EPiC Series in Computing

Volume 105, 2025, Pages 80–93

Proceedings of EUNIS 2024 annual congress in Athens

EU-Wallets, Security and Trust for HEI/EDU

Hermann Strack[1], Guido Bacharach[2], Carsten Schmidt[3], Hans Pongratz [4,6], Matthias Gottlieb[5], Mirko Stanic[8], Michael Lierath[7], Arn Wassmann[7], Björn Kleinert[1]

[1] Harz University, Germany
[2] GovPart GmbH, Germany https://orcid.org/0000-0002-7945-9118
[3] University of Tartu, Johan Skytte Institute for Political Studies Center for IT Impact Studies, Lossi 36, 51003 Tartu, Estonia, https://orcid.org/0000-0001-8435-4313
[4] Stiftung für Hochschulzulassung (SfH), Germany
[5] Bavarian State Ministry for Digital Affairs, Germany, https://orcid.org/0000-0001-5983-6556
[6] TU Dortmund University, Germany, https://orcid.org/0000-0002-8376-0384
[7] HIS Hochschul-Informations-System eG, Germany
[8] EMREX User Group
hstrack@hs-harz.de, guido.bacharach@freenet.de, carsten.schmidt@ut.ee, hans.Pongratz@hochschulstart.de, matthias.gottlieb@stmd.bayern.de, mirko.stanic@azvo.hr, lierath@his.de, wassmann@his.de, bkleinert@hs-harz.de

Abstract

The European Commission will launch the EU Digital Identity Wallet (EUDIW) prototype following the European Digital Identity Directive eIDAS 2.0. options and attestations, also for HEI/EDU purposes and applications, with SDG cross border. The regulation emphasizes trust, security and interoperability, contributing to the broader goals of the European Digital Single Market. We consider extensions for security, privacy and trust enhancements at these process and infrastructure environments.

1 Introduction

The European Commission is set to introduce the EU Digital Identity Wallet (EUDIW) prototype (ARF 2024), aligning with the European Digital Identity Regulation eIDAS 2.0 (European Council, 2024), aimed at facilitating secure identity data sharing for EU citizens and businesses.

Prior to its implementation across Member States, the EU Digital Identity Wallet EUDIW undergoes testing in four so-called large-scale projects (LSPs): POTENTIAL, NOBID, DC4EU, and EWC, commencing on April 1st, 2023. Involving over 250 private companies and public authorities across 25

Member States and three associated countries (Norway, Iceland, and Ukraine), these projects aim to evaluate EUDIW across various sectors.

The POTENTIAL European Consortiums for Digital Identity focuses on promoting the development and deployment of EUDIW through six use cases, identify to and access a digital public service, opening a bank account, applying for a SIM, receive and store the mobile driving licence, signing contracts and claiming prescriptions.

NOBID consortium, spanning Nordic and Baltic countries, Italy, and Germany, partners with banks to pilot EUDIW for payment authorization, addressing wallet issuance, payment means provision, and retail payment acceptance.

The Digital Credential for Europe (DC4EU) Consortium pilots EUDIW in the educational and Social Security domains, aligning with the European Learning Model and utilising the European Blockchain Services Infrastructure; the foreseen use cases are applying for a job and Accessing Social Security benefits. The EWC plans to use the EU Digital Identity Wallet for multiple purposes. First, it will store and display Digital Travel Credentials to facilitate seamless cross-border travel within Europe. Second, it will focus on creating digital identity wallets for businesses and enable individuals to authenticate themselves across Europe as valid representatives of their organisations. Finally, the EU Digital Identity Wallet will be used to securely store payment credentials and authorise various transaction types, including account-to-account, card-based, and potentially token-based transactions. Overall, the LSPs aim to enhance digital identity management and foster cross-border mobility, organisational representation, and secure payment transactions throughout Europe.

As part of the European project DC4EU (DC4EU, Digital Credentials for Europe, 2024) the development of a converter is planned, tentatively named "EduConv," aimed at facilitating interoperability between different data models used for digital certificates in the European education sector. Currently, ELMO (EMREX, the ELMO XML schema, 2024) and ELM (ELM, ELM Browser, 2024) are two prominent data models, with ELMO primarily used with EMREX (EMREX, 2024) or EWP (EWP, 2024), and ELM used in connection with Europass (Europass, 2022). The converter's objective is to seamlessly translate certificates between these models, considering semantic content but not creator verification and validity checks. The plan involves creating mappings between ELMO XML and ELM JSON-LD formats (in both directions), with potential for additional conversions in the future. The technical implementation includes the development of a Software Development Kit (SDK) and an API, ensuring platform and language independence. The project governance ensures open-source delivery of code. Ultimately, successful acceptance criteria include compatibility with EMREX Gateway and adherence to GDPR regulations. The process aims to provide a seamless transition between different data models while ensuring security and compliance, with considerationof security aspects still in progress. In a similar way, ELM converters based on Open Badges and Microcredential data standard are also planned in this project. These three converter development projects are cooperating to ensure interoperability of the solutions and synergies in the development effort.

Already, Leijnse and Scheers (EUNIS 2023) showed up open questions, challenges in connecting the EUDIW ecosystem with the educational sector and processes. In this paper, we consider some additional fundamental open questions in these environments with some approaches for solutions especially for security, privacy, and trust (also from developments in EU and Germany), also in contrast to other projects:

1. Attestations Signature problem for multiple Converter Formats, e.g. for diplomas
2. Wallets, educational Trust Services and Trust/Security Infrastructure
3. Interoperability issues and wallets, Exchange and Migration problems, SDG/OOTS.

