

Live-Webinar



„Datensouverän signieren mit Karte oder Fernsignatur“



Referent: Frank Lüneburg, Senior Key Account Manager

Berlin, November 2020

Inhalt

© secrypt GmbH 2020

Was Sie in den nächsten 30 Minuten erwartet:

1. Die secrypt GmbH
2. Überblick: Elektronische Signatur und rechtlicher Rahmen
3. Datensouveränität
4. Live-Demo:
Datensouverän signieren (beispielhaft mit qualifiziertem Zertifikat)
 - a) mit Signaturkarte
 - b) per Fernsignatur mittels Smartphone (ohne Signaturkarte)

secrypt im Überblick

© secrypt GmbH 2020

- **2002** gegründet mit Sitz in Berlin
- **Kernkompetenzen:**
Produkte, Lösungen und Beratung rund um die Themen
E-Signatur, E-Siegel, Zeitstempel und Verschlüsselung
- **Ziele:**
Gewährleistung von Authentizität, Manipulationsschutz und Vertraulichkeit für sichere,
effiziente und beschleunigte elektronische Geschäftsprozesse
- **Gesetzeskonformität:**
eIDAS-VO, Vertrauensdienstegesetz (VDA)
- **Mitgliedschaften:**
BITKOM, CCESigG, PDF/A Competence Center, TeleTrusT, Verband Sichere Digitale
Identität (VSDI)



secrypt im Überblick

© secrypt GmbH 2020

Unser Anspruch

- Entwicklung von Produkten mit denen der gesamten **Signatur-Lebenszyklus**, von der Signaturerzeugung in allen relevanten Signaturformaten, über die Signaturanreicherung und Signaturverifikation bis hin zur Beweiswerterhaltung abgedeckt werden kann.



- Komfortable und regelkonforme Einbindung der digiSeal® Produktfamilie in die prozessführende Applikation
- Anwendung und Umsetzung von anerkannten Standards
- Umsetzung von pragmatischen Signatur-Lösungen im Rahmen der Vorgaben

Rechtlicher Rahmen - Beweiswert - Datensouveränität

© secrypt GmbH 2020

E-Signatur = Die Unterschrift in der digitalen Welt

- Sie weist den Urheber sicher nach (Authentizität)
- Sie schützt das Dokument vor Manipulationen (Integrität)
- Sie ist beweiskräftig
- Sie basiert auf sehr starken State-of-the-Art Kryptografieverfahren (RSA, elliptische Kurven)
- Sie ist von unabhängigen Dritten prüfbar und nachvollziehbar



Rechtlicher Rahmen - Beweiswert - Datensouveränität

© secrypt GmbH 2020

Digitale Zertifikate

- Der angestrebte digitale Beweiswert von digitalen Dokumenten und Daten hängt wesentlich von der Art und dem Aussteller der verwendeten digitalen Zertifikates ab.
- Das digitale Zertifikat ist ein Datensatz, der definierte Eigenschaften von Personen oder Objekten bestätigt und dessen Authentizität und Integrität durch kryptografische Verfahren geprüft werden kann.
- Die Verwendung von digitalen Zertifikaten, die von einem qualifizierten Vertrauensdiensteanbietern (VDA) ausgestellt wurden, ist die Basis für den höchstmöglichen digitalen Beweiswert.

Rechtlicher Rahmen - Beweiswert - Datensouveränität

© secrypt GmbH 2020

Formen der elektronischen Signatur (fortgeschritten und qualifiziert)

- Fortgeschrittene elektronische Signatur / Siegelung
 - Signatur / Siegelung mittels Softzertifikat (Softtoken)

- Die „qualifizierte“ elektronische Signatur durch eine natürliche Person
 - Die qualifizierte elektronische Signatur ersetzt die per Gesetz geforderte Schriftform auf Papier (nach § 126 BGB) und ist damit gleichgestellt mit der eigenhändigen Unterschrift
 - Gesetzeskonform gemäß EU-Verordnung und Vertrauensdienstegesetz (VDG)

- Das „qualifizierte“ elektronische Siegel durch eine juristische Person (Organisation)
 - Rechtlich besitzt das qualifizierte Siegel einen sehr hohen Beweiswert („Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten“ (Art. 35 Abs. 2 eIDAS-VO))

Rechtlicher Rahmen - Beweiswert - Datensouveränität

© secrypt GmbH 2020

Einsatz auf Grundlage der Vorgaben des Gesetzgebers

- Schriftformerfordernis, Elektronische Rechnungen
- Arbeitnehmerüberlassungsverträge
- Vollständigkeitsangaben, Abfallnachweisdokumente
- Dokumentation im Gesundheitswesen
- ...



Digitales hochwertiges Beweismittel für geschäftskritische Unterlagen

- Hochdotierte Verträge (eigentlich formfrei)
- Nachweisdokumente mit hohem Haftungsrisiko
- Compliance-Unterlagen
- QM-Dokumentation
- ...



