Whitepaper

Herausforderungen und Lösungsansätze im Umgang mit elektronischen Identitätsnachweisen im Hochschulumfeld

Entstanden im Rahmen der Initiative *Big Picture* – einem hochschul- und bundesländerübergreifenden Gemeinschaftsvorhaben zur Umsetzung des Onlinezugangsgesetzes im Themenfeld Bildung, Lebenslage Studium. Das Vorhaben wurde initiiert durch die Universität Duisburg-Essen mit Unterstützung der KDU.NRW im Rahmen der *Digitalisierungsoffensive NRW*.

14. September 2022

Inhaltsverzeichnis

Abbildungsverzeichnis:

1 Einleitung

Das Onlinezugangsgesetz (OZG) als Bundesgesetz stellt die Hochschulen als umsetzungsrelevante Ebene im Rahmen des föderal organisierten Bildungssystems vor große Herausforderungen, die in verschiedenen Studien bereits ausführlich diskutiert wurden (vgl. Behaghel et al. 2021; vgl. Ruschmeier et al. 2020). Zur Bewältigung dieser Aufgaben ist die *Big Picture Initiative* als länderübergreifende Kooperation aus einer zunächst landesspezifischen Projektgruppe der Hochschulen in NRW zur Weiterentwicklung ihrer Campus Managementsysteme (CaMS) hervorgegangen. Schnell hat sich herausgestellt, dass die Anforderungen an die erforderlichen Rahmenbedingungen und Infrastrukturen zur Erfüllung des geforderten OZG-Reifegrads[1] sowie insgesamt der Digitalisierung von hochschulübergreifenden Prozessen keine länderspezifische Herausforderung sind, die die NRW-Hochschulen alleine umsetzen können. Die Herausforderungen sind oft weniger technischer Natur, sondern beinhalten in einem *Ökosystem Hochschulbildung* mit zahlreichen beteiligten Akteuren vor allem auch organisatorisch-rechtliche Aspekte wie die Verwendung gemeinsamer Standards, Referenzprozesse, Formate und Infrastrukturen sowie deren nachhaltige Pflege und Weiterentwicklung auf nationaler, EU- oder sogar internationaler Ebene.

Aus dem Anspruch heraus, nicht nur das OZG in einer *Minimalversion* fristgerecht umsetzen zu können, sondern einen wünschenswerten, idealtypischen *visionären Ansatz* von vorneherein mit möglichst allen am *Ökosystem Hochschulbildung* beteiligten Akteuren zu konzipieren und gemeinsam abzustimmen, hat die NRW-Projektgruppe Key-Player wie die Stiftung für Hochschulzulassung (SfH), den Deutschen Akademischen Austauschdienst (DAAD), uni-assist, CaMS-Hersteller, Vertretungen von Wissenschaftsministerien und insbesondere auch der Federführung für das Themenfeld Bildung im OZG sowie Hochschulvertretungen anderer Bundesländer an einen virtuellen Tisch geholt und die Initiative *Big Picture* gestartet.

Im Rahmen der *Big Picture Initiative* haben sich mehrere themenspezifische Arbeitsgruppen (AG) gebildet, die AG 1 hat sich mit dem Thema *elektronische Identitätsnachweise* oder kurz *digitale Identitäten* befasst.

[1] Eine vollständige digitale Abwicklung des Online-Services ist ab Reifegrad 3 möglich, siehe https://leitfaden.ozg-umsetzung.de/display/OZG/2.2+Digitale+Services+im+Sinne+des+OZG

Bei der Verfassung des vorliegenden Whitepapers ging es der AG 1 *nicht* darum, einen vollständigen Überblick über die vorhandenen Lösungen und Good/Best Practice Ansätze im Umfeld digitaler Identitäten zu geben bzw. diese umfassend zu erläutern sowie zu bewerten[2]. Vielmehr handelt es sich um eine *Momentaufnahme* aus Sicht des Ökosystems Hochschulbildung, welche grundsätzlich die Vielfalt und Komplexität der unterschiedlichen Ansätze, aber auch bereits existierende DE-/EU-Standards samt Infrastrukturen und Anwendungen als Assets im Umfeld digitaler Identitäten demonstrieren möchte und daraus abgeleitet die Notwendigkeit aufzeigt, weiterhin einheitliche interoperable Standards bzw. Rahmenbedingungen zu entwickeln und gemeinsame Infrastrukturen zu schaffen, welche die Hochschulen zur Bewältigung der Anforderungen aus der digitalen Transformation nutzen können.

Das nachfolgende Kapitel 2 liefert zunächst einen technischen und organisatorischen Rahmen. Die einzelnen Fachaufsätze in Kapitel 3 formulieren dabei zum Teil noch offene Fragen, die zur Umsetzung des *visionären Ansatzes* beantwortet werden müssen und bieten, wenn möglich, bereits erste Lösungsansätze an. Das Whitepaper soll dadurch helfen, für alle beteiligten Akteure Transparenz zu schaffen und Fragen auch in Hinblick auf das avisierte *OZG 2.0* zu adressieren und nach Möglichkeit erste Antworten liefern. Kapitel 4 fasst die Forderungen an die Gesetzgebung zusammen, die eine nahtlose Integration der benötigten Authentifizierungsverfahren in die digitalen Abläufe möglich machen bzw. vereinfachen sollen.

[2] eine möglichst vollständige Erfassung wäre sicherlich wünschenswert, ist aber allein aus *Big Picture* heraus nicht leistbar (vgl. Hochschulrektorenkonferenz 2022).

2 Technischer und organisatorischer Rahmen

Autoren: Pempe, Wolfgang; Soldo, Erwin (erweitert um rechtl. Ergänzung)

Dieses Kapitel soll einen kompakten Überblick über die allgemeinen technischen Komponenten und organisatorischen Konzepte geben, die bei der praktischen Umsetzung des Onlinezugangsgesetz (OZG) zum Einsatz kommen, d. h. sowohl bei der Bereitstellung digitaler Verwaltungsleistungen als auch bei deren Inanspruchnahme.

Grundlage und zugleich Hintergrund der fortschreitenden Verwaltungsdigitalisierung im Hochschulbereich ist – wie bereits in der Einleitung benannt – das OZG[3]. Im OZG wird unter anderem geregelt, dass die Identifikation sowie die Authentifizierung über die jeweiligen Serviceportale beziehungsweise die dort entweder integrierten oder parallel angebotenen Nutzer:innenkonten vorgesehen sind. Die entsprechenden Stellen der öffentlichen Verwaltung – sowohl Bund als auch die Länder – wurden generell verpflichtet, ein Nutzer:innenkonto zu betreiben. Auch die Selbstverwaltungskörperschaften wie Kommunen und eben u. a. auch die öffentlich-rechtlichen Hochschulen sind gleichfalls vom OZG angesprochen und vom Geltungsbereich umfasst (vgl. Denkhaus et al. 2019). Eine gewisse Einigkeit ist zudem darin zu erkennen, dass die vom OZG umfassten öffentlichen Stellen dahingehend frei sind, ein eigenes Nutzer:innenkonto bzw. Serviceportal anzubieten oder auf ein bereits vorhandenes System im Sinne der Interoperabilität der Systeme zurückzugreifen.

Generell erfüllen die Bundes- und Landesservice- bzw. Nutzer:innenkonten alle rechtlichen Anforderungen des Onlinezugangsgesetzes und sind somit hochschulseitig effektiv verwendbar. Nutzer:innen können selbstbestimmt für die Identifizierung/Authentifizierung den Weg über ein Nutzer:innenkonto eröffnen. Aufgrund der Interoperabilität nach § 1 Abs. 2 OZG kann eine Authentifizierung auch über das „Nutzerkonto Bund“ (NKB) erfolgen, insofern sich Nutzer:innen über ein angeschlossenes Serviceportal eines Bundeslandes registriert haben. Das heißt, auf diesem Wege muss auch die Zustellung von Verwaltungsentscheidung vorgenommen werden. Es spricht vieles dafür, dass die Hochschule sodann auch an diesen Weg bei der Übermittlung bzw. Zustellung von Verwaltungsentscheidungen gebunden ist. Bei einem alternativen Weg, der beschritten werden könnte, stellt sich offensichtlich die Frage, ob dieser

[3] Die VO (EU) 2018/1724 vom 2. Oktober 2018 über die Einrichtung eines einheitlichen digitalen Zugangstors zu Informationen, Verfahren, Hilfs- und Problemlösungsdiensten und zur Änderung der Verordnung (EU) Nr. 1024/2012 (Single Digital Gateway – SDG-Verordnung) stellt ebenfalls – neben dem OZG – bestimmte Vorgaben an die Ausgestaltung der Online-Services in den Mitgliedstaaten. Nach hiesigem Verständnis folgt aus ihr zum momentanen Zeitpunkt keine erweiterten Pflichten gegenüber denjenigen aus dem OZG. Hier wird die weitere Entwicklung zu beobachten sein.

dann noch *medienbruchfrei* im Sinne des Onlinezugangsgesetzes wäre. Des Weiteren müssten andere Identifizierungskomponenten als die vorher beschriebenen zunächst auf ihre Gesetzeskonformität, insbesondere mit Blick auf Datenschutz und Barrierefreiheit, überprüft werden. Die Schaffung anderer Zugangsmöglichkeiten in Form von z. B. eigenen Identifizierungskomponenten ist daher derzeit weder erforderlich noch praktikabel, wenngleich natürlich weiterhin möglich.

2.1 Portalverbund

Sämtliche vom OZG bzw. von dessen Leistungskatalog (LeiKa) adressierten Verwaltungsleistungen sollen den Nutzer:innen über entsprechende Verwaltungsportale der Kommunen, der Länder und des Bundes zugänglich gemacht werden. Angeschlossen an die Portale sind die jeweiligen *Fachverfahren* (die hochschulischen Fachverfahren entsprechen weitestgehend den *Online-Diensten* im OZG-Kontext, vgl. hierzu auch Kapitel 2.4.). Fachverfahren sind „Systeme zur Bearbeitung von Verwaltungsleistungen durch die Sachbearbeitung. Sie stellen die interne IT-Unterstützung für die Entgegennahme, Prüfung und Beantragung von Leistungen durch die Verwaltung dar“ (BMI 2021c, 99). Die Verwaltungsportale der Kommunen, der Länder und des Bundes sind im sogenannten *Portalverbund* zusammengeschlossen. Dieser dient einerseits als gemeinsamer technischer Rahmen für die angeschlossenen Portale und Fachverfahren, andererseits soll den Nutzer:innen hiermit ein einheitlicher und übersichtlicher Zugang zu allen digitalen Verwaltungsleistungen ermöglicht werden.

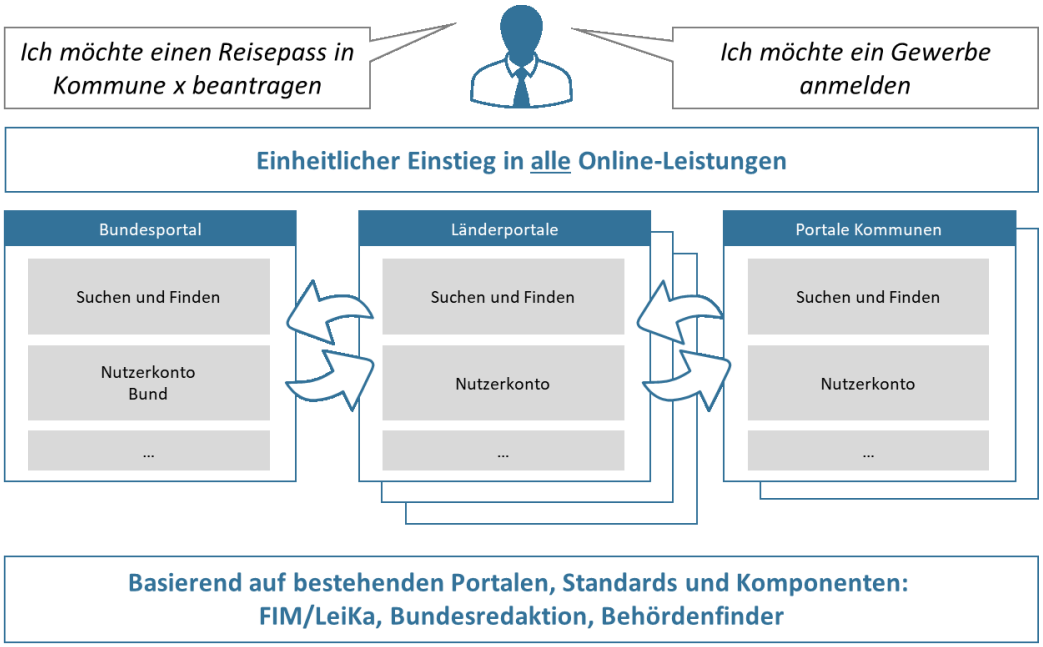

Abb. 1: Portalverbund als Zugang zu digitalen Verwaltungsleistungen (BMI 2021c, 50)

Im Rahmen des Portalverbunds sollen einheitliche Standards für Leistungen, Datenfelder und Prozesse gelten. Diesbezügliche Harmonisierung und Spezifikation erfolgt durch das sogenannte *Föderale Informationsmanagement* (FIM). Hierzu gehört weiterhin die Bereitstellung einheitlicher und leicht verständlicher Informationen für die Nutzer:innen. Hinsichtlich der Etablierung von Fachverfahren ermöglichen standardisierte Schnittstellen, Plattformen zur Integration von Online-Diensten und Landesnutzer:innenkonten in den Portalverbund zu entwickeln. Als Beispiel hierfür sei die Dataport Online-Service-Infrastruktur (OSI) genannt.[4]

2.2 Nutzer:innenkonto und Postfächer

2.2.1 Anträge und Bescheide

Die Inanspruchnahme von Verwaltungsleistungen über den Portalverbund folgt einer Antragslogik, d. h. formal betrachtet wird eine Verwaltungsleistung stets beantragt. Hierzu müssen sich die Nutzer:innen gemäß § 3 Abs. 2 OZG über vom Bund und den Ländern bereitgestellte *Nutzer:innenkonten* (im Fall von natürlichen Personen auch *Bürger:innenkonten* genannt) identifizieren und authentifizieren. Als Rückkanal zu diesem Antragswesen verfügen die Nutzer:innenkonten über eine sogenannte *Postfachfunktion* (nicht zu verwechseln mit einem E-

[4] Das Land Sachsen-Anhalt stellt hierzu einen Leitfaden bereit: https://ozg.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MF/OZG/Bilder/Leitfaden/2020-06-19_Leitfaden_zur_Anbindung_kommunaler_Online-Dienste_an_OSI_v1.3.pdf

Mail-Postfach), über die zum jeweiligen Antrag/Fachverfahren dann Bescheide und andere behördliche Mitteilungen von den Nutzer:innen empfangen werden. Das Versenden von Nachrichten seitens der Nutzer:innen per Rückkanal ist in diesem Modell nicht vorgesehen, kann jedoch im Fachverfahren z. B. in Form von Kontaktformularen integriert werden. Für den allgemeinen, antrags- und fachverfahrensunabhängigen digitalen Austausch mit der Verwaltung sind andere Verfahren vorgesehen, z. B. E-Mail.

2.2.2 Vertrauensniveaus / Levels of Assurance (LoA)

Mit der Identifizierung/Authentifizierung geht stets die grundsätzliche Frage einher, welches Vertrauensniveau erforderlich ist. Dies lässt sich anhand der zu erwartenden Risiken, die etwa mit einer Identitätstäuschung oder auch einer Datenpanne verbunden wären, bestimmen. Folglich sind insbesondere die Sensibilität der hinterlegten Daten und mögliche Auswirkungen einer Datenmanipulation relevant, sodass zu prüfen ist, welche Konsequenzen sowohl die betroffene Person als auch die verarbeitende Stelle tragen müssten. Nach kommen vor allem die aufgeführten Aspekte zum Tragen:

- Besonders schützenswerten Daten im Sinne des Art. 9 DSGVO.
- Eingriff in die Intim-, Privat- oder Sozialsphäre.
- Beeinträchtigung der persönlichen Unversehrtheit.
- negative Auswirkungen auf das Ansehen.
- finanzielle Auswirkungen.

Das Authentifizierungsniveau muss somit in einem angemessenen Verhältnis zum Gefährdungspotential stehen. Folglich sind für eine Verwaltungsleistung, bei der lediglich Daten mit geringem Schutzniveau übermittelt werden, auch keine überhöhten Anforderungen an die Authentifizierung zu stellen. Um ein Vertrauensniveau festzulegen, muss folglich stets eine Einzelfallprüfung durchgeführt werden.

Im Zuge der Einrichtung eines Fachverfahrens im Rahmen von Verwaltungsportalen wird nach entsprechender Sensitivitätsbewertung seitens des jeweiligen Anbieters festgelegt, welches Vertrauensniveau für welche Verwaltungsleistung jeweils mindestens benötigt wird. Die Anforderung eines *Mindestvertrauensniveaus* wird im Zuge des Anmeldevorgangs an das ausgewählte Nutzer:innenkonto übermittelt. Das Vertrauensniveau bzw. Level of Assurance (LoA) ergibt sich daraus, mit welchen Identifikationsmitteln ein Nutzer:innenkonto registriert wurde

und mit welchem dieser Identifikationsmittel die Authentifizierung im Zuge des Zugriffs auf eine Verwaltungsleistung erfolgt.

Die folgenden Ausführungen gelten für das „Nutzerkonto Bund“ (NKB), das auch eID-Systeme anderer EU-Mitgliedsstaaten unterstützt. Die Definition dieser Vertrauensniveaus orientiert sich an der eIDAS-Durchführungsverordnung und der staatlich regulierten Zuordnung bestimmter Identifikationsmittel zu den dort spezifizierten Sicherheitsniveaus „niedrig“, „substantiell“ und „hoch“ (vgl. EU Parlament und EU-Rat 2014; vgl. Europäische Kommission 2015). Das Vertrauensniveau „hoch“ wird daher mit den für das Vertrauensniveau (Level of Assurance) „hoch“ notifizierten, eIDAS-konformen eID-Systemen erreicht[5], die als Träger staatlich bestätigter Personendaten dienen. Für die Bundesrepublik Deutschland sind dies der elektronische Personalausweis mit eID-Funktion (PA/nPA), der elektronische Aufenthaltstitel (eAT) sowie die eID-Karte für EU-Bürger:innen (vgl. BMI 2022b). Für das „Nutzerkonto Bund“ ergibt sich somit folgende Zuordnung:

- Nutzername + Passwort: Vertrauensniveau *Basisregistrierung* bzw. *niedrig*
- ELSTER-Zertifikat: Vertrauensniveau *substantiell*
- Personalausweis mit eID-Funktion (PA/nPA), elektronischer Aufenthaltstitel (eAT), eID-Karte für EU-Bürger:innen: Vertrauensniveau *hoch*
- (notifiziertes eID-System eines EU-Mitgliedstaats: das jeweilige Vertrauensniveau)

Die eID-Karte für EU-Bürger:innen wurde unter anderem eingeführt, weil

- nicht alle EU-Mitgliedstaaten bereits über ein notifiziertes eID-System verfügen,
- manche europäischen eID-Systeme nur für die Vertrauensniveaus *niedrig* und *substantiell* notifiziert sind, sowie
- auf diese Weise mögliche Inkompatibilitäten mit eID-Systemen anderer Mitgliedstaaten ausgeschlossen werden können.

Eine Kurzübersicht zu den Vertrauensniveaus und deren technischen Komponenten auf Bürger/Client-Seite bietet die folgende Abb. 2.

[5] Eine Übersicht findet sich unter https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

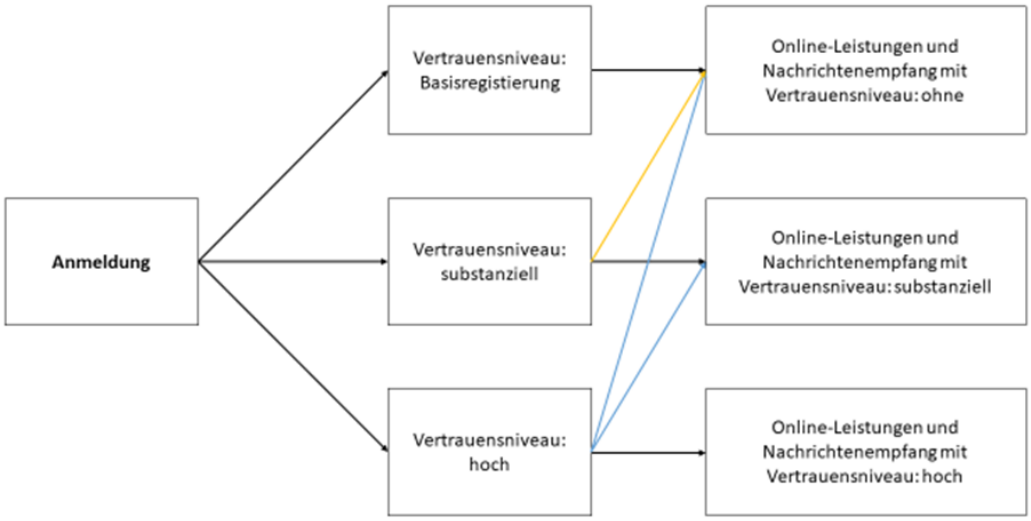

Abb. 2: Vertrauensniveaus im OZG-Ökosystem (BMI 2021c, 64)

Die Information, welches Vertrauensniveau aktuell bedient wird, wird nach der erfolgten Authentifizierung des Nutzenden vom Nutzer:innenkonto als sog. *Attribut* an die empfangende Dienstkomponente im Portal übertragen.

2.2.3 Über das „Nutzerkonto Bund“ verfügbare Daten (Attribute)

Der Minimalsatz an *personenbezogenen Daten*, die im NKB hinterlegt und im Zuge der Beantragung einer Verwaltungsleistung an den jeweiligen Dienst (Service Provider) übertragen werden können, orientiert sich an der eIDAS-Durchführungsverordnung (vgl. Europäische Kommission 2015):

- Aktueller Familienname
- Aktuelle Vornamen
- Geburtsdatum
- Unique Identifier (nicht in DE, siehe unten)

In aller Regel werden weiterhin Meldeadresse, Geburtsname, Geburtsort, Geschlecht, Anrede sowie ggf. akademische Titel, persönliche E-Mail-Adresse, DE-Mail-Adresse und eine Telefonnummer im Nutzer:innenkonto hinterlegt. Weiterhin werden die Nationalität der Nutzer:innen sowie die Kennung des EU-Mitgliedstaats, der das zur Registrierung/Anmeldung verwendete eID-System ausgestellt hat, erfasst.

Anstatt eines weltweit eindeutigen unique Identifiers für die Nutzer:innen kommt in den Nutzer:innenkonten eine *sector-specific Personal Identification Number* (ssPIN) zum Einsatz, das sog. *bereichsspezifische Personenkennzeichen*, kurz *bpK2*Fehler! Textmarke nicht definiert.. Hierbei handelt es sich um einen langlebigen Identifier, der jedoch pro Dienst bzw. Fachverfahren separat generiert wird und ein Dienst-übergreifendes Tracking der Nutzenden verhindern soll.

Darüber hinaus werden *technische Nutzdaten* an den betreffenden Dienst übertragen. Hierzu gehören beispielsweise das der gewählten Authentifizierungsmethode zugeordnete Vertrauensniveau (s. o.) und ein sog. Postkorb-Handle zur Identifizierung des Postfachs.

2.3 eID fähige Ausweise und deren Nutzung

Der aus Perspektive der Hochschulen sinnvolle Einsatz des NKBs bedingt die Nutzung der Möglichkeiten zur Authentifikation über das NKB. Hierzu stehen prinzipiell zwei Arten zur Verfügung: Die Nutzung eines ELSTER-Zertifikats oder die Nutzung eines eID-fähigen Ausweises. Hinsichtlich der eID-fähigen Ausweise stehen unterschiedliche Formate zur Verfügung:

- für deutsche Staatbürger:innen: Personalausweis mit integriertem elektronischen Personalausweis - nPA (ab 16 Jahre);
- für EU-Bürger:innen und EWR-Angehörige: eID-Karte (ab 16 Jahre, ersetzt nicht einen Personalausweis oder Reisepass und dient nur zur Nutzung von digitalen Dienstleistungen im Falle von nicht notifizierten eID-Systemen der Herkunftsländer und Problemen mit der Inkompatibilität[6] der eID Systeme zueinander);
- für Menschen außerhalb der EU und ERW: Elektronische Aufenthaltstitel - eAT (ab 16 Jahre, ersetzt nicht einen Reisepass mit entsprechenden Vermerken).

Das heißt, prinzipiell lassen sich eID-fähige Ausweise für die Authentifikation im Rahmen des NKBs nutzen und sind für alle Menschen beantragbar, die an einer deutschen Hochschule studieren möchten. Aufgrund zeitlicher Rahmenbedingungen bei der Beantragung dieser eID-fähigen Ausweise kann es zu Hemmnissen bei bestimmten Fällen wie der Immatrikulation kommen, da die notwenigen eID-fähigen Ausweise zu dem Zeitpunkt nicht vorliegen. Dies betrifft nicht die deutschen Staatsangehörigen, da bis auf Ausnahmefälle davon ausgehen werden kann, dass bei Erreichen der Hochschulzulassung ein Personalausweis mit nPA vorliegt und nur noch die Online-Funktionen (PIN-Nutzung) freigeschaltet werden muss.

[6] Beispielsweise kennen Frankreich und Dänemark das Vertrauensniveau *hoch* nicht.

Für die Nutzung des Vertrauensniveaus *substantiell* ist wie oben dargestellt ein ELSTER-Zertifikat notwendig. Dies ist aus der Perspektive der ausländischen Studierenden erst nach Klärung des Aufenthaltsstatus möglich und ist somit für den Beginn eines Studiums eher ungeeignet.

2.4 Integration CaMS - Nutzung OZG

Wie oben bereits dargestellt, können Verwaltungsleistungen entweder direkt durch die Hochschule und oder teilweise zukünftig über OZG-Portale abgebildet werden. Da prinzipiell immer die Möglichkeit der Abwicklung einer Verwaltungsleistung vor Ort existieren muss, ist die Abbildung dieser Leistungen im Rahmen der OZG-Portale als eine *zusätzliche* Abbildungsmöglichkeit zu sehen. Das bedeutet, dass die eigentliche Abbildung der Verwaltungsleistungen (im OZG-Kontext: Fachverfahren) in den Backendsystemen (im Anwendungsgebiet der Hochschulen: Campus Managementsysteme) vor Ort an den Hochschulen verbleibt und Online-Schnittstellen wie beispielsweise die bereits vorhandenen Hochschulportale oder OZG-Portale als Kommunikationsebene mit den Studierenden fungieren. Wichtig ist in diesem Zusammenhang anzumerken, dass die Campus Managementsysteme als Fachverfahren dem im Umfeld des OZG gängigen Begriff des *Online-Dienstes* gleichzusetzen sind, d. h. die hochschulspezifischen Fachverfahren beinhalten die Funktionalitäten der vom OZG geforderten *Online-Dienste*, so dass keine zusätzlichen vorgeschalteten Systeme erforderlich sind, wie dies bei *anderen Behörden* normalweise der Fall ist (vgl. Landesportal Sachsen-Anhalt 2022).
Somit ergeben sich aus der Perspektive der Hochschulen zunächst zwei Anwendungsfälle: Die Authentifikation der Studierenden im Rahmen von Verwaltungsprozessen und die Kommunikation zwischen Hochschule und den Studierenden bzw. der jeweiligen Vorgänge.
Für die Authentifikation[7] ist das NKB unter den Restriktionen des Einsatzes der eID-fähigen Dokumente (siehe oben) geeignet und bereits implementiert. Nach jetzigem Kenntnisstand ist es geplant die Postfachfunktion für die Kommunikation (Postfachhandle - aktuell noch nicht umgesetzt) weiter zu öffnen. D. h., hier wäre zukünftig eine Nutzung über das NKB möglich. Es ist davon auszugehen, dass nach einer längeren Übergangsphase (5-10 Jahre) ein Großteil der Studierenden über eID-fähige Ausweise mit Onlineausweisfunktion verfügt, deren aktive

[7] kein temporärer Login als Anwendungsfall seitens HISinOne

Nutzung bereits vor Beginn des Studiums erfolgt. Bis dahin müssen hinsichtlich der Authentifikation weiterhin auch andere Möglichkeiten vorgehalten werden.

3 Fachaufsätze

3.1 Konkretisierung von Anwendungsfällen gemäß OZG

Autoren: Bacharach, Guido; Knorr, Steffen; Pongratz, Hans; Weißenbacher, Rudolf

Das OZG verpflichtet auch die Hochschulen, im sog. OZG-Leistungskatalog definierte Verwaltungsleistungen digital anzubieten. Diese spezifischen OZG-Leistungen setzen Arbeitsschritte und Anforderungen voraus, die zunächst unabhängig von der konkret anzubietenden OZG-Leistung erfüllt werden müssen. Diese Schritte werden in diesem und den folgenden Kapiteln als Anwendungsfälle bezeichnet. Alle Anwendungsfälle beziehen sich auf das Hochschulumfeld, d. h. je nach Blickrichtung betrachten sie die unterschiedlichen fachlichen, technischen, organisatorischen oder rechtlichen Rahmenbedingungen, die für den operativen Hochschulbetrieb eine Rolle spielen. Die Anwendungsfälle im Kontext des digitalen Identitätsnachweises, die sich im Sinne des OZG ergeben, werden in diesem Kapitel in drei Gruppen aufgeteilt:

- Registrierung bei einer Plattform,
- Zuordnen von verifizierten Daten zu Personen,
- Autorisierung für Zugriff auf Bestandsdaten oder erstellte Dokumente.

Im folgenden Abschnitt werden die Anwendungsfälle und anschließend die damit verbundenen Herausforderungen beschrieben.

3.1.1 Anwendungsfälle

3.1.1.1 Fall 1: Registrierung bei einer Plattform

Im Rahmen der OZG-Umsetzung müssen CaMS-Hersteller die so genannten *Nutzer:innenkonten* implementieren, wenn sie gegenüber dem Portalverbund als Fachverfahren auftreten möchten. Von diesem Umstand sollte man grundsätzlich für alle Gruppen von Nutzer:innen Gebrauch machen, die in diesem Whitepaper behandelt werden (das Kapitel 3.2 geht detailliert auf die verschiedenen Gruppen von Nutzer:innen ein). Technisch gesehen spielt es dabei keine Rolle, ob das Nutzer:innenkonto eines Bundeslandes, beispielsweise das Servicekonto Niedersachsen, oder das „Nutzerkonto Bund“ (NKB) verwendet wird. Die Funktionalitäten sind identisch und manche Bundesländer verzichten bereits auf ein eigenes Landeskonto oder werden zukünftig auf ein eigenes Landeskonto verzichten (Haufe Online Redaktion 2022). Daher erscheint die Verwendung des NKB in einer überregionalen Betrachtung zunächst am sinn-

vollsten. Zudem ist das NKB eIDAS[8]-konform (BMI 2021b), so dass auch notifizierte europäische eID-Systeme zur Registrierung und Authentifizierung verwendet werden können, siehe hierzu Kapitel 2.2.

