligns with the need for proximity-based service access. A key differentiator of ISO 18013-5 is its enforcement of holder binding, which ensures that the credential is tied to the rightful user's device – a necessary property for identity documents. The standard also incorporates privacy and security features, such as credential revocation and data minimization, that support regulatory compliance and trustworthiness.

For the data model of the eduTAP Common ID, the eduGAIN schemas eduPerson and SCHAC were chosen as a conceptual baseline, as they provide a well-established academic identity model. This alignment ensures semantic interoperability and compatibility with existing HEI infrastructure.

4 Proposal: The EduTAP Common ID

To address the need for a standardized digital identity credential in the higher education context, we propose the eduTAP Common ID: a VC based on ISO/IEC 18013-5 and the eduGAIN schemas eduPerson and SCHAC, identified by the working draft identifier "`org.geant.edutap.pid.1`". If adopted, the eduTAP Common ID would align with the GÉANT Trust and Identity Service and complement eduGAIN, facilitating integration into the existing federated identity infrastructure.

HEIs and service providers require specific personal data, entitlements, and affiliation information to support student services, access control, and eligibility-based offerings — necessitating a credential tailored to academic contexts. The eduTAP Common ID encapsulates these attributes following the mDoc data model defined in ISO/IEC 18013-5. By drawing on the well-established eduGAIN schemas, it provides a common semantic framework that not only ensures interoperability across institutions, but also aligns with familiar data models used by HEIs, and avoids the need to redefine attribute names or semantics.

Due to the decentralized nature of VCs, HEIs act as the legal credential managers and issuers, maintaining control over their members' data without the need to transmit personal information to a central authority. The technical issuance process is carried out through credential management platforms (CMPs) integrated with existing institutional identity management (IDM) systems, ensuring consistency between online and offline identities. This integration further aligns with eduGAIN conventions and existing identity infrastructure. Credential lifecycle management — including issuance, renewal, and revocation — is handled according to institutional policies and established security frameworks, enabling HEIs to maintain accurate and up-to-date digital identities for students and staff.

4.1 Credential Structure

In the context of this proposal, the aforementioned working draft identifier also serves as the document type for the eduTAP Common ID, as required by the mDoc specification. The document type enables verifiers to request specific attributes from a given credential, such as confirming a user's HEI membership status for service eligibility.

For the credential's data model, we propose using a defined subset of attributes from the eduGAIN schemas eduPerson and SCHAC, as outlined in Table 1. Only attributes relevant to the function of an identity document are included, as many entries in eduPerson and SCHAC are intended for broader access management contexts.

4.2 Service Access

The eduTAP Common ID supports both in-person and remote identity verification, building on the transaction and communication models defined in ISO/IEC 18013-5 [10] and ISO/IEC 18013-7 [11].

For on-site authentication, the standard enables secure proximity-based verification through NFC, BLE, and Wi-Fi Aware [22], ensuring compatibility across different service environments. These mechanisms allow seamless identity confirmation at physical access points such as campus facilities, libraries, or public transportation, even in offline settings without reliable internet connectivity.

To enhance usability, identity verification can be combined with payment systems in a two-tap flow: for example, a student may first tap their device to verify their eligibility for a cafeteria discount and then complete the payment with a second tap at the payment terminal.

Table 1: Attributes of the eduTAP Common ID

Category	Attributes	Origin	Notes
Personal Data	jpegPhoto	eduPerson	Used for holder binding
	title	—"—	Honorifics
	givenName	—"—	First name
	sn (surname)	—"—	Family name
	schacDateOfBirth	SCHAC	Used for age verification
Affiliation Information	eduPersonAffiliation	eduPerson	Indicates general role (e.g., student, staff)
	eduPersonScopedAffiliation		Affiliation with domain context (e.g., student@univ.edu)
	eduPersonPrimaryAffiliation		Optional; primary role if multiple affiliations exist
Identifiers	eduPersonUniqueId	eduPerson	Persistent, non-reassigned user identifier
	eduPersonPrincipalName	—"—	A scoped identifier for a person.
	schacPersonalUniqueCode	SCHAC	May include European Student Identifier [9] or local enrollment number
Validity Information	schacExpiryDate	SCHAC	Credential expiration date
Contact	mail	SCHAC	Institutional email address
	homePostalAddress		Optional; for official correspondence
Additional Attributes	Academic Level	ESC	Proposed by European Student Card (ESC); e.g., bachelor, master, PhD
	Age Verification Fields	ISO 18013-5	Boolean fields for thresholds like 18+, 21+, etc.

