H. Roßnagel, C.H. Schunck, S. Mödersheim (Hrsg): Open Identity Summit 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 125

# Preservation of (higher) Trustworthiness in IAM for distributed workflows and systems based on eIDAS

Hermann Strack[1], Sebastian Karius[2], Marlies Gollnick[3], Meiko Lips[4], Sandro Wefel[5], Robert Altschaffel[6]

**Abstract:** The secure digitalisation of distributed workflows with different stakeholders (and trust relationships) using systems from different stakeholder domains is of increasing interest. Just one example is the workflow/policy area of student mobility. Others are from public administration and from economic sectors. According to the eIDAS regulation, eID and trust services (TS) are available across EU - upcoming also EUid & wallets (eIDAS 2.0) - to improve security aspects (providing interoperability or standards). We present some security enhancements to maintain higher trustworthiness in Identity and Access Management (IAM) services for different policy areas with mandatory, owner-based and self-sovereign control aspects - based on eIDAS and different standards and the integration of views/results from deployed or ongoing projects (EMREX/ELMO, Europass/ EDCI, eIDAS, EUid, Verifiable Credentials, NBP initiative, OZG implementation, Self-Sovereign Identities SSI, RBAC, ABAC, DAC/MAC, IPv6) and a trustsistor.

**Keywords:** eIDAS eID & TS (2.0), EUid, IAM, LoA, authentication, access control, notarisation, NBP initiative, OZG, Self-Sovereign Identities SSI, RBAC, ABAC, DAC/MAC, IPv6, trustsistor

## 1 Introduction

Digitization of workflows in different fields like Education, Public Administration, Health Services and Business needs for compliance realizations, checks and balances according to their policies. This includes the implementation and integration of security and trust services, as well as trusted entities/roles, using methods of security by design and management. Obviously, strong authentication and access control would improve the security against different threats and vulnerabilities from outside or inside the domains or interest groups involved. This includes, for example, exploiting vulnerabilities to obtain identities, roles or other data, or abusing user roles and administrator rights.
Important intermediate as well as final results at workflow level are documents, certificates and diplomas, with security requirements for integrity, authenticity and privacy, which also meet the requirements for reliable archiving. The integration of PKI

[1] Hochschule Harz, FB Automatisierung und Informatik, 38855 Wernigerode, hstrack@hs-harz.de
[2] Hochschule Harz, FB Automatisierung und Informatik, 38855 Wernigerode, skarius@hs-harz.de
[3] Hochschule Harz, FB Automatisierung und Informatik, 38855 Wernigerode, mgollnick@hs-harz.de
[4] Hochschule Harz, FB Automatisierung und Informatik, 38855 Wernigerode, mlips@hs-harz.de
[5] Martin-Luther-Universität Halle-Wittenberg, Institut für Informatik, 06120 Halle (Saale), sandro.wefel@informatik.uni-halle.de
[6] Otto-von-Guericke-Universität Magdeburg, Fakultät für Informatik, 39106 Magdeburg, Robert.Altschaffel@iti.cs.uni-magdeburg.de

cbe doi:18.18420/OID2022-11

based eIDAS, eID and TS would support securing the workflows and their policies and roles accordingly. This applies in particular in the IAM field, with access control policies and architecture elements in an EU wide interoperable resp. standardized manner. See ETSI[7] / TR BSI[8] for further new developments, e.g. eIDAS 2.0. see [KSSR20; KSSK20]. In chapter 2 we present the current status of the KOLIBRI NBP project, in which the authors' institutions are involved (BMBF funded). In chapter 3, we provide an outlook for security improvements in various policy areas. We will apply our experiences from implementing portions of the National Educational Platform (NBP) with Level of Assurance/LoA "high" to additional policy and IAM protection areas, including network segmentation, workflow/access controls based on trust and separation of duties (SOD).

## 2 National Educational Platform Initiative (NBP)

The project "KOLIBRI" has implemented a prototype for the National Educational Platform (NBP) in Germany based on open source and standards. In addition, important eIDAS components got successful security evaluations (e.g. Common Criteria ISO 15408). All types of educational institutions are enabled to connect to the platform in a secure and privacy-preserving manner, also via standards (ongoing) on metadata level.

