

Herzlich willkommen zum Live-Webinar



Elektronisches Siegel als digitaler Behörden- und Unternehmensstempel

Ursprung und Unversehrtheit von Dokumenten Ihrer Organisation
sicher nachweisen

Referent: Tatami M. Michalek, Geschäftsführer, secrypt GmbH
Berlin, 27. Mai 2020

Inhalt

© secrypt GmbH 2020

Was Sie in den nächsten maximal 30 Minuten erwartet:

1. Die secrypt GmbH
2. Überblick: Elektronisches Siegel und rechtlicher Rahmen
3. Sie erfahren, wie a) ein siegelberechtigter Personenkreis, z.B. in der öffentlichen Verwaltung, ein E-Siegel nutzt und b) wie Massenbelege automatisiert gesiegelt werden
4. Notwendige Komponenten und Bezugsquellen
5. Beispielhafte Anwendungsszenarien für unterschiedliche Branchen

secrypt im Überblick

© secrypt GmbH 2020

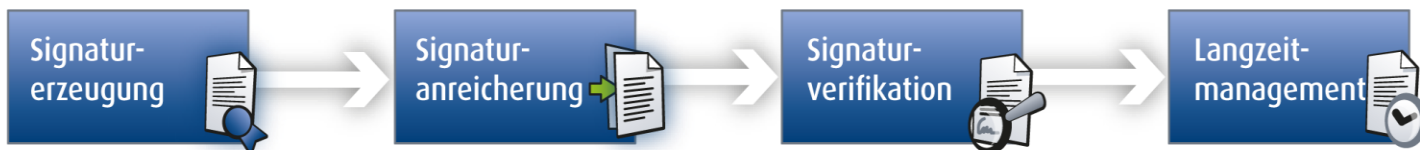
- **2002** gegründet mit Sitz in Berlin
- **Kernkompetenzen:** Produkte, Lösungen und Beratung rund um die Themen E-Signatur, E-Siegel, Zeitstempel und Verschlüsselung
- **Ziele:** Optimierung und Sicherung elektronischer Prozesse unter Gewährleistung von Authentizität, Manipulationsschutz und Vertraulichkeit digitaler Daten und Dokumente
- **Gesetzeskonformität:**
z.B. eIDAS-VO, deutsches Vertrauensdienstegesetz (VDG)



secrypt im Überblick

© secrypt GmbH 2020

Die digiSeal®-Softwarelösungen decken den gesamten Signatur-Lebenszyklus ab



EU-Verordnung eIDAS

© secrypt GmbH 2020



- Seit dem 01.07.2016 gilt in allen EU-Mitgliedsstaaten die „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt“.
- Vertrauensdienste: E-Signaturen, E-Siegel, Zeitstempel, elektronische Einschreiben, Website-Authentifizierungszertifikate, elektronische Bewahrungsdienste.
- Ziel: Einheitliche europäische Regelungen (rechtlich und technisch) und einheitlicher Umgang mit diesen Vertrauensdiensten im neu geschaffenen digitalen Binnenmarkt.
- Praxis: Gesiegelte und signierte Dokumente sind in allen EU-Staaten zu akzeptieren.
- EU-Vertrauenssiegel für eIDAS-konforme qualifizierte Vertrauensdiensteanbieter (VDA).
- VDAs sind in allen EU-Staaten zu akzeptieren.
- Die eIDAS-Verordnung ersetzt nationale Signaturgesetze, so auch das deutsche Signaturgesetz und die deutsche Signaturverordnung.
- Definition neuer Werkzeuge: z.B. E-Siegel für juristische Personen und Fernsignaturen, die Unterschriftsprozesse mittels Smartphone statt Signaturkarte ermöglichen sollen.

<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32014R0910>

E-Siegel und rechtlicher Rahmen

© secrypt GmbH 2020

- E-Siegel dienen als Nachweis, dass ein elektronisches Dokument von einer juristischen Person (GmbH, AöR etc.) ausgestellt wurde.
 - Sie belegen die Unversehrtheit (Integrität) und den Ursprung des Dokuments (Authentizität).
Achtung: Kein Ersatz für die handschriftliche Unterschrift!
 - Sie ist von unabhängigen Dritten prüfbar und nachvollziehbar.
 - Sie basiert auf sehr starken State-of-the-Art Kryptografieverfahren (RSA, elliptische Kurven).
 - Beweiswert & Rechtswirkung gemäß eIDAS Art. 35 (2):
Für ein qualifiziertes elektronisches Siegel gilt die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.
 - Ein Beweis auf Vermutungsbasis ist juristisch ein „scharfes Schwert“, denn er kann nur sehr schwer durch einen Gegenbeweis erschüttert werden.
- **Behördensiegel und Unternehmensstempel für das Internetzeitalter**



