

Der Signaturserver für die automatisierte Dokumentensicherung



Merkmale

Serversoftware für die automatisierte zentrale Massensignatur Signaturverifikation & Zeitstempelerzeugung
gesetzeskonform nach SigG und SigV
für Inhouse-Nutzung und Einsatz beim Outsourcing-Dienstleister (ASP)
für Geschäftskorrespondenz, Maschinenprotokolle, Rechnungen, elektronischer Zeitstempel für Posteingang
einfache und komfortable Handhabung
modularer Aufbau, flexible Konfiguration

Einsatzspektrum

für sehr große bis mittel-große Mengen von Daten bzw. Dokumenten
für einen hohen Automatisierungsgrad
für hohes und normales Sicherheitsniveau



secript GmbH
Bessemerstraße 82
D-12103 Berlin

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

sales@secript.de
www.secript.de

Papiergebundene Geschäftsprozesse erfordern den Transport und die Aufbewahrung von Dokumenten. Die Kosten, z.B. für Druck, Kuvertierung, Porto oder Lagerung, sind immens.

Die elektronische Signatur ermöglicht, flankiert von entsprechenden rechtlichen Rahmenbedingungen, die papierlose Abwicklung derartiger Vorgänge, verbunden mit großen Einsparungspotenzialen. Die elektronische Signatur dokumentiert die Identität des Unterzeichners und die Unversehrtheit des Dokumenteninhaltes – eine unmerkliche Manipulation ist damit unmöglich.

Beispiel: Internationales E-Invoicing

Um Vorsteuerabzug für elektronische Rechnungen geltend machen zu können, sind laut EU-Richtlinie und deutschem Umsatzsteuergesetz (§ 14 UStG) die Echtheit der Herkunft (Authentizität) und die Unversehrtheit der Rechnungsinhalte (Integrität) sicherzustellen. Die elektronische Signatur erfüllt diese Anforderungen auf einfache Art und Weise und ist international standardisiert und akzeptiert.



Abb.: Der "Baukasten" für die automatisierte Dokumentensicherung

Immer das richtige Format bei Signaturerzeugung und -verifikation

Der digiSeal® server erzeugt qualifizierte, fortgeschrittene und einfache Signaturen und unterstützt alle gängigen Signaturformate. Abhängig von speziellen Versender- und Empfängeranforderungen kann daher immer das passende Format eingesetzt werden. Beim Signieren eines PDF/A-konformen Dokuments bleibt die PDF/A-Konformität erhalten.

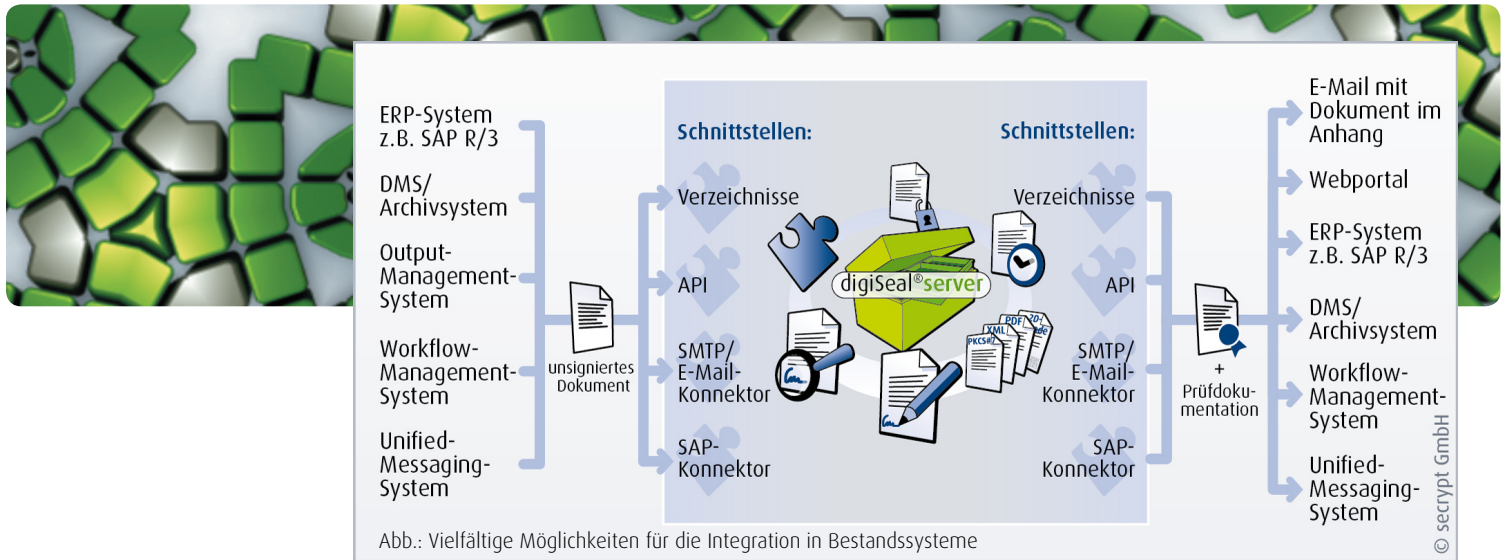
Signaturformate:

- PKCS#7-Signatur
- PDF-Signatur (Erhalt von PDF/A-Konformität)
- XML-Signatur (XML-DSig und XadES)
- EDI-Signatur
- 2D-Barcode speichert Signatur auf Papier und Fax

Verifikation mit Prüfdokumentation

Mit dem digiSeal® server sind alle gängigen standardkonformen Signaturformate automatisiert verifizierbar. Dabei wird bei Bedarf eine GDPdU-konforme Prüfdokumentation im PDF/A- oder XML-Format erzeugt. Der Empfänger von elektronisch signierten Dokumenten kann diese manuell verifizieren. Dafür steht die kostenlosen Prüfsoftware digiSeal® reader von secript zur Verfügung (Download unter www.secript.de). Alternativ kann man signierte PDF-Dokumente mit dem Adobe® Reader überprüfen – auch ohne den Einsatz von zusätzlichen Plug-ins.

digiSeal® server: der Baukasten für individuelle Signatur- und Zeitstempellösungen



Integration in die Komponenten z.B. folgender Anbieter:

- AGFA HealthCare
- Avaya
- CROSSGATE
- CAE
- Captaris
- Com2
- Cycos
- DETEC (Beta Systems Group)
- Fenestrae
- Ferrari Electronic
- Foxray
- Gräbert
- HYDMedia
- Insiders
- InterForm
- Inubit
- KOFAX
- MCA
- Net at Work
- SAPERION
- ...

Verschlüsselung:

Schutz vor unbefugtem Einblick

Sensible Daten, wie z.B. dem Datenschutz unterliegende personenbezogene Informationen, sind bei der Archivierung oder beim Transport vor dem Einblick unbefugter Personen durch Verschlüsselungsverfahren zu schützen. Der digiSeal® server unterstützt die leistungsstarke automatisierte Verschlüsselung von Dokumenten sowohl mit Passwort als auch mit dem öffentlichen Schlüssel eines X.509-Zertifikats.

Mandantenfähigkeit / komfortable Benutzeroberfläche

Der digiSeal® server kann eine Vielzahl von Prozessen parallel abarbeiten. Die Funktionen „Signieren“, „Verifizieren“, „Zeitstempeln“, „Verschlüsseln“ und „Per E-Mail versenden“ sind flexibel miteinander kombinierbar.

Beispiel: Ein Dokument wird signiert, dann verschlüsselt und anschließend per E-Mail versendet – in nur einem Prozess. Parallel können weitere Prozesse mit anderen Aufgaben, wie z.B. „Zeitstempeln“ oder „Verifizieren“, betrieben werden.

Die Administration der Prozesse und des Betriebs erfolgt über eine komfortable Benutzeroberfläche.

Farming / Ausfallsicherheit

Zur Erhöhung von Performance und Ausfallsicherheit ist der digiSeal® server im Farmingbetrieb einsetzbar.

Integrationsmöglichkeiten

Die Anbindung an Dokumentenmanagement, Warenwirtschafts-, ECM-, BPM oder ERP-Systeme und das Archiv erfolgt über Konnektoren (z.B. an SAP®, Navision® oder die Einbindung in einen SMTP-Datenstrom), eine Programmier-Schnittstelle (API) und eine Standard-Schnittstelle (Verzeichnisse). Außerdem ist der digiSeal® server in namhafte Workflow-Management-Systeme (z.B. Inubit BPM-Suite) integriert, die den Dokumentenfluss zentral steuern.

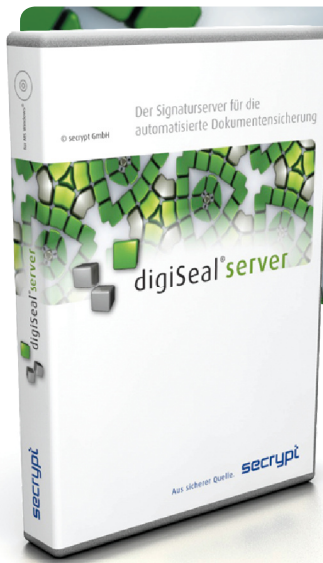
Grenzüberschreitender Einsatz, z.B. EU

Der digiSeal® server ist international einsetzbar – unabhängig davon, ob von Deutschland, Österreich, einem anderen EU-Land oder der Schweiz aus operiert wird. Bei der Umsetzung entsprechender Projekte bietet die secript GmbH umfassende Unterstützung, wie z. B. Beratung in Hinsicht auf landesspezifische Rahmenbedingungen.

