digiSeal®server

Der Server für Signatur & Siegelung mit automatisierter Massenverarbeitung

Highlights

eIDAS ready

Digitale Dokumente vor Cyberfälschung schützen

Serversoftware für universelle Zertifikatsnutzung, automatisierte zentrale Massensignatur, E-Siegel, Zeitstempel & Datenverschlüsselung

Für Inhouse-Nutzung und Einsatz beim Outsourcing-Dienstleister (ASP)

Vielfältige Möglichkeiten zur technischen Integration in Bestandssysteme und Workflows

Sofort einsatzbereit

eIDAS ready

Der Signaturserver im Überblick

Bei der Transformation des Geschäftsalltags in die digitale Sphäre gewinnt die Daten- und Dokumentensicherheit massiv an Bedeutung. Manipulationsschutz, Urhebernachweis, Datenverschlüsselung und der digitale Beweiswert rücken ins Zentrum der Aufmerksamkeit.

Für EU-weit einheitliche rechtliche und technische Standards sorgt seit 2016 die „Verordnung über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt" (eIDAS-VO).

Mit dem digiSeal®server können zentrale Sicherheitsfunktionen in individuellen Arbeitsprozessen parallel betrieben werden:

- **Elektronische Signatur & E-Siegel** – Automatisiertes Signieren und Siegeln großer Dokumentenmengen. Die E-Signatur und das E-Siegel stellen die Unversehrtheit der Inhalte (Integrität) sicher und weisen die Identität des Unterzeichners / Urhebers (Authentizität) nach.
- **Signaturanreicherung** – Augmentation von Signaturen mit Zeitstempeln und Validierungsdaten zur Aufwertung der AdES-Signaturstufe.
- **Signaturverifikation** – Automatisierte Verifikation signierter Daten inklusive Prüfdokumentation im PDF/A- oder XML-Format.
- **Zeitstempel** – Mittels Zeitstempel wird der Inhalt eines Dokuments bzw. Datensatzes zu einem „offiziellen" Zeitpunkt nachweisbar „eingefroren". (Das gewünschte Zeitstempelkontingent ist bei einem Vertrauensdiensteanbieter zu erwerben.)
- **Individualschritt** – Mit der Einbindung von Drittkomponenten lassen sich weitere Funktionen, wie Dateikonvertierung (z.B. TIF2PDFA), in den Verarbeitungsprozess integrieren.
- **Verschlüsselung** – Automatisierte Datenverschlüsselung auf Basis starker State-of-the-Art Kryptographie-Verfahren. Damit wird der Einblick von Unbefugten und Schnüfflern verhindert.
- **E-Mail-Versand** – Automatisiertes Versenden der Dokumente per E-Mail.

Einsatzspektrum

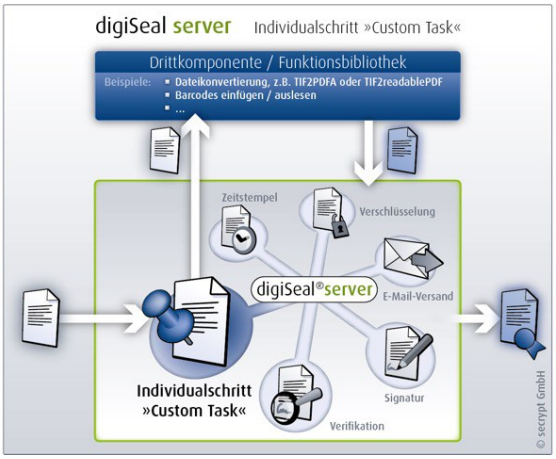
Signieren, siegeln, zeitstempeln, verschlüsseln Sie

- Massenbelege, z.B. Kontoauszüge, Rechnungen (EU-Umsatzsteuer-Systemrichtlinie, deutsches Umsatzsteuergesetz), Gehaltsabrechnungen
- Gesprächsmitschnitte (Audiodateien) z.B. Beratungsgespräche bei Verbraucherdarlehen
- Nachweisdokumentation
- Geschäftskorrespondenz
- Maschinenprotokolle
- Ersetzendes Scannen
- Medizinische Dokumentation
- u.v.m.

Technische Integration

Anbindung an Ihr DMS, ERP, Archiv etc. erfolgt mittels

- **Webservice** für webbasierte Lösungen
  Programmierschnittstelle (C-API)
- Java-, C#- oder Python-Wrapper
- **Verzeichnisse** („Hot folder")
- **Konnektoren** (z.B. für SAP)



Einbindung von Drittkomponenten für weitere Funktionalitäten

SecurITy made in Germany

TeleTrusT Quality Seal www.teletrust.de/itsmig

© secrypt GmbH

e.signature solutions secrypt

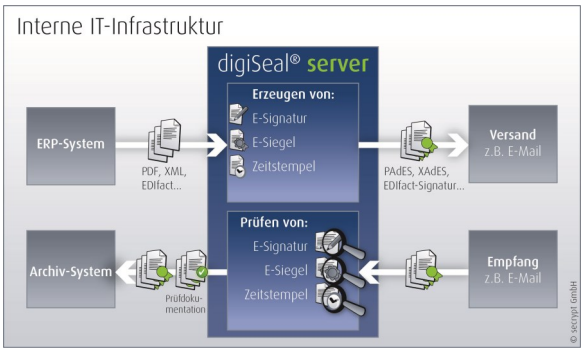
Der Baukasten für individuelle Signatur-, E-Siegel- und Zeitstempel-Lösungen