Motivation

© secrypt GmbH 2020

E-Siegel = Digitaler Stempel für Unternehmen und Organisationen der Privatwirtschaft, für Behörden und für Einrichtungen des Gesundheitswesens

„Intrinsisch“ motiviert



→ **Freiwillig, da Nutzen erkannt wird**

- Manipulationsschutz und Herkunftsnachweis für E-Dokumente im Außenverhältnis
- Hoher digitaler Beweiswert für geschäftskritische Unterlagen
- Positives Image „Digitale Vertrauenswürdigkeit“
- ...

„Extern“ motiviert



→ **Zwang**

- Gesetze und Verordnungen
- Vorgaben großer Geschäftspartner mit Machtfülle
- ...

Wie erhält meine Organisation ein qualifiziertes E-Siegel?

© secrypt GmbH 2020

Herausgeber: Qualifizierter Vertrauensdiensteanbieter (VDA) gemäß eIDAS-VO, z.B.

- D-TRUST - Ein Unternehmen der Bundesdruckerei (Deutschland)
- EuroCert (Polen)
- ...

Sichere Identifikation der juristischen Person

- Vertrauensniveau „hoch“ gemäß eIDAS-VO
- Identifikation durch Nachweisdokumente (z.B. Handelsregistrauszug) und zeichnungsberechtigte Person (z.B. Geschäftsführer, Prokurist)
- Unterschiedliche Identifikationsverfahren in Abhängigkeit vom VDA, z.B. PostIdent, VideIdent, RA-Officer, POSIdent (Point of Service)

Auslieferung des E-Siegels (genauer: des geheimen privaten E-Siegel-Schlüssels)

- Grundsätzlich: Speicherung auf einer „sicheren Siegelerstellungseinheit“ (SSEE)
- z.B. E-Siegel-Karte, Hardware Security Module (HSM) – abhängig vom VDA

E-Siegel-Karten vs. Hardware Security Module (HSM)

© secrypt GmbH 2020



- E-Siegel-Karte dezentral am Client
- E-Siegel-Karte zentral am Server

Achtung, je nach Siegel-Szenario die passende Karte wählen:

- Einzel-Siegel-Karte
 - (PIN-Eingabe pro Dokument)
- Multi-Siegel-Karte
 - (PIN-Eingabe pro Dokumentenstapel oder automatisierte Massensiegelung)
 - ca. 1 Siegel/Sekunde → 3.600 Siegel/Std



- Im sicheren Rechenzentrumsbetrieb vor Ort beim Kunden („on premise“)
- Für hochvolumige E-Siegel-Anwendungen
- HSM ermöglicht bis zu 3.000 RSA oder 2.500 ECDSA Siegeloperationen pro Sekunde
- Leistungsstarke Alternative zu E-Siegel-Karten
- „Fernsiegel“: E-Siegel auf HSM beim Vertrauensdienstanbieter zur Fernauslösung

E-Siegel-Karte am Client

© secrypt GmbH 2020

Ausstattung

- Siegelkarte
- Kartenlesegerät
- Einzelplatz-Software digiSeal®office (pro)

