



Data Security on IBM i

Signature & Encryption on IBM Power Systems

- » Automation
- » EDI- and Data Conversion
- » Communication
- » Signature & Encryption
- » Archiving



»» SIGNATURE & ENCRYPTION

„Safety First“ is „Safety Always“
Uncompromising data encryption, legally
compliant signatures and verification of
digital identities provide seamless security.



» *CRYPT – Uncompromising Security with 2048bit Encoding



» Security for your B2B



Data protection, back up, and security are keywords for safeguarding a company. Companies with B2B processes are focused on the integrity of electronic business transactions. A faulty security concept will most likely create a financial trap for companies due to internal or external data abuse. Many small and medium sized companies fail to implement effective security techniques.

Limited resources and concerns about administration costs are the main obstacles. i-effect®, the data integration solution, can help eliminate these obstacles.

The i-effect® *CRYPT module is an elegant solution integrated into your workflow for signing and encrypting sensitive business data directly on the IBM Power Systems for local storage and external distribution.

With i-effect®, you can sign and verify PDF documents. The signing function is integrated into the i-effect® *CRYPT module. For conversion of business data, the combination of the i-effect® spool converter with the modules *SPOOL and *SPOOL+ is also available.

To give your e-mail recipients added security, you can sign all outgoing e-mails using i-effect®. This way, all your outgoing e-mails can be identified, the contents remain intact, and misuse of sender addresses can be prevented. The recipient can see if the e-mail was sent with a trusted sender's signature, even before opening it. The combination of the i-effect® *CRYPT and *EMAIL modules are available for this purpose.

» EDI Invoicing

In Germany, it is only possible to replace written legal documents electronically with a qualified signature. The most important use for companies is electronic invoicing with a mass signature, for high invoice volumes.

The i-effect® *CRYPT and *SIGG modules can be combined to link qualified electronic signatures with documents by using legally required chip cards.

» 2048bit Encoding with AES

In combination with the *ZIP compression module, i-effect® *CRYPT encrypts ZIP archives according to the Advanced Encryption Standard (AES). Encrypted data can be decrypted and edited on any platform, anytime, and with any AES-compatible application. After doubts regarding the security of the Data Encryption Standard (DES) were confirmed in the late 90s by a test deciphering, AES (or Rijndale algorithm) became the leading cryptosystem.

» *CRYPT Functions

Advanced Digital Signature and Signature Verification

- » PDF documents & other files
- » E-mail communication (S/MIME)
- » Designed for AS2 communication
- » Multiple signatures for PDF documents
- » Visible and invisible PDF signature
- » Automatic scaling of signature size
- » Signature algorithm: RSA (Hash SHA-1, MD5)
- » PKCS#7 signature of PDF documents
- » Certification format: X.509 v3, DER, and PEM encoded

Encryption & Decryption

- » Any files (symmetrical with AES, asymmetrical with 3DES)
- » AES (256bit), 168bit triple DES, RSA (512-2048bit)
- » E-mail communication with S/MIME (content) and SSL (Transport)
- » AS2 communication (content + transport [SSL])
- » Cross-platform

» Extra Security for your Online Data Transfer

» Qualified Electronic Signature and Encryption



i-effect® offers all required modules to give your business processes greater transmission and informational security. Purchasing from online shops, distribution and logistics between manufacturer, suppliers, and customers, or electronic invoicing are paths of business communication, which are secured with digital signature and encryption.

