

# The signature server for automated mass signing and time stamping



Server software for automatic signatures for large document volumes, signature verification and timestamps

For invoices, credit notes, delivery notes, technical documents, quality documents, legal documents, etc.

Legally compliant

For in-house use and deployment by outsourcing and application service providers (ASPs)

Simple and convenient handling

eBilling & invoicing: compliant with EU Directive, international regulations and national legislation

Usable worldwide e.g. in the EU, Switzerland, USA, Brazil, Chile and Mexico

Paper-bound business processes require the transfer and archiving of physical documents. The costs for printing, enveloping, postage and storage, for example, are immense. However, when supported by a corresponding regulatory framework, the electronic signature now enables such processes to be completed without paper both in business and administration, and in so doing offers considerable savings potential.

The electronic signature verifies both the identity of the signatory and the integrity of the document itself – therefore making it impossible to manipulate documents without being noticed.

### Example: International eBilling

EU-Directive, international regulations and national legislation (e.g. the German Value Added Tax Act, Art. 14 UStG) also allow electronic billing to be accepted for VAT purposes as long as the authenticity of the origin and the integrity of the content of the electronic invoice is ensured.

Electronic signatures meet these requirements and are standardised internationally.

### Authentication with verification documentation

digiSeal® server enables automatic verification of all current standard-compliant signature formats, whereby GDPdU-compliant verification documentation can be generated in PDF/A or XML formats if required. The recipient can also manually verify incoming signed documents very easily using the free digiSeal reader verification software. In addition, PFD documents signed with digiSeal® server can also be easily and quickly checked using Adobe® Reader without the need for plug-ins.

### Always the right format for generating and verifying signatures

digiSeal® server generates qualified, advanced and simple signatures, and supports all standard signature formats. Therefore a format can always be used that meets the requirements of the sender and recipient. When signing a PDF/A-compliant document, the PDF/A conformity is preserved.

#### Signature formats:

- PKCS#7 signature
- PDF and PDF/A signature
- XML signature (XML-DSig and XadES)
- EDI signature
- 2D barcode stores signature on paper and fax
- Time stamp signature (RFC 3161)



secript GmbH  
Bessemerstr. 82  
D-12103 Berlin  
Germany

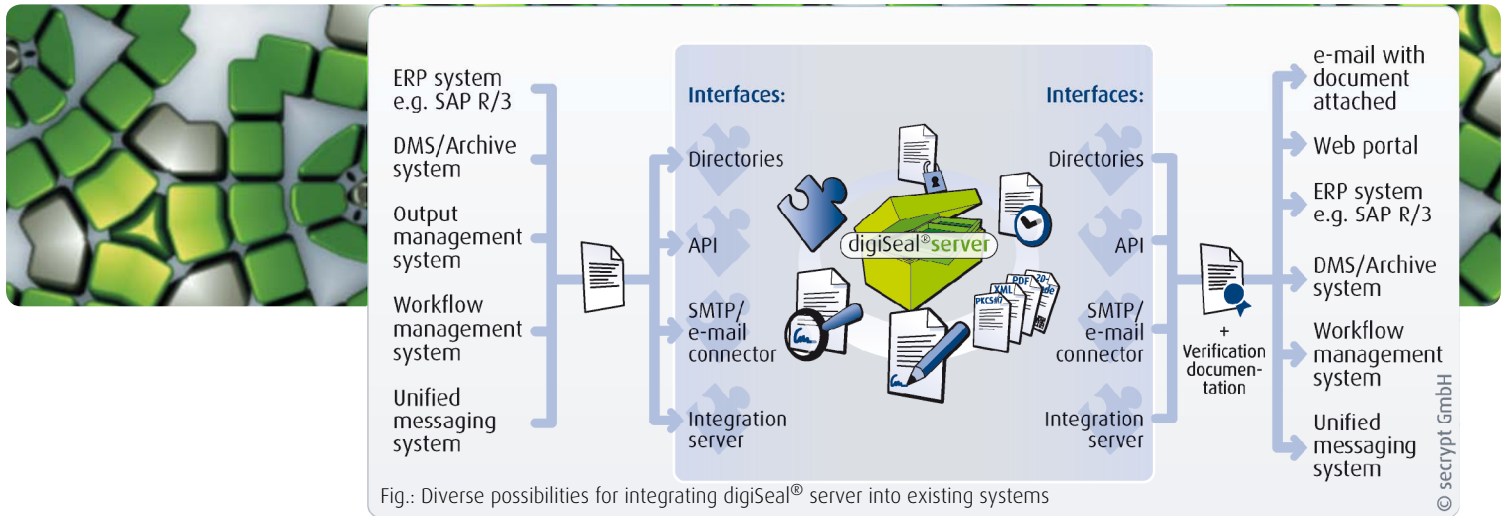
Phone: +49 (0)30.756 59 78-0  
Fax: +49 (0)30.756 59 78-18

