

Chapter 7b

Qualified Electronic Signature

Introduction

i-effect® *SIGG - At a Glance

- o Secure and closed system environment when used within IBM Power Systems .
 - o Parallel use of any number of card readers (scaling)
 - o Legally qualified signing
 - o High capacity mass signing of invoices.
 - o One license fee with an unlimited number of signatures.
 - o Integrated in i-effect® V1R5 or higher – the integrated solution for IBM Power Systems
-
- i-effect® *SIGG, the signature server module of i-effect® – the integrated solution for IBM Power Systems – can sign files generally, and PDF files in particular in accordance with the German signature ordinances (SigV) and the German signature law (SigG). The manufacturer’s declaration for i-effect® *SIGG is also in line with the requirements of SigV and SigG.
 - i-effect® *SIGG software is written in the Java programming language and requires a Java Runtime Edition of version 5.0 Update 6 or higher.
 - An installation license for the application software i-effect® - the integrated solution for IBM Power Systems -is required.
 - i-effect® *SIGG is the module which is responsible for generating qualified signatures.
 - i-effect® – the integrated solution for IBM Power Systems – creates and sends signature jobs to the signature server module i-effect® *SIGG. i-effect® – the integrated solution for IBM Power Systems – must be installed on the IBM Power Systems where the IXS PCI card is located. The *BASE module must also be installed in order to generate signature jobs. A detailed

description of the generation of signature jobs can be found under "Start Signature Job."

- i-effect® *SIGG offers a high level of security in a closed system environment.
- i-effect® *SIGG is run on an IXS PCI card within IBM Power Systems .

i-effect® *SIGG - Safe from Manipulation

To comply with the German signature law, i-effect® *SIGG is equipped with a mechanism that can diagnose manipulations of the software.

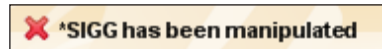
Even the setup file of i-effect® *SIGG can be tested. With our diagnostic tool, the hash sum of the file can be calculated and compared to the hash sum, corresponding to the setup file, on our website.

Successful testing gives the user reassurance that the setup file of i-effect® *SIGG is the original and has not been manipulated.

After i-effect® *SIGG is started, a status message as to the integrity of the software will be displayed.



Any manipulation is detectable directly after the application has been started.



If a manipulation is detected, signing sessions can no longer be activated. The server service, too, can no longer be started.

License

i-effect® *SIGG can manage and use several card readers for signature processes.

By purchasing **a license**, an **open slot** can be activated by one or more card readers for signature processes.

If the use of several slots for signature processes is desired, than the purchase of

more licenses is required. Every additional license guarantees the parallel use of one further slot.

The license encompasses the generation of signatures which are saved in a separate P7S file.

A license for the i-effect® module *CRYPT is required to create signatures, which will be embedded into the corresponding PDF document or saved in a file with the data that will be signed (P7M).

A license for the i-effect® module *EDIFACT is required to sign EDIFACT files with EANCOM 2002 Syntax 4; D.01B "Attached Digital Signature." "Attached Digital Signature" means that one signature will be generated for each EDIFACT message and embedded in this message.

After the start of i-effect® *SIGG the current status of the available licenses and modules will be shown.

A screenshot of the i-effect *SIGG status screen. The title is "i-effect *SIGG - V1R3 for i-effect V1R4M0" with the subtitle "Qualifizierte Elektronische Signatur". The Menten logo and company name "menten GmbH" are displayed, along with the address "Hauptstraße 136-140, 51465 Bergisch Gladbach". A list of status items is shown with green checkmarks: "*SIGG is fine", "Module *BASE available", "Module *CRYPT available", "Module *EDIFACT available", and "*SIGG license available".

Note: Slots are used to access the information which is saved on a SmartCard (provided by a Token). Signature jobs are processed by the logic which is contained in the slot.

Installation

Installation consists of many separate steps and requires Java Runtime Edition Version 5.0 Update 6 or higher.

In addition, the installation of a middleware is required, connecting one or more card readers with the inserted cards and the signature server. The software is an integral part of i-effect® *SIGG.

To view the original PDF documents and the signed PDF documents, in order to test the embedded signature, Adobe Acrobat Reader 8.x is required. Version 6.x of Acrobat Reader can be used, too. Version 7.x, however cannot be used to test the signed PDFs.

Recommendation: Currently, the verification software of D-Trust "D-SIGN Reader" is recommended for verifying signed files with separate signature files and PDFs. This software can be downloaded from the website of D-Trust (<http://www.d-trust.net>). Click on service and then on the left menu "kostenlose Prüfsoftware."

Installation of the Card Reader

The card reader CHIPDRIVE pinpad 532 from SCM Microsystems, which is in accordance with German signature law, is used.

Driver Installation

IMPORTANT! The driver must be installed and the system restarted before the card reader is attached!

The current driver version of the card reader will be on the installation volume. Start the installation by running "Setup.exe" and follow the installation instructions.

It is recommended that the option for manual restart is used.

Afterwards, the user will be asked to connect the card reader for a firmware update. This is normally not required, and possibly not desired, because for the generation of qualified digital signatures the Federal Network Agency only allows firmware version 4.15 or 5.10 for this type of card reader.

Note: A version downgrade can only occur by returning the device to the manufacturer.

Installation of Required Programs

Java Runtime Edition 5

The current version of Java Runtime Edition (JRE) can be downloaded from the Sun Microsystems website. The corresponding installation guide will also be available on the website.

Alternatively, a Java Runtime Edition installation file is included in the installation volume and can also be used. If you prefer to use this Runtime, you can open the installation file by double clicking. For the installation, please follow the installation instructions.

Middleware

The installation of the appropriate software for the SmartCard is also required.

It is also important to follow the legal guidelines for the generation of digital signatures. Restrictions for SmartCards may differ depending on the country.

The support of one additional signature creation device was integrated for Switzerland. Along with SmartCards from SwissCom that are based on CardOS 4.3B from Siemens, eTokens from Aladdin with qualified certificates from QuoVadis can also be used.

Middleware will either be provided by us or will be included with the SmartCard by the certification provider.

Supported Middleware

Only middleware that has a PKCS#11 standard interface can be used. The following is a list of compatible SmartCard-software-combinations and the countries in which they can be used.

Nexus Personal

Version: 4.6 or higher

PKCS#11 Library: personal.dll

(Standard) Path to PKCS#11-Library: \Program Files\Persona\bin

Supported SmartCard:

D-Trust multiscard (Germany)

Nexus Personal software will be included on the D-Trust installation CD/DVD. Start the file "PersonalSetup.exe" from the directory "NexusPersonal" from the CD and follow the installation instructions.

Siemens CardAPI

Version: 3.11 or higher

PKCS#11 Library: siecap11.dll

(Standard) Path to PKCS#11-Library: \WINDOWS\system32

Supported SmartCard:

Cards with Siemens CardOS 4.3B (Switzerland)

The middleware CardAPI from Siemens will either be provided on the installation CD or by the supplier.

To install the software, go to the subdirectory "Setup" of "Microsoft_Windows" of CardAPI Software and run the file "Setup.exe." Follow the installation instructions.

Aladdin PKIClient

Version: 4.5 or higher

PKCS#11-Library: eTPKCS11.dll

(Default-)Path of the PKCS#11-Library: \Windows\system32

Supported SmartCard:

eToken Pro 64K (4.2B) (Switzerland)

When using an Aladdin eToken, the software PKI Client from Aladdin is included on the installation media. Call up the 'PKIClient-x32-X.xx.msi' from the directory '04_Middleware\Aladdin eToken PKI Client' on the CD and follow the installation instructions.

A-Trust a.sign Client

Version: 1.2.x or higher

PKCS#11-Library: asignp11.dll

(Default-)Path of the PKCS#11-Library: \Windows\system32

Supported SmartCard:

a.sign Premium (Austria)

When using a a.sign Premium SmartCard, the software a.sign Client from A-Trust is included on the installation media. Call up the file 'acSetup.exe' from the directory '04_Middleware\A-Trust aSign' on the CD and follow the installation instructions.

Adobe Acrobat Reader 8.x

The Setup file for the installation of Adobe Acrobat Reader 8 can be found on the installation CD.

Installation of i-effect® *SIGG

If the requirements for the installation of i-effect® SIGG signature server software are met (Java Edition 5 or higher, middleware) the installation can be started by calling up the file "Setup_VxRxMx_Bx.exe."

The setup file name of i-effect® *SIGG can be interpreted thus:

VxRxMx is the version of i-effect® – the integrated solution for IBM Power Systems – with which the module i-effect® *SIGG is compatible.

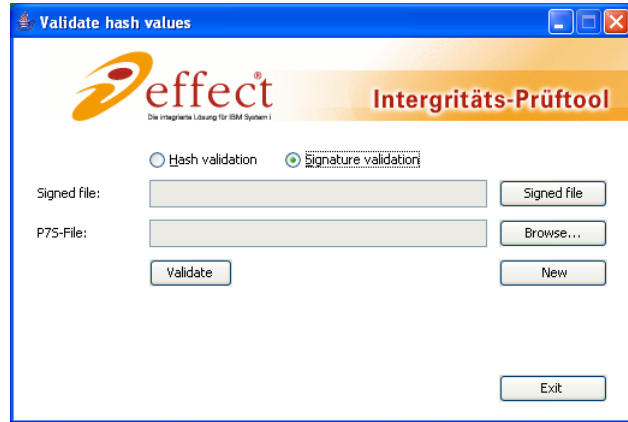
Bx is the current Build number of the i-effect® *SIGG module of this version. Newer builds have expansions or bug fixes of i-effect® *SIGG.

Testing the Integrity of the Setup File

If desired, the setup file of i-effect® *SIGG can be tested either with the CD/DVD or by the download area of the i-effect® website.