Für die Registrierung auf einer Plattform ist es meistens sinnvoll sicherzustellen, dass zum einen jede Person nur ein Nutzer:innenkonto eröffnet und zum anderen, dass die Erstellung von der tatsächlichen Person bzw. in deren Auftrag geschieht. Durch eine vorherige Verifizierung durch eine dritte Stelle, der beide Seiten ihr Vertrauen ausgesprochen haben, kann somit sichergestellt werden, dass die Person unter ihrem richtigen Namen agiert und dass ein für diese Person eindeutiger Identifikator ausgestellt wird. Dieser Identifikator soll dann dazu dienen, doppelte Registrierungen zu vermeiden und kann in Verbindung mit erneuter Verifizierung verwendet werden, um das Zurücksetzen von Anmeldeinformationen in Auftrag zu geben. Somit wird der Zugriff auf ein Konto nicht länger durch fehlende Anmeldeinformationen und veraltete E-Mailadressen beeinträchtigt und kann theoretisch ein Leben lang genutzt werden.

3.1.1.2 Fall 2: Zuordnung von verifizierten Daten zu Personen

Die meisten Anwendungsfälle, die eine sichere Identifizierung einer Person benötigen, verwenden außerdem Daten und Dokumente, wie z. B. Urkunden und Zeugnisse, die zu dieser Person gehören. Die Korrektheit der Daten und Dokumente wird vorausgesetzt, dennoch muss zusätzlich sichergestellt werden, dass diese Daten auch zu der jeweiligen Person gehören.

Bei in Deutschland ausgestellten Zeugnissen ist es beispielsweise meist üblich, alle Vor-, Zu- und Nachnamen, den Geburtstag und Geburtsort als Koordinaten anzugeben, die eine Person eindeutig identifizieren[9]. Dieses Modell bedingt allerdings, dass alle Informationen der Gegenstelle bereits korrekt und vollständig vorliegen und auch dann sind diese Daten nicht notwendigerweise eindeutig. Im angestrebten Modell einer Verifizierung muss folglich der Brückenschlag möglich sein, einen digital verifizierbaren Datensatz bzw. ein Dokument zu einer ausgestellten Kennziffer bzw. ID zuzuordnen. Eine Besonderheit bei diesem Anwendungsfall ist, dass er nicht notwendigerweise von der betroffenen Person angestoßen wird. So kann u. a.

[8] Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates.

[9] Es wäre zu prüfen, ob es in anderen Ländern dazu andere Lösungen gibt, die auch in Deutschland umgesetzt werden könnten (z. B. Österreich, Niederlande oder die Schweiz).

eine von der Person autorisierte Anfrage zu einer dritten Partei, z.B. einer Hochschule, verifizierte Daten übermitteln, die vor der Verarbeitung im Zielsystem der Person zugeordnet werden sollten. Umgekehrt ist das Erstellen von verifizierten Bescheiden und Dokumenten, die einer Person zugeordnet werden sollen, eine Variante dieses Falls. Mit der möglichen Verknüpfung einer Person zu ihren Daten beschäftigt sich auch das Kapitel 3.4 *Umsetzungsvorschlag Wallet Lösungen*.

3.1.1.3 Fall 3: Autorisierung für Zugriff auf Bestandsdaten oder erstellte Dokumente

Zuletzt gibt es noch besondere Fälle, in denen die Identität einer Person sichergestellt sein muss, um Daten oder Dokumente für diese Person freizugeben. Im Gegensatz zum Anwendungsfall 2 gehen wir hier davon aus, dass diese Daten und Dokumente sich nicht (mehr) im Besitz der Zielperson (Owner) befinden und eine Autorisierung auf den Zugriff zu diesen Dokumenten entweder verloren gegangen ist oder nie bestanden hat. Zwei Beispiele diesbezüglich sind a) der Auskunftsanspruch nach Datenschutzgrundverordnung (DSGVO) und b) Neuausstellung eines Hochschulabschlusszeugnisses für Alumni. Für den Auskunftsanspruch nach DSGVO (a) kann keine Registrierung vorausgesetzt werden, aber es muss dennoch festgestellt werden, ob die Daten der Person ausgehändigt werden dürfen. Ähnlich verhält es sich bei einer Zeugnisneuausstellung (b): Auch hier darf das Dokument nur an die zugehörige Person ausgestellt werden.

3.1.2 Herausforderungen

Alle Anwendungsfälle benötigen Daten über die Person, die von einer vertrauenswürdigen Stelle verifiziert wurden und im Idealfall elektronisch ausgewertet werden können. Es gibt bereits Standards zur digitalen zertifikatsbasierten Signierung von PDF-Dateien. Diese können elektronisch ausgewertet werden, indem sie eine *Signaturkette* zu einer Stelle mitliefern, der beide Parteien vertrauen. Dieses System hat einige Schwachstellen, sodass es bis dato keinen offiziellen Standard gibt, beliebige Datensätze verlässlich zu verifizieren.[10]
Darüber hinaus müssen für die elektronische Auswertbarkeit beide Parteien ein einheitliches Format verwenden. Hierfür gibt es bereits Standardisierungsprojekte, die aber noch nicht reif

[10] Mögliche Angriffsvektoren werden in folgendem Artikel ausgeführt: https://www.heise.de/select/ct/2021/13/2113210225251122429

für den Produktivbetrieb sind. Unter Anderem wird mit Lösungen über geschlossene Standards gearbeitet, die z. B. über Vertrauensdienstleister wie *D-Trust* zur Verfügung gestellt werden bzw. Dokumenten-Signaturen des *X509-Standards*, die für die Sicherung von *ELMO*[11]*-Dateien* im EMREX/EWP[12]-Umfeld genutzt werden. Hier ist zu prüfen, ob diese Standards genügen - speziell, inwieweit das Handling beim Ablauf von Zertifikaten dort gelöst ist.
Die Herausforderungen werden in den folgenden Abschnitten näher erläutert. Der Aspekt zur datenschutzkonformen Identifizierung von Nutzer:innen wird in Abschnitt 3.5.1 behandelt sowie übergreifend in Kapitel 3.7.

3.1.2.1 Verifizierungsstelle

In den drei vorstehend genannten Anwendungsfällen wird jeweils die Existenz einer vertrauenswürdigen Verifizierungsstelle vorausgesetzt. Im Rahmen des OZG werden derzeit zwei Instanzen dafür vorgesehen: Die Nutzer:innenkonten der Länder und des Bundes sowie das Benutzer:innenkonto der elektronischen Steuererklärung (ELSTER). Die Verwendung dieser Verifizierungsstellen bedarf jeweils einer vorherigen Registrierung, die im Falle des ELSTER-Zertifikats auch einen postalischen Versand miteinschließt. Bei allen Anwendungsfällen ist diese Vorbedingung also mitzudenken: Die Person und das Fachverfahren haben sich bereits bei einer Verifizierungsstelle registriert und vertrauen ihr.

3.1.2.2 Kommunikationswege

Die meisten Anwendungsfälle benötigen innerhalb der verwendeten Fachverfahren einen gegenseitigen Dialog des Erfragens und Bereitstellens von Informationen. Bei einseitiger Kommunikation vom Fachverfahren zur Person ist die sichere synchrone Kommunikation einfach zu realisieren. Es wird schwieriger, wenn nachträglich Informationen (außerhalb des OZG-Nutzer:innenkontos) gesendet werden sollen oder die Person selbst eine Anfrage schicken möchte. Der bisher übliche Weg ist dabei E-Mail, der manchmal durch das Ausfüllen eines Web-Formulars angestoßen wird. Beim Kommunikationskanal muss gesichert sein, dass jeweils diejenige Person die Informationen empfängt und sendet, die dafür vorgesehen ist. Eine

[11] ELMO und EMREX sind europäische Standards bzw. technische Lösungen für den Transfer von Studierendendaten; siehe auch https://emrex.eu/technical/

[12] Erasmus without paper

eingehende Nachricht muss außerdem analog zu Anwendungsfall 2 zuerst einer Person zugeordnet werden, allerdings gibt es für diesen Fall keine Verifizierungsstelle, die hierbei helfen könnte.

3.1.2.3 Namens- oder Geschlechtswechsel[13]

Bei den aktuell üblichen Attributen zur Identifikation einer Person können sich Probleme beim Wechsel der einzelnen, in der Regel als fest definierten Attribute ergeben. Konkret können sich Probleme bei den Anwendungsfällen ergeben, wenn sich der Name der Person während eines Verwaltungsvorgangs ändert, z. B. durch Heirat. Besonders bei Verwaltungsprozessen, die nicht innerhalb kurzer Zeit beendet sind, kann eine solche Änderung für große Probleme sorgen. Für diesen Fall wäre die Lösung die Vergabe einer personenspezifischen ID, die unabhängig von Name und Geschlecht ist.

3.1.2.4 Identifizierung von Minderjährigen

Die meisten Szenarien gehen davon aus, dass die agierende Person auch die Zielperson des Prozesses ist. Bei der Identifizierung von Minderjährigen (z. B. bei der Hochschulbewerbung oder der Immatrikulation) übernimmt jedoch eine andere (vertretungsberechtigte) Person die Durchführung. Hier muss eine prozessorientierte Klärung herbeigeführt werden: Soll sowohl die Identität der agierenden Person, als auch der bzw. des Minderjährigen sowie deren Rechtsverhältnis zueinander festgestellt werden? Was passiert, wenn die agierende Person wechselt, z. B. ein anderes Elternteil erziehungsberechtigt wird?

3.1.2.5 Personen aus Nicht-EU-Staaten

Eine Herausforderung für die Identitätsfeststellung stellen auch Personen aus Nicht-EU-Staaten dar, da hier zunächst keine Standards der Identifikation über verschiedene Vertrauensniveaus (wie z. B. in Europa für eIDAS) existieren. Es bleibt dann Land für Land zu prüfen, über welches Identifikationsmittel sich diese agierende Person mit dem jeweils hinreichenden Vertrauensniveau identifizieren kann (und dies muss dann für die genannten Anwendungsfälle umgesetzt werden). Sollte es frühzeitig (möglichst vor dem ersten Identifizierungsbedarf) schon einen Aufenthaltstitel geben, so kann dieser auch für NKB etc. wie ein Personalausweis

[13] Anmerkung: Der Personalausweis beinhaltet zwar kein (authentifiziertes) Geschlecht, allerdings wird durch einen Geschlechtswechsel auch gewöhnlich implizit ein Namenswechsel einhergehen.

verwendet werden und so tritt dieses Problem nicht auf. Die Herausforderungen für diese Personengruppe werden ausführlich in Abschnitt 3.2.1 behandelt.

3.2 Betrachtung von verschiedenen Gruppen von Nutzer:innen

Autor:innen: Bohr, Ingrid; Pasek, Gregor; Pongratz, Hans; Waßmann, Arn

In diesem Kapitel sollen spezielle Gruppen von Nutzer:innen betrachtet werden, die zwar nicht die Mehrheit aller Anwendungsfälle ausmachen, aber für die vollständige Digitalisierung dennoch betrachtet werden müssen.

3.2.1 Nutzer:innen aus der EU bzw. aus Nicht-EU-Staaten

Während der Nachweis der digitalen Identität für deutsche Staatsbürger:innen nach § 18 des Personalausweisgesetzes über die Funktion des neuen nPA erfolgen kann, können Personen ohne deutsche Staatsbürgerschaft dies in elektronischer Form mit ihrem Aufenthaltstitel nach § 78 Absatz 5 des Aufenthaltsgesetzes tun. Zwar gibt die eIDAS-Verordnung zum einen vor, dass die zum Identitätsnachweis verwendeten eID-Systeme von Mitgliedsstaaten nach Artikel 6 der eIDAS-Verordnung unter bestimmten Bedingungen auch in anderen Staaten der EU gültig sein sollen. Zum anderen umfasst diese Verordnung den Aufbau und die rechtliche Bedeutung von qualifizierten elektronischen Signaturen und dass diese von Mitgliedsstaaten gegenseitig anerkannt werden müssen (Artikel 25 eIDAS-Verordnung). Dies bedeutet für Nicht-EU-Ausländer:innen, dass sie sich gegenüber der deutschen Verwaltung nur mithilfe ihres Aufenthaltstitels digital ausweisen können.
Bei den Verfahren, die für den Hochschulbereich betrachtet werden, muss folglich immer zwischen EU-Inländer:innen und EU-Ausländer:innen (also Personen aus Nicht-EU-Staaten) unterschieden werden. EU-Ausländer:innen mit gültigem Aufenthaltstitel können technisch zu den EU-Inländer:innen zählen, wenn diese einen Aufenthaltstitel in einem EU-Mitgliedsstaat besitzen.. Eine Ausnahme bilden die Studienbewerber:innen, wie im Folgenden dargelegt wird.

3.2.1.1 Herausforderung

Der einleitend skizzierte Weg – die Verwendung von Aufenthaltstiteln zur technischen Gleichstellung der EU-Inländer:innen mit den EU-Ausländer:innen – ist für Hochschulen gerade im Umgang mit Studienbewerber:innen bzw. Studierenden aus Nicht-EU-Staaten meistens nicht

gangbar, da diese erst einen Aufenthaltstitel bekommen, sobald sie eine Immatrikulation an einer Hochschule nachweisen können. Um Studierende jedoch immatrikulieren zu können, ist eine Identitätsprüfung vorab notwendig. Dabei ist zudem zu beachten, dass Studierende nicht zwangsläufig mit Beginn ihrer Bewerbung zum ersten Mal in Kontakt mit der Hochschule kommen muss, sondern dies auch früher geschehen kann, z. B. wenn sie Kontakt mit dem Fremdsprachenzentrum aufnehmen. Aber auch ein vorheriger Kontakt mit der Universitätsbibliothek oder dem Hochschulsport ist denkbar. Hier wäre es sicherlich sinnvoll, Datenredundanz zu vermeiden, sofern dies technisch möglich ist.
Die digitale und internationale Lösung der Identitätsfeststellung gestaltet sich dementsprechend als schwierig, zudem die nationale Gesetzgebung in Bezug auf digitale Identitätsnachweise in nicht EU-Mitgliedstaaten sowie der technologische Stand der Staaten unterschiedlich stark ausgeprägt sein können.

3.2.1.2 Lösungsansatz

Ein möglicher Weg für Hochschulwechsler:innen könnte dementsprechend sein, dass die Identität der internationalen Studierenden von der Bildungseinrichtung überprüft wird, von welcher aus die Studierenden wechseln möchten und dies von der aufnehmenden Hochschule dann übernommen wird. Dies gestaltet sich jedoch als schwierig, da noch entsprechende Kanäle und Standards eingerichtet werden müssten, die von Hochschule zu Hochschule bzw. von Land zu Land unterschiedlich ausfallen können, sofern die betreffende Hochschule über keinen Identity Provider mit Anschluss an eine nationale Identity Federation (in Deutschland: DFN-AAI) verfügt. Andernfalls ist eine Authentifizierung und die Übertragung von Nutzer:innendaten über eduGAIN möglich[14]. Für dieses Vorgehen ist jedoch auch ein Einblick in die Wege notwendig, wie die Identität an der Ursprungshochschule geprüft wurde. Zudem muss es bei digitalen Dokumenten, wie z. B. Zeugnissen, möglich sein, deren Echtheit bzw. deren Zugehörigkeit zum Studierenden zu überprüfen. Dabei muss es sich bei Bildungseinrichtungen nicht zwangsläufig um Hochschulen handeln, da auch Schüler:innen nach ihrem Abschluss an eine Hochschule ins Ausland wechseln können.

[14] siehe https://edugain.org/

Vielversprechender scheint dementsprechend der Ansatz zu sein, die analog zu den für Papierdokumenten bereits existierende internationale Vereinbarungen (vgl. Reisepass) ins Digitale zu übertragen. Eine vergleichbare Lösung zu den Nutzer:innenkonten des Bundes und der Länder mit entsprechendem Vertrauensniveau für EU-Ausländer:innen ist nicht absehbar. Daher bieten sich hier Verfahren der freien Wirtschaft an, die zumindest gesellschaftlich als sog. Social-Login etabliert sind. Insbesondere Verfahren, welche OpenID Connect (OIDC – siehe OpenID Foundation 2022) nutzen, sind interessant. Durch die Erweiterung des Shibboleth Identity-Providers um eine Implementierung dieses Standards[15] gewinnt es auch an Bedeutung für die akademische Welt. Aktuell steht vor allem eine Erleichterung für die Nutzenden, wenn man eine Authentifizierung über kommerzielle Unternehmen anbietet, im Fokus. Bekannte Unternehmen mit OIDC-Konten, die verwendet werden könnten, sind unter anderen Microsoft, Google und Amazon. Eine Anmeldung über so eine bestehende Authentifizierung vereinfacht den Zugang gegebenenfalls durch den Entfall einer Registrierung. Allerdings wird man über das Vertrauensniveau *niedrig* in diesem Fall nicht hinauskommen. Ein kleiner Vorteil der Nutzung auch kommerzieller Anbieter ist zudem, dass die Daten - zumindest die E-Mail-Adresse - etwas gesicherter sind als durch die reine manuelle Eingabe. Hieraus entstehen datenschutzrechtliche Fragestellungen, da hier Daten mit Unternehmen (die außerhalb der EU ansässig sind) ausgetauscht werden müssten, die betrachtet werden sollten.

3.2.2 Betrachtung weiterer Nutzer:innengruppen

An einer Hochschule können weitere Gruppen von Nutzer:innen zusätzlich zu den wohl bekannten (Studierende, Bewerber:innen) identifiziert werden. Für einige dieser Gruppen ist analog hierzu eine gesicherte Identität notwendig oder zumindest hilfreich. Insbesondere können durch eine digitale Identität administrative Prozesse optimiert werden. Nicht selten werden diese weiteren Nutzer:innen durch die Sachbearbeitung manuell angelegt - im Gegensatz zu den digital ablaufenden Prozessen der Studierendendatenübernahme. Als Vorlage dient aktuell in der Regel ein Formular oder Antrag in Papierform, der abgetippt werden muss. Auch aus diesem Umstand entsteht der Wunsch, dass die Dateneingabe durch die Nutzer:innen selbst geschieht und durch entsprechende technische Verfahren abgesichert wird. Ist die Identität erst im System, dann können weitere Online-Verfahren genutzt werden.

[15] https://shibboleth.atlassian.net/wiki/spaces/IDPPLUGINS/pages/1376878976/OIDC+OP

Der OZG-Leistungskatalog fordert u. A., dass für die Aufnahme von Gaststudierenden eine digitale Verarbeitung möglich sein muss (LeiKa-Leistung: Gasthörerschaft Zulassung). Daher wird dieser Anwendungsfall separat und ausführlicher betrachtet (Abschnitt 3.2.4).
In der Folge werden einige Beispiele für weitere Gruppen von Nutzer:innen aufgeführt. Diese Aufzählung erhebt ausdrücklich keinen Anspruch auf Vollständigkeit, da jede Hochschule andere Anwendungsfälle hat und auch das Thema der Digitalisierung im Allgemeinen in unterschiedlicher Durchdringung vorantreibt. Daher werden abschließend noch weitere Gruppen benannt, die aber mutmaßlich eher kleinere Fallzahlen aufweisen. Eine Kosten-Nutzen-Analyse für die Digitalisierung der jeweiligen Prozesse muss jede Hochschule pro Gruppe selbst erstellen, da die Fallzahlen höchst unterschiedlich ausfallen können und somit auch die Priorität einer Digitalisierung unterschiedlich bewertet werden muss. Eine Nachfrage bei wenigen Hochschulen hat bereits ergeben, dass an einer Hochschule pro Semester nur etwa fünf Gasthörer:innen eingeschrieben werden, während an einer anderen 400 Gasthörer:innen erfasst werden. Die zu erwartenden Potenziale sind also höchst unterschiedlich. Dieser Unterschied kann im Prinzip auf alle Nutzer:innengruppen übertragen werden.

3.2.3 Grundsätzliche Anbindung

Je nach Nutzer:innengruppe werden die Identitäten in verschiedenen Softwaresystemen verarbeitet. Wenn das CaMS Zugang zu einer gesicherten Identität über ein Nutzer:innenkonto hat, so könnte es hier ebenfalls als Zugangstor dienen. Unabhängig davon könnte ein Verfahren zur Übernahme der Identität in das Campus Managementsystem (CaMS) immer gleich ablaufen (siehe dazu Abschnitt 3.1.1.1). Ausgehend von den über das Nutzer:innenkonto übermittelten Daten könnte anschließend ein Online-Verfahren gemäß den einschlägigen Hochschulprozessen folgen. Dazu gehört in diesem Beispiel vor allem eine Entscheidung über die Gasthörerschaft. Bei einer vollständigen Digitalisierung können idealerweise auch anfallende Gebühren direkt im Online-Verfahren gezahlt werden, sodass eine Freischaltung der notwendigen Funktionen im System und angeschlossene Prozesse (Erstellung einer Chipkarte, Übertragung ins IDM, Anlage einer elektronischen Akte etc.) automatisch angestoßen werden können.

3.2.4 OZG-Leistung zur Gasthörerschaft

Im Rahmen des *Bildungszugangs* definiert das Umsetzungsprojekt *Bildungsjourney* die Verwaltungsleistung *Gasthörerschaft Zulassung.* Zum heutigen Zeitpunkt[16] ist noch kein offizieller Beschreibungstext des Föderalen Informationsmanagements (FIM) auf der Informationsplattform verfügbar, daher ist der Inhalt der Verwaltungsleistung noch stark interpretierbar. Es herrscht an den Hochschulen ein sehr heterogenes Verständnis der Zusammensetzung dieser Gruppe. Zur Vereinfachung wird im weiteren Verlauf von Gaststudierenden gesprochen werden. Zu den weiteren Nutzer:innen kann man auch - je nach Definition an der jeweiligen Hochschule - Schüler:innen, Senior:innen, Teilnehmer:innen an Weiterbildungsangeboten etc. zählen.
Gemäß den Vorgaben zur Erreichung des Reifegrades 3 ist ein Online-Antrag vorzuhalten. Dies ist von den Gasthörenden auszufüllen und führt zur weiteren Bearbeitung. An dieser Stelle ist die Verbindung zu einer gesicherten digitalen Identität hilfreich.

3.2.5 Gruppen von Nutzer:innen mit großem Digitalisierungspotential

Analog zur Gasthörerschaft sollte den folgenden Gruppen ebenfalls ermöglicht werden, sich online mit Hilfe eines externen Authentifizierungsverfahrens zu registrieren. Auch hier gelten die bereits oben ausgeführten Unterschiede zwischen EU-In- und Ausländer:innen.

- **Externe (Zweit-)Prüfer:innen**: Personen dieser Gruppe zählen nicht zu den Mitgliedern der Hochschule. Sie müssen aber dennoch im CaMS erfasst werden, damit sie Abschlussarbeiten ansehen, Bewertungen abgeben und als Prüfer:innen auf den Abschlussdokumenten ausgegeben werden können. Auch müssen sie über ihre Kontaktdaten für die Studierenden, das Prüfungsamt und den Prüfungsausschüssen erreichbar sein.

- **Dozent:innen/Lehrbeauftragte**: Im Idealfall werden diese Nutzer:innen zuerst im Personalverwaltungssystem als identitätslieferndem Fachverfahren angelegt. Danach werden die Identitäten an die verschiedenen angebundenen Systeme verteilt. Es muss ein definiertes führendes System für die Datenhaltung dieser Gruppe von Nutzer:innen

[16] Juni 2022

geben. Mit einer Online-Authentifizierung der Personen über Nutzer:innenkonto können die Prozesse direkt mit gesicherten Daten ablaufen, unabhängig vom physischen Erscheinen der Person an der Hochschule.

- **Alumni**: Abhängig von den Satzungen der Hochschulen und der jeweiligen Rechtslage gelten die ehemaligen Studierenden noch als Mitglieder der Hochschule oder als Externe. In den meisten Fällen müssen die Studierenden aber noch zu Studienzeiten oder bereits im Rahmen der Immatrikulation der Datenübernahme in die Software zur Verwaltung des Alumni-Netzwerks einwilligen. Dies gilt auch, wenn es sich um ein mit dem CaMS integrierten System (z. B. HISinOne-ALU) handelt. Stammt die Identität direkt aus dem CaMS, kann dieser vertraut werden. Wenn die Registrierung erst nach dem Ausscheiden aus der Hochschule erfolgt, muss dieses Vertrauen erst wiederhergestellt werden. Auch hier können die bereits oben beschrieben Verfahren verwendet werden. Eine Verknüpfung mit einer Online-Bezahlkomponente erscheint sinnvoll, beispielsweise für die Begleichung von Mitgliedsbeiträgen oder für das Sammeln von Spenden.

- **Austauschstudierende/Austauschwissenschaftler:innen**: Zur Vorbereitung des Studiums bzw. Forschungsaufenthalts an der Hochschule für Personen, die von einem anderen Standort insbesondere aus dem Ausland kommen, ist eine gesicherte Identifizierung notwendig, um bestimmte administrative Prozesse bereits vor der Anreise zu erledigen oder zumindest starten zu können. Betrachtet man die Prozesse des *Erasmus+-Programms* als ein Beispiel für ein Austauschprogramm, erfolgt die Übertragung der Identität aus der abgebenden Hochschule. Dieser Identität kann im Rahmen des Programms vertraut werden. Ergänzend können auch hier die oben genannten Verfahren verwendet werden, insbesondere wenn es sich um *Freemover* handelt, die ohne festes Austauschprogramm ein Gastsemester in Deutschland verbringen. Hier müssen sich aber wieder entsprechende Anträge bzw. Antragsverfahren anschließen.

3.2.6 Weitere Gruppen ohne detaillierte Betrachtung

Im Folgenden werden weitere, aber eher selten mit dem CaMS in Verbindung stehende Gruppen von Nutzer:innen aufgeführt.

- **Externe** mit Zugangsberechtigung/Notwendigkeit zu Hochschulinfrastruktur. Hier geht es vor allem um die (elektronische) Zugangskontrolle, wie bspw. die Schranke auf dem Parkplatz oder Zugänge zu gesicherten Räumen.

    - Externe Dienstleister:innen: Wenn bspw. Malerarbeiten in einem Seminarraum durchgeführt werden und dieser der Öffentlichkeit nicht zugänglich ist, wird eine Zutrittskontrolle benötigt. Der Zugang für die Wartungs- und Pflegearbeiten kann durch eine Registrierung und digitale Überprüfung der Identität erfolgen. Der Einlass erfolgt dann mit Hilfe des Smartphones, welches als Hardware-Token bzw. Elektronischer Ausweis dient (NFC). In Pandemie-Zeiten kann dies mit dem Impf- und Gesundheitsstatus verbunden werden (*2G/ 2G+Regeln*). Ein weiteres Beispiel wäre der außerplanmäßige Zutritt von Raumreinigungskräfte eines externen Anbieters zu besonderen Anlässen.

    - Teilnehmer:innen am Hochschulsport oder den Angeboten von Studium Generale: Bei vorhandenen freien Kapazitäten gibt es Angebote, die gegen Entgelt auch den Nicht-Mitgliedern der Hochschulen verfügbar gemacht werden.

- **Teilnehmer:innen** an besonderen Programmen der Hochschulen, die nicht oder noch nicht zu den Mitgliedern der Hochschule zählen:

    - Schülerstudierende sind besonders qualifizierte Schüler:innen, die das Angebot bekommen, bestimmte Vorlesungen bereits vor dem Schulabschluss zu besuchen und Leistungen zu erbringen, die später in bestimmten Studiengängen angerechnet werden können.

    - Bei bestimmten Studiengängen gibt es Vorabprüfungen, die an den Hochschulen durchgeführt werden. Manche davon werden zentral für mehrere Hochschulen abgehalten, wie z. B. die sogenannte Deltaprüfung in Baden-Württemberg. Die Deltaprüfung ermöglicht Bewerber:innen mit Fachhochschulreife oder fachgebundener Hochschulreife das Studium an einer Universität oder Pädagogischen Hochschule (Universität Mannheim 2022).

3.3 Kontext Cybersecurity und Standards (wie eIDAS) im Bildungswesen

Autor: Strack, Hermann

Auch EU- und weltweit beachtete hochwertige technische Sicherheitsinnovationen samt Infrastrukturen/Komponenten und Rollouts wurden in den letzten 30 Jahren wesentlich aus Deutschland auf den Weg und in den Einsatz gebracht (wie IT-Sicherheitskriterien für Systemsicherheitsevaluierungen mit Transfer zu ITSEC/Common Criteria ISO, Signaturgesetz/VO mit SigG-PKI und Signaturchipkarten (samt Transfer zur EU-Direktive für elektronische Signaturen 1999/2000), erste Notifizierung eines eID-Ausweissystem nach eIDAS in der EU, DE 2017). Damit wurden essentielle Grundlagen und Pfeiler als Assets für auch stark gesicherte großflächige bundes- und länderweite Digitalisierungen in Wirtschaft und Verwaltung gelegt, was mit Blick auf dramatisch verschärfte IT-Sicherheitsbedrohungen und Angriffe grundsätzlich eine gute Aufstellung bzgl. Sicherheit und Schutz unterstützt. Allein sind über die Jahre trotz wichtiger *Leuchttürme* großflächige und durchgängige Integrationen dieser Sicherheits-Assets im Bereich der Verwaltungsdigitalisierung zurückgeblieben (im Gegensatz zu anderen EU-Ländern wie etwa Estland, mit stringenter Umsetzungsperformance). Weiter haben andere EU-Länder zum Teil seit mehr als 15 Jahren großflächige Digitalisierungen auch in der Verwaltung des Bildungswesens umgesetzt.

Im Rahmen der OZG-Umsetzungen für das Bildungswesen ist die Integration auch von hochwertigen Sicherheitsstandards (wie eID per Personalausweis und OZG-Nutzer:innenkonten) essentiell und obligatorisch, ebenso wie für kommende Innovationen im Bildungswesen, wie der Nationalen Bildungsplattform (BMBF). Vor diesen Hintergründen werden im Folgenden Asset-orientiert wichtige Grundlagen, Entwicklungen, Standards und Ergebnisse zu Innovationen für gesicherte Digitalisierungen im Bildungswesen (z. T. kursorisch) vorgestellt, auch zur Abgrenzung von postfaktischen Phänomenen. Für weitere Details und Vertiefungen wird auf Quellen verwiesen.

3.3.1 eID und TrustServices in EU versus Digitalisierungen Hochschulen/Schulen

Wichtige sicherheitsbezogene Teilthemen im OZG-Bereich, wie Infrastrukturen und Anbindungen zum föderierten Identitätsmanagement oder (fortgeschrittene) elektronische Signaturen per DFN-PKI, sind keineswegs neu im Hochschulumfeld. Die Integration und Nutzung von Diensten wie eduroam, DFN-AAI und Software wie Shibboleth (auf Basis von Standards wie SAML wie bei eIDAS eID) an deutschen/europäischen Hochschulen zeigt dies seit Jahren.

Durch die OZG-Umsetzung sind allerdings jetzt auch Verwaltungsbereiche von Hochschulen stärker involviert, insbesondere im Bereich des Bewerber:innen- und Studierendenmanagements.