2 Challenges, upcoming Projects, Trends

The 2017 Tallinn Declaration on eGovernment reaffirmed Member States' dedication to advancing the integration of their public eServices and implementing the once-only principle. This commitment aims to facilitate the provision of efficient and secure digital public services, ultimately enhancing the lives of citizens and businesses. Building upon these principles, the 2020 Berlin Declaration on Digital Society and Value-Based Digital Government emphasised user-centricity and user-friendliness while also outlining additional crucial principles for digital public services, such as trust, security, digital sovereignty, and interoperability (Krimmer et al., 2021). This Regulation seeks to uphold these commitments by prioritising users and ensuring their awareness of the Once Only Technical System (OOTS), its procedures, and the implications of its usage.

The Once Only Technical System (OOTS) facilitates information sharing among public administrations across EU borders, transcending sectors and potentially extending beyond the life events specified in the Single Digital Gateway Regulation (SDGR). It operationalises the Once-Only Principle, which stipulates that citizens should not be required to furnish information to authorities if another authority already possesses it in electronic form. Key advantages of OOTS include reducing administrative burdens, enhancing efficiency, safeguarding personal data, enabling cross-border communication, and integrating with the Single Digital Gateway.

The Implementing Act on the Once-Only Technical System (OOTS) is applying since December 12th 2023, for the update of the eIDAS regulation Council and Parliament on the November 8th 2023 reached a provisional agreement. The technical work will continue to complete the legal text in accordance with the provisional agreement. When finalised, the text will be submitted to the Member States' representatives (Coreper) for endorsement.

Interoperability in the field of transport/verification of educational data

For years, an increasing number of projects, systems, and standards have been produced, with few ever being productively deployed. Specifically, in the domain of transport and verification of educational data, different and incompatible transport and verification mechanisms are often applied.

The data formats used in this context are also frequently diverse. The few formats that have achieved a certain status as de facto standards include: ELMO, European Learning Model (ELM), Open Badges, National Standards (e.g., in Germany, XBildung/XHochschule), SDG/OOTS-Evidences.

Evidence exchange in the OOTS is based on bilateral exchange between competent authorities. The Evidence Request serves as a message initiated by the Evidence Requester, encompassing all pertinent details necessary for soliciting evidence. This request can query structured or unstructured documents, depending on preference and availability. Prior to the request, the Evidence Broker assists in determining acceptable evidence types for a given procedure. A directory of Evidence Providers, along with associated metadata, is consulted in preparation. The request is then directed to a specific Evidence Provider identified within the Data Service Directory (DSD).

In response, the Evidence Provider generates an Evidence Response, providing essential information and correlating data with the respective Evidence Request. The response messages categorize into three states: Success, Unavailable, Failure.

The Evidence Exchange specification firstly illustrates the scope, goals, and architecture requirements of the Exchange Data Models, and the underlying business requirements for Evidence Requests, Evidence Responses, and Error Responses. Additionally, the Evidence Exchange specification outlines the scope, goals, and architecture requirements of Exchange Data Models, alongside underlying business requisites for Evidence Requests, Responses, and Error Responses.

These models utilize the functional capabilities of the OASIS RegRep V4 Query Protocol, structuring request and response messages as query models. Syntax elements are mapped to the OASIS RegRep V4 Query Protocol and the SDG metadata profile, enhancing its capabilities. Each Exchange Data Model defines a specific SDGR Application Profile, comprising syntax mappings for necessary information entities. The shape of the Exchange Data Models is illustrated through class diagrams, tables, and XML examples within the Evidence Exchange documentation (European Commission, 2023).

The OOTS reuses the eDelivery Building Blocking, provided by the EU and uses its Access Point (AP) specification. The initial iteration of the eDelivery building block originated from the e-SENS project, later adopted by the Connecting Europe Facility (CEF) and subsequently enhanced and maintained. It evolved into the reference framework for data exchange within the EU's eGovernment services (Krimmer et al., 2022).

eDelivery serves as a foundational element facilitating interactions and data exchange among public administrations, businesses, and citizens in a manner that is both interoperable and secure. Operating as a decentralized network, participants within the system adhere to eDelivery technical specifications, enabling seamless data exchange without requiring additional infrastructure. Data transmission through eDelivery can occur at local, national, and cross-border levels, depending on the specific project and policy context.

The overarching objective of the eDelivery building block is to promote data exchange and contribute to the establishment of a European Digital Single Market (Schmidt & Krimmer, 2022). This solution enables organizations with diverse ICT systems to connect to the eDelivery network and exchange data securely and reliably. To achieve this, eDelivery employs a 'four-corner model' and utilizes the AS4 messaging protocol for communication, which is freely available to users. Furthermore, all backend systems involved in data exchange must be integrated with the AS4 recipient. For a successful data exchange to take place, the senders must know the recipient's capabilities with regard to document types and data transport methods. This information is made accessible through the Service Metadata Publisher (SMP) service, which stores interoperability metadata and facilitates accurate exchanges between counterparties. The eDelivery SMP profile adheres to the open specifications based on the OASIS SMP version 1.0 standards, ensuring consistency and compatibility within the four-corner network.