sales@secript.com  
www.secript.com



Fig.: The toolbox for automatically securing documents

# digiSeal<sup>®</sup> server: The toolbox for individual signature and timestamp solutions



### Integration in the components from, e.g., the following providers:

- 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
- ...

### Integration possibilities

digiSeal<sup>®</sup> server can be integrated into existing document generation and document management systems, such as DMS and ERP systems, via directories, a program interface (C-API), SMTP or an integration server (see figure above).

### Multi-process capacity / convenient user interface

digiSeal<sup>®</sup> server can execute a diverse range of processes in parallel. The functions 'Sign', 'Verify', 'Time stamp', 'Encrypt' and 'Send by e-mail' can be combined with one another.

Example: A document is signed, encrypted and then sent by e-mail – in just one process. Other processes with other tasks such as 'Time stamp' or 'Verify' can be carried out in parallel.

The processes and operation are administered via a redesigned, convenient user interface.

### Cross-border use, e.g. EU



digiSeal<sup>®</sup> server can be used internationally – regardless whether operating from Germany, Austria, another EU country or Switzerland. secript GmbH offers users comprehensive support in implementing corresponding projects, such as, for example, advising on the underlying regulatory framework in specific countries.

### Farming / System stability

To increase performance and system stability, digiSeal<sup>®</sup> server can also be used for server farms.

### Trust centres /

#### Signature Cards / Software-based certificates

It supports legally compliant signature cards from all German trust centres as well as signature cards from various EU Member States and Switzerland. Additional new signature cards are regularly incorporated into the software. In order to automatically generate electronic signatures, the signature cards used must meet specific technical prerequisites. In particular, the signature card must ensure that several signatures can be generated with a single PIN entry. In addition, software-based certificates can also be used for simple and advanced signatures.

### Encryption:

#### Protects against unauthorized viewing

Sensitive data, such as personal information subject to data protection requirements, need to be protected against unauthorized viewing through encryption procedures when being archived or transported. digiSeal<sup>®</sup> server supports the high-performance, automatic encryption of documents both with passwords and public keys used in X.509 certificates.

# digiSeal<sup>®</sup> server: High security, flexible and powerful

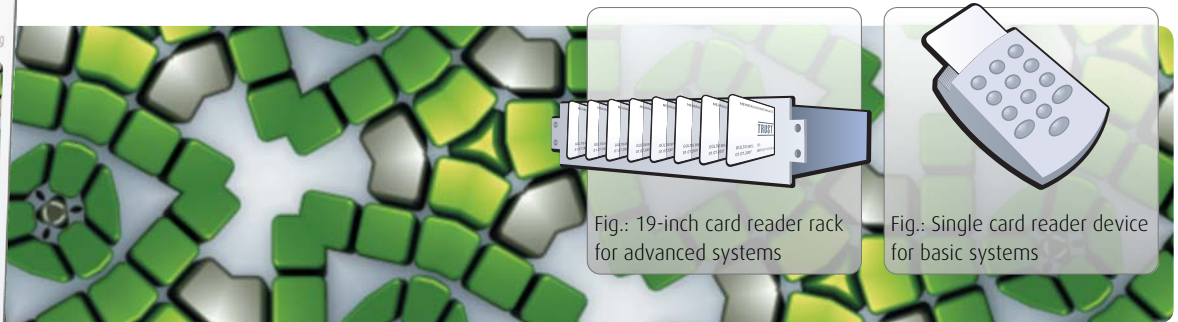
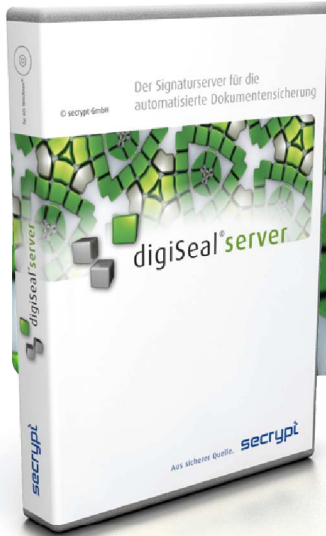