We have provided an integrity verification tool for this purpose. This tool is found either on the CD/DVD or in the download area of our i-effect® website.

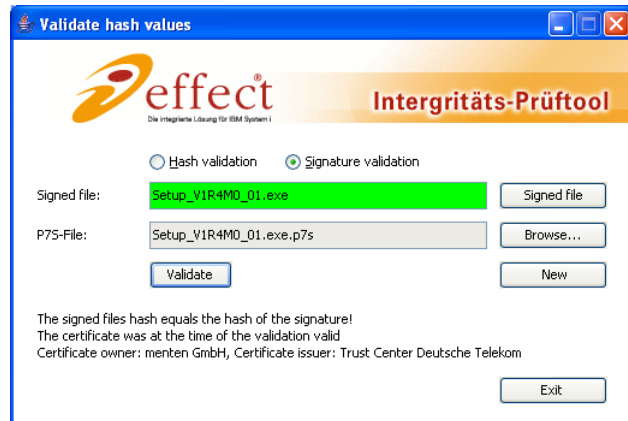
To start the verification tool, double click on the file "i-effect_Prueftool.jar" and choose "Signature Validation" from within the program.



Open i-effect® *SIGG's setup file by clicking on "sign.file."

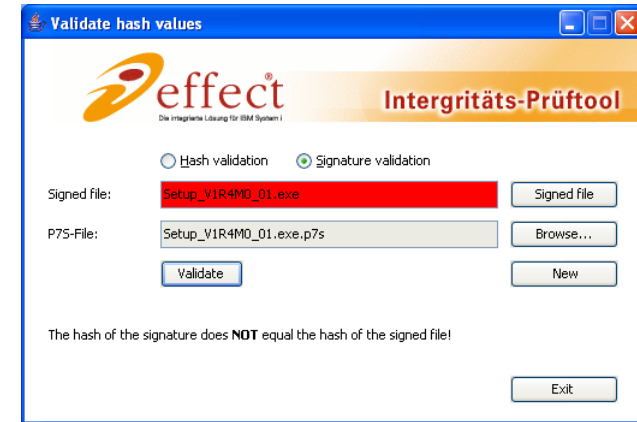
After the setup file has been opened, open the verification tool through "Browse..." and click on "Validate." The signature file has the same name as the setup file and ends with ".pks".

If the test was successful, the following display will appear:



Information about the validity of the certificate at the time of the test as well as information about the owner and creator of the certificate will be displayed.

An unsuccessful test will bring up this display:



Verify if the correct files were used.

If the correct files were used, do not use this setup file for installation! Download the setup file again from our website or from the installation CD.

Note: The software "D-SIGN" from D-Trust can also test the integrity of the setup file. This tool can test the online status of the certificate signature.

The software "D-SING Reader" can be found on the D-Trust's website (<http://www.d-trust.net>). Click on "Service" and then the link "kostenlose Prüfsoftware."

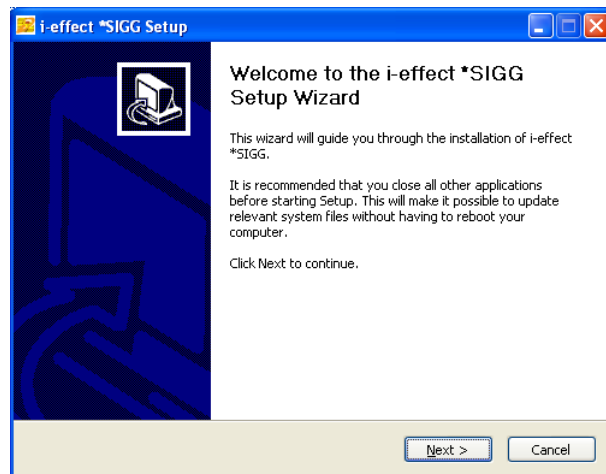
Installation of i-effect® *SIGG

After i-effect *SIGG's setup has been started, a window where the setup language can be chosen will appear.

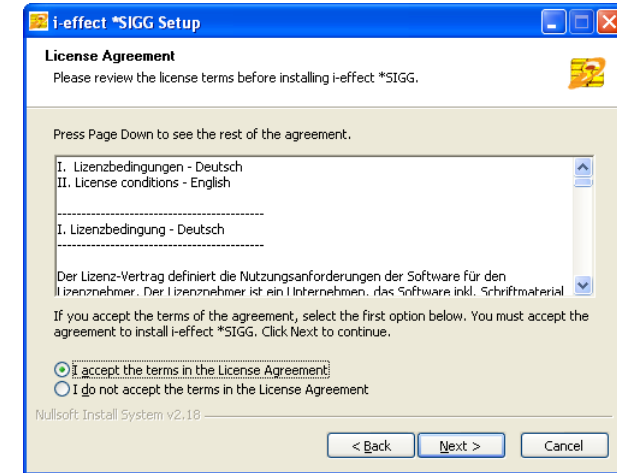
Choose the desired language or confirm the default setting by clicking on "OK."



The welcome message will give instructions for the installation of i-effect® *SIGG.

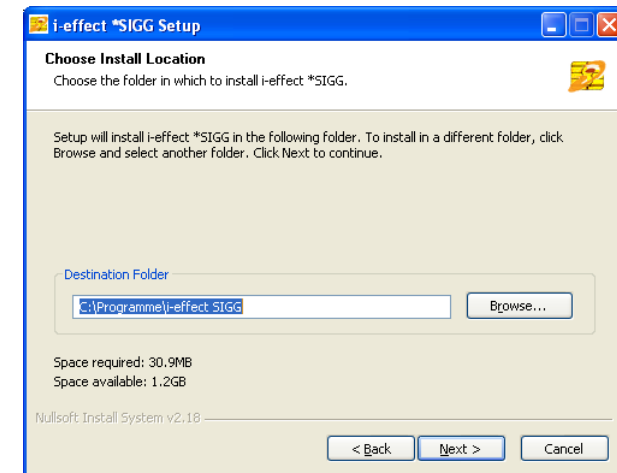


In the next dialog, the license conditions will be displayed.



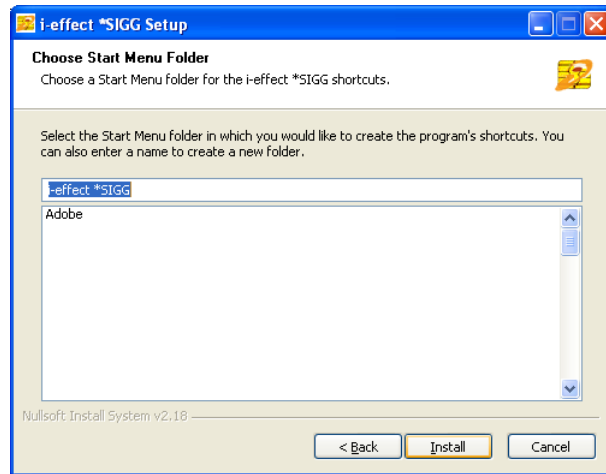
In this window, the install directory can be chosen manually.

We recommend the default directory path for the installation of i-effect® *SIGG.

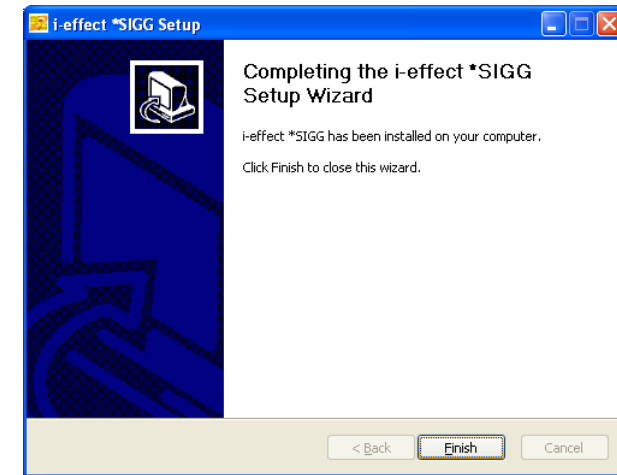


After the installation path has been determined, the start menu entry of i-effect® *SIGG can be assigned.

The installation starts after "Install" has been clicked.



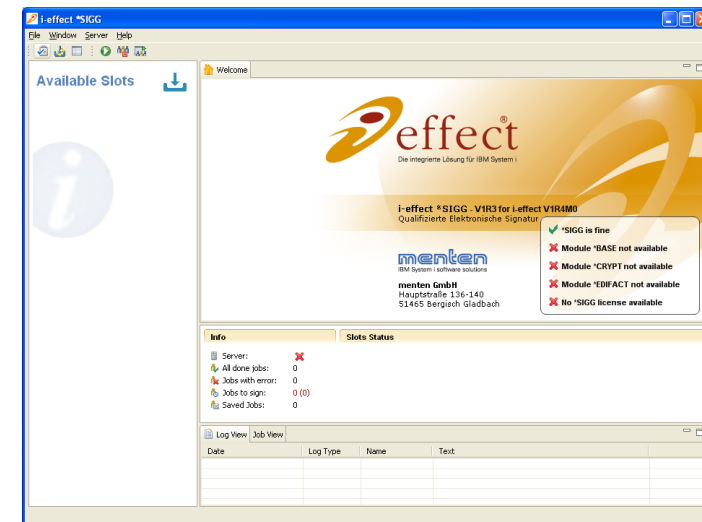
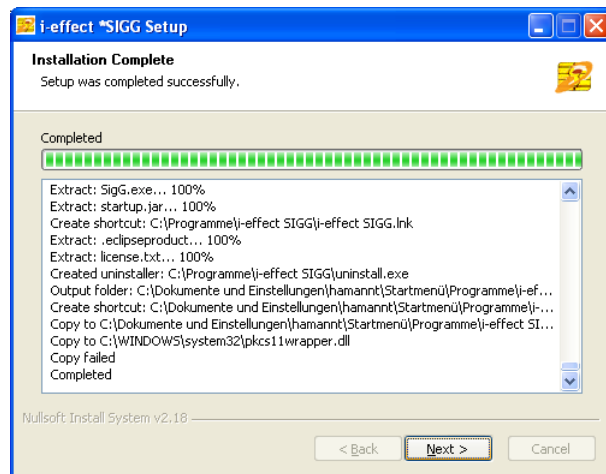
After installation a dialog will appear. Click on „Finish“ to end the installation program.