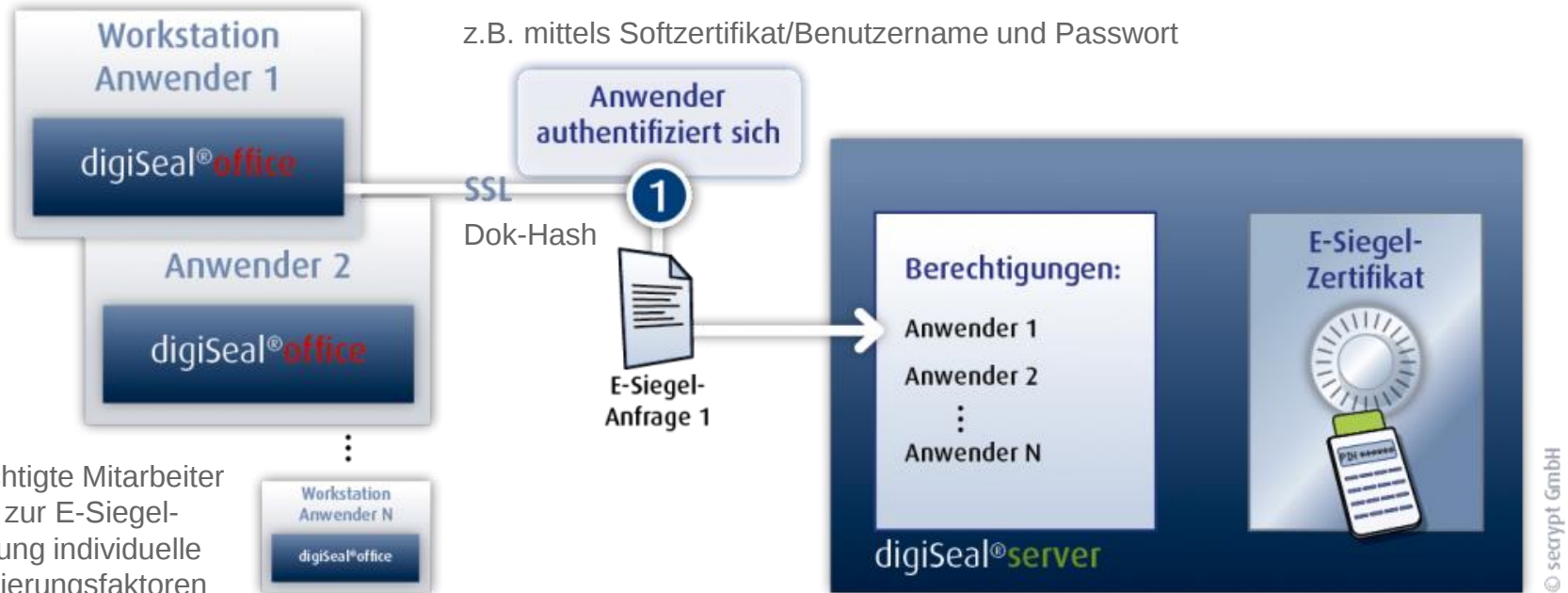
Vorgehen

- Zu siegelnde Dokumente, z.B. PDF, aufrufen/öffnen
- Siegelkarte in Kartenleser stecken
- PIN eingeben
- E-Siegel wird erzeugt



