Challenging eID & eIDAS at University Management

Hermann Strack[1] and Sandro Wefel[2]

Abstract: Based on national eID solutions for university scenarios, in this paper eIDAS extensions will be discussed, with benefits and Challenges (from eID to eIDAS)

Keywords: eID, eIDAS, electronic signature, legally binding, university management

1 Introduction

The use of security functions like qualified signatures and the eID of the German national identity card (eID/nPA or GeID/PA [Be08]) offered new possibilities for the electronization of processes with legally binding in university management. We report about some of these innovations within the projects "eCampus/Scampii" resp. "eID at universities", based on national signature and eID frameworks in Germany. At this background we will outline some proposals for eIDAS [In15] based extensions for secured university management.

2 eID and signatures for University Management (D)

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/service, with privacy enhancements (non traceable by eavesdroppers; eID data flow from the card to the eID service requires a pin authentication; the amount of eID data within the request from eID service will be mandatory filtered by the card item field profile, which is defined within the eID service certificate specific for the eID application provider; this eID certificate will be authorized by a federal administration office - the so called Bundesverwaltungsamt BVA - accordingly to privacy concerns of the eID application and application users). Furthermore, there will be offered additional optional functionality, organizational framework and legally bindings for special security contexts:

a) eID-Forms-Sign: In the case, that the eID application provider will be a public administration office, the eID based access to the application web site of the provider

[1] Hochschule Harz, Fachbereich Automatisierung und Informatik / netlab, Friedrichstr. 57-59, D-38855 Wernigerode, hstrack@hs-harz.de

[2] Martin-Luther-Universität Halle-Wittenberg, Institut für Informatik, Von-Seckendorff-Platz 1, D-06120 Halle (Saale), sandro.wefel@informatik.uni-halle.de

and the filling of contents to the application web forms of this office by the eID card owner allows an analogous legally binding of the contents like in the paper world case, with handwritten signature.

b) Defined by law, the user has the duty to apply for a German eID card at age of sixteen or if his former ID card would get invalid, by default the eID online function will be activated (the cancellation by user is on own choice). The eID card and user data management will be performed by special public administration offices, only.

c) eID-Card-Sign: optionally, the user could request at a qualified CA the activation of a qualified signature certificate (public key pair) on his eID card, usable for qualified signatures with fully legally binding.

At university management level there will be some principal benefits in case of using the eID for electronic processes:

A) A **strong eID based two factor authentication** for university electronic services / processes, without formerly physical presence of the user at the university

B) eID-Forms-Sign: fully legally bindings for **eID based electronic forms fillings**

C) **Mobile eID extensions**: mobile devices with NFC extended length interface could be used for eID/PA authentication directly (without an reader device), the SkiDentity platform [Hu15] offers to use security smart cards as a trust anchor (e.g. PA).

2.1 Intra domain eID applications

eID based applications within an university domain context will be presented at this section: eTestate, MyCredentials, eForms, eDiploma, eAccess.

eTestate: this was the first eID based application at Hs Harz to enable eID based registration application & login for lab exercises for students in a fully electronically manner with strong two factor eID authentication & qualified signatures, based on the eCampus architecture, see [SB13, St13, Pu12, St15] and Fig. 1.

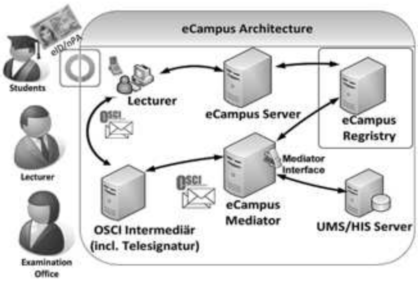
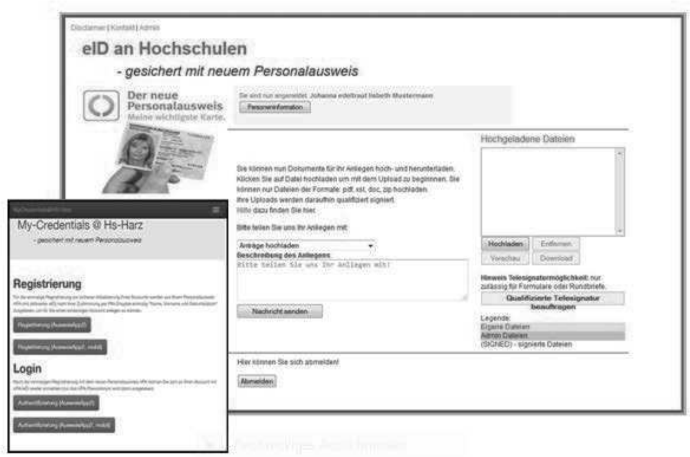


