

## Kapitel 8b

# Qualifizierte Elektronische Signatur

## Einleitung

### i-effect® \*SIGG - Auf einen Blick

- Sichere geschlossene Systemumgebung durch den Einsatz innerhalb von IBM Power Systems
- Parallele Nutzung beliebig vieler Kartenlesegeräte (Skalierung)
- Rechtsgültig qualifiziert signieren
- Massensignatur von Rechnungen mit hohem Durchsatz
- Eine Lizenzgebühr, unbegrenzte Anzahl Signaturen
- Vollintegriert in i-effect® V1R5 oder höher – die integrierte Lösung für IBM Power Systems
  
- i-effect® \*SIGG ist das Signaturserver-Modul von i-effect® – die integrierte Lösung für IBM Power Systems – und ermöglicht Dateien im Allgemeinen und PDF-Dateien im Besonderen qualifiziert nach den Vorgaben der deutschen Signaturverordnung (SigV) und des deutschen Signaturgesetzes (SigG) zu signieren. Wird von i-effect® \*SIGG gesprochen, so ist immer das Signaturserver-Modul von i-effect® – die integrierte Lösung für IBM Power Systems – gemeint, für welches entsprechend den Vorgaben von SigV und SigG eine Herstellererklärung verfasst wurde.
- i-effect® \*SIGG ist eine in der Programmiersprache Java geschriebene Software, die eine installierte Java Runtime Edition der Version 5.0 Update 6 oder höher voraussetzt.
- Darüber hinaus ist eine Installationslizenz der Anwendungssoftware i-effect® – die integrierte Lösung für IBM Power Systems – erforderlich.
- i-effect® \*SIGG repräsentiert das eigentliche Modul, welches für die Erzeugung der qualifizierten Signatur zuständig ist.

- i-effect® – die integrierte Lösung für IBM Power Systems – erstellt und übermittelt Signaturaufträge an den Signaturserver-Modul i-effect® \*SIGG.  
i-effect® – die integrierte Lösung für IBM Power Systems – muss auf der IBM Power Systems, in der sich die IXS PCI-Karte befindet, mit wenigstens dem \*BASE-Modul installiert sein, um Signaturaufträge erstellen zu können. Eine genaue Erläuterung über das Erstellen von Signaturaufträgen, finden Sie unter „Starte Signatur-Job“.
- i-effect® \*SIGG arbeitet zur Gewährleistung eines hohen Maßes an Sicherheit in einer geschlossenen Systemumgebung.
- i-effect® \*SIGG wird dabei auf einer IXS PCI-Karte innerhalb der IBM Power Systems ausgeführt.

## i-effect® \*SIGG - Sicher vor Manipulationen

Um den Anforderungen des deutschen Signaturgesetzes gerecht zu werden, ist i-effect® \*SIGG mit einem Mechanismus ausgestattet, Manipulationen an der Software feststellen zu können.

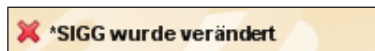
Darüber hinaus kann die Setup-Datei von i-effect® \*SIGG selbst auf Manipulation geprüft werden. Mit unserem Integritäts-Prüfwerkzeug kann der Hash-Wert der Datei berechnet werden und mit dem zu der Setup-Datei passenden Hash-Wert von unserer Webseite verglichen werden.

Eine erfolgreiche Prüfung gibt Ihnen die Sicherheit, dass Ihre Setup-Datei von i-effect® \*SIGG original ist und nicht manipuliert wurde.

Nach dem Start von i-effect® \*SIGG wird Ihnen der Status der Unversehrtheit der Software zur Anzeige gebracht:



Eine Manipulation an der Software ist direkt nach dem Start der Anwendung erkennbar.



Wurde eine Manipulation festgestellt, können keine Signatursitzungen mehr aktiviert werden. Auch der Serverdienst kann nicht mehr gestartet werden.

## Lizenz

i-effect® \*SIGG ist in der Lage mehrerer Kartenlesegeräte zu verwalten und für Signaturprozesse parallel zu verwenden.

Durch den Erwerb einer Lizenz kann ein verfügbarer Slot von einem oder mehreren angeschlossenen Kartenlesegeräten für Signaturprozesse aktiviert werden.

Möchten Sie mehrere Slots parallel für Signaturprozesse verwenden, ist der Erwerb weiterer Lizenzen erforderlich. Jede weitere Lizenz gewährt Ihnen die parallele Nutzung eines weiteren Slots.

Die Lizenz umfasst das Erstellen von Signaturen, die in einer separaten Datei des Typs P7S gespeichert wird.

Die Erstellung von Signaturen, die in das jeweilige PDF-Dokument bzw. zusammen mit den zu signierenden Daten in einer Datei gespeichert werden sollen (P7M), benötigen darüber hinaus eine Lizenz des i-effect® Moduls \*CRYPT.

Für das Signieren von EDIFACT-Dateien nach EANCOM 2002 Syntax 4; D.01B mit „**Attached Digital Signatur**“ benötigen Sie eine Lizenz des i-effect® Moduls \*EDIFACT. „**Attached Digital Signatur**“ bedeutet, dass je EDIFACT-MESSAGE eine Signatur erzeugt und in diese MESSAGE eingebettet wird.

Nach dem Start von i-effect® \*SIGG wird Ihnen der aktuelle Stand der verfügbaren Module entsprechende der vorhandenen Lizenzen angezeigt.

### Anmerkung:

Slots dienen dem Zugriff auf die auf einer SmartCard gespeicherten Informationen (bereitgestellt über einen Token). Darüber hinaus werden an einen Slot gesandte Signaturaufträge durch die in dem Slot enthaltene Logik verarbeitet.

## Installation

Die Installation besteht aus mehreren einzelnen Schritten und erfordert im Vorfeld die Installation der Java Runtime Edition der Version 5.0 Update 6 oder höher.

Darüber hinaus ist die Installation einer Middleware erforderlich, die die Verbindung zwischen einem oder mehreren installierten Kartenlesegeräten samt den in den Geräten eingesteckten Karten und dem SignaturServer herstellt. Die Software ist Bestandteil von i-effect® \*SIGG.

Weiterhin wird Adobes Acrobat Reader 8.x benötigt, um Original-PDF-Dokumente anzeigen und signierte PDF-Dokumente mit der eingebetteten Signatur korrekt prüfen zu können. Alternative kann der Acrobat Reader Version 6.x verwendet werden. Die Version 7.x kann für die Überprüfung der signierten PDF nicht verwendet werden.



### Empfehlung:

Gegenwärtig empfiehlt sich für die Prüfung von signierten Dateien mit separater Signaturdatei und PDFs die kostenlose Prüfsoftware der Firma D-Trust. Sie finden die Software „D-SIGN Reader“ auf der Webseite der Fa. D-Trust (<http://www.d-trust.net>). Klicken Sie auf „Service“ und anschließend im links erscheinenden Menü auf „kostenlose Prüfsoftware.“

## Installation des Kartenlesegerätes

Als Kartenlesegerät kommt der CHIPDRIVE pinpad 532 des Herstellers SCM Microsystems zum Einsatz, der den Anforderungen des deutschen Signaturgesetzes entspricht.

## Treiberinstallation



### WICHTIG!

Zuerst die Treiber installieren und anschließend nach dem Neustart des Systems erst das Kartenlesegerät anschließen!

Auf dem Installationsmedium befindet sich die aktuelle Treiberversion des Kartenlesegerätes. Starten Sie die Installation in dem Sie die ‚Setup.exe‘ ausführen und den Installationsanweisungen folgen.

Es empfiehlt sich nach erfolgter Installation in dem durch das Setup geöffneten Dialog den Punkt zu wählen, der den manuellen Neustart ermöglicht.

Anschließend erfolgt die Aufforderung, Kartenlesegeräte zwecks Firmwareupdate anzuschließen, was im Regelfall nicht erforderlich bzw. evtl. auch nicht erwünscht ist, da laut der

Bundesnetzagentur nur Geräte diesen Typs mit der Firmware Version 4.15 bzw. 5.10 für die Erzeugung qualifizierter digitaler Signaturen zulässig sind.



### Anmerkung:

Der Downgrade der Version kann nur durch das Einsenden an den Hersteller erfolgen.

## Installation notwendiger Programme

### Java Runtime Edition 5

Die aktuelle Java Runtime Edition (JRE) kann von der Internetseite <http://de.sun.com> von Sun Microsystems heruntergeladen werden. Dort finden Sie auch bei Bedarf die notwendigen Installationsanweisungen.

Alternativ befindet sich auf dem Installationsmedium eine entsprechende Java Runtime Edition-Installationsdatei, die verwendet werden kann. Bei Verwendung der mitgelieferten Runtime öffnen Sie die Installationsdatei mittels Doppelklick und folgen Sie den Installationsanweisungen.

### Middleware

In Abhängigkeit von der eingesetzten SmartCard ist die Installation der jeweiligen Software erforderlich, die diese SmartCard unterstützt.