The research prototype of the project "KOLIBRI" implements the following features: Security & Privacy (regarding eIDAS/eID & TS standards, GDPR, OZG[9]), an identity broker and authorisation system with Single Sign-On (SSO), central collaboration services, connectors/metadata for decentralised Identity Management Systems and Identity Providers (IDP), connection to user wallets (with SSI/eIDAS 2.0 functions), and connections to EU services and standards: EMREX/ELMO, Europass/EDCI/VC [Min17]. In particular, the integration of SSO (Single Sign-On) by „KOLIBRI" takes into account the different levels of assurance (LoA) for the strength of authentication security according to the EU eIDAS regulation (LoA: low, substantial, high).This is important for cross-domain user integration and SSO, also at LoA "High" using eID. More additional attributes such as group membership can be transmitted.

A central Identity Broker enables the connection of the identity providers (IDP) of the satellite systems of the education providers. In order to enable citizens without special educational membership to have secure identities with full legally binding at the document transmission level, the login was also connected via a governmental eID service provider with eID card enabled login (OZG-Nutzerkonto). This can be used for legally binding

[7] https://www.etsi.org/newsroom/news/1111-2016-07-etsi-publishes-european-standards-to-support-eidas-regulation
[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03130/TR-03130_TR-eID-Server_Part3.html
[9] OZG – Online-Zugangsgesetz/Online Access Law, OZG-Nutzerkonten: https://www.onlinezugangsgesetz.de

processes between state educational institutions, authorities and the platform, without extra qualified electronic signature (QeS).

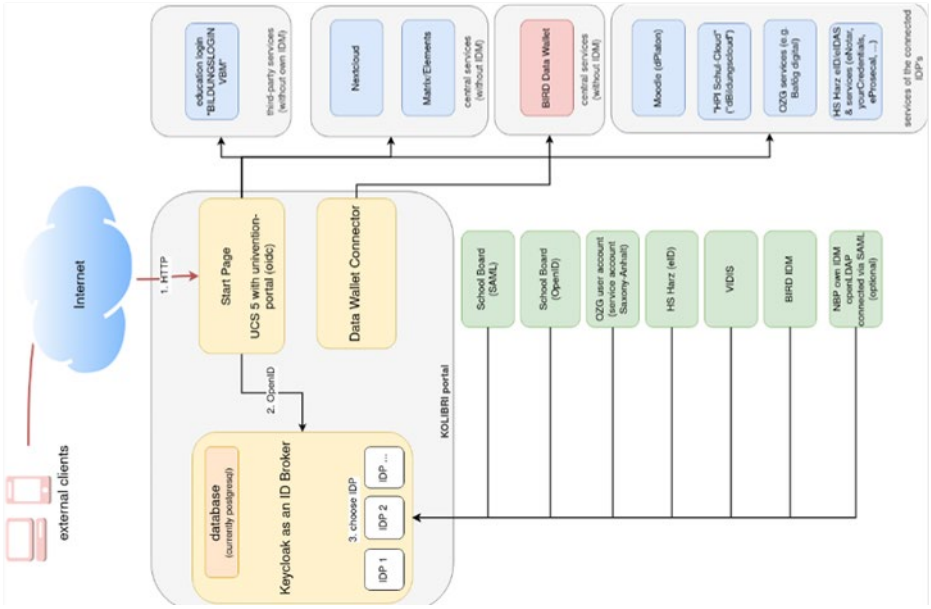


Fig. 1: KOLIBRI NBP: Keycloak as an ID Broker and eID/OZG services as IDP

The applications of the Harz University of Applied Sciences connected in the KOLIBRI platform use the online features of the German ID card to provide various services. These services are: eProsecal - provides highly secure authenticated access (LoA "high") for various university services/actors through an ID card-based logon and account process, including fully legally binding. Processes with multiple multi-user/role references (n:m) can also be mapped. Users have access to the data of all released processes via their eProsecal basic account and can also securely share them with other users and even with authorities in a legally binding manner (eID-based sharing). This results in a SSI (Self-Sovereign Identity) wallet function, without blockchain integration, based on the properties of the eID system in Germany. eInternship – internship management/contracts between university and company; eTor/eTestate - registration/attendance management for exams and lab practicals; eColloquium - signed colloquium exam forms/certificates (ELMO/EDCI/VC); eNotar - offers the possibility to provide documents with a qualified signature in a legally binding secure manner (public service laws in DE VwVfG §3a/§33, [SBKO19]). These services can be combined with further eIDAS-based services such as time-stamping and long-term storage services with oversignature (BSI Standard TR ESOR[10], eIDAS Preservation Standard). In addition, EU-wide time-dependent