Deutschland ist im europäischen aber auch weltweiten Vergleich mit erstmaligen hochwertigen Realisierungen und Rollouts für sicherheitstechnische Infrastrukturen aufgefallen (allerdings klar zu unterscheiden von einer breitflächigen stringenten Integration im Verwaltungswesen): Bereits 1997 wurden in Deutschland (erstmalig in Europa) Signatur-Gesetz und -Verordnung verabschiedet und unter hochwertigen Sicherheitsprüfungen (u. A. nach ITSEC und Common Criteria für Signaturkomponenten) entwickelt und zur Verfügung gestellt, wie SigG-TrustCenter/CA der Deutschen Telekom 1998/1999. Erste wegweisende Umsetzungen im E-Government und entsprechende Standardisierungen (wie XÖV) erfolgten im Projekt MEDIA@Komm (Förderung BMWi, 1999-2003) samt Begleitforschung ausgehend von den geförderten Preisträgerkommunen Bremen, Esslingen, Nürnberg (vgl. Strack 2001). In Europa war Deutschland 2017 der erste Staat, welcher sein nationales Personalausweis-eID-System nach eIDAS-Verordnung der EU[17] erfolgreich notifizieren ließ samt Umsetzung der eIDAS-eID-Konnektion (vgl. Projekt TREATS EU CEF 2017).

Hinsichtlich der Thematik der digitalen Identitäten (samt zugeordneter Authentisierungs- und Autorisierungssicherheitsfunktionen) wurden entsprechende Notwendigkeiten bereits vor Jahren sowohl auf nationaler als auch europäischer Ebene als strategische Themen für die staatliche Regulierung erkannt und insbesondere durch die Regulierung per eIDAS-Verordnung der EU zu einer eindrucksvollen Umsetzung von Interoperabilität bzgl. der jeweiligen (notifizierten) eID für Bürger und Verwaltungen der EU-Mitgliedsstaaten auf Basis der nationalen Bürgerausweise als auch zusätzlich per europäischen Standards/per ETSI für den Bereich der (signaturbasierten) TrustServices TS geführt haben (für beide eIDAS-Bereiche eID und TS werden dabei drei (aufsteigende) Sicherheitsniveaus, auch *Level of Assurance (LoA)*, unterschieden, siehe oben Abschnitt 2.2.2) . Dabei wurde EU-weit die eindeutige Identifizierbarkeit von Personen auf Basis des sogenannten *eIDAS-eID Minimum Data Set (MDS)* festgelegt und eine entsprechende in der EU grenzüberschreitende eIDAS-eID-Infrastruktur für

[17] eIDAS löste 2014 die vorherige EU-Direktive für elektronische Signaturen ab, und wurde technisch/organisatorisch vorbereitet durch die F&E-Projekte STORK der EU (vgl. Leitold et al. 2015).

eIDAS-notifizierte Mitgliedsstaaten EU-weit aufgebaut (per weltweitem SAML-Standard web-integriert, mit eIDAS-Konnektoren zur Kopplung der nationalen eID-Server/Service-Systeme). Diese Assets sind dann in EU-Projekten mit europäischen Förderungen zur Umsetzung (Erasmus, EU CEF) für den Bildungs- und Hochschulbereich integriert worden im Sinne der Umsetzung der EU-Beschlüsse von Göteborg 2017 zur EU-weiten Umsetzung der sogenannten Student eCard für Studierendenmobilität bis 2025 (vgl. European Campus Card Association 2020). Aus Deutschland sind hier insbesondere die deutschen EU-CEF-Projekte TREATS und StudIES+[18] zu nennen, welche erstmalig Prototypen nach eIDAS für wichtige Hochschulanwendungen entwickelt haben (andere EU-Projekte wie EMREX sind dabei in EU-Mitgliedsstaaten bereits produktiv im breiten Einsatz im Bildungs-/Hochschulwesen, wie für EMREX z. B. in Schweden, Norwegen, Niederlanden, Polen).

An der Hochschule Harz, Arbeitsgruppe Strack/netlab, wurden im Rahmen von F&E-Erprobungen (weiterentwickelte) Prototypen auch immer wieder ausgewählt in realen Hochschulprozessen eingesetzt (z. B. Prüfungswesen, Praktikumswesen, Nachweis- und Zeugniswesen, von 2009-2022), beginnend mit Kompetenzzentrumsprojekten wie SecInfPro/SeDiGov, dann e-Campus (EFRE, 2009-2013) mit Förderungen des Landes Sachsen-Anhalt. Dies führte bereits früh zu einer positiven Referenzierung dieser Arbeiten im EU-E-Government-Benchmark-Report 2012 sowie zur Aufnahme in die 1. E-Government-Initiative des Bundesministeriums des Innern (BMI, ab 2011/2012) zum (damals neuen) Personalausweis mit eID-Online-Ausweisfunktion (eID/nPA), hier als einzige Hochschule, mit Ergebnispräsentation u. A. auf der CeBIT 2013 in Hannover (Hochschule Harz 2013). Diese Projekt-Vorarbeiten sind wiederum eingegangen in nationale F&E-Projekte wie *SHIELD*[19] *(BMWi), CyberSecurity-Verbund-Sachsen-Anhalt (EFRE)*[20], insbesondere zu Prototypen aktuell aus 2022 zur Infrastruktur für die Nationale Bildungsplattform NBP (BMBF) samt OZG-Konten-Anbindungen, im Prototyp *KOLIBRI*[21] (vgl. Bechtle AG 2022; vgl. Strack et al. 2022a; vgl. Strack et al. 2022b) welche nicht nur Prototyp-Lösungen für OZG an Hochschulen, sondern übergreifend für den gesamten Bildungsbereich entwickelt haben.

[18] siehe auch https://studies-plus.eu/ sowie https://netlab.hs-harz.de/research/TREATSWS/

[19] siehe https://www.shield24.de/

[20] siehe https://cslsa.de/

[21] siehe auch https://www.bechtle.com/ch/ueber-bechtle/news/unternehmensmeldungen/pressemeldungen/2022/konsortium-um-bechtle-praesentiert-prototyp-fuer-nationale-bildungsplattform

Gerade im europäischen Vergleich hinsichtlich des Standes der (Verwaltungs-)Digitalisierung im Bildungswesen mit gewissen Basisansprüchen an Vereinheitlichung oder gar Standardisierung zeigen andere EU-Mitgliedsstaaten z. T. bereits seit Jahren oder gar Jahrzehnten klare Vorsprünge gegenüber der Situation in Deutschland, welche auch mit dem immer wieder gerne bemühten Hinweis auf den *Bildungsföderalismus* in Deutschland nicht befriedigend erklärt werden können. Hochschulübergreifende Digitalisierungen wurden bereits um 2007 im Rahmen der Gründung der Initiative RS3G (Rome Students, Systems, Standards, Group - heute eine EUNIS Task Force) aus mehreren EU-Mitgliedsstaaten vermeldet (wie u. A. aus Schweden, Niederlanden, Italien, Spanien, Irland - *ohne Anspruch auf Vollständigkeit hier*), welche sich einer EU-weiten Vereinheitlichung/Standardisierung von hochschulübergreifenden Verfahren widmete (*unter Mitwirkung des Autors hier*), insbesondere zu Studierendenmobilität in Europa im Bologna-Kontext.

Weiter ist heutzutage auch eine angemessene und zeitgemäße Weiterentwicklung hinsichtlich des Mindestniveaus an Schutz und Sicherheit bei öffentlichen Internet- und Web-Angeboten auch an Hochschulen angesichts der wachsenden Cyber-Bedrohungslage angezeigt (vgl. jährliche BSI-Lageberichte[22]), was auch bedeutet, sich zunehmend von herkömmlichen und nicht mehr zeitgemäßen Defaults wie Nutzer:innenauthentisierungen auf Niveau *niedrig* per Username/Passwort bei öffentlichen Internet-Zugängen bzw. sensitiven System- und Prozesszugängen zu verabschieden (zugunsten von Sicherungen auf eIDAS-Niveau *mittel* bzw. *hoch*). Seit Jahren zunehmende Internetgroßangriffe auf öffentlich-rechtliche Einrichtungen inkl. Hochschulen auch mitten in Deutschland zeigen dies mehr als deutlich. Hier sind grundsätzlich alle Bürger:innen in der EU bereits seit einigen Jahren mit der Einführung von höherwertigen Mehrfaktor-Authentisierungen im Zahlungswesen im Alltag konfrontiert, u. A. durch die Umsetzung der PSD2-Richtlinie (vgl. Deutsche Bundesbank 2018), eingeführt aus Sicherheitsgründen vor weltweit steigenden Cyberattacken.

3.3.2 Sicherheitstechnische Grundlagen, Randbedingungen und Standards/Umsetzungen

Mit der Entwicklung der grundlegenden Internetstandards TCP/IP sowie der Internetstandardisierung als solcher in den 1970er-Jahren ging zeitlich einher die grundlegende Entwicklung einer neuen Art von Kryptographie, der PublicKey-Kryptographie samt Infrastrukturen (PKI)

[22] siehe https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.htm

auf Basis der Arbeiten von Diffie, Hellmann und Merkle (vgl. Merkle 1980), gefolgt von erstmaligen Krypto-Implementierungen durch das RSA-Team (vgl. Rivest et al. 1978). PKI-Anwendungen gewannen insbesondere mit der Einführung des Web ab Mitte der 90er-Jahre samt späterer Einführung von *Basissicherungen* für Webserver/interaktive Webapplikationen per SSL-Sicherheitsprotokoll/PKI-Zertifikaten (Netscape, SSL als Ausgangspunkt für die späteren TLS-Internetstandards) an Bedeutung, da nun Web-Nutzer:innen per automatischem Browser-SSL-Zertifikate-Check die Authentizität der URL-Namenszuordnung der Website remote validieren konnte, samt automatisierten Aufbau nach Web-Session-Key-Vereinbarung dann einer verschlüsselten Webverbindung (https) zum Webserver zwecks Erhaltung der Authentizität und Vertraulichkeit des Web-Datenaustausches zwischen Webbrowser/Nutzer:innen und Webserver/Applikation. Die grundsätzlich als SSL/TLS-Option einer gleichzeitig möglichen Nutzer:innen-Authentisierung per persönlichem SSL-Zertifikat wurde oft zugunsten einer einfacheren Username/Password-Authentisierung der Nutzer:innen dagegen nicht genutzt. Mit dieser neuen *asymmetrischen* Kryptographie mit einem Schlüsselpaar aus öffentlichem PublicKey PK und geheimen SecretKey SK pro Nutzer:in waren nunmehr zwei grundlegende kryptografische Sicherheitsfunktionen möglich sowie ein gegenüber der traditionellen symmetrischen Verschlüsselung vereinfachtes Schlüsselmanagement auf Basis von (CA-signierten) PKI-Zertifikaten für öffentliche Nutzerschlüssel ohne jeden Geheimschlüsseltransfer (wie im symmetrischen Kryptofall bisher) und damit Internet-tauglich:

a) Gezielte Empfängerorientierte PKI-Verschlüsselungsfunktionen für Daten mit dem PK der Empfänger:innen, nur von diesem per SK entschlüsselbar.

b) Einzigartige Signierer-/Absenderorientierte digitale Signaturfunktionen/Signaturen mit dessen SK als Signierschlüssel, mit breiter öffentlicher Validierbarkeit der Signaturen durch alle Nutzer:innen/Empfänger:innen mit dem PK der Signierer:innen (z. B. über CA per Zertifikat zugänglich).

c) Die PKI-Kryptofunktionen werden zur Realisierung als PKI-Mechanismen mit Wirksamkeit auf Basis mathematischer Strukturen und Verfahren als Spezialgebiet der angewandten Mathematik zur Verfügung gestellt, und beruhen auf sogenannten *schweren* mathematischen Berechnungsproblemen (bei fehlenden Schlüsseln; bekanntlich bei RSA beruhend auf dem *schweren* Problem der Faktorisierung großer ganzer Zahlen in Primzahlen;

bei anderen Verfahren wie *ElGamal* basierend auf dem schweren Problem der Berechnung von diskreten Logarithmen in spezifischen Zahlbereichen), die hinreichende Auslegung der Kryptoverfahren und Parameter (auch im Laufe der Zeit) wird durch wissenschaftliche Communities von Kryptographen (Entwicklung) und Kryptoanalytikern (Brechungsversuche) mit öffentlicher jährlicher Dokumentation per Krypto-Fachtagungen sichergestellt, für staatlich regulierte hochwertige (qualifizierte) PKI (etwa früher nach Signaturgesetz, heute nach eIDAS) übernehmen ergänzend nationale Krypto-Behörden (wie BSI) bzw. deren EU-weiter Zusammenschluss (SoGiS EU[23]) basierend auf dem Stand der Wissenschaft diese Veröffentlichungsaufgaben in strukturierter, regelmäßiger und transparenter Form.

Grundsätzlich sind alle diese kryptographischen Wirksamkeitsaussagen *zeitbefristet* (üblich heute oft zwischen zwei und sechs Jahren), daher werden auch die PKI-Zertifikate entsprechend in der Gültigkeit zeitbefristet. Die Signatur von Nutzerzertifikaten durch CA zum Ausweis/zur *Beglaubigung* deren Echtheit/Vertrauenswürdigkeit (daher der Name TrustServices TS und TrustService Provider TSP für CA in der eIDAS VO) führt zu Zertifikatshierarchien, da die CA ihrerseits für ihre eigenen Signaturschlüssel für Nutzer:innenzertifikatssignierungen wiederum CA-Zertifikate benötigen. Die in der Regel dezentralen CA werden national bzw. EU-weit Meta-CA-ähnlich in sogenannten Vertrauenslisten mit Ihren CA-Zertifikaten (signiert) hierarchisch als Hierarchieabschluss (root) zusammengeführt, zur Überprüfbarkeit für Nutzer:innen.

Eine wichtige Randbedingung ist dabei, dass in der Laufzeitkomplexität sich praktikable asymmetrischer Kryptoverfahren[24] als wesentlich aufwändiger (ca. drei Größenordnungen, d. h. Faktor 1000) herausstellten als symmetrische Verfahren. Für den praktischen Einsatz bedeutet dies u. A., dass *Beschleunigungsmaßnahmen* essentiell für PKI-Anwendungen wurden, einmal per *komprimierenden* Krypto-Hash-Funktionen für zu signierende Dokumente (gleichzeitig Einwegverschlüsselungen) und dann Signatur nur dieser *kurzen* Hashwerte (statt des ganzen Dokumentes) als auch bei Sicherheitsprotokollen die PKI-Anwendung nur für die Vereinbarung eines symmetrischen Session-Keys, und dann dessen *schneller* symmetrischer Anwendung für

[23] siehe auch https://www.sogis.eu/uk/supporting_doc_en.html

[24] siehe auch https://www.bundesnetzagentur.de/EVD/DE/SharedDocuments/Downloads/Anbieter_Infothek/Algo_Empfehlungen2018.pdf

die Verschlüsselung der Protokolldaten. Die PKI-Zertifikate werden von Certification Authorities CA (Trustcenter, Zertifizierungsstellen) nach Nutzeridentifikation auf Antrag erzeugt, und in Verzeichnisdiensten zum öffentlichen Abruf oder beschränkt nur zur indirekten Prüfung bereitgestellt.

PKI-Zertifikate können von Nutzer:innen, der CA oder anderen Berechtigten widerrufen/gesperrt werden, mit entsprechenden Markierungen im PKI-Verzeichnisdienst. Die Gültigkeitsprüfung einer Signatur besteht aus zwei Teilen, welche beide positiv sein müssen:

- der mathematischen Signaturprüfung unter Anwendung des PublicKey des mutmaßlichen Signierenden auf dem signierten Objekt/Datensatz (PKI-Entschlüsselung)
- der Prüfung der PKI-Zertifikatskette oberhalb der Signaturebene (zwei Gültigkeitsmodelle: das Kettenmodell (wie ehemals exklusiv nach Signaturgesetz) erfordert die Gültigkeit der Zertifikatskette nur zum Signaturzeugungszeitpunkt, spätere Sperren sind unbeachtlich; das heute nach eIDAS eher favorisierte Schalenmodell erfordert die Ketten-Gültigkeit zum Prüfzeitpunkt, d. h. Zertifikatssperren führen zu einer ungültigen Signaturprüfung), vgl. auch BSI Anlage TR-ESOR-M.2: Krypto-Modul (BSI 2018).

Zertifikatssperren per CA-Verzeichnisdiensten könnten nach Schalenmodell daher auch bereits für den Widerruf von signierten Dokumenten genutzt werden (neben alternativen Infrastrukturen), z. B. zum Widerruf von digitalen Bildungsnachweisen bzw. Zeugniskopien.

Hinsichtlich der Vertrauenswürdigkeit[25], Sicherheit und Wirksamkeit werden *qualifizierte Signaturen/CA* mit erhöhten Anforderungen von *fortgeschrittenen Signaturen/CA* strukturell unterschieden (sicherheitstechnisch sowie organisatorisch wie z. B. sehr hochwertige Authentisierung der Nutzer:innen bei der CA-Registrierung mittels amtlichen Ausweisen sowie CA-Sicherheits-, Betriebs- und -Haftungsanforderungen). Insbesondere wird bei qualifizierten Signaturen (QES) zur Absicherung des *Secret Key* und seiner Verwendung eine sogenannte sichere Signaturerstellungseinheit verlangt (in der Regel durch Sicherheitshardware wie Kryptochipkarten, -HSM oder ähnlich umgesetzt, welche den Secret Key wirksam hinsichtlich Speicherung und Einsatz bei kryptografischen Rechnungen kapseln: Die zu signierenden Daten werden dieser Hardware dann zum Signieren zugeführt). Dieser hochwertige Schutz (LoA

[25] siehe auch https://www.elektronische-vertrauensdienste.de/cln_111/EVD/DE/Anbieter/Infothek/Grundlagen/start.html

hoch) führt dann u. A. zur EU-weiten rechtlichen Anerkennung als Unterschrifts- bzw. Schriftformersatz (eIDAS VO TS).

Die (recht enge) Zeitbefristung für die Gültigkeit von Signaturen (vgl. BSI 2018), insbesondere voll rechtsverbindlichen QeS, führt zu Problemen bei langfristig angelegten Verwendungen, wie Zeugnissen oder anderen langlebigen Bescheinigungen/Urkunden, wie z. B. Eichunterlagen von Geräten. Dieses war Ausgangspunkt zur Entwicklung langlebiger Sicherungsverfahren für signierte archivierte Daten, nach dem *ArchiSig/Save-Prinzip* (ursprünglich u. A. durch die PtJ Braunschweig[26]), welche dann zu BSI-Standards *TR-ESOR* (vgl. BSI 2018) bzw. *eIDAS Preservation Services* unter Anwendung von automatisierten sogenannten „Übersignaturen" in digitalen Langzeitarchiven führten, mit denen die Gültigkeit signierter Daten prinzipiell unbegrenzt in die Zukunft gerettet werden kann (durch Iteration); mit Integration verschiedener Gültigkeitsmodelle.

Für weitere Details sei auf das PKI-Handbuch des BSI verwiesen, welches sich auf die Verhältnisse bis zur Einführung der eIDAS TS bezieht, ein eBook-Update unter Einschluss der eIDAS samt ETSI-Normierung ist angekündigt. Weiter ist hilfreich hier die Webseite der zuständigen Bundesnetzagentur[27]. Zum notwendigen *Security by Design* für den Einsatz in der Applikationsentwicklung (samt Berücksichtigung von Krypto-Agilität) auf Basis von Standards und Komponenten (vgl. Assmann et al. 2021). Zusätzlich sind bei OZG-Kontenzugängen entsprechende Separierungen der Daten-Zugänge nach LoA-Stufen zu beachten.

Hochwertige Signaturen nach Signaturgesetz (DE 1997) wurden nach Verwaltungsverfahrensgesetz und BGB für Verwaltung und Wirtschaft als Schriftformersatz rechtlich anerkannt (kurz nach 2000). Allerdings gestaltete sich das Rollout im Sinne von bundesweiten Massenanwendungen nicht wie erwartet (zögerlich sowie mit geringen Nutzer:innenzahlen), insbesondere für Verwaltungsanwendungen, einmal da die Finanzierung der Signaturausrüstung komplett den Bürger:innen überlassen wurde, andererseits da es kaum elektronische Angebote insbesondere bei den für Bürger:innen besonders wichtigen Kommunen gab (im Gegenteil oft sogenannte negative elektronische Zugangseröffnungen für signaturhaltige Einreichungen bei

[26] siehe auch https://www.ptb.de/cms/archisafe/startseite.html

[27] siehe https://www.elektronische-vertrauensdienste.de/cln_111/EVD/DE/Anbieter/Infothek/Grundlagen/start.html

Verwaltungen, auch mangels entsprechender Verpflichtungen für die Verwaltungen). Im Rahmen der Föderalismusreformen mit Einführung u. A. des IT-Planungsrates 2010 mit bundesweiten Kompetenzen und Regulierungskontexten (vgl. IT-Planungsrat 2022) auch zur Durchsetzung von eGovernment-Standards auf allen Verwaltungsebenen (ebenfalls nPA mit eID 2010) sowie sukzessive der Einführung E-Government-Gesetzen in Bund und Ländern wurden zunehmend elektronische Zugangseröffnungen der Verwaltungen für QES-signierte bzw. eID-basierte Daten/Formular-Einreichungen verpflichtend, zuletzt per OZG-Einführung 2017. Die eID-basierte Daten-Einreichung auch per OZG-Konten - hier auf der höchsten OZG-Authentisierungsstufe per eID - wirkt als eine Art *eID-Privileg* nur gegenüber Behördenportalen auch als alternativer Schriftformersatz vgl. VwVFG § 3a (auch ohne QeS), weiter werden hier entsprechende elektronische Bescheidzustellungen der Behörden über sogenannte OZG-Postfächer der OZG-Nutzer:innenkonten (allerdings sind Behörden-Authentisierungen im Kontext der OZG-Postfächer noch in Konzeption/Entwicklung, laut NKB-Sprechstunde 08/2022). Unternehmen können per OZG-Unternehmenskonten als Clients integriert werden, nicht jedoch als OZG-Serviceanbieter (dagegen sind Unternehmensportale mit eID-BerCert-Berechtigungszertifikat und eID-Zugängen zu Unternehmensservices möglich, inkl. eIDAS/eID).

Grundsätzlich werden sowohl Signaturen/TrustServices als auch eID über verschiedene CA mit PKI gesichert (erstere in der Regel privatwirtschaftlich, eID-PKI in der Regel mit staatlichen Anteilen). Im eID-Anwendungsfall sind die sicherheitstechnischen Infrastrukturen gesetzlich rechtlich geregelt (vgl. Personalausweisgesetz) sowie sicherheitstechnisch durch BSI-eID-Standards (BSI TR 03124 bis TR 03130), ergänzend auch für OZG-Konten. Durch das hochwertige (HW-basierte) sicherheitstechnische Integrieren von eID-Personalausweiskarte samt (kostenloser) AusweisApp2-ClientSoftware (Bürger:innen) sowie von HSM-abgesicherten eID-Services in Web-Portalzugängen über verschlüsselte und signierte Protokoll-Anbindungen nach SAML-Standard im Sinne eines eID-basierten Identitätsmanagements (für Serviceanbieter z. B. Behörden, jeweils mit eID-Berechtigungszertifikat) wird das Sicherheitsniveau der (nun stets beiderseitigen) eID-Authentifikation auf *hoch* gehoben, im Vergleich etwa zu vorherigen Username/Password-Lösungen (*niedrig*), siehe nachfolgende Abb. 3 des BSI:

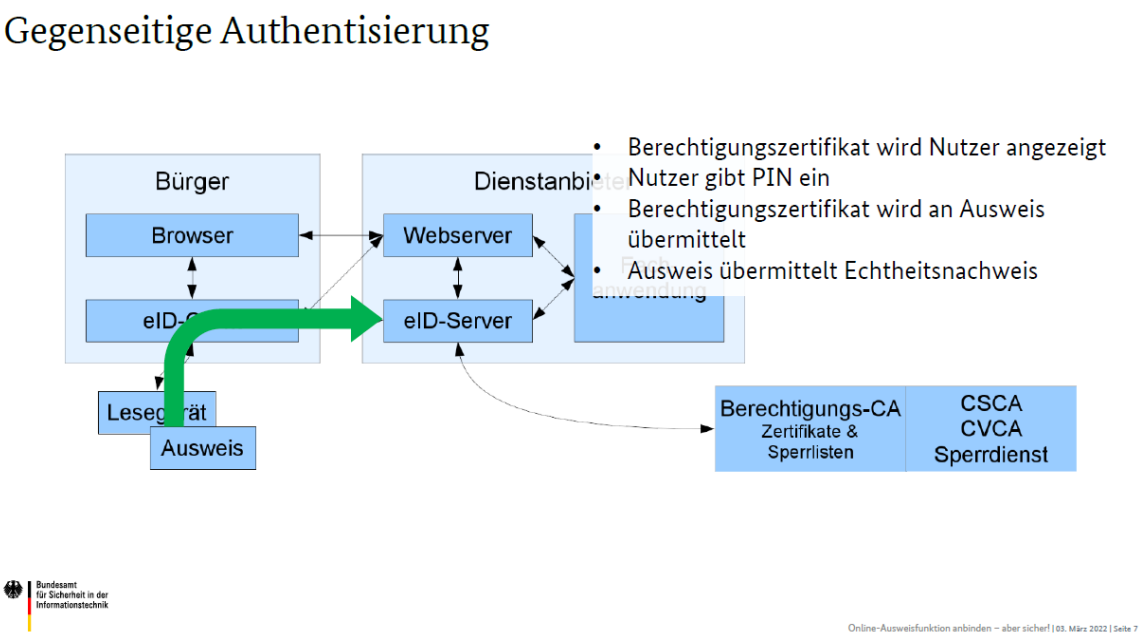

Abb. 3: Gegenseitige Authentisierung (BSI)

Während in qualifizierten PKI-Zertifikaten für Signaturlösungen/TrustServices in der Regel nur sparsam per Name/Vorname als Personendaten obligatorisch sind (weitere Feld-Optionen sind möglich bei Nutzer:innenzustimmung, z. B. auch Feldsetzungen für berufliche Zulassungen oder Vertretungsmachten für Dritte), stehen grundsätzlich in eID-aktivierten Ausweisen die vollen Klartext-Ausweisdaten samt Nutzer:innen-Portal-spezifischem Pseudonym (jedoch ohne Biometriedaten) zur Identifikation nach beiderseitiger Authentisierung Bürger:innenausweis vs. Webportal/eID-Service mit Berechtigungszertifikaten bereit, allerdings im Sinne des Datenschutzes im Daten-Austausch wirksam beschränkt einerseits durch die vorgesehenen Feld-Attribute im eID-Berechtigungszertifikat des Portals (Berechtigung geprüft/erteilt vom Bundesverwaltungsamt), und andererseits durch die erforderlich Zustimmung der Nutzer:innen per PIN-Eingabe zur Ausweiskarte. Die eID-Services werden in der Regel remote über dezentrale (privatwirtschaftliche) zugelassene eID-Serviceanbieter eingebunden, sehr große Anwender (wie Deutsche Rentenversicherung) betreiben auch eigene eID-Server/Services. Im Rahmen der Umsetzung der eIDAS-Notifizierung des deutschen Personalausweiswesens wurden die eID-Services DE um eIDAS-Konnektoren zur eID-Validierung von Ausweisen aus anderen notifizierten EU-Mitgliedsstaaten erweitert[28]. Weiter werden OZG-Kontenzugänge (auch mit eID-Berechtigungszertifikat) über den Bund und die Bundesländer angeboten, und in der

[28] siehe auch https://netlab.hs-harz.de/research/TREATSWS

Regel per SAML an Behördenportale angebunden (entheben daher dann Behörden wie Kommunen eigener eID-Service-Anbindungen).

Die PKI/Zertifikats-Einsatzzwecke sind also verschieden: Im Signatur-/TrustService-Fall zielen diese auf die (ohne eIDAS Preservation Services zunächst recht eng zeitbefristete) Umsetzung von PKI-basierten Signatur-/TS-Validierungen für elektronische Dokumente (insbesondere zum Schriftformersatz per QeS) z. B. für Bildungsnachweise oder Zeugniskopien, im eID-Fall zielen diese dagegen auf hochwertige Online-Zugangs-Authentisierungen der Nutzer:innen für WebPortale, samt nachfolgender Übermittlung standardisierter Ausweis-Personendatensätze (per eIDAS/eID auch EU-weit) im Positivfall sowie bei Nutzerfreigabe an das WebPortal (bei OZG nur von Behörden). Im Sinne eines hochwertigen Datenschutzes bzw. Missbrauchsschutzes werden bei der eID-Lösung zum deutschen Personalausweis die autorisierten Ausweisdaten in (Session-temporär) verschlüsselten / signierten SAML-Containern nach der Entschlüsselung bewusst nur als Klartext in den WebPortal-Anwendungen zur Verfügung gestellt (d. h. ohne Signatur- oder andere Krypoto-Zusätze auf den entschlüsselten Personendatensätzen), im Sinne einer sogenannten *(Transport-)Kanalbindung* in WebSessions, um so ansonsten einer unberechtigten/ missbräuchlichen Weitergabe von *nachweislich hochwertigen* amtlichen Personendaten vorzubeugen. Andererseits muss damit die (berechtigte) eID-Anwendung für eine klare Trennung/Unterscheidung zwischen *hochwertigen* eID-Daten der Nutzer:innen und manuell eingetragenen Nutzer:innendaten sorgen (z. B. zum Nachweis des eID-Schriftformersatzes). Während die persönlichen Identitätsdaten langlebig sind (auch bei Ausweiswechsel) wechselt das kryptographische Ausweispseudonym bei einem Ausweiswechsel, zur Re-Aktivierung des eID-Pseudonym-basierten Zugangs zu den bisherigen eID-Konten mit dem erneuerten Ausweis gibt es verschiedene Übergangsmöglichkeiten[29], vgl. alternativ auch den YourCredentials-Notarisierungsdienst für Identitäten in StudIES+ 2019 (Strack et al. 2019).

Elektronische Signaturformate/-infrastrukturen sind inzwischen in der EU von ETSI standardisiert[30] auch als Building Blocks für E-Governement, insbesondere die Signaturformate CAdES, PAdES (für PDF-Integration) und XAdES (für XML-Integration). In Zusammenhang mit PDF-Integrationen von Signaturen wurden Schwachstellen bei Validierungsprogrammen/ Readern

[29] siehe auch https://www.personalausweisportal.de/SharedDocs/faqs/Webs/PA/DE/Haeufige-Fragen/9_pseudonymfunktikon/pseudonymfunktion-liste.html

[30] siehe auch https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Standards+and+specifications

vermeldet[31], hier von der PDF-Assoziation jedoch auf nicht standardkonforme Implementierungen zurückgeführt.[32] Hilfreich können hier Sicherheitszertifizierungen für Validierungsprogramme/-services (z. B. nach Common Criteria) oder das (temporäre) alternative Ausweichen auf Detached Datei-Signaturen sein[33].

Für die Zukunft von PKI generell könnten bei erfolgreichem weiteren Ausbau des sogenannten Quantencomputings gravierende Sicherheitsprobleme (Brechen) für heute übliche PublicKey-Kryptoverfahren insbesondere auch für Signaturen auftreten (Schätzungen sehen erste Relevanzen zwischen ca. 2030 und 2050). Daher wurden bereits vor vielen Jahren Entwicklungen für sogenannte PostQuantum-Signaturen/Verschlüsselungen auf den Weg gebracht sowie zusätzliche Standardisierungsbemühungen (u. A. NIST 2017) , welche in 2022 bei der Standardisierungseinrichtung NIST der USA (vergleichbar DIN DE) zu ersten PostQuantum-Kryto-Standards[34] geführt haben.

