eIDAS eID & eSignature based Service Accounts at University environments for cross boarder/domain access

Hermann Strack[1], Oliver Otto[2], Sebastian Klinner[3], André Schmidt[4]

Abstract: University domain/scenario use cases based on eIDAS eID & eSignature extended user service accounts are implemented in the EU CEF projects TREATS and StudIES+, integrating hybrid ID concepts (legacy & eID). eNotar services will offer to integrate legacy binding in process and document flows, transfers to other areas are considered (Industry 4.0, ABAC).

Keywords: eIDAS, eID, eSignature, Serviceaccount, University, eNotar

1 Introduction

Use cases at university student/user management were implemented as eID/eIDAS based web accounts & applications to support cross boarder/domain usage & mobility (EU) for students and researchers as well as for study applicants for enrolment [Str17]: MyCredentials, MyResearch & Development (MyRaD), MyFBAI. eID/eIDAS based authentication and authorization extensions were integrated in pre-existing GeID-based applications (German national eID/identity card), funding/co-financing by EU CEF program 2015, project "TREATS[5] - Trans-European Authentication Services", Action No. 2015-DE-IA-0065. An outlook to ongoing work/results by the EU CEF 2017 funded project StudIES+[6] is given (Student's identification and electronic signature services), Action No. 2017-DE-IA-0022, especially to the ePracticum/eInternship service accounts/ applications and the eNotar/YourCredentials cross domain concepts. During the TREATS project the german eID [BKM08] server technical rules TR03130 [BSI17] were extended to include the eIDAS [EU14, LLR15] connector interfaces [EU15] and services (via SAML over TLS) to check cross boarder eID accesses from other EU MS (European Member States). During the StudIES+ project additionally some eIDAS (remote) eSignature based university services and applications are under development (ongoing work), e.g. ePracticum/eInternship, eDiploma/eTOR or YourCredentials, see section 3/4.

[1] Hochschule Harz, FB AI, Friedrichstr. 57-59, Wernigerode 38855, hstrack@hs-harz.de
[2] Hochschule Harz, FB AI, Friedrichstr. 57-59, Wernigerode 38855, ootto@hs-harz.de
[3] Hochschule Harz, FB AI, Friedrichstr. 57-59, Wernigerode 38855, sklinner@hs-harz.de
[4] Hochschule Harz, FB AI, Friedrichstr. 57-59, Wernigerode 38855, aschmidt@hs-harz.de
[5] TREATS Partners: Governikus (lead), Bundesdruckerei, MTG, Openlimit, AKDB, HS-Harz, sixform, HSH
[6] StudIES+ Partners: Francotyp-Postalia (lead), Bundesdruckerei, FU Berlin, HS-Harz, sixform

2 (G)eID and eIDAS policies and architectures

In 2017 we had some changes in law and contexts, concerning the eID online function in Germany (GeID) [Met17]: eIDAS/eID extensions, remote web application services for Application Service Provider (ASP) to check GeID for ASP domains/applications - as an eID-remote-ID-service-Provider (IDRP) with one single "eID-Berechtigungszertifikat (BerCert)" (in external extension of the formerly only offered remote eID-Server (per ASP domain), which checks GeID versus BerCert mandates from ASP domains), the IDRP BerCert will have generally a broader task profile (not further specific for single eID applications), no general switch-off of GeID for citizens.

To remember: the eID online function of the national identity card in Germany offers a strong two factor and doubled end-to-end authentication between the identity card at the card reader and the eID server with privacy enhancements. User Uploads/Form Fillings by user GeID at web sites of German administration offices (e.g. universities) are recognized as "qualified signed" with legally binding by law. The technical rules TR03130 for the eID server were extended according to the eIDAS framework in 2017 (ed. by BSI) [BSI17], by integration of eIDAS connectors and message flows to eID services of other EU member states (SAML/https based)[Bru17].

