

eID & eIDAS at University Management - Chances and Changes for Security & legally Binding in cross boarder Digitalization

H. Strack¹, S. Wefel², P. Molitor³, M. Räckers⁴, J. Becker⁵, J. Dittmann⁶, R. Altschaffel⁷, J. Marx Gómez⁸, N. Brehm⁹, A. Dieckmann¹⁰

¹ Hochschule Harz, Fachbereich Automatisierung und Informatik, hstrack@hs-harz.de

² Martin-Luther-Universität Halle-Wittenberg, Institut für Informatik, sandro.wefel@informatik.uni-halle.de

³ Martin-Luther-Universität Halle-Wittenberg, Institut für Informatik, paul.molitor@informatik.uni-halle.de

⁴ Westfälische Wilhelms-Universität Münster, Institut für Wirtschaftsinformatik, michael.raeckers@ercis.uni-muenster.de

⁵ Westfälische Wilhelms-Universität Münster, Institut für Wirtschaftsinformatik, becker@ercis.uni-muenster.de

⁶ Otto-von-Guericke-Universität Magdeburg, Institut für Technische und Betriebliche Informationssysteme (ITI), jana.dittmann@iti.cs.uni-magdeburg.de

⁷ Otto-von-Guericke-Universität Magdeburg, Institut für Technische und Betriebliche Informationssysteme (ITI), robert.altschaffel@iti.cs.uni-magdeburg.de

⁸ Carl von Ossietzky Universität Oldenburg, jorge.marx.gomez@uni-oldenburg.de

⁹ Ernst-Abbe-Hochschule Jena, Fachbereich Wirtschaftsingenieurwesen, nico.brehm@fh-jena.de

¹⁰ Ministerium für Wirtschaft Wissenschaft und Digitalisierung des Landes Sachsen-Anhalt, Magdeburg, andreas.dieckmann@mw.sachsen-anhalt.de

Keywords

eID, eIDAS, electronic signature, legally binding, university management, TREATS

1. SUMMARY / ABSTRACT

Based on national eID solutions for university process scenarios this paper discusses eIDAS extensions with regard to chances, changes, benefits and challenges compared to eID.

2. Overview

Several initiatives in Europe are involved in the development of frameworks to improve student mobility. These aim at the harmonization of student data formats/forms and appropriate IT support for administrative procedures. Examples include the EUNIS task force for students mobility (formerly RS3G) or the Groningen Declaration Network or the Erasmus without Paper Project [11, 12, 25, 29]. Besides the standardization of forms and procedures security, privacy and legal binding of these is an important issue and hence discussed in this paper. The use of security functions like qualified signatures and the eID of the German national identity card (eID/PA or GeID/PA [2]) opened up new possibilities for the digitalization of legally binding processes in university management in Germany. Some of these innovations were developed within the projects "eCampus/Scampii" and "eID at universities" [20, 22, 23, 24], based on national signature and eID frameworks in Germany. Furthermore, chances and changes for security and legal binding by eIDAS regulation ([10], prepared by the STORK projects [14]) based extensions at university management are discussed in regard to the ongoing EU funded project TREATS (Trans European Authentication Services, funded by EU CEF Program).