3.3.3 Infrastrukturen und Anwendungen im Bildungswesen mit Sicherheitsintegrationen

Es werden F&E-Projektergebnisse für Hochschul- und Bildungswesen aus den jüngeren Projekten KOLIBRI (BMBF), CyberSec-LSA (EFRE), StudIES+ (EU CEF), SHIELD (BMWi), TREATS (EU CEF), eCampus (EFRE) samt KAT-Vorprojekten SeDiGov/SecInfPro vorgestellt, diese sind immer wieder auch in produktiven Realverfahren mit echten Nutzern in beschränktem Maßstab erprobt worden, neben vorherigen Erprobungen mit Testdaten/nutzenden.

3.3.3.1 Ergebnisüberblick CyberSec-LSA, StudIES+, SHIELD, TREATS

Die Hochschule Harz ist die erste deutsche Hochschule, die die Online-Funktion des deutschen Personalausweises (eID) für den Kontakt mit ihren Studierenden nutzt und für das europäische eIDAS/eID-Netzwerk erweitert hat, dabei auch mit eIDAS-basierte Anbindung an das EMREX-Netzwerk EU.

[31] siehe https://pdf-insecurity.org/

[32] siehe https://www.pdfa.org/recently-identified-pdf-digital-signature-vulnerabilities/

[33] siehe vgl. StudIES+ / HS Harz 2019.

[34] siehe https://csrc.nist.gov/Projects/post-quantum-cryptography

Folgende eIDAS-Anwendungen sind entstanden:

- eProsecal – Nutzer-Hochschulbasiskonto mit eIDAS/eID & TS (u. a. QES, Siegel, …), für gesicherte Anmeldungen mit Up-/Downloads von Formularen/Daten, sowie mit gesichertem Datei-Sharing bzw. Zugangssicherungen für andere Nutzer per eID/eIDAS
- eNotar – elektronische Beglaubigung von Dokumenten (VwVfG §33) und Identitäten
- eInternship – Praktikumsverwaltung/-verträge zwischen Hochschule und Betrieben
- eTor/eTestate – Anmeldung/Teilnahme-Verwaltung für Prüfungen und Laborpraktika
- Your/MyCredentials – Beglaubigungen für (abgeleitete) Identitäten/Attribute, für gesicherte Überbrückungen in Zeit, Raum sowie Organisationsstrukturen und Rollenrelationen.
- eKolloquium – eID/eIDAS gesichertes Formularmanagement für (remote) Abschluss-Kolloquien (E-Prüfungsmanagement).

Das Hochschulkonto (Virtual Wallet) eProsecal stellt durch ein eIDAS/eID-basiertes Anmelde- und Konten-Verfahren hochsicher authentisierte Zugänge (LoA *high*) für verschiedene Hochschuldienste/-akteure in Prozessen bereit, auch schriftformersetzend. Dabei sind auch Prozesse mit multiplen Mehrnutzer-/Rollenbezügen (nm) abbildbar. Nutzer:innen haben über das Ihnen zugeordnete eProsecal-Basiskonto Zugriff auf die Daten aller freigegebenen Prozesse und können diese auch mit anderen Nutzer:innen und sogar schriftformersetzend mit Behörden sicher teilen (eID-basiertes eSharing).
Mit eNotar steht eine Plattform bereit, um Zeugnisse, Lernnachweise oder Dokumente (bzw. zugeordnete Digitale Kopien) digital beglaubigt per qualifizierter Signatur, rechts- und fälschungssicher und datenschutzkonform nur für eID-Berechtigte bereitstellen zu können (per eID/eIDAS & TrustServices). Dies bietet auch bei der Umstellung von Papierszenarien (z. B. Zeugnisse) in voll digitalisierte Szenarien deutliche Vorteile durch die gesicherte Verknüpfung beider Welten. Die Plattformen sind an das dezentrale EMREX-Netzwerk der EU angeschlossen und mit der zuständigen Behörde UNIT in Norwegen getestet. Das Verfahren ist föderal skalierbar für Schulen und Hochschulen (mit internen/externen eNotaren), samt gesichertem remote Hosting-Konzept für Stakeholder-interne eNotare (z. B. für Schulen mit reduzierten IT-Ressourcen). In 2022 wurde das Verfahren zur Beglaubigung von Abiturzeugnissen mit dem Gymnasium Martineum Halberstadt produktiv verwendet.

Per YourCredentials wird das eNotar-Prinzip auf die Beglaubigung von Relationen abgeleiteter Identitäten samt Attributen und Relationen (z. B. Ausweiswechsel, Eltern-Kind-Attribute, Übergang von initialen externen Low-Level-Authentifikationen zu späteren eAT/eID für EU-

externe Nutzer:innen/Bewerber:innen) hinsichtlich deren Vertrauensdomänen bzw. für domänenübergreifende Workflow-Erweiterungen fortentwickelt.

Vorgenannte Applikationen und Infrastrukturen wurden/werden übertragen auf Sicherung von Industrie 4.0-Netzwerken z. B. für Zugangskontrollen, mit weiteren Sicherheitsdiensten/Security by Design/Management im CyberSecurity-Verbund Sachsen-Anhalt.[35] Die eID/eIDAS-Lösungen sind hinsichtlich Integrationen und Migrationen sowohl für hybride Identitäten (mit vorhandenen Legacy-Identitäten) als auch für Migratioen via Post-eID-Ansätzen (eID-Authentifikation nachträglich zu vorhandenen Legacy-ID-Auth., wie derzeit) oder Präe-ID-Ansätzen (erstmalige Authentifikation per eID, mit nachträglicher Legacy-ID-Anbindung, wie bei vollem OZG-Konten-Rollout) vorbereitet.

3.3.3.2 StudIES+ [36]- Grenzüberschreitende digitale Studierenden-Mobilität in Europa

Eines der Ziele des 1999 gestarteten Bologna-Prozesses bestand in der Verbesserung der studentischen Mobilität innerhalb und zwischen den Ländern nicht nur der Europäischen Union, sondern des gesamten Europäischen Hochschulraums, unterstützt durch die europäischen Programme Erasmus/Erasmus+ zum Studierendenaustausch (unter Anrechnung von erworbenen ECTS-Punkten für Studienleistungen entsprechend European Credit Transfer System (ECTS)). Weitere Beschlüsse zur Verbesserung der Studierendenmobilität in der EU wurden ausgehend vom EU-Gipfel in Göteborg 2017 gefasst, u. A. durch die Einführung einer grenzüberschreitenden elektronischen Identifikation und Authentifizierung für Studierende - EU Student eCard (European Campus Card Association 2020) - auf Basis aktueller EU-Regelungen und -Standards (z. B. der eIDAS-Verordnung der EU für elektronische Identitäten und signaturbasierte Trust Services (eID & TS)) bis 2025.
Bisher sind in der Praxis mitunter aufwändige und langwierige Prozesse notwendig, da Studienleistungen und andere Dokumente beglaubigt, in Papierform verschickt (teilweise auch übersetzt) und schließlich geprüft werden müssen. In einem EU-weiten Wettbewerb waren der Berliner Digitalisierungsdienstleister Francotyp-Postalia Holding AG, die Bundesdruckerei, die auf digitale Formulare spezialisierte Sixform GmbH sowie die Freie Universität Berlin und die Hochschule Harz mit dem gemeinsamen Antrag zum nunmehr EU-CEF-geförderten Projekt

[35] siehe https://cslsa.de
[36] siehe https://studies-plus.eu/

StudIES+ erfolgreich, um neue Anwendungen für die digitale studentische Mobilität zu entwickeln. Finanziert wird das Projekt aus Mitteln des EU-Programms Connecting Europe Facility (CEF) Telecom, mit dem Anwendungen zur Verbesserung der grenzüberschreitenden Interaktion zwischen öffentlichen Verwaltungen, Unternehmen und Bürger:innen der EU auf Basis der eIDAS-Verordnung der EU gefördert werden sollen.

Eine bei Projektstart StudIES+ aufgenommene detaillierte Analyse der Datenaustauschprozesse zwischen deutschen und ausländischen Hochschulen ergab, dass die angestrebte Verbesserung der internationalen Mobilität insbesondere durch neue digitale Anwendungen in drei Bereichen unterstützt werden kann: Bei hochschulübergreifenden Prozessen (wie etwa der Beglaubigung von Zeugnissen oder Praktikumsbescheinigungen mittels eID und digitalen Signaturen u. A. für Bewerbungsverfahren), bei studentischen Ausweisen (wie etwa der Zugangskarte für die Bücherei) und bei digitalen Signaturen (etwa unter Arbeits- oder Mietverträgen). Im Rahmen der fast zweijährigen Projektlaufzeit kollaborierten die StudIES+-Partner bei der Entwicklung einer ganzen Reihe von Anwendungen, mit denen Lücken in den drei genannten Bereichen geschlossen werden sollen – darunter dem Beglaubigungsdienst eNotar, der ECTS-, Noten- und Kursverwaltung eExamResults mit der mobilen Student eCard oder dem Job-Onboarding-Tool eJob. Die zentrale Projektaufgabe der Hochschule Harz bestand dabei darin, eine sichere Plattform für den Austausch von Dokumenten (ePROSECAL) sowie den bereits erwähnten digitalen Beglaubigungsdienst (eNotar) zusammen mit weiteren eIDAS-basierten Hochschulanwendungen (wie eInternship zur Praktikumsverwaltung, eTestate zur gesicherten Prüfungs- und Labor-Anmeldung, eTOR zum gesicherten Austausch von Prüfungsergebnissen) zu entwerfen, prototypisch zu entwickeln und zu testen. Im Zusammenspiel gestatten die Anwendungen heute den Austausch elektronischer Dokumente zwischen Hochschulen sowie zwischen Hochschulen und Studierenden (sowie auch Praktikumsbetrieben im Fall eInternship) in einer sicheren und rechtsverbindlichen Form unter Verwendung von auf eIDAS basierenden Vertrauensdiensten. Kooperiert wurde im Rahmen der Entwicklungsarbeit unter anderem mit der mit der Stiftung für Hochschulzulassung in Dortmund (SfH), die bundesweit wie auch grenzüberschreitend für die Zulassung in NC-beschränkten Studiengängen zuständig ist sowie mit dem niederländischen Dienst Uitvoering Onderwijs (DUO), dem u. A. die zentrale Verwaltung von Studierendendaten in den Niederlanden obliegt.

Weiter wurde die eNOTAR-Plattform erfolgreich an das dezentrale EMREX-Netzwerk in der EU angeschlossen und mit der zuständigen Behörde UNIT in Norwegen getestet, wobei EMREX

den jeweiligen Absolventen erlaubt eigene Zeugnisse und Bildungsnachweise von der herausgebenden Stelle in eIDAS-gesicherter Form zu weiteren Institutionen zu transferieren (z. B. für Bewerbungen).

Neben der Programmierung und dem Test der Anwendungen konnten im Rahmen des Projekts auch unmittelbare Verbesserungen für die Studierenden der beiden beteiligten Hochschulen eingeführt werden. So wurde etwa im Mai 2019 auf dem Campus der Hochschule Harz in Wernigerode das erste eIDAS-fähige EU-Bürger-Terminal an einer Hochschule in Sachsen-Anhalt von StudIES+-Projektleiter H. Strack und SiXFORM-Geschäftsführer R. Phillipeit in Betrieb genommen. Hier können deutsche wie internationale Studierende eID-basierte Dienstangebote aus dem Bereich Verwaltung und Wirtschaft wahrnehmen, wie unter anderem einen De-Mail-Account für die rechtsverbindliche Kommunikation per E-Mail freischalten, ihren *Punktestand* in Flensburg abfragen oder ein polizeiliches Führungszeugnis – etwa für einen studentischen Nebenjob – anfordern.

Das Projekt konnte zum Jahresende 2019 erfolgreich abgeschlossen werden, ein positiver grenzüberschreitender Online-Test der EU mit eIDAS-Testeinrichtungen aus Estland, Italien und Österreich erfolgt im Januar 2020. Die Projektergebnisse wurden auf zahlreichen internationalen Tagungen wie etwa der ISSE 2019 in Brüssel, der OID 2019 in Garmisch-Partenkirchen oder der EUNIS 2019 in Trondheim vorgestellt, sowie auf dem Wirtschaftsschutztag 2019 des Landes Sachsen-Anhalt oder der CeBit 2018 präsentiert, sowie in den laufenden Prozess zur Umsetzung des Online-Zugangsgesetzes (OZG) in Deutschland eingebracht (Federführung im OZG-Bereich Bildungswesen bundesweit durch Land Sachsen-Anhalt) und in mehreren wissenschaftlichen Veröffentlichungen publiziert. Nach einem Vorschlag von H. Strack bereits im Jahre 2007 zur Einführung von E-Government-Standards im Hochschul- und Bildungswesen präsentiert auf der EUNIS 2007 in Grenoble[37] (unter Weiterentwicklung von XÖV per XUni/XStudy), reiht sich das Projekt StudIES+-Projekt mit den Umsetzungen von eIDAS-Regelungen und Standards im Hochschulwesen ein in eine Folge mit aufeinander aufbauenden Projekten wie TREATS zur Anbindung von Deutschland an das europäische eIDAS-eID-Netzwerk (Förderung EU-CEF und Land Sachsen-Anhalt) sowie eCampus (Förderung EFRE und Land Sachsen-Anhalt), jeweils mit der der Hochschule Harz mit Projektleiter Prof. Strack als Partner. Einen guten Überblick über die im Rahmen von StudIES+ entwickelten Anwendungen und ihre

[37] siehe https://netlab.hs-harz.de/research/Eunis2007_fullpaper_StraKa_OSCI_eBologna_v2___205_v009_13aaa.pdf

Vorteile für Hochschulen wie auch für individuelle Studierende bietet die Webseite des Projektkonsortiums[38].

Die Finanzierung des Projekts StudIES+ an der Hochschule Harz erfolgte anteilig über das Programm *Connecting Europe Facility (CEF) 2014-2020 TELECOM Call 2017* der Europäischen Union (EU) sowie über Mittel des Landes Sachsen-Anhalt.

3.3.4 Kurzübersicht eIDAS-basierte Zeugnis-Beglaubigung und –Validierung

Vor dem Hintergrund der aktuellen OZG-Thematik und insbesondere der Diskussionen und OZG Digitalisierungslabore zum Thema Zeugnisse sollen hier Möglichkeiten und Lösungsansätze aufgezeigt werden, welche auf langjährig erforschten, erprobten und bewährten Technologien auf Basis von Standards aufsetzen (vgl. BSI TR, SOGIS EU, eIDAS, ETSI, zusätzlich gibt es hierzu Komponenten/Produkte mit Sicherheitsevaluierungen/ Zertifizierungen (z. B. nach Common Criteria[39], BSI).

Im Rahmen dieses Papiers wird eine auf PKI-Technologien basierende, insbesondere eIDAS-basierende, Lösung zur digitalen Zeugnisbeglaubigung mit Delegation und Validierung vorgestellt. Diese Lösung ist nach derzeitigem Kenntnisstand mit den derzeit in Bund und Ländern gültigen Gesetzlichkeiten vereinbar und erfordert keine Gesetzesänderungen. Die Lösung stützt sich dabei insbesondere auf §3 a VwVfG und VwVfG § 33 (6)-(7) (auch Schriftformersatz). Der vorgestellte Ansatz ist dabei dokumentenorientiert.

Die Zeugnisdokumente selbst werden mit Hilfe einer qualifizierten elektronischen Signatur beglaubigt (mit Schriftformersatz, siehe Vertrauensdienstegesetz, in Nachfolge zum Signaturgesetz). Dabei spielt es keine Rolle, ob es sich um einfache PDF-Dateien, hybride Formate mit eingebetteten maschinenlesbaren Informationen oder sonstige eGovernment-Datei-Formate handelt. Dieser Vorgang ist wie oben beschrieben durch folgende Passagen aus dem Verwaltungsverfahrensgesetz § 33 (6) - (7) gestattet:

[38] siehe https://studies-plus.eu/

[39] siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheiskriterien/CommonCriteria/commoncriteria_node.html

Die nach Absatz 4 hergestellten Dokumente stehen, sofern sie beglaubigt sind, beglaubigten Abschriften gleich.

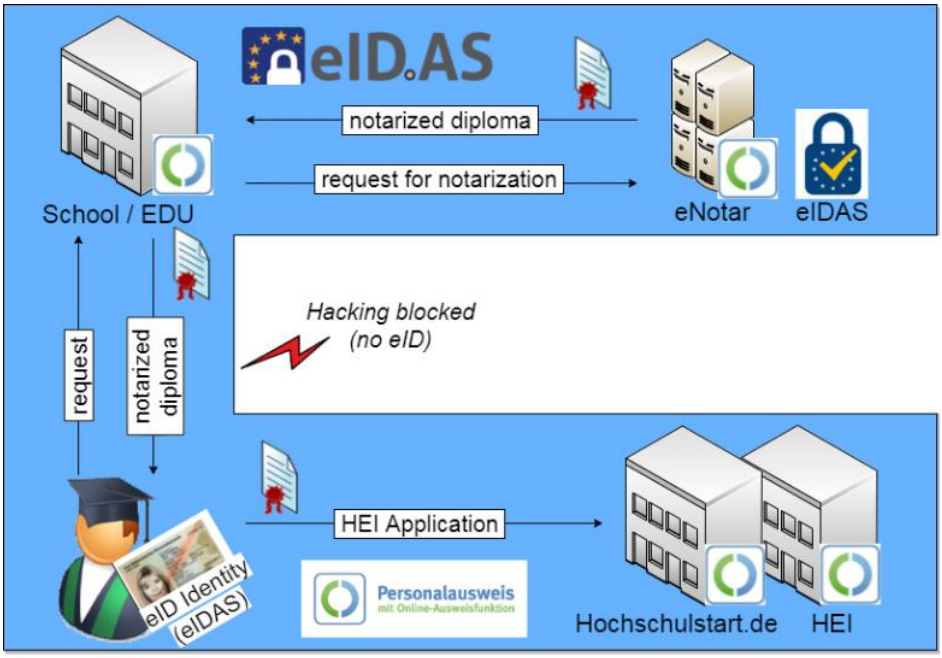

Abb. 4: eNotar-Beglaubigungen per eIDAS TS/QeS, mit eID-Zugangssicherungen

(6) *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.*

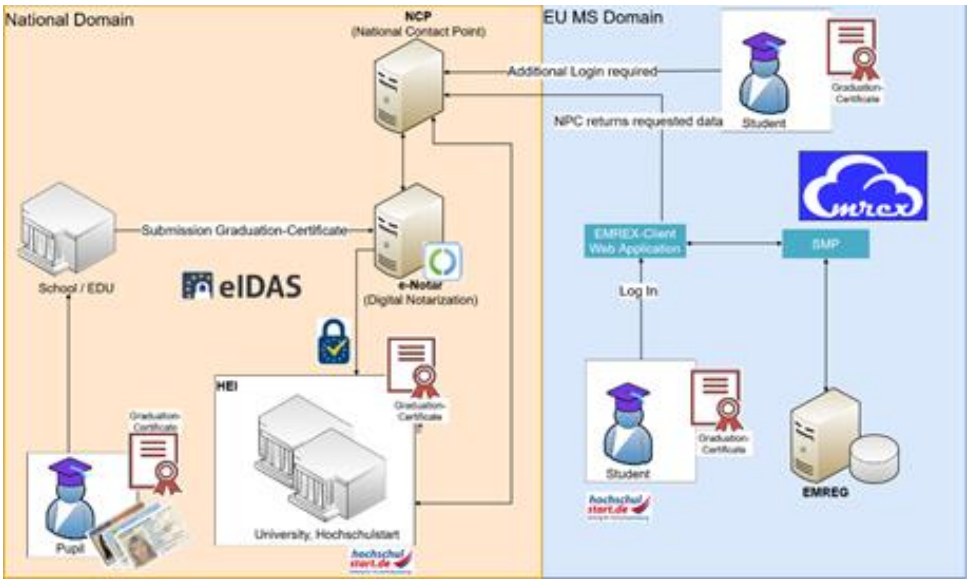

Abb. 5: eNotar-Beglaubigung Schulen/Hochschulen, mit eID/eIDAS/OZG/EMREX-Zugang

Die vorgestellte Lösung ist in der Beantragung rein Zeugnisinhaber:in-orientiert und somit durch Einholung seiner Genehmigung EU-DSGVO konform. Eine Validierung der beglaubigten Zeugniskopien ist rein software-basiert über erprobte, schon vorhandene PKI-Infrastrukturen möglich. Zudem erfolgt die Weitergabe der beglaubigten Zeugniskopien, nur zwischen per eID hoch authentisierten Nutzer:innen und verschlüsselt. Somit ist ein weitreichender Schutz der persönlichen Daten gewährleistet.

Die Lösung unterstützt virtuelle Wallets (eProsecal) und ist vorbereitet für die zukünftige Anbindung physischer Wallets. Bzgl. der Langzeitspeicherung/-sicherung sei verwiesen auf etablierte Standards siehe TR-ESOR des BSI[40]/eIDAS-Preservation Services (Sicherheit, Standardisierung, Effizienz). Der Personalausweis mit eID online Ausweisfunktion hat bereits SSI-Features (Self-sovereign Identity) siehe BSI[41], ohne Blockchain-Erfordernisse.

Die Lösung ist dem Sicherheitsniveau *hoch* zu zuordnen (gemäß LOA Level Struktur nach eIDAS-EU). Dem Nutzer wird dabei explizit das Niveau LOA *hoch* vermittelt, in Abgrenzung zu alternativen Angeboten. Die Lösung ist vorbereitet für die Verwendung mit verschiedenen Formatstandards (EU), wie ELMO/EMREX oder EDCI/Europass vgl. Abbildung 5 (XHochschule bzw. xBildung in Vorbereitung), inklusive der Einbindung von OZG-Nutzer:innenkonto OSI LSA bzw. Nutzer:innenkonto-Bund. Weiter wurde das Verfahren in den KOLIBRI[42]-Prototypen zur Nationalen Bildungsplattform (BMBF) integriert.

3.3.5 Architektur und Implementierung

Der vereinfachte Ablauf für die Anfrage und Auslieferung eines beglaubigten elektronischen Zeugnisses ist in Abbildung 6 dargestellt. Die Architektur sieht dabei ein Nutzer:innenkonto vor, welches als eigenständiges Konto (z. B. OZG-Nutzer:innenkonto) oder auch als Bestandteil eines eNotar-Portals ausgeführt sein kann. Im Anwendungsfall für Schulen, ist für die Anfrage ein Nutzer:innenkonto beim eNotar-Portal vorgesehen. Beim eNotar selbst handelt es sich wiederum um einen Service, der über das Nutzer:innenkonto verwendet werden kann und die eigentliche Verarbeitung der Zeugnisse durchführt.

[40] siehe https://www.bsi.bund.de/DE/Themen/Oeffentliche-Verwaltung/Moderner-Staat/Beweiserhaltende-Langzeitspeicherung-TR-ESOR/beweiserhaltende-langzeitspeicherung-tr-esor_node.html

[41] siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.html

[42] siehe KOLIBRI-Konsortium: Bechtle (Lead), Dataport, Univention, HS Harz (assoz.: MLU, OVGU, HIS, u. A.): Abschlussbericht, BMBF 2022.

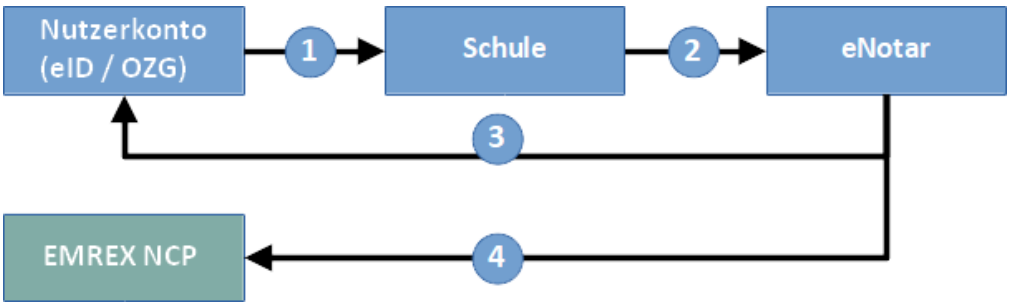

Abb. 6: Modellablauf im eNotar-Prozesswesen

Um den Vorgang zu starten, muss sich der Zeugnisinhaber zunächst mit seinem Personalausweis/eID am eNotar-Portal/Nutzer:innenkonto anmelden (auch mobil). Das Nutzer:innenkonto ermöglicht nach der Anmeldung die Beantragung (Schritt 1 in Abb. 6) dabei schriftformersetzend, einer beglaubigten elektronischen Zeugniskopie, welche dank der qualifizierten elektronischen Signatur sowohl rechtlich, als auch technisch auf dem aktuellen Stand der Forschung und Technik sicher ist, entsprechend dem eIDAS-TS-Kryptomanagement (vgl. BSI TR-02102[43] „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ und SOGIS[44] EU). Nachdem die beglaubigte Zeugniskopie beantragt ist, erhält die entsprechende Bildungseinrichtung eine Mitteilung, per Rolle Beglaubigungsbeauftragter/eNotar. Dieser meldet sich mit dem Personalausweis am eNotar-Portal per Schulkonto der Bildungseinrichtung an und überprüft dann die eingereichten Daten, lädt die Zeugniskopie und den Beglaubigungsvermerk hoch (Schritt 2 in Abb. 6). In der Rolle als eNotar wird die Zeugniskopie mit einer qualifizierten elektronischen Signatur zur Beglaubigung versehen. Mit dieser Signatur sind über bestehende PKI-Infrastrukturen (eIDAS-TS) die Echtheit und der Schutz vor Manipulation sichergestellt. Der Zeugnisinhaber erhält abschließend eine Benachrichtigung über den abgeschlossenen Vorgang und kann die beantragte beglaubigte Zeugniskopie herunterladen (Schritt 3 in Abb. 6).

Darüber hinaus können die beglaubigten Zeugniskopien vom Inhaber per EMREX im europäischen Bildungsraum bei weiteren Parteien eingereicht werden (Schritt 4 in Abb. 6). Auf diese Weise können beglaubigte Zeugniskopien direkt an z. B. Unternehmen, Schulen, Hochschulen

[43] siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

[44] siehe https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf

oder weitere Institutionen für Bewerbungszwecke geleitet werden. Diesen stehen beglaubigte Zeugniskopien so innerhalb kürzester Zeit zur Verfügung. Die Echtheit der beglaubigten Zeugniskopie kann dank der qualifizierten elektronischen Signatur mit im Internet erreichbaren Validierungs-Services jederzeit überprüft und sichergestellt werden.
Neben dem oben beschriebenen Ablauf, bei dem die Rolle des Beglaubigungsbeauftragten und die Rolle des eNotar von der gleichen Person übernehmen wird, kann dies auch durch zwei Personen/Rollen getrennt erfolgen.

3.3.6 Voraussetzungen

Da das Verfahren als Service im Wesentlichen von einem Provider ÖV - wie Dataport oder Hochschule Harz - bereitgestellt und über einen Web-Browser aufgerufen wird, sind die technischen Anforderungen für die Benutzer gering. Es wird lediglich ein Kartenleser oder ein Smartphone und die kostenfreie AusweisApp2[45] benötigt, um die Authentifizierung mittels des Personalausweises zu ermöglichen.

3.3.6.1 Hinweise zum Rollout

Die elektronische Beglaubigung von Zeugnissen ist als Ergänzung auf gesetzlicher Grundlage des § 33 VwVfG zu einer papierbasierten Zeugnisbeglaubigung zu sehen, bietet aber gerade auch in Corona-Zeiten den Vorteil sowohl den Beglaubigungsablauf (bei Schulen), als auch die Einreichung der Beglaubigung (durch Absolvent:innen) z. B. bei Hochschulen oder Unternehmen rein elektronisch in gesicherter und rechtskonformer Weise auf Basis von Standards zu ermöglichen. Per gesichertem Hosting bei eIDAS-Ressourcenträgern/RZ ÖV können Schulen auch ohne eigene eIDAS-Ressourcen die eNotar-Funktionen selber remote wahrnehmen.

3.3.6.2 Ausblick

Die Beglaubigung mittels eNotar ist nicht auf Schulzeugnisse beschränkt, sondern können auch auf andere Anwendungsszenarien sowohl im Bildungsbereich[46] als auch in der allgemei-

[45] siehe https://www.ausweisapp.bund.de

[46] siehe https://ozg.sachsen-anhalt.de/fileadmin/Bibliothek/Politik_und_Verwaltung/MF/OZG/Bilder/Themenfeld_Bildung/eIDAS_basierte_Beglaubigung_und_Validierung_von_Bildungsnachweisen.pdf

nen Verwaltung ÖV für die elektronische Beglaubigung von Dokumenten genutzt werden. Neben eNotar stehen bereits weitere prototypische eID/eIDAS/OZG-Anwendungen insbesondere für den Bildungsbereich bereit:

- eProsecal – Hochschulkonto mit eIDAS/eID & TS (u. A. QES, Siegel, ...) sowie eID-Shares
- eInternship – Praktikumsverwaltung/-verträge zwischen Hochschule und Unternehmen
- eTor/eTestate – Anmeldung/Teilnahme-Verwaltung für Prüfungen und Laborpraktik
- eKolloquium – Abbildung des Kolloquiumsprozesses (zur mündlichen Verteidigung der Abschlussarbeit)
- eHiWi – Anmeldung/Verwaltung von studentischen Mitarbeitern
- Your/MyCredentials – abgeleitete Identitäten und Beglaubigungen
- Integration für Prototypen Nationale Bildungsplattform (BMBF) - KOLIBRI.

Dabei stellt eProsecal ein eIDAS/eID-basiertes Anmelde- und Konten-Verfahren für hochsicher authentisierte Zugänge (LoA *high*) für verschiedene (Hochschul-)Dienste/-Akteure, auch schriftformersetzend bereit. Dabei sind auch Prozesse mit multiplen Mehrnutzer-/Rollenbezügen abbildbar. Nutzer:innen haben über das ihnen zugeordnete eProsecal-Basiskonto Zugriff auf die Daten aller freigegebenen Prozesse und können diese auch mit anderen Nutzern und sogar schriftformersetzend mit Behörden sicher teilen (eID-eSharing). eProsecal bietet hierdurch die Funktionalität einer Cloud-Wallet mit SSI-Features. (vgl. auch BSI Eckpunktepapier SSI[47] (siehe oben)).
Per YourCredentials wird das eNotar-Prinzip auf die Beglaubigung abgeleiteter Identitäten in Erweiterung von Vertrauensdomänen/Workflows fortentwickelt, dadurch ergibt sich eine Beglaubigung von Identitätsverknüpfungen. Neben der Verknüpfung der Identitäten einer Person, können hiermit auch Identitätsbeziehungen, wie z. B. zwischen Erziehungsberechtigten und ihren Kindern elektronisch beglaubigt umgesetzt werden.

<u>Weitere Optionen:</u>

Zur Vereinfachung kann im Beglaubigungsvermerk die Gültigkeitsdauer der Beglaubigung eingetragen werden, sodass die Nutzer:innen ohne technischen Mehraufwand die Gültigkeitsdauer direkt, ohne zusätzliche Tools, einsehen kann. Da diese technisch von der der Gültigkeit der Zertifikatskette abhängt, lässt sich die Gültigkeit aus dieser ableiten und im Dokument menschenlesbar eintragen.

