eIDAS eID & eSignature for HEI/EDU Applications

H. Strack, G. Bacharach
EUNIS 2019, 06.06.2019

Connecting Europe Facility
TREATS (TRans-European AuThentication Services)
Action-No: 2015-DE-IA-0065
StudIES+ (Student's Identification and Electronic Signature Services)
Action No. 2017-DE-IA-0022

Co-financed by the European Union
Connecting Europe Facility
Agenda

- WAYF

- Projects:
  - Campus/Scampii: Security- & E-Gov.-Standards @ University (GeID; no eDiploma register D)
  - GeID at HEI – cross domain
  - eIDAS at HEI/EDU – cross boarder/domain: TREATS/StudIES+ (EU CEF), hybrid IDs/accounts, applications/platforms/services & academic attributes & eID/eSign.

- Conclusions/Outlook (esp. implementing new law OZG, ~ 2022)
HZU, MLU, OVGU, SfH

- Uni. Faculties/Institutes/Research Groups:
  - Automation and Computer Science (HZU/netlab)
  - Institute for Computer Science (MLU/IFI)
  - Workgroup Multimedia and Security (OvGU/AMSL)

- Research Cooperation at IT & Cyber Security
  - Cyber-Sec. (Saxony-Anhalt) joint research & coop. (EFRE 2019)
  - Federal/Local State (Saxony-Anhalt) & EU Funding

- Stiftung für Hochschulzulassung (hochschulstart.de)
  - Allocation of university places in study programs with nationwide and local admission restriction
eIDAS – building blocks (cross-boarder interop. eID + trust services)

eIDAS:
- interoperable eID cross-boarder
- trust services (eSignature, eSeal, time stamps,...)

[Zeitstrahl der eIDAS Verordnung des Rates, der Kommission und des Parlamentes]

[07.09.2014: eIDAS-VO in Kraft]

[01.07.2016: Konsolidierung nachfolgender Vertrauensdiensteanbieter und -verfahren gemäß eIDAS]

[Rohstock, TREATS-Workshop 2017]
(G)eID at University Management
GeID skeleton, Motivation, national projects

German electronic Identity Card (GeIDC), Rollout until 2020

- 2-Factor-Authent. & 2x-end2end
  • nontracable eID / privacy
  • BerCert mandates GeID fields for SP
  • decentralized eID services/server
  • Form filling access/upload by GeIDC at public SP: substitution for the QES Sign. Level
- 8/2017: GeID eIDAS notification, level „high“

Challenges HEI/EDU integration:
- Existing legacy HEI ID/credentials ?
- HEI/EDU cross domain extension ?
- eIDAS cross boarder extension ?
eCampus Integration Architecture (hybrid: GeID,...)

- Integration of eGovernment-Standards @ Legacy University Campus Management & electronic Processes by Security Shell Architecture

- GeID for Authentication (hybrid Ids), OSCI for secure Delivery, QES Signature

- Projects Funding: EU & Federal/Local State (DE)

Förderungen: MW, Land Sachsen-Anhalt, EFRE-Massn.11.03/41.03, FKZ: 11.03-08-03
MyCredentials (hybrid Ids/Accounts)
Mobile Request for new Credentials (GeID)
GeID/eIDAS at Universities Management
GeID proxy for cross domain university access (HZU-MLU)
eIDAS @ University Management
eIDAS @ Universities – „saving the missing donut“?

Extension of the eID Access Topology (D): the cross-boarder way (EU, interop.)
TREATS Consortium Partners:

- MTG (media transfer AG)
- OpenLimit SignCubes GmbH
- Governikus GmbH & Co. KG
- HSH Soft- und Hardware Vertriebs GmbH
- SiXFORM GmbH
- Bundesdruckerei GmbH
- Harz University of Applied Science
- Anstalt für Kommunale Datenverarbeitung in Bayern (AKDB)

Co-financed by the European Union
Connecting Europe Facility

TREATS (TRans-European AuThentication Services)
Action-No: 2015-DE-IA-0065 (EU CEF)
TREATS – TRansEuropean Authentication Services (eIDAS)

HS-Harz - eIDAS extended Applications (3 * APEX use case) :
*Student Mobility, Research, Local Appl.-Infrastructure*

EU „MS boarder“

[EU/eIDAS, based on STORK]
TREATS – eIDAS eID Server/Service extension

TREATS workshop @ Berlin 8.6.2017: http://netlab.hs-harz.de/TREATWS/

by SAML/TLS, [BSI 2017, TR03130]
MyResearch (HZU): eIDAS eID APEX & System/Process Integration

Connecting Europe Facility
TREATS (TRans-European AuThentication Services)
Project-No: 2015-DE-IA-0065

MyResearch @ Hochschule Harz

Up/Download - Research Partner
Up/Download - Research Office

- eIDAS Uni.ID integration:
  shell architecture (Authent. & Autoriz.)
- eIDAS-Signature:
  out of project scope TREATS

elD/eIDAS minimal data set:

<table>
<thead>
<tr>
<th>eIDAS MDS</th>
<th>German eID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current family name(s)</td>
<td>Last Name</td>
</tr>
<tr>
<td>Current first name(s)</td>
<td>First name</td>
</tr>
<tr>
<td>Date of birth</td>
<td>Date of birth</td>
</tr>
<tr>
<td>Uniqueness identifier</td>
<td>Pseudonym</td>
</tr>
<tr>
<td>Name(s) at birth</td>
<td>Birth Name (if present)</td>
</tr>
<tr>
<td>Place of birth</td>
<td>Place of birth</td>
</tr>
<tr>
<td>Address</td>
<td>Address</td>
</tr>
<tr>
<td>Gender</td>
<td></td>
</tr>
</tbody>
</table>

[BSI, Bender, 2017]
StudIES+ (EU CEF)
Student’s Identification and Electronic Signature Services - Objectives

StudIES+ as a distributed platform

• will **facilitate the mobility** of students in the European Union (Gothenborg Declaration 2017)
• **build trust** for secure e-services among students (~ 2025)
• will **incorporate digital services** for Higher Education Institutions (HEIs) students
• services will be accessible via
  – eID (including eIDAS eID) and
  – **derived eIDs** (Erasmus Student eCard) as well as provide
  – eSignature/eSeal/time stamp services that rely on DSS for eSignature generation and verification.