E-Siegel-Karte zentral am Server

© secrypt GmbH 2020



**Digitale Umsetzung des behördlichen „Holzstempelprozesses“
für siegelführende bzw. siegelberechtigte Personen!**

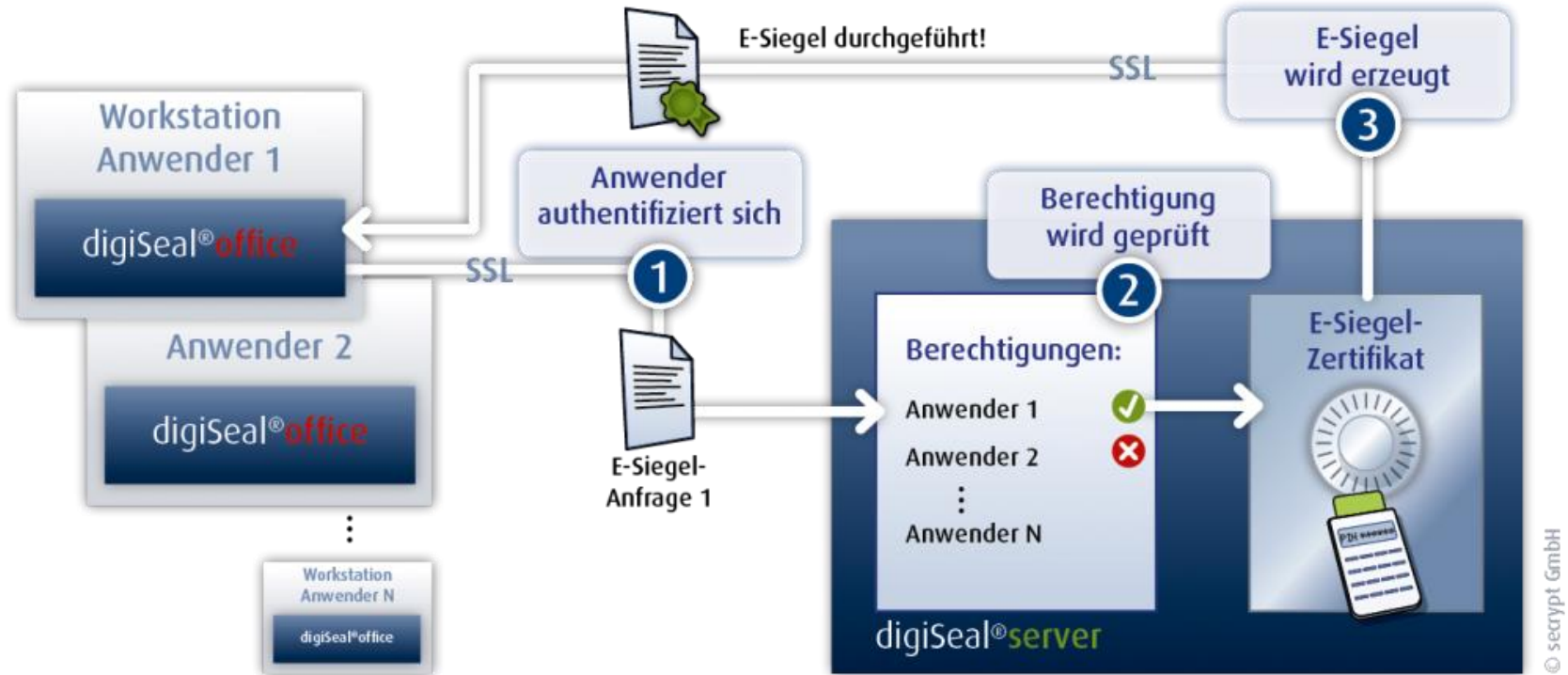
E-Siegel-Karte zentral am Server

© secrypt GmbH 2020



E-Siegel-Karte zentral am Server

© secrypt GmbH 2020

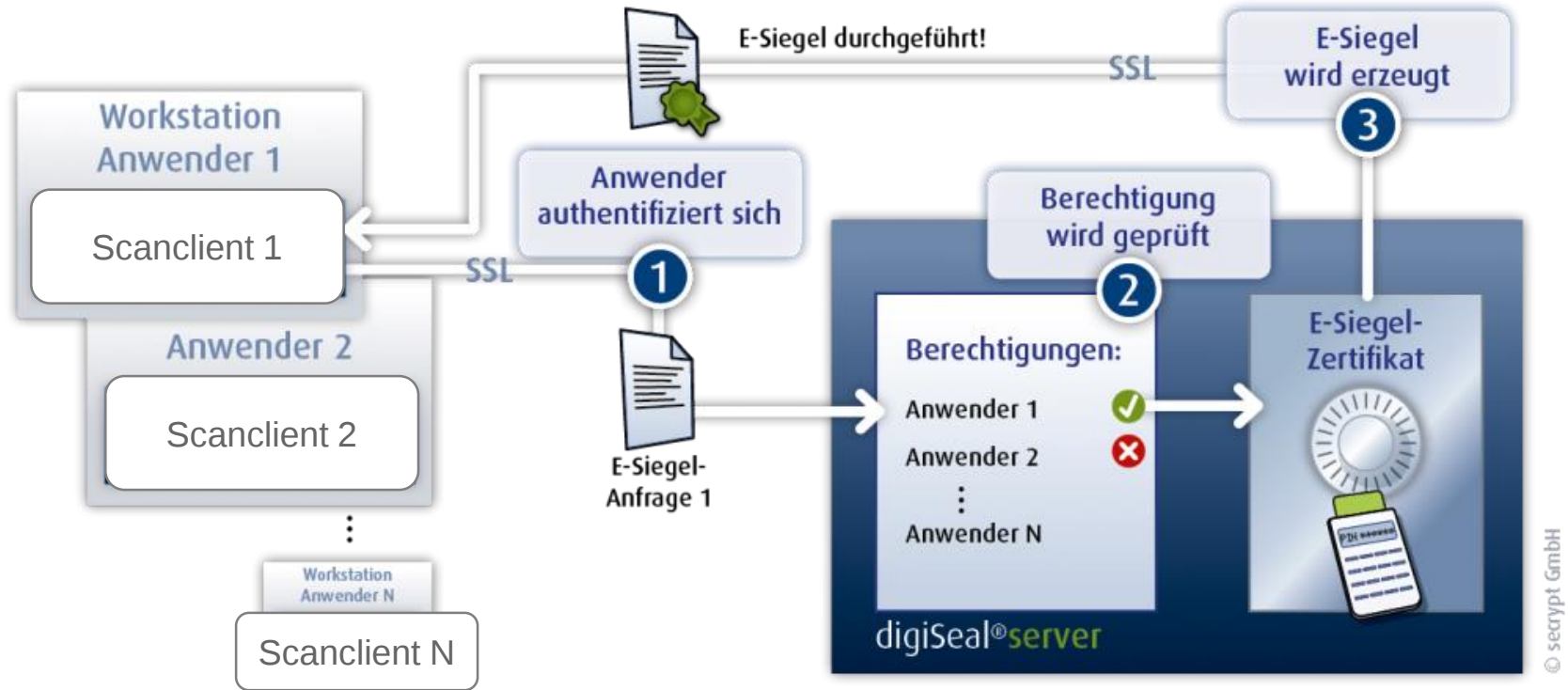


Client: Gesiegelter Dok-Hash (technisch: mit dem privaten RSA-Siegelschlüssel verschlüsselter