In addition to on-site usage, remote presentation is supported through ISO/IEC 18013-7 and OpenID for Verifiable Presentations (OpenID4VP) [11, 20]. Credentials stored in a digital wallet can be presented online via two main interaction modes:

- **Deep linking:** A service triggers the wallet app via an `mdoc://` link, enabling attribute presentation after user consent. This method is suitable for same-device flows.
- **Cross-device:** The verifier displays a QR code which the user scans with their mobile wallet, allowing remote authentication from another device. This approach supports

possession-based authentication and can be used as a second factor.

Both approaches follow a decentralized model in which the issuer is not involved during presentation, and only user-approved data is disclosed. This prevents centralized tracking of identity usage and aligns with GDPR and eIDAS principles [5, 6, 15].

Consent-Driven Access Control. A core feature of ISO/IEC 18013-5 – and by extension the eduTAP Common ID – is its consent-driven access mechanism, requiring explicit user approval before any credential data is shared. This enforces the principle of data minimization mandated by the GDPR [5] and ensures user control over disclosing personal data, in contrast to physical ID cards which typically expose all data without restriction.

However, requiring consent at every transaction may introduce operational friction in frequent-use contexts. ISO/IEC 18013-5 anticipates this by outlining a pre-consent mechanism, though its implementation remains undefined. To address this, [14] presents a prototype with pre-consent capabilities. Users can authorize specific verifiers in advance for specific attributes – e.g., eduPersonAffiliation to apply a cafeteria discount – streamlining routine interactions while preserving privacy boundaries.

By integrating both explicit consent and pre-consent options, eduTAP balances usability with privacy protection. It ensures that digital identity verification remains user-centric and standards-compliant, while still meeting the efficiency demands of everyday service interactions in academic environments.

5 Conclusion and Outlook

The transition to digital identity solutions is ongoing and inevitable. As the EUDI-Wallet gains traction and mobile wallets extend beyond payment use cases, student and staff IDs must also be integrated into these digital ecosystems. The eduTAP framework offers a structured approach to implementing seamless on-site service access for HEIs, with interoperability and mobility as core design goals. In this paper, we proposed the eduTAP Common ID: an identity VC based on ISO/IEC 18013-5, with the working draft identifier `"org.geant.edutap.pid.1"`. Designed for issuance by all HEIs, it enables trusted proximity-based authentication for on-campus services and supports decentralized, verifier-driven online identity verification, aligning with emerging European digital identity frameworks. By bridging physical and digital identity through eduGAIN and globally recognized standards, the eduTAP Common ID lays the groundwork for a secure, interoperable, and privacy-preserving digital mobile identity standard for HEIs.

Next Steps. To transform this proposal into a widely adopted standard, the following steps must be taken:

1. Establish eduTAP – either as a whole or specifically as the Common ID – as a GÉANT Trust and Identity Project.

2. Develop a REFEDS standard for the Common ID to ensure interoperability and uniform implementation, in relation to the REFEDSs of eduPerson [17] and SCHAC [18]

3. Gain acceptance of the REFEDS standard by the EUDI-Wallet, Google, and Apple, enabling official support for issuance and storage in mobile wallets.

4. Implement multiple verification solutions, including smartphone applications, hardware readers, and backend systems, to facilitate widespread adoption by service providers.

5. Provide implementation support for HEIs, either through a dedicated software platform or integration tools.

6. Leverage Erasmus+ European University Alliances as early adopters to demonstrate feasibility and scalability.

By following these steps, eduTAP can help establish a trusted and standardized approach to digital student and staff IDs, ensuring security, usability, and broad acceptance across the higher education sector.

References

[1] Apple. Verify with Wallet. https://developer.apple.com/wallet/get-started-with-verify-with-wallet/.

