



Handreichung zu elektronisch verifizierbaren Nachweisen am Beispiel von digitalen Hochschulabschlusssdokumenten

Diese Handreichung ist im Rahmen der AG EZevN entstanden. Bei Fragen und Anregungen wenden Sie sich an die bwOZG-Gesamtkoordinatorin Zineta Topcagic zineta.topcagic@ku-bwuni.digital.

Oktober 2026

Einleitung	3
1. Rahmenbedingungen für elektronisch verifizierbare Nachweise	4
2. Erstellung elektronisch verifizierbarer Nachweise	5
3. Zustellung elektronisch verifizierbarer Nachweise	9
Zentrales Bürger:innenpostfach (ZBP)	9
4. Ausblick	11
5. Literatur- und Quellenverzeichnis	12

Einleitung

Elektronisch verifizierbare Nachweise bieten Hochschulen die Möglichkeit, digitale Dokumente in einer fälschungssicheren Form auszustellen und somit eine durchgängige Digitalisierung von Prozessen. Diese Handreichung legt ihren Schwerpunkt auf Hochschulabschlussdokumente als eine der relevanten umzusetzenden Onlinezugangsgesetz (OZG)-Leistungen.¹ Hochschulabschlussdokumente, die elektronisch verifizierbar sind, tragen dazu bei, den steigenden Anforderungen einer zunehmend digitalen Studien- und Arbeitswelt gerecht zu werden.

Hochschulabschlussdokumente werden in Bewerbungsprozessen bereits heute überwiegend in digitaler Form eingereicht. Häufig handelt es sich dabei jedoch um eingescannte Dokumente, deren Echtheit meist nur durch eine Sichtung des Originals überprüft werden kann. Zudem lassen sich solche Dokumente mit geringem Aufwand verändern oder fälschen.

Elektronisch verifizierbare Nachweise ermöglichen es Empfangsstellen hingegen, die Authentizität eines Dokuments sofort zu prüfen. Durch die Bereitstellung maschinenlesbarer Daten wird zudem eine Grundvoraussetzung für die automatisierte Erfassung von Leistungsdaten geschaffen. Dadurch entfallen fehleranfällige manuelle Eingaben von Daten durch Antragstellende sowie die zeitintensiven Datenabgleiche auf Hochschuleseite, etwa beim Vergleich von Noten im Bewerbungsverfahren.

Mit fortschreitender Digitalisierung der Bildungsnachweise werden Hochschulen zukünftig elektronisch verifizierbare Nachweise erstellen² und verwalten. Diese können von Antragstellenden oder Behörden im Rahmen von Fachverfahren abgefragt, geprüft und maschinell verarbeitet werden. Diese Entwicklung gewinnt insbesondere vor dem Hintergrund der Registermodernisierung sowie der zukünftigen Nutzung der European Digital Identity Wallet (EUDI)-Wallet, eine europäische digitale Brieftasche zur sicheren Verwaltung und Übermittlung von (Identitäts-)nachweisen³, an Bedeutung: Nachweise werden künftig nicht mehr nur als klassische Dokumente, sondern als gezielt ausgewählte Datensätze übertragen.

Zukünftig werden Hochschulen elektronisch verifizierbare Nachweise auf Basis unterschiedlicher

¹ OZG-Leistung „Hochschulabschlussdokumente Erstellung“ (Schlüssel 99061037032000)

² Die Erstellung elektronisch verifizierbarer Hochschulabschlussdokumente erfolgt im Sinne der OZG-Konformität auf Grundlage eines vollständig digitalen Antragsprozesses. Die Antragswege, die für die Erstellung von Hochschulabschlussdokumenten an Hochschulen derzeit teilweise noch papierbasiert umgesetzt werden, stehen nicht im Mittelpunkt dieser Handreichung.

³ Vgl. Bundesministerium für Digitales und Staatsmodernisierung (2026)

technischer Anforderungen bereitstellen müssen: Im nationalen Kontext ist primär der XBildungs-Standard maßgeblich, bei dem XML-Daten erstellt werden, die als Anhang eines PDF-Dokuments ausgehändigt werden. Für den europäischen Kontext werden verifizierbare PDFs und Datenmodelle wie das European Learning Model oder EMREX/ELMO relevant.