3. Scope, Objectives, Results for electronic University Management

- a1. A full digitalization of student mobility processes in EU aiming to provide security, privacy and legal binding for the relevant electronic process steps. This requires a certain level of interoperability across borders.
- a2. Important electronic security functions to reach the goal state in a1 are (qualified) signatures, eID functions and encryption. However, there was a lack of interoperability in the EU concerning a cross border viewpoint, which then was regulated by eIDAS (EU, [10]).
- a3. For public administrations in Germany (which includes Universities & Schools) the integration of eID online functionality of the German Identity Card (PA) as exclusive mean of access to an University web form enables filled in web forms to reach fully legally binding (presumed that the University as an eID application provider will use integrity means to secure the web form contents). This is an alternative to the use of qualified signatures. In addition the eID online functionality of the PA will offer a strong 2-factor double sided authentication scheme to users and service providers, including strong privacy. There are similar approaches in some other EU member states. These are strong foundations for the full electronization of sensitive university processes, like matriculation or diploma certification. eID applications for such purposes were developed in the projects eCampus/Scampii at HS Harz & MLU [20, 22, 23, 24] (also cross university domain borders).
- a4. The eIDAS regulation of the EU (based on former work, e.g. STORK [14]) offers a solid level of interoperability of remote and mobile trust services like (qualified) signatures, seals and of national eID functions across borders working at same security level. Therefore, sensitive process steps like user authentication at matriculation processes, legally binding processes or the security of diploma certificate documents (including notarization), could be reached single-handed by electronic means. Examples are under development at TREATS project [27].
- a5. The concept of "interoperable Servicekonten" [4] (at this point still under ongoing evaluation) would allow the integration of strong eID/eIDAS authentication functions for new fully electronic application processes of pupils/students lifecycle at universities (e.g. for matriculation) or even for other qualifications in Germany. The electronic notarization of electronic copies of administration documents is allowed by federal law (§33 VwVfg [28]), but university regulations at local state law may require adaption here, e.g. for allowing electronic notarization of university diploma certificates (similar for school certificates).

4. Integrated Services

4.1. eTestate - eID registration & login for lab exercises

The eTestate application was the first eID based application at HS Harz to enable eID based registration & login for lab exercises for students in a fully electronical manner with strong two factor authentication, based on the eCampus architecture, as shown in [9, 21, 22]. Additionally, the lecturer was enabled to grade and sign the student results via qualified signature QES and to deliver it securely to the legacy campus management system HIS via OSCI egovernment standards and security gateways.

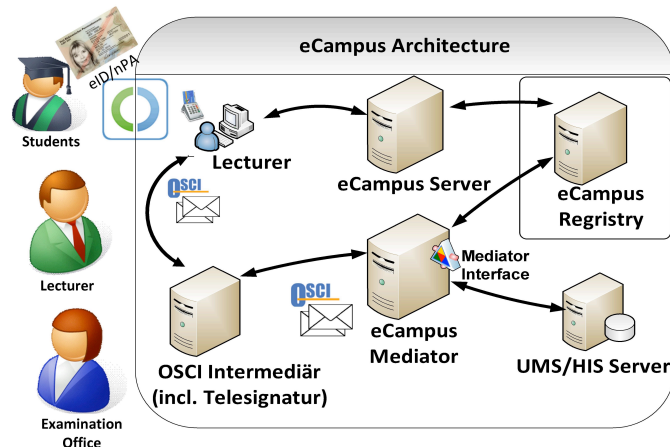


Figure 1: The eCampus security shell architecture, integrating GeID, OSCI, QES standards

4.2. MyCredentials - refreshing credentials remotely by eID

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 (GeID), we recently enabled 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).

The applied new credentials will be uploaded by the administrator in an encrypted manner to the mycredentials 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, applied at the eID based website. 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 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 and enterprises), which are planned in Germany [4, 15, 16].

Figure 2 shows the registration and login form for the MyCredentials site.

MyCredentials@HS-Harz
Startseite
Disclaimer
Administration
Kontakt

MyCredentials @ Hochschule Harz

- gesichert mit neuem Personalausweis

Registrierung


Für die einmalige Registrierung zur sicheren Initialisierung Ihres Accounts werden aus Ihrem Personalausweis nPA (mit aktivierter eID) nach Ihrer Zustimmung per PIN-Eingabe einmalig "Name, Vorname und Geburtsdatum" ausgelesen, um für Sie einen eindeutigen Account anlegen zu können.

