

Qualifiziertes E-Siegel auf Hardware Security Module für hohe Leistung im Rechenzentrumsbetrieb

Die secrypt GmbH bietet eine Komplettlösung aus Serversoftware digiSeal server und zertifiziertem HSM für hochperformante E-Siegel-Anwendungen in Wirtschaft, Verwaltung und Gesundheitswesen an. Mehr zu dem Thema erfahren Interessierte vom 8. bis 10. Oktober auf der it-sa in Halle 9 am Stand 9-210 in der Bitkom Security Area.

Berlin, 25.09.2019. Für größere Unternehmen und Organisationen aus Wirtschaft, Verwaltung und Healthcare mit eigenen Rechenzentren erlaubt nun die Verwendung eines zertifizierten HSM in Kombination mit digiSeal server die Umsetzung extrem leistungsfähiger und flexibler eIDAS-konformer E-Siegelprozesse., z.B. für digitale Kontoauszüge, Behördenbescheide, Patientenakten eines Krankenhauses, digitale Rechnungen oder die Authentifizierung zum Kontenzugriff durch FinTechs gemäß PSD2 (Payment Services Directive 2). Digitale Dokumente und Daten, die auf diese Weise mit einem qualifizierten E-Siegel versehen werden, können aufgrund einheitlicher EU-weiter Standards von unabhängigen Dritten auf Integrität und Authentizität geprüft werden – eine essentielle Voraussetzung für die Schaffung von Vertrauen in elektronische Geschäftsprozesse und Arbeitsabläufe.

Serversoftware digiSeal server integriert E-Siegel in IT-Prozesse

Der digiSeal server ermöglicht die Integration von E-Siegel, E-Signatur und Zeitstempel für beliebige Datenformate, z.B. PDF oder XML, in prozessführende Anwendungen, wie DMS, ERP oder sonstige Fachverfahren mittels diverser Schnittstellen, wie einem Webservice. Das Rollenkonzept mit differenzierten Zugriffsrechten für Administrator und Anwender erlaubt es, Siegelberechtigungen zuzuteilen und zu entziehen.

Hardware Security Module für sehr hohen Datendurchsatz und Flexibilität

Insbesondere für Siegelprozesse, die einen sehr hohen Dokumenten- bzw. Datendurchsatz, einen hohen Automatisierungsgrad und/oder die Verwendung mehrerer paralleler E-Siegel-Zertifikate vorsehen, stellen Siegelkarten einen technisch-organisatorischen Flaschenhals dar. Während aktuelle Siegelkarten bei der Verwendung des RSA-Algorithmus und 2.048 Bit Schlüssellänge ungefähr ein Siegel pro Sekunde leisten, also 3.600 Siegel pro Stunde, schaffen derzeit am Markt verfügbare Hardware Security Modules (HSM), die i.d.R. als 19-Zoll-Rack gestaltet sind, bis zu 3.200 Siegel pro Sekunde, d.h. ca. 11,5 Millionen Siegel pro Stunde. Zudem können viele unterschiedliche E-Siegel-Schlüssel auf einem HSM gespeichert und parallel betrieben werden.

Voraussetzungen für den HSM-Betrieb

Für die Speicherung qualifizierter E-Siegel muss das HSM über eine Zertifizierung verfügen, z.B. gemäß „Common Criteria for Information Technology Security Evaluation (CC)“, für das „Protection Profile prEN 419 221-5 Protection Profiles for TSP Cryptographic Modules – Part 5: Cryptographic Module for Trust Services“. Zudem hat der Betrieb beim Anwender vor Ort in einem sicheren Rechenzentrum (RZ), das beispielsweise ein Zutrittskontrollsystem besitzt, zu erfolgen.

Die ENISA (The European Union Agency for Cybersecurity) untermauert diesen Anwendungsfall in ihrer Veröffentlichung „Assessment of Standards related to eIDAS -

secrypt GmbH
Bessemmerstr. 82
D-12103 Berlin
Maria Johannsmann

Fon: +49 (0)30.756 59 78-58
Fax: +49 (0)30.756 59 78-18

presse@secrypt.de
www.secrypt.de

Recommendations to support the technical implementation of the eIDAS Regulation” aus November 2018.

Wie erhält eine juristische Person ein E-Siegel?