Trustcenter / Signaturkarten / Softwarebasierte Zertifikate

Es werden gesetzeskonforme Signaturkarten aller deutschen Trustcenter sowie aus verschiedenen EU-Mitgliedsstaaten und der Schweiz unterstützt. Weitere aktuelle Signaturkarten werden regelmäßig in die Software gepflegt. Daneben sind – für die einfachen und fortgeschrittenen Signatur – auch softwarebasierte Zertifikate einsetzbar.

digiSeal[®] server: hohe Sicherheit, flexibel und hochperformant



Neuerungen ab Version 2.2.2.0

Betrieb der Software als
Microsoft[®] Windows[®]-
Systemdienst

abgesetzte
Benutzeroberfläche zur
Konfiguration und
Bedienung

umfangreiche
Benutzerverwaltung
(inkl. differenzierter
Zugriffsrechte und
Rollenkonzepte)

Prüfdokumentation
in weiteren Sprachen
(jetzt: DE, EN, ES, FR, IT, NL, PL)

Sicherheit

Um einem Missbrauch der automatisierten qualifizierten Signatur vorzubeugen, muss ein entsprechendes System grundsätzlich in einer gesicherten Umgebung eingesetzt werden.

Darüber hinaus muss der Signaturschlüsselinhaber laut Bundesnetzagentur die Möglichkeit haben, den Inhalt der Daten vor dem Signieren zunächst einzusehen und erst nach Prüfung der Richtigkeit den Signaturprozess mittels Eingabe der PIN bei Festlegung eines Zeitfensters oder einer maximalen Signaturanzahl zu starten.

Der digiSeal[®] server erfüllt alle diese Anforderungen. Der Nachweis seiner Konformität zum deutschen Signaturgesetz wurde gegenüber der Bundesnetzagentur durch eine Herstellererklärung erbracht.

Weitere ausgewählte Eigenschaften

- automatisierte Ansprache externer Zeitstempeldienste
- automatisierter Dokumentenversand per E-Mail (die E-Mail kann zusätzlich mit einem softwarebasierten Zertifikat signiert werden)
- E-Mail-Alert-System für die Meldung betriebsbedingter Ereignisse
- umfangreiches dokumentenbezogenes Logging der durchgeführten Prozessschritte
- Mehrfachsignaturen in einem Dokument
- Sicherheitsmechanismen gegen Missbrauch der automatisierten Signaturerzeugung (siehe "Sicherheit")
- sichere PIN-Eingabe direkt am Kartenlesegerät

Technik

Betriebssysteme:

Windows[®] Server 2008 / 2003 / 2000
Windows[®] 7 / Vista / XP / 2000

Systemvoraussetzungen:

aktueller Prozessor, z.B. Intel Core2Duo oder AMD Athlon / ab 2,5 GHz
ab 2 GB Arbeitsspeicher (RAM)
Festplattenspeicher: mind. 100 MB für Installationspaket

Konform zu internationalen Standards:

Common PKI (vormals ISIS-MIT), Profil über international verbreitete und anerkannte Standards für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen.

Signaturaustauschformate:

PKCS#7/CMS embedded (*.pk7);
PKCS#7 detached (*.p7s);
PKCS#7 S/MIME multipart-signed (*.p7m);
PDF-Signatur (*.pdf gemäß Adobe[®] PDF Reference 1.6);
XML-Signatur (*.xml gemäß XML-DSig);

erweiterte XML-Signatur (gemäß XAdES);
2D-Barcode speichert Signatur auf Papier und Fax (*.pdf, *.tif, Fax Group 3, Fax Group 4 für signierten Faxversand);
EDI-Signatur (embedded und AUTACK) GS1 EANCOM DE, Ideal Message Schweiz, EANCOM AECOC ES, Editel[®] CZ, GS1 EANCOM CZ, Edicom[®] / GS1 EANCOM FR

Zertifikatsformat:

X.509 v1 bis v3, DER-codiert

Signaturalgorithmus:

RSA (mit folgenden Hashalgorithmen)

Hashalgorithmen:

SHA1, SHA-2, SHA-224, SHA-256, SHA-384, SHA-512, RIPEMD160, MD2, MD5

Verschlüsselungsalgorithmen:

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

Schlüsselspeicherung:

Signaturkarten: ISO 7816 SmartCards;
Softwarezertifikate: PKCS#12 (*.pfx, *.p12)

Kartenlesegeräte:

Klassen 1 bis 3 / CTAPI, PC/SC

Kartenkommunikationsprotokoll:

T0, T1

Zeitstempelunterstützung:

gemäß IETF RFC 3161 Time-Stamp Protocol
D-TRUST-Zeitstempel (SSL-Authentifikation)
TeleSec-Zeitstempel (HTTP-Authentifikation)

Unterstützte Signaturkarten:

Für die Nutzung des digiSeal[®] server muss eine sogenannte Mehrfach- bzw. Multi-Signaturkarte eingesetzt werden, die das Erzeugen mehrerer Signaturen bei einmaliger PIN-Eingabe zulässt.

Dabei werden die Signaturkarten gängiger Trustcenter bzw. CAs unterstützt, wie z.B. D-TRUST, TC TrustCenter, TeleSec, S-TRUST, Signtrust, Bundesnotarkammer, Swisscom Solutions, Quo Vadis, GS1 Switzerland und A-CERT.

Die technisch unterstützten Karten entnehmen Sie bitte der Technischen Spezifikation.



ein Produkt der

secrypt GmbH
Bessemerstraße 82
D-12103 Berlin

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

sales@secrypt.de
www.secrypt.de