Fig. 1: The eCampus security shell architecture, integrating GeID, OSCI, QES standards

My-Credential: in case of loss of university credentials (like passwords or PKI certificates), the current policy at universities often requires the physical presence & authentication of the credential owner at the computer center of the university to apply for new credentials. By using the eID function of the German ID Card, we enabled now a remotely usable new eID based platform solution "myCredentials" to apply for new credentials by customers, which are pre-registered by eID at the platform (Fig. 2). The applied new credentials will be uploaded by the administrator in an encrypted manner to the web site of the customer (e.g. via AES based ZIP archive encryption), a decryption enabling PIN will be transferred over a separate channel, e.g. via SMS to the smartphone of the customer. Therefore, a strong protection for a confidential credential exchange (e.g. passwords, secret keys) will be established. In the future, this scheme could be extended also to exchange other confidential documents in an effectively managed and analogously end-to-end secured manner by eID (using pre-encrypted key and document exchanges by eID), usable for multiple parties/customers (pre-registered by eID at the platform), without the need for additional PKI schemes/keys, This could be an interesting add-on feature for so called "interoperable Bürgerkonten" (interoperable public administration accounts for citizens), which are planned in Germany [BMI15, Ma16, Me16, BIT16].


Disclaimer | Kontakt | Admin
eID an Hochschulen
- gesichert mit neuem Personalausweis
Der neue Personalausweis
Meine wichtigste Karte.
Personeninformation
Hochgeladene Dateien
Hochladen
Entfernen
Vorschau
Download
Qualifizierte Telesignatur beauftragen
Nachricht senden
Abmelden
My-Credentials @ Hs-Harz
- gesichert mit neuem Personalausweis
Registrierung
Registrierung (AusweisApp2)
Registrierung (AusweisApp2, mobil)
Login
Authentifizierung (AusweisApp2)
Authentifizierung (AusweisApp2, mobil)

Sie sind nun angemeldet: Johanna edeltraut liselotte Mustermann

Sie können nun Dokumente für Ihr Anliegen hoch- und herunterladen.
Klicken Sie auf Datei hochladen um mit dem Upload zu beginnen. Sie können nur Dateien der Formate: pdf, xsl, doc, zip hochladen.
Ihre Uploads werden daraufhin qualifiziert signiert.
Hilfe dazu finden Sie hier.

Bitte teilen Sie uns Ihr Anliegen mit:

Anträge hochladen

Beschreibung des Anliegens

Bitte teilen Sie uns Ihr Anliegen mit!

Hinweis Telesignatermöglichkeit: nur zulässig für Formulare oder Rundbriefe.

Legende:
Eigene Dateien
Admin Dateien
(SIGNED) - signierte Dateien

Hier können Sie sich abmelden!

Fig. 2: My-Credentials- & eForms-Platform - Security via eID/PA-Access/Upload

eForms: eID based Registration and Login by a eID extended web site will be offered to visitors or partners of the university, additionally an upload feature with combined remote qualified signing of the uploaded contents is available (as tele signature), with legally binding. This platform could also be used for application and matriculation of student applicants. If electronic certificates for higher education entry qualifications (qualified signed by schools) are allowed by law, then the whole process of matriculation could be implemented electronically.

eDiploma: As a variation of the visitor web site with eID the eDiploma application will be configured. By using his eID, the graduated student could download here his (by university) qualified signed electronic diploma certificate (as an electronic copy to the paper based certificate). Additionally, the graduated student will have by access control rights the ability to delegate temporary read access rights to other parties (e.g. to a potential employer, to whom the graduated student made an application). To improve privacy and traceability of the diploma certificate data, the owner could produce a self-signed temporary watermark overlay - with specifically produced watermark [Di00] for the granted accessor of the original diploma certificate data, signed by the university.

eAccess: WLAN and other network based services requires reliable authentication mechanism. Furthermore, authorization and accounting mechanism are needed in multi user environments with varied type of users, e.g. for university management. Therefore AAA[3] systems like RADIUS[4] are used.