Registriervorgang mittels AusweisApp2
Registriervorgang mittels AusweisApp2 mobil

Login

Nach der einmaligen Registrierung mit dem neuen Personalausweis nPA können Sie sich an Ihren Account mit nPA/eID wieder anmelden (nur das nPA-Pseudonym wird dann ausgelesen)

Authentifizierung mittels AusweisApp2
Authentifizierung mittels AusweisApp2 mobil



Hochschule Harz
 EUROPÄISCHE UNION
 Investition in unsere Zukunft
 Europäischer Fonds
 für regionale Entwicklung
 EFRE-FKZ: 11.03/41.03
 EFRE-FKZ: 121108.007
 Projekte
 eCampus - Zur Research-Seite
 SecInfPro-Geo - InnovationLab




Figure 2: MyCredentials-Plattform - Credential Security via eID/PA-Access

4.3. Web forms with eID access -- legally binding uploads for visitors

Web based Registration and Login by eID will be offered to visitors or partners of the university. Additionally an upload feature with combined remote qualified signing (QES) of the uploaded contents is available (as tele signature) with involved legally binding. Figure 3 shows the upload form.

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.

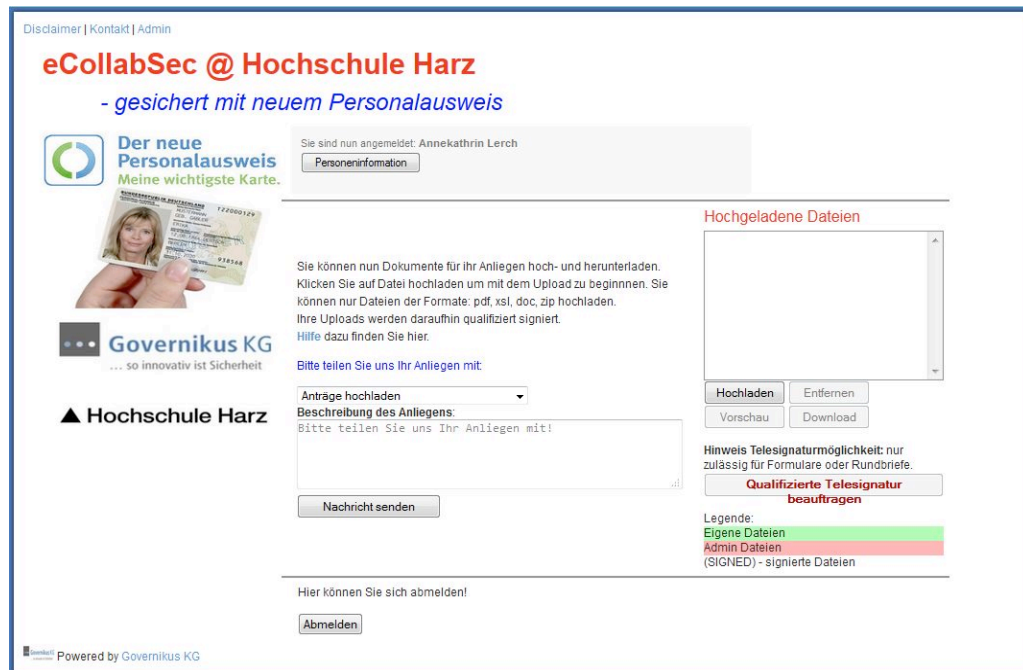


Figure 3: eCollabSec Platform - Security & legally binding via eID/PA

4.4. Electronic Diploma Certificate (copy) with enhanced privacy & integrity -- eID based diploma certificate checks via delegation by the diploma owner

As a variation of the visitors web site with eID the eDiploma Certificate will be configured. By using his eID, the graduated student could download here his qualified signed electronic diploma certificate (as an electronic copy to the paper based certificate). Additionally the graduated student will have 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) by using access control rights. To improve privacy and traceability of the diploma certificate data, the owner could use quality reduction techniques such as reducing resolutions or producing a self-signed temporary watermark overlay - with specifically produced watermark for the granted accessor of the original diploma certificate data (which are signed by the university). For quality reduction and watermarking, the requirements should be investigated in more detail in the future and potential useful approaches selected. For example invertible watermarks combined with electronic signatures might be useful to reproduce also the original document if required, see work in [3, 7, 8, 13, 18, 26].