Fig.: 19-inch card reader rack for advanced systems

Fig.: Single card reader device for basic systems

## What's New in version 2.2.2.0

Operating as  
Microsoft<sup>®</sup> Windows<sup>®</sup> service

separate GUI for  
configuration and operation

extensive user administration  
(incl. comprehensive  
access rights and  
role concepts)

verification documentation  
in more languages  
(DE, EN, ES, FR, IT, NL, PL)

## Security

In order to prevent the misuse of qualified signatures that are automatically generated, the respective system must always be used in a secure environment. Furthermore, the Bundesnetzagentur (German Federal Network Agency) requires that before signing data, the signature key holder must be able to first of all view the content of the data and, only after verifying that it is correct, start the signature process by entering the PIN when specifying a time window or a maximum number of signatures. digiSeal<sup>®</sup> server meets all these requirements.

Proof that digiSeal<sup>®</sup> server conforms with the German Digital Signature Act was established by means of a manufacturer's declaration submitted to the German Federal Network Agency.

## More features

- Automatic communication with external time stamp services
- Automatic document delivery by e-mail (e-mails can be additionally signed with a software-based certificate)
- E-mail alert system for reporting operational events
- Comprehensive document-related logging of completed processes
- Multiple signatures in a single document
- Security mechanisms to prevent misuse of automatically generated signatures (see "Security")
- Secure PIN entry directly on the card reader
- Self-verification mechanism within the software

## Technology

### Operating systems:

Windows<sup>®</sup> Server 2008 / 2003 / 2000  
Windows<sup>®</sup> 7 / XP / Vista / 2000

### System requirements:

current processor, e.g. Intel Core2Duo or AMD Athlon / 2 GHz or higher;  
2 GB memory (RAM) or higher;  
hard drive capacity:  
100 MB for installation pack

### Common PKI (formerly ISIS-MTT)

The Common PKI Specification describes a profile of internationally widespread and acknowledged standards for electronic signatures, encryption and public key infrastructures.

### Signature exchange formats:

PKCS#7/CMS embedded (\*.pk7);  
PKCS#7 detached (\*.p7s);  
PKCS#7 S/MIME multipart-signed (\*.p7m);  
PDF signature (\*.pdf according to Adobe PDF Reference 1.6);  
XML signature (\*.xml according to XML-

DSig); expanded XML signature (XAdES);  
2D barcode stores signature on paper and fax (\*.pdf, \*.tif, Fax Group 3, Fax Group 4 for signed fax delivery);  
EDI-Signature (embedded und AUTACK) GS1 EANCOM DE, Ideal Message Schweiz, EANCOM AECOC ES, Editel<sup>®</sup> CZ, GS1 EANCOM CZ, Edicom<sup>®</sup> / GS1 EANCOM FR

### Certificate format:

X.509 v1 to v3, DER-coded

### Signature algorithm:

RSA (with following hash algorithms)

### Hash algorithms:

SHA1, SHA-2, SHA-224, SHA-256, SHA-384, SHA-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)

### Card reader:

Class 1 - 3 / CTAPI, PC/SC

### Card communication protocol:

TO, T1

### Time stamp support:

according to IETF RFC 3161 Time Stamp Protocol; D-TRUST time stamp with SSL authentication; T-Telesec time stamp with HTTP authentication

### Supported signature cards:

In order to use digiSeal<sup>®</sup> server it is necessary to deploy so-called multiple (multisign) signature cards that enable several signatures to be generated with a single PIN entry. digiSeal<sup>®</sup> server supports signature cards from all major trust centres and CAs such as D-TRUST, TC TrustCenter, T-TeleSec, S-TRUST, Signtrust, Bundesnotarkammer, PCA-1, Swiscom Solutions, Quo Vadis, GS1 Switzerland and A-CERT.



A product by

secript GmbH  
Bessemmerstr. 82  
D-12103 Berlin  
Germany

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

sales@secript.com  
www.secript.com