To combine the advantage of reliable and strong eID authentication and fast certificate based challenge-response mechanism we use the eID function for the first authentication. A secret token is generated during the authentication process and stored on the device of the authenticated user, e.g. the laptop or smartphone. The token allows the challenge-response authentication for a limited time. After expiration a reauthentication process with eID is required. As an example of the practical application we use the authentication for WLAN access. eID authentication allows foreign users the self-registration process to get a WLAN account and an user specific token which can be used for future authentication. Additionally, in future the level of eID based authentication could be differentiated and marked by remotely signed eID specific attributes (e.g. SAML), which were added within the authentication process.

2.2 Cross domain eID applications

The federal administration office assigns eID certificate to access the information of identity cards in the domain of the specific eID application provider. An eID certificate assigned to one university offers access for more than one application but limited to the domain of the certificate owner. The limit prohibits a cross domain usage between universities. But access from domains of other universities are required for joint eID based services. An example for cross domain authentication and authorization service is eduroam (education roaming). Eduroam offers secure network access, especially to WLAN, for matriculated student ore researchers of foreign European universities and colleges when visiting an institution other than their own [Ed16]. The authentication process is delegated by the RADIUS protocol to the home institution of the user, which needs to be a part of the inherent domain hierarchy. As authentication factor a username

[3] AAA: Authentication, Authorization, Accounting

[4] RADIUS: Remote Authentication Dial-In User Service

password combination is used. To allow the authentication with eID cards we need cross domain access to the eID function.

To overcome the problem of the domain limitation, we use eID delegation with an eID proxy system analogous to the eduroam authentication. Fig. 3 shows the system and the eID extended communications (projects "eCampus/Scampii"[5] and "eID at Universities").

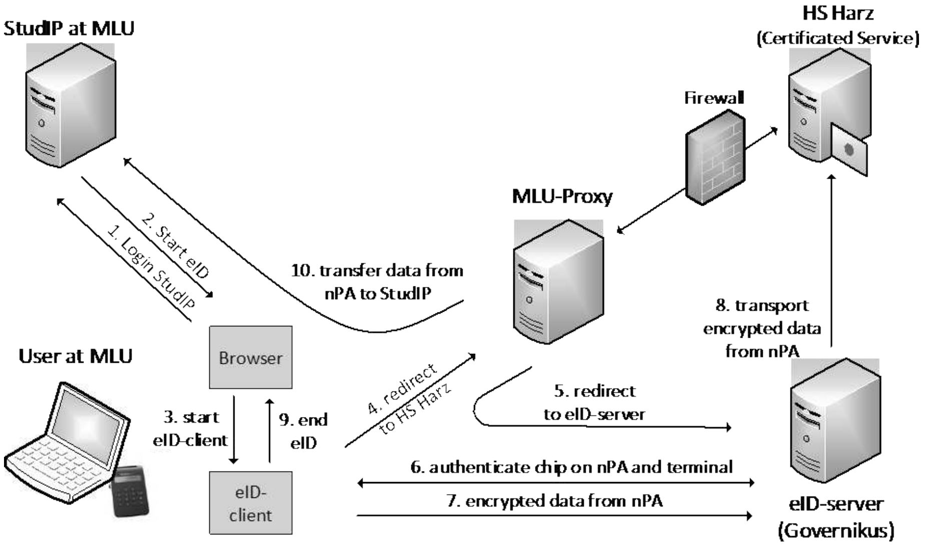


Fig. 3: eID proxy system for cross domain university access

3 University Services & eIDAS - Challenges & Benefits

The new eID solutions based on the nation German ID Card would enable strong two factor authentications (at level "high") with legally bindings for German users and also for such foreign users, which are originated from countries outside the European Union. Now, to cover also the users from the other EU member states an eIDAS based eID extension of national eID services at the same security & trust level would be obligatorily needed [Me16]. New EU Project proposals (CEF Telecom Program[6]were made for such architectures and solutions, based on former EU projects [Le15]. There is no such duty for integration of other eID solutions of EU member states at lower levels. An eID based extension of local eduroam authentications in a member state with an eID

[5] Supported by European Fund for Regional Development ERDF (EFRE FKZ: 11.03-08-03)

[6] https://ec.europa.eu/inea/en/connecting-europe-facility/cef-telecom

(SAML) attribute could be considered to close this gap for university authentications, more trustworthy. Furthermore, a standard solution would be needed for handling the eID authentication data from other EU member state for university processes.