5. University 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, therefore for enabling the legal base accordingly the local government university law of Saxony-Anhalt was changed [1].

To overcome the technical problems of the domain limitation, we use eID delegation with an eID proxy system analogous to the eduroam authentication. Figure 4 shows the test system and the eID extended communications (projects¹ "eCampus/Scampii" and "eID at Universities").

¹ Supported by European Fund for Regional Development ERDF (EFRE FKZ: 11.03-08-03)

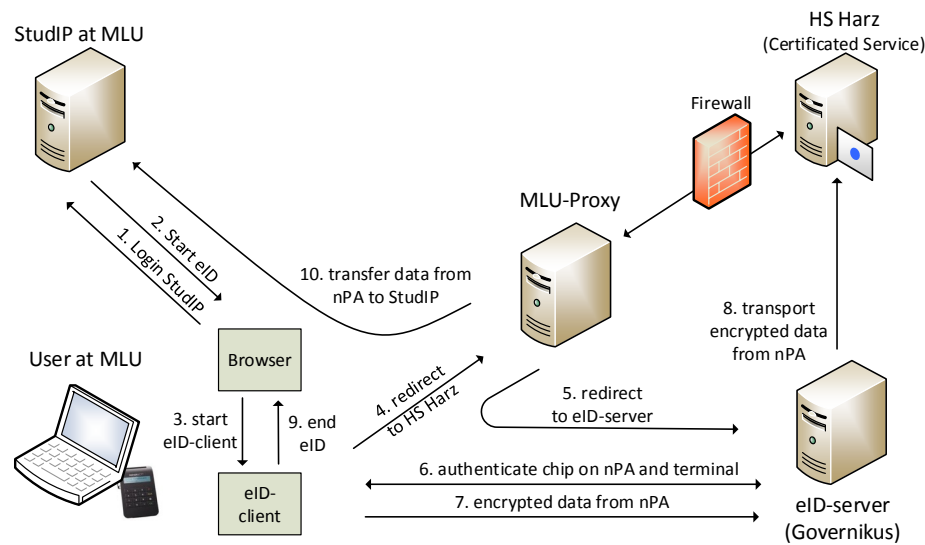


Figure 4: Cross domain university access with eID proxy test system

An example for cross domain authentication and authorization service is eduroam (education roaming). Eduroam offers secure network access, especially to WLAN, for matriculated student or researchers of foreign European universities and colleges when visiting an institution other than their own [5]. The authentication process is delegated by the RADIUS² protocol to the home institution of the user, which needs to be a part of the inherent domain hierarchy. As authentication factor a username password combination is used. To allow the authentication with eID cards we need cross domain access to the eID function.

eID allows alternative methods for delegated user authentication and authorization. Instead of sending authentication factors like username and passwords to the home institution only a distinct ID consisting of name and e.g. birthday will be transmitted. The reliable authentication factor is determined by the eID function from the ID card at the local institution. The mapping between the ID and person is made by the home institution.

To combine the advantage of reliable and strong eID authentication and fast challenge-response password mechanism we use the eID function only 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.

