deutsches forschungsnetz

# Technische und rechtliche Aspekte bei Dokumentensignaturen

Ralf Gröper

November 2022

# Worum geht es?

- Dokumentensignatur
  - i.d.R. PDF-Dokumente, aber auch andere Datenstrukturen
  - Alles, was derzeit auf Papier existiert und in irgendeiner Form unterschrieben oder gesiegelt wird und digitalisiert werden soll
    - Z.B. Abschlusszeugnisse, Arbeitsverträge, Promotionsurkunden, mitbestimmungspflichtige Vorgänge (Personalrat),…

- Es geht nicht um:
  - E-Mailsignatur (zumindest in der Mehrzahl der Anwendungsfälle)
  - Client-Authentisierung
  - Verschlüsselung

# Rechtliche Aspekte

## Welche Möglichkeiten?

- Einfache Signatur
- Fortgeschrittene Signatur
- Qualifizierte Signatur

## Rechtliche Grundlage?

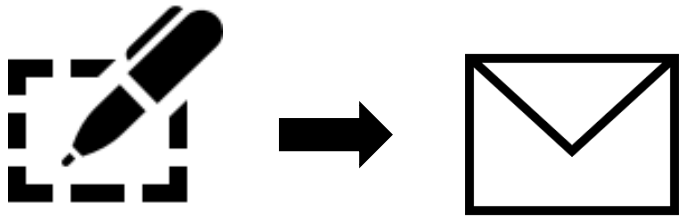
eIDAS-VO (VO (EU) 910/2014)

# Einfache Signatur

- Art. 3 Nr. 10 eIDAS: „Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet.“ (das war‘s!)

- Ersteller der Signatur wird **nicht persönlich identifiziert**
- **Kein Zertifikat notwendig**, „nackter“ Signaturschlüssel reicht auch

- Beweiskraft?

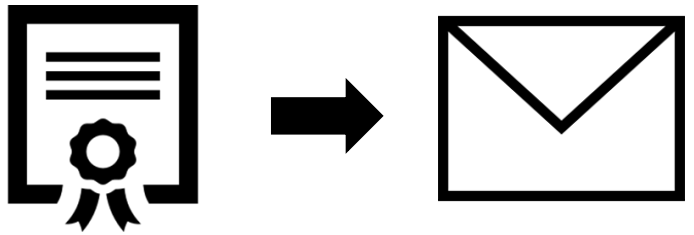


# Fortgeschrittene Signatur

- Art. 26 eIDAS: Eine fortgeschrittene elektronische Signatur erfüllt alle folgenden Anforderungen:
  a) Sie ist **eindeutig** dem Unterzeichner **zugeordnet**.
  b) Sie ermöglicht die **Identifizierung** des Unterzeichners.
  c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner **alleinigen Kontrolle** verwenden kann.
  d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung** der Daten erkannt werden kann.

- Eindeutige Zuordnung der Signatur zu Unterzeichnendem
  - Identifizierung der Person möglich

- Beweiskraft?



# Qualifizierte Signatur

- Art. 3 Nr. 12 eIDAS: „**fortgeschrittene elektronische Signatur**, die von einer **qualifizierten elektronischen Signaturerstellungseinheit** erstellt wurde und auf einem **qualifizierten Zertifikat** für elektronische Signaturen beruht“
  - Weitere Ausdetaillierung der Anforderungen in Anhängen I – IV eIDAS
- Rechtswirkung wie eine handschriftliche Unterschrift
  - Wann erforderlich?
- Beweiskraft?

# Vergleich der Signatur-Arten

| | Einfache elektronische Signatur (EES) | Fortgeschrittene elektronische Signatur (FES) | Qualifizierte elektronische Signatur (QES) |
|---|---|---|---|
| Beweiskraft | niedrig | hoch | sehr hoch |
| Anwendung | Dokumente ohne gesetzliche Formvorschrift mit geringem Haftungsrisiko | Dokumente ohne gesetzliche Formvorschrift mit kalkulierbarem Haftungsrisiko | Dokumente mit gesetzlicher Formvorschrift und/oder hohem Haftungsrisiko |
| Vertrauen & Sicherheit | Geringe Sicherheit bei der Identität und einfache Signaturauslösung | Identität geprüft anhand eines offiziellen Identitätsdokuments | Identität geprüft durch autorisierte Stelle, Signaturauslösung mit 2FA, nach eIDAS handschriftlicher Unterschrift gleichgestellt |

# Elektronische Siegel

## Welche Möglichkeiten?

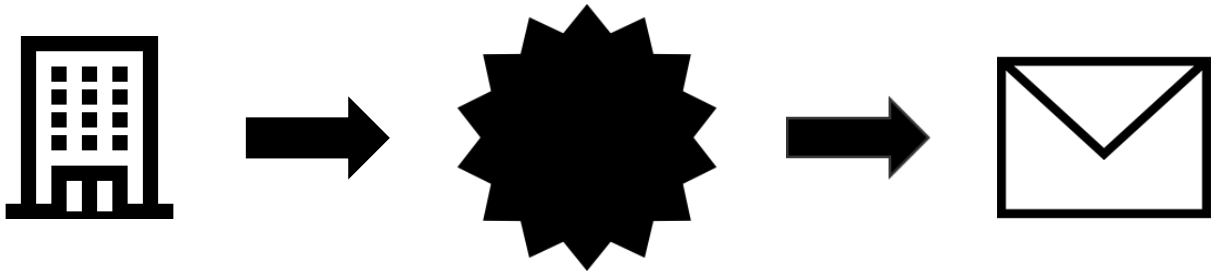
- Einfache Siegel
- Fortgeschrittene Siegel
- Qualifizierte Siegel