Setup

After successful installation i-effect® *SIGG can be started.

After the installation is complete, an overview of the actions that were performed will be shown.

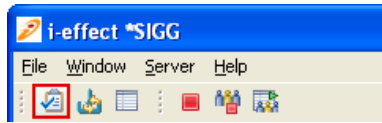


The next step is the setup of the application.

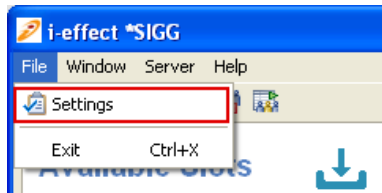
Program Settings

With the help of the settings dialog the configuration of the program can be changed.

The dialog can be opened from the toolbar:



Or from the menu File->settings:



The configuration dialog is divided into several tabs, from which the program components can be configured.

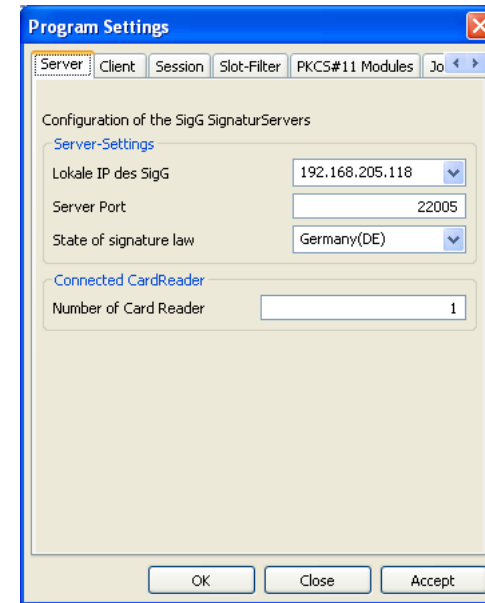
By clicking on "OK" the configurations will be saved and the window will close.

When values are changed, clicking on "Apply" saves them without closing the configuration window.

By clicking on "Cancel" the values that were changed will not be taken over and the configuration window will be closed.

Server

Through this tab, the IP address and port which will receive the incoming tasks can be determined.



The following server settings can be changed:

Local IP of SigG

Menu of the available IP addresses.

Server Port

The port on which the server waits for incoming tasks.

Default port 22005

Country

The choice of country ensures that only SmartCards, signature processes, and possible security measures for the generation of (qualified) electronic signatures, which are in compliance with that countries regulations, will be activated.

IMPORTANT: It is absolutely necessary that the correct country is chosen and not changed! If the country is not correct, it cannot be guaranteed that the generation of qualified electronic signatures is in accordance with the law, as stated in the manufacturer's declaration.

Number of Card Readers

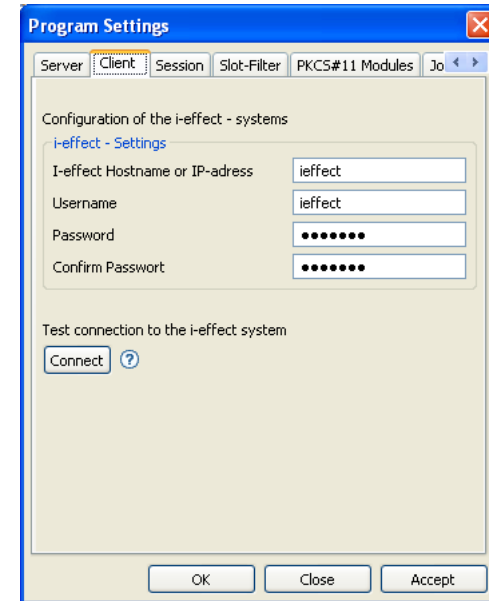
The number of card readers that are connected and will be used for signature processes.

Default Value 1

Client

The client, as far as i-effect® *SIGG is concerned, is i-effect® – the integrated solution for IBM Power Systems –, which sends jobs to the signature server.

The settings in this tab serve the signature server to access the i-effect® - IBM Power Systems in order to allow license queries, to realize that the processing of jobs can be followed via the i-effect® logbook, and to continue the processing of jobs which were aborted or interrupted.



The following settings for i-effect® access can be changed:

i-effect Host Name or IP address

The host name or the IP address of the system on which i-effect is installed.

User Name

The user name with which the signature server can login to i-effect.

Password

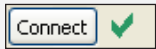
The current user's password.

Confirmation

Confirmation of the password which was entered before in order to avoid that a wrong password is saved.



The settings for the connection to the i-effect system can be tested with the button "Connect."



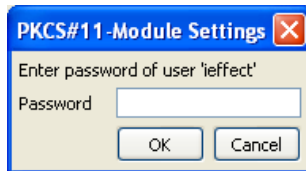
If the connection to the i-effect system was successful, then a green check mark will appear.



If the connection failed, then a red "X" will appear.

The cause of the error can be seen in the log display.

If no password was specified for the user, it can be entered here:



If no password was entered or saved for the user, a popup window will appear when clicking „Connect“ and the user will be asked to enter a password.

Session

The session is in effect, the central point of i-effect® *SIGG because signature processes can only be run in an active session.

Due to the fact that i-effect® *SIGG can produce mass signatures, it is required that the validity of a session be limited to fulfill the requirements of German signature law. The owner of the SmartCard decides how long a signing session for signature processes is valid.

The settings in this tab influence the standard validity of signing sessions for all slots of SmartCards.

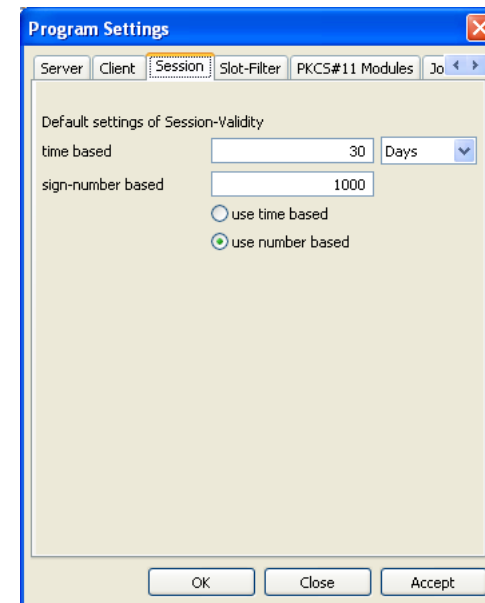
It is possible to adjust the signing session settings for the individual slots if more card readers are used.

Individual settings of a slot overwrite the defaults.

Information about individual settings for validity of slots can be found under "Slot Settings."

Once a session is activated, any* number of signatures can be generated. A limit on the number of signature processes or the time limit of session activities is required to fulfill the requirements of German signature law.

(* as long as the certificate is valid.)



Time Based

The value (in the chosen time unit) entered here will be added to the activation date when a signing session is activated.

A signing session that was activated on the 6/June/2006 at 12 PM and which is valid for 5 days, will be valid until the 6/June/2006 12 PM.

To create further signatures, a new activation is required.

Number Based

The value entered here determines the number of signatures which can be run during the signing session before the session loses its validity.

An active signing session with a predetermined value of 100 can only run 100 signatures before the session loses its validity.

To create further signatures, a new activation is required.

Use Time Based

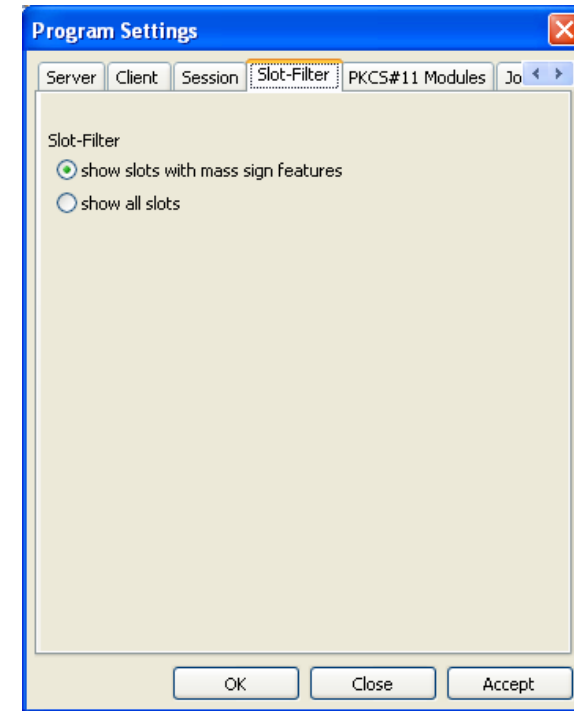
The validity of a signing session is determined by the specified time in the chosen time unit.

Use Number Based

The validity of a signing session is determined by the specified number of signatures that are to be realized.

Slot-Filter

This tab determine the slots to be displayed.

**Show Slots with Mass Sign Features**

Only slots which are able to produce mass signatures will be shown in the overview of available slots.