Interoperable Europe Act

Interoperability is characterised by the capacity of organisations to collaborate effectively towards shared objectives, involving the exchange of information and knowledge through their supported business processes via data interchange among their ICT systems. Legal, organisational, semantic, and technical interoperability play pivotal roles in the successful implementation of digital government strategies.

Recent years have seen an increased focus on ensuring the interoperability of digital government systems, underscored by various EU-level initiatives. This emphasis aims to optimise the efficacy of digital solutions within the Single Market. The European Interoperability Framework (EIF), adopted in 2017, stands out as an important tool in advancing interoperable public services, particularly across national borders.

The establishment of the EIF was prompted by a significant need experienced by public administrations in the EU; the need for more specific guidance for public administrations on how to improve the governance of their interoperability activities Furthermore, the EC outlined two main problems in the field of interoperable digital public services:

- the fragmented delivery of digital public services in the EU and
- the fragmentation in the organisation and format of public data in the EU.

These topics are addressed by the proposal for a “Regulation laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act)” published in 2022.

All of this leads to a high level of complexity. This complexity can be drastically reduced through standardization. Approaches to Solutions, especially for exchange of diplomas or diploma attestations, in contexts of SDG and EU-Wallets include:

- Standardizing the diversity of solutions by selecting proven systems, including data formats and interfaces and avoiding the unnecessary development of new systems, if suitable using bridge constructs/converters if multiple de facto standards already exist, including security.
- Ideally, striving for standardization in the semantic, organizational, and legal realms across national borders. Ensuring that public funding supports the integration of existing solutions and standards into an interoperable ecosystem.

There are now some promising results on this topic, especially within the European framework:

- A European law is now in place to ensure interoperability (EU Commission, New Interoperable Europe Act, 2022)). An EU working group on interoperability (e.g., working groups of the EU Digital Education Hub, (EU Commission, 2024)) has commenced its work.
- The data formats ELMO (used by solutions for the exchange of digital credentials EMREX and EWP) and ELM (used by the Europass solution) have been made 100% semantically equivalent. Converters between these two data standards will be developed in the European project DC4EU (DC4EU, 2024), security aspects are work in progress (e.g. for signed data).
- A working group of the Directorate DIGIT of the European Commission and the EMREX Executive Committee have developed a proof-of-concept (PoC) of a technical and semantic bridge between EMREX and SDG/OOTS. This makes it possible to access EMREX data via SDG/OOTS and, in the medium term, also process it semantically. Discussions on the further development, security issues, maintenance, and support of this bridge are currently underway (European Commission, 2024), security aspects are work in progress.

These and other developments are expected to lead to an interoperable ecosystem in the medium term. However, a challenge remains as there is currently no general governance in the EU framework that can monitor and control the various standards as well as some security aspects, work in progress.

Digital School and University Certificates in Germany

The development of a digital university entrance qualification in Germany is gaining momentum. After the solution involving blockchain technology was discarded due to IT security issues (BSI 2021, Strack, H. et. al., EUNIS 2023), a new technological implementation was developed in 2023 in collaboration of several German ministries and the "Mein Bildungsraum" platform (BMBF - Mein Bildungsraum, 2024), based on earlier Research Projects for the "Nationale Bildungsplattform" (NBP) formerly – see Projects StudIES+ (EU CEF), NBP Infrastructure Kolibri (BMBF) (Strack et.al. 2019 - 2023), where at StudIES+ the first time an eIDAS eID/TS based eProSecal Wallet was developed (with the HEI/Edu applications eNotar and YourCredentials for attestations), where NBP and later Mein Bildungsraum with developments/rollouts in the BIRD project were supported by the German Ministry of Research and Education (BMBF), and intensively tested, see Knoth et. al. (EUNIS 2023). The tests of Mein Bildungsraum for eDiploma/Certificates were so successful that this solution is recommended for all German federal states under the German Online Access Act OZG (according to the One-for-All

principle - EfA). Additionally, in 2024, a so-called "field test" is planned to be initiated with selected schools and universities in the federal state of North Rhine-Westphalia.

The certificates thus created are intended to be utilized in other European projects and initiatives:

- In the European project DC4EU, a use case is planned to utilize digital German Upper Secondary School Certificates for application to European universities.
- A similar use case is envisaged in the EU project EBSI-VECTOR (EBSI-VECTOR, 2024).
- A concept is currently being developed with the Dutch study admission organization Studielink, (Studielink, 2024) enabling German school graduates to digitally apply to Dutch universities with German Upper Secondary School Certificates. An automated process through semantic application data extraction is planned.
- Similar initial discussions are underway with Croatia.

3 Approaches & Trials for improved Security & Trust

The Tasks for admission to higher education are supported by SfH (Stiftung für Hochschulzulassung, SfH) for German universities in the distribution of study places. On behalf of all 16 federal states of Germany, the SfH centrally grants study places for the nationally admission-restricted degree courses in human medicine, veterinary medicine, dentistry and pharmacy. In addition, the SfH coordinates the allocation of study places for around 2,000 locally admission-restricted and admission-free degree courses for around 160 universities on behalf of the universities. Statistical data for the allocation of study places for the winter semester 2023/2024: 259,462 applicants (heads) submitted 1,774,593 applications, 186,242 admissions for a study place were granted. For further statistics, see [*].