Weiterhin ist zu beachten, welche gesetzlichen Vorgaben für die digitale Signatur zu berücksichtigen sind. Daraus ergeben sich je nach Land Einschränkungen hinsichtlich einsetzbarer SmartCards.

Darüber hinaus wurde für den Schweizer Raum die Unterstützung einer weiteren Signaturerstellungseinheit integriert. Neben dem Einsatz von SmartCards der SwissCom basierend auf dem CardOS 4.3B der Firma Siemens können auch eTokens der Firma Aladdin mit Qualifizierten Zertifikaten der Firma QuoVadis eingesetzt werden.

Die Middleware wird entweder von uns direkt oder dem Zertifizierungsdienstleister zusammen mit der SmartCard ausgeliefert.

## Unterstützte Middleware

Es kann nur Middleware eingesetzt werden, die über eine PKCS#11-Standard- Konforme Schnittstelle verfügt. Im folgenden sind die Kombinationen an Software und SmartCards aufgelistet, die gegenwärtig von unserer Software unterstützt werden und in welchem Land diese Kombination eingesetzt werden kann.

### Nexus Personal

Version: 4.6 oder höher

PKCS#11-Bibliothek: personal.dll

(Standard-)Pfad zur PKCS#11-Bibliothek: **ProgrammePersonal\bin**

#### Unterstützte SmartCard:

D-Trust multiscard (Deutschland)

Bei Einsatz einer D-Trust multiscard erhalten Sie mit dem Installationsmedium die Software Nexus Personal. Starten Sie die Datei „**PersonalSetup.exe**“ aus dem Verzeichnis „**NexusPersonal**“ von der CD und folgen Sie den Installationsanweisungen.

### Siemens CardAPI

Version: 3.11 oder höher

PKCS#11-Bibliothek: siecap11.dll

(Standard-)Pfad zur PKCS#11-Bibliothek: **WINDOWS\system32**

#### Unterstützte SmartCard:

Karten mit Siemens CardOS 4.3B (Schweiz)

Die Middleware CardAPI von Siemens wird entweder mit dem Installationsmedium oder durch den Lieferanten der SmartCard bereitgestellt.

Um die Software zu installieren, gehen Sie in das Unterverzeichnis „**Microsoft\_Windows**“ und dort in das Verzeichnis „**Setup**“ der CardAPI-Software und führen die Datei „**Setup.exe**“ aus. Folgen Sie den Installationsanweisungen.

### Aladdin PKIClient

Version: 4.5 oder höher

PKCS#11-Bibliothek: eTPKCS11.dll

(Standard-)Pfad zur PKCS#11-Bibliothek: **Windows\system32**

#### Unterstützte SmartCard:

eToken Pro 64K (4.2B) (Schweiz)

Bei Einsatz eines Aladdin eToken erhalten Sie mit dem Installationsmedium die Software PKI Client der Fa. Aladdin. Rufen Sie diese Datei „**PKIClient-x32-X.xx.msi**“ aus

dem Verzeichnis „**04\_Middleware\Aladdin eToken PKI Client**“ von der CD auf und folgen Sie den Installationsanweisungen.

### A-Trust a.sign Client

Version: 1.2.x oder höher

PKCS#11-Bibliothek: asignp11.dll

(Standard-)Pfad zur PKCS#11-Bibliothek: **Windows\system32**

#### Unterstützte SmartCard:

a.sign Premium (Österreich)

Bei Einsatz einer a.sign Premium SmartCard erhalten Sie mit dem Installationsmedium die Software a.sign Client der Fa. A-Trust. Rufen Sie diese Datei „**acSetup.exe**“ aus dem Verzeichnis „**04\_Middleware\A-Trust aSign**“ von der CD auf und folgen Sie den Installationsanweisungen.

## Adobe Acrobat Reader 8.x

Auf dem Installationsmedium finden Sie die Setup-Datei für die Installation von Adobe Acrobat Reader 8.

## Installation von i-effect® \*SIGG

Sofern die Voraussetzungen für die Installation der Software i-effect® SIGG Signaturserver geschaffen sind (Java Edition 5 oder höher, Middleware), kann die Installation mit dem Aufruf der Datei „Setup\_VxRxMx\_Bx.exe“ gestartet werden.

**Die Namensgebung der Setup-Datei von i-effect® \*SIGG setzt sich wie folgt zusammen:**

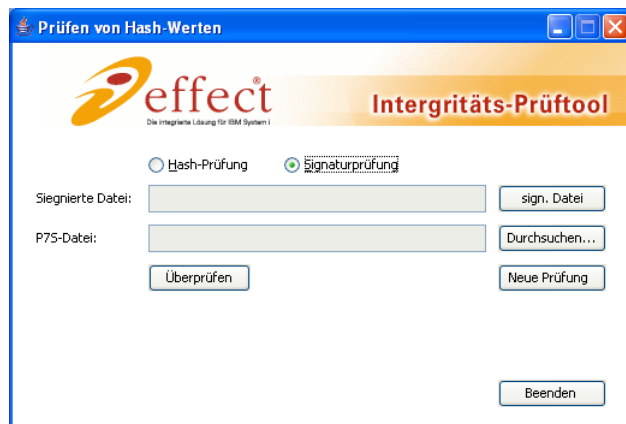
- VxRxMx bezeichnet die Version von i-effect® – die integrierte Lösung für IBM Power Systems – zu der das Modul i-effect® \*SIGG kompatibel ist.
- Bx steht für die aktuelle Build-Nummer des i-effect® \*SIGG Modules innerhalb dieser Version. Neuere Builds enthalten Ergänzungen bzw. Bug-Fixes von i-effect® \*SIGG.

### Prüfen der Integrität der Setup-Datei

Auf Wunsch können Sie die mit der CD/DVD oder über den Downloadbereich der i-effect® - Webseite erhaltene Setup-Datei von i-effect® \*SIGG überprüfen.

Wir stellen Ihnen für diese Zwecke unser Integritäts-Prüftool zur Verfügung. Sie finden es ebenfalls auf der CD/DVD oder in unserem Downloadbereich auf unserer i-effect® - Webseite.

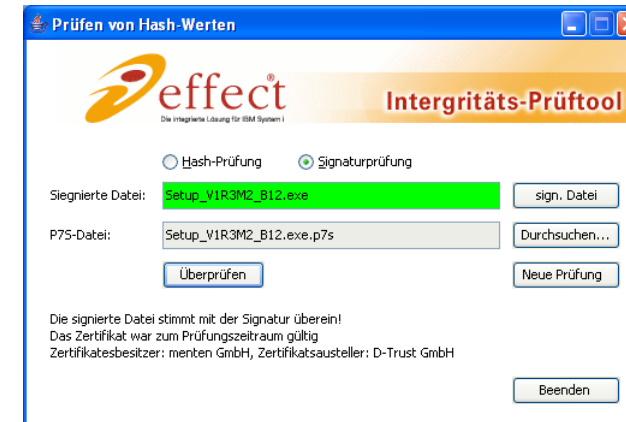
Starten Sie durch einen Doppelklick auf die Datei „**i-effect\_Pueftool.jar**“ das Integritäts-Prüftool und wählen Sie innerhalb des Programms „**Signaturprüfung**“ aus:



Öffnen Sie über Klicken auf „**sign. Datei**“ die Setup-Datei von i-effect® \*SIGG.

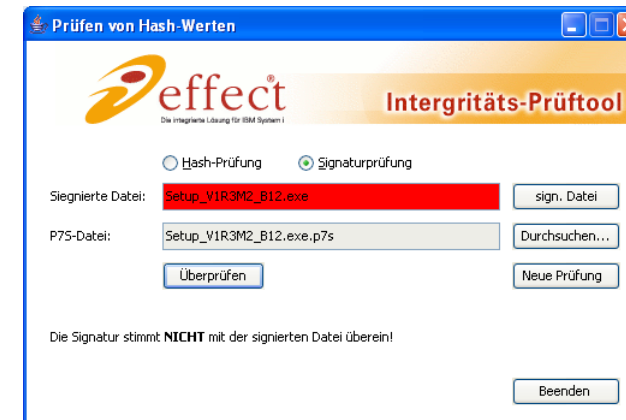
Anschließend öffnen Sie über „**Durchsuchen...**“ die Signaturdatei mit dem Prüftool und klicken anschließend auf „**Überprüfen**“. Die Signaturdatei hat den gleichen Namen wie die Setup-Datei und endet auf „**.pks**“.

Sie sollten bei einer erfolgreichen Überprüfung folgende Anzeige erhalten:



Sie erhalten über die eigentliche Prüfung hinaus Angaben über die Gültigkeit des Zertifikates zum Prüfzeitpunkt sowie Information über den Zertifikatinhaber und -aussteller.

Eine fehlgeschlagene Überprüfung läuft auf folgende Ansicht hinaus:



Überprüfen Sie bitte, ob Sie die korrekten Dateien verwendet haben.

Sollte dies der Fall gewesen sein, verwenden Sie diese Setup-Datei nicht für die Installation! Bitte laden Sie die Setup-Datei erneut von unserer Webseite herunter oder vordern eine Fassung auf CD an.