Show all slots

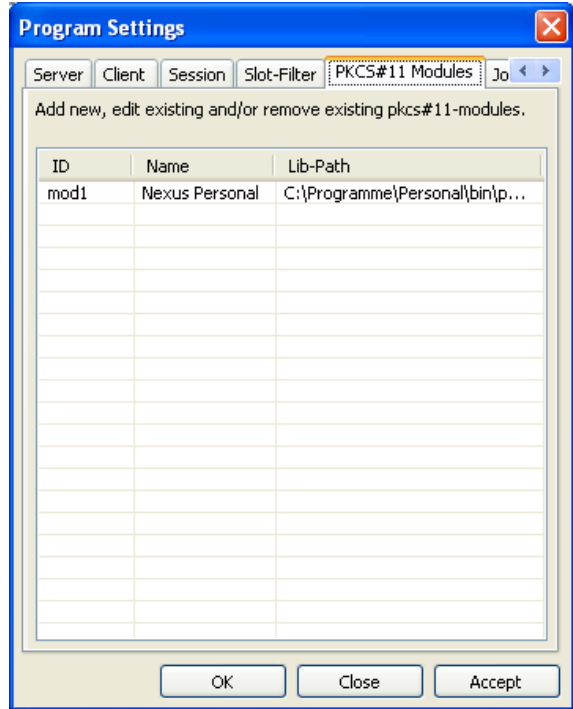
All available slots will be shown in the overview, even if they cannot be used.

PKCS#11 Module

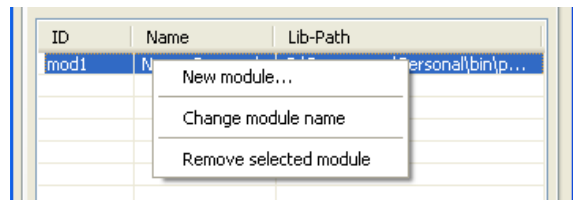
The tab PKCS#11 Module serves to manage the PKCS#11 Libraries. This tab allows to access the card reader, and therefore the inserted smart cards.

Generally, several modules can be integrated.

If the library was properly loaded during the runtime of the program, the overview of available slots with regard to their respective modules will be displayed.



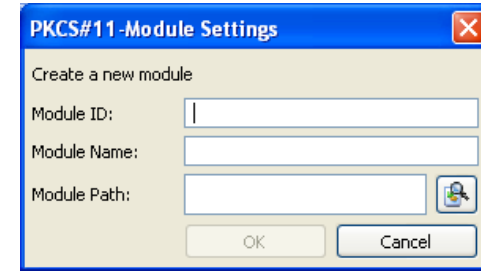
By clicking the right mouse button in the module table, it is possible to add modules, erase single modules, or edit the module name of an existing module.



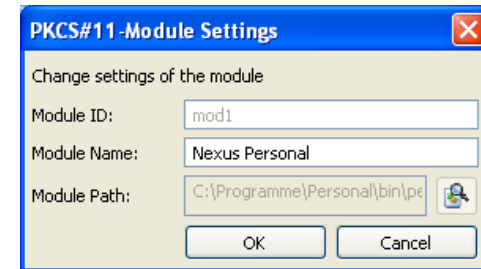
It is required that the module ID and the path to the module library be entered, if a new module is added.

The module ID must start with the letters "mod" which usually will be followed by a number (or character string) without spaces.

With the help of the file dialog, the module library can be searched on the system.



Only the module name can be changed, when editing the module.

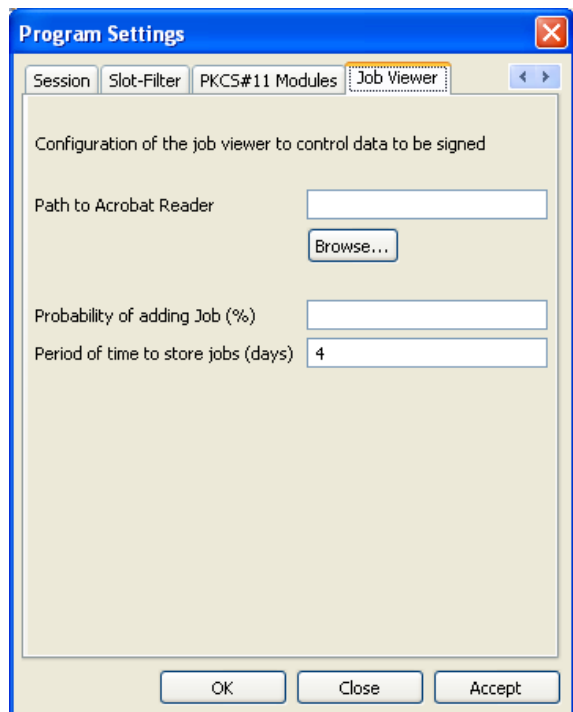


Job Viewer

The job viewer serves the user to save jobs sent to i-effect® *SIGG for monitoring purposes. The original files, which are to be signed, will be saved to enable the testing of job data.

The settings here determine the time in which the data will be saved and the probability of incoming job to be placed into the overview.

The path to the start file of Adobe Acrobat Reader should be entered here, so that PDF documents can be called up from the overview. All non-PDF files will be opened with the Standard Text Editor, if possible.



Adobe Acrobat Reader Path

To display PDF documents the path to the program file of Adobe Acrobat Reader must be specified.

PDF documents can be displayed with Acrobat Reader and checked for their integrity if an embedded signature exists in the PDF document. The verification is only possible with version 6.x and version 8.x.

Using Acrobat Reader version 7, the verification seems to function faultily and signals changes in the document.

Note: Non-PDF files will be opened with the Text Editor from MS Windows, if possible.

Probability of Acceptance (%)

Jobs which are sent to i-effect® *SIGG are placed in the job viewer with their appointed probability.

The German signature law requires that, before signing starts, a job overview is listed in order to check the data to be signed.

This makes sure that corrupted or manipulated data can be detected.

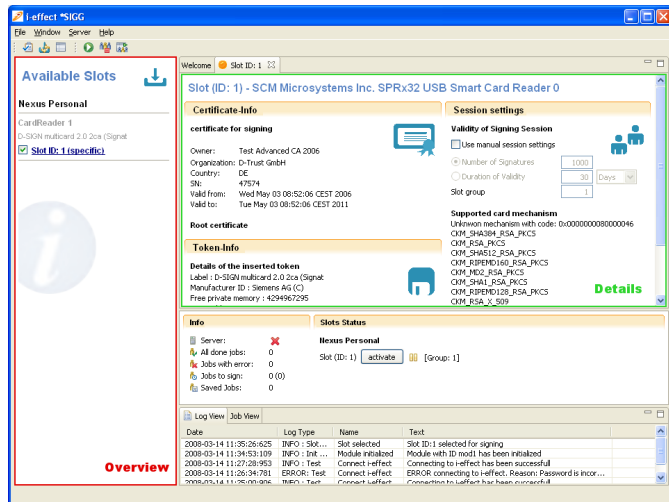
Choose a values between 5% and 100%

Storage Time (days)

The jobs, stored in i-effect® *SIGG for control purposes, will be deleted after the defined time has expired. .

Values between 1 and 7 can be specified.

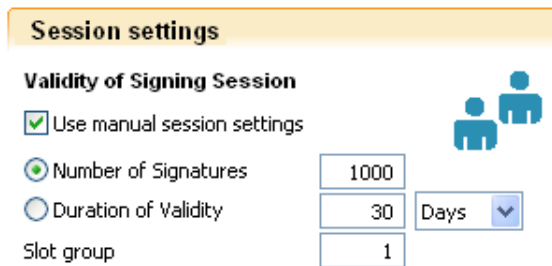
Slot Settings



By clicking on the link (slot specific) in the overview of available slots, the details of a slot will be called up.



The detailed display enables to determine the individual values for the validity of the signing session. The individual settings overwrite the default values, which were set in the program settings.



Use Manual Session Settings

By checking this box, the default values of the program settings will be overwritten and values that were provided for this slot will be taken over.

Number of Signatures

The number entered here determines the number of signatures that can realized after the slot has been activated. As soon as this number is reached, the slot will automatically be deactivated.

Duration of Validity

The option to determine the validity of a signing session, based on a time limit, sets the time interval and the time unit.

When the signing session is activated, the time when the session will lose its validity will be determined.

Slot Group

Allocating a slot to a card group allows the creation of a pool of slots, which serves to divide the jobs or to share the loads of signature jobs.

For example, one group can be used to sign invoices and another group to sign other files.

IMPORTANT: Changes that are made to the individual settings of a slot will be saved immediately and DEACTIVATE any active session of this slot.

The detail screen shows information about the certificate and the root certificate that are saved on the card.

This information includes the owner, the validity, and the serial number of the certificate.

Token-Info

Details of the inserted token

Label : D-SIGN multiscard 2.0 2ca (Signat
 Manufacturer ID : Siemens AG (C)
 Free private memory : 4294967295
 Free public memory : 4294967295
 Maximum PIN length : 8
 Firmware version : 1.00
 Hardware version : 1.00



Information about the token on the SmartCard can also be viewed.

Certificate-Info

certificate for signing

Owner: Rene Hamannt
 Organization: menten GmbH
 Country: DE
 SN: 194979
 Valid from: Wed Apr 18 09:25:37 CEST 2007
 Valid to: Fri Apr 18 09:25:37 CEST 2008



Root certificate

Owner: TEST D-TRUST Qualified CA 1
 Valid from: Wed May 03 08:44:41 CEST 2006
 Valid to: Tue May 03 08:44:41 CEST 2011

Program Launch

Before launching i-effect® *SIGG a few settings must be made, which are described here in detail.