Darüber hinaus spielt die EUDI-Wallet im Rahmen von Bewerbungs- und Zulassungsverfahren⁴ eine Rolle, beispielsweise wenn Bewerber:innen die elektronische Hochschulzugangsberechtigung über die EUDI-Wallet bereitstellen oder diese im Zuge der Identitätsprüfung während des Immatrikulationsprozesses nutzen.⁵ Damit legt diese Handreichung den Grundstein für zukünftige Anforderungen an eine Ende-zu-Ende digitalisierte Verwaltungs- und Nachweislandschaft.

1. Rahmenbedingungen für elektronisch verifizierbare Nachweise

Bei der Einführung elektronisch verifizierbarer Hochschulabschlusssdokumente müssen die rechtlichen Rahmenbedingungen berücksichtigt werden. Die Form der Ausstellung von Hochschulabschlusssdokumenten wird durch die jeweilige Prüfungsordnung der Hochschule festgelegt.⁶ Das baden-württembergische Landeshochschulgesetz schließt eine elektronische Ausstellungsform der Hochschulabschlusssdokumente nicht explizit aus.⁷ Eine elektronische Ausstellung von Nachweisen ist daher zulässig, sofern sie in den rechtlichen Regelwerken der Hochschulen, z. B. in der Rahmenprüfungsordnung, vorgesehen ist.⁸

Mit der Anpassung des rechtlichen Regelwerks an der Hochschule geht die Klärung der rechtlichen Grundlagen einher: Wenn künftig Papier- als auch digitale Hochschulabschlusssdokumente ausgestellt werden, muss geklärt werden, welche Ausführung, also die digitale oder die Papierversion, das Original ist.

⁴ Eine Nutzung der EUDI-Wallet für privatrechtliche Bereiche im Hochschulkontext (z. B. digitale Arbeitsverträge im Personalwesen) ist denkbar, fällt jedoch nicht in den Bereich des Verbundprojekts bwOZG.

⁵ Da die EUDI-Wallet nicht direkt den deutschen XHochschule-Standard verarbeiten kann, ist die Entwicklung eines Transformationsverfahrens erforderlich, um die Interoperabilität zwischen deutschen und europäischen elektronisch verifizierbaren Nachweisen sicherzustellen.

⁶ Siehe „DFN-Infobrief Recht 6/2025“ der Forschungsstelle Recht im DFN und Handreichung „Digitale Zeugnisse“ (2024) vom BSI

⁷ Vgl. Vortrag „Elektronische Signaturen in Hochschulzeugnissen (in Baden-Württemberg)“ Philipp Schöbel, 26.06.2025. Folien siehe: https://www.ku-bwuni.digital/wp-content/uploads/Elektronische-Signaturen-Hochschulzeugnisse-BaWue_Schoebel_2025_final.pdf

⁸ In Thüringen stellt die Universität Erfurt Hochschulabschlusszeugnisse ausschließlich digital aus.

Auch ist festzulegen, ob elektronische Nachweise mit einem personenunabhängigen elektronischen Siegel der ausstellenden Organisation, einer personalisierten elektronischen Signatur, aus der die Organisationszugehörigkeit hervorgeht, oder einer Kombination aus beiden versehen werden müssen. Die rechtliche Zulässigkeit elektronischer Zeugnisse mit elektronischer Signatur und/oder elektronischem Siegel wird durch die eIDAS-Verordnung und die Ersetzung der Schriftform durch das OZG gestützt.

Hochschulen, die neben dem Hochschulsiegel auch das baden-württembergische Landeswappen auf den Hochschulabschlusssdokumenten aufbringen, sollten in Absprache mit dem Ministerium für Wissenschaft, Forschung und Kunst (MWK) klären, wie sie das Landeswappen zukünftig digital abbilden.⁹

Zudem ist zu beachten, dass nicht nur druckbare Dokumente (in der Regel im PDF-Format) einen digitalen Signaturdatensatz tragen können. Auch maschinenlesbare Anhänge dieser Dokumente besitzen einen eigenen Signaturbereich. Für diesen ist festzulegen, ob und auf welche Weise er signiert bzw. gesiegelt wird, etwa qualifiziert oder fortgeschritten.