[47] siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Eckpunkte_SSI_DLT.pdf

Ähnlich dem CRL-Ansatz können auch digital beglaubigte Zeugnisse widerrufen werden. In erweiterter Form könnten zusätzlich Zeugniskorrekturen eingetragen werden (Verzeichnisdienste). Mit weiteren Diensten kann eine Limitierung der Verwendung der Kopien für digitale Zeugnisse ermöglicht werden, andererseits ein unbefristete gesicherte Langzeitspeicherung umgesetzt werden (BSI TR-ESOR).
Zur Inhaberbezogenen Sicherung des Dokumenten-Flows (z. B. für beglaubigte Zeugniskopien) im Rahmen von eID/Authentisierungen für Portalzugänge und Dokumente können verschiedene Sicherheitsfunktionen genutzt werden – z. B. YourCredentials um das *Matching* verschiedener Identitäten einerseits für Portalzugang (Bewerbung/Immatrikulation) und andererseits der Inhaberidentität des Zeugniskopiedokuments vertrauenswürdig zu beglaubigen (ansonsten Fehlerrückgabe bei der Einreichung).
Um die unberechtigte Weitergabe von Zeugnissen oder Urkunden besser nachvollziehen zu können (Datenschutz), kann die Möglichkeit der Anbringung digitaler Wasserzeichen geschaffen werden. Diese Wasserzeichen erlauben grundsätzlich auch individualisierbare Kopien. Auf Wunsch können auch Statistik-Übersichten für Stakeholder integriert werden.

Die zuvor beschriebenen Implementierungen und Services wurden auch erfolgreich in den Prototypen der Nationale Bildungsplattform (BMBF) – Verbundprojekt KOLIBRI eingebracht[48].

Vorschläge für übergeordnete Regulierungen:

a) Einrichtung von Supportstellen für Hochschulen (ähnlich Nutzer:innenkontoBund-Support)
b) Nutzen der Post-eID- und Prä-eID-Ansätze aus StudIES+ für ID-Migrationen, z. B. für EU-externe Bewerber:innen mit Migrationen von externen ID zu eAT vor Ort
c) Ausbau von in OZG zurückgestellten BürgerSafes zur Sicherung langlebiger (signierter) Daten (mit eIDAS Preservation Services)
d) Vereinheitlichung von LoA-Zugangsleveln für Hochschulverfahren/Verpflichtung mit Fristen für Einführungen

[48] siehe Kurzbericht KOLIBRI: https://dropin.hs-harz.de/getlink/fiUXGRghC6Vwiwoj8YsqoHyj/Kurzbericht-KOLIBRI.pdf

e) Einrichtung von eIDAS-eID/TS-basierten Diensten für Sicherung/Notarisierung von Bildungsnachweisen/Zeugniskopien (vgl. eNotar HS Harz), Verzicht auf Blockchain-Verfahren mangels Standards sowie mangels nachgewiesenen Mehrwerten/Langzeit-Sicherungen sowie wg. verschiedener Sicherheitsprobleme, vgl. mehrere Stellungnahmen des BSI[49] sowie fehlende bzw. mangelnde Berücksichtigung entsprechender essentieller Sicherheitsfragen im White-Paper NDN[50] (u. A. bzgl. Sicherheitsstandards, Krypto-Agilität, Transparenz zu bekannten Schwachstellen und Angriffen, Langzeitsicherung, Effektivität), vgl. auch entsprechende News, wie Verabschiedung Digitalstrategie Bund September 2022[51] bzw. Anhörung im Bundestag zu Digitalen Identitäten Juli 2022[52] bzw. EU-Unterrichtung zu eIDAS2.0 im Bundesrat[53] Juli 2021

f) Notwendige Einführung für Schüler:innen/Abiturient:innen durch die Bundesagentur für Arbeit im Rahmen von Berufsberatungsmaßnahmen, insbesondere Einführung in eID, OZG in Nutzer:innenkonto und Handhabungen.

3.4 Umsetzungsvorschlag: Wallet Lösungen

Autor:innen: Knorr, Steffen; Pongratz, Hans; Teloo, Britta; Waßmann, Arn

Die digitale Identität im engeren Sinne ist fest mit einer Person verknüpft und kann diese durch ein Set von personenbezogenen Merkmalen identifizieren. So können mithilfe der in diesem Whitepaper beschriebenen Nutzer:innenkonto folglich Personen authentifiziert werden, aber für eine echte Validierung der von ihnen eingereichten bzw. auf eine Plattform hochgeladenen digitalen Nachweise fehlt die Verknüpfung der Person mit den jeweiligen Dokumenten. Es ist zwar bedingt ein Abgleich über die personenbezogenen Daten wie Name, Vorname(n), Geburtsdatum etc. möglich, dies unterliegt aber potentiell der Gefahr von Fehlern (z. B. bei Personen mit identischen Merkmalen oder wenn die Angabe der Vornamen auf dem Nachweis von den im Nutzer:innenkonto registrierten Vornamen abweicht), insbesondere wenn der Abgleich automatisiert erfolgen soll. Weiterhin bieten die Nutzer:innenkonto keine Tresorfunktion in der Form, dass Dokumente an zentralen oder auch dezentralen Orten gespeichert und von dort bei Bedarf wieder abgerufen werden können. Aus diesem Grund wird auch für das

[49] siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kryptografie/Blockchain/blockchain_node.html

[50] siehe http://netzwerkdigitalenachweise.de/static/doc/Whitepaper_digitales_Zeugnis_de.pdf

[51] siehe https://www.onlinezugangsgesetz.de/SharedDocs/kurzmeldungen/Webs/OZG/DE/2022/09_digitalstrategie.html

[52] siehe https://www.bundestag.de/dokumente/textarchiv/2022/kw27-pa-digitales-identitaeten-901172

[53] siehe https://www.bundesrat.de/SharedDocs/beratungsvorgaenge/2021/0501-0600/0598-21.html

Thema *Wallet Lösungen* im Sinne des angestrebten *visionären Ansatzes* in diesem Whitepaper ein Umsetzungsvorschlag erarbeitet, auch wenn das Wallet-Konzept kein *Allheilmittel* ist und bis Ende 2022 auch keinesfalls umsetzbar sein wird. Im Folgenden wird zunächst eine Begriffsdefinition gewagt und Beispiele verschiedener Wallets aufgeführt. Anschließend werden die eigentlichen Anforderungen beschrieben.

3.4.1 Begriffsdefinition Wallet und Anwendungsbeispiele

Der Begriff Wallet (Brieftasche) kam ursprünglich im Rahmen der Kryptowährungen auf. In diesem Zusammenhang mit diesem Anwendungsgebiet handelt sich um ein Programm (Software), in dem gespeichert wird, welche Schlüssel aus einer Blockchain einem gehören. Somit ist eine Wallet hier eher eine Art elektronischer Schlüsselbund. Natürlich gehören noch weitere Funktionen, wie bspw. der Transfer dieser Schlüssel zu anderen Wallets, dazu. Es gibt für dieses spezielle Anwendungsgebiet viele verschiedene Wallets, die sich mehr oder weniger unterscheiden.

Apple versteht unter einer Wallet hingegen etwas viel Allgemeineres. In der *Apple Wallet* (Apple Inc. 2022b) können verschiedenste virtuelle Objekte gespeichert werden. Dabei wird nur auf den mobilen Einsatz fokussiert. Anwendungsbeispiele sind hier ganz allgemein digitale Ausweise, Gutscheine oder Eintrittskarten (Apple Inc. 2022a). Auch die elektronische Bezahlfunktion spielt hier eine wichtige Rolle, wobei als Datentransferprotokoll NFC für das Auslesen der Daten eingesetzt wird (die NFC-Fähigkeit des Endgeräts wird damit vorausgesetzt).

Während der Corona-Pandemie sind die meisten Menschen mit digitalen Impfnachweisen in Berührung gekommen. Auch diese werden in einer Wallet gespeichert (CovPass, Corona-Warn-App). Es wird auch eine App zur Verifikation der Nachweise zur Verfügung gestellt (Robert Koch-Institut 2022).

Die Erasmus+ App kann einen digitalen Studierendenausweis auf Basis des European Student Identifiers (ESI) bereitstellen. Auch die EU arbeitet an einer Wallet-Lösung für einen Identitätsnachweis und zur Aufbewahrung von Dokumenten (Europäische Kommission 2022). Als ein weiteres Beispiel aus dem Bildungsbereich kann hier auch die in den Projekten BIRD/Digitaler Campus entwickelte Wallet erwähnt werden, die bereits erfolgreich getestet wurde (BMBF 2022).

3.4.2 Anforderungen und mögliche Aufgaben

Aktuell fehlt die Möglichkeit, auf technischer Ebene elektronische Dokumente (z. B. XML oder JSON) und digitale Dokumente (z. B. PDF oder JPEG) sicher und langfristig mit einer (digitalen) Identität zu verknüpfen. Die Umsetzung könnte mit einer eindeutigen technischen ID realisiert werden, die jede Person erhält. Dazu gibt es bereits verschiedene Initiativen auf EU-, Bundes- und Branchenebene. Technisch gesehen würde genau eine ID ausreichen, wenn diese allgemein und übergreifend genug gestaltet wäre und gleichzeitig der rechtliche Rahmen dies entsprechend ermöglichen würde. In der aktuellen Diskussion zeichnet sich aber ab, dass eine Person nicht die eine ID sondern eine Vielzahl von *Identifikatoren* erhält, die jeweils nur für spezifische Anwendungsfälle verwendet werden dürfen (siehe dazu Abschnitt 3.5). Somit muss die technische Verknüpfung (Verlinkung) dieser IDs bei der Person selbst geschehen oder in den jeweiligen Fachanwendungen. Nun kann die Person über ein Bündel von *Identifikatoren*, bPK2) aus einer vertrauenswürdigen Quelle (andere Verwaltung, Nutzer:innenkonto) verfügen, oder der Dienst erzeugt überhaupt erst eine ID (z.B. ESI), weil dies zu seinem Aufgabenspektrum gehört. Mit Ausgabe des Bescheids werden die bekannten und verifizierten, also vertrauenswürdigen IDs mit ausgegeben (XHEIE) und können als Nachweis an anderer Stelle in einem Folgeprozess wiederverwendet werden. Jetzt muss die Person ebenfalls wieder über eine vertrauensvolle Stelle diese ID nachweisen. In diesem Fall reicht ein simpler Vergleich der IDs und der Beweis, dass ein Dokument zu einer Identität gehört, ist erbracht. Jeder Bescheid / Nachweis kann eine Liste von IDs einer Person tragen. Wird also einer ID aus einem Nachweis vertraut und diese in Übereinstimmung mit einer Person gebracht, so könnte eine Hochschule in Betracht ziehen auch allen anderen, bisher noch unbekannten IDs, zu vertrauen und mit Einwilligung des Nutzenden in den hochschuleigenen ID-Speicher (im CaMS) zu überführen. Je mehr IDs eine Hochschule zu einer Person kennt, desto höher ist die Wahrscheinlichkeit, einen sicheren Treffer beim automatischen Abgleich zu landen.

Herausforderung bei dieser Vorgehensweise wäre die datenschutzkonforme Umsetzung, wonach die Daten der Nutzenden in diesem Umfang verarbeitet werden dürfen. Ohne weiteres gangbar wäre das bei einer entsprechenden gesetzlichen Rechtsgrundlage, die aber noch zu schaffen wäre. Ob das Gleiche auch aufgrund einer Einwilligung der Betroffenen gestaltbar wäre, müsste datenschutzrechtlich noch näher untersucht werden. Eine entsprechende Einwilligung für die Verarbeitung der Daten durch die Nutzenden ist umso wahrscheinlicher, die

höher die Vorteile der digitalen Vorgehenseiwese eingeschätzt werden. Alternativ müsste ansonsten wieder auf einen analogen Nachweis zurückgegriffen werden, was die Effizienz von Arbeitsabläufen erschwert.

Abb. 7 illustriert den Kreislauf von Dokumenten. Jeder Bescheid einer Hochschule kann, nach OZG-Terminologie, durch Verwendung zu einem Nachweis an einer anderen Hochschule werden.

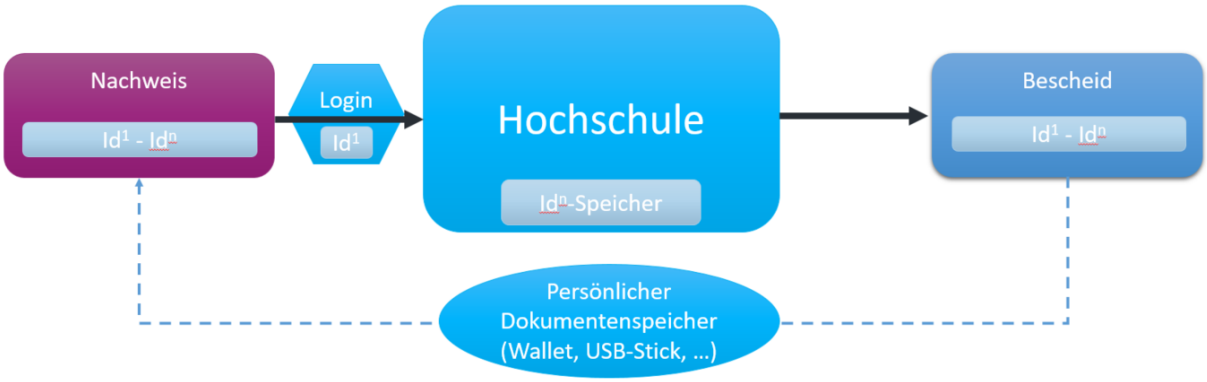

Abb. 7: Schematische Darstellung des Dokumentenkreislaufs

Das sichere und vertrauenswürdige Speichern und Ausgeben dieser Fülle an technischen IDs könnte eine Aufgabe auf Seiten der Nutzer:innen sein. Daneben können durch eine Wallet auch die Bescheide angenommen und als Nachweise ausgegeben werden. Die Herstellung der nötigen Vertrauenswürdigkeit ist dabei die große Herausforderung, insbesondere dann, wenn IDs und Dokumente nicht getrennt voneinander bzw. nicht an der gleichen Stelle liegen.

Wenn ein Bescheid bspw. als PDF-Datei vorliegt, dann dient das PDF selbst als Träger der Information, die beschieden werden soll. Trennt man die Präsentation vom Inhalt und stellt ein strukturiertes Format für die Informationen sicher (EMLO, XHEIE), dann kann auf die Präsentationsschicht auch verzichtet werden. Die Darstellung für die Nutzer:innen könnte dann auch von der Wallet selbst übernommen werden. In der Verarbeitungsinstanz, i. d. R. dem Fachverfahren, also hier das Campus Managementsystem, sollten die Daten übernommen werden um weiter verarbeitet zu werden und werden dann ohnehin in den eigenen Masken dargestellt (Strack et al. 2022b, 8 ff.).

In der Hochschulwelt ist das Bescheidwesen sehr heterogen. Die Hochschulen nehmen für die Individualisierung der Vorlagen teilweise hohe Investitionskosten in Anspruch. Beim Verzicht auf die Präsentationsschicht und bei der gleichzeitigen Nutzung eines Datenstandards würden Ressourcen freigesetzt werden.

Eine Wallet könnte die Nutzer:innen auch beim Thema Sicherheit unterstützen. Signaturen bzw. die Zertifikate, anhand derer die Signaturvalidierung erfolgt, sind nur eine begrenzte Zeitspanne über gültig. Die Wallet kann frühzeitig darauf hinweisen, dass ein Nachweis demnächst ungültig wird. So kann man sich frühzeitig um einen Ersatz bemühen. Sollte ein Bescheid von einer Hochschule widerrufen werden, so wird auch dies den Nutzer:innen in der Wallet transparent und die Wallet kann die Stellen, mit denen ein Nachweis geteilt wurde, ebenfalls informieren. Das könnte natürlich auch direkt mit einer Ersatzlieferung verbunden werden. Wenn die Wallet mit der AusweisApp2 verbunden ist, dann könnte es auch authentifizierte Personendaten tragen und weitergeben. Die AusweisApp2 liefert die Daten des nPA, des eAT oder der eID-Karte für EU-Bürger:innen. Im Beispiel einer postalischen Adresse handelt es sich beim nPA um die Meldeadresse der Person. Nun wird aber nicht immer die Meldeadresse benötigt, sondern auch die aktuelle Postanschrift, unter der die Person erreichbar ist. Auch diese Daten könnten hier, ggf. auch auf verschiedenen Vertrauensniveaus, vorliegen. Voraussetzung ist, dass die Wallet die Daten verifizieren authentifizieren kann. Gleiches gilt für weitere Daten, die für das Fachverfahren, also das CaMS, relevant bzw. wichtig sind, aber nicht aus einem Nutzer:innenkonto übertragen werden. Dazu zählen bspw. elektronische Adresse, Telefonnummern und das Geschlecht der Person. Auch hier sollte die Vertrauensstellung und das Vertrauen in die Daten berücksichtigt werden.

Die Wallet könnte die Nutzer:innen bei der Steuerung der Informationsflüsse unterstützen. Aus der bereits erwähnten Dokumentation der Freigaben bzw. der Aufstellung mit wem, wann und warum eine Information geteilt wurde, kann hervorgehen, wer die Daten aktuell verarbeitet. Die Zurverfügungstellung dieser Informationen könnte aber noch sehr viel gezielter, also selektiver, stattfinden. Das Fachverfahren fordert ein Datum bzw. ein Bündel von Daten für einen bestimmten Verarbeitungszweck und die Nutzer:innen selektieren aus dem Fundus der Nachweise gezielt einzelne Daten. Wenn bspw. aus einem Schulzeugnis nur die Abschlussnote und die Teilnote eines bestimmten Leistungskurses für die Durchführung des Verfahrens notwendig sind, müsste nicht das gesamte Zeugnis mit allen Teilnoten übertragen werden (Datensparsamkeit).

Nach § 9 OZG muss für die digitale Bekanntgabe eines Verwaltungsaktes der Bescheid zwangsläufig im Postfach eines Nutzer:innenkontos zugestellt werden. Die Anbindung einer Wallet an dieses Postfach über eine definierte Schnittstelle erscheint sinnvoll. Aktuell müsste die Datenübernahme händisch über das lokale Endgerät der Nutzenden erfolgen. Auch könnte die

Bekanntgabe nach § 41 VwVfG in eine Wallet erfolgen. Insgesamt wäre auch eine Harmonisierung dieser beiden Verfahren sehr sinnvoll und hilfreich.
Abschließend soll noch auf die Einbindung in die Bestrebungen rundum die Nationale Bildungsplattform hingewiesen werden. Die sich dort abzeichnende Vernetzung der verschiedenen Systeme kann als Transportweg für die Daten dienen. Eine Wallet wäre dann dort ein End- und ein Anfangspunkt.

3.4.3 Herausforderungen

3.4.3.1 Zuordnung von Nachweisen

Digitale und elektronische Dokumente können auf Integrität und Authentizität geprüft werden. Dafür stehen klassische Signierungsverfahren auf Basis von Zertifikaten zur Verfügung. Auch eine manuelle Verifikation ist bereits über das CaMS oder ein angebundenes Dokumentenmanagementsystem der Hochschule möglich. Was in keinem aktuell verwendeten Verfahren möglich ist, ist die eindeutige und gesicherte Verknüpfung zu einer Identität. So kann aktuell ein Dokument nach allen Prüfungen als echt bewertet werden, aber jemand anderem „gehören“, bspw. einer verwandten Person. Das gilt auch für elektronische Verfahren wie bspw. EMREX (EMREX network 2022), wenn der Account einer anderen Person zur Datenübertragung verwendet wird. Es bleibt nur die Überprüfung der typischen Personenmerkmale (Vor- und Nachname, Geburtsdatum und -ort, E-Mail-Adresse, etc.) die aber nicht in jedem Fall verfügbar sind und auch Änderungen unterliegen. Insbesondere wenn einigermaßen viel Zeit zwischen der Erzeugung und der Verwendung des Dokuments liegt, sind Änderungen wahrscheinlich. Daher kann eine solche Prüfung bestenfalls als Indiz für eine unpassende Verwendung gewertet werden, aber nicht als Beweis. Eine manuelle Intervention bspw. durch die Sachbearbeitung wird notwendig.

3.4.3.2 Aktualität

Authentisierte Personenstammdaten lassen sich mit einem hohen Vertrauensniveau aus einem Nutzer:innenkonto, wie bspw. dem NKB, übernehmen. Diesen ist entsprechend § 8 OZG auch zu vertrauen. Zudem ist das Verfahren eIDAS-konform und so in der Theorie auch von allen EU-Bürger:innen und EU-Ausländer:innen sowie von Personen mit elektronischem Auf-

enthaltstitel nutzbar. Dies dürfte für einen grundsätzlichen Identitätsnachweis, bspw. im Rahmen einer Online-Immatrikulation, völlig ausreichend sein. Bei den Daten handelt es sich um die gleichen Daten, die auch auf dem Personalausweis stehen. Allerdings bedeutet dies nicht, dass die Personendaten auch aktuell sind. Insbesondere die (postalische) Adresse muss nicht mehr stimmen; selbst mit gutem Willen ist es den Nutzer:innen nicht immer möglich, diese Daten aktuell zu halten. Für die Studierendenverwaltung und die Meldung an die amtliche Statistik werden aber die aktuelle Semesteranschrift bzw. relevante Adresse (Heimatanschrift) benötigt. Beide können von der Adresse, welche aktuell auf dem Personalausweis steht, abweichen. Zudem wird das Geschlecht der Person nicht geliefert; es wird auch nicht auf dem Personalausweis ausgewiesen. Alle Daten werden in Großbuchstaben geliefert, was u.U. nicht den Anforderungen des verarbeitenden Systems genügt.

3.4.3.3 Datenhoheit

Wem gehören eigentlich zu welchem Zeitpunkt welche Daten bzw. Dokumente? Wer kann und darf diese widerrufen? Diese Fragen werden häufig im Zusammenhang mit digitalen Identitäten aufgeworfen. Es besteht oftmals der Wunsch, dass eine Person (im Sinne von *Self-Sovereign Identity* bzw. *selbstbestimmter Identität*) umfassend über die Verwendung ihrer eigenen Daten bestimmen kann und somit auch bspw. im Rahmen eines Bewerbungsverfahrens (Studium, Karriere) Daten widerrufen, also zurückfordern kann. Gleiches gilt aber auch für eine ausstellende Stelle, die für eine Person bestimmte Daten/Dokumente widerrufen kann. Dies kann neben Täuschungsversuchen natürlich auch zum Zwecke der Fehlerkorrektur oder auch aus sonstigen Gründen erforderlich sein.

3.4.3.4 Akzeptanz

Die Digitalisierung der Verwaltungsprozesse schreitet im Rahmen der OZG-Umsetzung voran. Interessant ist an dieser Stelle auch zu erwähnen, dass das Postfach des NKB nur empfangen, aber nicht senden kann, siehe Abschnitt 2.2. Das heißt, wenn die Nutzer:innen eine Meldung bekommen und darauf antworten wollen, müssen sie ein anderes System verwenden (*Medienbruch*). Auch ist zu berücksichtigen, dass insbesondere junge Leute noch keine Erfahrung im Umgang mit einer öffentlichen Verwaltung haben. Der erste Kontakt mit der deutschen Behördenwelt erfolgt daher sehr wahrscheinlich im Rahmen einer Studienplatzbewerbung. Folglich sollte vermieden werden, dass durch zu komplizierte technische Verfahren oder sehr

knappe Handlungsfristen Nutzer:innen in das klassische analoge Verfahren gedrängt werden. Es gilt daher neben den technischen Austauschformaten (XHEIE) und Systemanbindungen (NKB, DoSV) auch die Prozesse digital neu zu denken. Auch könnten verschiedene Angebote in den gleichen Angelegenheiten zu Verwirrungen führen. Auf der anderen Seite kann gerade für IT-affine Personengruppen eine Auswahl verschiedener Zugangswege attraktiv sein. So erfolgt z. B. die Bekanntgabe des Verwaltungsaktes nach Verwaltungsverfahrensgesetz § 41 VwVfG in das private Mail-Postfach, nach § 9 OZG in das Postfach eines Nutzer:innenkontos, welches allerdings ggf. erst noch erstellt und auf das nötige Vertrauensniveau gehoben werden muss.

Insgesamt besteht die Gefahr, dass die beschriebene digitale Lösung aus Sicht der Nutzer:innen zunächst unbequemer ist. Daher sind flankierende Maßnahmen zur Attraktivitätssteigerung, insbesondere in der Anfangsphase, notwendig. Der Helpdesk der Hochschule muss den gesamten Prozess mit all seinen Systemen und Anwendungen im Blick haben.

3.4.4 Anforderungen an eine Wallet aus unterschiedlichen Nutzungsperspektiven

Um die Sinnhaftigkeit bzw. die Anforderungen an eine Wallet näher zu beleuchten, werden im folgenden unterschiedliche Perspektiven eingenommen. Hierbei wird die technische Perspektive zunächst vernachlässigt.

3.4.4.1 Bewerber:innensicht

Der gängige Anwendungsfall ist hier die LeiKa Leistung *Bewerbung an einer Hochschule*. Hierbei wird im ersten Schritt nur die dezentrale Bewerbung an der jeweiligen Hochschule betrachtet.

Bei der dezentralen Bewerbung wäre es in jedem Fall eine Erleichterung, wenn die Bewerbenden im ersten Schritt keinen neuen Account anlegen müssten, sondern sich direkt mit ihrem persönlichen Nutzer:innenkonto (Land oder Bund) anmelden könnten. Idealerweise liegt die Wallet innerhalb des Nutzer:innenkontos und stellt keinen losgelösten *Speicherort* dar. Durch die Anbindung an das Nutzer:innenkonto könnten Dokumente direkt aus der Wallet abgerufen und freigegeben werden. Sofern an der Hochschule eine Authentifizierung auf einem speziellen Vertrauensniveau erforderlich ist, wäre eine Verwaltung der digitalen Identität(en), beispielsweise der edu-ID als lebenslange, digitale Identität für Forschung und Bildung (DFN-Verein 2020, 12–14), über die Wallet ebenfalls wünschenswert.

Aus Sicht der Bewerber:innen ist aus Datenschutzgründen eine aktive Steuerung, welche Dokumente im Rahmen der Bewerbung zur Verfügung gestellt werden, von zentraler Bedeutung. Insbesondere wenn es um den Sachverhalt des Hochschulwechsels geht und im Sinne der Interoperabilität Dokumente zwischen den Behörden bzw. Hochschulen weitergegeben werden dürfen. D. h. hier sollte als Diskussionsansatz die Wallet als Lösung im Sinne der Nutzer:innen als Schnittstellen/Transportmedium fungieren, bei der alle Daten/Dokumente über die Nutzer:innen laufen.

Auch eine Unterteilung in einen *privaten* und in einen *öffentlichen* Bereich wäre praktisch, damit auch private Dokumente in der Wallet verwaltet werden können, die gar nicht unbedingt originär in Form eines Nachweises bei einer öffentlichen Stelle eingereicht werden müssen. Dies könnten auch studiengangsabhängige Nachweise sein, wie bspw. Erste-Hilfe-Kurse oder ein Kettensägenschein. Ein zusätzliches Feature könnte eine Übersicht sein, welche Dokumente bzw. Nachweise mit welchen Behörden geteilt wurden. Im Zuge dessen könnte auch eine Widerrufsmöglichkeit implementiert werden. Wie sich ein Widerruf aus der Ferne auf die Fachverfahren auswirken würden, müsste aber noch intensiv beleuchtet werden.

Natürlich muss eine Erreichbarkeit von allen Endgeräten, mobil und Desktop, möglich sein, damit flexibel auf die Wallet zugegriffen werden kann. Vorteilhaft wäre auch ein Datenaustausch zwischen Wallets, so dass auch direkt Daten von einer privaten Wallet in das der Behörden fließen kann und umgekehrt.

3.4.4.2 Studierendensicht

Die Aspekte, die bei der Bewerber:innensicht angeführt wurden, lassen sich auch auf die Studierendensicht übertragen. Allerdings rückt bei der Betrachtung der Authentifizierungsthematik das Thema *Hochschulkennung* bzw. Login für alle Anwendungen für diese Nutzer:innengruppe in den Fokus. Erste Prototypen von CaMS zeigen, wie sich die üblicherweise autarken Authentifizierungsmechanismen an einer Hochschule mit dem Bürgerkonto (Nutzer:innenkonto) verbinden lassen. Das CaMS kann hier die Rolle des Zugangstors nach außen spielen und den lokalen Account der Hochschule mit dem des Bürgerkontos verlinken. Selbstverständlich kann dies auch über einen Authentifizierungsserver der Hochschule erfolgen, sofern dieser für die Kommunikation mit dem Bürgerkonto ausgerüstet ist. Ergänzend dazu wäre eine automatische Übernahme der Dokumente zum Studienverlauf (Studienbescheinigungen, Leistungsübersichten, Exmatrikulationsbescheinigung, Abschlussdokumente etc.) in die Wallet

sehr praktisch. Auch hier sollte die Steuerung bzw. aktive Freischaltung der Funktion beim Studierenden liegen.

3.4.4.3 Hochschulsicht

Grundsätzlich wäre es aus Hochschulsicht ebenfalls wünschenswert, dass eine Authentifizierung initial erfolgt und auf das definierte Vertrauensniveau abgestimmt ist. Ein Zusammenhang, zwischen den aus der Wallet übermittelten Dokumenten und der einreichenden Person muss in jedem Fall hergestellt werden. Ist dies nicht möglich, so kann kein Automatismus in der Fallbearbeitung implementiert werden und die Sachbearbeitung muss jeden Nachweis händisch überprüfen. Eine nennenswerte Prozessbeschleunigung zu aktuellen bereits etablierten digitalen Hochschulverfahren kann sonst nicht erwartet werden. Auch die Integrität und Authentizität der Daten müssen jederzeit gewährleistet sein.
Letztlich könnte eine Wallet dann einen *Andockpunkt* für den Empfang und die Bereitstellung von digitalen Nachweisen sein. Das sind, wie in den vorherigen Abschnitten bereits angedeutet, z. B. Nachweise im Rahmen der Bewerbung und Einschreibung. Auch wenn die Hochschulzugangsberechtigung beim direkten Übergang von Schule zu Hochschule zwischen den Behörden digital übermittelt werden soll, ist dieser direkter Übergang in vielen Fällen nicht gegeben. Aus Hochschulsicht wäre es sinnvoll, alle Dokumente direkt in die Wallet zu übermitteln oder zumindest eine Schnittstelle zu entwickeln, die es den Nutzer:innen ermöglicht, Dokumente aktiv in die Wallet zu übernehmen. Die digitalen Dokumente sollten einem festgelegten Standard (XSchule, XHochschule) folgen, damit eine Weitergabe der Dokumente bzw. eine Weiterverarbeitung von Daten nahtlos möglich ist. Um weitere Anwendungsfälle abzudecken sollte hier auch ein europäischer Standard (EWP, ELMO) angestrebt werden, bspw. für Auslandsmobilitäten.
Auch aus Hochschulsicht muss es die Möglichkeit der Revokation geben. Ein falsch ausgestelltes Dokument, insbesondere wenn es offiziellen Charakter hat, muss sich in jedem Fall widerrufen lassen. Wichtig aus Sicht der Verwaltung ist zudem, dass sich der letztendlich vom Studierenden gewählte Ablageort transparent verhält. Das bedeutet, dass die Sachbearbeitung in ihren Abläufen keine Sonderbehandlungen oder Einschränkungen zu berücksichtigen hat. So bleibt bspw. das Führen der elektronischen Studierendenakte von dem gewünschten Speicherort des Studierenden unberührt.

