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

Strack H., Bacharach G.,Klinner S., Otto O., Schmidt A.

[1.] Hochschule Harz, Friedrichstr 57-59, 38855 Wernigerode, hstrack@hs-harz.de
[2.] Stiftung für Hochschulzulassung, Sonnenstraße 171, 44137 Dortmund, guido.bacharach@hochschulstart.de
[3.] Hochschule Harz, Friedrichstr 57-59, 38855 Wernigerode, sklinner@hs-harz.de
[4.] Hochschule Harz, Friedrichstr 57-59, 38855 Wernigerode, ootto@hs-harz.de
[5.] Hochschule Harz, Friedrichstr 57-59, 38855 Wernigerode, aschmidt@hs-harz.de

Keywords: eID, eIDAS, electronic signature, legally binding, university management, TREATS, StudIES+, EMREX, eDiploma, eTOR, eNOTAR, hybrid ID.

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).

Co-financed by the European Union
Connecting Europe Facility

1. INTRODUCTION

Further use cases at HEI/EDU management were implemented as combined eIDAS eID & eSignature ((EU, 2015), (Leitold H., 2015)) based hybrid web accounts & applications to support cross boarder/domain usage & mobility (EU) for students and researchers as well as for study applicants for enrollment/eDiploma together with the german Stiftung für Hochschulzulassung in the EU CEF project StudIES+. 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[1] - Trans-European Authentication Services" (TREATS-Pressemitteilung, 2017), Action No. 2015-DE-IA-0065. An outlook to ongoing work/results by the EU CEF 2017 funded project StudIES+[2] is given (Student's identification and electronic signature services), Action No. 2017-DE-IA-0022 (Francotyp-Postalia Holding AG), especially to the ePracticum/eInternship service accounts/ applications and the YourCredential cross domain concepts. During the TREATS project the german eID server technical rules TR03130 (Norder J.J., 2018), BSI were extended to include the eIDAS connector interfaces 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, e.g. ePracticum/eInternship, eDiploma/eTOR, eTestate or YourCredentials, see section 4.

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) (Bender, 2008) (Metzler, 2017): 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

[1] TREATS Partners: Governikus (lead), Bundesdruckerei, MTG, Openlimit, AKDB, HS Harz, HSH, sixform

[2] StudIES+ Partners: Francotyp-Postalia (lead), Bundesdruckerei, FU Berlin, HS Harz, sixform

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 citiziens.

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 TR03031 for the eID server were extended according to the eIDAS framework in 2017 (ed. by BSI), by integration of eIDAS connectors and message flows to eID services of other EU MS (SAML/https based), s. Figure 1. (BSI, 2017)

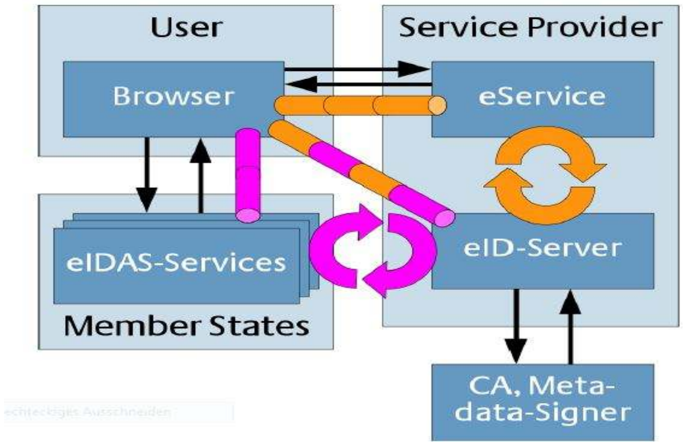

Figure 1: eIDAS extensions of the german eID server (BSI, TR03031, 2017)

The extension of the GeID policy rules by law (especially the allowance of IDRP) would allow to use other (secured) protocols between ASP and IDRP than in TR03031 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. UINIVERSITY USE CASES & EIDAS/EID BASES SOLUTIONS (TREATS)

Initially, a selection process was done, to choose three APEX eIDAS extension demonstrator cases, considering pre-existing work concerning German eID-based use cases and eID applications/user accounts (see project eCampus/Scampii (Strack, 2016)).

The eID integration policy for all applications is (at the moment) "eID post (user enrollment)", because the enrollment/matriculation processes were originally developped without eID.

For the choosen 3 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. 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 3 applications have been connected successfully to the Governikus eIDAS eID (test) middleware infrastructure and to the eID test infrastructure in Austria (both tested sucessfully).