Dok-Hash) wird in Dokument eingebaut, z.B. im PAdES-Format (PDF embedded seal)

Siegelberechtigungen können entzogen werden, ohne dass Siegelkarten ausgetauscht werden müssen

E-Siegel-Karte zentral am Server

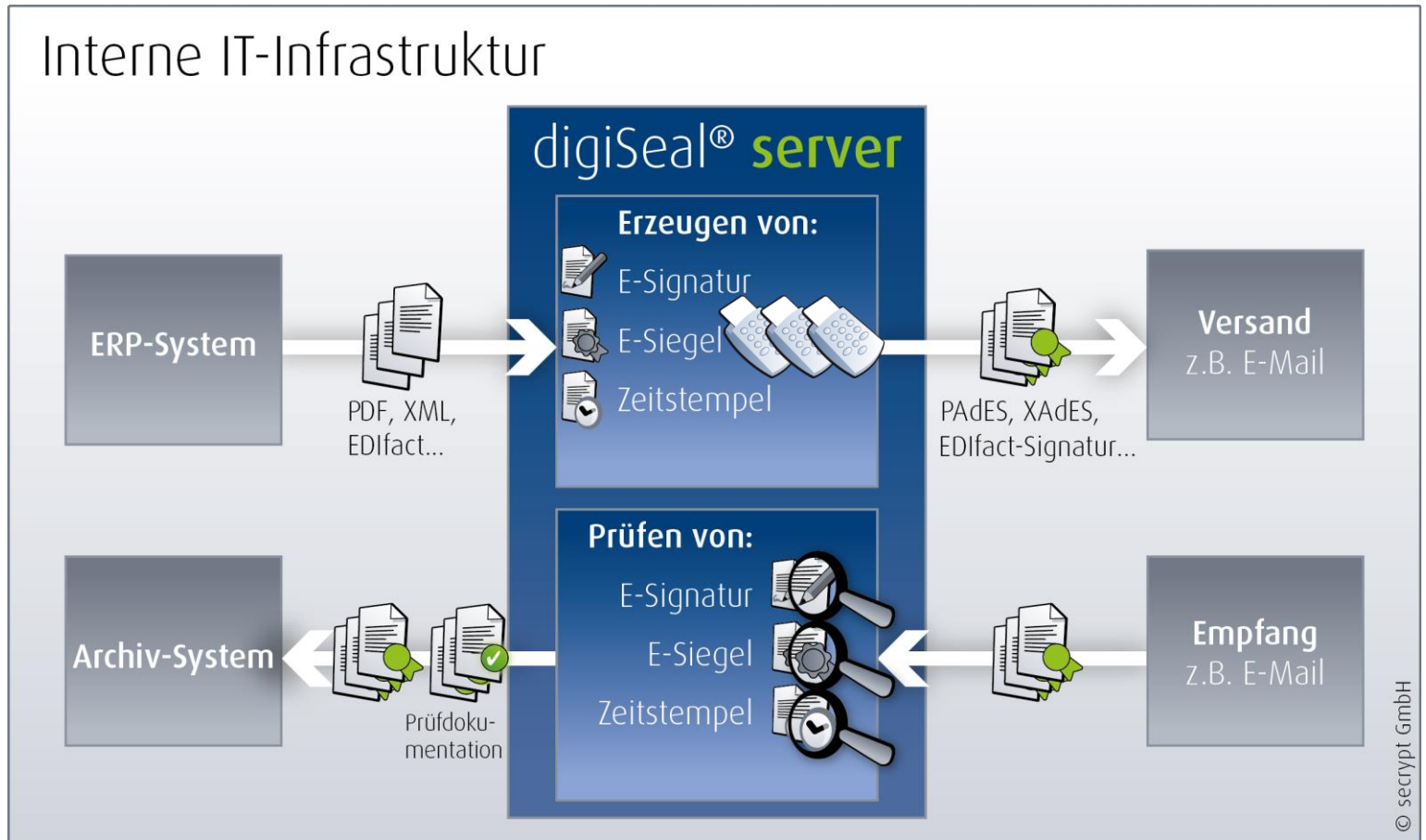
Beispiel: Dezentrales Scannen



- Deutschlandweit dezentrale Scanstationen
- Gescannte Dokumente werden stapelweise gesiegelt
- Scan-Operator (Anwender) authentifiziert sich pro Dokumentenstapel