The extension of the GeID policy rules by law (especially the allowance of IDRP) would allow using other (secured) protocols between ASP and IDRP than in TR03130 between ASP and eID-Server (e.g. secure web services). The eIDAS framework rules will enforce since September 2018 the recognition of notified eID systems from other MS in each MS, in the case they are notified to the trust level "substantial" or "high".

3 University Use Cases & eIDAS/eID based Solutions (TREATS)

Initially, a selection process was done, to choose three APEX eIDAS extension [Str17] demonstrator cases, considering pre-existing work concerning German eID-based use cases and eID applications/user accounts (see project eCampus/Scampii).

The eID integration policy for all applications is (at the moment) "eID post (user enrolment)", because the enrolment/matriculation processes were originally developed without eID. For the chosen three APEX cases (MyCredentials, MyResearch & Development / MyRaD, MyFacultyAI) the architecture and implementation planning was done, considering the integration and extension of existing university infrastructure (e.g. user LDAP, GeID middleware to Governikus eID Services), especially. The chosen 3 APEX eIDAS-demonstrators use cases (as follows) have been implemented by integration of eIDAS eID-Service, considering pre-existing work concerning German eID-based use cases and are capable to work with the eIDAS eID minimum data set according to eIDAS eID regulations (e.g. at the user registration process).

For all applications, the according university LDAP database was extended to a hybrid eIDAS/legacy ID based permanent student account, with additional academic attributes in StudIES+. The (unchanged) document signing function in all applications uses the German Tele-Signatur (unchanged), but it is extendable to use eIDAS eSignature in the future. The three applications have been connected successfully to the Governikus eIDAS eID (test) middleware infrastructure and to the eID test infrastructure in Austria (both tested successfully). For all use cases, at first the users have to register themselves at the application. During the registration process, the user is identified in the university LDAP database by the eIDAS eID data and the user pseudonym and the eIDAS eID data are stored in the local database. After the registration, each application can used by entering the login process. During the login process, the user will be identified with the eIDAS eID by its pseudonym/unique identifier, stored locally and in the university LDAP database.

Two of the APEX eIDAS-demonstrators in more detail:

1. MyCredentials: Concerning student mobility, this application supports the refreshing of Student University credentials remotely by accessing an eIDAS/eID authentication based web application "MyCredentials" to apply for new credentials, then provided there.
2. MyResearch & Development / MyRaD: Concerning research and researcher mobility resp. distribution, this application supports researcher accounts at HS Harz, where the authentication at the account access procedures for the user is based on eIDAS/eID. Additionally an upload/download infrastructure e.g. for research grant contracts/forms is available at the researcher account, which integrates a HS Harz server-based signature functionality for contract legally binding and a back office for the university research department (including administration & authorization, file exchange).

Upon registration/login request of the user the eID application will make a SAML request call to the eID/eIDAS server for authentication of the user by eID, which would involve eID services from other MS for foreign IDs via eIDAS connector, in case of success returning a SAML response with the eID/eIDAS data of the user (minimum dataset).

4 Use Cases & eIDAS/eID & eSign.-based Solutions (StudIES+)

Within the project StudIES+ for chosen use cases the integration of eIDAS eSignatures to university applications/accounts is considered, additionally. The following use cases are analysed and going for prototype implementations together with partners:

- ePracticum/eIntership for (incoming/outgoing) students
- eNOTAR/eDiploma/eTOR student application (e.g. at hochschulstart.de / SfH)
- YourCredentials - eNOTAR services for signing derived IDs.

While the use cases at the TREATS project have a user to ASP account roles relation structure like n:1 the StudIES+ use cases will extend this to an n:m structure, involving several additional roles, even for university internal processes. Additionally, university external services may be of interest (e.g. housing for incomings) [Str18].

The ePracticum/eInternship use case involves besides the student and the student office, a professor, an ePracticum Delegate of the faculty and an (external) ePracticum Employer (PEY), which have to sign some forms together/mutually before students starting at PEY, see Fig. 1.