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 be 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. However, the only difference to the registration is that only the unique pseudonym will be returned. This is enough to identify the person in the local. Therefore, the legacy student IDs/attributes will be combined together with the eIDAS minimum data set for a new hybrid identity at user account level.

Two of the APEX eIDAS-demonstrators in more detail:

a) 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.

b) 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 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 data set/MS).

4. UNIVERSITY USE CASES & EIDAS/EID & ESIGN. BASES SOLUTIONS (STUDIES+)

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

- ePracticum/eIntership management for (outgoing) students
- eNOTAR/eDiploma/eTOR student application (e.g. at hochschulstart.de / Stiftung für Hochschulzulassung) using eIDAS eSignature
- eTestate - eIDAS-based student exercise registration and attendance tracking
- 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 ones used in StudIES+ 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).

4.1. ePracticum/eInternship

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 Figure 2. For legally binding reasons eIDAS eID (registration) and eIDAS eSignature (signing forms/contracts) are used.

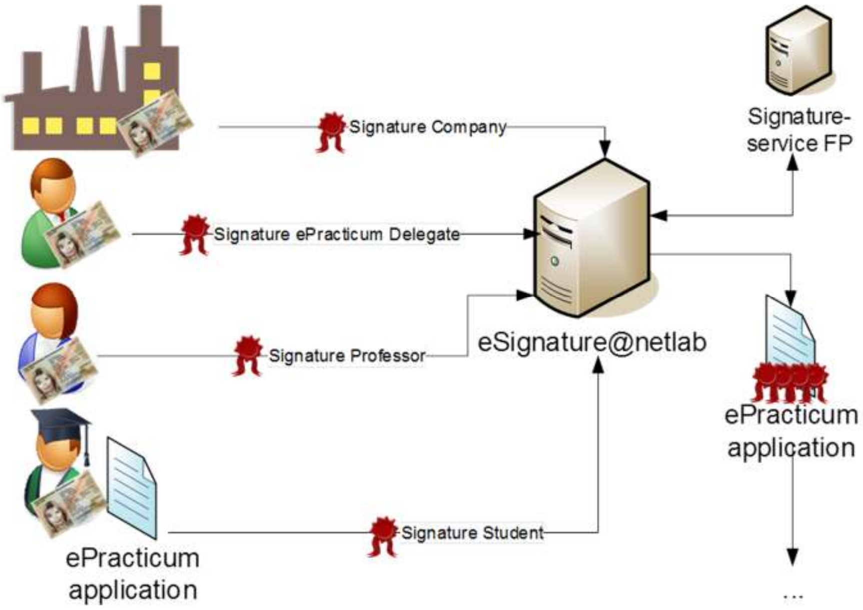

Figure 2: ePracticum/eInternship use case with mutual multi party signing

4.2. eNotar, eDiploma, eTor and EMREX

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/enrollments. 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[3] (and references to it at local government laws), would allow the electronically signed eNotarization of public adminstration office documents, which consists of 3 electronic document parts:

electronic copy of doc. + 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 the eNOTAR accounts, which are integrated at federally distributed offices. Those uploaded documents could than be accepted as legally binding by institutions like Stiftung für Hochschulzulassung, HEIs or other administration offices. 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 software, card reader, internet access. Of course, also an integration of 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 ((Mincer-Daszkiewicz, 2017), (EMREX, 2018)) (using the ELMO xml data structures) to be integrated there as a result service, see Figure 3, by which the student could trustworthy download and transfer his eDiploma to other HEI and employers for application.

[3] §33 (6)-(7) (as in local state law):... "Jede Behörde soll von Urkunden, die sie selbst ausgestellt hat, auf Verlangen ein elektronisches Dokument nach Absatz 4 Nummer 4 Buchstabe a oder eine elektronische Abschrift fertigen und beglaubigen."