Das E-Siegel ist ein EU-weit anerkanntes Signaturwerkzeug für juristische Personen, wie eine AG, GmbH oder AöR. Es ist der digitale Stempel für Unternehmen und Organisationen der Privatwirtschaft, für Behörden und für Einrichtungen des Gesundheitswesens. Das qualifizierte E-Siegel wird von qualifizierten Vertrauensdiensteanbietern (VDA, oder auch „Trustcenter“), die strengen gesetzlichen und regulatorischen Anforderungen unterliegen, herausgegeben. Die juristische Person wird vom VDA sicher identifiziert. Dazu wird in der Regel eine zeichnungsberechtigte natürliche Person der Organisation inklusive erforderlicher Nachweisdokumente, wie einem Handelsregisterauszug, persönlich, beispielsweise per PostIdent-Verfahren, identifiziert. Nach erfolgreicher Identifizierung generiert der VDA ein individuelles E-Siegel-Zertifikat inklusive eines geheimen privaten Schlüssels, mit dem mittels starker kryptographischer Verfahren die E-Siegel erzeugt werden.

Der E-Siegel-Schlüssel ist auf sicherer zertifizierter Hardware, sogenannten „Sicheren Siegelerstellungseinheiten“ (SSEE) zu speichern, damit er nicht von Unbefugten missbraucht werden kann. Die qualifizierten VDAs bieten dafür Siegelkarten - Smartcards mit Kryptochip - an, die sowohl für Einzelsiegel- als auch Massensiegelprozesse eingesetzt werden können. Für das Auslösen eines E-Siegels ist der Nachweis einer PIN notwendig, die der VDA per PIN-Brief mitteilt.

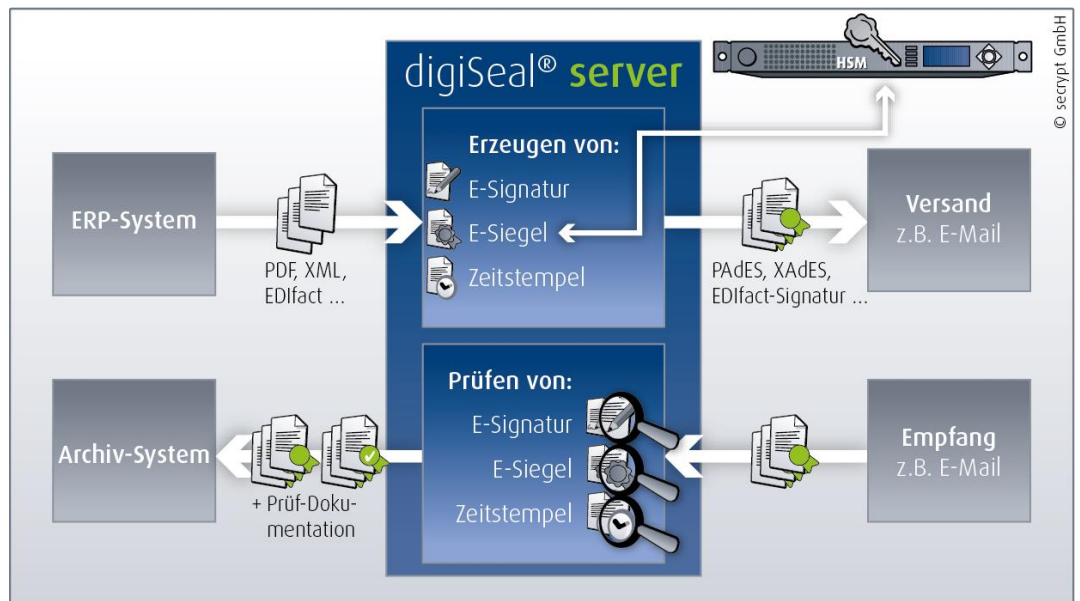
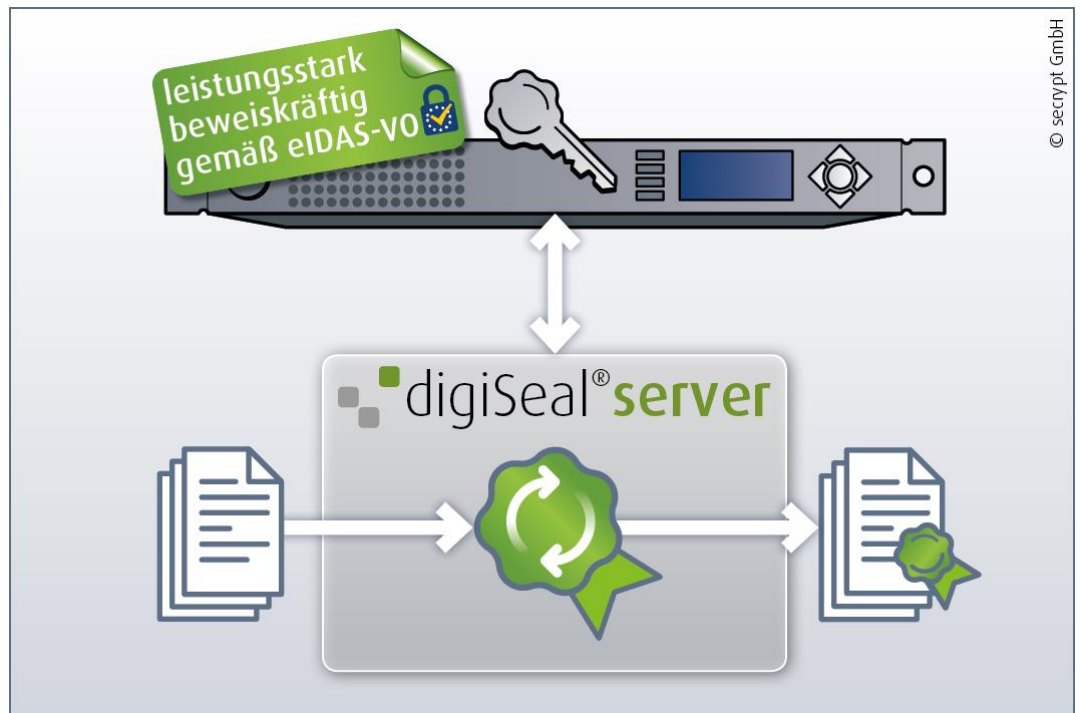
Kostenlose Gastkarte für die it-sa 2019