[10] https://bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR-ESOR-LEIT.pdf

cybersecurity crypto requirements are covered, with the accompanying cryptoalgorithm management (EU SOGIS ) providing a further basis for trust.; YourCredentials – extend the eNotar principle to the authentication and notarisation of derived identities and attributes (e.g. by RBAC/ABAC, [AHAZ19]) from their trust domains, e.g. for wallets for eIDAS 2.0 / EUid[11]. This enables the handling of multiple identities of a person arising from different phases/providers in that person's life. The notarisation of identity assignment by the trust service is extensible to relationships of related identities such as parents and children.

## 3 Protection of workflows/roles/systems via IAM & Trustsistor

With current technology the use of TPM attestations/attributes at IAM would enable additional higher LoA contexts, including for mandatory control policies across domain/system boundaries. In context of our NBP prototype, it can be used for enhanced protection of important workflow roles like eNotar or system administrator roles, also in scenarios where eID is not available or necessary [We22, Kl09, JA09]. Additionally, it is important to protect workflows & trusted roles (e.g. eNotar roles as well as system administrator roles and RBAC/ABAC control schemes), entities, documents and systems against attacks on network or systems vulnerability levels, especially hacking from outside and inside, or misuse of separation of duties (SOD) [MZNO19]. Important measurements are information flow protections and network segmentations based on classifications of networks, entities and systems using firewalls and data diodes[12] [BJBR14], see Fig. 2 (inspired by privacy/BLP/MAC/MLS policies). But to protect additionally against IAM attacks (bypassing), it could be combined with different LoA levels for IAM. Therefore, also Mandatory LoA IAM attributes (cryptografically protected/binding, e.g. by MACs, derived/based e.g. on YourCredentials notarisations, could be securely added to protocol messages by using sub-header principles as well as on document level. This can be done in an analogous manner to IPv6[13] and would be worth exploring for enhanced and extended authentication and access control layers based on firewall, data diodes, and access control components, e.g. for improving ZeroTrust[14] schemes. Therefore, we introduce the concept of a „Trustsistor“ TSO component that is integrated, e.g. into firewall or proxy components, and reinforces trust relationships by adding trust attributes of a TSP to IP flows, e.g. between client and server as additional IAM (mandatory) access control information (MACI contexts). The notion is similar in some sense to the "transistor concept" in electrical flows. This means, we would differentiate between a service user SU, a service provider SP and service access controller SPC, as well as a trust service provider TSP notarising ACI[15] trust attributes TACI, e.g., by signatures/MACs.

[11] https://ec.europa.eu/commission/presscorner/detail/de/IP_21_2663
[12] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6949883
[13] https://www.ietf.org/blog/ipv6-internet-standard/
[14] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
[15] ACI: Access Control Information

Further we propose the components “Trustsistor-Injector (TSOI)” for injecting trust identifiers/labels into the IP flow on the part of the service client using e.g. IPv6 sub-headers and the “Trustsistor-Controller (TSOC)” for checking the required TACI attributes on the part of the service provider/controller according to a TACI access policy. By the way: for better multilateral system integrity security the TSOI/TSOC components should be protected by TPM. Based on the TSO model, secure implementation of access control policies can be done with additional TACI attributes on IP flows. The research conducted here was partly funded by 3 EU funded projects under the umbrella of ”CyberSec LSA”[16] (EFRE).