Server Setup

- First, it is necessary to setup the server by confirming the IP address of the local system which will receive the server jobs.
- If a port other than the default port 22005 should be used, the new port must be entered.
- Note: Changing the port requires a change in the i-effect® system settings or indication of the target port at the start of a signature job.

Changes will be saved by clicking on "Apply"

More information about the individual points of server configuration can be found in the program settings.

Client Setup

- o Indication of the host name or the IP address of the system where i-effect® is being run.
- o Indication of a valid user name on the IBM Power Systems .
- o If desired, the password of the specified user can also be entered and saved.
 If nothing is entered, a password request will appear where it is required.
- o The settings can be tested by clicking on "Connect."

Changes will be saved by clicking on "Apply"

More information about the individual points of client configuration can be found in the program settings.

Setup of a PKCS#11 Module

- o To add a new module, use the click right on the table select "New Module" in the menu.
- o It is required to enter a module ID (which begins with the letters "mod").
- o Entering a module name is optional.
- o It is required that the path of the module library be entered.

Changes will be saved by clicking on "Apply" or "OK."

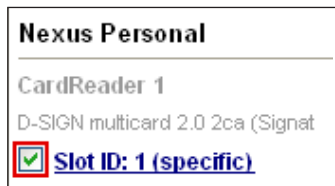
More information about the individual points of module configuration can be found in the program settings.

Session Activation for Signature Operations

Using signature options require an active session.

Slot Choice

A slot must be chosen by checking it in the overview.



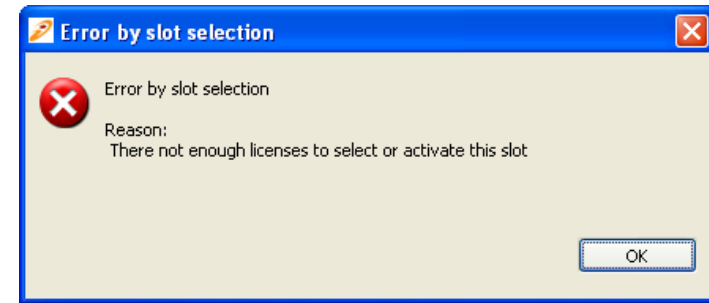
Note: Only slots supporting mass signatures can be checked. These slot will be marked "Specific."

License Testing

By checking a slot, the license test of i-effect® *SIGG will be activated.

It will be checked if the required number of licenses is owned in order to use the desired number of slots.

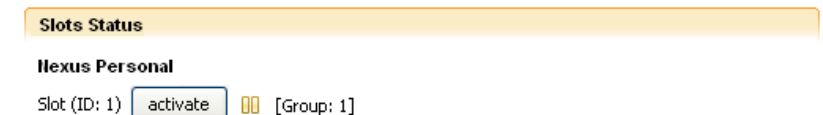
If the correct number of licenses is not owned to use the desired number of slots, the following error message will appear:



Display Selected Slots

If a slot was chosen, the slot will appear in the section "Slots Status."

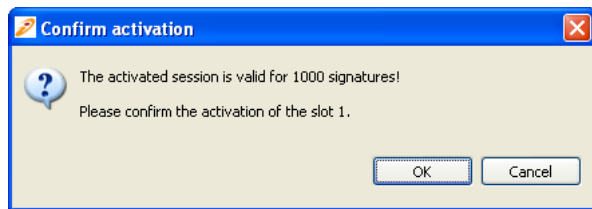
In this section, all chosen slots will be sorted according to their modules. All chosen slots are deactivated, which means that the session was not yet activated.



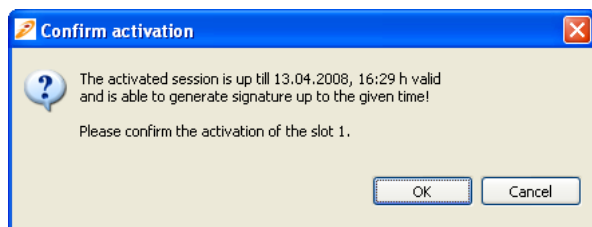
Slot Activation

Click on "Activate" to activate a slot and the generation of an active session for signature operations.

In order to make sure that the signature process meets the requirements of the German signature law and German signature ordinances, the user will be asked to confirm the job before the session is activated.



This dialog informs the user that only a fixed number (the current value will be displayed) of signatures can be generated, or that signatures can only be generated until the defined time period has expired (current value will be displayed).



The confirmation guarantees that the authorized person, in accordance with SigV, §15 (1) "at the generation of a qualified electronic signature c) "the generation of a signature will be previously clearly displayed." For mass signatures, it will be clearly stated how many signatures can be created, or for how long they can be created.

This dialog is country specific and will only be displayed if the country for i-effect® *SIGG configurations has been set to "Germany."

Entering the PIN for the token in the slot will be requested.

Depending on the SmartCard, the PIN will either be entered with the system keyboard or the card reader.

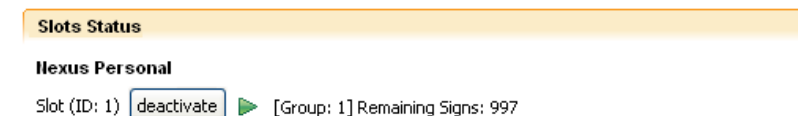
Note: In Germany it is required that the PIN be entered directly on the card reader. It is not allowed that the PIN is entered and transmitted by signature software. Therefore, only middleware and cards allowing that the PIN is entered directly at the card reader are permitted.

In Switzerland, the situation is different. The type of the certificate and the securing of the certificate in the signature creation device are important. A so-called eToken,

which is similar to a USB stick, and represents a card reader with an integrated SmartCard and without a PIN pad, can be used. The keyboard can be used for login.

The signing session will be initialized after the PIN was entered successfully. The default or the individual settings determine the validity of the session.

If the signing session was successfully activated, a green arrow will appear. The form of validity (number of signatures or time frame) and the number of remaining signatures or the ending time of the session will be displayed.



Note: The signature server will be started automatically if i-effect® *SIGG is not active at the time of session activation.

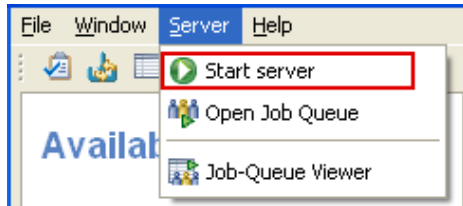
i-effect® *SIGG Start

i-effect® *SIGG can be started or stopped either from the tool bar or from the menu "Server".

Starting the server from the tool bar:



Starting the sever form the menu Server->Start Server



Start Signature Job

To start a signature job, calling up the green screen from i-effect® – the integrated solution for IBM Power Systems – is required.

To get to the menu for encryption and signatures, enter 12 in the i-effect® main menu and press enter.

```

IEFFECT          i-effect - The integrated solution for IBM System i
                                     System:  I5EFFECT

Options:

10. To the conversion tasks
11. To the compression tasks
12. To the signature- and encrypting tasks
13. To the communication tasks
    
```

By choosing menu item 3 and pressing enter, a job for the generation of a qualified signature can be created.

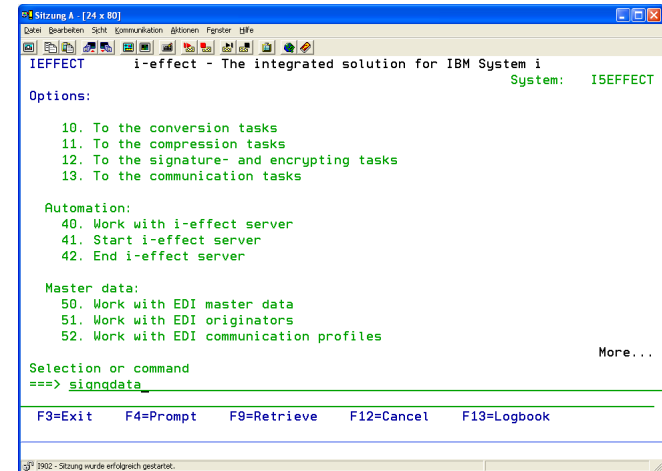
```

CRYPT          i-effect signature- and encryption tasks
                                     System:  I5EFFECT

Options:

Signature:
1. Sign PDF file(s)
2. Verify PDF file(s)
3. Sign file(s) qualified
4. Encrypt file(s)
5. Decrypt file(s)
    
```

Alternatively, the parameters of ,signqdata' will be displayed by entering the command SIGNQDATA and F4.

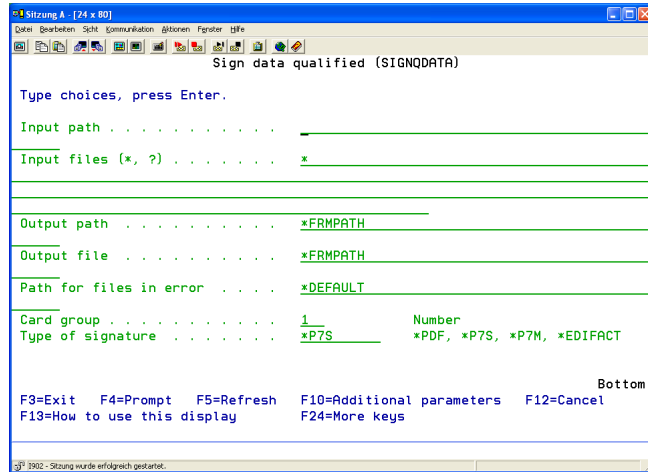


The functions for performing signature jobs can be determined here. Depending on signature type, there are up to three parameter pages, where the respective parameters can be specified.

Note: The command SIGNQDATA exclusively creates signature jobs, which i-effect® sends from the IBM Power Systems to the signature server (i-effect *SIGG). The signature job transfers information about the data, which is to be signed, and in which form the data will be signed. In order to avoid misuse of i-effect® *SIGG, the security concept of the IBM Power Systems allows the user to define authorized user for the command SIGNQDATA, .