Rechtlicher Rahmen - Beweiswert - Datensouveränität

© secrypt GmbH 2020

Datensouveränität

- Bei den digiSeal® Komponenten handelt es sich um "On-Premise-Signatursoftware", die direkt beim Anwender oder im hausinternen Rechenzentrum installiert und betrieben sowie von der internen IT, administrativ betreuet wird.
- Da die Signaturfunktionalitäten vor Ort vorhanden sind, bleiben die Dokumente beim Anwender und werden zum Signieren in keine externe Cloud übertragen, womit die Datensouveränität unmittelbar und nachvollziehbar gewährleistet ist. Auch kann lokale Hardware, wie Signatortokens, -karten und Kartenleser, problemlos genutzt werden, ggf. für "Offline"-Signaturszenarien.
- Selbst bei Verwendung der sign-me-Fernsignatur in Kombination mit einer geeigneten Software, wie digiSeal®office, werden keine Dokumente an den Online-Fernsignaturservice übermittelt, sondern nur anonyme Prüfsummen (Hash des Dokuments).

Rechtlicher Rahmen - Beweiswert - Datensouveränität

© secrypt GmbH 2020

Multifaktorauthentifizierung / Benutzerverwaltung bei personenbezogener Signatur

- digiSeal® Komponenten sind Signaturanwendungskomponenten mit der beliebige Daten und Dokumente signiert werden können. Es ist vorab keine Authentifizierung des Users an der Signaturanwendungskomponente nötig. Die Nutzungssteuerung erfolgt über das Betriebssystem oder die prozessführende Applikation.
- Eine Authentifizierung der Person erfolgt bereits bei dem Erwerb bzw. bei der Beantragung des Signatur-Zertifikates. Nach der Zuteilung des Zertifikates ist eine eindeutige Authentifizierung der Person über "Besitz" (Besitz des Zertifikates) und "Wissen" (Kenntnis des Passwortes oder des Pins) gewährleistet.
- Aus diesem Grund ist eine Benutzerverwaltung in den digiSeal® Komponenten nicht nötig.

Rechtlicher Rahmen - Beweiswert - Datensouveränität

© secrypt GmbH 2020

Verfügbarkeit der Zertifikatsdaten im signierten Dokument

- Alle Daten zum Zertifikat sind auch nach der Signatur im Dokument verfügbar und überprüfbar.
- Die Originaldaten des Dokumentes werden mit der Signaturanwendungskomponente nicht verändert oder verwaltet.
- Bei den signierten Dokumenten handelt es sich um "frei transportfähige" Dokumente, bei denen die Signatur entsprechend internationalen Standards umgesetzt wurde. Eine Überprüfung bzw. Verifikation ist mit beliebigen Produkten (u.a. Acrobat Reader) möglich.

Notwendige Voraussetzungen für die E-Signatur

© secrypt GmbH 2020

Signatur mit Signaturkarte



- Digitales Zertifikat auf Signaturkarte
 - Identifizierung für qualifiziertes Signaturzertifikat (Postident)
- Kartenlesegerät
- Signatursoftware z.B. digiSeal®office

Fernsignatur mit Smartphone



- Digitales Zertifikat "hinterlegt" bei einem Vertrauensdiensteanbieter (sign-me Account)
 - Identifizierung für qualifiziertes sign-me Zertifikat (eID + AusweisApp oder über Videoident)
- Smartphone
- Signatursoftware z.B. digiSeal®office
- digiSeal®-Punkte zur Abrechnung der sign-me Signaturen

Live-Demonstration

© secrypt GmbH 2020



Live-Demo: „Qualifiziert“ elektronisch signieren

- a) mit Signaturkarte
- b) per Fernsignatur mittels Smartphone (ohne Signaturkarte)

Zusammenfassung - Vor- und Nachteile

© secrypt GmbH 2020

Signatur mit Signaturkarte



- Keine Kosten pro Signatur
- Keine Begrenzung der Signaturanzahl
- Auch "offline" möglich
- Nur eine Signatur-PIN zu merken



- „Spezial“-Hardware notwendig (Signaturkarte und Kartenleser)
- Lieferzeit der Signaturkarte 7 bis 14 Tage
- Postident

Fernsignatur mit Smartphone



- Nach ca. 30 Minuten nutzbar
- Schnelle Online-Identifizierung
- keine „Spezial“-Hardware nötig



- Kosten pro Signatur
- Smartphone notwendig
- Nur "online" möglich
- Benutzername und Passwort sowie mobile TAN pro Signatur via Smartphone

Vielen Dank!

© secrypt GmbH 2020

Sprechen Sie uns an, wir unterstützen Sie gern!

secrypt
e.signature solutions

Frank Lüneburg
Senior Account Manager

E-Mail: sales@secrypt.de
Telefon: +49 (30) 756 59 78-0
Internet: www.secrypt.de