**Anmerkung:**

Die Integrität der Setup-Datei kann auch mittels der Software D-SIGN Reader der Firma D-Trust geprüft werden. Dieses Tool beherrscht auch die Überprüfung des Online-Status des für die Signatur verwendeten Zertifikates.

Sie finden die Software „D-SIGN Reader“ auf der Webseite der Fa. D-Trust (<http://www.d-trust.net>). Klicken Sie auf „Service“ und anschließend im links erscheinenden Menü auf „kostenlose Prüfsoftware“.

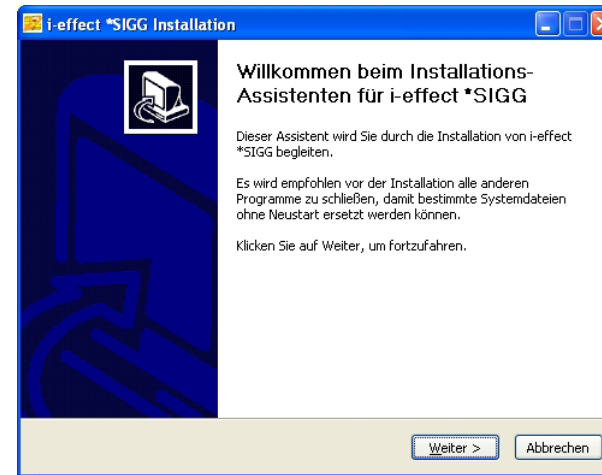
## Installation von i-effect® \*SIGG

Nach dem Starten des Setup's von i-effect® \*SIGG erscheint das Sprachauswahl-Fenster.

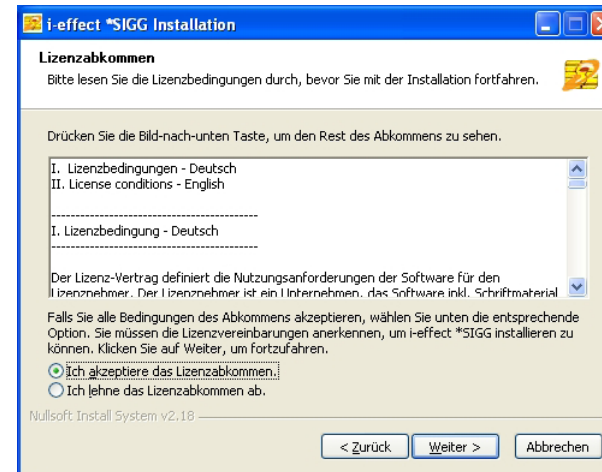


Wählen Sie die gewünschte Sprache oder bestätigen die Voreinstellung mit dem klicken auf „OK“.

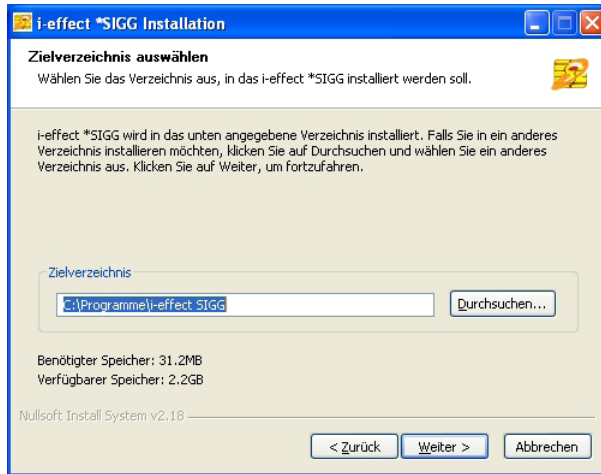
Das Willkommensfenster weist Sie auf die Installation des i-effect® \*SIGG hin.



Anschließend erhalten Sie Einblick in die Lizenzbedingungen, denen Sie zustimmen müssen, um die Installation fortfahren zu können.

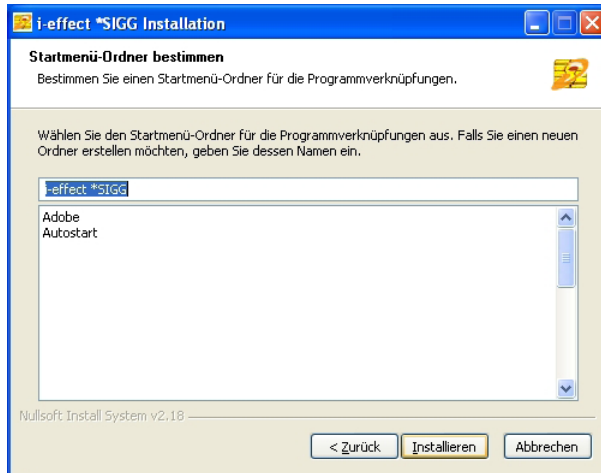


Innerhalb dieses Fensters können Sie ein eigenes Installationsverzeichnis auswählen. Wir empfehlen Ihnen, den vorgegebenen Verzeichnis-Pfad für die Installation von i-effect® \*SIGG zu verwenden.

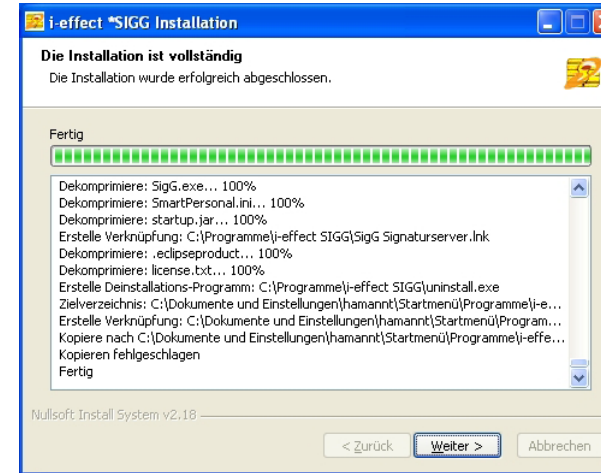


Im Anschluss an die Festlegung des Installationspfades können Sie den Startmenü-Eintrag für i-effect® \*SIGG festlegen.

Die eigentliche Installation des Programms startet nach einem Klick auf „**Installieren**“.



Nach erfolgreicher Installation erhalten Sie einen Überblick der getätigten Aktionen.

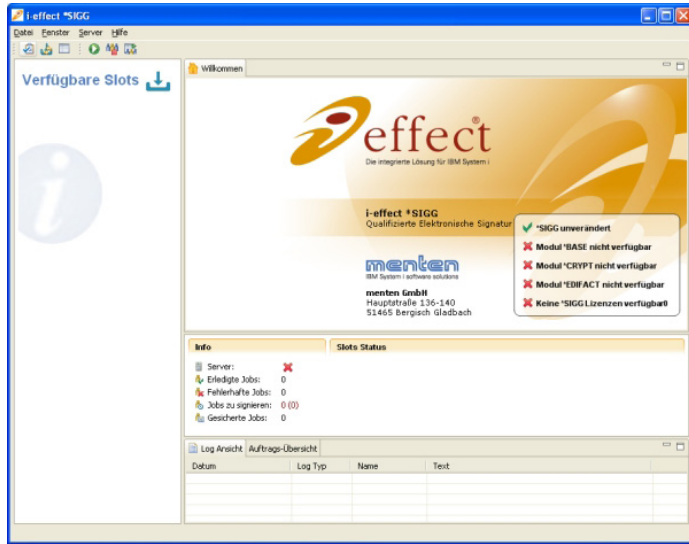


Abschließend wird der Beendigungs-Dialog zur Anzeige gebracht. Ein Klicken auf „**Fertig stellen**“ beendet das Installations-Programm.



## Einrichtung

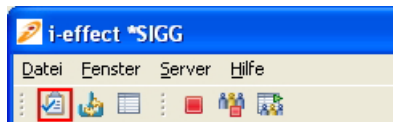
Nach erfolgreicher Installation kann i-effect® \*SIGG gestartet werden.



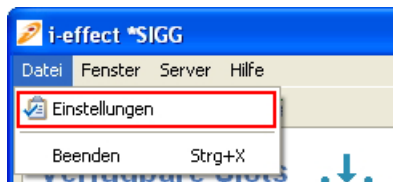
Der nächste Schritt liegt in der Einrichtung der Applikation.

## Programm-Einstellungen

Mit Hilfe des Einstellungs-Dialoges werden die wesentlichen Konfigurations-Einstellungen des Programms vorgenommen.



Der Dialog lässt sich wie folgt über die **Symboleiste** öffnen:



Oder über die Menüleiste **Datei->Einstellungen**:

Der Konfigurations-Dialog ist in mehrere Reiter aufgeteilt, über die die einzelnen Programm-Komponenten konfiguriert werden können.