Damit sind zwei Prüfungen mit unterschiedlichen Zwecken möglich: Die Signatur des XML-Anhangs bestätigt die Echtheit und Unverändertheit der XML-Daten und ist insbesondere für die automatisierte Weiterverarbeitung relevant. Die Signatur des PDF-Dokuments bestätigt die Unverändertheit des gesamten Dokuments, also sowohl der PDF-Datei als auch des darin eingebetteten XML-Anhangs. Wird der XML-Anhang später aus der PDF herausgelöst und separat verarbeitet, bleibt seine eigene Signatur bzw. sein eigenes Siegel gültig. Damit lässt sich jedoch nicht mehr prüfen, ob die ursprüngliche PDF-Datei als Ganzes unverändert geblieben ist. Hierfür ist die Signatur der vollständigen PDF-Datei erforderlich.¹⁰

2. Erstellung elektronisch verifizierbarer Nachweise

Digitalisierungsvorhaben, wie das der Registermodernisierung, streben langfristig einen dokumentenlosen Austausch an und legen den Fokus auf die Abfrage der maschinenlesbaren Nachweisdaten. Dabei ersetzen strukturierte Datenfelder im Fachverfahren den klassischen Nachweis. Dennoch ist zum jetzigen Stand davon auszugehen, dass PDF-Dateien, ergänzt mit strukturierten Daten im Anhang, in der Hochschulwelt vorerst bestehen bleiben.¹¹ Hochschulen sollten daher in der Lage sein, sowohl menschenlesbare (PDF-Datei) als auch maschinenlesbare

⁹ Diese Frage betrifft nur Schmuckdokumente in PDF-Form. Die generelle Frage, ob ein qualifiziertes elektronisches Siegel als Ersatz zu einem Dienstsiegel gesehen werden kann liegt dem MWK vor.

¹⁰ Weitere Informationen dazu finden sich in der Spezifikation XHochschule unter II.3.3 „XML Signature Syntax and Processing Version 2.0“.

¹¹ Das PDF ist und bleibt die Form, die den Personen unmittelbar vorgelegt und von ihnen geprüft werden kann. Nicht jede Hochschule kann maschinenlesbare Nachweisdaten verarbeiten. Ein signiertes PDF ist universell, JSON- oder XML-Daten sind das aktuell noch nicht.

elektronisch verifizierbare Nachweise bereitzustellen.

Die fachlichen Grundlagen für maschinenlesbare Bildungsnachweise werden im nationalen Kontext durch den Standard XBildung, für den Hochschulbereich betreffend XHochschule, geschaffen. Laut Beschluss des IT-Planungsrats ist der Datenstandard XBildung, einschließlich XSchule, XHochschule und XBerufsbildung, ab dem Jahr 2029 für den Anwendungsbereich der Zeugnisse verbindlich. Für Hochschulen ist eine Übergangszeit von zwei Jahren ab 2027 vorgesehen.¹² Dieser Verbindlichkeitsbeschluss bedeutet für Hochschulen, dass sie spätestens ab 2029 Hochschulabschlusssdokumente in ihrer digitalen Form gemäß dem XHochschule-Standard ausstellen müssen. Der XHochschule-Standard umfasst in der aktuellen Version 1.2 in Bezug auf die Hochschulabschlusssdokumente folgende Bescheinigungen und Nachweise: Diploma Supplement, Hochschulabschlusszeugnis und Transcript of Records.¹³

Die Erstellung eines elektronisch verifizierbaren Nachweises¹⁴ umfasst grundsätzlich folgende Schritte:

- 1) Zusammenstellung der Nachweisdaten aus vorliegenden Daten im Campusmanagementsystem (CaMS)
- 2) Erzeugung eines maschinenlesbaren Datensatzes auf Basis der relevanten Standards wie z. B. XHochschule¹⁵ und European Learning Model¹⁶ (ELM) sowie Daten im Format wie XML oder JSON¹⁷
- 3) In der Regel Erstellung eines druckfähigen (PDF-)Dokuments
- 4) Integration des maschinenlesbaren Datensatzes als Anhang
- 5) Signatur bzw. Siegelung des Datensatzes im dafür vorgesehenen Signaturfeld für die vollautomatisierte Annahme und Auswertung
- 6) Signatur bzw. Siegelung des druckfähigen Dokuments für einen für Menschen

¹² Vgl. IT-Planungsrat (2025), Beschluss B-2025/43-IT

¹³ Zu den Hochschulabschlusssdokumenten gehört in der Regel auch eine Urkunde. Diese ist derzeit noch kein Bestandteil des XHochschule-Standards. Dies wurde im Rahmen des XHochschule-Kommentierungsverfahrens im Sommer 2026 von mehreren Hochschulen thematisiert.