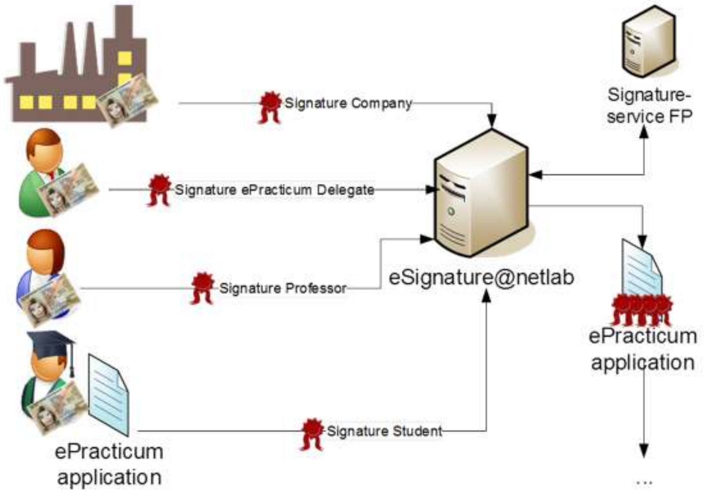

Fig. 1: ePracticum/eInternship use case with mutual multi party signing

The eNOTAR use case is a kind of meta use case, i.e. trustworthy signed eNOTAR statements are important for secured and trustworthy digitalization of many multi party processes, e.g. for applications of graded pupils (A-level certificate notarization) at universities/enrolments. While other MS have electronic Diploma Registers (including the A-Level) like The Netherlands (by law enabled by DUO) or Norway (by law enabled by UNIT) this is not the case in Germany, where we have a "diploma paper" driven pupil/student live cycle at schools and universities/HEI, which are organized federally according to local government laws. In Germany, the Bundesverwaltungsverfahrensgesetz §33 VwVfG (6)-(7) (and references to it at local government laws), would allow the electronically signed eNotarization of public administration office documents, which consists of 3 electronic document parts:

> electronic copy of document + notarization statement text + qualified eSignature by office, in short: DOC + NotarSTX + QES.

We propose digitalization use case models, which would allow the schools / HEI on request of a student/pupil/applicant to upload the eDiploma doc + Notarization Text Statement by GeID to eNOTAR accounts similar to MyRAD at federally distributed offices at SfH or HEI or other administration office locations - with legally binding. The eNOTAR offices would sign this DOC + NotarSTX by QES, and store or forward this eDiploma to the requested target office (by the applicant). Therefore, the schools would need only a simple electronic infrastructure (no eSignature infrastructure): office software, eID/PA & eID client, card reader and internet access. Of course, also an integration of eIDAS remote eSignature infrastructure at school level would be feasible (with higher integration costs), if wanted.

The eNOTAR/register proposal could be combined with the EMREX architecture [Min17] (using the ELMO xml data structures) to be integrated there as a result service, see Fig. 2, by which the student could trustworthy download and transfer his eDiploma to other HEI and employers for application (ongoing implementation).