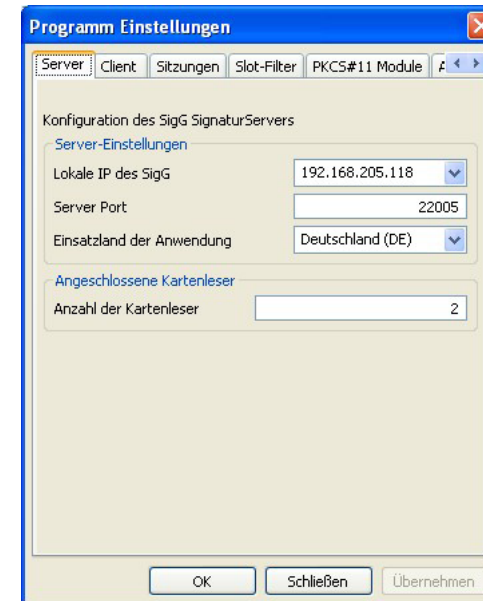
Die Konfiguration wird mittels „**OK**“ gespeichert und das Konfigurationsfenster schließt sich.

Geänderte Werte können mittels „**Übernehmen**“ gespeichert werden, ohne dass sich das Konfigurations-Fenster schließt.

Das Klicken auf „**Abbrechen**“ bewirkt, dass geänderte Werte nicht übernommen werden. Das Konfigurations-Fenster wird geschlossen.

## Server

Über diesen Reiter kann eingestellt werden, an welcher IP-Adresse und an welchem Port des lokalen Systems der Server eingehende Aufgaben entgegen nehmen soll.



Es können die folgenden Einstellungen am Server vorgenommen werden:

### Lokale IP des SigG

Auswahlmensü der auf diesem System verfügbaren IP-Adressen.

## Server Port

Der Port, an dem der Server auf eingehende Aufgaben wartet.

**Voreingestellter Port** 22005

## Einsatzland

Die Auswahl des Einsatzlandes dient weitestgehend der Sicherstellung, dass nur für das jeweilige Land durch deren Gesetzgebung freigegebene SmartCards für Signaturprozesse verwendet werden können und evtl. vorhandene weitergehende länderspezifische Absicherungsmaßnahmen für das Erzeugen von (qualifizierten) elektronischen Signaturen aktiviert werden.



### WICHTIG:

*Es ist zwingend erforderlich, dass das richtige Einsatzland eingestellt ist und nicht verändert wird! Nur so kann z.B. für Deutschland eine Gesetzes-konforme Erzeugung qualifizierter elektronischer Signaturen gewährleistet werden, wie auch die Herstellererklärung vorgibt!*

## Anzahl der Kartenleser

Die Anzahl der angeschlossenen Kartenlesegeräte, die für Signaturprozess verwendet werden können.

**Voreingestellter Wert** 1

## Client

Der Client aus Sicht von i-effect® \*SIGG ist das auf der IBM Power Systems installierte i-effect® – die integrierte Lösung für IBM Power Systems –, welches Aufträge an den Signaturserver sendet.

Die Einstellung in diesem Reiter dienen dem Zugriff des Signaturservers auf das i-effect® - System, um Lizenz-Abfragen zu ermöglichen, die Verfolgung der Abarbeitung von übertragenen Aufgaben über das i-effect® Logbuch zu realisieren und abgebrochene bzw. unterbrochene Bearbeitungsprozesse wieder korrekt fortführen zu können.

Es können die folgenden Einstellungen für den Zugriff auf i-effect® vorgenommen werden:

### i-effect Hostname oder IP-Adresse

Den Rechnernamen bzw. die IP-Adresse des Systems, auf dem i-effect® installiert ist.

### Benutzername

Den Benutzernamen, mit dem sich der Signaturserver an i-effect® anmelden kann.

### Passwort

Das zu dem angegebenen Benutzer zugehörige Passwort.

## Passwort bestätigen

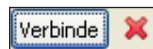
Die Bestätigung des eingegebenen Passwortes, um die Speicherung eines fehlerhaften Passwortes zu verhindern.



Die eingegebenen Einstellungen für die Verbindung zum i-effect® - System können mit Hilfe von „**Verbinde**“ getestet werden.



Im Falle einer erfolgreichen Verbindung zum i-effect® - System wird ein grünes Häkchen zur Anzeige gebracht.



Im Falle einer Zurückweisung des Verbindungsaufbaus zum i-effect® - System wird ein rotes „**X**“ angezeigt.  
In der Log-Anzeige des Signaturservers kann die Ursache für diesen Fehlversuch nachgelesen werden.



Eingabe des Passwortes, falls für den angegebenen Benutzer keine Eingabe erfolgte:

Wurde kein Passwort für den angegebenen Benutzer eingetragen oder gespeichert, erscheint beim Klicken auf ‚Verbinde‘ ein PopUp-Fenster mit der Aufforderung, dass Passwort einzugeben.

## Sitzungen

Eine Sitzung ist in gewisser Hinsicht das Kernstück von i-effect® \*SIGG, da mit Hilfe einer aktivierten Sitzung Signaturprozesse durchgeführt werden können

Da i-effect® \*SIGG Massensignatur unterstützt ist es nach dem deutschen Signaturgesetz notwendig, die Gültigkeit einer aktiven Sitzung zu limitieren. Der Inhaber der SmartCard entscheidet, wie lange eine durch Ihn aktivierte Signatursitzung für Signaturprozesse verwendet werden darf.

Die Einstellungen dieses Reiters beeinflussen die Standard-Gültigkeit der Signatursitzungen aller Slots eingesetzter SmartCards.

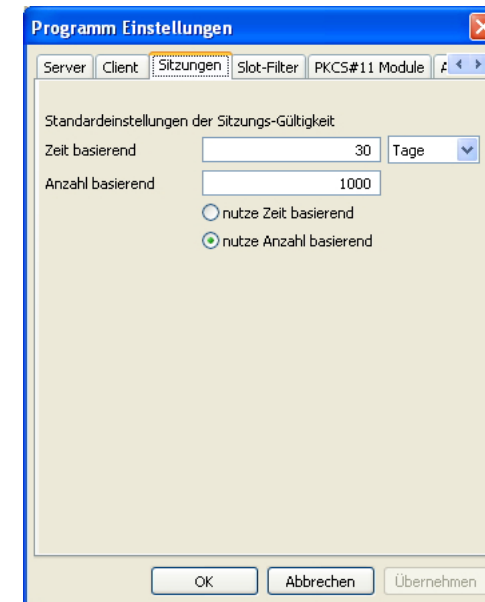
Darüber hinaus besteht natürlich auch die Möglichkeit bei der Nutzung mehrerer Kartenlesegeräte individuelle Einstellung der Gültigkeit einer Signatursitzung je Slot vorzunehmen.

Individuelle Einstellungen eines Slots überschreiben die hier angegebenen Voreinstellungen.

Wie Sie individuelle Einstellungen der Gültigkeit an einem Slot vornehmen können, finden Sie unter „**Slot-Einstellungen**“.

Da eine einmalige Aktivierung einer Sitzung reicht um anschließend beliebig viele(\*) Signaturen erstellen zu können, ist eine Limitierung der Anzahl durchführbarer Signierprozesse bzw. der zeitlichen Begrenzung der Aktivität der Sitzung erforderlich, um der deutschen Signaturgesetz zu entsprechen.

(\* solange wie das Zertifikat gültig ist)



### Zeit basierend

Der hier angegebene Wert wird in der ausgewählten Zeiteinheit bei der Aktivierung einer Signatur-Sitzung auf das Aktivierungs-Datum aufgerechnet.

Eine am 1.6.2006, 12:00 Uhr aktivierte Signatur-Sitzung mit einer eingestellten Gültigkeitsdauer von 5 Tagen würde bis zum 6.6.2006, 12:00 Uhr gültig sein.

Eine erneute Aktivierung für das Durchführen weiterer Signaturen ist erforderlich.

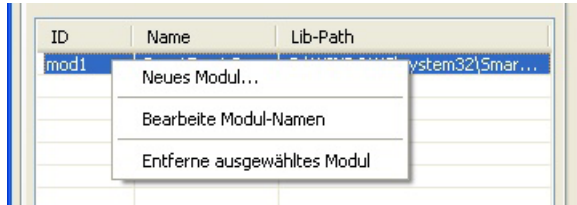
### Anzahl basierend

Der hier angegebene Wert bestimmt die Menge an Signaturen, die diese Signatur-Sitzung durchführen kann, bevor diese Sitzung ungültig wird.

Eine aktivierte Signatur-Sitzung mit voreingestelltem Wert von 100 kann genau 100



Durch Klicken der rechten Maustaste in die Modul-Tabelle ist es möglich Module neu hinzuzufügen, einzelne Module zu löschen oder den Modul-Namen eines bereits existierenden Moduls zu bearbeiten.



Beim Anlegen eines neuen Moduls sind zumindest die Angabe einer Module-ID und der Pfad zur Modul-Bibliothek erforderlich.

Die Module-ID muss mit der Buchstabenfolge ‚mod‘ beginnen, gefolgt in der Regel durch eine laufende Nummer (oder einer beliebigen Zeichenfolge) ohne Leerzeichen.

Der Pfad zur Modul-Bibliothek kann mit Hilfe des Datei-Dialoges auf dem System gesucht werden.