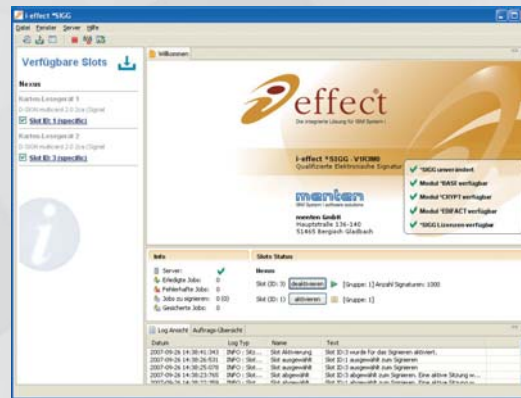
According to the German Signature Law (SigG), a qualified electronic signature can replace a personal signature. Such signatures are mainly used for invoices, which – depending on volume – can lower processing costs up to 90%. To sign invoice documents on the server, the signature module of i-effect® uses a signature generated by a chip card. Signatures can be attached to PDF invoices for e-mailing or to EDI messages.

Signature sessions (Slot) can be set up easily using the graphical interface (GUI) of the Java-based signature server. Signature operations can easily be added to document-related business processes.

Automating your administrative processes will allow you to make the best use of your time and human resources, and consequently, to devote them to revenue-generating activities and to gaining a competitive advantage. By eliminating expenses associated with paper-based invoicing (e.g. postage or printing costs), you will be able to significantly reduce your operating costs.

Additionally, invoices are delivered to their intended recipients much faster and more reliably. This, in turn, gives the recipients the possibility to digitally edit the received data, avoid late fees as well as to take advantage of cash discounts. Time and money are saved, because proofreading and changes in storage media are no longer necessary.

These standards also make data uneditable, data transfers confidential, and guarantee the authenticity of communications partners.



» Qualified Electronic Signature: *SIGG

Approved by the German signature law (SigG) and meeting the US (15 U.S.C. ch. 96) and EU eSign act requirements.

Signature

- » Creates signatures using P7S, P7M for e-mail attachments
- » Generates signatures for EDIFACT messages

- » Integrated PDF signatures (invisible, exact page placement, exact positioning, exact image placement, time/date, signature identity, reason for signature)
- » Certificate formats X.509 v3, DER-encoded
- » Signature algorithm RSA
- » SHA256 hash algorithm

Signaturprozess

- » Scalable signature performance (signatures per hour)
- » Additional Slot with *SIGG+; simultaneous activation of extra readers
- » Mass signature (1-time PIN entry)
- » Signature operations monitoring, self-test mechanism
- » Logging and caching of signature server jobs

Chip Card Slot

- » Secure PIN entry directly on the card reader
- » Overview of the available slots
- » Slot filter: display of mass signature capable slots
- » Individually modifiable validity values for signing sessions for each slot
- » Automatic slot deactivation when the validity expires

Requirements

- » Operating system: i5/OS V5R3 or higher)
- » Signature card D-TRUST multi-card (D-TRUST c-card V2.1)
- » Chip card reader SPR532