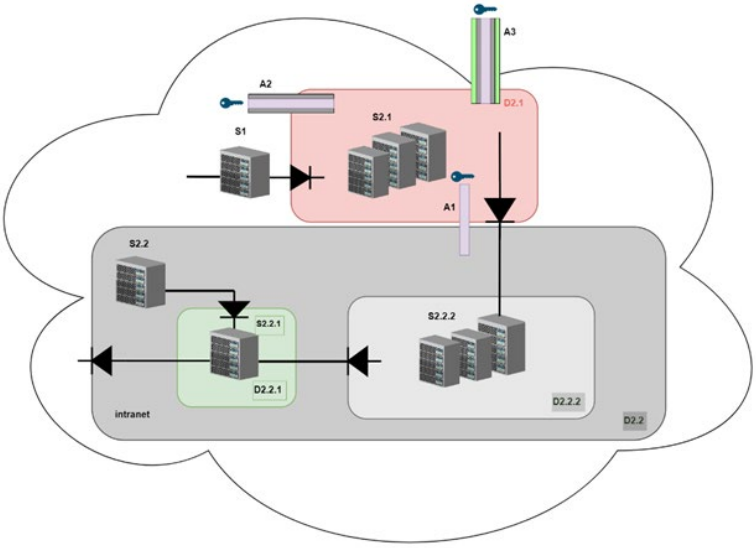


Fig. 2: Combined protections of privacy/flows/MAC and LoA Auth./IAM/trusts level at domains

## 4 Conclusion

The development of a prototype of the National Education Platform NBP revealed strengths and weaknesses of current Single Sign On (SSO) solutions. We showed that the use of eID-based authorization (LoA high) can be usefully employed in the area of SSO in the context of IAM. Using HW can significantly improve the security of platforms such as NBP and also the simplicity of authentication, since in best cases only a few strong IAM systems are needed. To further prevent security vulnerabilities such as access forgery, spoofing, leakage, etc. at the network transmission and security layer, we have outlined how the use of data diodes and network packets marked with Trust-ACI attributes

[16] https://cslsa.de

can preserve the security gained through strong authentication in conjunction with TACI notarisations at the network layer. This can be done by combining appropriate firewall rules and Trustsistor TSO injection and Trustsistor TSO controller components. Thus, the authorization defined at the IAM level is extendable by (mandatory) Trust Attributes (also LoA high), also at the network level.

## Bibliography

[AHAZ19] Aftab, M.U.; Qin, Z.; Hundera, N.W.; Ariyo, O.; Zakria; Son, N.T.; Dinh, T.V. Permission-Based Separation of Duty in Dynamic Role-Based Access Control Model. *Symmetry* 2019, *11*, 669. DOI: 10.3390/sym11050669

[BJBR14] Bhatkalkar, B. J.; Ramegowda: A Unidirectional Data-flow Model for Cloud Data Security with User Involvement during Data Transit, 2014 International Conference on Communication and Signal Processing, IEEE Explore, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6949883

[EU14] EU: Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, 2014.

[HH20] Hühnlein, D.; Hühnlein, T.; Hornung, G.; Strack, H. (2020): Towards Universal Login. In: *LNI (Open Identity Summit 2020)*, 193–200. DOI: 10.18420/ois2020_18

[Kl09] Klenk, A.; Kinkelin, H.; Eunicke, C.; Carle, G.. 2009. Preventing identity theft with electronic identity cards and the trusted platform module. In *Proceedings of the Second European Workshop on System Security* (*EUROSEC '09*). ACM, NY, USA, 44–51. DOI: 10.1145/1519144.1519151

[KSSK20] Kusber T.; Schwalm, S.; Shamburger K.; Korte U.: Criteria for trustworthy digital transactions - blockchain/DLT between eIDAS GDPR, data and evidence preservation, In: *LNI (Open Identity Summit 2020)*, DOI: 10.18420/ois2020

[KSSR20] Kubach, M.; Schunck, C. H., Sellung, R. ; Roßnagel, H.: Self-sovereign and Decentralized identity as the future of identity management?. In: *LNI (Open Identity Summit 2020)*, 35-47. DOI: 10.18420/ois2020_03

[Min17] Mincer-Daszkiewicz, J.: EMREX and EWP offering complementary digital services in the higher education area, *Proceedings of EUNIS*, Münster, 2017.

[SBKO19] Strack, H.; Bacharach, G.; Klinner, S., Otto, O.; Schmidt, A.: eIDAS eID & eSignature for HEI/EDU Applications - eIDAS eID & eSignature based Service Accounts at University environments for crossboarder/domain access. In: *European Journal of Higher Education IT* 2019-1 https://www.eunis.org/erai/2019-1/

[We22] Web Authentication: An API for accessing Public Key Credentials, https://www.w3.org/TR/webauthn-2/#sctn-attestation, accessed: 21/02/2022.