Every organization having an application process where authenticated diplomas are an essential input would have an enormous benefit out of this solution (like SfH). SfH pursues two tasks of services for the admission to study at German nonprivate colleges and universities on behalf of the German federal states. Its first and "original" task is to allocate university places in courses of study with nationwide admission restriction (in Germany that are courses of study for medicine, veterinary medicine, dentistry and pharmacy). Additionally it operates a service procedure for local admission restricted courses of study (also called dialogue-oriented service procedure - in German: „DoSV"). In its "original" task SfH has to check content and sufficiency of the submitted documents, especially the university entrance certificate – the "diplomas". Due to the fact that normally that documents does not exist in digital (and authenticated) form in Germany, there is a lot of paperwork and still a lot of broken lines in the cooperation between the different digital and non-digital processes at SfH. To optimize these processes and to make them more efficient SfH already started to exchange digital diplomas with other countries (Norder J.J., 2018). But what SfH really needs to optimize their processes are also German diplomas as

- Scan of the original document (as PDF) & signed notarization
- Plain data like grade, name of certifying org., date of certification, type of qualification

etc. e.g. in XML/ELMO (Mincer-Daszkiewicz, 2017) to make that data computable within the process. Getting that prototype SfH will be able at least to test that optimization and digitizing of its application and verification process (ongoing integration of EMREX and ELMO attributes). For that purpose there is an ongoing integration of EMREX and ELMO attributes.

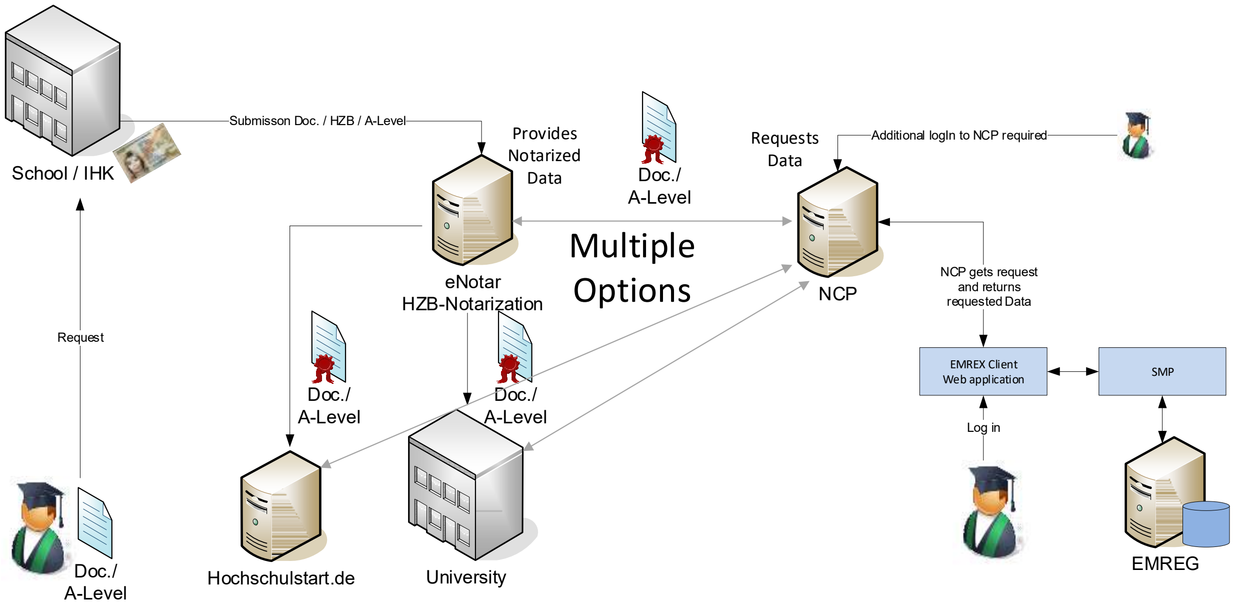

Figure 3: eNOTAR use case combined with EMREX accesses for student applications

EMREX is a solution for electronic transfer of student records from higher education institutions (Mincer-Daszkiewicz, 2017). The transfer of data is currently established between the following countries: Norway, Sweden, Denmark, Finland, Italy, Poland and the Netherlands. The prototype to be created will work as a so-called NCP (short for National Contact Point), and will be the entry point that EMREX will use to fetch data from a country (for more technical details see http://emrex.eu/technical and https://github.com/emrex-eu/standard).