Automatisiertes Siegeln von Massenbelegen

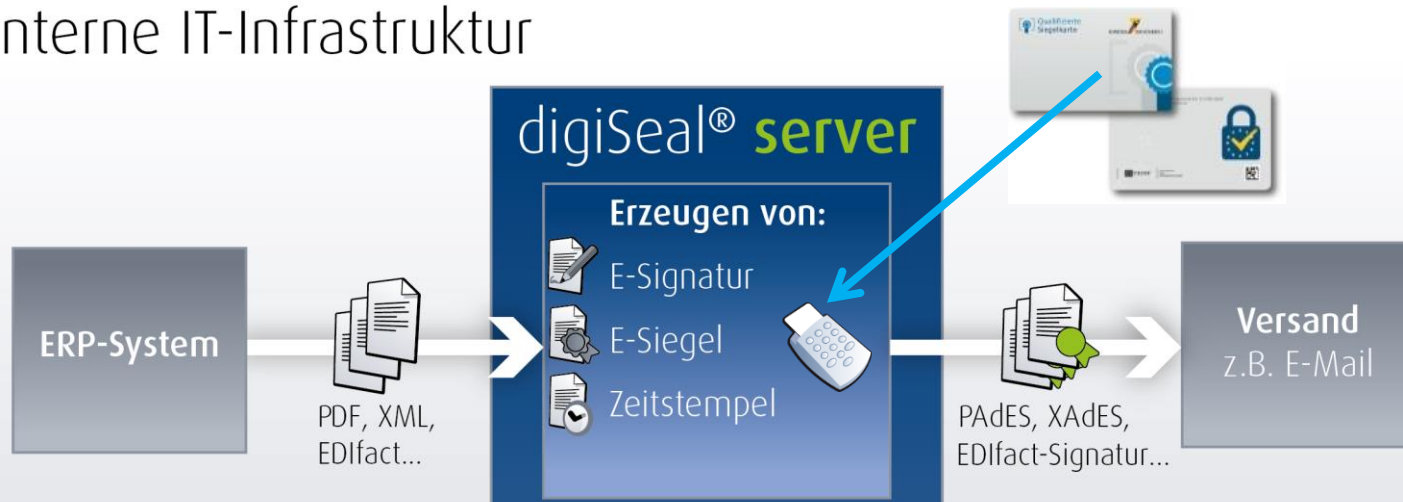
© secrypt GmbH 2020



Massenbelege siegeln

Beispiel: PDF-Auskünfte schützen

Interne IT-Infrastruktur



- Eine zentrale Multi-Siegelkarte
- Gesiegelte Auskünfte im PAcES-Format (PDF embedded seal) im Portal
- Weitere mögliche Aufgaben: Zeitstempeln, Validieren, Augmentieren, Verschlüsseln, Wandeln nach PDF/A etc.

