# digiSeal®server

## The signature server for automated mass signing & document security

### Highlights

eIDAS ready

Protect digital documents against fraud

Server software for universal certificate usage, automated mass signing, electronic seals, timestamps & data encryption

For in-house useage & deployment by outsourcing & application service providers (ASPs)

Broad variety of technical implementation in established systems and workflows

Ready for use

### The signature server at a glance

With the transformation of everyday business life into the digital sphere, data and document security is becoming extremely important.

Tamper protection, copyright verification, data encryption and the digital probative value have increasingly become the center of focus for IT strategies, compliance and the social discourse.

The "Regulation on electronic identification and trust services for electronic transactions in the internal market" (eIDAS) has ensured EU-wide legal and technical standards since the year 2016.

digiSeal®server enables central security functions to be operated in parallel in individual work processes:

- **Electronic signature and seal** – Automatically sign and seal large document volumes. The digital signature and the electronic seal ensure the integrity of the content and verify the identity of the signer/author (authenticity).
- **Signature enhancement** – Enhancement (augmentation) of signatures with time stamps and validation data to enhance the AdES signature level.
- **Signature verification** – Automatic verification of signed data including the verification documentation in PDF/A or XML format.
- **Timestamps** – Using a timestamp, the content of a document or data record is verifiably "frozen" at an "official" point in time. (The desired timestamp contingent must be acquired from a trust centre.)
- **Custom Task** – The integration of third-party components enables any other functionalities, such as file conversion (for example, TIF2PDFA), to be integrated in the processing.
- **Encryption** – Automatic encryption based on strong state of the art cryptography. This serves as a protection against unauthorized viewing.
- **Email** – Automatic document delivery by e-mail.

### Application examples

Signing, sealing, timestamping and encryption of

- Bulk receipts, e.g. bank statements, invoices (as part of international eInvoicing projects, EU VAT System Directive), payslips
- Recording discussions (audio files) e.g. consultations for personal loans
- Business correspondence
- Machine logs
- Digitised documents as part of replacement scanning
- Medical reports
- And many more

### Integration

Integration into your DMS, ERP, archive etc. via:

- **Webservice** for web-based solutions

**Programming interface** (C-API)

- Java-, C#- or Python-**Wrapper**
- **Directories** („Hot folder“)
- **Connectors** (e.g. SAP)

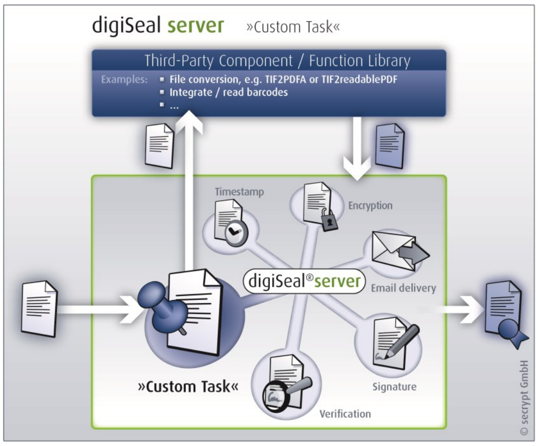


Fig.: Integration of third-pary components for further functionalities

SecurITy made in Germany

TeleTrusT Quality Seal
www.teletrust.de/itsmig

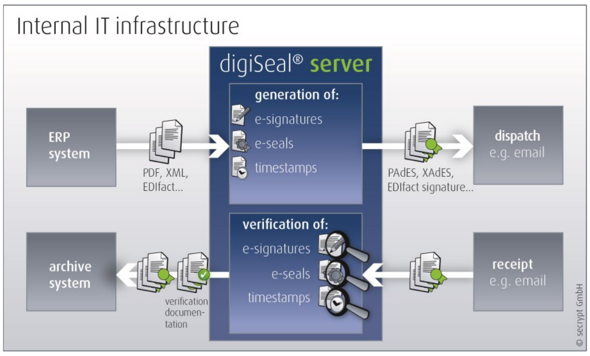
# digiSeal®server: the toolbox for individual signature, seal and timestamp solutions

### Successful integration in the components of the following providers

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

## Further features (selection)

- Operating as Microsoft® Windows® service
- Separate GUI for configuration and operation
- Extensive user administration (incl. comprehensive access rights and role concepts)
- Email alert system for reporting operational events
- Comprehensive document-related logging of completed processes
- Support of signature cards, software based certificates and HSMs (Hardware Security Modules)
- Generation and verification of qualified and advanced electronic signatures, seals, time stamps
- Compliant with EU regulation eIDAS
- Farming increases performance and system stability



## Keep sovereignty over your sensitive data

By using suitable signature software, your confidential documents are not uploaded to an external cloud, but stay with you. When using on-premise signature solutions like digiSeal®server, you keep full control over the sovereignty of your data — traceable at all times.

## Technology

### Operating systems

Windows® Server 2019 / 2016 / 2012 R2 / 2012 / 2008 R2 / 2008
Windows® 10 / 8.1 / 8 / 7

### System requirements

2.5 GHz or faster processor
2 GB memory (RAM) or higher
Hard drive capacity: at least 500 MB for installation package

### Signature exchange formats

Supports all AdES signature formats in accordance with eIDAS (B-B, B-T, B-LT):
PAdES (PDF signature; *.pdf)
CAdES (PKCS#7 sign.; container: pk7, p7m / detached: p7s)
XAdES (XML signature; detached / enveloped), XMLDsig
EDI signature (embedded and AUTACK);
GS1 EANCOM DE, Ideal Message Swiss, EANCOM AECOC ES, Editel® CZ, GS1 EANCOM CZ, Edicom® / GS1 EANCOM FR;
2D barcode stores signature on paper and fax (*.pdf, *.tif, fax group 3 and 4)

### Supported signature cards

It is necessary to use so-called multiple (multisign) signature cards that enable several signatures to be generated with a single PIN entry.

digiSeal®server supports signature cards from all major trust centres such as
Germany: D-TRUST, T-TeleSec, DGN/medisign, Bundesnotarkammer
Switzerland: Swisscom Solutions, Quo Vadis, GS1 Switzerland, SwissSign
Austria: A-CERT, A-TRUST

Please find further information about the technically supported cards in our technical specification.

### Certificate format

X.509 v1 bis v3, DER coded

### Signature algorithms

ECDSA, RSA (with following hash algorithms)

### Hash algorithms

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

### Encryption algorithms

asymmetric: RSA;
symmetric: 3-Key-Triple-DES, AES, RC2 and PKCS#5 for generating keys

### Key storage

Signature cards: ISO 7816 SmartCards;
Software certificate: PKCS#12 (*.pfx, *.p12),
HSMs (via PKCS#11)

### Card reader

Class 1 to 3 / CTAPI, PC/SC

### Card communication protocol

T0, T1

### Timestamp support

acc. to IETF RFC 3161 Timestamp Protocol,
e.g. D-TRUST (SSL authentication),
T-TeleSec (HTTP authentication)

### Compliant with international standards

eIDAS, Common PKI (formerly ISIS-MTT), profile of internationally widespread and acknow-ledged standards for electronic signatures, encryption and public key infrastructures.

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

sales@secrypt.de
www.secrypt.de

Disclaimer: All rights reserved including misprints, errors and modifications.
Date: 2022/07

e.signature solutions