6. TREATS (TRans-European AuThentication Services, by eIDAS)

Hs Harz is part of the ongoing project consortium TREATS to implement eID based infrastructure and applications according eIDAS in Germany (funded by EU CEF program 2015³, s. [27]), which regulates the acceptance of "high" notified eID solutions from other EU member states at eID servers in Germany by September 2018. Hs Harz is going to implement eIDAS based eID access extensions for existing eID/PA applications in the fields of student mobility, researcher mobility & partnership and local eID/eIDAS campus infrastructure, see Figure 5 concerning R&D (ongoing work in TREATS). Indirectly only, and in a limited way, user uploads to these eID/eIDAS extended websites could gain a kind of local substitution of qualified document signatures, by eGovernment Laws, if these are

² RADIUS: Remote Authentication Dial-In User Service

³ The sole responsibility of this publication lies with the author. The European Union is not responsible for any use that may be made of the information contained therein.

applicable for universities. But in the future, for a fully legally binding cross border, because of eIDAS regulation, additionally the integration of eIDAS/eSignatures/eSeals would be required. While (federal) administrative procedure laws (e.g. Verwaltungsverfahrensgesetz [28]) would allow to produce electronic document copies with electronic signatures and notarizations of the issuer administration, accordingly at local government university law some extension may be required [1]. Because of ongoing law adjustments in Germany (e.g. because of eIDAS and other regulations), accordingly here may be some important scope of designs with importance for university procedures.

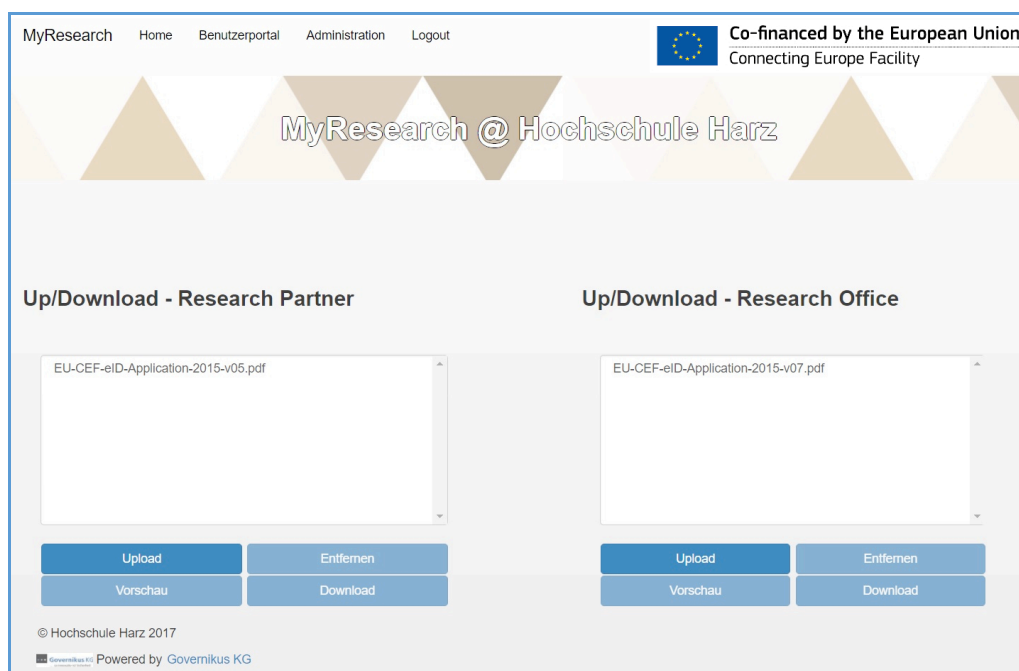


Figure 5: eID based R&D Admin. web site, for eIDAS extension (TREATS)

7. TRANSFER & Outlook

Some items of this work at university context has options for transfer to public administration, e.g. in the context of approval of professional qualifications and of electronic service access to public administrations [6], especially the upcoming legal validity of eIDAS regulation concerning eID in September 2018. Furthermore, in some contexts a fully digitalization with effectively securing of (university) documents may need some legal procedure adjustments nowadays. Not only because of the known threat potentials for the authenticity and integrity of paper documents, an according regulation of effectively secured digitalization of such documents security and egovernment standards acc. state of the art (QES, eSignature/eSeals, eIDAS) would be important in the future. In future, potential valuable combinations of cryptographic security mechanisms with media security approaches should be further researched to increase the overall security and privacy, especially for hybrid approaches (paper and digitally based documents). For example, in respect to data origin authenticity and/or data integrity the combination of approaches which modify the original data (called also active approaches) might be useful. This includes steganography and digital watermarking (as already discussed briefly in section 4). Questions about the additional security value needs to be discussed and appropriated algorithms selected or further enhanced, see as discussed in [17].