Die Bearbeitung eines Moduls lässt nur die Änderung des Modul-Namens zu.

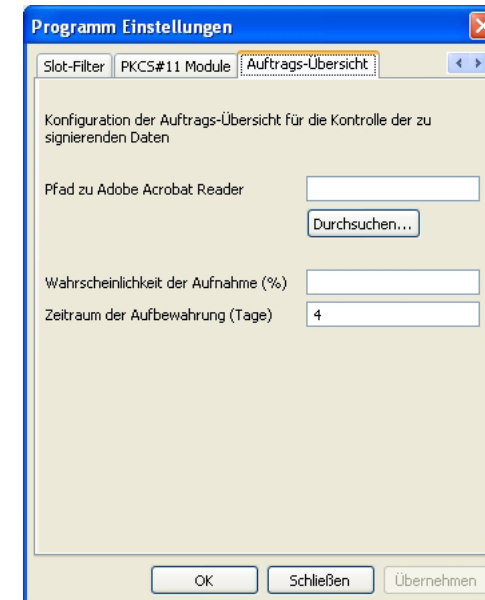


## Auftrags-Übersicht

Die Auftrags-Übersicht dient dem Speichern der an i-effect® \*SIGG übergebenen Aufträge zu Kontrollzwecken. Es werden die Originaldateien, die es zu signieren gilt, gespeichert um ein nachträgliches Überprüfen der Auftrags-Daten zu ermöglichen.

Die hier vorgenommenen Einstellungen ermöglichen es Ihnen, die Wahrscheinlichkeit der Übernahme eines eingehenden Auftrags in die Übersicht und den Zeitraum der Speicherung dieser Daten einzustellen.

Weiterhin ist hier der Pfad zur Programm-Start-Datei von Adobes Acrobat Reader anzugeben, um PDF-Dokumente aus der Übersicht direkt aufrufen zu können. Alle Nicht-PDF-Dateien werden sofern möglich mit dem Standard-Text-Editor von Microsoft angezeigt.



### Pfad zu Adobe Acrobat Reader

Für die Anzeige der PDF-Dokumente ist die Angabe des Pfades zur Programm-Datei des Adobe Acrobat Reader erforderlich.

PDF-Dokumente können mit Hilfe des Acrobat Reader angezeigt und die Inhalte auf Unversehrtheit geprüft werden, wenn eine eingebettete Signatur in das PDF-Dokument integriert wurde. Die Verifizierung funktioniert zur Zeit mit dem Adobe Acrobat Reader Version 6.x und Version 8.x.

#### Anmerkung:

Nicht-PDF-Dateien werden mit dem Text-Editor von MS Windows versucht zu öffnen.



**!** Die Verifizierung der Version 7 des Readers scheint fehlerhaft zu funktionieren und meldet Veränderungen am Dokument.

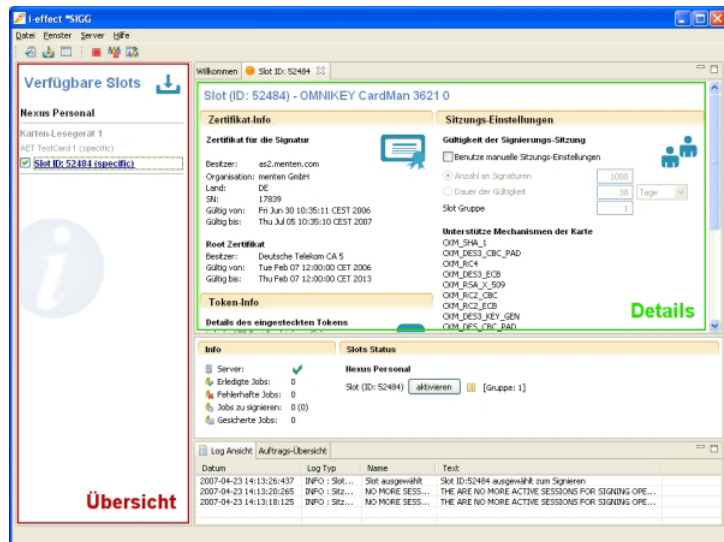
### Wahrscheinlichkeit der Aufnahme (%)

An i-effect® \*SIGG übergebene Aufträge werden mit der eingestellten Wahrscheinlichkeit in die Auftrags-Übersicht aufgenommen.  
 Die Notwendigkeit des Führens der Auftrags-Übersicht ergibt sich aus den Anforderungen des Signaturgesetzes, die eine Überprüfung von zu signierenden Daten vorschreibt.  
 Die Überprüfung soll ermöglichen, dass fehlerhaft übermittelte oder manipulierte Daten erkannt werden können.  
 Es können Werte zwischen 5 und 100 % eingetragen werden.

### Zeitraum der Aufbewahrung (Tage)

Die in i-effect® \*SIGG zur Kontrolle gespeicherten Aufträge werden nach Ablauf des eingestellten Zeitraumes gelöscht.  
 Es können Werte zwischen 1 und 7 Tagen eingetragen werden.

## Slot-Einstellungen



Durch das Klicken auf den Link (Slot-Bezeichner) in der Übersicht verfügbarer Slots wird die Detail-Ansicht eines Slots geöffnet.



Diese detaillierte Ansicht ermöglicht u.a. die Einstellung individueller Werte für die Gültigkeit der Signatur-Sitzung. Diese individuellen Einstellungen überschreiben die voreingestellten Werte, die man in den Programm-Einstellungen vornehmen kann.

### Sitzungs-Einstellungen

**Gültigkeit der Signierungs-Sitzung**

Benutze manuelle Sitzungs-Einstellungen

Anzahl an Signaturen: 1000

Dauer der Gültigkeit: 30 Tage

Slot Gruppe: 1

### Benutze manuelle Sitzungs-Einstellungen

Das Setzen des Häkchens an dieser Stelle, bewirkt, dass die Standardwerte der Programm-Einstellungen überschrieben und die für diesen Slot vorgesehenen Werte übernommen werden.

### Anzahl an Signaturen

Die angegebene Anzahl bestimmt, wie viele Signaturen nach der Aktivierung des Slots durchgeführt werden können. Ist diese Anzahl erreicht, wird der Slot automatisch deaktiviert.

### Dauer der Gültigkeit

Die Auswahl für die Bestimmung der Gültigkeit einer Signatur-Sitzung auf Basis einer zeitlichen Begrenzung bewirkt die Übernahme des Zeit-Intervalls und der ausgewählten Zeit-Maßeinheit.

Bei der Aktivierung einer Signatur-Sitzung wird der Zeitpunkt ermittelt, an dem diese Sitzung ihre Gültigkeit verliert.

## Slot Gruppe

Die Zuteilung eines Slots zu einer Kartengruppe ermöglicht einen Pool von Slots zu definieren, die zur Aufgabenverteilung oder auch Lastverteilung von Signaturaufgaben verwendet werden können.

So kann eine Gruppe nur für das Signieren von Rechnungen verwendet werden und eine zweite Gruppe für die Signierung sonstiger Dateien.



### WICHTIG:

Änderungen an den individuellen Einstellungen eines Slots werden umgehend gespeichert und bewirken, dass eine aktive Sitzung dieses Slots **DEAKTIVIERT** wird!

Darüber hinaus zeigt Ihnen die Detail-Ansicht Informationen über das auf der Karte gespeicherte Zertifikat mit samt dessen Root-Zertifikat an.

Diese Informationen geben unter anderem Auskunft über den Besitzer, die Gültigkeit und die Serien-Nummer des Zertifikates.

### Token-Info

#### Details des eingesteckten Tokens

Label : Office identity card (specific )  
 Manufacturer ID : D-TRUST QUAL Multi 2K  
 Free private memory : 4294967295  
 Free public memory : 4294967295  
 Maximum PIN length : 8  
 Firmware version : 1.00  
 Hardware version : 2.01



Auch Informationen über den Token können hier eingesehen werden, der sich auf der SmartCard befindet.

### Zertifikat-Info

#### Zertifikat für die Signatur

Besitzer: Ralph Menten  
 Organisation: menten GmbH  
 Organizationseinheit: For test purposes only!  
 Land: DE  
 SN: 77136086123417730004  
 Gültig von: Tue Apr 25 14:44:45 CEST 2006  
 Gültig bis: Wed Apr 25 14:44:45 CEST 2007



#### Root Zertifikat

Besitzer: D-TRUST Test CA 2003 1:PM  
 Gültig von: Thu Oct 02 13:29:32 CEST 2003  
 Gültig bis: Fri Oct 02 13:29:32 CEST 2009

## Inbetriebnahme

Für die Inbetriebnahme von i-effect® \*SIGG sind einige wenige Einstellungen vorzunehmen, die im Folgenden erläutert werden.

### Einrichten des Servers

- Zunächst ist es notwendig, den Server einzurichten, in dem die IP-Adresse des lokalen Systems bestätigt wird, an der der Server Aufgaben entgegen nehmen soll.
- Wenn ein anderer Port als der voreingestellte Port 22005 verwendet werden soll, ist der neue Port einzutragen.
- Anmerkung: Eine Änderung des Ports bedeutet auch eine notwendige Änderung der i-effect® Systemeinstellungen oder eine Angabe des Ziel-Ports beim Starten eines Signatur-Jobs .