The application platform [†], the so-called application portal of the dialogue-oriented service procedure (DoSV), was updated with a connector to the BundID to ensure conformity with the OZG. The Online Access Act (OZG) was intended to facilitate the implementation of the European Single Digital Gateway (SDG) Regulation and has similar objectives at German level.
The BundID is a building block and serves to identify and authenticate citizens for online administrative transactions and implements the requirements of the European eIDAS Regulation in Germany. It is under the responsibility of the Federal Ministry of the Interior and Community[‡]. Around 10,000 accounts via BundID were created for applications for the winter semester 2023/24. As the SfH itself is permitted to send electronic notifications with legal effect via its own DoSV portal, the additional OZG functionality “BundID Inbox” is not used by the SfH.

Several types of access can be stored in the BundID OZG account. These are selected means of identification: user name & password, ELSTER certificate, online ID / German eID or a not German EU identity. A challenge for the connection was the transmission of only capital letters when using the German eID (identity card) and the collection of all first names in just one field. The eIDAS Regulation defines three different levels of security and trust (s. https://id.bund.de/de/faq):

- Basic - with the use of the "username & password" access type.
- Substantial – with use of the "ELSTER certificate" access type and individual "EU identities".
- High - with the use of the "online ID card" access type (e.g. online function of the eID card or electronic residence permit) and individual "EU identities" (EU citizen card).

[*] SfH statistics: https://www.hochschulstart.de/startseite/statistik/statistik-2024
[†] Application platform DoSV-Portal: https://dosv.hochschulstart.de
[‡] https://id.bund.de/de

The (German) National Feedback Component (NFK) is the central, multi-client solution in Germany for anonymous feedback on SDG services. The component can be integrated into applications and portals to record and collect user feedback. The feedback will then be forwarded to the OOTS. In the context of SDGs, the implementation or at least the integration of a feedback component is required. The SfH is currently not planning to develop a solution itself, but is examining the use of an announced NFK of ITZBund for the German National Once-Only Technical System (NOOTS), which is connected to the OOTS. Further, at universities digital enrollments with the LoA "high" level of authentication/trust based on eID/BundID in the SIS HISinOne are enabled, there is no need to appear in person when enrolling at a university (e.g. Univ. of Freiburg). The OZG return channel enables the legally compliant and digital delivery of notifications.

For the public administration E-Government at OZG, the Free State of Bavaria and the State of Schleswig-Holstein are looking at secure end-to-end processes. A first technical breakthrough was demonstrated at the Smart Country Convention 2023 in Berlin, using the respective state portals as the front-end and the OZG cloud as the back-end. In terms of security, this results in end-to-end encryption. This means not only the intermediate transport routes, but also from user input to processing and vice versa. Notifications from the administration are then sent to “Mein Unternehmenskonto Account”, which acts not only as an identity provider but also as a mailbox. Further the “Verwaltungsverfahrensgesetz” was changed 2024: all public administrations are allowed now to use qualified eIDAS seals for representing fully legally binding on administrative documents and notifications.

Wallets, Educational Trust Infrastructure, and Services Management

At the basic general infrastructure of the EU-Wallet EUDIW some points are further under development, e.g. trust management Chapter 6 (ARF 2024) or concerning the kind of PID implementation, see e.g. the proposal at Germany[§] (BMI 2023): 3 variants with favourites on signed eID data, similar like QEAA. This would be a new paradigm here, because in the past the German eID system did not sign eID data according to the secure channel principle for eID services BSI (2017), this may improve scalability in checking PID (reduced hardware access). Therefore, some security and trust aspects of the ARF concept and the German Architecture proposal for EUDIW are considered as “to be done”. Figure 1 shows a schematic illustration of the components of the EUDI Wallet.

But we consider now some security, privacy, and trust impacts/extensions for educational purposes at EU wallets and SDG/OOTS, e.g. for diplomas/ToR as EAA/QEAA, at different infrastructural levels.

1.) Obviously, a priority decision by regulation/law would be helpful between directly on EU-wallets stored Diplomas/QEAA (local copy) or such one derived from SDG portal/services based/Evidences on national registries. Using registries e.g. for diplomas, if available, would have more transparencies concerning trust/certificate chains for signatures/seals (e.g. with SDG mark-ups), including also options for integrated eIDAS preservation services for long term validation and concerning withdrawal options.

2.) It would be useful for HEI/Edu purposes, also to present the relationship of persons, not just their single PID. E.g. the “child/parent” relationship. Authentic sources for such attestations /evidence could be public administration registers or HEI/Edu institutions (different domains) on users’ journey, using YourCredentials Services.

3.) Different language and converter options e.g. for diploma content formats would cause additional effort and problems with multiple signing/sealing as equivalent valid formats,

[§] https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept-v1/-/tree/main

especially if the original issuer and signer/sealer are not involved - like for converters embedded in SDG portals. Similar concepts/services like the eIDAS preservation services might be helpful here, to avoid some additional trust services/providers for equivalencies attestations, only. Alternatively, the converter services should be available for the issuer and signatories of diplomas so that the converted data (with reference to the original) can also be signed and referenced multiple times by the issuer.