Further, media security approaches which passively investigate authenticity and integrity (called also passive approaches) might be valuable to increase the security of the involved processes. This include media forensics (posterior, without any prior information as known from digital forensics). This addresses doubts on the integrity or authenticity of involved documents as well as suspicious

traces during document life cycle processing. Image manipulation detection techniques can support this by determining and locating originality and integrity infringements of the electronic documents or checking printed document versions. Media forensics approaches need to be selected and further enhanced for its application for important documents, see work for example in [19]. As the digitalization of industrial processes is an ongoing important topic, the securing of identity and configuration management at these sites could be accordingly supported.

8. REFERENCES

- [1] Beck W., Bernstein A., Drögehorn O., Haupt M., Henning M., Knöchel M., Müller D. L., Pollmächer D., Richers S., Schaper P., Strack H., Wefel S., Werner H., Wossal F. (2016) *Innovationen in Studium und Lehre im Hochschulbereich: E-Government-Anwendung für die Identifikation (eID) durch gesetzlich zugelassene elektronische Identitätsnachweise*. Magdeburg.
- [2] Bender J., Kügler D., Margraf M., & Naumann I. (2008) *Sicherheitsmechanismen für kontaktlose Chips im deutschen elektronischen Personalausweis*. DUD, 3/2008.
- [3] BMI-IT4 (2016) *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.
- [4] Bundesministerium des Inneren, BMI (2015) *Studie zu interoperablen Identitätsmanagement für Bürgerkonten*. Berlin, Retrieved August 1, 2016 from http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Projekte/Steuerungsprojekte/eID/Studie_Identitaetsmanagement_BK.pdf?__blob=publicationFile&v=2.
- [5] *eduroam Governance and Infrastructure*. Retrieved August 1, 2016, from <https://www.eduroam.org>.
- [6] Dieckmann, A. (2017) *EAST-4.0: Der Einheitliche Ansprechpartner in der Praxis*. Proceedings IT-Planungsrat. Retrieved May 12, 2017, from http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Fachkongress/5FK2017/26April_III_EAST4.html;jsessionid=4E22D3D695E4C3A8BA00F8E4C04A7328.1_cid350?nn=7923522.
- [7] Dittmann, J., Katzenbeisser, S., Schallhart, C., & Veith, H. (2004) *Provably Secure Authentication of Digital Media Through Invertible Watermarks*. Cryptology ePrint Archive, Report 2004/293.
- [8] Dittmann, J. (2000) *Digitale Wasserzeichen*. Springer-Verlag, Berlin.
- [9] European Commission (2012) *Public Services Online, Centric eGovernment performance in Europe - eGovernment Benchmark 2012*. HS Harz: pp. 47.
- [10] EU: *eIDAS - Interoperability Architecture* (2015) Retrieved Nov. 6, 2015, from https://joinup.ec.europa.eu/sites/default/files/eidas_interoperability_architecture_v1.00.pdf.
- [11] EUNIS Students Mobility Task Force (2017) Retrieved May 12, 2017, from <http://www.eunis.org/task-forces/rome-student-systems-and-standards-group-rs3g/>.
- [12] Groningen Declaration Network (2017) Retrieved May 12, 2017, from <http://www.groningendeclaration.org/about-network>.
- [13] Katzenbeisser, S. & Dittmann, J. (2004). *Malicious attacks on media authentication schemes based on invertible watermarks*. Proc. SPIE 5306, Security, Steganography, and Watermarking of Multimedia Contents VI, 838 (June 22, 2004).
- [14] Leitold H., Liyo A., & Ribeiro C. (2015) *Stork 2.0: Breaking New Grounds on EID and Mandates*. Retrived May 12, 2017, from <https://www.eid-stork2.eu>.
- [15] Maas, S., BMWI (2016) *Stand der Anpassung des nationalen Rechts an die eIDAS-Verordnung*. BMWi-Workshop "elektronisches Siegel". Berlin, 7.3.2016.
- [16] Meister, G. Giesecke & Devrient G&W (2016) *BMWi-Workshop 'elektronisches Siegel'*. Berlin.