• **Digital Transaction Management (DTM) platform** will be connected to the StudIES+ platform in order to offer a platform for eSigned document exchange between students, HEI, HEI services organisations on the one hand and businesses on the other hand.

• Secure exchange of the documents will also be ensured by deploying **secure document exchange** (ePROSECAL) and **notarization platform/services** (eNOTAR)
StudIES+ Scope & Overview

Francotyp-Postalia (lead)
Bundesdruckerei, FU Berlin, HS Harz, sixform

HS Harz Part – Application Scope:
- MyCredentials ➔ YourCredentials (signed)
- …eNotar-platform/services (sign. integration)
- …MyPracticum, MyDiploma, MyToR …
StudIES+-Partners - News, Outlook

- 12/2017: Gotenborg Declaration (EU): eID-4-Students
- 03/2018: Kickoff StudIES+
- 03/2018: eIDAS & ESC Student projects workshops @ EU (1)
- 05/2018: Hochschulstart.de + netlab @DUO NL
- 09/2018: StudIES+ Spec. & Prototyping
- 01/2019: eIDAS & ESC Student projects workshop @ EU (4)
- 06/2019: eIDAS & ESC Student projects workshop @ EU (5)
- mid term outlook (OZG law for eGov.-Online DE ~ 2022):
  eQualification @ eID-Service-Konto

Related Projects (EU):
EWP/Erasmus without Paper, Emrex,
ESC/The European Student Card,
eduGain, ESMO
StudIES+ (EU CEF) – ongoing work (HZU)
eIDAS user/student hybrid IDs & account(s), academic attributes, applications & platforms/services

- Hybrid Ids / Accounts:
  – Uni Ids (legacy)
  – GeID/eIDAS pseudonym / identifier (application & PA specific)
  – Uni & Citizien service accounts
  – Academic Attributes

- eIDAS based Applications/APEX (eID/eSign.):
  - eInternship – management of student mobility for Internships/Practica
  - eNotar – (remote) notarization of eDiploma/eToR etc. (no eDiploma register DE*), coop.
    „Stiftung für Hochschulzulassung/hochschulstart.de“
  - eTestate: eLab/eExam–Registration
  - Application backend for Security support: eProSecal platform/services

*)but by law: … public admin. **should** give QES eNotarizations for their doc…. (§33 VwVfG (6)-(7))
elInternship forms - by eIDAS eID & eSign. mutually
eInternship - by eIDAS eID & eSign. mutually
eTestate – Lab/Exam registration by eIDAS eID/eSign.

- Hybrid Account / ID (HEI legacy vs. eID)
- LDAP vs. eID Pseudonym/uniq. ID
- Legally binding for docs: eSign.
eNotar + Emrex – by eIDAS eID & eSign. (ongoing/prototyping)
ELMO – Additional data for German Upper Secondary School diploma

**USS-Diploma**
- Institution / School
- Pupil
- Course A: Grade A
- Course B: Grade B
- Others

**ELMO (XML) Diagram**
- `<learner>`
  - Gender, placeOfBirth, birthName, address
  - Pupil
- `<report>`
- `<issuer>`
  - Address
  - Institution
- `<learningOpportunitySpecification>`
  - <specifies> and/or <hasPart>
    - Course A: Grade A
- `<learningOpportunitySpecification>`
  - <specifies> and/or <hasPart>
    - Course B: Grade B
- `<attachment>`
  - (signed) PDF File
- `<signature>`
  - X509Certificate

**Create Meta / XML File**
- Create PDF (opt. signed)

**Note:**
- Average grade, grade in points - 300-900, grade in points - 280-840
YourCredentials (StudIES+, ongoing)

- eNotarization for derived Ids (signed d.ID shares/matches)
- eID Sharing Hochschulen LSA (HSG, LSA)

eNotar @
△ Hochschule Harz
https://netlab.hs-harz.de
PASSED

- OvGU Magdeburg
- FU Berlin
- MLU Halle
Conclusions/Outlook

→ eIDAS extensions of eID/eSign. Infrastruct. & Applicat. for HEI/EDU (TREATS/StudIES+, EU CEF)

→ Use Cases at HEI/EDU DE & at public/private Sector, eg. eNOTAR for eDiploma/eExam/eCert/IDs

→ eInteroperability for Student Mobility Services by eIDAS / EMREX (ongoing)

→ interoperable eServices (eIDAS) by Law DE (OZG, ~ 2022)
Thanks for your kind Attention,
Interests in cross-boarder testings,
Questions?

Prof. Dr. H. Strack
Hochschule Harz, FB AI, netlab
Friedrichstr. 57-59
38855 Wernigerode
Tel: +49 3943 659 341
Mail: hstrack@hs-harz.de
https://studies-plus.eu
https://netlab.hs-harz.de/research/
https://netlab.hs-harz.de/TREATSWS/

Bacharach Guido
Stiftung Hochschulzulassung
Sonnenstraße 171
44137 Dortmund
Mail: guido.bacharach@hochschulstart.de