

Qualifiziertes E-Siegel auf Hardware Security Module für hochvolumige und flexible Anwendungen



Lösungspaket für die
zentrale E-Siegel-Erzeugung
bestehend aus:

HSM Utimaco CryptoServer CP5
von der Utimaco IS GmbH

und

Serversoftware digiSeal®server
von der secrypt GmbH

Unternehmensstempel und Behördensiegel für die digitale Welt

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 das Gesundheitswesen.

Beweiswert gemäß EU-Verordnung eIDAS

Für ein qualifiziertes elektronisches Siegel gilt die
Vermutung der Unversehrtheit der Daten (Integrität)
und der Richtigkeit der Herkunftsangabe der Daten
(Authentizität), mit denen das qualifizierte
elektronische Siegel verbunden ist (eIDAS Art. 35 (2)).

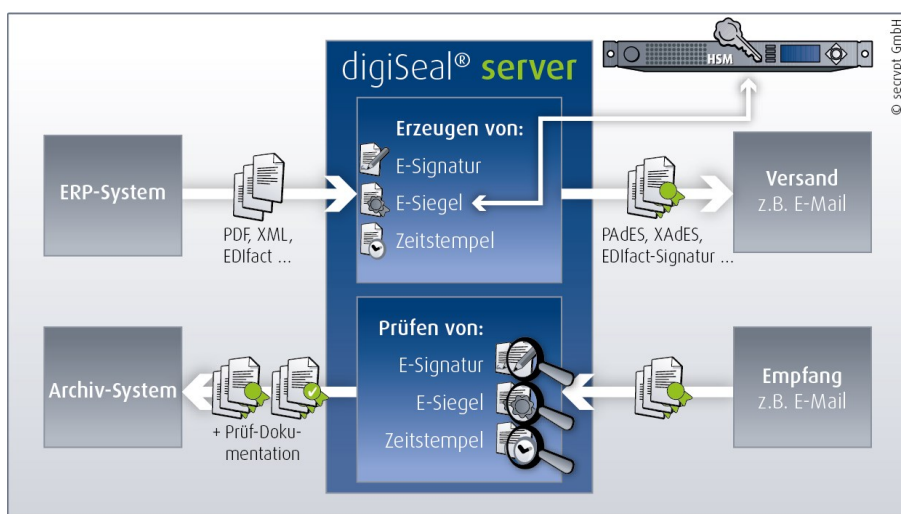


Hohe HSM-Leistung und Flexibilität

- bis zu 3.000 RSA oder 2.500 ECDSA
Siegeloperationen pro Sekunde im Bulk-Modus
- mehrere E-Siegel-Zertifikate parallel einsetzbar

Serversoftware digiSeal®server

- E-Siegel-Integration in prozessführende
Anwendungen z.B. via
 - Webservice
 - C-API
 - Java-, C#- und Python-Wrapper
 - Verzeichnisse („Hot folder“)
 - Konnektoren (z.B. SAP)
- Siegelberechtigungen mittels Rechtemanagement
zuteilen oder entziehen
- Signaturformate: Unterstützung aller AdES-
Konformitätsstufen gemäß eIDAS (B-B, B-T, B-LT):
 - PAdES (PDF-Signatur)
 - CAdES (PKCS#7-Signatur detached / enveloped)
 - XAdES (XML-Signatur detached / enveloped)
- Zeitstempel
- Elektronische Signatur
- Verifikation mit Prüfdokumentation (XML und PDF)
- Augmentierung (Dateianreicherung mit
Validierungsdaten, wie OCSP-Antworten, für spätere
Prüffälle)



SecurITy
TeleTrust Quality Seal
www.teletrust.de/taarng
made
in
Germany

Ein Beweis auf Vermutungsbasis ist nur sehr schwer
durch den Gegenbeweis zu erschüttern.

Utimaco CryptoServer CP5

Common Criteria-zertifiziert und eIDAS-konform

- eIDAS Protection Profile (PP) EN 419 221-5
„Cryptographic Module for Trust Services“.
- gemäß ENISA Assessment of Standards related to
eIDAS - Recommendations to support the technical
implementation of the eIDAS Regulation
- Sichere Schlüsselverarbeitung und -speicherung
innerhalb des HSM
- Mandantenfähigkeit

Einsatz-Szenarien

- Massenbelege, wie Kontoauszüge
- Behördenbescheide, Beglaubigungen, Urkunden,
Zeugnisse
- Patientenakten und Entlassbriefe
- Rechnungen, Lieferscheine, Auftragsbestätigungen
- Authentifizierung zum Kontenzugriff durch FinTechs
gemäß PSD2 (Payment Services Directive 2)
- Ersetzendes Scannen (mit Integritätssicherung nach
BSI TR-RESISCAN)

© secrypt GmbH

Tel.: +49 30 7565978-0
Fax: +49 30 7565978-18

sales@secrypt.de
www.secrypt.de

Haftungsausschluss: Alle Rechte sowie Druck-
fehler, Irrtümer und Änderungen vorbehalten.
Stand: 2022/07

e.signature solutions **secrypt**