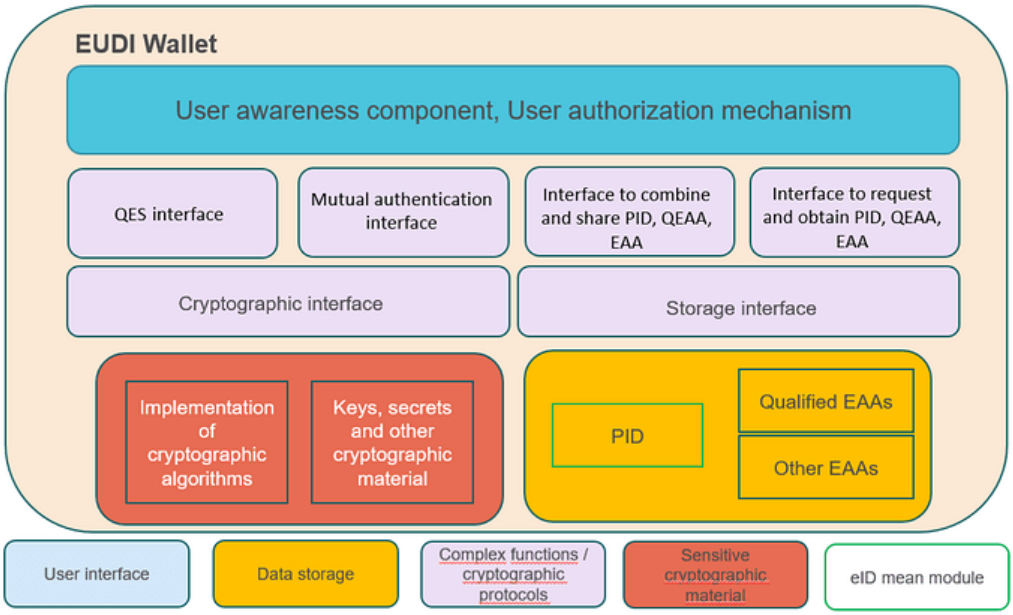

Fig 1: EUDI-Wallet (s. https://forum.eid.as/t/european-digital-identity-architecture-and-reference-framework/216)

4.) Different language and converter options e.g. for diploma content formats would cause additional effort and problems with multiple signing/sealing as equivalent valid formats, especially if the original issuer and signer/sealer are not involved - like for converters embedded in SDG portals. Similar concepts/services like the eIDAS preservation services might be helpful here, to avoid some additional trust services/providers for equivalencies attestations, only. Alternatively, the converter services should be available for the issuer and signatories of diplomas so that the converted data (with reference to the original) can also be signed and referenced multiple times by the issuer.

5.) Apparently, the SDG portals in conjunction with millions of EU wallets and connected NOOTS in the EU member states could cause some single points of dramatic failures and impact on the whole EU (security & safety), especially in case of cyberattacks. Therefore, we propose an enhanced trust infrastructure and management for the embedded protection of this highly distributed infrastructure and applications including wallets (short: Trustsistor).

Extended trust infrastructure and management

At network level, increasing IAM (Identity and Access Management) security is mostly achieved by using different security techniques. We propose here an extension with TPM protected Trust

Attributes integrations at IAM. Through these, it becomes possible to use additional higher levels of trust (LoA) across domains and systems, e.g. to protect the OOTS/NOOTS distributed systems. Through TPM-based authentication, a higher level of protection of processes and user and administrator roles can also be achieved in scenarios, where eID is not available. Specific roles (e.g. system administrators, RBAC/ABAC rule/attribute administrators) as well as network areas need to be specially protected from attacks and vulnerabilities both inside and outside. The aim should therefore also be to enforce a strict separation of roles, tasks, and net areas. To achieve this, firewalls and data diodes are used in the past to protect information flow and network segmentation based on network classifications. As additional protection against IAM attacks/circumvention, the IAM can be combined context-based with LoA trust level control attributes (TCA). For this purpose, mandatory IAM trust attributes can be used, which are cryptographically multilateral protected and added to protocol messages. These TCA attributes can be used both at document level and at transmission level, e.g. in sub-headers of IPv6.

Now, for adding trust-based control at the network level, we have introduced the concept of a "Trustsistor" component (Strack et.al. OID 2022, ICTA eMos 2022/2024). Figure 2 shows an Trustsistor architecture overview with the sub-components. This can add TCA IAM attributes of a Trust Service Provider TSP to IP flows and be inserted as additional mandatory IAM access control information between client (e.g. wallet) and server (e.g. also OOTS/NOOTS). The process is similar to the transistor concept for electrical circuits. We distinguish between a service user (SU), a service provider (SP), a service access controller (SPC) and a trust service provider (TSP). The latter is responsible for the (notarised) authentication of the TCA IAM attributes, e.g. through signatures/macs.

In addition, a "Trustsistor Injector" (TSOI) and a "Trustsistor-Controller" (TSOC) is required. The "Trustsistor Injector" (TSOI) inserts trust identifiers on the service client side into the IP flow (e.g. as IPv6 sub headers), based on monitoring and validation of the client site. The "Trust Controller" (TSCO) checks the trust identifiers on the flow to the service provider site according to a trust attribute access policy. In a multilateral protected environment, the TSOI and TSOC components must be protected by a TPM to ensure secure implementation and operation.The key point of the Trustsistor is the externalisation of trust relations, i.e., trust relations are established also independently from the communicating parties. The trust relation exists directly between the communicating party, the TSP and the Trustsistor and thus indirectly based on the TSP rule authorities at operational and supply chain level, e.g. by security evaluations/certification according to Common Criteria (Enisa 2024, BSI CC).