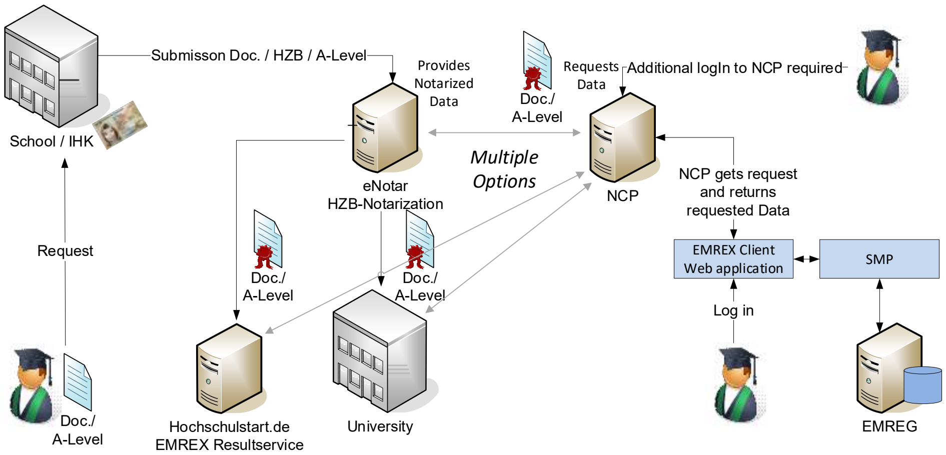

Fig. 2: eNOTAR use case combined with EMREX accesses for student applications

5 Resume, related Work & Synergies, Outlook

There is an ongoing discussion, between a group of EU funded projects and EU, to look for synergies, especially with the projects ESMO [ESM19], eID4you, EWP [EWP19], EMREX [EMR19], ESC [ESC19] - acc. to the Gothenborg declaration of the EU, concerning the rollout of eServices for European student mobility until 2025. Especially, a (standardized) set of academic attributes and its secure binding is of special concern. On the one hand more eIDAS/eID driven attribute bindings (so called domain specific eID attributes) are under discussion compared to eIDAS/eID & eSignature driven documents & attribute bindings alternatively (e.g. StudIES+ hybrid account, also “interoperables Servicekonto im E-Government/OZG (D)” [BMI16], according to german laws/regulations), which has also some relations to the ABAC proposals (attribute based access control, see https://nvlpubs.nist.gov/). The YourCredentials eNOTAR signing of derived IDs (chains of matching derived IDs/ trees/meshed structures) at StudIES+ (e.g. SAML based) would support also trustworthy bridging in time and space eID for gaps in long term eID authentifications at eID accounts, because of new pseudonyms in case of lost or expired ID cards, and for cross domain authentications/authorizations in space (also transfer to Industry 4.0 control scenarios).

Bibliography

[BKM08] Bender J., Kügler D., Margraf M., Naumann I.: Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. In DUD, 2008.

[BMI16] BMI: Studie zu interoperablen Identitätsmanagement für Bürgerkonten, Berlin, accessed 01/08/2016.

[Bru17] Bruns, H.: eIDAS-Erweiterungen für eID-Server, TREATS-Workshop, Berlin, 2017.

[BSI17] BSI: Technical Guideline TR-03130-3 eID-Server – Part 3: eIDAS-Middleware-Service for eIDAS-Token, Version 2.1.2, accessed 25/10/2017.

[EMR19] EMREX: Homepage: http://www.emrex.eu, accessed 01/02/2019.

[ESC19] ESC: Homepage: https://europeanstudentcard.eu/, accessed 01/02/2019.

[ESM19] ESMO: Homepage: http://www.esmo-project.eu/, accessed 01/02/2019.

[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.

[EU15] EU: eIDAS – Interoperability Architecture, Version 1.00, 2015.

[EWP19] EWP: Homepage: https://www.erasmuswithoutpaper.eu/, accessed 01/02/2019.

[LLR15] Leitold H., Lioy A., Ribeiro C.: Stork 2.0: Breaking New Grounds on EID and Mandates, 2015.

[Met17] Metzler, B. (BMI): Status der eIDAS-Notifizierung des Personalausweises und Status zum Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises, TREATS-Workshop, Berlin, 2017.

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

[Str17] Strack H. et.al: eID & eIDAS at University Management - Chances and Changes for Security & legally Binding in cross boarder Digitalization, Proc. of EUNIS, 2017.

[Str18] Strack H.: eID/eIDAS-Anwendungen -grenzüberschreitende Sicherheit und Interoperabilität für Bürger, Hochschulen, Verwaltungen und Wirtschaft (EU). In (Marx Gòmez, J. et.al): Smart Cities/Smart Regions – Technische, wirtschaftliche und gesellschaftliche Innovationen: Konferenzband zu den 10. BUIS-Tagen, 2018, also Springer Vieweg, 2019.