- [17] Miller, M. L. (2002) *Is asymmetric watermarking necessary or sufficient?* 11th European Signal Processing Conference, Toulouse, 2002, pp. 1-4.
- [18] Roßnagel, A. (2016) *Vertrauensdienste-Gesetz*. CAST-Forum, FHG-SIT, Darmstadt.
- [19] Sencar, T.H., Memon, N. (2013) *Digital Image Forensics: There is More to a Picture than Meets the Eye*. Springer New York.
- [20] Strack H., et.al. (2013) *Hochschule Harz - eID-Anwendungskonzept (eTestate)*. BMI E-Government-Initiative eID/PA, Retrived May 12, 2017, from <http://www.personalausweisportal.de>.
- [21] Strack H. (2015) *eID/nPA und E-Government-Standards für das elektronische Hochschulmanagement*. BSI-CAST-Workshop "Die elektronische Identität des Personalausweises", Darmstadt: FHG-SIT 23.9.2015.
- [22] Strack H., Brehm N., et al. (2012) *eCampus - Services & Infrastrukturen für elektronische Campusverwaltung mit verbesserter Sicherheit auf Basis von eGov.-Standards/Komponenten*. eGovernment Review.
- [23] Strack H. (2013) *Authentication and security integration for eCampus services at the University of Applied Sciences Harz using the German Electronic Identity Card/eID and eGovernment Standards*. Proc. Open Identity Summit, Kloster Banz: GI Lecture Notes in Informatics (LNI).
- [24] Strack, H., & Wefel, S. (2016) *Challenging eID & eIDAS at University Management*. Proc. Open ID Summit, Rome: GI, LNI 264.
- [25] Strack, H., Karich C. (2007) *A Distributed Architecture for the Management of Transcripts of Records and Student Mobility Data within the Bologna Process Framework*. Universities of Grenoble and University P.M. Curie of Paris France: Proceedings of EUNIS 2007.
- [26] Strack, H. (2007) *Architecture and procedures for the exchange of student data using eGovernment standards*, Proc. RS3G Foundation Workshop, Rom.
- [27] TREATS-Pressemitteilung (2017) *Deutsche eID-Infrastruktur rüstet sich für Europa gemäß eIDAS -- EU-Projekt-Start des deutschen Konsortiums*. Retrieved May 12, 2017, from <https://www.governkus.de/newsroom-presse>, Bremen.
- [28] *Verwaltungsverfahrensgesetz Bund (VwVfG, §33)*
- [29] <http://www.erasmuswithoutpaper.eu/?q=news/ewp-publishes-research>

9. AUTHORS' BIOGRAPHIES



Prof. Dr. Ing. Hermann Strack, a full professor for network management and computer sciences since 2000, 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/nPA) and eID/eIDAS. <http://netlab.hs-harz.de/research/>



Dr. Sandro Wefel is working for the Technical Computer Science Department of the Institute of Computer Science of Martin-Luther-University Halle-Wittenberg where he focuses on Network Systems and Electronics and Information Security on Embedded Systems. His interests include Microcontroller Electronics, Network and Information Security and applied Cryptography.

<http://www.informatik.uni-halle.de/ti/mitarbeiter/wefel/>