Our approach exceeds the zero-trust concept (Rose et.al., NIST 2020) and differs also from implementations such as data diodes. Data Diodes enforce one-way communication and are used, for example, for separation of classified net areas or in industrial plants to separate OT (operation technology, here industrial control) from IT (information technology, here office network). One-way communication, whereby user data, for example log data, can only be transferred from the OT to the IT network. Attacks from the IT into the OT network are prevented. Moreover, the Trustsistor allows the attributing authority to enforce rules multilaterally, so that these rules cannot be circumvented by either communicating party, even in collaboration. We call these rules mandatory rules. A connection passing a Trustsistor, and therefore meeting all (multilateral Trust) policy requirements, is called a (Trust)policy-compliant connection.The Trustsistor concept allows the controlling domain to enforce policy-compliance by creating mandatory rules. These rules must cover the policy they are intended to enforce, which is the responsibility of the rule creator. Thus, establishing multilateral trust. In order to enforce the mandatory rules, it is necessary to prevent the Trustsistor from being bypassed or any of the communication partner's systems from being tampered with. Bypassing can be prevented by the Trustsistor itself attaching a cryptographic attribute to the packet after the rules have been applied. This allows the recipient to track that the packet has passed through a Trustsistor. Tampering with the communication partner's systems is prevented by TPMs. These enable to detect changes in the system down to the application and network level and to prevent the sending or receiving of network packets in the event of manipulation.

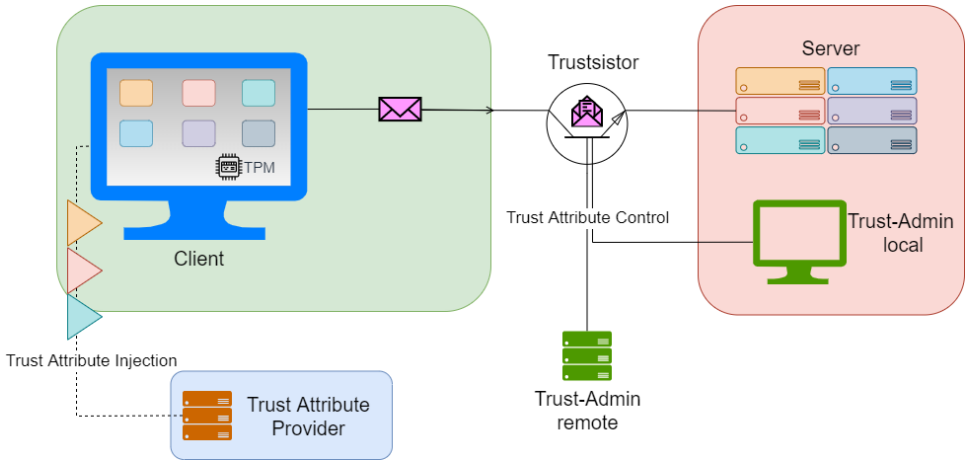

Fig. 2: Trustsistor Architecture (Source: Strack et.al. (2022c/d))

Attributes provided by the attribute provider and ultimately generated by the communication partners are attached to the network packets. Since the attributes are cryptographic attestations for the server, they generally have similarity to cryptographic authentication attributes. Therefore, the attributes used for the Trustsistor can be attached to the network packet equivalent to IPSec AH attributes (RFC4302) if operating at the IP layer. The benefit is that it is applicable to IPv4 and IPv6 and thus for the majority of network connections. Trustsistor could be used not only to protect the distributed OOTS/NOOTS infrastructure, but also the communication relations between EUDIW wallets and these infrastructures. Therefore, additional Wallet interfaces for using TCA attributes are required, e.g. included in the wallet setup process. A binding of TCA attributes to security valuations/certifications e.g. acc. to Common Criteria would allow new Trust enhancements connections between security by design and managements methods, extensible also to HEI/Edu certification standards.

4. Conclusions

The EUDIW initiative is an essential step towards enhancing digital identity management and facilitating secure cross-border interactions within Europe. The large-scale projects POTENTIAL, NOBID, DC4EU and EWC provide a comprehensive evaluation framework covering different use cases from access to public services to the management of educational credentials. The development of interoperability solutions, such as the EduConv converter, underlines the commitment to ensure seamless data integration between different systems, we added proposals to integrate signatures/trust services after conversion. For the application of the EUDIW eco system also to educational purposes some add-ons and extensions are necessary or useful, especially for security, privacy and trust, some of them still announced as to be done at ARF, some other under development in DC4EU. For improvements, we made proposals for additional enhancements, architectures, components and embeddings for security and trust at current developments at DE/EU at application and infrastructure levels (e.g. Trustsistor based), e.g. to protect the distributed OOTS/NOOTS large infrastructures as well as EUDIW, which will be available to all EU member states citizens. Parts of the underlying research were supported by funds from the EFRE/ERDF and the federal State of Saxony-Anhalt, www.cslsa.de .