[2] European Commission. EU Digital Identity Wallet. https://ec.europa.eu/digital-building-blocks/sites/display/EUDIGITALIDENTITYWALLET/EU+Digital+Identity+Wallet+Home.

[3] European Blockchain Services Infrastructure (EBSI). European Blockchain Services Infrastructure (EBSI) Website. https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home.

[4] eduGAIN website. https://edugain.org/about-edugain.

[5] European Parliament and Council of the European Union. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.

[6] European Parliament and Council of the European Union. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.

[7] Daniel Fett, Kristina Yasuda, and Brian Campbell. Selective Disclosure for JWTs (SD-JWT). Internet-Draft draft-ietf-oauth-selective-disclosure-jwt-17, Internet Engineering Task Force, March 2025. Work in Progress.

[8] Google. Google Wallet Identity. https://developers.google.com/wallet/identity.

[9] GÈANT. European Student Identifier. https://wiki.geant.org/display/SM/European+Student+Identifier.

[10] ISO and IEC. Personal identification – ISO-compliant driving licence – Part 5: Mobile driving licence (mDL) application. Standard ISO/IEC 18013-5:2021(E), International Organization for Standardization, 2021.

[11] ISO and IEC. Personal identification – ISO-compliant driving licence – Part 7: Mobile driving licence (mDL) add-on functions. Standard ISO/IEC TS 18013-7:2024, International Organization for Standardization, 2024.

[12] T Lodderstedt, K Yasuda, and T Looker. OpenID for Verifiable Credential Issuance. Technical report, OpenID Foundation, 2024.

[13] Alexander Loechel, Simon Lund, José Filipe Alves, and Morgan Persson. eduTAP – a Concept and System of Digital Identities for proximity on-site service access. Scientific Paper for EUNIS Conference 2025, 2025.

[14] Simon Lund. Spezifikation und Implementierung eines Pre-Consent Mechanismus im Kontext der Digitalisierung von Hochschulausweisen als Verifiable Credentials auf Basis von ISO/IEC 18013-5. Master's thesis, Ludwig-Maximilians-Universität München, Germany, 2025.

[15] Alexander Mühle, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. A survey on essential components of a self-sovereign identity. *Computer Science Review*, 30:80–86, 2018.

[16] U.S. Department of Homeland Security. Participating States and Eligible Digital IDs. https://www.tsa.gov/digital-id/participating-states.

[17] REFEDS. eduPerson Object Class Specification. Schema, REFEDS, 2022.

[18] REFEDS. SCHema for ACademia. Schema, REFEDS, 2022.

[19] Manu Sporny, Dave Longley, David Chadwick, and Orie Steele. Verifiable Credentials Data Model v1.1. Standard REC-vc-data-model-20220303, World Wide Web Consortium (W3C), 2022.

[20] O Terbu, T Lodderstedt, K Yasuda, and T Looker. OpenID for Verifiable Presentations. Technical report, OpenID Foundation, 2025.

[21] Oliver Terbu, Daniel Fett, and Brian Campbell. SD-JWT-based Verifiable Credentials (SD-JWT VC). Internet-Draft draft-ietf-oauth-sd-jwt-vc-08, Internet Engineering Task Force, 2024. Work in Progress.

[22] Wi-Fi Aware website. https://www.wi-fi.org/discover-wi-fi/wi-fi-aware.

Author Biographies

Simon Lund, is a developer at LMU München, contributing to identity management projects. He is involved in the implementation of eduTAP@LMU. Simon completed his master's degree in computer science with a contribution to eduTAP by specifying and implementing a preconsent 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

Alexander Loechel, Referent IT-Projekte, is a senior IT Manager at LMU München, responsible for strategic IT project management, digitalization, IT architecture, technology, and innovation management. He is the project lead of eduTAP. Alexander graduated in Informatics and researched in Operations Research about managing complexity and situational awareness systemd. Alexander Loechel's profiles on the web, LinkedIn: https://www.linkedin.com/in/alexander-loechel-323a176b/, GitHub: https://github.com/loechel, ORCID: https://orcid.org/0009-0003-9132-646