¹⁴ Im Folgenden wird von einem elektronisch verifizierbaren Nachweis mit maschinenlesbarem Anhang ausgegangen. Ein solcher Nachweis kann grundsätzlich auch ohne maschinenlesbaren Anhang als PDF-Dokument erstellt werden.

¹⁵ Es kann für die Erzeugung ein Validator genutzt werden, mit dem XML-Nachweise hinsichtlich des Standards „XHochschule“ validiert und geprüft werden können, ob sie der Schema- und Schematron-Konformität entsprechen.

¹⁶ Siehe „Introduction to the European Learning Model (ELM)“ der European Commission (o. A.).

¹⁷ Die EUDI-Wallet-kompatible Nachweise befinden sich bei den verschiedenen Campusmanagement-Herstellern aktuell in der Konzeptionsphase. Die konkreten technischen und organisatorischen Verfahren werden derzeit in verschiedenen Projekten auf Bundes- und Länderebene erarbeitet, u. a. durch Pilotprojekte in NRW und Sachsen.

nachvollziehbaren Echtheitsnachweis mithilfe einer Betrachtungssoftware für druckfähige Dokumente

- 7) Bereitstellung des Nachweises für die Weitergabe an Antragsstellende
- 8) Kopie in Akte und Archivierung

Zur Erstellung elektronisch verifizierbarer Nachweise in PDF-Form werden Siegel- bzw. Signaturzertifikate benötigt.¹⁸ Eine Signatur ist einer natürlichen Person zugeordnet und entspricht einer Willenserklärung; ein Siegel ist einer juristischen Person, z. B. einer Hochschule, zugeordnet. Signaturformen können gemäß eIDAS-Verordnung in drei Vertrauensniveaus unterteilt werden: einfach, fortgeschritten und qualifiziert.¹⁹ Das Vertrauensniveau der qualifizierten elektronischen Signatur hat die höchste juristische Beweiskraft und ist mit einer handschriftlich ausgestellten Urkunde (ggf. mit Siegelstempel) gleichzusetzen.²⁰

Ein mit einer qualifizierten elektronischen Signatur oder einem qualifizierten elektronischen Siegel versehener Nachweis kann von externen Personen oder Einrichtungen validiert werden. Diese Prüfung weist nach wann (signierter Zeitstempel), womit (Zertifikat bzw. Vertrauensdienstanbieter) und von wem (Authentizität) das Dokument ausgestellt wurde und dass der Inhalt des Dokuments nicht verändert wurde (Integrität).²¹

Der elektronisch verifizierbare Nachweis sollte im Rahmen des Siegelungs- bzw. Signaturprozess mit einem qualifizierten elektronischen Zeitstempel versehen werden, um eine Langzeitvalidierbarkeit (LTV) des Dokuments, auch nach dem Ablaufdatum des zugrunde liegenden digitalen Zertifikats, zu gewährleisten.²²

Bei der Auswahl der Anwendungsfälle für elektronische Signaturprozesse sollten die jeweiligen Fallzahlen berücksichtigt werden. So lässt sich feststellen, ob Einzel- oder Stapelverfahren notwendig sind und welche Signaturkomponenten dafür geeignet sind. Je nach Anwendungsfall und Bedarf der Hochschule sollte ergebnisoffen entschieden werden, welche Lösung geeignet ist und welche Bedarfe an der jeweiligen Hochschule Priorität haben.

Ein Verständnis davon, wie die Erstellung von Nachweisen für die Fachverfahren im Detail erfolgt, ist für die Prozessklärung unerlässlich. Die Hochschulen müssen daher prüfen, wann und

¹⁸ Diese Handreichung setzt Wissen zu elektronischen Siegeln und Signaturen voraus. Detaillierte Informationen, insbesondere zu elektronischen Signaturen, finden sich im White Paper „Digitalisierung der Unterschrift in Verwaltungsprozessen“ des „KU-bwUni.digital-Think-Tanks 01“ (2021).