3.5 Eindeutige elektronische ID

Autoren: Bacharach, Guido; Michels, Thorsten; Pirkovitsch, Armin; Rohrbacher, Boris; Wiedermann, Wolfgang

Das Thema dieses Kapitels ist nicht spezifisch für die Hochschulwelt. Da es einerseits ungelöst ist, andererseits aber in bestimmten Kontexten von grundlegender Bedeutung sein kann, wird es in dieses Whitepaper aufgenommen, auch um die Varianz der Möglichkeiten darzustellen, mit denen bei der Erarbeitung der Lösungen für das Themenfeld Bildung, Lebenslage Studium umgegangen werden muss.

Eine wesentliche Grundlage für digitale Verwaltungsabläufe - auch im Hochschulumfeld - ist die eindeutige Zuordnung einer Person zu einer elektronischen Identität. Als eine Lösung der erforderlichen Identifizierung von Personen für verschiedene Verwaltungsleistungen wird eine lebenslang eindeutige ID diskutiert, die überall verwendet werden kann und darf. Eine global eindeutige ID wird zum Beispiel bei der registerübergreifenden Zusammenarbeit bzw. beim Datenaustausch zwischen Servicekonten benötigt, insbesondere hinsichtlich der Umsetzung des Once-Only Prinzips im Rahmen des OZG Reifegrad 4 (BMI 2022d). Um auch über die gesamte Lebensdauer einer Person das Once-Only-Prinzip anwenden zu können, ist eine lebenslang eindeutige ID in der Diskussion. In diesem Kapitel werden zunächst verschiedene Ansätze für die eindeutige elektronische ID beschrieben.

In Deutschland existieren drei europaweit akzeptierte elektronische ID-Tokens[54] auf hohem Vertrauensniveau: Der *neue Personalausweis* mit Online-Ausweisfunktion, kurz nPA (BSI 2022), der elektronische Aufenthaltstitel[55] sowie die sog. eID-Karte für EU-Bürger:innen und Angehörige des Europäischen Wirtschaftsraums[56], die mit der mit Online-Ausweisfunktion letztlich alle auf demselben technischen System basieren, siehe hierzu auch Abschnitt 2.2.

Mit der Wahl des nPA ist das Problem der begrenzten Laufzeit nicht gelöst. Ein Personalausweis hat jeweils eine begrenzte Geltungsdauer, d. h. ein neuer Ausweis bedeutet zunächst auch eine neue elektronische Identität.

[54] siehe https://ec.europa.eu/digital-building-blocks/wikis/display/EIDCOMMUNITY/Overview+of+pre-notified+and+notified+eID+schemes+under+eIDAS

[55] siehe https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/elektronischer-aufenthaltstitel/elektronischer-aufenthaltstitel-node.html

[56] siehe https://www.personalausweisportal.de/Webs/PA/DE/buergerinnen-und-buerger/eID-karte-der-EU-und-des-EWR/eid-karte-der-eu-und-des-ewr-node.html

Ein ähnliches Problem betrifft die Erlangung eines hohen Vertrauensniveaus für ein OZG-Nutzer:innenkonto, bzw. den Übergang der Authentifizierung am OZG-Nutzer:innenkonto, wenn der nPA abgelaufen bzw. durch einen neuen nPA ersetzt worden ist. Wie kann das OZG-Nutzer:innenkonto auf den neuen nPA umgestellt werden, wenn der alte nicht mehr gültig ist? Eine zwischenzeitliche Verwendung eines Passworts oder sog. Sicherheitsfragen am Nutzer:innenkonto, um den neuen nPA zu registrieren, senkt das Niveau der Identifizierung. Dieses Problem entsteht insbesondere auch bei Namens- oder Geschlechtswechsel (siehe oben, Abschnitt 3.1.2.3).
Anhand des nPA werden dienstspezifische IDs generiert und ausschließlich diese für den jeweiligen Dienst verwendet. Dies hat den Vorteil, dass dienstübergreifendes *User Tracking* verhindert wird (Datenschutz).

Eine naheliegende Lösung des Problems ist eine lebenslang eindeutige ID. Die ID sollte über das gesamte Leben eindeutig bleiben, auch wenn man z. B. den Wohnsitz, Namen oder Geschlecht wechselt. Wenn man in ein anderes Bundesland umzieht und sich dort ein neues Nutzer:innenkonto des Landes erstellt, wird die alte ID zwar nicht ungültig, aber man erhält eine zweite ID.

Es gibt verschiedene Lösungsansätze für die genannten Probleme, die durch verschiedene Interessensgruppen vorangetrieben bzw. in die Diskussion eingebracht werden. Ein Lösungsansatz wird im Registermodernisierungs- sowie im Identifikationsnummerngesetz verfolgt: Hier wird eine elektronische ID über die lebenslang eindeutig vergebene Steueridentifikationsnummer erstellt. Allerdings werden auch hier für spezifische Anfragen spezifische IDs erstellt (siehe hierzu den nächsten Abschnitt), was datenschutzrechtlich zu begrüßen ist, jedoch den Austausch von Informationen zwischen den verantwortlichen Stellen im Sinne des Once-Only-Prinzips erschwert.

Wirtschaft und Politik drängen auf eine Wallet-basite Infrastruktur. Nachweise verbleiben als *Verifiable Credentials* (VC*)* bei den Nutzenden - abgelegt in einer digitalen Brieftasche/Wallet auf einem (mobilem) Endgerät - und werden bei Bedarf präsentiert. Hierbei besteht grundsätzlich die Möglichkeit, dass nur gewisse, aus einem VC abgeleitete Informationen übertragen werden. Damit wird die Umsetzung des Once-only-Prinzips auf die Bürger:innen übertragen und die Datenschutzdiskussion in diesem Bereich umgangen.

Die Europäische digitale Identität EU-ID ist ein Vorschlag der EU-Kommission, einen in allen Mitgliedsstaaten akzeptierten digitalen Nachweis über die eigene Person einzuführen (vgl. Klein 2021). Damit einher geht der EU-ID-Entwurf für die eIDAS-Ergänzung, Art. 11 a) 1.: „When notified electronic identification means and the European Digital Identity Wallets are used for authentication, Member States shall ensure unique identification."

Die Beachtung des Datenschutzes einerseits die Ermöglichung der Verbindung verschiedener Daten andererseits führen zu den folgenden Diskussionsansätzen.

3.5.1 Diskussionsansatz: Datenschutzkonforme eID

Eine feste ID pro Person birgt das Risiko, dass alle mit dieser ID getätigten Aktionen einfach einander zugeordnet werden können (VFR Verlag für Rechtsjournalismus 2022). Das NKB geht dabei den Weg, jedem Dienst bzw. Fachverfahren eine eigene bereichsspezifische Personenkennziffer, kurz bPK, auszuliefern (siehe oben, 2.2.3). Somit kann die ID nicht zwischen zwei Parteien verglichen werden. Dieser Ansatz erschwert aber dementsprechend den Austausch verifizierter Daten zwischen den Parteien, da die spezifische ID dafür nicht verwendet werden kann.

Im Gegensatz zu einer festen ID kann auch die Langlebigkeit der spezifischen ID ein Problem darstellen, da sie dauerhaft bei der Verifizierungsstelle vorgehalten werden muss und nicht geteilt werden soll. Bisherige Lösungen wie das NKB lösen dieses Problem einer lebenslangen ID nicht. Eine übergeordnete Stelle, die Identitätsabfragen zum bereichsübergreifenden Datenaustausch (z. B. über anfragespezifische bPKs) koordiniert, wäre eine mögliche Lösung.

Vor dem Hintergrund, dass wir uns in einem geschlossenen System befinden (es dürfen nur öffentliche Verwaltungen am Nutzer:innenkonto teilnehmen), könnte aber auch folgender Ansatz diskutiert werden: Allen Beteiligten darf unterstellt werden, dass sie sich gegenseitig vertrauen (können) und die Daten nicht außerhalb des Systems bekanntgemacht werden. Sollte innerhalb des Systems dann nicht die Verwendung einer einheitlichen ID möglich sein, um die übergreifende Umsetzung der Prozesse innerhalb des Systems zu ermöglichen? Hierfür gibt es bislang aber keine technische Lösung. Eine weitere Option wäre es, den Nutzer:innen zu ermöglichen, bestimmte bPKs bei Bedarf zusammenzuführen bzw. miteinander zu verknüpfen.

3.5.2 Diskussionsansatz: Lebenslang eindeutige Kette von IDs statt lebenslange eindeutige ID

Wie bereits dargestellt wird es in Deutschland aufgrund der DSGVO, aber vor allem auch aus historischen Gründen schwierig werden, gesetzlich eine lebenslange eindeutige zentral administrierte ID zu etablieren. Diese Schwierigkeit besteht in vielen anderen Ländern innerhalb und außerhalb Europas nicht. Wie aber vorstehend bereits ausgeführt, existieren in Deutschland schon einige durchaus vielversprechende Ansätze, die aber immer nur eine eindeutige ID für eine spezielle Lebenssituation oder gar Aktivität (z. B. im Sinne eines Antragsprozesses) liefern. Könnte man hier für eine (entsprechend rechtlich gesicherte) Anschlussfähigkeit dieser unterschiedlichen IDs sorgen, wäre es möglich, so zumindest für bestimmte Prozesse und Aktivitäten durch eine Kettenbildung dieser IDs temporär für eine situative eindeutige ID zu gewährleisten.

Ein weiterer Punkt, den es zu beachten gäbe, wäre die Anschlussfähigkeit dieser Glieder einer ID-Kette zu europäischen Lösungen wie der oben erwähnten EU-ID. Eine solche Übertragbarkeit im Sinne einer gewissen Kompatibilität müsste zumindest bei den Übergängen der jeweiligen ID-Kettengliedern gegeben sein, was zu prüfen wäre. Es sind Herausforderungen bezüglich des gesetzlichen Rahmens zu erwarten.

3.6 Interoperabilität als Grundvoraussetzung

Autoren: Bacharach, Guido; Pongratz, Hans; Waßmann, Arn; Wiedermann, Wolfgang

3.6.1 Stufen der Interoperabilität

Interoperabilität bedeutet, dass Systeme, Techniken oder Organisationen nahtlos zusammenspielen können. Dabei kann auch von einer gewissen Heterogenität ausgegangen werden mit dem Hauptziel, die verschiedenen Systeme in Interaktion zu bringen. Damit diese Interaktion funktioniert, sind verabredete Regeln/Normen notwendig, an die sich alle beteiligten Akteure halten. Interoperabilität kann in der IT auf verschiedenen Stufen erreicht werden (vgl. Sinsel 2020):

1. Strukturelle Interoperabilität (Konnektivität): Bezeichnet die Fähigkeit, Nutzdaten von einem zum anderen System zu übertragen.

2. Syntaktische Interoperabilität: Bezeichnet die Fähigkeit, einzelne (semantisch bewertbare) Informationseinheiten und Datenstrukturen in den übertragenen Nutzdaten zu identifizieren und zum Zwecke einer weiteren Verarbeitung zu extrahieren.

3. Semantische Interoperabilität: Bezeichnet die Fähigkeit, die extrahierten Informationseinheiten semantisch korrekt zu interpretieren.

4. Organisatorische Interoperabilität: Bezeichnet die Fähigkeit, interagierende Prozesse effektiv und effizient zu organisieren.

Die erste Stufe wird im Allgemeinen als technische Interoperabilität verstanden (vgl. van der Veer und Wiles 2008). Im Rahmen der Umsetzungsbemühungen des OZG wurde vom Bundesministerium des Innern und für Heimat ein Servicestandard veröffentlicht (vgl. BMI 2022a). Das Prinzip 16, eingruppiert in den Abschnitt *Technischer Betrieb*, zielt dabei auf die Herstellung von Interoperabilität ab. In der Präambel heißt es dort: „Die Interoperabilität von Komponenten wird durch gemeinsame Standards, definierte Schnittstellen und kompatible Architekturen gewährleistet“ (BMI 2022c). Insbesondere wird unterstrichen, dass durch Interoperabilität sinngemäß auch erreicht werden soll, dass kein einzelnes Unternehmen eine Monopolstellung erreichen kann. Es wird somit noch eine wirtschaftliche Perspektive angeführt. Auch die Bundes-Arbeitsgemeinschaft der Kommunalen IT-Dienstleister e. V (Vitako) hat schon, u. a. aus diesem Grund, zu Beginn der OZG-Umsetzung auf die Notwendigkeit von Interoperabilität hingewiesen und sich gegen Zentralisierung ausgesprochen (vgl. Vitako 2022). Die weitere Konzentration liegt auf technischen Aspekten: Daten, Schnittstellen und Datenübertragung. Interoperabilität wird, so der Eindruck, vorwiegend aus rein technischer Sicht (Systeme müssen Daten austauschen können) und wirtschaftlicher Betrachtung (Investitionsschutz, Erhalt der Heterogenität) gefordert – ergänzt von rechtlicher Interoperabilität. Dies kann so auch in den Bemühungen der XHEIE-Standardisierung durch die Init AG im Auftrag des Landes Sachsen-Anhalts beobachtet werden.
Nun soll das OZG aber auch benutzerorientiert umgesetzt werden. Dem widerspricht das Auslassen der Betrachtung der prozessualen (organisatorischen) Interoperabilität. Aus Sicht der

Nutzer:innen ist es vielleicht sogar wünschenswert, dass Daten (idealerweise mit Einwilligung und im Auftrag der Nutzer:innen) übertragen werden. Wenn jedoch die Prozesse nicht abgestimmt sind, so wird meistens doch eher unklar bleiben, welche Daten genau eigentlich gebraucht werden – Stichwort Datensparsamkeit. Auch wird es weiterhin notwendig sein, den Nutzer:innen erklären zu müssen, wann sie für welche Prozessschritte welches System mit welchen Daten zu nutzen haben. Hier wird die Nutzer:innenfreundlichkeit der digitalen Lösungen umso schwerer zu erreichen sein, desto komplexer sich ein Prozess darstellt. So mag die Antragsstellung eines *Anwohnerparkausweises* noch recht simpel und unproblematisch sein; im Gegenzug dazu gestaltet sich der Prozess der *Immatrikulation* mit dem vorgelagerten *Zulassungsverfahren* und den damit verbundenen Hilfsanträgen als sehr viel komplizierter. Hier müssen eine Vielzahl von Systemen (CaMS, DoSV, NKB, IDM der Hochschule, Abrechnung, Chipkartensystem usw.) für einen nahtlosen Datenfluss ineinandergreifen, ohne dass es je zu einer prozessualen Standardisierung gekommen ist. Die Nutzer:innenzentrierung ist spätestens hier verloren gegangen. Die XHEIE-Datenmodelle sind sehr allgemein gehalten und nicht an Anwendungszwecken ausgerichtet. Bei vielen Nachweisen, die im Prozess benötigt werden, ist keine echte Digitalisierung zu erwarten. Wenn die verschiedenen Hersteller nicht in Eigeninitiative agieren, besteht die Gefahr, dass zwar eine technisch funktionierende, aber kaum nutzbare Lösung entsteht. Die Akzeptanz durch die Nutzer:innen wäre dann gefährdet und möglicherweise würde unverhältnismäßig oft auf die analogen Prozesse, die im Sinne der Nutzenden erhalten bleiben müssen, zurückgegriffen – weitere Synergieeffekte durch die Digitalisierung blieben dann aus.

3.6.2 Schaffung neuer Standards

Beim Blick auf den Aspekt der technischen Standardisierung kann festgestellt werden, dass (gerne) neue Datenmodelle entwickelt werden. Bestehende und ggf. etablierte Konzepte werden zwar gesichtet, aber oft weder genutzt noch weiterentwickelt. Der Fokus richtet sich auch vor allem auf Deutschland, und die EU / Welt wird dabei vernachlässigt. Als Beispiel kann XHEIE und XSchule angeführt werden. Hier entstehen, auch abweichend von den ursprünglichen Ambitionen, neue und nationale Standards. Es entsteht ein Effekt, den XKCD humoristisch, aber treffend in der Abb. 8 dargestellt hat: Es entstehen immer weitere Standards für die gleiche Sache.

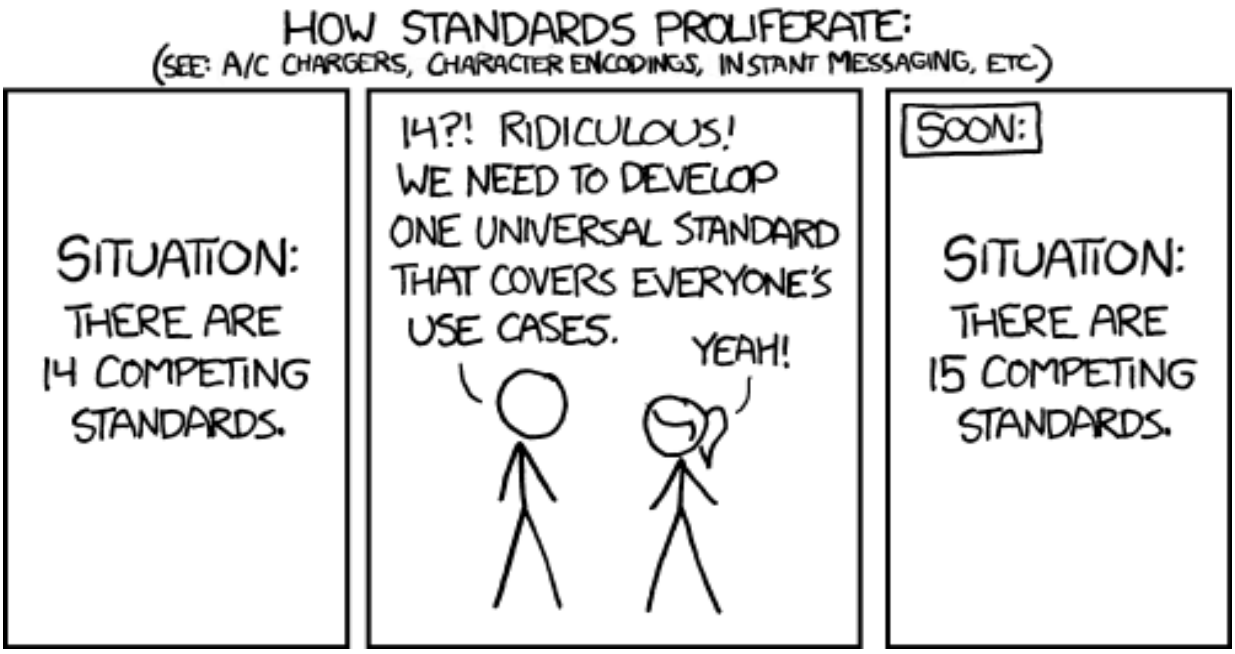

Abb. 8: Datenstandards als Grundlage der technischen Interoperabilität (xkcd 2022)

3.6.3 Empfehlungen für die weitere OZG-Umsetzung

Ausgehend von oben beschriebenen Herausforderungen wird dringend empfohlen, im Hochschulumfeld die vierte Stufe der *Organisatorischen Interoperabilität* anzustreben und zu fördern, insbesondere mit direkter Einbeziehung der Softwarehersteller. Basierend auf den Leika könnten Anwendungsfälle und Prozesse beschrieben werden, die interoperabel umgesetzt werden. Im Zentrum des Ganzen stehen die Nutzer:innen mit ihren digitalen Identitäten, die über ihre Einwilligungen die Datenflüsse steuern. Der *Ist-Zustand* der Interoperabilität elektronischer Identitäten ist aktuell in Deutschland und Europa wie folgt:

- Elektronische Identitäten werden an der Hochschule zentral/dezentral, aber hauptsächlich anwendungsfallbezogen (siehe Kapitel 3.1) verwaltet.

- Dabei gibt es sehr unterschiedliche existierende Ansätze wie:
    - eID, lokaler ESI, fremde ESI, Person-ID auf Basis der Steuer-ID (bald), NKB-bPK2, NKB-Postkorb-Handle, ORCID, lokale Matrikelnummer, KV-Versichertennummer, Bewerber-ID (BID), lokale Bewerbernummer, lokale PersonId, eduGAIN, etc.

    - OIDC-Accounts (z.B. Social Login wie Microsoft, Google, AppleId, ...), etc.

- In diesen Fällen wird je nach Anwendungsfall und Funktion jeweils eine andere ID verwendet.

- Das Projekt XHEIE führt aktuell eine Liste von allen möglichen Identifikatoren (xbd:Identifikationsnummer).

Ein wünschenswerter *Soll-Zustand* ist, wie in den obigen Kapiteln für das Thema *Interoperabilität* schon allgemein beschrieben, wäre:

- die Wiederverwendung von Identifikatoren zum sicheren identifizieren einer Person und

- das Übereinbringen von Dokumenten/Daten zu einer Person.

Das Thema *Interoperabilität von elektronischer Identifizierung* wird auch im Kapitel 3.5 behandelt.

3.7 Datenschutzrechtliche Betrachtung

Autor:innen: Pasek, Gregor; Teloo, Britta

In diesem Kapitel werden neben allgemeinen datenschutzrechtlichen Fragestellungen, die sich im Rahmen der Umsetzung des OZG und dem E-Government-Gesetz ergeben[57], auch spezielle Anwendungsgebiete beleuchtet und dazu Handlungsempfehlungen erarbeitet. Hierbei fokussiert man sich auf die Kernaspekte der Diskussion.

3.7.1 Datenschutz in Bezug auf Onlinezugangs- und E-Governmentgesetz

Einen guten Einblick in das Themenfeld gibt beispielsweise ein Podcast „Das Onlinezugangsgesetz OZG und der Datenschutz“ vom 26. Oktober 2021 mit dem bayerischen Landesbeauftragten für den Datenschutz, Herrn Prof. Dr. Thomas Petri, dessen vollständiger Inhalt online abrufbar ist (vgl. DS Praxis: Der Podcast 2021). Prof. Petri identifizierte insbesondere folgende datenschutzrechtliche Herausforderungen im Kontext OZG: Zweckbindung, zentrale Datenspeicherung und -verwaltung, Dauerprotokollierung, Verantwortlichkeiten oder Transparenz.

[57] siehe auch Handreichungen des BMI: https://leitfaden.ozg-umsetzung.de/display/OZG/Arbeitshilfen?preview=/12583387/49315865/210115_Datenschrechtliche%20Einordnung.pdf

Als Lösungsansätze nannte er etwa ein Datenschutzcockpit oder einen bestimmten Freigabeprozess, damit Bürger jederzeit die Kontrolle über Ihre persönlichen Daten behalten.
Grundsätzlich lässt sich also festhalten, dass das OZG mit den Servicegedanken des Once-Only-Prinzips und der Nutzerorientierung zwar dem Bürger:innen zu Gute handelt, aber das dadurch nicht die Grundsätze der Datenschutz-Grundverordnung sowie des IT-Grundschutzes gemäß Bundesamt für Sicherheit in der Informationstechnik außer Acht gelassen werden dürfen (Haak und Winter 2022). Zu den wichtigsten Aspekten folgt ein kurzer Überblick.

Die DSGVO definiert verschiedene allgemeine Grundsätze. Dabei sollte erwähnt werden, dass die DSGVO zwar noch durch weitere Gesetze wie das Bundesdatenschutzgesetz oder die Landesdatenschutzgesetze (deren Anwendungsbereich auf die Verarbeitung personenbezogener Daten durch öffentliche Stellen beschränkt ist) weiter konkretisiert wird, was aber nichts an der grundsätzlichen Anwendbarkeit der DSGVO bzw. ihrer Allgemeingültigkeit ändert.

- Grundsätze für die Verarbeitung personenbezogener Daten - Art. 5 DSGVO:

- Rechtmäßigkeit - Für die Verarbeitung der personenbezogenen Daten muss eine Einwilligung oder eine anderweitige Rechtsgrundlage vorliegen.

- Treu und Glauben - Für die Person, deren Daten verarbeitet werden, darf durch die Verarbeitung keine *unerwartete Verarbeitung* stattfinden. Dies ist z. B. bei der heimlichen Verarbeitung von personenbezogenen Daten oder einer Zweckentfremdung (Sicherheitsaufzeichnungen werden für Leistungskontrolle genutzt) der Fall.

- Transparenz - Alle Informationen zur Verarbeitung müssen leicht zugänglich, verständlich und in einfacher klarer Sprache der betroffenen Person zur Verfügung gestellt werden.

- Zweckbindung - Der Zweck zu dem die personenbezogenen Daten verarbeitet werden muss eindeutig sein. Wird in § 9 der Datenschutzgrundordnung NRW noch einmal explizit inkl. der Problemstellung von Herrn Prof. Petri behandelt.

- Datenminimierung - Die personenbezogenen Daten die erhoben/verarbeitet werden müssen auf das für den Zweck der Verarbeitung notwendige Maß beschränkt werden.

- Richtigkeit - Die personenbezogenen Daten müssen richtig sein und der Verantwortliche i. S. d. Art. 4 Abs. 7 DSGVO muss angemessene Maßnahmen ergreifen, damit diese richtig sind/bleiben.

- Speicherbegrenzung - Es muss sichergestellt werden, dass die Daten nicht länger als erforderlich gespeichert werden. Hierfür müssen Löschfristen sowie eine regelmäßige Prüfung (inhaltliche Richtigkeit und Durchführung der Löschung) erfolgen.

- Integrität - Die Daten müssen unverfälscht sein.

- Vertraulichkeit - Es muss sichergestellt werden, dass nur berechtigte Personen die personenbezogenen Daten einsehen können.

- Rechenschaftspflicht - Der Verantwortliche nach Art. 4 Abs. 7 DSGVO muss die Einhaltung der datenschutzrechtlichen Regelungen nachweisen können.

1. Rechtmäßigkeit der Verarbeitung personenbezogener Daten - Art.6 DSGVO

Im Datenschutz gilt das Prinzip des *Verbots mit Erlaubnisvorbehalt* d. h. grds. ist die Verarbeitung von personenbezogenen Daten verboten. Eine Verarbeitung von personenbezogenen Daten wird lediglich legitimiert, sofern gesetzliche Regelungen (z. B. i.S.d. Art. 6 DSGVO) oder eine explizite Einwilligung (u. A. auch in Art. 6 DSGVO genannt) vorliegen.

Bedingungen für die Einwilligung - Art. 7 DSGVO

- Eine Einwilligung ist jederzeit widerrufbar.
- Das Ersuchen um Einwilligung hat in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen. Sie muss sich klar von anderen Sachverhalten abgrenzen.
- Die Einwilligung muss freiwillig zu erfolgen. Insbesondere muss klar sein, dass die die Einwilligung sich auf Daten bezieht, die für die Erfüllung eines Vertrages nicht notwendig sind.

Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft - Art. 8 DSGVO

- Als Kind gilt, wer das 16. Lebensjahr noch nicht vollendet hat. Das Alter kann von den Mitgliedsstaaten auf das 13. Lebensjahr heruntergesetzt werden.
- Unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen, muss überprüft werden, dass die Einwilligung tatsächlich dem Wunsch des Kindes entspricht.

Verarbeitung besonderer Kategorien personenbezogener Daten - Art. 9 DSGVO

- Das Recht, diese Daten zu verarbeiten wird noch stärker eingeschränkt.
- Bei diesen Daten handelt es sich um Daten, aufgrund derer eine Diskriminierung wahrscheinlich ist, wie z. B. Weltanschauung, ethnische Zugehörigkeit, Gewerkschaftszugehörigkeit, aber auch biometrische Gesundheitsdaten oder genetische Daten. Diese werden in § 9 DSGVO abschließend definiert.

Verarbeitung von personenbezogenen Daten über strafrechtliche Verfolgung - Art. 10 DSGVO

- Darf nur unter behördlicher Aufsicht vorgenommen werden.
- Oder durch ein Gesetz der Mitgliedsstaaten delegiert werden, dass entsprechende Garantien vorsieht.
- Strafregister dürfen nur unter behördlicher Aufsicht geführt werden.

Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist - Art. 11 DSGVO

- Ist die Identifizierung einer Person nicht mehr notwendig, ist es zur Einhaltung dieser Verordnung nicht notwendig Daten weiter aufzubewahren, einzuholen oder zu verarbeiten, um die betroffene Person zu identifizieren.
- Ist der Verantwortliche nicht in der Lage eine Person zu identifizieren, unterrichtet er sie wenn möglich hierüber.

- In diesen Fällen finden die Artikel 15 bis 20 keine Anwendung, es sei denn, die betroffene Person stellt zur Ausübung ihrer in diesen Artikeln niedergelegten Rechte zusätzliche Informationen bereit, die ihre Identifizierung ermöglichen.

Recht auf Datenübertragbarkeit - Art. 20 DSGVO

- Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten.
- Sie hat das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln, sofern eine entsprechende Einwilligung vorliegt und der Austausch automatisiert erfolgt.
- Werden von der verarbeitenden Stelle Aufgaben, die im öffentlichen Interesse liegen oder in Ausübung öffentlicher Gewalt erfolgen Daten übermittelt, gilt Artikel 17 DSGVO nicht.

Die Grundsätze des IT-Grundschutzes können in drei Schritten erreicht werden, die in einem Leitfaden des BSI gut zusammengefasst werden (BSI 2017, 14 ff.):
Schritt 1: Initiierung des Sicherheitsprozesses

- Verantwortung übernehmen/ der Informationssicherheitsbeauftragte als zentrale Rolle
- Geltungsbereich
- Sicherheitsziele festlegen und Leitlinie erstellen

Schritt 2: Organisation des Sicherheitsprozesses

- Aufbau einer Organisation zur Informationssicherheit
- Integration in bestehende Abläufe und Prozesse
- Konzeption und Planung des Sicherheitsprozesses

Schritt 3: Durchführung des Sicherheitsprozesses

- Auswahl und Priorisierung der Bausteine

- IT-Grundschutz-Check
- Umsetzung der Sicherheitskonzeption

Um die Grundsätze greifbarer zu machen, stellen die nächsten Abschnitte einen konkreten Bezug zu den Anforderungen im Rahmen des OZG Reifegradmodells[58] her und brechen diese Anforderungen auf die einzelnen OZG Leistungen sowie die technischen Grundlagen herunter.

3.7.2 Konkretisierung von Anwendungsfällen gemäß OZG

3.7.2.1 Betrachtung auf Basis des „OZG-Reifegradchecks“

Bei der Umsetzung der OZG Leistungen gilt als Maßgabe das Reifegradmodell mit insgesamt zehn Kriterien. Im ersten Schritt muss bis Ende 2022 der Reifegrad 3 erreicht werden, letztlich aber dann auch der Reifegrad 4 mit den Grundgedanken des *Once-Only-Prinzips* und der *Interoperabilität* umgesetzt werden. Bei genauerem Blick in die einzelnen Fragestellungendes „OZG-Reifegradchecks“ (vgl. BMI 2021a) fallen Aspekte ins Auge, die von besonderer datenschutzrechtlicher Relevanz sind. Im Folgenden werden daher zunächst die einzelnen Kriterien beurteilt.

Kriterium 1: Leistungsbeschreibung	
1	Existiert eine mit der Bundesredaktion und dem Fachressort abgestimmte Leistungsbeschreibung gemäß FIM?
2	Sind Informationen zur Beantragung der Leistung auf Ihrer Website vorhanden?

