



Digitale Signaturen

Sprechstunde am 26.01.2023

Ein Kooperationsvorhaben empfohlen durch die:



INNOVATION DURCH KOOPERATION

Gefördert durch

Ministerium für
Kultur und Wissenschaft
des Landes Nordrhein-Westfalen



Wozu sind „digitale“ oder „elektronische“ Signaturen gut?

Einordnung:

Ersetzung der gesetzlich vorgesehenen Schriftform durch die elektronische Form, vgl. **§§ 126 Abs. 1 u. 3, 126a BGB**:
„Die schriftliche Form kann durch die elektronische Form ersetzt werden, wenn sich nicht aus dem Gesetz ein anderes ergibt.“

Hintergrund:

Im Zivilrechtsverkehr gilt der **Grundsatz der Formfreiheit** für Willenserklärungen.

Das bedeutet: In der Regel ist für den Abschluss von Verträgen oder die Abgabe anderweitiger Willenserklärungen gar **keine Schriftform** erforderlich!

Ausnahmen:

Mietverträge mit Laufzeit über 1 Jahr (§ 550 BGB), Kündigung von Arbeitsverträgen/Aufhebungsverträge (§ 623 BGB), Öffentlich-rechtliche Verträge (§ 54 VwVfG NRW), ausdrückliche Parteivereinbarungen usw.

Dennoch bietet die Schriftform in der Praxis für Vertragspartner:innen wesentliche Vorteile.

- **Nachweisbarkeit** wichtiger (Vertrags-)Bestandteile
- **Dokumentation** des Inhalts
- **Beweiswert** vor Gericht hinsichtlich der Person des/r Vertragspartner:in und bezüglich der Echtheit des (Vertrags-)Inhalts
- Vermutung der **Vollständigkeit und Richtigkeit** unterzeichneter Vertragsurkunden

Bei der Nutzung von digitalen Signaturen im Rahmen des elektronischen Geschäftsverkehrs werden insbesondere **vertrags-, beweis- und datenschutzrechtliche Aspekte** tangiert. Somit gehen mit der Nutzung derartiger Signaturen unterschiedliche Herausforderungen in tatsächlicher und rechtlicher Hinsicht einher.

Rechtlicher Rahmen:

- EU-Verordnung Nr. 910/2014 über elektronische Identifizierung Vertrauensdienste für elektronische Transaktionen im Binnenmarkt (= **eIDAS-VO**)
- **§§ 126, 126a BGB**

Die 3 Signaturstufen im Überblick

Einfach elektronisch	Fortgeschritten elektronisch	Qualifiziert elektronisch
<p>Darunter fallen elektronische Daten, die anderen Daten beigefügt oder logisch mit diesen verbunden werden und von dem/r Verwender:in zur Unterzeichnung genutzt werden.</p> <p>Bsp. Eingescannte Unterschrift; eine mit Namen unterzeichnete E-Mail</p> <p>Art. 3 Nr. 10 eIDAS-VO</p>	<p>Hierbei handelt es sich um eine unter Verwendung elektronischer Signaturerstellungsdaten* hergestellte Unterschrift, die eine eindeutige Zuordnung zum/r Unterzeichner:in, sowie dessen/deren Identifizierung ermöglicht.</p> <p>Darüber hinaus lässt die fortgeschrittene elektronische Signatur nachträgliche Veränderungen an den Daten erkennen.</p> <p>Bsp. Installiertes Software-Zertifikat</p> <p>Art. 3 Nr. 11 i.V.m. Art. 26 eIDAS-VO</p> <p><small>*Art. 3 Nr. 13 eIDAS-VO: Eindeutige Daten, die von Unterzeichner:in zum Erstellen einer elektronischen Signatur verwendet werden.</small></p>	<p>Die qualifiziert elektronische Signatur zeichnet sich dadurch aus, dass diese einerseits von einer qualifizierten elektronischen Signatureinheit* erstellt wurde und weiterhin auf einem elektronischen Signaturzertifikat staatlich anerkannter Anbieter:innen basiert.</p> <p>Art. 3 Nr. 12 eIDAS-VO</p> <p>Diese Signaturart bietet durch die doppelte Verifizierung & Identifikation den höchsten Sicherheitsstandard!</p> <p>Bsp. beA</p> <p><small>*Qualifiziert elektronische Signatureinheit, Art. 3 Nr. 31 eIDAS-VO (wie z.B eine Signaturkarte mit Lesegerät)</small></p>

Funktionsweise

Einfach elektronisch	Fortgeschritten elektronisch	Qualifiziert elektronisch
<p>Maschinenschriftliche Herstellung durch Unterzeichner:in selbst</p>	<p>DFN-Zertifikat</p> <p>Der DFN-Verein organisiert mit dem Dienst DFN-PKI eine Public Key Infrastruktur, um digitale Zertifikate auszustellen, zu verteilen und zu prüfen. Dabei werden fortgeschrittene Zertifikate auf Basis des X.509 Standards verwendet und für eine sichere Kommunikation (zwischen Hochschulen) bereitgestellt.</p>	<p>1. Chipkarte & Lesegerät</p> <ul style="list-style-type: none">• Chipkarte bzw. Hardware enthält den persönlichen Schlüssel• Schlüssel ist durch Wissen (PIN) & Besitz geschützt <p>2. Fernsignatur</p> <ul style="list-style-type: none">• Vertrauensdiensteanbieter erstellt im Auftrag für Nutzer:innen die Signatur• Keine zusätzliche Soft- oder Hardware erforderlich• 2-Faktor-Sicherheit <p>Nur bei dieser Signatur kann eine gesetzlich angeordnete Schriftform durch die elektronische Form wirksam ersetzt werden, vgl. § 126a BGB!</p>