Änderungen mit Klicken auf „Übernehmen“ speichern.

Mehr Informationen zu den einzelnen Punkten der Server-Konfiguration können den Programm-Einstellungen entnommen werden



### Einrichten des Client

- Angabe des Host-Namen oder der IP-Adresse des Systems, auf dem i-effect® läuft.
- Angabe eines gültigen Benutzernamens auf der IBM Power Systems.
- Auf Wunsch kann das Passwort des eingegebenen Benutzernamens mit angegeben und gespeichert werden.
- Eine Nicht-Eingabe bewirkt, dass an notwendiger Stelle eine Passwort-Abfrage erscheint.
- Ggfs. Testen der Einstellungen durch Maus-Klick auf „Verbinde“.

Änderungen mit Klicken auf „Übernehmen“ speichern.

Mehr Informationen zu den einzelnen Punkten der Client-Konfiguration können den Programm-Einstellungen entnommen werden

## Einrichten eines PKCS#11-Moduls

- Anlegen eines neuen Moduls mittels Maus-Rechts-Klick in die Tabelle und anklicken des Menü-Punktes ‚Neues Modul...‘
- Eintragen einer Modul ID (die ersten drei Buchstaben müssen „mod“ entsprechen) ist erforderlich.
- Eintragen des Modul-Namen ist optional
- Eintragen des absoluten Pfades zur Modul-Bibliothek ist erforderlich

Änderungen mit Klicken auf „Übernehmen“ oder „OK“ speichern.



Mehr Informationen zu den einzelnen Punkten der Modul-Konfiguration können den Programm-Einstellungen entnommen werden

## Aktivieren einer Sitzung für Signatur-Operationen

Als Vorbereitung für die Durchführung von Signaturoperationen ist die Aktivierung einer Sitzung erforderlich.

### Auswählen eines Slots

SmartTrust Personal	
Karten-Lesegerät 1	
<input type="checkbox"/>	Slot ID: 0
<input checked="" type="checkbox"/>	Slot ID: 1 (specific)

Zunächst muss ein Slot ausgewählt werden, in dem in der Übersicht der verfügbaren Slots das entsprechende Häkchen gesetzt wird.



#### Anmerkung:

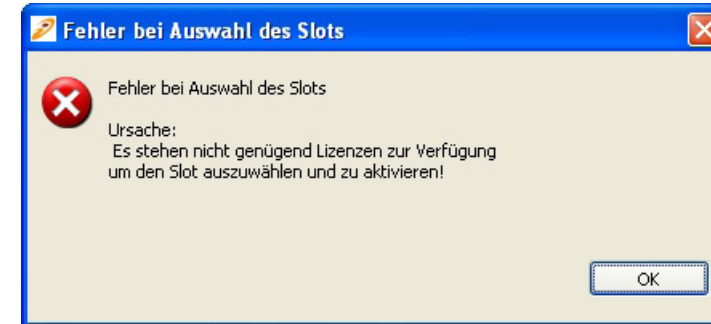
Ein Häkchen kann nur bei den Slots gesetzt werden, die für Massensignatur geeignet sind. Die entsprechenden Slots sind mit dem Vermerk ‚specific‘ gekennzeichnet.

## Lizenzüberprüfung

Durch das Setzen des Häkchens bei Auswahl eines Slots wird die Lizenzprüfung von i-effect® \*SIGG aktiviert.

Es wird überprüft, ob Sie die notwendige Anzahl an Lizenzen besitzen, um die gewünschte Anzahl an Slots auswählen zu können.

Sollten Sie nicht über die notwendige Anzahl an Lizenzen verfügen, um die gewünschte Anzahl an Slots auswählen zu können, erscheint die folgende Fehlermeldung:



## Anzeige ausgewählter Slots

Wurde ein Slot ausgewählt, erscheint dieser Slot in dem Bereich „Slots Status“.

In diesem Bereich werden alle ausgewählten Slots nach ihrem Modulen sortiert angezeigt. Nach der Auswahl befinden sich die Slots im deaktivierten Zustand, was bedeutet: deren Sitzung wurde noch nicht aktiviert.

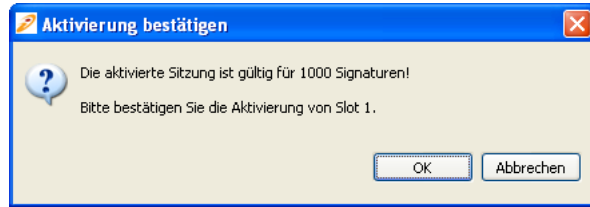
Slots Status	
Smart Trust Personal	
Slot (ID: 1)	aktivieren <input type="checkbox"/>

## Aktivierung eines Slots

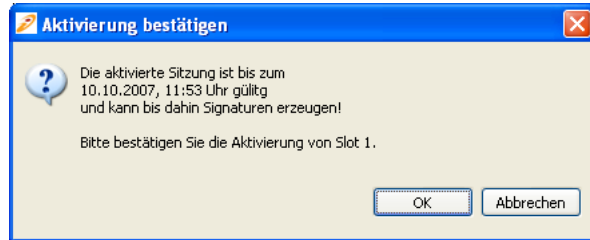
Die Aktivierung eines Slots und somit das Erzeugen einer aktiven Sitzung für Signatur-Operationen erfolgt durch einen Maus-klick auf „aktivieren“.

Um der Anforderung des deutschen Signaturgesetzes bzw. der deutschen Signaturverordnung gerecht zu werden, wird vor dem eigentlichen Aktivieren einer Sitzung ein Bestätigungsdialog angezeigt.

Dieser Dialog weist ausdrücklich darauf hin, dass durch die Aktivierung der Sitzung entweder eine bestimmte Anzahl (aktuell eingestellter Wert wird angezeigt)



bzw. bis zu einem bestimmten Zeitpunkt (aktuell eingestellter Wert wird angezeigt)



Signaturen erzeugt werden können.

Über diesen Bestätigungsdialog wird gewährleistet, dass die autorisierte Person nach SigV, §15 (1) „bei der Erzeugung einer qualifizierten elektronischen Signatur“ c) „die Erzeugung einer Signatur vorher eindeutig angezeigt wird“. Im Sinne der Massensignatur wird hier eindeutig angezeigt, für wie viele bzw. für wie lange das Erzeugen von Signaturen erlaubt wird.

Dieser Dialog ist Länder-spezifisch und wird zur Zeit nur angezeigt, wenn das Einsatzland innerhalb der i-effect® \*SIGG-Konfiguration auf „Deutschland“ gesetzt wurde.

Es erscheint die Aufforderung der PIN-Eingabe für die Authentifizierung des in dem Slot befindlichen Token.

Je nach SmartCard erfolgt die Eingabe entweder über die System-Tastatur oder die Tastatur des Kartenlesegerätes.



#### Anmerkung:

In Deutschland erfordert das qualifizierte Signieren laut Signaturgesetz die Eingabe der PIN direkt am Kartenlesegerät. Eine Eingabe und Übermittlung der PIN durch die Signatursoftware ist nicht zulässig. Daher können nur solche Karten und dazugehörige Middleware eingesetzt werden, die nur die Eingabe am Kartenlesegerät zulassen.

In der Schweiz stellt sich die Situation anders da. Hier ist die Art des Zertifikates und die Absicherung des Zertifikates auf seiner Signaturerstellungseinheit ausschlag gebend. Hier können sog. eTokens eingesetzt werden, die einem USB-Stick gleichen oder auch SmartCards ohne Eingabe der PIN am Lesegerät selber. Eine Anmeldung kann hier über die Tastatur erfolgen.

Im Anschluss an die erfolgreiche Eingabe der PIN wird die Signatur-Sitzung initialisiert. Je nach den im Vorfeld vorgenommenen Einstellungen wird die Gültigkeit der Sitzung auf die voreingestellten Werte bzw. die individuellen Werte gesetzt.

Eine erfolgreiche Initialisierung der Signatur-Sitzung wird durch einen grünen Pfeil angezeigt. Darüber hinaus wird in Abhängigkeit der gewählten Form der Gültigkeit (Anzahl Signaturen oder Zeitraum) die Anzahl der verbleibenden Signaturen bzw. der End-Zeitpunkt der Sitzungsgültigkeit angezeigt.

#### Slots Status

##### SmartTrust Personal

Slot (ID: 3)  Gültig bis: 2006-11-16 10:58:00

#### Anmerkung:

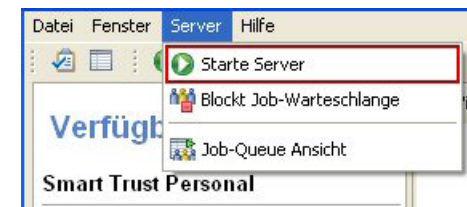
Ist i-effect® \*SIGG zum Zeitpunkt des Aktivierens einer Sitzung nicht aktiv, wird der Signaturserver automatisch gestartet.