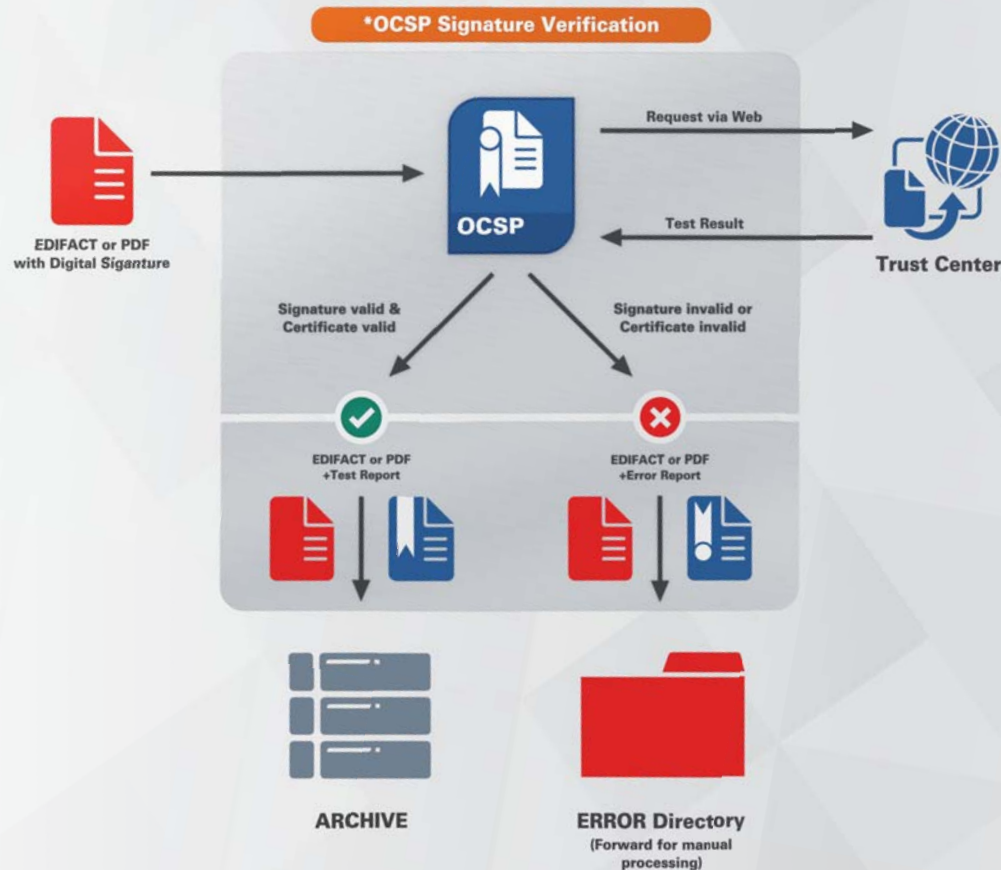
» Real-time Certificate Verification with *OCSP



The i-effect[®] *OCSP module provides information about the status of a certificate.

*OCSP offers quick and automated verification of certificates. *OCSP requests the status of the given certificate from a Trust Center via a secure Internet connection. If the certificate is valid, *OCSP verifies the incoming data and creates a verification report, which is added to the signed document and forwarded to the workflow.

If the certificate has expired or is blocked, an error message will be created and it will be forwarded for manual processing. By means of the manufacturers declaration, the product is compatible with SigG compliant applications, according to the German Signature Law, which increases the security of certificates.



» *OCSP Signature Verification

Signature Verification

- » Real-time status testing
- » Online testing of X.509 certificates
- » Automatic testing of signed documents at reception
- » Archiving of status logs
- » Output of the test reports in different languages
- » Communication protocols HTTP or HTTPS
- » Defined in RFC 2560

The i-effect[®] *OCSP module can be combined with other modules!

»» Modular Structure for Perfect Integration in Every Work Environment

The modularly built standard software i-effect® is the only IBM Power Systems solution, which controls the complete workflow and lifecycle of electronic data exchange, independent of sector and server-based and opens new and existing markets.

»» FOUNDATION MODULE



***BASE**
Central control of all modules. Base module of all i-effect® implementations. Contains WebControl.

»» AUTOMATION



***SERVER**
i-effect® workflow automation and management of other processes and applications.

»» HIGH AVAILABILITY



***IASP**
Connection to IBM's high-availability solution, directly on IBM i via XSM and iASP.

»» EDI – CONVERSION



***MAPGUI**
Graphical mapping application over the eclipse® expansion.



***XML**
XML – EDI Mapper, responsible for processing XML documents.



***EDIFACT**
UN/EDIFACT – EDI Mapper, responsible for processing UN/EDIFACT documents.



***TRADACOMS**
TRADACOMS – EDI Mapper, responsible for processing TRADACOMS documents.



***DB**
DB – EDI Mapper, responsible for processing databases like DB2, MySQL and Oracle.



***FLATFILE**
Flatfile EDI Mapper, responsible for processing Flatfile documents.



***X12**
ANSI X.12 – EDI Mapper, responsible for processing ANSI X.12 documents.



***CSV**
CSV – EDI Mapper, responsible for processing CSV documents.

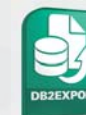
»» DATA – CONVERSION



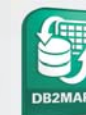
***SPOOL**
Converts SCS, AFPDS, IPDS, PCL, AFPDLINE Spool's into PC formats such as PDF, XLS, HTML, TIF, GIF, RTF, TXT, SAV...