Vor- & Nachteile, sowie Signaturniveaus

Praktikabilität, Effizienz & Nachhaltigkeit, Schnelligkeit der (Vertrags-) abwicklung

	Einfach elektronisch	Fortgeschritten elektronisch	Qualifiziert elektronisch
Zuordnung & Identifizierung	Nein. (Manipulationsgefahr)	Ja. Einmalig bei der Ausstellung.	Ja. Bei jeder Transaktion.
Schriftformersatz	Nein	Nein	Ja! Sofern elektronische Form gesetzlich nicht ausgeschlossen.
Authentifizierung	Nein	Ja. Allerdings keine besonderen Anforderungen an Verschlüsselungstechnik.	Ja. Weitreichende Sicherheitsanforderungen.
Transparenz nachträglicher Veränderungen	Nein	Ja	Ja
Zeitliche Befristung	Nein	Ja	Ja
Kontrolle durch Dritte (Vertrauensdiensteanbieter i.S.v. Art. 3 Nr. 19 eIDAS-VO)	Nein	Ja	Ja

	Einfach elektronisch	Fortgeschritten elektronisch	Qualifiziert elektronisch
Prozessuale Beweiskraft	Sehr niedrig	Im mittleren Bereich	Sehr hoch
	<ul style="list-style-type: none"> Echtheit des Dokuments Abgabe der Erklärung von dem/r Aussteller:in <p>unterliegen:</p> <p>Freier richterlicher Beweiswürdigung gemäß § 286 ZPO</p>	<ul style="list-style-type: none"> Echtheit des Dokuments Abgabe der Erklärung von dem/r Aussteller:in <p>unterliegen:</p> <p>Freier richterlicher Beweiswürdigung gemäß § 286 ZPO</p>	<p>Sofern das Gericht eine erfolgreiche Signaturprüfung vorgenommen hat:</p> <p>Voller Beweis dafür, dass die inhaltliche Erklärung von dem/r Aussteller:in des Dokuments abgegeben wurde</p> <p>= Anscheinsbeweis der Echtheit (§§ 371a, 416 ZPO)</p>

Nutzungsmöglichkeiten und -empfehlungen

1. Wie entscheide ich mich für die „richtige“ Signaturart? Durch Abwägung der wesentlichen Faktoren...
 - **Besteht ein Schriftformerfordernis?** (Dann ist lediglich die qualifiziert elektronische Signatur geeignet)
 - **Vorgaben von/Vereinbarungen mit Vertragspartner:innen oder Förderern?**
 - **Wie ist meine Einrichtung finanziell aufgestellt? Bestehendes Budget für elektronischen Rechtsverkehr?**
 - **Wie hoch ist das Risiko eines Rechtsstreits?** (Dies hängt u.a. von Vertragspartner:in und Gegenstand der Erklärung ab)
 - **Welches wirtschaftliche Risiko kann ich im Rahmen eines Rechtsstreites tragen?**

2. Einsatzmöglichkeiten:
 - a. **Fortgeschritten elektronische** Signatur: Insb. für hochschulinterne Prozesse geeignet (in pdf-Formulare einpflegen)
 - b. **Qualifiziert elektronische** Signatur:
 - Relevant für rechtliche Erklärungen, welche gerichtlich bedeutend sein können
 - Zwingend bei bestehendem Schriftformerfordernis! Ansonsten: Rechtsfolge der Formnichtigkeit, **§ 125 BGB**

Fazit:

Die Entscheidung sollte individuell aufgrund einer Abwägung der Praktikabilität bei gleichzeitiger Rechtssicherheit erfolgen!

Quellen

- FH MÜNSTER, Buddemeier/Rieke/Welp-Dasenbrock: Elektronische Signaturen – eine erste Annäherung, Stand: 14.11.22
- Voigt/Herrmann/Danz: Die elektronische Signatur und ihre Einsatzmöglichkeiten für digitale Vertragsschlüsse, NJW 2020, 2991, Stand: 02.01.23
- 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**)
- <https://www.pki.dfn.de/ueberblick-dfn-pki>

Kommende Veranstaltungen

- **09.02.23**, 14 Uhr: Offene Sprechstunde
- **23.02.23**, 11 Uhr: Sprechstunde zu dem Projekt AuROA – Autor:innen und Rechtssicherheit für Open Access
- **09.03.23**, 14 Uhr: Offene Sprechstunde

Kontakt Landesinitiative openaccess.nrw

openaccess.nrw@uni-due.org

- Dr. Miriam Kötter (Projektleitung): miriam.koetter@uni-due.de
- Nadine Schlimok (Projektassistenz): nadine.schlimok@uni-due.de
- Isabelle Aydin (Juristische Beratung): isabelle.aydin@uni-due.de