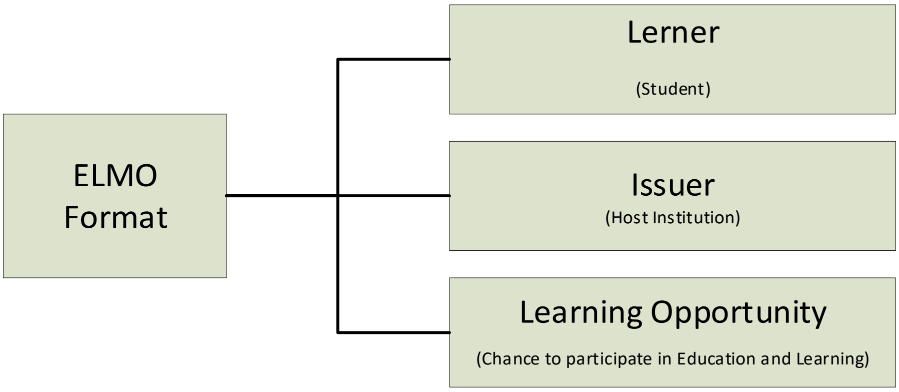

Figure 4: ELMO Format (own representation)

The XML files returned in EMREX NCP responses are called ELMO files(see figure 4). Current ELMO XML schema release is version 1.4.0 (Vangen, Emrex-EU, 2019). Trying to use this ELMO version for German upper secondary school diplomas (“HZB – Hochschulzugangsberechtigung”) the problem showed up, that the following data necessary for a German “HZB” do not exist in this version of ELMO schema:

- Institution-specific characteristic
  - Address
- Person-specific characteristics
  - Gender, placeOfBirth, birthName, address
  - Note: Due to the fact that there is no unique electronic identity in Germany by law, it is not possible to get this personal information by that eID.
- Certificate-specific characteristics
  - kind-of-diploma, county-of-acquisition, state-of-acquisition, country-of-acquisition, date-of-acquisition
  - Additionally three grading schemes have to be defined for German HZBs to describe an average grade and a score:
  - Average grade, grade in points 300-900, grade in points 280-840

The implementation of the missing institution-, person- and certificate-specific characteristics will have to be done mainly in a later release of the ELMO XML schema. In the meantime a temporary solution was found to add that characteristics within the definition of the ELMO XML schema version 1.4.0. The core idea is to use the element "identifier" using custom types. The custom types introduced by us all start with the prefix "de.hochschulstart" to ensure a clear delimitation. For example the custom type "de.hochschulstart.address" was introduced to represent the address of the school.

Person-specific characteristics can be added to the "learner" structure. For a more detailed description of the student, custom types were defined here and used in "identifier" elements accordingly.

EMREX and the ELMO Standard describe a certificate with the structures "learningOpportunity-Specification" and "learningOpportunityInstance". Here, too, the introduction of custom types and their free use in "identifier" elements has already been provided for by the standard.

As a result of the project StudIES+ a prototype for a German NCP will be created using the adopted ELMO schema described above and its address will be added to the EMREG register. As soon as that is done every EMREX HEI Client will be able to access the NCP and to fetch the diploma data stored on that system (see Figure 3 and the EMREX architecture (Vangen, Emrex-EU, Emrex Architecture, 2019)). Especially SfH will be able to fetch that German diploma data due to the fact that they are already running an EMREX client in their application portal.

4.3. eTestate

eTestate is a conceptual platform to replace a paper-based workflow which is utilized in HEIs to enroll students and track the student attendance in laboratory exercises (see figure 5). Up until now, the examiner/professor had to track the attendance of each student by hand and write everything down into a minutes document that afterwards is the base to grant a testate required for the student to pass a module at the end of an academic semester.