***SPOOLMAPS**
Report definitions for outputs in XML, XLS and DB2.



***DB2EXPORT**
Direct export from DB2 databases in CSV, XML, XLS, HTML, PDF.



***DB2MAPS**
Export definition for XML, XLS and XLSX. Excel import in DB2.




***REPORT**
Modern layout of database reports, fitted to your corporate design.





Tailor an i-effect[®] module combination to your specific needs and use the full version for a free, 30-day trial period.


» <http://www.i-effect.com>


» **COMMUNICATION**


 ***AS2**
Internet-based communication with electronic signature and encryption for secure EDI (EDI INT).

 ***HTTP**
Standard protocol for web communication. Transmission with SSL (HTTPS).


 ***FTP**
Send and receive large data volumes with FTP. (SFTP and FTPS with *CRYPT).

 ***FAX**
Send all printer outputs with eFAX – without hardware, without a fax server and without a modem.


 ***TELEBOX**
Send and receive with Telebox/400 service of the Deutsche Telekom or AS2 Gateway.


 ***EMAIL**
Send and receive e-mails directly with IBM i.


 ***OFTP**
Sending and receiving with OFTP (Odette File Transfer Protokoll) via ISDN X.25 or TCP/IP.

 ***SOA**
Supports and compliments an existing IT environment through request/response applications.


» **SIGNATURE & ENCRYPTION**

 ***SIGG**
Signature module for qualified digital signature. Approved by the German Federal Network Agency.

 ***OCSP**
Online tests of certificate status and verification of qualified digital signatures.

 ***CRYPT**
Secures data with unbreakable 2048-bit encryption.

» **ADDITIONS**

 ***ZIP**
Data compression for less data traffic. WinZip compatible for IBM i.






» Interested in our Solutions on IBM i?

Try i-effect® now on a „no cure – no pay“ base.



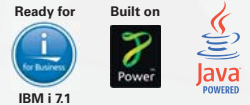
HERE IS THE MODEL:

---- NO OBLIGATIONS, NO HASSLE, NO FEES AND NO CREDIT CARD ----

-  You supply some basic system information.
-  We make a quotation without engagement.
-  You let us know if you accept the offer.
-  We install the i-effect® solution on your system.
(remote Teamviewer installation; on-site available on request)
-  You test i-effect® during 30 days.

AFTER THE TEST PERIOD:

- If you're not entirely convinced: we uninstall i-effect® and say goodbye.
No invoice is sent.
- If you're satisfied with the results: you simply continue using i-effect® and we send you an invoice according to our offer.



Orders, Information, Consultation



www.i-effect.com

For a free 30-day test version, detailed overview of module functions visit www.i-effect.com

You can also contact us at **+49 2202 2399 0**


menten GmbH – Short Profile



The company's main focus is on small and medium-sized businesses of all sectors using IBM Power Systems. Since 1989 menten's team has specialized in developing server-based IBM i Standard Solutions. Service and maintenance, system technology, and hardware sales accompany the IT services around the server family.

© 2014, menten GmbH. All rights reserved. i-effect is a registered trademark of menten GmbH. All other company, brand or product names can be the copyright of other companies. Errors excepted.





menten GmbH

 An der Gohrsmühle 25
51465 Bergisch Gladbach
Germany

 +49 2202 2399 0
 +49 2202 2399 23

 info@menten.com
 www.menten.com

 Managing Director: Ralph Menten
 Local court Cologne: HRB 47762