## Starten von i-effect® \*SIGG

i-effect® \*SIGG kann entweder über die Symbolleiste oder das Menü „**Server**“ gestartet (bzw. gestoppt) werden.



Starten des Servers über die Symbolleiste:



Starten des Servers über das Menü Server->Starte Server

# Starte Signatur-Job

Für das Starten eines Signatur-Jobs ist es zunächst notwendig den Green Screen von i-effect® – die integrierte Lösung für IBM Power Systems – aufzurufen.

Vom i-effect® - Hauptmenü aus gelangt man über die Eingabe von **12 <ENTER>** in das Menü für die Auswahl von Verschlüsselung bzw. Signaturen.

```
IEFFECT      i-effect - Die integrierte Lösung für IBM iSeries
System:      IEFFECT

Auswahlmöglichkeiten:

10. Zu den Konvertierungsaufgaben
11. Zu den Komprimierungsaufgaben
12. Zu den Signatur- und Verschlüsselungsaufgaben
13. Zu den Kommunikationsaufgaben
```

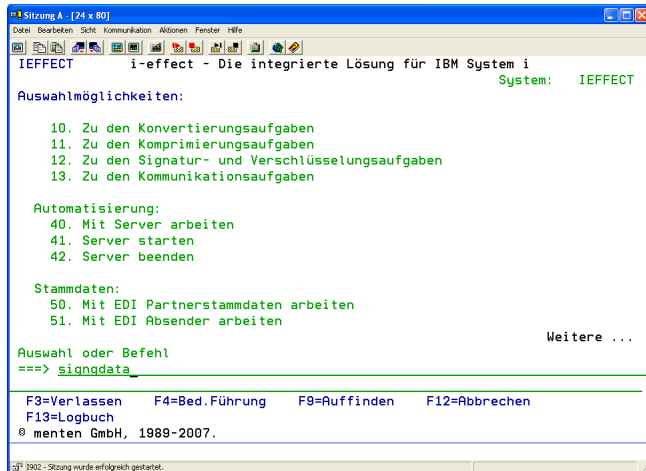
Hier können Sie durch die Auswahl des dritten Menüpunktes mit **3 <ENTER>** einen Auftrag für das Erstellen einer qualifizierten Signatur erteilen.

```
CRYPT        i-effect Signatur- und Verschlüsselungsaufgaben
System:      IEFFECT

Auswahlmöglichkeiten:

Signatur:
1. PDF Datei(en) signieren
2. PDF Datei(en) Verifizieren
3. Datei(en) qualifiziert signieren
4. Datei(en) verschlüsseln
5. Datei(en) entschlüsseln
```

Alternative: Mit Hilfe des Aufrufs **signqdata + <F4>** werden die Parameter des Befehls ‚signqdata‘ angezeigt.



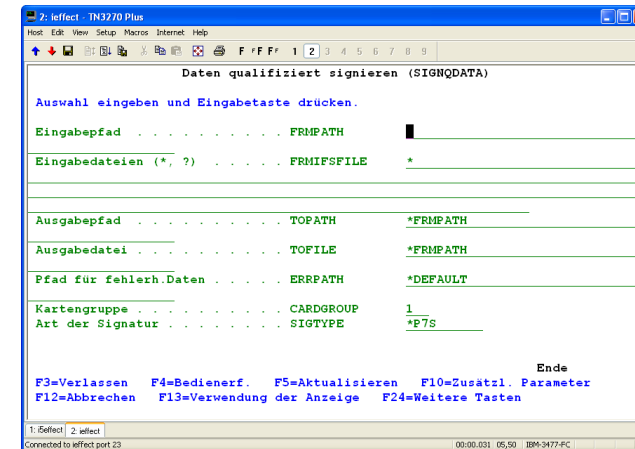
Von hier aus wird die Arbeitsweise für die Ausführung eines Signature-Jobs festgelegt. Insgesamt gibt es je nach gewählter Signatur-Art bis zu drei Parameterseiten, auf denen entsprechend Parameter gesetzt werden können.

## Anmerkung:

Der Befehl `signqdata` erstellt ausschließlich Signatur-Jobs, die durch i-effect® von der IBM Power Systems aus an den eigentlichen Signaturserver (i-effect® \*SIGG) übertragen werden. Der Signatur-Job übermittelt die Informationen zu den zu signierenden Daten und in welcher Form sie signiert werden sollen. Das in die IBM Power Systems integrierte Sicherheitskonzept ermöglicht es, genau zu definieren wer autorisiert ist den Befehl `signqdata` auszuführen, um den Missbrauch von i-effect® \*SIGG zu verhindern.

Auf der ersten Seite werden die grundlegenden Einstellungen der Parameter vorgenommen, wie Dateipfad-Angaben und die Auswahl der Art der Signaturerstellung. Die Auswahl der Art der Signaturerstellung bewirkt, dass sich der Konfigurations-Dialog entsprechend anpasst.

Mit Hilfe von **<F10>** können die weiteren Seiten von Parametern, basierend auf der getroffenen Auswahl, angezeigt und anschließend mit **<Bild-ab>** bzw. **<Bild-auf>** durchlaufen werden. Mit **<F9>** können alle Parameter des Befehls zur Anzeige gebracht werden.



## Eingabepfad [FRMPATH]

Den absoluten Pfad zu der zu signierenden Datei.

## Eingabedateien (\*,?) [FRMIFSFIL\*]

Die Dateinamen der zu signierenden Dateien.

## Ausgabepfad [TOPATH]

Optional: absoluter Pfad zum Ausgabeverzeichnis.

### Voreinstellung:

**\*FRMPATH** Bewirkt die Übernahme des Eingangspfades zu der zu signierenden Datei.

## Ausgabedatei [TOFILE]

Optional: Dateiname, unter der die signierte Datei abgelegt werden soll.

### Voreinstellung:

**\*FRMPATH** Bewirkt die Übernahme des Eingangspfades zu der zu signierenden Datei.

Im Falle einer PDF-Signatur wird der Originaldateiname verwendet. Wurde bei TOPATH ebenfalls die Voreinstellung \*FRMPATH ausgegeben, wird bei erfolgreicher Signatur der PDF-Datei die Originaldatei durch die signierte Datei ersetzt.

Im Falle einer P7S-Signatur wird an den Dateinamen die Endung „.p7s“ angehängen.

Im Falle einer P7M-Signatur wird der Dateiname mit der Endung „.p7m“ verwendet.

Im Falle der EDIFACT-Signatur wird der Originaldateiname verwendet. Wurde bei TOPATH ebenfalls die Voreinstellung \*FRMPATH verwendet, wird bei erfolgreicher Signatur der EDIFACT-Datei die Originaldatei durch die signierte Datei ersetzt.

## Pfad für fehlerh.Daten [ERRPATH]

Optional: Pfad zum Fehlerverzeichnis, in den nicht signierte Dateien aufgrund eines aufgetretenen Fehlers abgelegt werden sollen.

### Voreinstellung:

**\*DEFAULT** Übernimmt das Standard-Fehlerverzeichnis. Es befindet sich innerhalb des i-effect® Installationsverzeichnisses unter sigg/error.

## Kartengruppe [CARDGROUP]

Es ist möglich einzelnen Slots eine sog. Kartengruppe zuzuordnen. Die Kartengruppe ermöglicht es, das Erzeugen einer Signatur von einer bestimmten Karte durchführen zu lassen. Der Signaturauftrag kann nur von einem Slot durchgeführt werden, der der entsprechenden Kartengruppe angehört.

## Art der Signatur [SIGTYPE]

Es wird zwischen vier Signatur-Typen unterschieden:

**\*PDF** Die Signatur wird in das PDF-Dokument eingebettet

**\*P7S** Die Signatur wird in einer separaten Datei vom Typ „.p7s“ gespeichert.

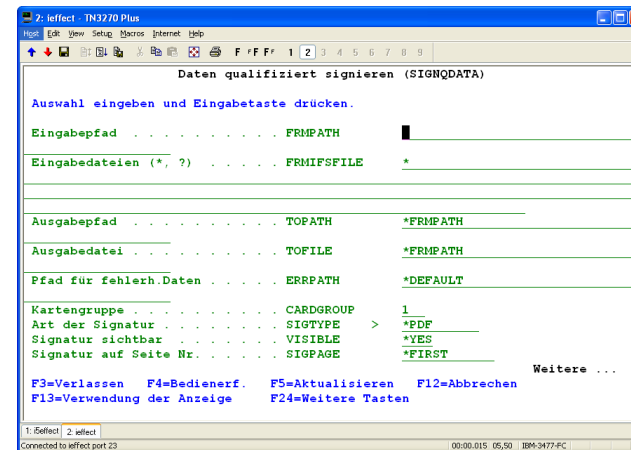
**\*PKCS7** Die Signatur wird zusammen mit den signierten Daten in einen „SignedData“-Container im ASN.1-Format gepackt und als Datei gespeichert.