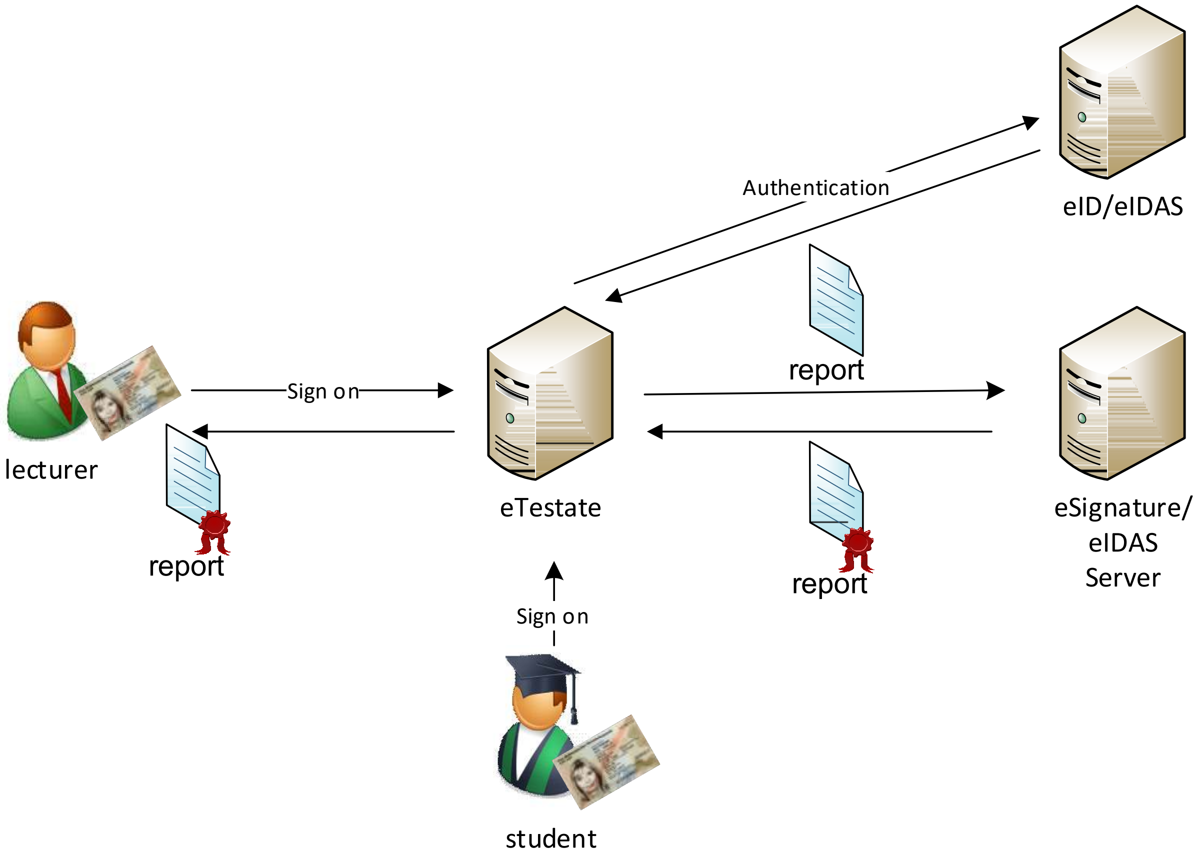

Figure 5: eTestate Overview

In order to use the electronic eTestate platform the examiner has to login by the means of eID/eIDAS. When new testate is created by the examiner, each student has to present his/her form of eIDAS document to login to the testate and therefore prove its attendance within the selected testate. Each of these personal Logins is documented within the minutes of the testate and the student is added to the list of people to grant the testate to.

The minutes data consists of the name of the examiner, the name of the course and the list of students that attended. This minutes document is generated at the end of the session and signed with a local software signature to guarantee its integrity until the examiner requests a qualified electronic eIDAS based signature of the document for legally binding.

Since the document is now signed with a qualified signature, it is a full replacement of the former paper form that was utilized before.

Process Security Application Platform (ePROSECAL)

During studies several application scenarios exist, in which students have to deal with electronic processes in which they have to provide electronic documents. Some of these scenarios are the registration for internships, exercise or exams. The challenge here is to handle these documents, which are assigned to different students with different or hybrid identities (e.g. the eID from the personal identity card or the matriculation number which identifies a student for internal usage).

Therefore a middleware and service platform was introduced to handle such documents and (eIDAS) security functions, called Process Security Application Platform (ePROSECAL), which eases to apply security by design in the HEI application field. Furthermore ePROSECAL has to ensure legal and technical validity of these documents by eIDAS qualified signature and has to manage access rights to these documents (e.g. acc. to GDPR). To face these requirements ePROSECAL provides a REST like API.With the usage of eID and eSignatures based security functions, ePROSECAL implements a trusted environment. Every user (e.g. student or professor) has to make it's registration with it's personal eID. Every service provided by ePROSECAL is accessible for users with their personal eID only. Once a user is registered in ePROSECAL he is capable to upload, sign, seal, timestamp and deploy electronic documents. The platform ePROSECAL ensures basic integrity by assigning a cryptographic signature to uploaded electronic documents.

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, eID4you, EWP, EMREX, ESC ((ESMO, 2018), (EWP, 2018), (EMREX, 2018), (ESC, 2018)) - acc. to the Gothenborg declaration of the EU, concerning the rollout of eServices for Erasmus+ Students until 2025. Especially, a (standardized) set of academic attributes and its secure binding is of special concern. More eIDAS/eID driven attribute bindings (so called domain specific eID attributes) are under discussion compared to eIDAS/eID&eSignature driven attribute bindings (e.g. StudIES+, interoperables Servicekonto im E-Government/OZG), which has also some relations to the ABAC proposals (attribute based access control, see https://nvlpubs.nist.gov/) (Bundesministerium des Inneren, BMI, 2016). A ePROSECAL Process Application Security Platform will support security by design in HEI Application develloping environments, integrating hybrid IDs. The YourCredentials eNOTAR signing & trustworthy notarizing of derived IDs (chains/trees/meshed structures) at StudIES+ (e.g. SAML based) would support in trustworthy bridging in time and space eID gaps in long term eID authentifications at eID accounts, because of BerCert/Pseudonym time limits, as well as domain extension of local domain derived IDs.