Hardware Security Module (HSM) + eIDAS-Siegel

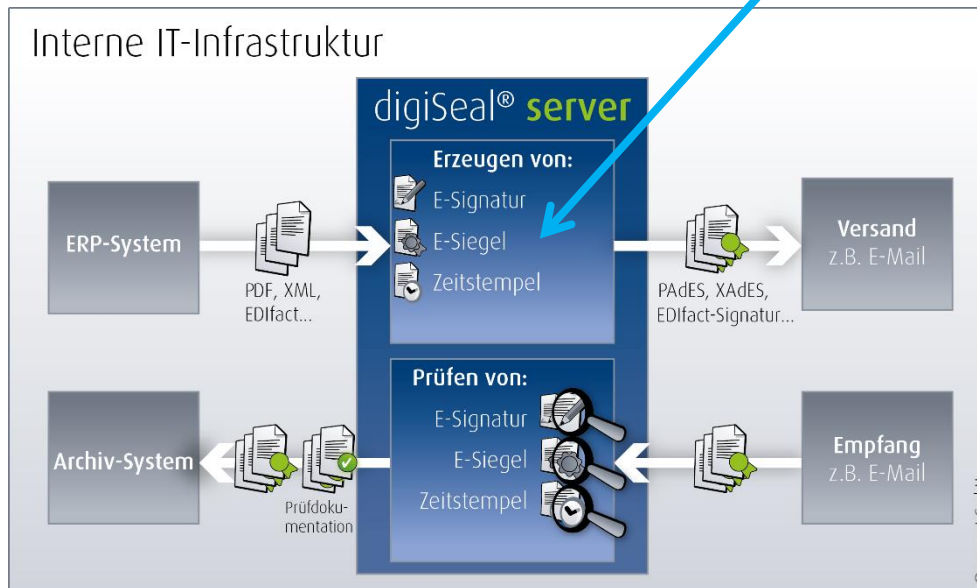
© secrypt GmbH 2020



z.B. Utimaco CryptoServer CP5



z.B. SafeNet Luna Network HSM 6



Zakład Ubezpieczeń Społecznych
Polnische Sozialversicherungsanstalt
E-Siegel von EuroCert Sp. z o.o

digiSeal[®]server Funktionen

© secrypt GmbH 2020



E-Signatur



E-Siegel



Zeitstempel



Verifikation



Verschlüsselung



Individualschritt

digiSeal®server Funktionen



© secrypt GmbH 2020

- Siegel/Signaturaustauschformate:
 - PAdES (PDF-Signatur; *.pdf)
 - CAdES (PKCS#7-Sign.; Container: pk7, p7m / abgesetzt: p7s)
 - XAdES (XML-Signatur; detached / enveloped)
 - und weitere...
- Unterstützung von Siegelkarten und Signaturkarten (es sind Multikarten einzusetzen)
gängiger Vertrauensdienstanbieter in DACH und weitere, z.B.: D-TRUST, TeleSec, DGN/medisign (D), A-TRUST, A-CERT (A), SwissSign, Swisscom, Quo Vadis (CH)
- Unterstützung von HSMs (Hardware Security Modules) und Softzertifikaten (PFX, P12)
- Zeitstempel gemäß IETF RFC 3161 Time-Stamp Protocol
- Umfangreiches prozessbezogenes Logging
- Farmingbetrieb zur Erhöhung von Performance und Ausfallsicherheit
- E-Mail-Alert-System für die Meldung betriebsbedingter Ereignisse
- Interoperabilität durch internationale Standards, z.B. ETSI, CEN

digiSeal®server Integration in Bestandssysteme

© secrypt GmbH 2020

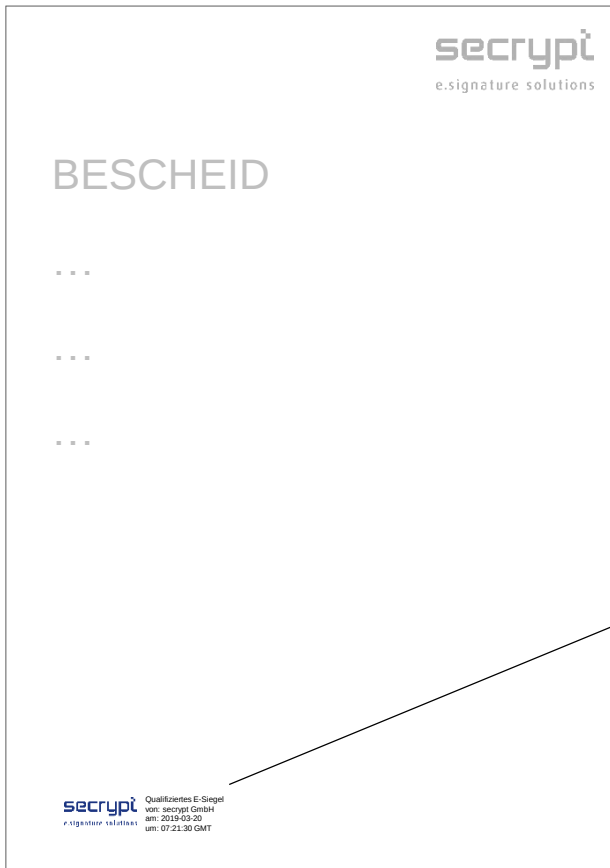
Integration in DMS, ERP, Workflow, Scansoftware und E-Archiv via...