References

ARF 2024 - Architecture and Reference Framework 1.3.0 (2024): European Digital Identity Framework, https://github.com/eu-digital-identity-wallet/eudi-doc-architecture-and-reference-framework/blob/main/docs/arf.md

BMI 2024: Architecture Proposal for the German eIDAS Implementation EUDIW (2024): https://gitlab.opencode.de/bmi/eudi-wallet/eidas-2.0-architekturkonzept

BSI CC: Certification to CC, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/zertifizierung-nach-cc_node.html

European Commission (2023). OOTS Technical Design Documents https://ec.europa.eu/digital-building-blocks/sites/display/TDD/OOTS+Technical+Design+Documents+v1.0.0

ENISA 2024: Cybersecurity Assessments, Evaluations & Certifications - State of Play 2018-2022, January 2024: https://www.enisa.europa.eu/publications/cybersecurity-market-assessments

Fridell Tor, Vangen Geir, Mincer-Daszkiewicz Janina, Norder Jan-Joost, Rautio Kimmo, Drvodelić Igor, Bacharach Guido (2023):The future is in your wallet – how EMREX plans interaction with the EUDI wallet. In: Jean-François Desnos und Martín López Nores (ed.): Proceedings of EUNIS Congress 2023. Vigo, EasyChair, Journal EPiC Series in Computing, vol 95, p. 209-215

Hühnlein, Detlef; Hühnlein, Tina; Hornung, Gerrit; Strack, Hermann (2020): Towards Universal Login. In: Lecture Notes in Informatics (LNI) (Open Identity Summit 2020), S. 193–200. DOI: 10.18420/ois2020_18

Knoth Alexander, Soldo Erwin, Clancy Kathleen and Lucke Ulrike (2023): A Distributed Infrastructure for Secure Diplomas: Proof of Concept and First Experiences; In: Jean-François Desnos und Martín López Nores (ed.): Proceedings of EUNIS Congress 2023. Vigo, EasyChair, Journal EPiC Series in Computing, vol 95, p. 181-192

Krimmer, R., Dedovic, S., Schmidt, C., & Corici, A.-A. (2021). Developing Cross-border E-Governance: Exploring Interoperability and Cross-border Integration. In N. Edelmann, C. Csáki, S. Hofmann, T. J. Lampoltshammer, L. Alcaide Muñoz, P. Parycek, G. Schwabe, & E. Tambouris, Electronic Participation Cham.

Krimmer, R., Solvak, M., Alishani, A., Dedovic, S., Schmidt, C., & Castle, S. (2022). European Interoperability Landscape Report 2022 Public Report.

Leijnse Peter, Scheers Menno (2023): The need for sectoral ownership to steer developments of the European Digital Identity Wallet for the benefit of education.In: Jean-François Desnos und Martín López Nores (ed.): Proceedings of EUNIS Congress 2023. Vigo, EasyChair, Journal EPiC Series in Computing, vol 95, p. 119-128

Mein Bildungsraum (2024), Retrieved February 20, 2024, from https://www.meinbildungsraum.de/en/

Rose Scott, Borchert Oliver, Mitchell Stu, Connelly Sean (2020): Zero Trust Architecture, NIST Special Publication 800-207, https://doi.org/10.6028/NIST.SP.800-207

Schmidt, C., Krimmer, R. (2022). How to implement the European digital single market: identifying the catalyst for digital transformation. Journal of European Integration, 44(1), 59-80. https://doi.org/10.1080/07036337.2021.2011267

Strack, Hermann; Otto, Oliver; Klinner, Sebastian; Schmidt, André (2019): eIDAS eID & eSignature based Service Accounts at University environments for cross boarder/domain access. In: Heiko

Roßnagel, Sven Wagner und Detlef Hühnlein (ed.): Open Identity Summit 2019. Proceedings. Open Identity Summit 2019. Garmisch-Partenkirchen, Germany, Gesellschaft für Informatik e.V. (GI) (Lecture Notes in Informatics (LNI) - Proceedings, P-293), S. 171–176.

Strack, Hermann; Bacharach, Guido.; Klinner, Sebastian; Otto, Oliver; Schmidt, André (2019): eIDAS eID & eSignature for HEI/EDU Applications. Proceedings of EUNIS 2019, NTNU Trondheim. In: European Journal of Higher Education IT 2019 (1). Online verfügbar unter https://eunis.org/erai/2019-1/

Strack H., Steiper R.-D., Waßmann A., Bacharach G., Gottlieb M., Radenbach W., Pongratz H., and Norder J. J. (2021b). "Progress on Digitization of Higher Education Processes towards Standards EU & DE." Pp. 77–88, in EPiC Series in Computing.

Strack H., Gollnick M., Karius S., Lips M., Wefel S., Altschaffel R., Bacharach G., Gottlieb M., Pongratz H., and Radenbach W. (2022a). "Digitization of (Higher) Education Processes: Innovations, Security and Standards." EPiC Series in Computing 86:22–29. doi:10.29007/rrg4.

Strack H. (2022b). „Additional Proposals for extensions ELMO/EMREX by Hochschule Harz (HSH)" https://github.com/emrex-eu/elmo-schemas/issues/81

Strack, H.; Karius, S.; Gollnick, M.; Lips, M.; Wefel, S.; Altschaffel, R. (2022): Preservation of (higher) Trustworthiness in IAM for distributed workflows and systems based on eIDAS. In: Heiko Roßnagel, Christian H. Schunck und Sebastian Mödersheim (ed.): Open Identity Summit 2022, Copenhagen, Denmark. Gesellschaft für Informatik. Bonn: Gesellschaft für Informatik (Lecture notes in Informatics (LNI) Proceedings, volume P-325), S. 125–130.