Die Leistungsbeschreibung beinhaltet in der Regel allgemeingültige Informationen zum Prozess, den die jeweilige OZG Leistung repräsentiert.

[58] Im Rahmen der Umsetzung des OZG ist die Frage zu klären, welchen Digitalisierungsgrad eine Verwaltungsleistung erreichen muss, um die Vorgaben des OZG zu erfüllen. Auf Basis eines Modells der Europäischen Kommission zur Messung der Online-Verfügbarkeit von Verwaltungsleistungen wurde daher ein Reifegradmodell entwickelt. Damit lässt sich der digitale Entwicklungsstand einzelner Leistungen bewerten. Das Reifegradmodell gibt die einheitliche Auffassung der Ressorts wieder und soll den Behörden als verlässliche Grundlage bei der Bewertung der OZG-Konformität ihrer bestehenden und geplanten Online-Verwaltungsleistungen dienen. Das Modell (vgl. BMI 2021a) misst die Online-Verfügbarkeit auf einer Skala von 0 (die Leistung ist nur offline verfügbar) bis 4 (die Leistung kann vollständig digital abgewickelt werden).

Allerdings kann die Hochschule, je nach Konzept *Anbindung an den Portalverbund bzw. Verwaltungssuchmaschine*, ihre Leistungen bzw. Leistungsbeschreibungen noch um Informationen anreichern, die den Prozess der Hochschule betreffen. Dazu können auch Informationen zur zuständigen Stelle und den Kontaktpersonen zählen. Wenn hier personenbezogenen Daten weitergegeben werden, gilt es hochschulintern entsprechende Einwilligungen einzuholen, insofern nicht andere Rechtsgrundlagen dies erlauben, wie z. B. § 27 Mutterschutzgesetz. Da diese Entscheidung aber von jeder Hochschule autark getroffen und entsprechend gesteuert werden kann, wird dieser Aspekt nicht weiter behandelt.

Kriterium 2: Antragsprozesse und Kontextintegration	
1	Kann die Beantragung der Leistung vollständig online erfolgen?
2	Erfolgt bei Leistungen ohne Antragspflicht die Leistungsgewährung automatisch (bei Vorliegen der Voraussetzungen)
3	Können Stammdaten und andere bereits eingegebene Daten der Nutzer:innen mit Einwilligung aus anderen Bereichen des Portalverbundes und aus verwandten oder bereits gestellten Anträgen übernommen werden?
4	Ist ein Antragsformular online verfügbar?

Im Rahmen des *Kriteriums 2*, *den Antragsprozessen und der Kontextintegration*, ergeben sich zu den gelb eingefärbten Punkten datenschutzrechtliche Fragestellungen, die besondere Sensibilität erfordern. Wenn die Beantragung online erfolgt, sollte neben der entsprechenden Datenschutzinformation passend zum Antrag bzw. dahinterliegenden Prozess, die datenschutzrechtliche Einwilligung als Teil des Antrages abgebildet werden. Da die Einwilligung nach Artikel 7 DSGVO verbunden mit dem Recht auf Löschen auch widerrufen werden kann, muss die Hochschule hier entsprechende Voraussetzungen schaffen (Widerrufs- und Löschmanagement). Ebenso muss das Auskunftsrecht der betroffenen Person (Art. 15 DSGVO) von Beginn an mitgedacht werden, damit ein etwaiges Auskunftsersuchen fristgerecht und transparent beantwortet werden kann.

Insbesondere der Aspekt Übernahme von Stammdaten, der in Richtung Interoperabilität geht, muss technisch und auch datenschutzrechtlich gelöst und abgesichert werden. Auch hier steht die Einwilligung der antragsstellenden Person im Mittelpunkt und die Rechte auf Löschung und Auskunft müssen übergreifend gedacht und realisiert werden.

Kriterium 3: Nutzer:innenkonto (falls relevant)	
1	Ist das Angebot eines Nutzer:innenkontos aus Nutzerperspektive sinnvoll?
2	Ist bereits ein Nutzer:innenkonto vorhanden?
3	Handelt es sich um ein Nutzer:innenkonto innerhalb des Portalverbundes?

Die Möglichkeit, dass sich Interessent:innen oder Bewerbende ein Nutzer:innenkonto anlegen, ist nicht neu und wird von den Hochschulen datenschutzkonform umgesetzt. Aber im Falle des OZG ist es der Gedanke, dass sich die Bürger:innen idealerweise einmalig ein Konto anlegen und sich mit diesem einen Konto bei allen Behörden registrieren können. Entscheidend ist also auch hier wieder, Transparenz darüber zu schaffen, welche Daten im Rahmen dessen übertragen werden. Gleichzeitig stellt sich aus Bürger:innensicht vermutlich die Frage, ob und von wem protokolliert wird, bei welchen Behörden sie sich mit dem Nutzer:innenkonto registriert haben. Ebenso ist hier der Sicherheitsaspekt im Kontext *Missbrauch von Nutzer.innendaten* von großer Relevanz und entsprechende BSI Standards sind umzusetzen.

Kriterium 4: Authentifizierung (falls erforderlich)	
1	Ist eine Authentifizierung des Nutzers erforderlich?
2	Ist eine Authentifizierung auf dem erforderlichen Vertrauensniveau online möglich?

Je nach Verwaltungsleistung und gefordertem Vertrauensniveau sind andere Nachweise erforderlich. Grundsätzlich kann die Hochschule selber definieren, ob für eine bestimmte Ver-

waltungsleistung eine Authentifizierung erforderlich ist und im Zuge dessen auch das erforderliche Vertrauensniveau. Hilfreich wäre eine bundesweite Entscheidung, ob jede Hochschule das Thema Authentifizierung dezentral lösen muss oder ob rechtzeitig eine zentrale Lösung über den Portalverbund geschaffen wird. Fakt ist, dass im Falle einer erforderlichen Authentifizierung diese auch auf entsprechendem Niveau möglich sein muss, um Reifegrad 3 zu erfüllen (und dies bis Ende 2022).

Kriterium 5: Bezahlprozess (falls erforderlich)	
1	Ist eine Bezahlkomponente erforderlich?
2	Ist eine Bezahlung von im Vorfeld zu entrichtenden Gebühren online möglich?

Aktuell erfolgen nach wie vor Abstimmungen, wie sich ein länderübergreifender Bezahldienst für Hochschulen realisieren lässt. In NRW könnte *ePayBL* hier eine Lösung sein, da der Dienst dort auf Landesebene (außerhalb des Hochschulbereichs) bereits genutzt wird. Die Fragen des Betriebs und der Organisation stellen dabei eine große Herausforderung dar. Definitiv müssen bei der Einbindung einer solchen Komponente die datenschutz- und sicherheitstechnischen Aspekte im Vordergrund stehen. Im Sinne des Datenschutzes muss zudem geklärt werden, ob im Zusammenspiel mit *ePayBL* ein Auftragsverarbeitungsvertrag inkl. technischer und organisatorischer Maßnahmen geschlossen werden muss.

Kriterium 6: Nachweise (falls erforderlich)	
1	Müssen im Rahmen der Antragstellung Nachweise in Form von Dokumenten beigefügt werden?
2	Können Dokumente digital beigefügt werden?
3	Können alle für die Abwicklung erforderlichen Dokumente digital beigefügt werden?
4	Können Dokumente, die der Verwaltung bereits vorliegen, auch direkt aus den Quellsystemen abgerufen werden?

Beim Thema digitale Nachweise sind wieder die bereits genannten Grundsätze der DSGVO zu beachten. Die Transparenz und die Betroffenenrechte müssen gewahrt werden und ein Abruf oder die Weitergabe von Dokumenten (auch im Sinne der Interoperabilität) erfolgt nicht ohne Einwilligung der Bürger: innen bzw. ohne eine andere wirksame Rechtsgrundlage.
Unter Umständen leiden hierunter gegebenenfalls der Servicegedanke und die Bedienungsfreundlichkeit, wenn solche zusätzlichen Einwilligungen und Informationen in den Prozess eingebunden werden müssen.

Kriterium 7: Nutzererfahrung und Konformität	
1	Berücksichtigt das Online-Antragsverfahren die Anforderungen gemäß Barrierefreie-Informationstechnik-Verordnung (BITV 2.0), Usability ISO 9241-110:2006 und den BSI-Standard 200-2 (IT-Grundschutz)?
2	Ist der Antrag zusätzlich auf Basis von Nutzertests unter Einbeziehung der Endanwender digital umgesetzt worden und ist die Nutzbarkeit auf mobilen Endgeräten sichergestellt und optimiert?

Hinsichtlich des *Kriteriums 7* ist der Aspekt IT-Grundschutz auch im Kontext *Datenschutz* relevant. Da dieser an Hochschulen grundsätzlich eingehalten werden muss, stellt es in diesem Sinne keine neue Anforderung dar. Bei der Implementierung neuer Services, wie zum Beispiel einer Bezahlkomponente oder einem Authentifizierungsverfahren, müssen die Aspekte von Beginn an mit betrachtet werden.

Kriterium 8: Kommunikation	
1	Ist eine Kommunikation zwischen Antragstellenden und Sachbearbeitenden per E-Mail (ggf. verschlüsselt) möglich?
2	Kann die Kommunikation innerhalb der Fachanwendung (auf der Website/ dem Fachportal) erfolgen?

Die Kommunikation, insbesondere, wenn sie außerhalb des Hochschulnetzwerkes stattfindet, ist ebenso relevant im Kontext *IT-Sicherheit*. Unter Punkt 3.7.2.3 wird erläutert, was bei der E-Mail-Kommunikation zu beachten ist.

Kriterium 9: Bescheid (falls erforderlich)	
1	Wird im Rahmen der Antragsabwicklung ein Bescheid erstellt?
2	Wird dem Nutzer ermöglicht, den Bescheid rechtsverbindlich digital abzurufen?

Sofern ein Bescheid notwendig ist, sollte dieser im geschützten Bereich des jeweiligen Hochschulportals zur Verfügung gestellt werden, wo zum Abruf eine Authentifizierung mit einem Nutzer:innenkonto erforderlich ist.

Kriterium 10: Portalintegration	
1	Ist das Online-Antragsverfahren in einem Portal des Portalverbundes, beispielsweise dem Bundesportal integriert?
2	Erfolgt die Integration über einen Link oder über einer Oberflächenintegration?

Die technische Anbindung an ein Landesportal, welches sich dann im übergreifenden Portalverbund wiederfindet, wird in NRW mittels einer Verwaltungssuchmaschine (VSM) als zentraler „Datendrehscheibe“ realisiert. Die Anbindung an die VSM kann auf drei unterschiedlichen Wegen erfolgen, beispielsweise kann eine Anbindung an die VSM per RDFa Tags[59] auf der eigenen Website erfolgen. Wenn hier nur leistungsbezogene, beschreibende Inhalte übermittelt werden, ist der Datenschutzaspekt zu vernachlässigen. Werden auch Kontaktpersonen übermittelt, gilt hier entsprechend der Hinweis zu *Kriterium 1*. Weitere Informationen zu den Anbindungsmöglichkeiten finden sich im Handbuch zur Teilnahme am Portalverbund NRW (vgl. d-NRW 2020).

[59] RDFa-Tags enthalten den LeiKa-Schlüssel der Leistung, den Allgemeinen Regionalschlüssel (ARS) des Gebiets, für das die Zuständigkeit gilt sowie den Link zum Onlineverfahren.

3.7.2.2 Betrachtung auf Basis einzelner OZG-Leistungen

Mit Blick auf die konkreten OZG-Leistungen, mit Fokus auf die Hochschule als hauptverantwortliche Stelle, lässt sich nach aktueller Einschätzung hinsichtlich der in Punkt 3.7.2.1 aufgeworfenen besonders datenschutzrelevanten Aspekte folgendes ableiten:

- Bewerbung um ein Studium an einer Hochschule (LeiKa-Schlüssel: 99061039000000)
  - Nutzer:innenkonto erforderlich
  - Zusätzlich Authentifizierung auf Vertrauensniveau vermutlich nicht erforderlich
  - Bezahlprozess noch nicht erforderlich
  - Digitale Nachweise erforderlich

- Nachteilsausgleich (LeiKa-Schlüssel: 99061034000000)

Ein Antrag auf Nachteilausgleich wird in der Regel im Rahmen der Bewerbung gestellt und ist daher nicht gesondert zu betrachten.

- Immatrikulation (LeiKa-Schlüssel: 99061003000000)
  - Nutzer:innenkonto erforderlich
  - Authentifizierung auf Vertrauensniveau erforderlich
  - Bezahlprozess erforderlich
  - Digitale Nachweise erforderlich

- Antrag auf Notenverbesserung (LeiKa-Schlüssel: 99061021000000)

Ein Antrag auf Notenverbesserung wird in der Regel im Rahmen der Bewerbung gestellt und ist daher nicht gesondert zu betrachten.

- Anrechnung und Anerkennung von Studienleistungen (LeiKa-Schlüssel: 99061023000000)

Ein Antrag auf Anrechnung und Anerkennung kann im Rahmen der Bewerbung gestellt werden und ist daher nicht gesondert zu betrachten.

- Semesterbeitrag (LeiKa-Schlüssel: 99061017000000)

Sowohl der Semesterbeitrag als auch die Studiengebühr werden initial bei der Immatrikulation erhoben. Hier ist der Aspekt des Bezahldiensts – der logischerweise dann auch für interne Studierende, die sich zurückmelden, relevant wird – von zentraler Bedeutung.

- Teilzeitstudium (LeiKa-Schlüssel: 99061032000000)

Ein Antrag auf Teilzeitstudium ergibt sich aus der Bewerbung auf das passende Studium (z. B. duales Studium) und wird daher nicht gesondert betrachtet, da der dahinterliegende Prozess dem der Bewerbung entspricht.

- Promotionsstudium (LeiKa-Schlüssel: 99061033000000)

Der Prozess der Einschreibung in ein Promotionsstudium ist hinsichtlich der betrachteten Aspekte dem der Immatrikulation recht ähnlich und wird daher nicht gesondert behandelt.

- Unterbrechung des Studiums (LeiKa-Schlüssel: 99061001000000)
    - Nutzer:innenkonto erforderlich
    - Authentifizierung mittels Studierenden-Account
    - Bezahlprozess nicht erforderlich
    - Digitale Nachweise müssten im Sinne der Interoperabilität bei Bedarf an entsprechende Behörden übermittelt werden

- Veränderungsmitteilung (LeiKa-Schlüssel: 99061011000000)
    - Nutzer:innenkonto erforderlich
    - Authentifizierung mittels Studierenden-Account
    - Bezahlprozess nicht erforderlich
    - Digitale Nachweise erforderlich

- Hochschulabschlusszeugnis (LeiKa-Schlüssel: 99061037000000)
    - Nutzer:innenkonto erforderlich
    - Authentifizierung mittels Studierenden-Account

- Bezahlprozess nicht erforderlich
- Digitale Nachweise müssten im Sinne der Interoperabilität bei Bedarf an entsprechende Behörden übermittelt werden

- Gasthörerschaft (LeiKa-Schlüssel: 99061031000000)
  - Nutzer:innenkonto erforderlich
  - Authentifizierung auf Vertrauensniveau erforderlich
  - Bezahlprozess erforderlich

- Exmatrikulation (LeiKa-Schlüssel: 99061002000000)
  - Nutzer:innenkonto erforderlich
  - Authentifizierung mittels Studierenden-Account
  - Bezahlprozess nicht erforderlich
  - Digitale Nachweise müssten im Sinne der Interoperabilität bei Bedarf an entsprechende Behörden übermittelt werden

Insgesamt bleibt es bei der Betrachtung der aktuell relevanten OZG-Leistungen im Feld Bildungszugang und -abschluss bei den vier Aspekten: Nutzer:innenkonto, Authentifizierung, Bezahlprozess und digitale Nachweise, die im folgenden Teil aus technischer Sicht ganz grundsätzlich betrachtet werden.

3.7.2.3 Betrachtung aus technischer Sicht

1. Übermittlung von personenbezogenen Daten

personenbezogene Daten	*besonders schützenswerte personenbezogene Daten*
Daten mithilfe derer eine Person direkt oder indirekt identifiziert werden könnte, auch in Kombination mit anderen Datenquellen oder Zusatzwissen. Geschlecht alleine ist z. B. kein personenbezogenes Merkmal, solange sich damit keine bestimmte Person identifizieren lässt. Um eine Identifizierung einer Person durch die Zuhilfenahme von Zusatzwissen oder anderer Datenquellen zu verhindern, empfiehlt es sich zusätzlich – wenn möglich – Daten zu aggregieren.	Daten, aufgrund derer eine Diskriminierung wahrscheinlich ist, wie z. B. Weltanschauung, ethnische Zugehörigkeit, Gewerkschaftszugehörigkeit, aber auch biometrische Gesundheitsdaten oder genetische Daten. Diese werden in Art. 9 DSGVO abschließend definiert.

Auch wenn das OZG vorschreibt, dass von Hochschulen spezielle Dienstleistungen über das Serviceportal anzubieten und auch darüber abzuwickeln sind, kann nicht ausgeschlossen werden, dass Studierende ebenfalls versuchen, Daten und Informationen, wie z. B. Nachweise auch auf anderem Wege (beispielsweise per E-Mail) zu übermitteln. Da es sich dabei auch um personenbezogene Daten handeln kann, ist es wichtig, vorab die technischen Voraussetzungen und rechtliche Details zu klären.

Bei *personenbezogenen Daten* handelt es sich um Daten, mithilfe derer eine Person identifiziert werden könnte, auch in Kombination mit anderen Datenquellen (sog. Zusatzwissen). Während sich eine Person mithilfe eines Namens oder einer Adresse relativ sicher ermitteln lässt, sieht dies bei manchen Merkmalen, die man spontan als *personenbezogene Daten* definieren würde, durchaus anders aus. Wird z. B. bei einem Fragebogen nach dem Geschlecht

gefragt, muss es sich bei dem Merkmal Geschlecht nicht um ein *personenbezogenes Merkmal* handeln, insofern das Geschlecht an sich keine Rückschlüsse auf eine bestimmte Person zulässt. Falls dies jedoch in Kombination mit anderen Daten (wie beispielsweise Alter und Größe) möglich ist, gelten all diese Informationen als *personenbezogen*. Hierbei ist herauszustellen, dass es sich nicht nur um *körperliche Merkmale* handeln muss, die als personenbezogen gelten. Es kann sich z. B. auch um Meinungsäußerungen handeln, die auf bestimmte Personen zurückzuführen sind. Darüber hinaus hat die DSGVO schützenswerte *personenbezogene Daten* definiert. Dies sind Daten aufgrund derer eine Diskriminierung wahrscheinlich ist bzw. in der Geschichte auch erfolgt ist, wie z. B. Weltanschauung, ethnische Zugehörigkeit, Gewerkschaftszugehörigkeit, aber auch biometrische- oder Gesundheitsdaten sowie genetische Daten (vgl. Art. 9 DSGVO).

Um nun die Kommunikation, die beim Austausch dieser Daten erfolgt, zu sichern, kommen zwei verschiedene Verfahren in Betracht: Die Transport- und die Inhaltsverschlüsselung. Die erstere, z. B. die Transport Layer Security (TLS), kann relativ einfach mithilfe der gängigen E-Mail-Programme eingerichtet werden. TLS hat jedoch den Nachteil, dass diese nur den Transportweg zwischen Server zu Server verschlüsselt. Liegt die Nachricht auf dem E-Mail Server an sich, kann dies unverschlüsselt geschehen. Zudem wird vom BSI laut technischer Richtlinie TR-02102-2 eine TLS Verschlüsselung erst ab der Version 1.2 als sicher erachtet. Abseits davon wäre jedoch eine Verschlüsselung durch die momentan aktuelle TLS-Version 1.3 zu empfehlen. Dementsprechend ist eine TLS-Verschlüsselung (unter bestimmten Voraussetzungen) nur für einfache personenbezogene Daten zulässig. Zudem muss unterschieden werden, ob die Hochschule *Sender* oder *Empfänger* der Nachricht ist: *„Die Verantwortung für den einzelnen Übermittlungsvorgang liegt bei dem Sender. Wer jedoch gezielt personenbezogene Daten per E-Mail entgegennimmt, ist verpflichtet, die Voraussetzungen für den sicheren Empfang von E-Mail-Nachrichten über einen verschlüsselten Kanal zu schaffen. Das bedeutet, dass der Empfangsserver mindestens den Aufbau von TLS-Verbindungen (direkt per SMTPS oder nach Erhalt eines STARTTLS-Befehls über SMTP) ermöglichen muss und hierbei ausschließlich die in der BSI TR 02102-2 aufgeführten Algorithmen verwenden darf“* (Konferenz der unabhängigen Datenschutzaufsichtsbehörden 2021, 5). Bei der Nutzung von TSL ist zudem zu beachten, dass die Konfiguration korrekt ist. Oftmals wird bei den Einstellung TLS nicht erzwungen, sondern nur

als optional eingestellt. Dieses Vorgehen bietet zwar den Vorteil, dass auch Dateien entgegengenommen werden, die nicht mittels TLS verschlüsselt worden sind, führt jedoch auch dazu, dass dies eben nicht datenschutzkonform geschieht.

Werden jedoch *besonders geschützte personenbezogene Daten* ausgetauscht, so ist neben der Transportverschlüsselung sicherzustellen, dass dies auch mithilfe einer Inhaltsverschlüsselung geschieht: *„Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei denen der Bruch der Vertraulichkeit ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er sowohl qualifizierte Transportverschlüsselung […] als auch den Empfang von Ende zu Ende verschlüsselter Nachrichten ermöglichen“* (Konferenz der unabhängigen Datenschutzaufsichtsbehörden 2021, ebd.) Auch wenn diese Verschlüsselungssoftware häufig kostenfrei ist und auch von Behörden genutzt werden kann, kann sich die Einrichtung einer Inhaltsverschlüsselung für unerfahrene Endanwender:innen aufwändig und technisch fordernd gestalten oder es treten Schwierigkeiten bei bestimmten Betriebssystemen auf. Ein Beispiel für eine derartige Anwendung ist GnuPG VS-Desktop, welches durch das BSI bis zum Geheimhaltungsgrad *vertraulich – nur für den Dienstgebrauch* zertifiziert ist. *„Nimmt ein Verantwortlicher Daten gezielt per E-Mail entgegen, bei den der Bruch der Integrität ein hohes Risiko für die Rechte und Freiheiten der betroffenen natürlichen Personen darstellt, dann muss er bestehende (PGP- oder S/MIME-) Signaturen qualifiziert prüfen“* (Konferenz der unabhängigen Datenschutzaufsichtsbehörden 2021, ebd.). Neben der E-Mail bieten sich ebenfalls Plattformen an, auf denen Nachweise hochgeladen werden können. Diese bieten den Vorteil, dass hier nur eine Partei die technischen Standards erfüllen muss, während es bei eine E-Mail-Kommunikation sowohl beim Absender, als auch Empfänger gewährleistet sein muss.

Abschließend muss festgehalten werden, dass in diesem Abschnitt nur die sichere Übertragung der Daten betrachtet wurden. Selbstverständlich schließt sich hieran z. B. auch noch eine Speicherung im System an, die ebenfalls technisch und organisatorisch auf die Beine gestellt werden muss.

<u>Authentifizierung</u>

Wie bereits unter 3.7.2.1 und 3.7.2.2 dargelegt, bedarf es nicht bei jedem Prozess bzw. jeder OZG-Leistung einer Authentifizierung. Ebenso ist noch nicht geklärt, welches Authentifizie-

rungsverfahren auf welchem Vertrauensniveau notwendig ist und ob es hier einen bundesweiten Standard geben wird. Ein gängiges Verfahren, welches sich aber nur langsam etabliert, ist die Authentifizierung per nPA und wird hier exemplarisch aus Datenschutzsicht beschrieben.

Bei Benutzung der Ausweisfunktion werden nicht alle auf dem nPA gespeicherten Daten übermittelt. Vielmehr muss ein Dienstanbieter, der auf bestimmte Informationen des nPA zugreifen möchte, vorher ein entsprechendes Berechtigungszertifikat durch die Vergabestelle für Berechtigungszertifikate genehmigt bekommen. In diesem Zertifikat wird auch festgelegt, welche Informationen (Datenfelder) vom nPA an den Dienstanbieter übermittelt werden. Liegt ein entsprechendes Zertifikat nicht vor, erfolgt keine Datenübermittlung durch den nPA. Liegt ein entsprechendes Zertifikat vor, müssen Nutzer:innen unter Einsicht der zu übermittelnden Daten der Übermittlung mittels PIN zustimmen. Informationen, die mit diesem Verfahren dabei an Dienstleister übermittelt werden können, sind:

> Familienname(n); Vorname(n); Doktorgrad; Tag der Geburt; Ort der Geburt; Anschrift; Dokumentenart; dienst- und kartenspezifisches Kennzeichen (für die *pseudonyme Kennung*); Abkürzung *D* für Bundesrepublik Deutschland; Angaben, ob ein bestimmtes Alter über- oder unterschritten ist (die sogenannte *Altersverifikation*); Angabe, ob ein Wohnort dem abgefragten Wohnort entspricht (die sogenannte *Wohnortverifikation*); Ordens- oder Künstlername.

Bei dieser Auflistung sind insbesondere drei Funktionen besonders zu beachten: Das sog. *kartenspezifisches Kennzeichen*, die *Altersverifikation* und die *Wohnortsverifikation*. Bei der Nutzung der letzten beiden Funktionen wird der empfangenden Stelle nur übermittelt, ob ein bestimmtes Alter erreicht wurde oder ein bestimmter Wohnort aktuell ist. Die Übermittlung des konkreten Geburtsdatums entfällt beispielsweise hierbei. Besonderer Beachtung bedarf das *kartenspezifische Kennzeichen*. Dieses ermöglicht die Verifikation einer Identität ohne die Preisgabe personenbezogener Daten. Dies kann unter anderem zum Einsatz kommen, wenn die benötigten Informationen bereits vorliegen (z. B. bei Internetanbietern) und nur noch bestätigt werden muss, dass ein neuer Auftrag (Umstellung auf einen neuen Tarif) von der bereits bekannten Person stammt.

Für den Abruf biometrischer Daten, die ebenfalls auf dem nPA gespeichert sind, wird kein Berechtigungszertifikat an Dienstleister:innen ausgestellt. Der Zugriff bleibt einzig und allein eine Möglichkeit für Behörden. Biometrische Daten umfassen dabei neben dem Lichtbild auch ggf.

Fingerabdrücke. Wird die online Ausweisfunktion des nPA beim Servicekonto z. B. mittels AusweisApp2 genutzt, werden an das Servicekonto sämtliche Daten übermittelt, die auch Dienstleister:innen abfragen könnten. Diese werden beim Anlegen eines Servicekonto.NRW übernommen. Zudem gibt es die Möglichkeit dort noch folgende Angaben zu ergänzen:

Nebenbestimmungen; E-Mail-Adresse; DE-Mail-Adresse; Mobilfunknummer.

Die spezielle OZG Leistung nutzt dann nur die für das Verwaltungsverfahren benötigten Daten. Ein permanentes Nutzer:innenkonto ist jedoch nicht zwangsläufig erforderlich, um die Identifizierungsfunktion des Servicekonto NRW zu nutzen. Wird kein permanentes Servicekonto.NRW angelegt, werden die übermittelten Daten nach Nutzung gelöscht.

Fall des Bezahlprozesses:

Auch wenn es aus Sicht der Hochschule möglicherweise bei der Auswahl eines Bezahldienstes darauf ankommt, dass die Zahlungsvorgänge zuverlässig sind und schnell abgewickelt werden können und hierbei eher die Schnittstellenentwicklung in Richtung Haushaltskassensystem und Campus Management in den Fokus rücken, so sind doch datenschutzrechtliche Aspekte von enormer Wichtigkeit. Als Bürger:in kann es weder von Interesse sein, dass transparent wird, für welche Services Bezahldienste genutzt werden, noch, dass die Bankdaten öffentlich werden.

Die wesentlichen Fragestellungen, die im Vorfeld zu klären sind, lauten (vgl. Herold 2020):

I. Wahl des Anbieters: Es ist zu prüfen, ob einzelne Paymentdienstleister:innen aus datenschutzrechtlicher Sicht überhaupt genutzt werden dürfen. Womöglich sind Anbieter:innen in einem Drittstaat angesiedelt, wodurch insbesondere nach der „Schrems II“-Entscheidung des EUGH vom 16. Juli 2020 erschwerte Bedingungen gelten können.

II. Analyse des Paymentprozesses: Unternehmen sollten sich damit auseinandersetzen, welche personenbezogenen Daten erfasst und den Paymentanbieter:innen übermittelt werden. Ebenso: Sind die Kund:innen darüber informiert und damit

einverstanden oder muss ggf. separat eingewilligt werden? Diese Einwilligung muss gegeben werden, falls externe Dienstleister:innen eingebunden worden sind.

III. Auftragsverarbeitung: Es wurde bereits angedeutet, dass je nach Konstellation eine Auftragsverarbeitung vorliegen kann. Entsprechend ist zu prüfen, ob ein Vertrag mit Auftragsverarbeiter:innen zu schließen ist.

IV. Verschlüsselung: Die Übermittlung personenbezogener Daten sollte grundsätzlich verschlüsselt erfolgen. Bei der Onlinezahlung gilt dies zwar seit Jahren als üblich, dennoch ist zu prüfen, ob auf der Website eine angemessene SSL (Secure Socket Layer) -Verschlüsselung verwendet wird.

V. Wahl der Plugins: Bei der technischen Integration in eine Website greifen viele Unternehmen auf Plugins zurück. Plugins sind komfortable Softwareerweiterungen für CMS-Plattformen, auf denen Websites basieren. Viele Onlineshops bauen beispielsweise auf Magento oder Oxid eSales auf, andere Websites häufig auf WordPress. Sofern Plugins zum Einsatz gelangen, ist zu überprüfen, ob diese eine ausreichende Sicherheit bieten. Plugins können vom Payment-Anbieter selbst (Paypal bietet z. B. eine große Anzahl eigener Plugins an) oder auch von externen Anbieter:innen stammen. Dabei ist auch zu prüfen, ob durch Plugins ein Transfer in Drittstaaten stattfindet und für welche Zwecke die Daten dort verwendet werden.

VI. Datenschutzerklärung: In der Datenschutzerklärung der Website ist zu erläutern, in welchem Umfang und zu welchem Zweck personenbezogene Daten mit dem Bezahlanbieter ausgetauscht werden. Entsprechend ist es notwendig, die Datenschutzerklärung anzupassen.

<u>Fall der digitalen Nachweise:</u>

Bei digitalen Nachweisen muss zum einen geklärt werden, in welcher Form sie ursprünglich entstanden sind (digital oder analog) und in welcher Form diese vorliegen müssen (einfache Kopie, beglaubigte Kopie oder als Original). Während es bei digital entstandenen Dokumenten, die mit einem entsprechenden Siegel oder einer entsprechenden Signatur versehen wurden (falls bereits technisch möglich), theoretisch simpel ist, alle Formerfordernisse zu erfüllen,

können ursprünglich analog erstellte Dokumente nur dann digital eingereicht werden, wenn eine einfache Kopie ausreichend ist. Die Möglichkeit analoge Dokumente mit gleicher Beweiskraft in digitale Dokumente mittels ersetzendem Scannen umzuwandeln, ist momentan technisch nicht gegeben. Hier ist es, z. B. nach EGovG NRW, weiterhin möglich, von der Behörde Papierunterlagen zu fordern.