¹⁹ In der „EU-Trusted-List“ sind gemäß eIDAS-Verordnung Vertrauensdiensteanbieter aufgeführt, die für die qualifizierte Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln berechtigt sind.

²⁰ Vgl. Verordnung Nr. 910/2014 des europäischen Parlaments und des Rates, Einleitung (49)

²¹ Vgl. ebd., Kap. 3, Abschnitt 4, Art. 32

²² Vgl. ebd., Kap. 3, Abschnitt 6, Art. 42

in welchem System der Nachweis entsteht, in welchem Prozessschritt er mit welchem Fachverfahren gekoppelt und von wem signiert und gesiegelt wird.²³ Das Ziel sollte darin bestehen, eine von der Erstellung über die Zustellung bis zur Archivierung vollständig digitalisierte Prozessmodellierung zu erarbeiten.

Zur Verdeutlichung sind im Folgenden Signatur-/Siegelverfahren mit unterschiedlichem Automatisierungsgrad beispielhaft abgebildet:

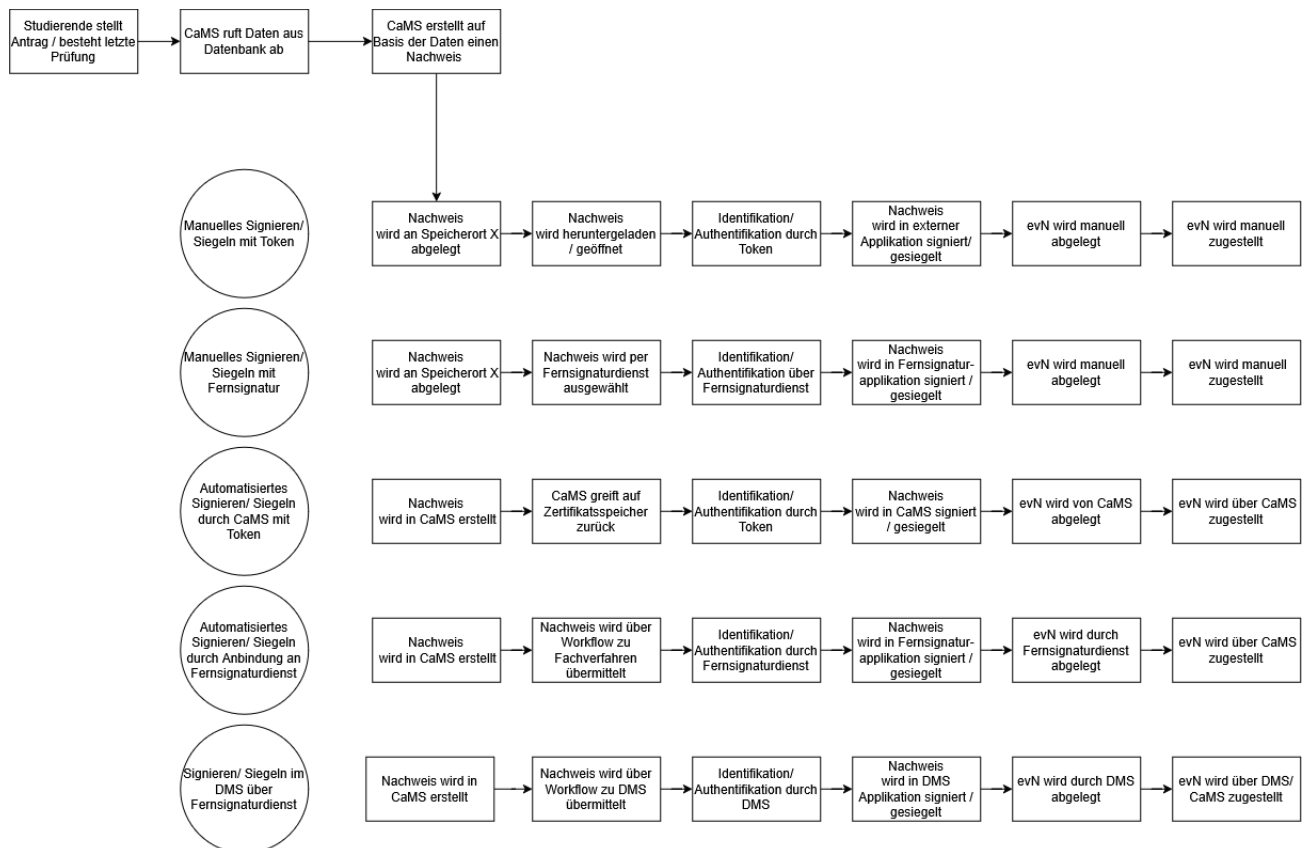


Abbildung 1. Signatur-/Siegelverfahren von elektronisch verifizierbaren Nachweisen (evN) mit unterschiedlichem Automatisierungsgrad. Eigene Darstellung

²³ Zu beachten gilt, dass es in Baden-Württemberg Studiengänge gibt, bei denen für die Erstellung von Hochschulabschlusssdokumenten externe Prüfungsämter bzw. Landesprüfungsämter zuständig sind. Dies betrifft die Studiengänge Medizin, Rechtswissenschaften sowie Katholische Theologie - Kirchliches Examen. Inwiefern die Landesprüfungsämter die OZG-Anforderungen und eine Erstellung von elektronisch verifizierbaren Hochschulabschlusssdokumente anstreben, ist aktuell unklar und wurde seitens der bwOZG-Gruppe gegenüber dem MWK thematisiert.

3. Zustellung elektronisch verifizierbarer Nachweise

Bereits heute stellen Hochschulen Dokumente und Bescheinigungen in digitaler Form als PDF-Dateien über ihr Campus-Management-System den Studierenden bereit. Die rechtssichere elektronische Zustellung wird dabei in der Regel durch entsprechende Regelungen im OZG, Landesgesetzen und in den hochschulspezifischen Regelwerken sichergestellt.²⁴