Strack, Hermann; Bacharach, Guido; Steiper, Ramona-Denisa; Gottlieb, Matthias; Radenbach, Wolfgang; Waßmann, Arn; Pongratz, Hans, Norder, Jan-Joost. (2021): Progress on Digitization of Higher Education Processes towards Standards EU & DE. In: Proceedings EUNIS 2021, EasyChair, Journal EPiC Series in Computing, 78, 77-88.

Strack, Hermann (2022): Kontext Cybersecurity und Standards (wie eIDAS) im Bildungswesen. In: Herausforderungen und Lösungsansätze im Umgang mit elektronischen Identitätsnachweisen im Hochschulumfeld, S. 28–51. Bic Picture NRW, Online: https://kdu.dh.nrw/fileadmin/user_upload/kdu/Whitepaper_Digitale_Identitaeten_Hochschulen.pdf

Strack, Hermann; Gollnick, Marlies; Karius, Sebastian; Lips, Meiko; Wefel, Sandro; Altschaffel, Robert et al. (2022a): Digitization of (Higher) Education Processes: Innovations, Security and Standards. In: Proceedings of EUNIS 2022, University of Göttingen, EasyChair Journal EPiC Series in Computing, 86, S. 22–33.

Strack, Hermann; Gollnick, Marlies; Karius, Sebastian; Kopitz, Robin; Lips, Meiko; Wefel, Sandro (2022d): Multilevel Trustworthiness for improved Process and Network Security in Critical Infrastructures and Domains. In: Proceedings of ICTA-EMoS 2022. Arusha, Tanzania, 24. - 25.11.2022, Springer Nature, 2024, https://doi.org/10.1007/978-3-031-56603-5_16

Strack, Hermann; Gollnick, Marlies; Karius, Sebastian; Bacharach, Guido; Fridell, Tor; Gottlieb, Matthias, Jan-Joost Norder, Hans Pongratz, Wolfgang Radenbach, Carsten Schmidt, Mirko Stanić, Geir Megne Vangen, Arn Wassmann, Sandro Wefel (2023): EU CrossBorder and OOT for HEI/Edu Workflows and Infrastructures with Interoperability, Standards and Security. In: Jean-François Desnos und Martín López Nores (ed.): Proceedings EUNIS Congress 2023. Vigo, 13.06 - 16.06.2023: EasyChair, Journal EPiC Series in Computing, 95, 266-246

Studielink (2024), Retrieved February 20,2024, from https://www.studielink.nl/

Author biographies

Guido Bacharach, Former Head of Strategy and Digitization Unit at the Stiftung für Hochschulzulassung in Dortmund. After his study he had management positions especially in the sales area and in public services. The focus of his work is on strategic digitization, process improvement and project management. He is a member of the Deutsche Gesellschaft für Projektmanagement (GPM e.V.) and VOICE e.V. and co-founder of the Netzwerk Digitale Nachweise.

Prof. Dr. Hans Pongratz is CIO of the Stiftung für Hochschulzulassung (SfH), full professor at the Technical University of Dortmund and former Senior Vice President for IT-Systems & Services and the Chief Information Officer (CIO) of the Technical University of Munich (TUM), Germany. He is member of numerous boards, committees, reviewer groups, and co-founder of the digital credentials consortium (DCC).

Carsten Schmidt has a judicial background and works for the Johan Skytte Institute of Political Studies, University of Tartu; His focus is coordinating the mGov4EU project research and development activities at the University of Tartu. Previously he was involved in several other European projects like the Once-Only Principle Project (TOOP) as sustainability manager and the other large-scale projects, e-SENS and e-CODEX, as project coordinator. He worked as a senior legal officer for the Ministry of Justice of North-Rhine Westphalia, Germany.

Prof. Dr. Hermann Strack, a full professor for network management and computer sciences since 2000 at HS Harz, also the coordinator for Informatics / E-Administration study course, the speaker of the Competence Centre as well as the head of the Network Laboratory (netlab) and the ICT Innovation Laboratory - SecInfPro-Geo (Security, Infrastructure, Process Integration & Geographical Information Systems), as well as the coordinator of CyberSecurity Network LSA (see https://clsa.de). Furthermore, he is a member of the Gesellschaft für Informatik (GI e.V.) and the Competence Center for Applied Security Technology (CAST e.V.). In 2007 Prof. Strack was a co-founder of the European rs3g-group in Rome - rome-student-systems-and-standards-group (rs3g) - a group which moved to European University Informations Systems as an EUNIS task force in 2009. Prof. Strack has focused his research activities mainly on the conception, the development/implementation of systems in the areas of IT-Security and E-Government. Specifically, he focuses on the development of eID based applications with the identity card in Germany (eID/PA) and eID/eIDAS, namely in the EU CEF Projects TREATS, StudIES+ and Cyber Security Alliance Saxony-Anhalt (EFRE), https://studies-plus.eu https://cslsa.de

Dr. Matthias Gottlieb is project manager at the Bavarian State Ministry for Digital Affairs, Germany. He is Deputy Editor-in-Chief of the International Journal of Engineering Pedagogy (iJEP) and reviewer of numerous journals and conferences. After studying computer science and did his Ph.D. and was senior researcher at the Technical University of Munich (TUM), Germany. He engaged in Information Systems research areas such as Big Data and Human Computer Interaction. His current research interests are Digitization of Business Processes, Business Development, Digital Transformation, and Digital Credentials of Higher Education Institutions.