On the first page, the basic parameter settings are made, such as file path entry and the selection of signature setting type. The selection of signature setting type sets the configuration dialog according to the settings.

By pressing F10 further pages of parameters, based on previous selections, can be displayed and paged through using the scrolling keys. F9 displays all parameters of the command.



Input Path [FRMPATH]

The absolute path of the file to be signed.

Input File(*,?) [FRMIFSFILE]

The file name of the files to be signed.

Output Path [TOPATH]

Optional: Absolute path of the output directory.

Default:

**FRMPATH* Determines the input path of the file.

Output File [TOFILE]

Optional: File name under which the signed file will be saved.

Default:

**FRMFILE* Uses file name of the input file.

In the case of PDF signatures, the original file name will be used. If **FRMPATH* is selected in the *TOPATH* parameter, the successfully signed PDF file will replace the original.

"p7" will be added to the file name if a P7S signature is used.

"p7m" will be added to the file name if a P7M signature is used.

In the case of EDIFACT signatures, the original file name will be used. If **FRMPATH* is selected in the *TOPATH* parameter, the successfully signed EDIFACT file will replace the original.

Path for Error Data [ERRPATH]

Optional: Path of the error directory where files that were not correctly signed will be stored.

Default:

**DEFAULT* Uses the default error directory. It can be found in the i-effect installation directory under *sigg/error*.

Card Group [CARDGROUP]

It is possible to assign slots to card groups. The card groups enable the user to generate one signature with one specific card. The signature job can only be performed by the slot that belongs to the corresponding card group.

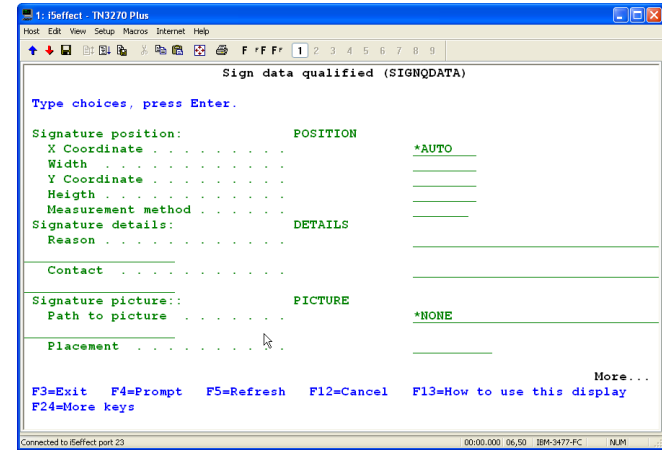
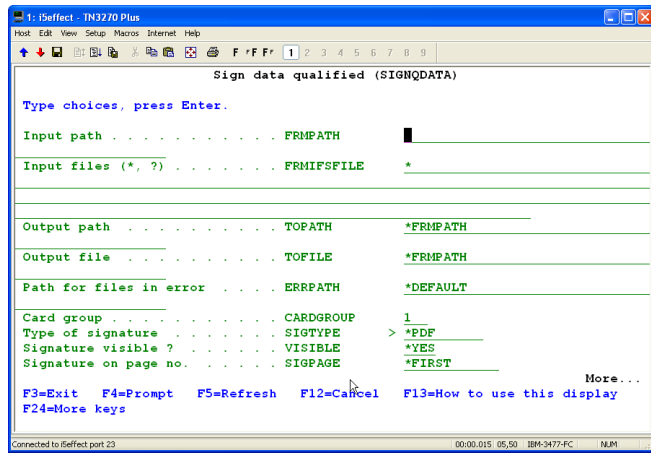
Signature Type [SIGTYPE]

There are four different signature types:

<i>*PDF</i>	The signature is embedded in the PDF document.
<i>*P7S</i>	The signature is saved in a separate "p7" file
<i>*PKCS7</i>	The signature is packed and saved as a file in the ,SignedData'-Container in the ASN.1 format.
<i>*P7M</i>	The signature is saved with the file in a new "p7m" file.
<i>*EDIFACT</i>	"Attached Digital Signature" according to EANCOM 2002 Syntax 4. All or only one message type will be signed. The signature(s) will be embedded in the original file.

Configuration for the Creation of PDF-Signatures:

If *PDF is selected as signature type, specific parameters that only apply to PDF signatures will appear on the first configuration page.



Configuration-Page 2 of ,signqdata'
(This form only applies to signature type *PDF):

Visible Signature [VISIBLE]

Only PDF signatures! Determines if the signature is visible in the PDF document.

Default:

- *YES Yes, the signature is visible.
- *NO No, the signature is not visible.

Configuration page 2 from "signqdata" (only visible with signature type *PDF):

Signature on Page No. [SIGPAGE]

Only PDF signatures! Determines the page on which the signature will appear.

Default:

- *FIRST The embedded signature will appear on the first page.

Signature Position [POSITION]

Only PDF Signature!

X-coordinate

Distance between the signature display and the left side of the PDF document.

Default:

- *AUTO The standard values will be used for the x- and y- coordinates, and for width and height.

x-coordinate: 1

width: 5

y-coordinate: 1

Height: 2

Unit of measurement: cm

Width

Width of the signature in the PDF document.

Y-Coordinate

Distance between the signature and the bottom of the PDF document.

Height

Height of the signature in the PDF document.

Unit of measurement.

Unit of measurement for the coordinates, width, and height, which determine the position in the PDF document.

Signature Details [DETAILS]

Only PDF signatures!

Reason

Optional: Reason for the signing the PDF document.

Contact

Optional: Contact information.

Signature Picture [PICTURE]

Only PDF signatures!

Path to the Image File

Optional: The path to the image file used as background for the visible signature in the PDF document.

The following file formats are possible: JPG, GIF, BMP, or PNG.

Default:

*NONE No image will be used. The PDF Reader uses its own standard image.

Alignment

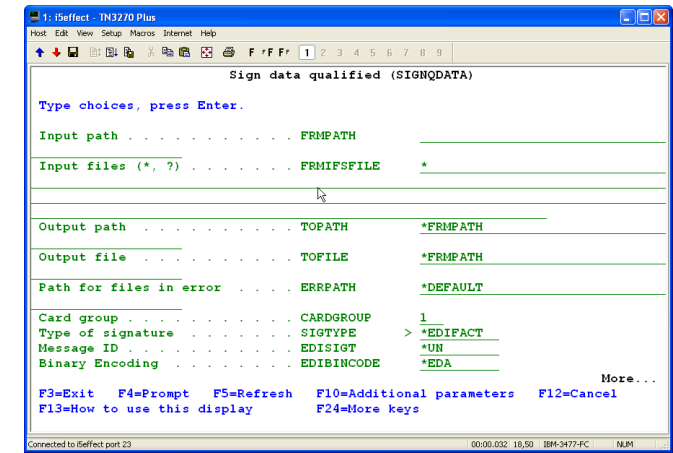
Optional: Determines the position of the image within the signature.

Possible Values:

- *RIGHT The image will be aligned middle-right.
- *LEFT (Default) The image will be aligned middle-left.
- *TOP The image will be aligned middle-top.
- *BOTTOM The image will be aligned middle-bottom.

Configuration for the Creation of an EDIFACT-Signature:

If *EDIFACT is selected as signature type, specific parameters that only apply to EDIFACT signatures will appear on the first configuration page.



Signature Type [EDISIGT]

The type or format of the EDIFACT signature can be specified here.

There are 4 types of EDIFACT signatures:

- *UN** (Default) The format defined by the UN for signing EDIFACT files, with the corresponding segments a data element.
- *EANCOM** Format recommended by EANCOM for signed EANCOM files with the corresponding structure of segments and data elements. Generally corresponds to the UN format.
- *IMS30** The "Ideal Message Switzerland" format of signed EANCOM-based files Version 3.0.
- *IMS31** The "Ideal Message Switzerland" format of signed EANCOM-based files Version 3.1. The only difference to Verion 3.0 is a correction of data element structure.

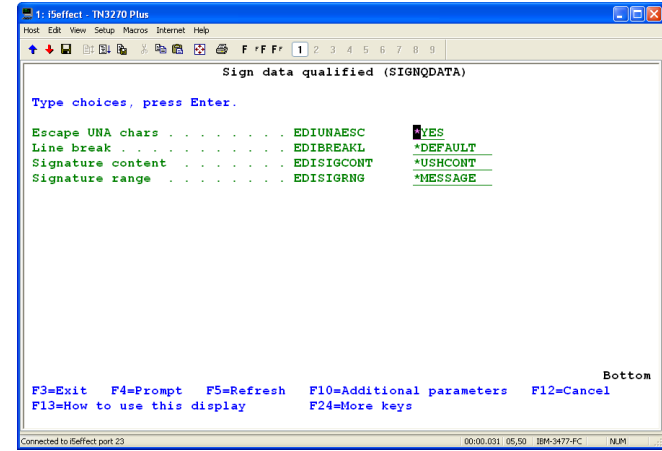
The format corresponds to the EANCOM format for signed EANCOM files, because IMS VerSsion 3.1 was developed as a basis for the EANCOM standard.

Binary Encoding [EDIBINCODE]

This encoding format, in which binary values of data elements are encoded, is used to insure that no forbidden characters are used.