Erfolgreiche Integration in die Komponenten folgender Anbieter

AGFA HealthCare
Com2
d.velop
DETEC
Fenestrae
Ferrari Electronic
HYDMedia
InterForm
KOFAX
Lexmark
Lobster
NEXUS / MARABU
Net at Work
Saperion
ReadSoft
SEEBURGER
Synedra
XBOUND

Weitere Eigenschaften (Auswahl)

- Betrieb als Microsoft® Windows® Systemdienst
- abgesetzte Benutzeroberfläche zur Konfiguration und Bedienung
- umfangreiche Benutzerverwaltung (inkl. differenzierter Zugriffsrechte und Rollenkonzepte)
- E-Mail-Alert-System für die Meldung betriebsbedingter Ereignisse
- umfangreiches prozessbezogenes Logging
- Unterstützung von Signaturkarten, Softzertifikaten und HSMs (Hardware Security Modules)
- Erzeugung und Verifikation qualifizierter und fortgeschrittener E-Signaturen, E-Siegel, Zeitstempel
- Erfüllung von Anforderungen der Bundesnetzagentur (BNetzA): Konformitätsnachweis (Herstellererklärung)
- Farmingbetrieb erhöht Performance und Ausfallsicherheit



Datensouveränität bewahren

Nutzen Sie eine geeignete Signatursoftware, bleiben Ihre sensiblen Dokumente bei Ihnen und werden zum Signieren in keine externe Cloud übertragen. Somit ist bei der Nutzung von On-Premise-Signaturlösungen wie digiSeal®server Datensouveränität stets unmittelbar und nachvollziehbar gewährleistet.

Technik

Betriebssysteme
Windows® Server 2022 / 2019 / 2016 / 2012 R2 / 2012 / 2008 R2
Windows® 11 / 10 / 8.1 / 8

Systemvoraussetzungen
aktueller Prozessor ab 2,5 GHz
Arbeitsspeicher (RAM): ab 2 GB
Festplattenspeicher: mind. 500 MB für Installationspaket

Signaturaustauschformate
Unterstützung aller AdES-Konformitätsstufen gemäß eIDAS-VO (B-B, B-T, B-LT):
PAdES (PDF-Signatur; *.pdf)
CAdES (PKCS#7-Sign.; Container: pk7, p7m / abgesetzt: p7s)
XAdES (XML-Signatur; detached / enveloped), XMLDsig
EDI-Signatur (embedded und AUTACK);
GS1 EANCOM DE, Ideal Message Swiss, EANCOM AECOC ES, Editel® CZ, GS1 EANCOM CZ, Edicom®, GS1 EANCOM FR;
2D-Barcode speichert Signatur auf Papier und Fax (*.pdf, *.tif, Fax Group 3 und 4)

Unterstützte Signaturkarten
Es sind sogenannte Mehrfach- bzw. Multi-Signatur- bzw. -Siegelkarten einzusetzen, die das Erzeugen mehrerer Signaturen/Siegel bei einmaliger PIN-Eingabe erlauben.

Es werden die Signatur- und Siegelkarten gängiger Trustcenter unterstützt, wie z.B.
Deutschland: D-TRUST, TeleSec, DGN/medisign, Bundesnotarkammer
Schweiz: Swisscom Solutions, Quo Vadis, GS1 Switzerland, SwissSign
Österreich: A-CERT, A-TRUST

Informationen zu den technisch unterstützten Karten entnehmen Sie bitte der Technischen Spezifikation.

Zertifikatsformat
X.509 v1 bis v3, DER-codiert

Signaturalgorithmen:
ECDSA, RSA (mit folgenden Hashalgorithmen)

Hashalgorithmen
SHA1, SHA2-224, SHA2-256, SHA2-384, SHA2-512, RIPEMD160, MD2, MD5

Verschlüsselungsalgorithmen
asymmetrisch: RSA;
symmetrisch: 3-Key-Triple-DES, AES, RC2 u. PKCS#5 zur Schlüsselgenerierung

Schlüsselspeicherung
Signaturkarten: ISO 7816 SmartCards;
Softzertifikate: PKCS#12 (*.pfx, *.p12)
HSMs und Tokens (via PKCS#11)

Kartenlesegeräte
Klassen 1 bis 3 / CTAPI, PC/SC

Kartenkommunikationsprotokoll
T0, T1

Zeitstempelunterstützung
gemäß IETF RFC 3161 Time-Stamp Protocol
z.B. D-TRUST (SSL-Authentifikation), TeleSec (HTTP-Authentifikation)

Konform zu internationalen Standards
eIDAS-VO, Common PKI (vormals ISIS-MTT), Profil über international verbreitete und anerkannte Standards für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen.

digiSeal®server by secrypt

© secrypt GmbH

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

sales@secrypt.de
www.secrypt.de

Haftungsausschluss: Alle Rechte sowie Druckfehler, Irrtümer und Änderungen vorbehalten.
Stand: 2023/05

e.signature solutions secrypt