Gemäß OZG kann eine rechtssichere elektronische Zustellung von Nachweisen und Bescheiden über das Zentrale Bürger:innenpostfach (ZBP) erfolgen.²⁵ Um die Anforderungen des OZG zu erfüllen, muss das CaMS eine Identifizierung von Personen auf dem erforderlichen höchsten Vertrauensniveau ermöglichen. Dies kann durch eine Anbindung des CaMS an die BundID realisiert werden, denn über die BundID können sich Studierende mit dem entsprechenden Vertrauensniveau gegenüber dem CaMS eindeutig authentifizieren.

Für die elektronische Zustellung von Nachweisen sind folgende Szenarien denkbar:

1. **Elektronische Zustellung über das CaMS:** Nachweise werden im Self-Service des Campus-Management-Systems bereitgestellt. Ergänzend erhalten Studierende eine Portalnachricht im ZBP, dass ein neuer Nachweis zum Download im CaMS verfügbar ist.
2. **Elektronische Zustellung über das Zentrale Bürger:innenpostfach:** Nachweise werden unmittelbar und OZG-konform an das ZBP übermittelt.

Die Zustellung ins ZBP setzt die Verknüpfung des BundID-Kontos mit dem Universitäts- bzw. CaMS-Konto voraus. Dadurch wird die persönliche Postfach-ID hinterlegt. Auch wenn Verwaltungsakte im Rahmen des OZG elektronisch ins ZBP bereitgestellt werden können, muss für Studierende, die keine BundID nutzen oder die gemäß §9 Abs. 1 OZG einer elektronischen Zustellung widersprechen, eine alternative Form der rechtssicheren Benachrichtigung möglich sein.

Zentrales Bürger:innenpostfach (ZBP)

Das ZBP in Verbindung mit der BundID ermöglicht es Behörden auf Bundes-, Landes- und Kommunalebene, Nachweise²⁶ oder Informationen auf elektronischem Weg den Bürger:innen zuzustellen. Darüber hinaus sollen Antragstellende über Statusnachrichten regelmäßig über den

²⁴ Mehr zum Schriftformersatz und den rechtlichen Regelungen siehe „Die Ersetzung der Schriftform durch § 9a OZG an Hochschulen in Baden-Württemberg: Wenn Kafkas Bürokratie digital wird – vom Prozess elektronisch zu signieren und zu siegeln“ bwOZG-Verbundprojekt (Mai 2025)

²⁵ Vgl. § 9 Abs. 1 OZG

²⁶ Siehe bwOZG-Handreichung „Die Ersetzung der Schriftform durch § 9a OZG an Hochschulen in Baden-Württemberg: Wenn Kafkas Bürokratie digital wird – vom Prozess elektronisch zu signieren und zu siegeln“ (Mai 2025)

aktuellen Bearbeitungsstand ihrer Anliegen informiert werden.

Das ZBP ist Bestandteil des Nutzer:innenkontos der BundID und damit Teil des Portalverbunds.²⁷ Voraussetzung für den Übermittlungsweg ans ZBP ist eine produktive BundID-Anbindung der Hochschule. Für die technische Anbindung stellt das ZBP eine Schnittstelle bereit, die allerdings nur aus den Netzen des Bundes oder über das Verbindungsnetz erreichbar ist. Ein direkter Zugriff von außerhalb dieser Netze ist nicht möglich. Um trotzdem Nachrichten und Statusinformationen aus Verwaltungssystemen oder Onlinediensten an das ZBP übertragen zu können, steht die sogenannte Brückenkopf-Lösung „ZBP-Adapter“ von FIT-Connect zur Verfügung. Diese leitet die verschlüsselten Pakete ans ZBP weiter und ermöglicht so die gewünschten Nachrichten und Statusmeldungen dort einzustellen.²⁸

Beim Nachrichtenversand über FIT-Connect nimmt das CaMS die Rolle eines Onlinedienstes ein.²⁹ Alle an den Portalverbund angebotenen Systeme müssen gemäß § 2 ITSiV-PV technische Richtlinien des BSI zur Gewährleistung der IT-Sicherheit einhalten sowie Maßnahmen zur Gewährleistung der IT-Sicherheit treffen.³⁰

Auf dem Weg zu einer produktiven ZBP-Adapter-Anbindung sind folgende Schritte nötig:

1. MeinUnternehmenskonto erstellen (personalisiertes ELSTER-Organisationszertifikat für Login-Prozesse im BundID Self-Service Portal beantragen)
2. Anbindung Komponente Authentifizierung
3. Anbindung Komponente Postfach
4. Anbindung Fit-Connect Adapter zur Übertragung in die Netze des Bundes (sofern nicht im Einzelfall eine Direktanbindung an die Netze des Bundes geplant ist)
5. Anpassungen Prozesse und Rahmenbedingungen sowohl im CaMS als auch in den dafür zu Grunde liegenden rechtlichen Formalia bezüglich Schriftformersatz; Klagefristen und Zustellungswege in Satzungen, Zulassungs- und Immatrikulationsordnung sowie Rahmenprüfungsordnungen

Die FITKO stellt eine ausführliche ZBP-Adapter-Dokumentation³¹ zur Verfügung. Zudem sollte die Dokumentation des eigenen Campus-Management-Herstellers berücksichtigt werden.

27 Vgl. § 2 Abs. 7 OZG

28 Siehe „Zentrales Bürgerpostfach“: <https://docs.fitko.de/fit-connect/docs/organisation-tasks/buergerpostfach-entscheider/>

29 Vgl. § 1 Abs. 4 S. 2 ITSiV-PV

30 Anforderung aus § 2 Abs. 6 ITSiV-PV

31 Siehe „FIT-Connect und das Zentrale Bürgerpostfach (ZBP)“: <https://docs.fitko.de/fit-connect/docs/zbp/#anbindung-des-zbp-au%C3%9Ferhalb-des-verbindungsnetz>

4. Ausblick

Die Erstellung von elektronisch verifizierbaren Dokumenten wie Hochschulabschlusszeugnissen ist bereits heute technisch und rechtlich realisierbar. Voraussetzung ist, dass Hochschulen die erforderlichen elektronischen Signaturen und Siegel einführen und in ihre bestehenden Verwaltungsprozesse integrieren. Dadurch können Hochschulabschlusssdokumente im Falle eines digitalen Antrags medienbruchfrei beantragt, menschen- und maschinenlesbar erstellt, elektronisch unterzeichnet und rechtskonform bereitgestellt werden.

Für eine erfolgreiche Umsetzung ist jedoch eine enge abteilungsübergreifende Zusammenarbeit erforderlich. Insbesondere Prüfungsämter, das Campus-Management, die Rechtsabteilung sowie die für die Verwaltung elektronischer Signaturen und Siegel zuständigen Stellen müssen ihre Prozesse aufeinander abstimmen. Nur durch eine gemeinsame Planung und Koordination können technische, organisatorische und rechtliche Anforderungen gleichermaßen berücksichtigt und ein durchgängiger digitaler Prozess geschaffen werden.

Die Digitalisierung von Hochschulabschlusssdokumenten stellt damit nicht allein eine technische Herausforderung dar, sondern erfordert auch eine institutionelle Zusammenarbeit über organisatorische Grenzen hinweg.

5. Literatur- und Quellenverzeichnis

Bohr, Ingrid et al. (2021): bwUni.digital White Paper – Think-Tank 01. Digitalisierung der Unterschrift in Verwaltungsprozessen (Februar 2021), <https://www.bwuni.digital/think-tank-01/>

(zuletzt abgerufen am 19.09.2026)

Bundesministerium für Digitales und Staatsmodernisierung: EUDI-Wallet „d-you“. URL: <https://bmds.bund.de/themen/digitaler-staat/digitale-identitaeten/eudi-wallet> (zuletzt abgerufen am 21.09.2026)

Bundesamt für Sicherheit in der Informationstechnik (2024): Handreichung „Digitale Zeugnisse“ Version: 1.0. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Oeffentliche_Verwaltung/Moderner-Staat/Handreichung-Digitale-Zeugnisse.pdf?__blob=publicationFile&v=4 (zuletzt abgerufen am 19.09.2026)

bwOZG: Die Ersetzung der Schriftform durch § 9a OZG an Hochschulen in Baden-Württemberg: Wenn Kafkas Bürokratie digital wird – vom Prozess elektronisch zu signieren und zu siegeln. Nicht veröffentlicht (Mai 2025)

European Commission (o. A.): Introduction to the European Learning Model (ELM)“. URL: <https://europa.eu/europass/elm-browser/index.html> (zuletzt abgerufen am 19.09.2026).

FIT-Connect: FIT-Connect und das Zentrale Bürgerpostfach (ZBP). URL: <https://docs.fitko.de/fit-connect/docs/zbp/#anbindung-des-zbp-au%C3%9Ferhalb-des-verbindungsnetz> (zuletzt abgerufen am 24.08.2026)

FIT-Connect: Zentrales Bürgerpostfach. URL: <https://docs.fitko.de/fit-connect/docs/organisation-tasks/buergerpostfach-entscheider/> (zuletzt abgerufen am 24.08.2026).

Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen (Onlinezugangsgesetz – OZG), abrufbar unter: <https://www.gesetze-im-internet.de/ozg/> (zuletzt abgerufen am 19.02.2026)

IT-Planungsrat (2025): Verbindlichkeit von XBildung B-2025/43-IT. URL: <https://www.it-planungsrat.de/beschluss/b-2025-43-it> (zuletzt abgerufen am 19.09.2026)

Schöbel, Philipp (2025): Elektronische Signaturen in Hochschulzeugnissen (in Baden-Württemberg), Vortrag vom 26.06.2025. Folien siehe: https://www.ku-bwuni.digital/wp-content/uploads/Elektronische-Signaturen-Hochschulzeugnisse-BaWue_Schoebel_2025_final.pdf (zuletzt abgerufen am 19.09.2026).

Verein zur Förderung eines Deutschen Forschungsnetzes e.V. (2025): DFN-Infobrief Recht 6 / 2025. URL: https://recht.dfn.de/wp-content/uploads/2025/06/Infobrief_Recht_6-2025.pdf (zuletzt abgerufen am 24.08.2026).

Verordnung zur Gewährleistung der IT-Sicherheit der im Portalverbund und zur Anbindung an den Portalverbund genutzten IT-Komponenten (IT-Sicherheitsverordnung Portalverbund - ITSiv-PV), abrufbar unter <https://www.gesetze-im-internet.de/itsiv-pv/BJNR001800022.html> (zuletzt abgerufen am 24.08.2026)

Verordnung Nr. 910/2014 des europäischen Parlaments und des Rates, abrufbar unter: <https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R0910> (zuletzt abgerufen am 19.09.2026)