Four encoding types are possible:

- *EDA** (Default) The EDA filter according to ISO 9735-5 is an encoding that creates binary data in a coded record with the character range from UNOA. Data records increase in size because of encoding at a rate of 3/2. 2 of the 3 parts are reference data (50% larger data volume)
- *EDC** The EDC filter according to ISO 9735-5 is an encoding that creates binary data in a coded record with the character range from UNOC. The data record increases in size because of encoding at a rate of 8/7. 7 of the 8 parts are reference data (17% larger data volume)
- *HEX** HEX encoding converts binary data into a hexadecimal character string with characters 0-9 and A-F. The encoded data volume doubles the size of the actual binary file size.
- *BASE64** BASE64 encoding converts binary data into a string of printable characters, which consists of 64 characters: A-Z, a-z, 0-9, +, / (without umlauts and ß). The size of the encoded data volume increases approximately 33% over the original data volume.
- *NONE** No encoding will be used. Binary data will be added to file unencoded.



Configuration Page 2 of ,signqdata' (Only visible for *EDIFACT signature types):

UNA Escape Charaters [EDIUNAESC]

Determines if the UNA characters in the newly inserted signature segment of the EDIFACT file will be replaced with escape characters.

Possible Values:

- *YES** (Default) UNA characters present within the new segments will be replaced with the escape character defined by the UNA segment (',' is the standard character).
- *NO** Existing UNA characters within the new segments will not be replaced with escape characters.

Line Breaks [EDIBREAKL]

This parameter determines if a CRLF will be inserted at the end of a segment or not. Depending on the settings, the original file will be changed and line breaks will be inserted or removed.

Alternatively, the default setting can be used, which leaves the file unchanged with regard to line breaks.

Possible Values:

- *DEFAULT** (Default) The file will be left unchanged with regard to existing or non-existing CRLF characters.
- *YES** If no line breaks are in the original file, they will be inserted.
- *NO** Line breaks in the original file will be removed.

Signature Content [EDISIGCONT]

This parameter determines which contents will make up the signature, when EDIFACT messages are signed.

Possible Values:

- *USHCONT* (Default) The new signature header and the contents of the message will be signed. Existing signature segments from previous signature processes will not be used in signature calculation.
- *USHTOUST* Message contents from the beginning of the new signature header to the new signature trailer segment will be used in signature calculation. Previous signatures in the message will be a part of the new signature.

Signature Range [EDISIGRNG]

This parameter sets the signature range within an EDIFACT interchange (files).

Possible Values:

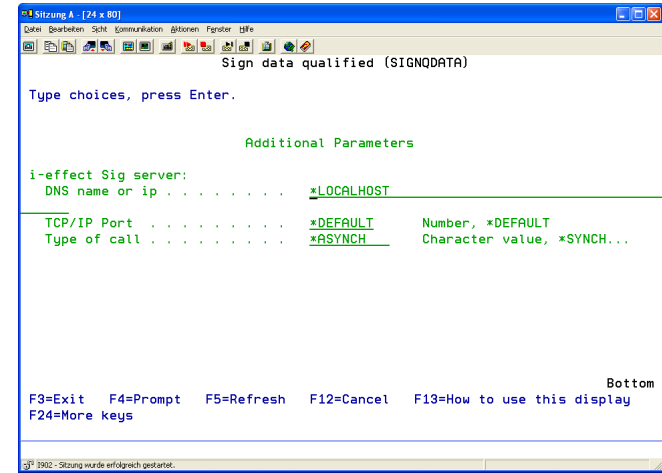
- *MESSAGE* (Default) Every message of an interchange will be signed (as long as the message type was not limited with EDITYPE).
- *INTCHANGE* The entire EDIFACT data stream (file) will be signed. Only one signature will be created for the all of the received data.
- *GROUP* Every group within an EDIFACT interchange will be signed.

EDIFACT Message Type [EDITYPE]

Either all message types (**ALL*) or one specific message type can be signed (e.g ORDERS, INVOICE).

Default Setting:

- *ALL* All message types of EDIFACT files will be signed.



Final Configuration Page of ‚signqdata‘:

i-effect *SIGG Server [EFFSERVER]

DNS Name or IP

Name or IP address of the system where the signature server is run.

Default:

**LOCALHOST*

Note: The IP address of the sever must be entered because the signature sever is not run locally.

TCP/IP Port

TCP/IP port of the signature server.

Default:

**DEFAULT* The default port of the i-effect system will be used (22005).

Type of Query

Determines how the server will deal with requests.

- *ASYNCH (Default) The signature server causes i-effect not to wait for the end of a signature job.
- *SYNCH i-effect waits until a signature job has been ended by the signature server.

System Monitoring

Overview of Running Program Activities

The overview informs the user about the activities executed by i-effect® *SIGG.

Info

- Server: ✘
- All done jobs: 0
- Jobs with error: 0
- Jobs to sign: 0 (0)
- Saved Jobs: 0

Server

This field shows whether the signature server is running (green check) or is deactivated (red X)

Finished Jobs

This field shows the sum of all successfully completed signatures of individual files since the start of the program.

Incomplete Jobs

Shows the sum of incomplete jobs.

Jobs to Sign

The first value is the number of jobs that are to be signed.

The second value (in parentheses) is the number of jobs that have been cached because of a repairable error but that have not yet been placed in the queue again.

Note: The display of the jobs queue shows the jobs in the queue and jobs in the buffer in order to delete them.

Saved Jobs

Shows the number of saved jobs. Jobs will be saved if the server is stopped, even if the jobs are in the queue. At the next start of the server, these jobs will be restored.

If the system crashes or fails or the program crashes, jobs will be restored in the same manner.

Note: *SIGG jobs that are started synchronously will not be saved; they will be ended by ABORT.

Job View

In the menu "Job View" all jobs will be displayed that were deposited in i-effect® *SIGG, based on their probability. This overview is a test mechanism, which allows a spot check of the data to be signed.

This control mechanism checks the data for possible manipulation from unauthorized persons and meets the German signature law, which requires that data (the non-signed version) be viewable before signing.

Session	Original	Signed	File-Name	Sign-Type	Inserted
334			invoices.pdf	PDF	2008-03-14 12:19:13:625

Session

Shows the session number under which the job will appear in the i-effect logbook.

Original

With a double click on the symbol the original file can be displayed with Adobe Acrobat Reader 6.0 or with MS Windows Editor, depending on the file type.

Signed

If the original file is a PDF document, and the signature was embedded in the document, after the document has been successfully signed, a symbol will appear in this column. Double clicking on the symbol opens the file in Adobe Acrobat Reader 6.0.

File Name

The name of the file to be signed.

Inserted

Time when the file was sent to the signature server.

Display of the "Job View" with the signed PDF document:

Session	Original	Signed	File-Name	Sign-Type	Inserted
334	[icon]	[icon]	invoices.pdf	PDF	2008-03-14 12:19:13:625

The context menu can be called up by clicking right on the desired job.

The original file and, if present, the signed file can be opened through the menu.

If a signed PDF document exists, the menu will appear as follows:

Session	Original	Signed	File-Name	Sign-Type	Inserted
334	[icon]	[icon]	invoices.pdf	PDF	2008-03-14 12:19:13:625

Logging

i-effect® *SIGG keeps a record of all important processes within the program and displays them in the "Log View":

Date	Log Type	Name	Text
2008-03-14 12:16:26:265	INFO : SigG...	Starting SigGSe...	Starting Server
2008-03-14 12:16:20:750	INFO : Ses...	Slot activation	Slot ID:1 has been activated for signing.
2008-03-14 11:52:02:609	INFO : SigG...	Stopping SigGSe...	Stopping Server
2008-03-14 11:51:59:609	INFO : Ses...	NO MORE SESS...	THE ARE NO MORE ACTIVE SESSIONS FOR SIGNING OPE...
2008-03-14 11:51:58:421	INFO : Sec...	NO MORE SESS...	THE ARE NO MORE ACTIVE SESSIONS FOR SIGNING OPE...

Log files are kept and updated for all messages in the installation directory in the folder workspace\logs.

By clicking right, the context menu will open, which allows the user to copy one or more logbook entries onto the clipboard, or to open the log file in the log view.

Date	Log Type	Name	Text
2008-03-14 12:16:26:265	INFO : SigG...	Starting SigGSe...	Starting Server
2008-03-14 12:16:20:750	INFO : Ses...	Slot activation	Slot ID:1 has been activated for signing.
2008-03-14 11:52:02:609	INFO : SigG...	Stopping SigGSe...	Stopping Server
2008-03-14 11:51:59:609	INFO : Ses...	NO MORE SESS...	THE ARE NO MORE ACTIVE SESSIONS FOR SIGNING OPE...
2008-03-14 11:51:58:421	INFO : Sec...	NO MORE SESS...	THE ARE NO MORE ACTIVE SESSIONS FOR SIGNING OPE...

Copy onto the Clipboard

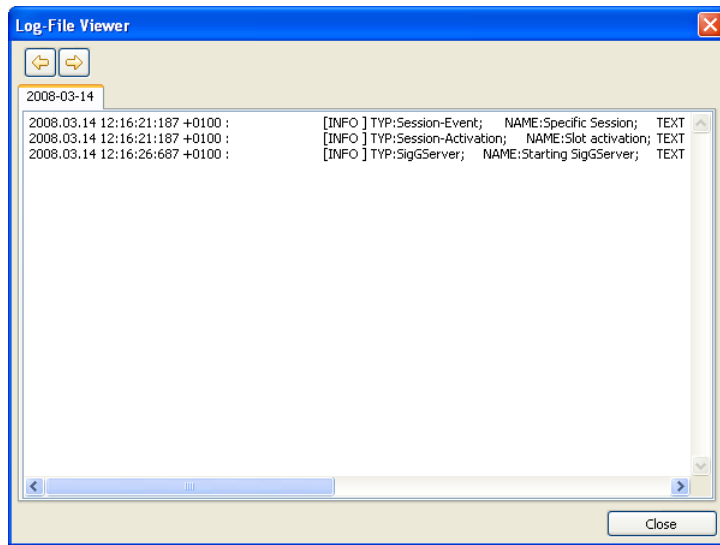
Copies the contents of the selected lines onto the clipboard. The contents of the table's individual lines will be converted to the output format in the log file.