The TREATS MyCredential eID solution was transferred as a prototype solution to an Industry 4.0 control problem called DACCROM: Door Access Control for Route Policy Management at Industrial Plants Supply chain. Based on eID/eIDAS authentication of suppliers the access control rights are mapped to an web server based access control.

6. REFERENCES

Bender, J. K. (2008). Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis", in DUD), 3/2008.

BSI. (2017). Technical Guideline TR-03130-3eID-Server – Part 3: eIDAS-Middleware-Service for eIDAS-Token", Version 1, 05. May 2017, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03130/tr-03130.html.

Bundesministerium des Inneren, BMI. (2016). Studie zu interoperablen Identitätsmanagement für Bürgerkonten", Berlin, Retrieved August 1, 2016, http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/ Steuerungsprojekte/eID/Studie_Identitaetsmanagement_BK.pdf?__blob= publicationFile&v=2.

EMREX. (2018). Homepage of the EMREX Project: http://www.emrex.eu.

ESC. (2018). Homepage of the European Student Card Project: http://europeanstudentcard.eu/.

ESMO. (2018). Homepage of the ESMO Project: http://www.esmo-project.eu/.

EU. (2015). eIDAS - Interoperability Architecture Retrieved Nov. 7, 2015, from https://joinup.ec.europa.eu/sites/default/files/eidas_interoperability_architecture_v1.00.pdf.

EWP. (2018). Homepage of the EWP Project: https://www.erasmuswithoutpaper.eu/.

Francotyp-Postalia Holding AG. (kein Datum). Konsortium startet unter der Führung von Francotyp-Postalia Entwicklung von Digital-Lösungen mittels eIDAS, Retrieved March 9, 2018, from http://ircenter.handelsblatt.com/websites/ircenter_handelsblatt10/German/9020/news.html?newsID=1678371.

Leitold H., L. A. (2015). Breaking New Grounds on EID and Mandates. Retrieved May 12, 2017, from https://www.eid-stork2.eu.

Metzler, B. (. (2017). Status der eIDAS-Notifizierung des Personalausweises und Status zum Entwurf eines Gesetzes zur Förderung des elektronischen Identitätsnachweises", TREATS-Workshop"eIDAS-Erweiterungen für eID-Szenarien" vom 8. Juni 2017, Berlin, Landesvertretung Sachsen-An. halt, https://netlab.hs-harz.de/TREATSWS.

Mincer-Daszkiewicz, J. (2017). EMREX and EWP offering complementary digital services in the higher education area, Proc. EUNIS 2017. Münster.

Norder J.J., B. G. (2018). Germany goes digital. Right now!, Proc. EUNIS 2018, Paris.

Strack, H. W. (2016). Challenging eID & eIDAS at University Management. Proc. Open Identity Summit, Rome, GI Lecture Notes in Informatics, LNI 264.

TREATS-Pressemitteilung. (2017). Deutsche eID-Infrastruktur rüstet sich für Europa gemäß eIDAS -- EU-Project-Start des deutschen Konsortiums. Retrieved May 12, 2017, from https://www.governikus/newsroom-presse. Bremen.

Vangen, G. (14. 05 2019). Emrex-EU. Von Github: https://github.com/emrex-eu/elmo-schemas/releases/tag/v1.4.0 abgerufen

Vangen, G. (14. 05 2019). Emrex-EU, Emrex Architecture. Von Github: https://github.com/emrex-eu/standard/blob/master/images/arch1.png abgerufen

7. AUTHORS' BIOGRAPHIES

Prof. Dr. Ing. 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). 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-stand-ards-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 and the implementation of (mobile) 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. http://netlab.hs-harz.de/research/

Guido Bacharach, Head of IT at the Stiftung for Hochschulzulassung in Dortmund since 2014. After his study he had managing 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 member of the Deutsche Gesellschaft für Projektmanagement (GPM e.V.). http://www.hochschulstart.de