- Webservice für webbasierte Lösungen
- Transparente Programmierschnittstelle (C-API)
- Java-, C#- oder Python-Wrapper
- Verzeichnisse ("Hot folder")
- Konnektoren (z.B. für SAP)
- Bereits bestehende Integrationen in Dritt-Software



Sichtbarer „Siegel-Stempel“

© secrypt GmbH 2020



Visueller „Siegel-Stempel“

Frei positionierbar

Individuell gestaltbar

Interaktiv (z.B. in Adobe Acrobat Reader)

z.B. Logo oder Wappen

secrypt
e.signature solutions

Qualifiziertes E-Siegel
von: secrypt GmbH
am: 2019-03-20
um: 07:21:30 GMT

Funktionen digiSeal®office

© secrypt GmbH 2020



- Beliebige Dokumentenformate siegel/signierbar (z.B. PDF)
- Hochwertiges PDF/A einfach z.B. aus Word erzeugen (über „Drucken“ -> „digiSeal“)
- Signatur/Siegelformate: PAdES (PDF embedded Signatur), XAdES (XML-Signatur), CAdES (PKCS#7-Signatur)
- Mit gängigen Siegelkarten, Signaturkarten, Heilberufsausweis (HBA) und IHK-Sachverständigen-Signaturkarte einsetzbar
- Mit sign-me-Fernsignatur nutzbar ➔ Es werden nur anonyme Hashwerte - keine Dokumente - an den Fernsignatur-Dienstleister (D-TRUST) übermittelt
- Mehrere Siegel/Signaturen in einem Dokument
- Individueller Grafik-Stempel (z.B. Logo, Wappen, Schriftzug) im PDF beliebig platzierbar
- Dokumente mit einem Zeitstempel versehen
- Siegel- und Signaturprüfung
- Dokumente ver- und entschlüsseln
- digiSeal®office pro für Stapelsiegelung/signatur (100 / 250 / 500)
- Integration über diverse Schnittstellen

Benötigte Komponenten

© secrypt GmbH 2020

1. Qualifiziertes E-Siegel-Zertifikat

- A) E-Siegel-Karte
- B) Hardware-Security Module (HSM)



2. Kartenlesegerät

Beim Einsatz von E-Siegel-Karten



3. Siegelsoftware

Client-Software digiSeal®office

Server-Software digiSeal®server



Bezugsquellen

© secrypt GmbH 2020

Szenario A: E-Siegel-Karten



- E-Siegel-Karten von D-TRUST GmbH
 - Antragslinks: <https://shop.secrypt.de/>
 - Identifizierung über PostIdent
- Kartenlesegerät von REINER SCT
<https://shop.secrypt.de/>
- Client-Software digiSeal®office
<https://shop.secrypt.de/>
- Kostenlose digiSeal®office Testversion
<https://shop.secrypt.de/produkt/digiseal-office-pro-testversion/>
- Server-Software digiSeal®server
 - Individuelle Beratung

Szenario B: E-Siegel auf Hardware Security Module (HSM)



- E-Siegel von EuroCert (polnischer VDA)
- HSM Utimaco CryptoServer CP5
- Server-Software digiSeal®server

➔ Individuelle Beratung

Anwendungsszenarien

© secrypt GmbH 2020

Anwendungsszenarien

- Behördenbescheide, Beglaubigungen
- Urkunden, Zeugnisse
- Geschäftsrechnungen, Lieferscheine, Auftragsbestätigungen
- Massenbelege, wie Kontoauszüge
- Entlassbriefe, pflegerische Dokumentationen, unkritische Laborbefunde
- Ersetzendes Scannen von Bestandsakten
(Integritätssicherung nach BSI TR RESISCAN)
- Angebote und eVergabe-Unterlagen
- Gesprächsmitschnitte (Audiodateien)
- ...



Weitere Webinare

© secrypt GmbH 2020

Unsere nächsten Webinar-Termine:

Donnerstag | 04.06.2020 | 11:00 Uhr

<< Elektronische Signatur im Gesundheitswesen – Wie signiere und prüfe ich digitale medizinische Dokumente und archiviere diese beweiswerterhaltend? >>

Mittwoch | 17.06.2020 | 11:00 Uhr

<< Ist die E-Signatur gültig? – Verifikation von elektronischen Signaturen, E-Siegeln und Zeitstempeln >>

Mittwoch | 01.07.2020 | 11:00 Uhr

<< Dokumente am Arbeitsplatz, z.B. im Homeoffice, elektronisch signieren >>

Vielen Dank!

© secrypt GmbH 2020

Sprechen Sie uns an, wir unterstützen Sie gern!

secrypt
e.signature solutions

Tatami M. Michalek
Geschäftsführer

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