Wer mehr über die Anwendungsmöglichkeiten von elektronischen Signaturen, Siegeln und Zeitstempeln erfahren möchte, sollte secrypt auf der it-sa am Stand 9-210 (Bitkom Security Area) besuchen. Auf der Webseite <https://www.secrypt.de/messetermin> können Interessierte einen persönlichen Termin vereinbaren und sich eine kostenlose Gastkarte für die it-sa sichern.

secrypt GmbH
Bessemmerstr. 82
D-12103 Berlin
Maria Johannsmann

Fon: +49 (0)30.756 59 78-58
Fax: +49 (0)30.756 59 78-18

presse@secrypt.de
www.secrypt.de



secrypt GmbH
Bessemerstr. 82
D-12103 Berlin
Maria Johannsmann

Fon: +49 (0)30.756 59 78-58
Fax: +49 (0)30.756 59 78-18

presse@secrypt.de
www.secrypt.de

Über die secrypt GmbH

Die secrypt GmbH ist spezialisiert auf gesetzeskonforme elektronische Signaturen, E-Siegel und Zeitstempel, mit denen sich digitale Geschäftsprozesse optimieren, beschleunigen und sichern lassen. Zusammen mit seinen Partnern bietet secrypt praxisorientierte, flexible und einfach zu integrierende Lösungen an, z.B.:

- Zentrales serverbasiertes E-Siegel mit Hardware Security Module
- Signieren mit Smartcard und fernausgelöst per Smartphone (Remote signature)
- Ersetzendes Scannen von Bestandsdokumenten mit maximaler digitaler Beweiskraft
- Nahtlose Integration und Nutzung von Signaturwerkzeugen in DMS, ERP, Fachverfahren etc.
- PDF/A und die Beweiswerterhaltung mit Zeitstempeln im E-Archiv

Die secrypt GmbH sorgt mit der digiSeal®-Produktfamilie für Authentizität, Manipulationsschutz und Vertraulichkeit von sensiblen elektronischen Daten sowie die beweiswerterhaltende elektronische Archivierung. Seine Expertise bringt das Unternehmen unter anderem in den Fachgremien des BITKOM ein.

www.secrypt.de

Kontakt:

Maria Johannsmann

Bessemerstr. 82

D-12103 Berlin

Telefon: +49 30 756 59 78-58

presse@secrypt.de

www.secrypt.de

secrypt GmbH
Bessemerstr. 82
D-12103 Berlin
Maria Johannsmann

Fon: +49 (0)30.756 59 78-58

Fax: +49 (0)30.756 59 78-18

presse@secrypt.de

www.secrypt.de