## Rechtliche Grundlage?

eIDAS-VO (VO (EU) 910/2014)

# Unterschied zwischen Signatur und Siegel

- Bei der Signatur = natürliche Person als Unterzeichner
- Bei Siegel = juristische Person als Unterzeichner
- Siegel = digitaler Stempel einer Organisation zur Bestätigung der Echtheit des Dokuments



# Technische Aspekte

# Kontrolle des privaten Schlüssels

## Welche Möglichkeiten?

Privater Schlüssel beim Signierenden

Für qualifizierte Signaturen „sichere Signaturerstellungseinheit“ notwendig

Remotesignatur Privater Schlüssel bei Drittem

In eIDAS explizit vorgesehen - starke Authentisierung beim Signaturersteller notwendig!

## Welche Möglichkeiten?

Signatur als atomarer Prozessschritt

Know-How beim Signaturersteller notwendig

Signatur als Teil eines komplexen Workflows

Unterstützung in Workflow-Software notwendig (z.B. Studierendenverwaltung, HISinOne)

# Welche Möglichkeiten?

DFN-PKI „Global“

Durch DFN-Verein betriebene PKI
Läuft Mitte kommenden Jahres aus!

DFN-PKI „TCS“

Ablösung DFN-PKI „Global“
Von GÉANT ausgeschrieben, kommerzieller Vertrauensdiensteanbieter (derzeit: Sectigo)

# Elektronische Signaturen in der DFN-PKI

- **Einfache Signaturen** sind (trivialerweise) mit allen Zertifikaten aus der DFN-PKI möglich
- **Qualifizierte Signaturen** sind derzeit kein Leistungsbestandteil der DFN-PKI
- Und was ist mit **fortgeschrittene Signaturen**…?
  - Dazu müssen wir in die Details schauen!

# Fortgeschrittene Signaturen in der DFN-PKI

- Erinnerung: 4 Anforderungen an eine fortgeschrittene elektronische Signatur aus eIDAS:
  a) Sie ist **eindeutig** dem Unterzeichner **zugeordnet**.
  b) Sie ermöglicht die **Identifizierung** des Unterzeichners.
  c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner **alleinigen Kontrolle** verwenden kann.
  d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung** der Daten erkannt werden kann.

# Fortgeschrittene Signaturen in der DFN-PKI

a) Sie ist **eindeutig** dem Unterzeichner **zugeordnet**.

- Alle Sicherheitsniveaus der DFN-PKI bieten Zertifikate an, in denen die eindeutige Zuordnung möglich ist durch die Kombination von **Name**, **Organisationszugehörigkeit** und **E-Mailadresse**

# Fortgeschrittene Signaturen in der DFN-PKI

b) Sie ermöglicht die **Identifizierung** des Unterzeichners.

- DFN-PKI „Global“ hat **umfangreiche Anforderungen** an Durchführung und Dokumentation der Identifizierung
  - Organisationen und Personen, die mit fortgeschrittenen Signaturen in „Global“ arbeiten, können die korrekte Identifizierung im Streitfall nachweisen (sofern sie sich an die Vorgaben der Policy der DFN-PKI „Global“ halten)

- DFN-PKI „TCS“ fordert ebenfalls eine geeignete Identifizierung, es gibt aber **keinerlei Anforderungen** an die Durchführung und Dokumentation der Identifizierung
  - Organisationen und Personen, die mit fortgeschrittenen Signaturen in TCS arbeiten, müssen darauf vorbereitet sein, dass sie diese Eigenschaften im Streitfall ggf. anhand **eigener Unterlagen** nachweisen müssen

# Fortgeschrittene Signaturen in der DFN-PKI

c) Sie wird unter Verwendung elektronischer Signaturerstellungsdaten erstellt, die der Unterzeichner mit einem hohen Maß an Vertrauen unter seiner **alleinigen Kontrolle** verwenden kann.

d) Sie ist so mit den auf diese Weise unterzeichneten Daten verbunden, dass eine **nachträgliche Veränderung** der Daten erkannt werden kann.

- Diese Anforderungen liegen außerhalb des Kontrollbereichs des Vertrauensdienste-Anbieters bzw. der CA und damit der DFN-PKI
  - Organisation und Personen müssen darauf vorbereitet sein, dass sie diese Eigenschaften im Streitfall anhand **eigener Unterlagen** nachweisen können

# Fortgeschrittene Signaturen in der DFN-PKI

- Es ist also mit Zertifikaten aus der DFN-PKI **grundsätzlich** möglich, fortgeschrittene Signaturen zu erstellen

- Die Organisation bzw. der Unterzeichner müssen dafür sorgen, dass im Streitfall alle vier Anforderung der eIDAS **nachgewiesen** werden können
  - Die DFN-PKI verfügt **nicht** zentral über alle Nachweise!
  - Dies erfordert **lokale** Dokumentationen und Nachweise, die im Streitfall als Beweisstücke dienen