4 Forderungen an die Gesetzgebung

In der Gesamtbetrachtung zeigt sich, dass zahlreiche in diesem Whitepaper angesprochenen Punkte nicht rein technischer Natur sind, sondern auch rechtliche und politische Aspekte betreffen. Wichtig erscheint es aus Sicht der öffentlichen Akteure vor allem, die Bürger:innen und damit die Nutzer:innen von OZG-Leistungen insgesamt auf den Weg der Digitalisierung mitzunehmen und diesen gemeinsam mit ihnen zu bestreiten. Die Mehrwerte der medienbruchfreien Digitalisierung wie die bequeme Erreichbarkeit der Online-Services, transparente Prozesse und der Abbau bürokratischer Hürden bieten eigentlich genug Argumente, um die Bürger:innen von den Vorteilen der neuen Instrumente zu überzeugen. Die elektronische Identifikation von Antragsstellenden ist dabei nur der erste Schritt eines Prozesses - wichtig ist dabei, Formulare und letztlich die Prozesse selbst nicht nur zu „elektrifizieren“, sondern digital zu transformieren, d. h. Abläufe müssen einfacher, durchgängiger und behördenübergreifend auch strukturell homogener werden, um eine schnellere und medienbruchfreie Nutzbarkeit zu gewährleisten.

Mit Blick auf ein avisiertes *OZG 2.0* erscheint der Anspruch auf eine vollständig digitalisierte Gesamtprozessbearbeitung (Ende-zu-Ende) auf der Basis vereinheitlichter und verbindlicher technischer Standards im Gegenzug zur Schaffung reiner Online-Dienste als wichtigste Forderung. Weitere Forderungen an den Gesetzgeber, die sich aus den Kapiteln dieses Whitepapers ergeben, sind nachfolgend zusammengefasst.

4.1 Vermeidung unterschiedlicher Nutzer:innenkonten

Im Sinne der Vereinfachung und Homogenisierung von Strukturen zeigt es sich, dass die Integration des „Nutzerkontos Bund“ als alleiniges Instrument für die Hochschulen von Vorteil wäre. Eine Nutzung von unterschiedlichen Nutzer:innenkonten wird nicht angestrebt. Sowohl auf der Aufwandsseite bei den Anpassungen der Backendsysteme als auch der Ansprache der Studierenden ist hier ein Konto, das NKB, der einfachste Weg.

Aufgrund der aktuell noch geringen Anzahl an für die Onlinenutzung freigeschalteten nPAs wird es in den kommenden Jahren aber auch weiterhin andere Verfahren geben müssen. Die Zielsetzung gegenüber den Studierenden ist es, möglichst niedrige Einstiegshürden für ein Hochschulstudium in Deutschland zu ermöglichen. Durch einfache Verwendung der Authentifizierungsmethode auf Seiten der Studienbewerber:innen und Studierenden werden Anreize

für die Nutzung des NKB gesetzt und ein Beitrag für die stärkere Nutzung der Onlineausweisfunktionen geleistet.
Um hier die Akzeptanz an den Hochschulen zu erhöhen wären folgende Aspekte im Rahmen der politischen Diskussion zu erörtern:

- Hochschulautonomie: Anerkennung der Tatsache, dass die Verwaltungsleistungen in Hochschulen immer in der Hoheit der Hochschulen und deren Backendsysteme (Campus Managementsysteme) bleiben werden. Das Schaffen einer Kommunikationsebene im Rahmen der OZG Vorhaben kann nicht mit einer „Einer für Alle“ Methodik (z.B. im Vergleich zur Beantragung eines KFZ-Kennzeichens) gleichgestellt werden. Diese Kommunikationsebene in Form von eigenen Portalen existiert bereits an den meisten Hochschulen. Somit sind die OZG-Vorhaben hier teilweise als Ergänzung zu bereits stark digitalisierten Verfahren zu sehen.

- Vereinfachung der Nutzung des „Nutzerkontos Bund“:

    - Öffnung der Nutzbarkeit des NKBs auch für Hochschulen in privater/ kirchlicher Trägerschaft und andere (vertrauenswürdige) Teilnehmer.
    - Das Schriftformerfordernis sollte in Bezug auf den Austausch mit den Studierenden nur in absoluten Ausnahmefällen vorgesehen werden. Die Nutzung von eIDAS in der Domäne Bildung sollte konsequent für alle Beteiligten kostenfrei sein, also nicht mehr Kosten verursachen, als die Nutzung traditioneller papierbasierter Ausweismöglichkeiten. Dies schließt private Bildungsanbieter mit ein.
    - Erweiterung der Schnittstellen des NKB, um zu ermöglichen, dass die Funktionen des NKBs auch durch andere technische Komponenten (beispielsweise Wallets, Email Client, Campus App ...) genutzt werden können. Dafür sind offene und interoperable Schnittstellen zu schaffen, die eine Integration in unterschiedlichste IT-Komponenten ermöglichen. Damit wäre eine schnelle Integration in die Backendsysteme möglich, da hier **nur eine Schnittstelle** implementiert werden müsste.

4.2 Rechtliche Rahmenbedingungen, insbesondere Datenschutz

Bestehende und neue Rechtsvorschriften des Bundes und der Länder werden in zunehmenden Maße sog. „Digital-Checks“ unterzogen, um eine digitale Verwaltung zu ermöglichen. Trotzdem existieren an vielen Stellen noch mehr oder weniger versteckte Hürden (Bsp. Schriftformerfordernis im Hochschulzulassungsrecht), die eine vollständig medienbruchfreie digitale Verwaltung verhindern. Die Umsetzung des OZG verlangt somit neben den technischen Instrumenten auch die Schaffung der erforderlichen rechtlichen Grundlagen.

Datenschutz als besondere rechtliche Rahmenbedingung dient dem Schutz personenbezogener Daten wird aber gerade von den Betroffenen häufig als hinderlich empfunden, wenn Abläufe dadurch zu bürokratisch oder umständlich erscheinen. Datenschutz und die IT-Sicherheit sind von enormer Bedeutung, sollten aber aus Sicht der Kernziele des OZG (wie Once-Only-Prinzip und Nutzer:innenzentrierung) nicht zum Hemmschuh werden. Auch hier ist eine sensible und konstruktive Herangehensweise und Umsetzung im Sinne der Nutzenden geboten.

4.3 Bereitstellung von Ressourcen

Die Schaffung neuer Regelungen und Technologien erfordert auf Seiten des Gesetzgebers den Weitblick, welche Konsequenzen und Dimension dies kurz- bis mittelfristig auf die Ressourcen der Beteiligten haben wird. Neben dauerhaften Kosten für den Betrieb geht es hier auch um die Qualifizierung oder Rekrutierung von Personal, welches in der Lage sein muss, die Brücke zwischen operativen Prozessen und technischer Infrastruktur immer wieder zu schlagen, um so die Weiterentwicklung der Services auf dem Weg zum OZG-Reifegrad 4 weiter konsequent voranzutreiben.

Als Besonderheit im Hochschulumfeld wäre es hierbei notwendig, die durchgängig genutzten Fachverfahren (insbesondere die CaMS), als *EfA-Online-Dienste* im Sinne des OZG anzuerkennen und ihnen somit für die erforderliche Weiterentwicklung Zugang zu den Konjunkturmitteln des Bundes zu ermöglichen.

5 Liste der Autor:innen

Wir danken ausdrücklich allen, die tatkräftig an der Entstehung dieses Whitepapers mitgewirkt und ihre Zeit dafür investiert haben!

Liste aller Autor:innen:

Name	**Einrichtung**
Bacharach, Guido	freier Autor
Bohr, Ingrid	Kooperationsunterstützung bwUni.digital
Gobert, Oliver	KDU.NRW
Heimlicher, Silke	KDU.NRW
Knorr, Steffen	Stiftung für Hochschulzulassung
Michels, Thorsten	TU Kaiserslautern
Pasek, Gregor	TU Dortmund
Pempe, Wolfgang	DFN e.V.
Pirkovitsch, Armin	TU Graz/Campus Online
Pongratz, Prof. Dr., Hans	Stiftung für Hochschulzulassung
Rohrbacher, Boris	TU Graz/Campus Online
Soldo, Erwin	DAAD e.V.
Strack, Prof. Dr., Hermann	Hochschule Harz
Teloo, Britta	Hochschule Ruhr West
Waßmann, Arn	HIS eG
Weißenbacher, Rudolf	TU Graz/Campus Online
Wiedermann, Dr., Wolfgang	OTH Regensburg

Rechtsberatung: Wirtschaftskanzlei GvW Graf von Westphalen

6 Anhang: Überblick über relevante Rechtsquellen

- Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz - OZG) vom 14. August 2017 (BGBl. I S. 3122, 3138), das zuletzt durch Artikel 16 des Gesetzes vom 28. Juni 2021 (BGBl. I S. 2250) geändert worden ist.

- Gesetz zur Förderung der elektronischen Verwaltung in Nordrhein-Westfalen (E-Government-Gesetz Nordrhein-Westfalen - EGovG NRW) In Kraft getreten am 16. Juli 2016 (GV. NRW. S. 551); geändert durch Gesetz vom 21. Juli 2018 (GV. NRW. S. 403), in Kraft getreten am 28. Juli 2018; Artikel 12 des Gesetzes vom 14. April 2020 (GV. NRW. S. 218b), in Kraft getreten am 15. April 2020; Artikel 1 des Gesetzes 30. Juni 2020 (GV. NRW. S. 644, ber. S. 702), in Kraft getreten am 14. Juli 2020; Artikel 1 des Gesetzes vom 1. Februar 2022 (GV. NRW. S. 122), in Kraft getreten am 19. Februar 2022.

- Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG (eIDAS-VO).

- Registermodernisierungsgesetz (RegMoG) vom 28. März 2021 (BGBl. I S. 591), das zuletzt durch Artikel 11 des Gesetzes vom 9. Juli 2021 (BGBl. I S. 2467) geändert worden ist.
  Das Registermodernisierungsgesetz (RegMoG) bildet rechtlich gesehen die Grundlage, um Verpflichtungen aus dem OZG vollständig umzusetzen. Ziel des RegMoG ist ein registerübergreifendes Identitätsmanagement; das heißt, dass künftig jedes Datum möglichst nur in einem Register der originär zuständigen Behörde vorhanden sein und nur von dort gepflegt werden soll. So können Widersprüchlichkeiten und Redundanzen in der Datenhaltung aufgelöst werden. Hierzu soll eine einheitliche Identifikationsnummer in die relevanten Verwaltungsregister eingeführt werden. Folglich versetzt die digitale Verfügbarkeit von hochwertigen Basisdaten über Personen oder Unternehmen sowie die Vernetzung von harmonisierten Registern die Verwaltung überhaupt erst in die Lage, Verwaltungsleistungen ohne Medienbrüche vollständig digital zu erbringen. Vorteilhaft wirkt sich im Weiteren aus, dass die Daten nicht immer wieder neu bei der betroffenen Person erhoben werden müssen, sondern in einem geprüften und verlässlichen Zustand durch die Behörden abgerufen werden können. Nach aktuellem Kenntnisstand ist es die Pflicht der regis-

terführenden Stellen, innerhalb der Umsetzungsfrist des RegMoG die Identifikationsnummer als zusätzliches Ordnungsmerkmal zu erheben und zu speichern. Zur Erfüllung dieser Aufgabe sollen die registerführenden Stellen die fehlenden Daten bei der Registermodernisierungsbehörde abrufen. Die Datenabrufe erfolgen sodann im automatisierten Verfahren; d. h. wenn die registerführende Stelle mindestens den Familiennamen, den Wohnort, die Postleitzahl sowie das Geburtsdatum der betroffenen Person im Abrufersuchen angibt, übermittelt die Registermodernisierungsstelle die Identifikationsnummer.

7 Literaturverzeichnis

Apple Inc. (2022a). Studierendenausweis zu Apple Wallet auf dem iPhone oder auf der Apple Watch hinzufügen. Online verfügbar unter https://support.apple.com/de-de/HT208965 (abgerufen am 07.07.2022).

Apple Inc. (2022b). Wallet - Apple Developer. Online verfügbar unter https://developer.apple.com/wallet/ (abgerufen am 07.07.2022).

Assmann, Tobias/Banse, Christian/Bastian, Paul/Breuer, Jennifer/Breuer, Jörg/Fischer, Jörg/Gasiba, Tiago Espinha/Girg, Wolfram/Goldberg, Philipp/Haas, Werner/Heinemann, Andreas/Hellemann, Niklas/Hemmert, Tobias/Hilgert, Jan (2021). Deutschland, digital, sicher. 30 Jahre BSI : Tagungsband zum 17. Deutschen IT-Sicherheitskongress. Gau-Algesheim, SecuMedia Verlag.

Bechtle AG (2022). Konsortium um Bechtle präsentiert Prototyp für Nationale Bildungsplattform. Online verfügbar unter https://www.bechtle.com/ch/ueber-bechtle/news/unternehmensmeldungen/pressemeldungen/2022/konsortium-um-bechtle-praesentiert-prototyp-fuer-nationale-bildungsplattform (abgerufen am 12.09.2022).

Behaghel, Katrin/Bohr, Ingrid, Fischer, Uwe/Grundke, Monika, Kurz, Daniela/Mann, Thomas/Maurer, Axel/Nitzsche, Norman/Reineke, Dr. Henning, Sattel, Christina/Walter/Prof. Dr. Thomas (2021). bwUni.digital White Paper - Think-Tank 04. Positionsbestimmung und Empfehlungen für die Universitäten des Landes Baden-Württemberg bezüglich OZG, SDG und XHochschule.

BMBF (2022). Erstes Pilotprojekt für Nationale Bildungsplattform startet. Bundesministerium für Bildung und Forschung. Online verfügbar unter https://www.bmbf.de/bmbf/de/home/_documents/erstes-pilotprojekt-fuer-nationale-bildungsplattform-startet.html (abgerufen am 07.07.2022).

BMI (2021a). Arbeitshilfen - OZG-Leitfaden - OZG-Leitfaden. Bundesministerium des Innern und für Heimat. Online verfügbar unter https://leitfaden.ozg-umsetzung.de/display/OZG/Arbeitshilfen (abgerufen am 07.06.2022).

BMI (2021b). Das Nutzerkonto Bund wird eIDAS-konform. Bundesministerium des Inneren und für Heimat. Online verfügbar unter https://www.personalausweisportal.de/SharedDocs/kurzmeldungen/Webs/PA/DE/2021/eidas-konformitaet-nutzerkonto-bund.html (abgerufen am 07.07.2022).

BMI (2021c). Integrationsleitfaden Bund. Version 1.7. BMI. Online verfügbar unter https://www.onlinezugangsgesetz.de/SharedDocs/downloads/Webs/OZG/DE/integrationsleitfaden-bund.pdf?__blob=publicationFile&v=10 (abgerufen am 06.09.2022).

BMI (2022a). Der Servicestandard für die digitale Verwaltung. Bundesministerium des Inneren und für Heimat. Online verfügbar unter https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/servicestandard/servicestandard-node.html (abgerufen am 03.06.2022).

BMI (2022b). Personalausweisportal. Bundesministerium des Innern und für Heimat. Online verfügbar unter https://www.personalausweisportal.de/Webs/PA/DE/startseite/startseite-node.html (abgerufen am 07.09.2022).

BMI (2022c). Prinzip 16: Interoperabilität. Bundesministerium des Inneren und für Heimat. Online verfügbar unter https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/servicestandard/prinzip-16/prinzip-16-node.html;jsessionid=B207EE681A5F336C89A9CB9AC7CB8F90.2_cid287 (abgerufen am 07.07.2022).

BMI (2022d). Prinzip des Servicestandards. Bundesministerium des Inneren und für Heimat. Online verfügbar unter https://www.onlinezugangsgesetz.de/Webs/OZG/DE/umsetzung/servicestandard/prinzip-4/prinzip-4-node.html (abgerufen am 07.07.2022).

BSI (2017). Leitfaden zur Basis-Absicherung nach IT-Grundschutz. In drei Schritten zur Informationssicherheit. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden_zur_Basis-Absicherung.pdf?__blob=publicationFile&v=3 (abgerufen am 07.06.2022).

BSI (2018). BSI Technische Richtlinie 03125 (BSI TR-03125). Version 1.2.1. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_Anlage_M2_V1_2_1.pdf (abgerufen am 12.09.2022).

BSI (2022). Diensteanbieter der Online-Ausweisfunktion. Bundesamt für Sicherheit in der Informationstechnik. Online verfügbar unter https://www.ausweisapp.bund.de/fuer-diensteanbieter (abgerufen am 07.07.2022).

Denkhaus, Wolfgang/Richter, Eike/Bostelmann, Lars (2019). E-Government-Gesetz, Onlinezugangsgesetz. Mit E-Government-Gesetzen der Länder und den Bezügen zum Verwaltungsverfahrensrecht : Kommentar. München, C.H. Beck.

Deutsche Bundesbank (2018). PSD2. Online verfügbar unter https://www.bundesbank.de/de/aufgaben/unbarer-zahlungsverkehr/psd2/psd2-775434 (abgerufen am 12.09.2022).

DFN-Verein (2020). DFN-Mitteilungen. Erkennung & Reaktion neuer DFN-Dienst Security Operations. Verein zur Förderung eines Deutschen Forschungsnetzes e. V. Online verfügbar unter https://www2.dfn.de/fileadmin/5Presse/DFNMitteilungen/DFN_Mitteilungen_98.pdf (abgerufen am 09.09.2022).

d-NRW (2020). Handbuch zur Teilnahme am Portalverbund NRW v1.3. d-NRW. Online verfügbar unter https://www.d-nrw.de/fileadmin/user_upload/PDF/Handbuch_zur_Teilnahme_am_Portalverbund_NRW_v1.3.pdf (abgerufen am 07.06.2022).

DS Praxis: Der Podcast (2021). Interview mit Dr. Thomas Petri. Das Onlinezugangsgesetz OZG und der Datenschutz, Datenschutz-Praxis. Online verfügbar unter https://www.datenschutz-praxis.de/grundlagen/ozg-und-der-datenschutz-podcast-folge-26/ (abgerufen am 03.06.2022).

EMREX network (2022). Technical | EMREX. Online verfügbar unter https://emrex.eu/technical/ (abgerufen am 07.07.2022).

EU Parlament/EU-Rat (2014). VERORDNUNG (EU) Nr. 910/2014 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG. EUROPÄISCHEs PARLAMENTS UND RAT. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910&from=BG (abgerufen am 07.09.2022).

Europäische Kommission (2015). DURCHFÜHRUNGSVERORDNUNG (EU) 2015/1502 DER KOMMISSION zur Festlegung von Mindestanforderungen an technische Spezifikationen und Verfahren für Sicherheitsniveaus elektronischer Identifizierungsmittel gemäß Artikel 8 Absatz 3 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt. Europäische Kommission. Online verfügbar unter https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=OJ%3AJOL_2015_235_R_0002 (abgerufen am 07.09.2022).

Europäische Kommission (2022). Europäische digitale Identität. Online verfügbar unter https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_de (abgerufen am 07.07.2022).

European Campus Card Association (2020). Overview of pre-notified and notified eID schemes under eIDAS - eID User Community. Online verfügbar unter https://eidproject.eu/download/rIdnRjLW0wIigwEypMXFhmTHUrY1MhHBIAHzY2KCt4Zm08dCJqeSssHTwUfCkXDXRCbjp-U39bAQ4KNzYoK3hmbT90Imp6PDEBMBRtVERLMAojZztTf1sBDhk6S3ttPDUjaCVSZ3krLB08FHwFIkZlSRAmKh8PVhUKHjEbKD8uNSBjCiF6VXZyK3ZAVFlcRXQeJWUqU2lbEgABPggjICg9O2Q5YBd-MDcfBhJwHw0dPxYrVioYNyYBHQI4DCI7KQNiUiRrO-GYrNyg3GH4pTFlkSGJ5KxdxVVMDDDwOY3V4OSEvKw/collaboration_with_existing_eid_projects_-_report_nov_2020.pdf (abgerufen am 09.09.2022).

Haak, Andreas/Winter, Nico (2022). OZG und DSGVO: Nutzerkonto und Once Only-Prinzip müssen Datenschutz einhalten | VdZ|Verwaltung der Zukunft. Online verfügbar unter https://www.vdz.org/digitalpolitik/ozg-und-dsgvo-nutzerkonto-und-once-only-prinzip-muessen-datenschutz-einhalten (abgerufen am 07.07.2022).

Haufe Online Redaktion (2022). Nutzerkonto des Bundes wird in Hessen und im Saarland eingeführt. Online verfügbar unter https://www.haufe.de/oeffentlicher-dienst/digitalisierung-transformation/nutzerkonto-des-bundes-wird-in-hessen-und-im-saarland_524786_561224.html (abgerufen am 07.07.2022).

Herold, Philipp (2020). Digitales Payment: Worauf Sie beim Datenschutz rund um Paypal und Co. achten müssen. Online verfügbar unter https://www.mein-datenschutzbeauftragter.de/blog/digitales-payment-worauf-sie-beim-datenschutz-rund-um-paypal-und-co-achten-muessen/ (abgerufen am 08.06.2022).

Hochschule Harz (2013). Hochschule Harz zeigt innovative Forschungsprojekte auf der CeBIT in Hannover. Hochschule Harz, Pressemitteilung vom 2013. Online verfügbar unter https://netlab.hs-harz.de/research/Messepraesentation_CeBIT_Forschungsprojekte_Hochschule%20Harz_040313.pdf (abgerufen am 12.09.2022).

Hochschulrektorenkonferenz (Hg.) (2022). Erhebung und Kartierung einschlägiger Projekte und Initiativen zur Digitalisierung von Anerkennungs- und Anrechnungsprozessen an Hochschulen.

IT-Planungsrat (2022). Aufgaben | IT-Planungsrat. Online verfügbar unter https://www.it-planungsrat.de/der-it-planungsrat/aufgaben (abgerufen am 12.09.2022).

Klein, Manfred (2021). Was ist die Europäische digitale Identität (EUid)? eGovernment Computing. Online verfügbar unter https://www.egovernment-computing.de/was-ist-die-europaeische-digitale-identitaet-euid-a-1072948/ (abgerufen am 07.07.2022).

Konferenz der unabhängigen Datenschutzaufsichtsbehörden (2021). Orientierungshilfe der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder. Maßnahmen zum Schutz personenbezogener Daten Maßnahmen zum Schutz personenbezogener Daten bei der Übermittlung per E-Mail. Online verfügbar unter https://www.datenschutzkonferenz-online.de/media/oh/20210616_orientierungshilfe_e_mail_verschluesselung.pdf (abgerufen am 08.06.2022).

Landesportal Sachsen-Anhalt (2022). OZG-Lexikon. Online verfügbar unter https://ozg.sachsen-anhalt.de/grundlagen/ozg-lexikon/#c241548 (abgerufen am 07.09.2022).

Leitold, H./Lioy, A./Ribeiro, C. (2015). Stork 2.0: Breaking New Grounds on EID andMandates. Online verfügbar unter https://www.eid-stork2.eu.

Merkle, R. C. (1980). Protocols for Public Key Cryptosystems. IEEE Symposium on Security and Privacy, 122.

OpenID Foundation (2022). Home » Welcome to OpenID Connect. OpenID Foundation. Online verfügbar unter https://openid.net/connect/ (abgerufen am 02.06.2022).

Projekt TREATS EU CEF (2017). Unterlagen zum TREATS Workshop. Online verfügbar unter https://netlab.hs-harz.de/research/TREATSWS/ (abgerufen am 12.09.2022).

Rivest, R. L./Shamir, A./Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM 21 (2), 120–126. https://doi.org/10.1145/359340.359342.

Robert Koch-Institut (2022). CovPassCheck-App: Digitale COVID-Zertifikate der EU schnell prüfen. Online verfügbar unter https://www.digitaler-impfnachweis-app.de/covpasscheck-app/ (abgerufen am 07.07.2022).

Ruschmeier, R./Gilch, H./Lessig, M./Friedrich Stratmann, F./Wannemacher, K. (2020). Herausforderungen bei der Umsetzung des Onlinezugangsgesetzes im Kontext der Digitalen Hochschulbildung. Arbeitspapier Nr. 55. Berlin. Hochschulforum Digitalisierung. BMBF. Online verfügbar unter https://hochschulforumdigitalisierung.de/de/news/studie-onlinezugangsgesetz-hochschulen-arbeitspapier (abgerufen am 27.05.2022).

Sinsel, Alexander (2020). Das Internet der Dinge in der Produktion. Smart Manufacturing für Anwender und Lösungsanbieter. Berlin, Springer Vieweg.

Strack, H./Karius, S./Gollnick, M./Lips, M./Wefel, S./Altschaffel, R. (2022a). Preservation of (higher) Trustworthiness in IAM for distributed workflows and systems based on eIDAS. Proc. of OID 2022 Kopenhagen.

Strack, Hermann (Hg.) (2001). MEDIA@Komm - the Pilot Project for E-Government and E-Commerce in Germany, Information Security Solutions Europe, London.

Strack, Hermann/Bacharach G./Klinner S./Otto O./Schmidt, A. (2019). eIDAS eID & eSignature for HEI/EDU Applications—EIDAS eID & eSignature based Service Accounts at University environments for crossboarder/domain access. European Journal of Higher Education IT 1. EUNIS 2019.

Strack, Hermann/Gollnick, Marlies/Karius, Sebastian/Lips, Meiko/Wefel, Sandro/Altschaffel, Robert/Bacharach, Guido/Gottlieb, Matthias/Pongratz, Hans/Radenbach, Wolfgang/Waßmann, Arn (2022b). EUNIS: Digitization of (Higher) Education Processes: Innovations, Security and Standards.

Universität Mannheim (2022). Deltaprüfungen. Online verfügbar unter https://www.uni-mannheim.de/studium/bewerbung/bewerbung-von-a-bis-z/studieren-ohne-abitur/deltapruefung/ (abgerufen am 07.07.2022).

van der Veer, Hans/Wiles, Anthony (2008). Achieving Technical Interoperability - the ETSI Approach. ETSI. Online verfügbar unter https://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf (abgerufen am 03.06.2022).

VFR Verlag für Rechtsjournalismus (2022). Bürger-Identifikationsnummer: Macht die Steuer-ID uns künftig zum gläsernen Menschen? Datenschutz.org. Online verfügbar unter https://www.datenschutz.org/buerger-identifikationsnummer/ (abgerufen am 07.07.2022).

Vitako (2022). Stellungnahme: Interoperabilität statt Zentralisierung - Zum Digitalisierungsprogramm des IT-Planungsrates. Online verfügbar unter https://www.vitako.de/Publikationen/Vitako_Positionspapier_Digitalisierungsprogramm.pdf (abgerufen am 03.06.2022).

Abkürzungsverzeichnis

Abb ..... Abbildung
Abs ..... Absatz
AG ..... Arbeitsgruppen
Art. ..... Artikel
BGB ..... Bürgerliches Gesetzbuch
BID ..... Bewerber-ID
BITV ..... Barrierefreie-Informationstechnik-Verordnung
bPK ..... bereichsspezifische Personenkennziffer
BSI ..... Bundesamt für Sicherheit in der Informationstechnik
CA ..... Certification Authority
CAdES ..... CMS Advanced Electronic Signatures
CaMS ..... Campus Managementsystem
CeBIT ..... Centrum für Büroautomation, Informationstechnologie und Telekommunikation
CEF ..... Connecting Europe Facility, Connecting Europe Facility
CRL ..... Certificate Revocation List
DAAD ..... Deutscher Akademischer Austauschdienst
DFN ..... Deutsches Forschungsnetz
DoSV ..... dialogorientierte Serviceverfahren
DSGVO ..... Datenschutz-Grundverordnung
DUO ..... Dienst Uitvoering Onderwijs
e. V ..... eingetragener Verein
eAT ..... elektronische Aufenthaltstitel
ECTS ..... European Credit Transfer and Accumulation System
edu-ID ..... education ID
EfA ..... Einer für Alle
EGovG ..... E-Government-Gesetz
eID ..... Elektronische Identität
eIDAS ..... Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates
eJob ..... Job-Onboarding-Tool
ELMO, EMREX ..... ELMO und EMREX sind europäische Standards bzw. technische Lösungen für den Transfer von Studierendendaten
ELSTER ..... elektronische Steuererklärung
ePayBL ..... E-Payment Bund und Länder
Erasmus ..... European Region Action Scheme for the Mobility of University Students
ESI ..... European Student Identifiers
ETSI ..... European Telecommunications Standards Institute
EU ..... Europäische Union
EUNIS ..... European University Information Systems
EWP ..... Erasmus without paper
F&E ..... Forschung & Entwicklung
FIM ..... Föderale Informationsmanagement, Föderalen Informationsmanagement
GnuPG ..... GNU General Public Licence Privacy Guard
HISinOne-ALU ..... Alumni-Management der HIS eG
HSM ..... Hardware Security Module
ID ..... Identifikationsnummer

IDM ..... Identity Management
IP ..... Internetprotokoll
ISO ..... Internationale Organisation für Normung
ISSE ..... International Students for Social Equality
IT ..... Informationstechnologie, Informationstechnologie
ITSEC ..... Information Technology Security Evaluation Criteria
KV ..... Krankenversicherung
LeiKa ..... Leistungskatalog
LoA ..... Levels of Assurance
MDS ..... Minimum Data Set
NC ..... Numerus Clausus
NFC ..... Near Field Communication
NKB ..... Nutzerkonto Bund
nm ..... multiple Mehrnutzer-/Rollenbezügen
nPA ..... neuer Personalausweis
OIDC ..... OpenID Connect
OSI ..... Online-Service-Infrastruktur
ÖV ..... Öffentliche Verwaltung
OZG ..... Onlinezugangsgesetz
PAdES ..... PDF Advanced Electronic Signatures
PIN ..... persönliche Identifikationsnummer
PKI ..... public key infrastructure, PublicKey-Kryptographie und -Infrastrukturen
QES ..... qualifizierte elektronische Signatur
RDFa ..... Resource Description Framework in Attributes
RegMoG ..... Registermodernisierungsgesetz
RS3G ..... Rome Students Systems
SfH ..... Stiftung für Hochschulzulassung
SigG ..... Signaturgesetz
SK ..... SecretKey
SMTPS ..... Simple Mail Transfer Protocol Secure
SSI ..... Self-sovereign Identity
SSL ..... Secure Socket Layer
ssPIN ..... sector-specific Personal Identification Number
TCP ..... Transmission Control Protocol
TLS ..... Transport Layer Security
TR ..... Technische Richtlinie
TS ..... TrustServices
TSP ..... TrustService Provider
VC ..... Verifiable Credentials
VSM ..... Verwaltungssuchmaschine
VwVfG ..... Verwaltungsverfahrensgesetz
XAdES ..... XML Advanced Electronic Signatures
XHEIE ..... XHigherEducationInstitutionExchange
XKCD ..... bedeutungslose Buchstabenkombination (Webcomic)
XÖV ..... XML in der öffentlichen Verwaltung

KDU.NRW

Ein Kooperationsvorhaben empfohlen durch die:

DIGITALE HOCHSCHULE NRW

INNOVATION DURCH KOOPERATION

Gefördert durch:

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen