

Rechtliche Anforderungen an digitale Hochschulzeugnisse

83. DFN-Betriebstagung | 08.10.2025

Philipp Schöbel

Gliederung



- 1. Digitale Zeugnisse
- 2. Qualifizierte elektronische Signatur
 - 1. Elektronische Signaturen
 - 2. Elektronische Siegel
- 3. "Umwandlung" von Hochschulzeugnissen
- 4. Handlungsmöglichkeiten für Hochschulen

Digitale Zeugnisse

Welche Dokumente sind gemeint?

DFN

Urkunde

Zeugnis

Transcript of Records

Diploma Supplement

z.B.:

Beurkundet

Verleihung

Hochschulgrad +

Unterschrift

Vorsitzende

Gemeinsame

Kommission + Datum

+ Uni-Siegel

z.B.:

Note + Thema

Abschlussarbeit +

Datum letzte

Prüfungsleistung +

Unterschrift Vorsitz

Prüfungsaus-schuss

+ Uni-Siegel

z.B.:

Leistungsübersicht:

alle Module +

Prüfungsleistungen +

Studienleistungen +

Noten + Thema

Abschlussarbeit; +

Unterschrift Vorsitz

Prüfungsausschuss +

Uni-Siegel + Datum

z.B.:

Angaben zur Person

+ Infos Art und

Ebene Abschluss +

Status Hochschule +

Info

Studienprogramm +

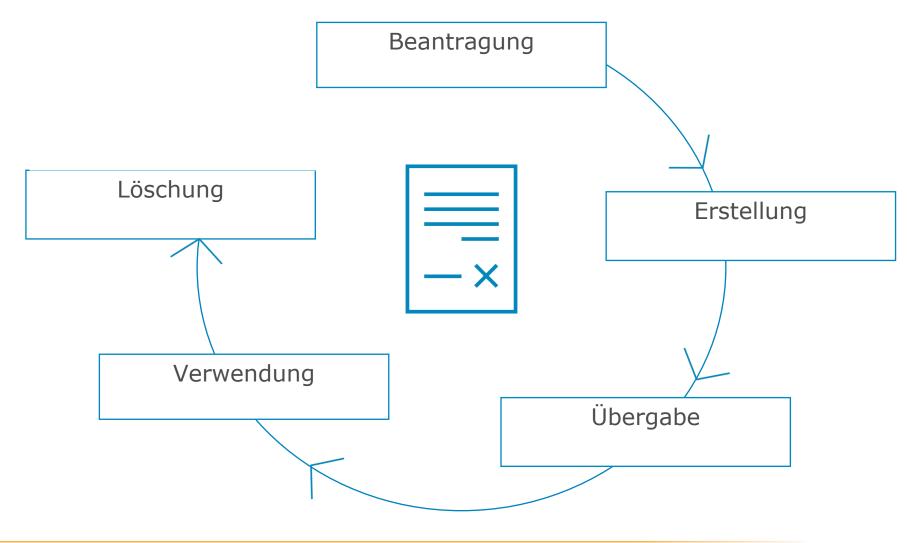
Verweis

Originaldokumente +

National Statement

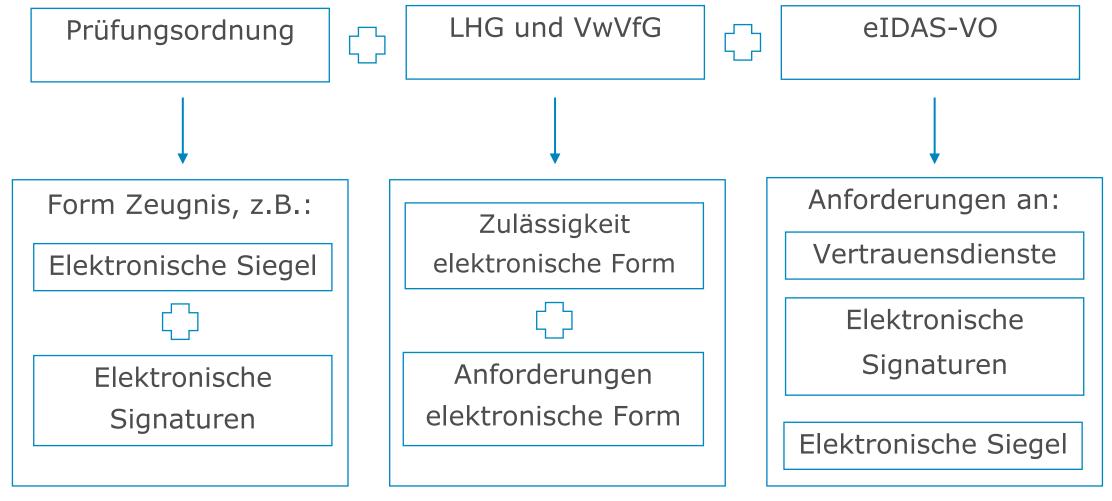
Lebenszyklus eines elektronischen Hochschulzeugnisses





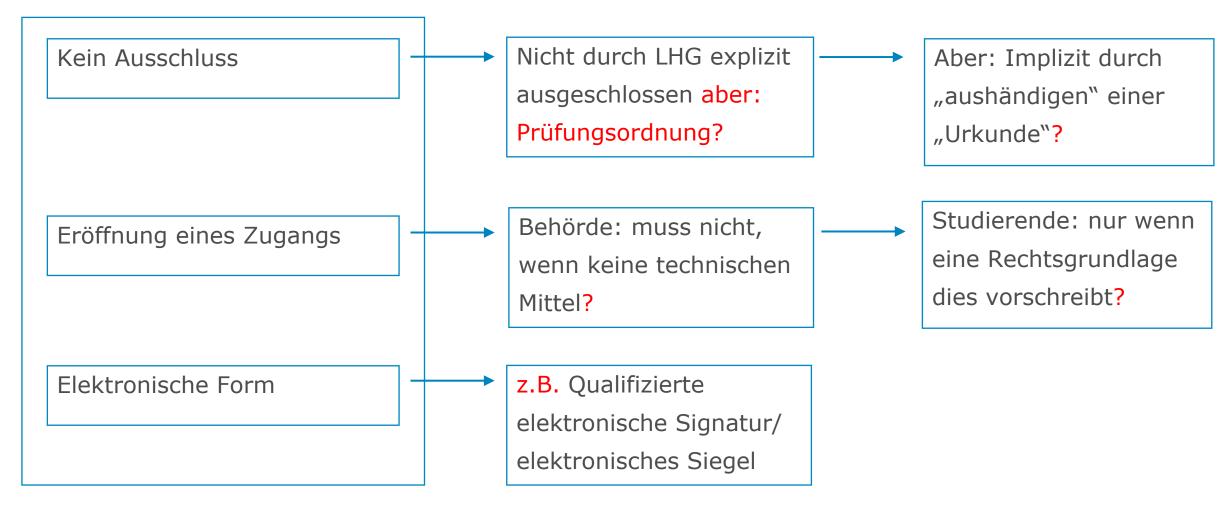
Rechtliche Anforderungen digitale Zeugnisse





Ausstellung digitaler Zeugnisse nach § 3a VwVfG





Qualifizierte Elektronische Signatur

Funktionsweise der elektronischen Signatur



3. Hash-Berechnung Verschlüsselung **Prüfung Versand** Dokument wird in Hash-Wert wird mit Dokument und Signatur mit Public Hashwert Private Key Signatur werden Key entschlüsseln umgewandelt verschlüsselt zusammen Hash-Wert des übersandt → Digitale Signatur **Dokuments** berechnen und vergleichen

Arten der elektronischen Signatur



Elektronische Signatur

Fortgeschrittene e.S.

Qualifizierte e.S.







Elektronische Signaturen (Art. 3 eIDAS-VO)



Elektronische Signatur

Daten in elektronischer

Logisch mit anderen Daten verbunden

Unterzeichner:in verwendet sie zum Unterzeichnen

Fortgeschrittene e.S.

Elektronische Signatur

Eindeutig Unterzeichner:in zugeordnet

Ermöglicht Identifizierung der Unterzeichner:in

Erstellt mit elektronischen Signaturerstellungsdaten

Mit unterzeichneten Daten so verbunden, dass nachträgliche Veränderung erkennbar ist

Qualifizierte e.S.

Fortgeschrittene Elektronische Signatur

Von qualifizierten elektronischer Signaturerstellungseinheit (Soft- o. Hardware) erstellt

Beruht auf qualifiziertem Zertifikat für elektronische Signaturen

Form

Qualifizierte elektronische Signatur

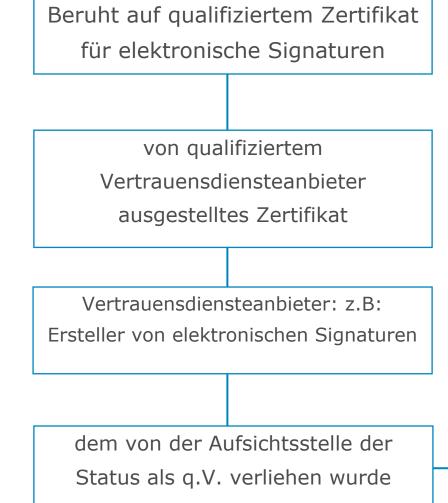


Von qualifizierter elektronischer Erstellungseinheit erstellt



konfigurierte Software oder Hardware die Anforderung aus Anhang II erfüllt

Vertraulichkeit der
Signaturerstellungsdaten,
Einmaligkeit der
Signaturerstellungsdaten,
Cybersicherheit etc.



das Anhang I
erfüllt, z.B.:
Pseudonym des
Unterzeichners,
Gültigkeitsdauer
des Zertifikats etc.

in DE: Bundesnetzagentur

Unterschied elektronische Signaturen und Siegel



Elektronische Signatur

Elektronisches Siegel

Ausstellerin: natürliche Person

Willenserklärung

Ersetzt handschriftliche Unterschrift Ausstellerin: juristische Person

Herkunftsnachweis

Ersetzt Behördensiegel (oder Unternehmenstempel)

Kombination möglich

Elektronisches Siegel

DFN

Elektronische Siegel

Daten in elektronischer Form

Logisch mit anderen Daten verbunden

Um Ursprung und Unversehrtheit der Daten sicherzustellen

Fortgeschrittenes e.S.

Elektronische Siegel

Eindeutig Siegelersteller:in zugeordnet

Ermöglicht Identifizierung der Siegelersteller:in

Erstellt mit elektronischen Sigelerstellungsdaten

Mit unterzeichneten Daten so verbunden, dass nachträgliche Veränderung erkennbar ist

Qualifiziertes e.S.

Fortgeschrittenes Elektronisches Siegel

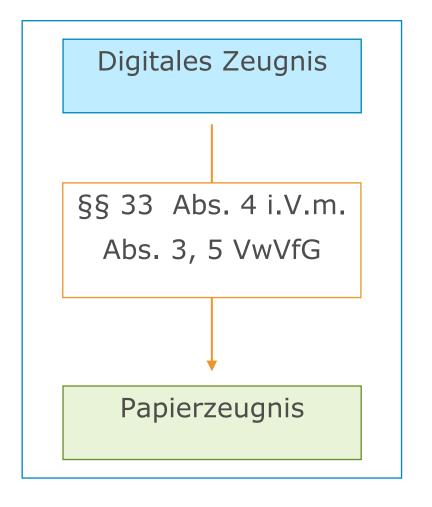
Von qualifizierten elektronischer Siegelerstellungseinheit (Soft- o. Hardware) erstellt

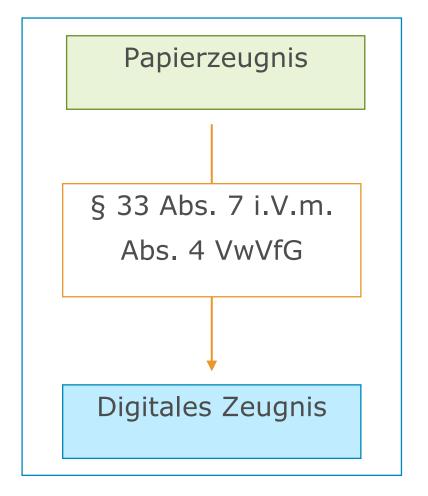
Beruht auf qualifiziertem Zertifikat für elektronische Siegel

Umwandlung von Hochschulzeugnissen

"Umwandlung" von Zeugnissen nach § 33 LVwVfG (Beglaubigung von Abschriften)







Schriftliche Beglaubigung eines digitalen Zeugnisses



§ 33 Abs. 3 VwVfG



§ 33 Abs. 5 VwVfG

Genaue Bezeichnung des Schriftstücks

Feststellung: beglaubigte Abschrift stimmt mit vorgelegtem Schriftstück überein

Ort u. Tag Beglaubigung, Unterschrift zuständigen Bediensteten und Dienstsiegel

Hinweis: Beglaubigte Abschrift nur zur Vorlage bei der angegebenen Behörde, wenn nicht von Behörde ausgestellt

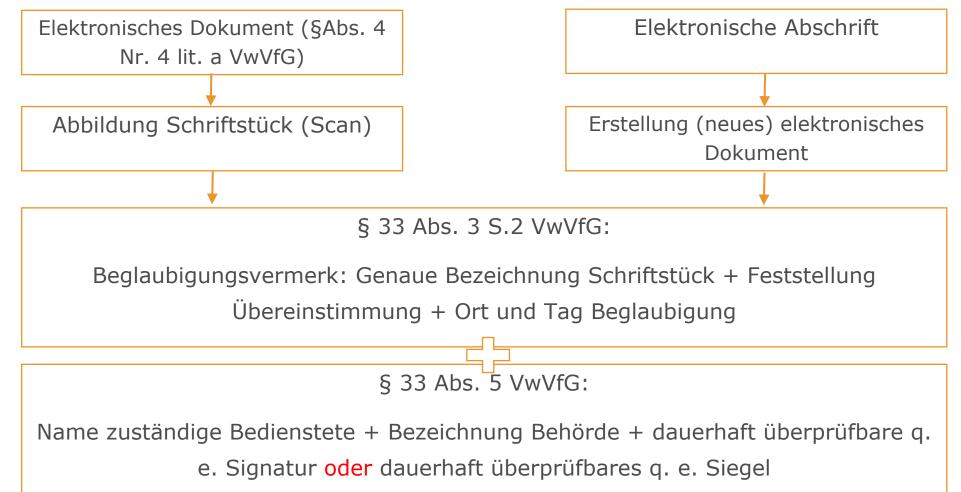
Wen die Signaturprüfung als Inhaber der Signatur oder des Siegels ausweist

Zeitpunkt Signaturprüfung für die Anbringung der Signatur oder des Siegels

Welche Zertifikate mit welchen Daten Signatur oder Siegel zu Grunde lagen

Ablauf digitale Beglaubigung Papierzeugnis (Alternativen nach § 33 Abs. 7 LVwVfG)





Digitale Ausstellung eines Papierzeugnisses



§ 33 Abs. 7 VwVfG

Selbst ausgestellte Urkunde Antrag Zeugnisinhaber:in notwendig "Auf Verlangen" Elektronisches Dokument oder elektronische §§ 33 Abs. 4 Nr. 4 lit. a VwVfG Abschrift Ausfertigen und beglaubigen

Handlungsmöglichkeiten für Hochschulen

Handlungsmöglichkeiten



1

Digitales Zeugnis

Papierzeugnis **2**.

Papierzeugnis

Auf Antrag:

Digitales Zeugnis 3.

Digitales Zeugnis

Auf Antrag:

Papierzeugnis

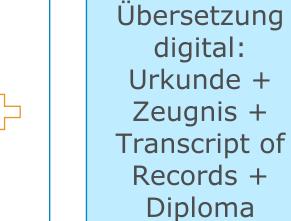
Weitere Handlungsmöglichkeiten



Papierurkunde



Digitales
Zeugnis,
Transcript of
Records,
Diploma
Supplement



Weitere
Kombinationen je
nach
Prüfungsordnung
möglich

Englische

Supplement

Haben Sie noch Fragen?

DFN

► Kontakt

Forschungsstelle Recht im DFN

E-Mail: recht@dfn.de

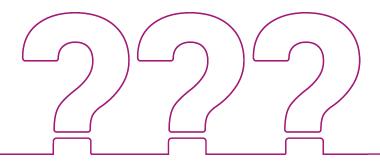
Telefon: 0251 83 - 38616/ 030 2093-91443

Anschrift:
Forschungsstelle Recht im DFN
Humboldt-Universität zu Berlin
Unter den Linden 11
10117 Berlin

Philipp Schöbel

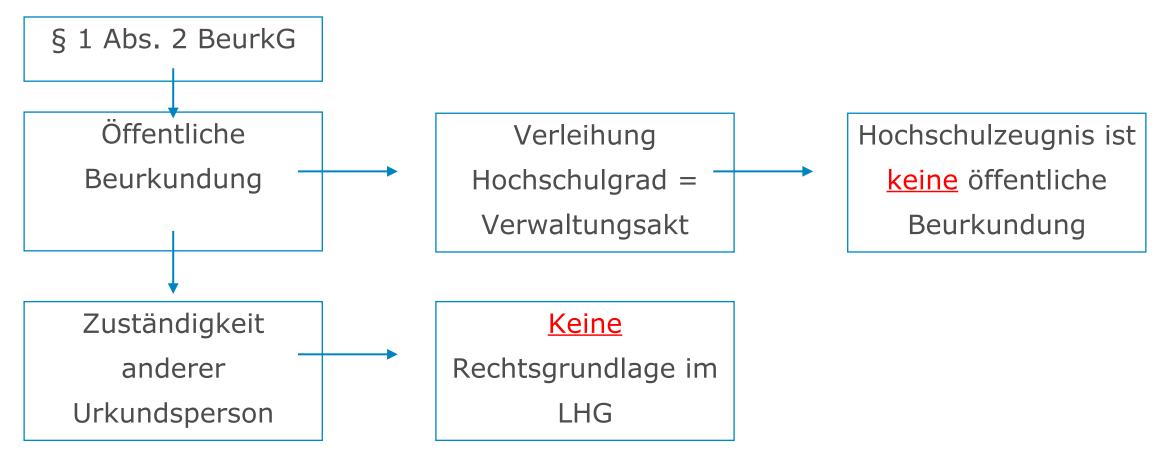
E-Mail: philipp.manuel.schoebel@hu-berlin.de

Telefon: 030 2093-91443



Keine Anwendbarkeit des BeurkG für Hochschulzeugnisse





Arten qualifizierte elektronische Signatur: Unterschiede

Signatur	mit	lokalem	Zertifikat
----------	-----	---------	------------

Fernsignatur (Remotesignatur)

Speicherort Schlüssel

Smartcard/USB-Token beim Nutzer

Hardware-Sicherheitsmodul beim Vertrauensdiensteanbieter

Hard- und Softwarebedarf Kartenleser, ggf. spezielle Software

Keine spezielle Hardware beim Nutzer

Kontrolle über Schlüssel Nutzer direkt

Vertrauensdiensteanbieter verwaltet Schlüssel, Nutzer autorisiert

Signaturerstellung

Lokal auf Nutzergerät

Zentral auf Server des Vertrauensdiensteanbieters

Authentifizierung

i. d. R. PIN am Gerät

Zwei-Faktor-Authentifizierung (z. B. App, SMS)

Referenzstandards, Spezifikationen und Verfahren für fortgeschrittene elektronische Signaturen nach Art. 26 Abs. 2 eIDAS



Kommission bewertet: Braucht Wenn ja, dann Erlass per es Referenzstandards, Durchführungsrechtsakt Spezifikationen und Verfahren? durch Kommission Vermutung Einhaltung Einhaltung der festgelegten Wenn ja, dann der gesetzlichen Referenzstandards, Anforderungen Spezifikationen und Verfahren?

Die EUDI-Wallet nach Art. 5a eIDAS



Rechtliche Anforderungen an die Wallets der Mitgliedstaaten

Bereitstellung

Unmittelbar vom Mitgliedstaat

Im Auftrag Mitgliedstaat

Unabhängig, aber vom Mitgliedstaat anerkannt

Quellcode Open-Source-Lizenz

Ausnahme möglich:

Für bestimmte Komponenten und

"hinreichend begründete Fälle" Vorgeschrieben Funktionen u.a.:

Elektronische Attributsbescheinigungen

Pseudonyme generieren und speichern

Unterzeichnen mit q.e. Signaturen oder Siegeln

Vorgeschriebene Funktionen der EUDI-Wallet



Art. 5a eIDAS

Anfordern, Speichern, Löschen Bescheinigungen Pseudonyme generieren und speichern

Unterzeichnen mit q.e. Signaturen oder Siegeln

sichere Authentifizierung mit anderen Personen Zugang zur internen Protokollierung Download Nutzerdaten u. Attributsbescheinigungen

Recht auf Datenportabilität

Interaktionen zwischen EUDI-Wallets

Löschung personenbezogener Daten

Zustellung elektronischer Hochschulzeugnisse



§ 5 Abs. 5 VwZG



§ 5 Abs. 6 VwZG

Eröffnung Zugang Empfänger:in

Qualifizierte elektronische Signatur

Schutz Kenntnisnahme Dritter

Absendende Behörde

Name und Anschrift Adressat:in

Name übermittelnde Bedienstete