Display Contents of the Log file

Opens the log file overview with the log file in which the contents of the selected line are saved. If more entries are chosen from the table, several tabs will be opened in the log file overview (dependent on the entries in which the files are found).

The log file overview allows to run through all available log files by using the arrow keys in the upper part of the window.

The log file will be created according to the pattern siggserver-YEAR-MONTH-DAY.log for the calendar day on which the program was run.



i-effect®'s Job Logging

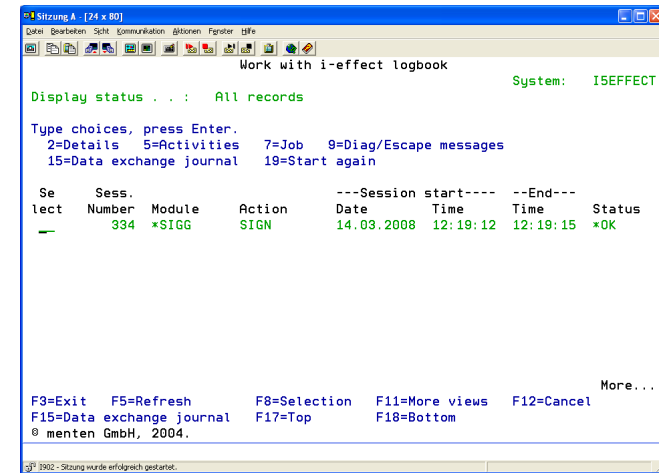
All messages regarding intermediate steps and events for signature jobs, which were created by i-effect® - the integrated solution for IBM Power Systems -, will be entered in the i-effect® logbook.

In the i-effect® logbook, the current status of a signature job can be viewed.

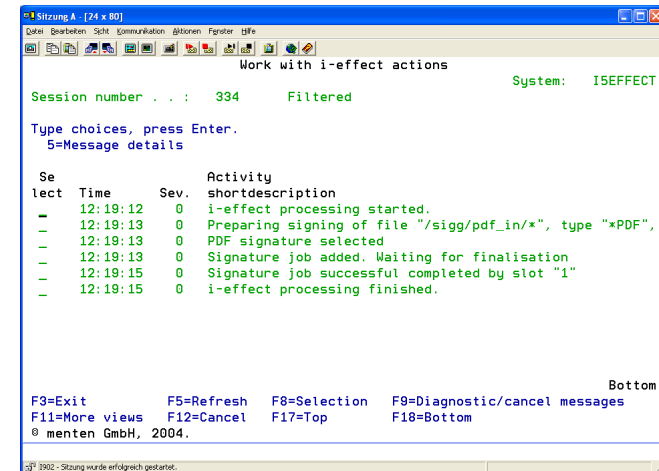
As long as a job has ACTIVE status, it has not been finished by i-effect® *SIGG and not sent back to i-effect®.

A job can be finished with the status *OK, *DIAG or *ERROR.

If a job has been successfully signed, the signature server sends *OK back to i-effect®.



The display of a job's messages shows its history: which file(s) were processed by which slot and which type was process by i-effect® *SIGG.



The message *DIAGNOSE at the end of a job means that not all of the files have been signed successfully. Check the messages to find out the cause for the individual problems.

The message *ERROR at the end of a job can have many causes. Only checking the messages in the job log can reveal the cause.

Logging in i-effect®'s "internal" Directory

In the "internal" directory of an i-effect® installation detailed information about the processes of the individual i-effect® modules is protocolled. This serves to find and correct problems that occur.

The log file for the *SIGG module will be saved according to the pattern "YEAR-MONTH-DAY.sigg.log."

This is an expansion of the i-effect® logbook, which accepts information regarding the *SIGG signature sever ONLY.

i-effect® *SIGG Updates

In order to install a new version of i-effect® *SIGG, the older version must be uninstalled before.

i-effect® *SIGG can be uninstalled either from the Control Panel-> Software or from the Windows menu:



After uninstalling is successfully completed, the new version of i-effect® *SIGG can be installed as is described under "i-effect® *SIGG installation."

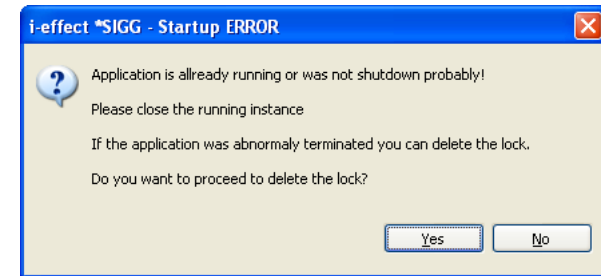
IMPORTANT: If an update of i-effect® - the integrated solution for IBM Power Systems – is desired, it is required that the version of i-effect® *SIGG also be updated to the correct version!

Debugging

Error Message during Program Start-up

A lock mechanism is activated to prevent simultaneous running of several instances of the *SIGG signature server.

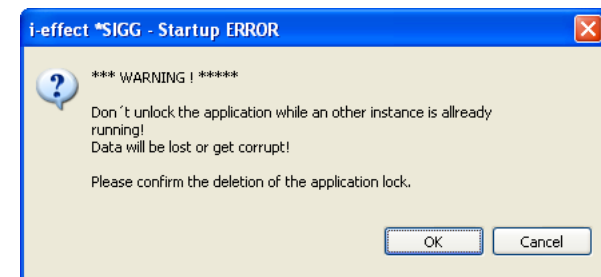
If the *SIGG signature server is activated a second time, the following message will appear:



The start of the *SIGG signature server is interrupted.

If this display appears, even though no second instance is running, the locking can be removed. In the case of a program crash, it might happen that the locking could not longer be removed.

In this case, the locking can immediately be removed .



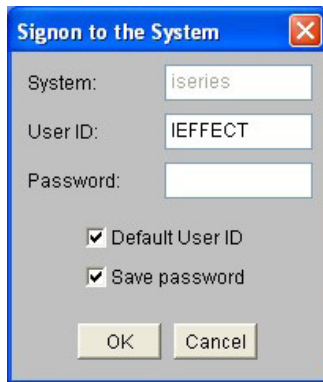
Note: IMPORTANT !!! It is possible to remove the locking, even if another instance of the program is run! If the locking is removed in this case, the signature server will start. Consequences: data loss, damage to the program configurations, job errors.

Password is Incorrect

If an incorrect password has been entered in the program settings for the user of IBM Power Systems, a dialog will be created from the framework, which enables access to the resources of IBM Power Systems.



By closing the first window opens a further dialog, where the users password can be entered.



Do not enter the password here, and close the dialog by using CANCEL! The password cannot be saved by SigG signature server if entered here!

Delete Unprocessed Jobs

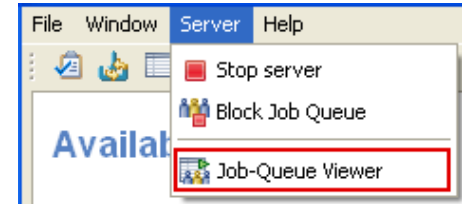
Jobs which were sent to the server can be deleted manually by opening the queue overview. Deleted jobs will be logged in the i-effect® Systems logbook as ABORT.

Note: As long as the overview is open, no jobs in the queue will be processed (the queue will be blocked)!

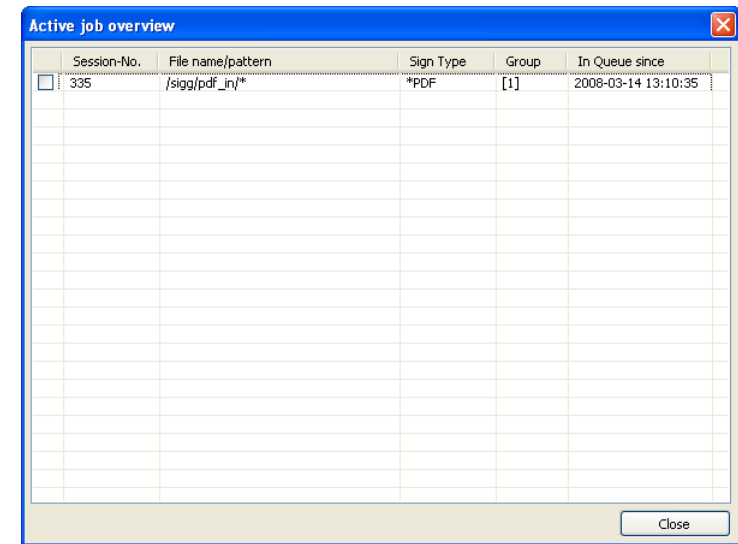
The queue overview can be opened either through the tool bar:



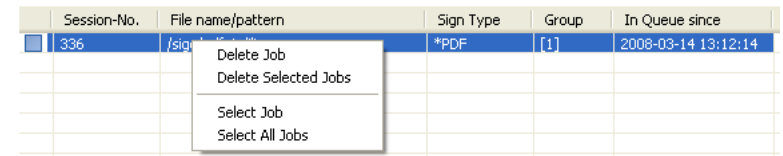
or through the menu Server->Job-Queue:



In the queue overview all current jobs being managed by the server will be displayed.



By right clicking in the table this overview will open in the context menu:



Delete Jobs

The job selected by clicking right will be deleted.

Delete Selected Jobs

All jobs which were selected (checked) will be deleted.

Select Job

The job which was clicked right mouse button will be selected (checked).

Select all Jobs

All jobs in the overview will be selected (all items will be checked).