An extension of the national solution with legally binding for eID based form fillings e.g. for matriculation would require to integrate eIDAS solutions from other EU member states, which are accredited for strong personal authentication (level "high"). For electronic university documents with legally bindings, a decision would be needed, if qualified eIDAS signatures or seals are adequate, or both of them. E.g. at paper level, nowadays, diploma certificates are signed manually by two professoral roles of the faculty. A problem could occur, if the eID solution of the other member state would not meet the level "high". In this case, as an alternative, an upload solution for qualified signed documents could be offered.

4 Summary

Electronic eID solutions for Universities based on eIDAS could improve and standardize aspects of the electronic processing at universities in a dramatically way (incl. privacy and legally bindings), especially at the Bologna Process background. In Germany, a special need for changes of administrative regulations or laws at university level could occur. For electronic university documents/forms with legally bindings, future decisions are required, if qualified eIDAS signature or seals are needed, or both of them. The integration of different eID trust levels could generate a problem at some university processes, because of document/forms with legally bindings - therefore, alternative solutions could use qualified signatures/seals The use of eIDAS eID, signatures or seals would require long term storage solutions embedded in an electronic document management environment, accordingly. Different trust levels at eIDAS eID based access solutions may require signed eID (SAML) attributes.

References

[Be08] Bender J.; Kügler D.; Margraf M.; Naumann I.: Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis. DUD, 3/2008.

[SB12] Strack H.; Brehm N.; et al.: eCampus – Services & Infrastrukturen für elektronische Campusverwaltung mit verbesserter Sicherheit auf Basis von eGov.-Standards/ Komponenten. eGovernment Review, 2012.

[St13] Strack H.; et.al.: Hochschule Harz - eID-Anwendungskonzept (eTestate"). BMI E-Government-Inititative eID/PA (BMI ed.), http://www.personalausweisportal.de, 2013.

[Pu12] European Commission (ed.): Public Services Online, Centric eGovernment performance in Europe – eGovernment Benchmark 2012. Hs Harz, pp. 47, 2012.

[SH12] Strack H..: Authentication and security integration for eCampus services at the University of Applied Sciences Harz using the German Electronic Identity Card/eID and eGovernment Standards. Open Identity Summit, Kloster Banz 2013, GI Lecture Notes in

Informatics (LNI), 2013.

[BMI15] Bundesministerium des Inneren (BMI): Studie zu interoperablen Identitätsmanagement für Bürgerkonten. http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Steuerungsprojekte/eID/Studie_Identitaetsmanagement_BK.pdf?__blob=publicationFile&v=2, Berlin, 2015.

[Hu15] Hühnlein D.: SkIDentity macht den Personalausweis mobil - Vertrauenswürdige Identitäten nun auch für mobile Endgeräte (2015). https://www.skidentity.de

[Le15] Leitold H., Lioy A., Ribeiro C.: Stork 2.0: Breaking New Grounds on EID and Mandates. https://www.eid-stork2.eu, 2015.

[St15] Strack H.: eID/nPA und E-Government-Standards für das elektronische Hochschulmanagement. BSI-CAST-Workshop"Die elektronische Identität des Personalausweises", , FHG-SIT, Darmstadt, 23.9.2015.

[Ro16] Roßnagel, A.: Vertrauensdienste-Gesetz. CAST-Forum, FHG-SIT, Darmstadt, 28.1.2016

[Ma16] Maas, S.: (BMWI): Stand der Anpassung des nationalen Rechts an die eIDAS-Verordnung, BMWi-Workshop "elektronisches Siegel", Berlin, 7.3.2016.

[Me16] Meister, G.: (G&D): BMWi-Workshop 'elektronisches Siegel'". Berlin, 7.3.2016.

[In15] EU: eIDAS – Interoperability Architecture. https://joinup.ec.europa.eu/sites/default/files/eidas_interoperability_architecture_v1.00.pdf, 6.11.2015.

[BIT16] BMI-IT4 (ed.): Die grenzüberschreitende gegenseitige Anerkennung elektronischer Identifizierungsmittel im E-Government nach Umsetzung der eIDAS-Verordnung - Umsetzungsbedarf und Auswirkungen für elektronische Verfahren der deutschen Verwaltung. Berlin, 25.4.2016.

[Ed16] eduroam Governance and Infrastructure. https://www.eduroam.org, 1.8.2016.

[Di00] Dittmann, J.: Digitale Wasserzeichen. Springer-Verlag, Berlin, 2000.