**\*P7M** Die Signatur wird Zusammen mit der Datei in eine neue Datei vom Typ „.p7m“ gespeichert.

**\*EDIFACT** „Attached Digital Signature“ nach EANCOM 2002 Syntax 4. Es werden alle oder nur ein angegebener Nachrichtentyp signiert. Die Signatur/-en wird/werden in der Originaldatei eingebettet.

## Konfiguration für das Erstellen einer PDF-Signatur:

Durch die Auswahl von \*PDF bei „Art der Signatur“ erscheinen bereits auf der ersten Konfigurationsseite im Anschluss spezifische Parameter, die nur bei der PDF-Signatur Anwendung finden.



## Signatur sichtbar [VISIBLE]

Nur PDF-Signatur! Legt fest, ob die Signatur innerhalb des PDF-Dokumentes sichtbar ist oder nicht.

### Voreinstellung:

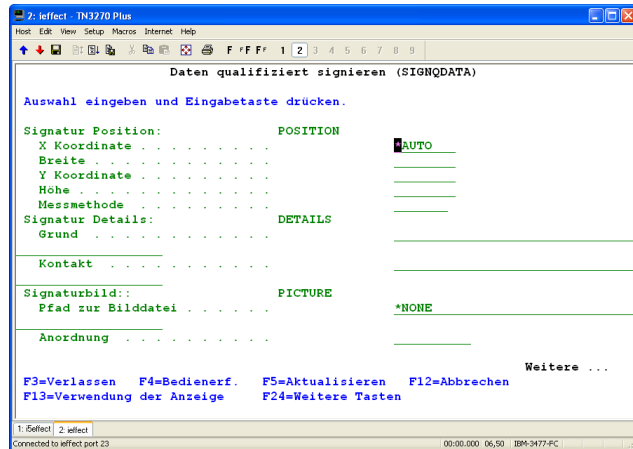
**\*YES** Der Wert \*NO bewirkt die nicht sichtbare Einbindung der Signatur.

## Signatur auf Seite Nr. [SIGPAGE]

Nur PDF-Signatur! Legt fest, auf welcher Seite die Signatur zu sehen sein soll.

### Voreinstellung:

**\*FIRST** Bewirkt die Einbindung der sichtbaren Signatur auf der ersten Seite



Konfigurations-Seite 2 von „signqdata“ (Nur bei Signatur-Typ \*PDF in dieser Form sichtbar):

## Signatur Position [POSITION]

Nur PDF-Signatur!

### X Koordinate

Abstand der Anzeige der Signatur von der linken Seite des PDF-Dokuments.

### Voreinstellung:

**\*AUTO** Bewirkt, dass für X-, Y-Koordinaten, Breite und Höhe die Standard-Einstellungen verwendet werden.

X-Koordinate: 1

Breite: 5

Y-Koordinate: 1

Höhe: 2

Messmethode: cm

### Breite

Breite der Signatur innerhalb des PDF-Dokuments.

## Y Koordiante

Abstand der Anzeige der Signatur vom unteren Rand des PDF-Dokuments.

## Höhe

Höhe der Signatur innerhalb des PDF-Dokuments.

## Messmethode

Maßeinheit der Angaben X-, Y-Koordinate, Breit und Höhe für die Bestimmung der realen Position innerhalb des PDF-Dokuments.

## Signatur Details [DETAILS]

Nur PDF-Signatur!

### Grund

Optional: Angabe eines Grunds für das Signieren des PDF-Dokuments.

### Kontakt

Optional: Angabe eines Kontakts.

## Signaturbild [PICTURE]

Nur PDF-Signatur!

### Pfad zur Bilddatei

Optional: Angabe eines absoluten Pfades zu einer Bilddatei, die als Hintergrund der sichtbaren Signatur im PDF-Dokument verwendet werden soll.

Die Datei kann vom Typ JPG, GIF, BMP oder PNG sein.

### Voreinstellung:

**\*NONE** Es wird kein eigenes Bild verwendet. Der PDF-Reader verwendet sein eigenes Standardbild.

## Anordnung

Optional: Gibt an, wie das Bild innerhalb der Signatur angeordnet werden soll.

### Erlaubte Werte:

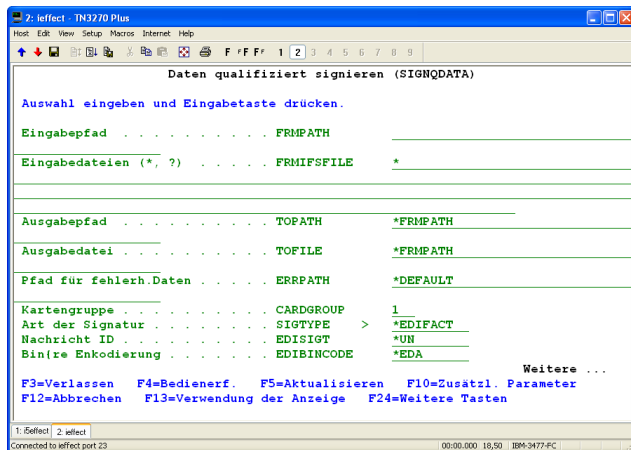
**\*RIGHT** Bild wird Rechts-Mitte angeordnet

**\*LEFT** (Voreinstellung) Bild wird Links-Mitte angeordnet

- \*TOP** Bild wird Mitte-Oben angeordnet
- \*BOTTOM** Bild wird Mitte-Unten angeordnet

## Konfiguration für das Erstellen einer EDIFACT-Signatur:

Durch die Auswahl von **\*EDIFACT** bei „Art der Signatur“ erscheinen auf der ersten Konfigurationsseite im Anschluss spezifische Parameter, die nur bei der EDIFACT-Signatur Anwendung finden.



### Signatur Typ [EDISIGT]

Die Art bzw. das Format der EDIFACT-Signatur kann hier angegeben werden.

Es wird zwischen vier EDIFACT-Signatur-Typen unterschieden:

- \*UN** (Voreingestellt) Das von der UN definierte Format signierter EDIFACT-Dateien mit den entsprechend aufgebauten Segmenten und Datenelementen
- \*EANCOM** Das von der EANCOM empfohlene Format signierter EANCOM-Dateien mit dem entsprechenden Aufbau der Segmente und Datenelementen. Entspricht weitestgehend dem UN-Format.
- \*IMS30** Das „Ideal Message Schweiz“-Format signierter EANCOM-basierender Dateien in der Version 3.0.

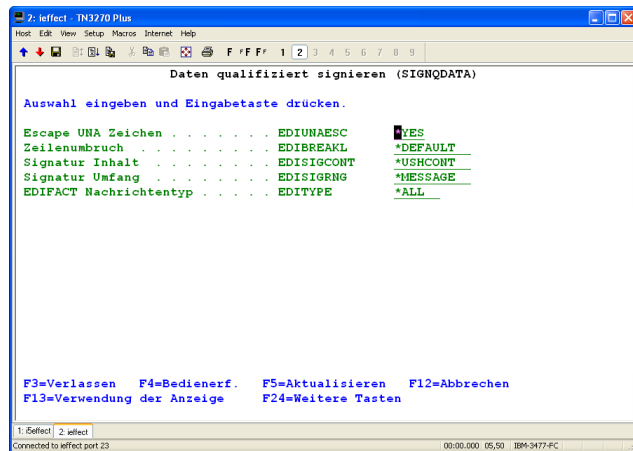
- \*IMS31** Das „Ideal Message Schweiz“-Format signierter EANCOM-basierender Dateien in der Version 3.1. Es unterscheidet sich von der Version 3.0 nur in Korrekturen des Aufbaus der Datenelemente.  
Im Grunde entspricht dieses Format dem EANCOM-Format für signierte EANCOM-Dateien, da IMS Version 3.1 als Basis für den EANCOM-Standard erarbeitet wurde.

### Binäre Encodierung [EDIBINCODE]

Das Encoding-Format, mit dem binäre Werte von Datenelementen kodiert werden sollen, um sicherzustellen, dass keine nicht erlaubten Zeichen innerhalb der Datei verwendet werden.

Es werden vier Encoding-Typen unterstützt:

- \*EDA** (Voreingestellt) Bei dem EDA Filter nach ISO 9735-5 handelt es sich um ein Encoding, welches Binärdaten in einen kodierten Datensatz mit dem Zeichensatzumfang von UNOA erzeugt. Der Datensatz vergrößert sich durch das Encoding um die Rate 3/2, wobei 2 der 3 Teile den Nutzdaten entsprechen (50% größere Datenmenge)
- \*EDC** Bei dem EDC Filter nach ISO 9735-5 handelt es sich um ein Encoding, welches Binärdaten in einen kodierten Datensatz mit dem Zeichensatzumfang von UNOC erzeugt. Der Datensatz vergrößert sich durch das Encoding um die Rate 8/7, wobei 7 der 8 Teile den Nutzdaten entsprechen (ca. 17% größere Datenmenge)
- \*HEX** Das HEX-Encoding wandelt Binärdaten in eine Hexadezimale Zeichenkette mit den Zeichen 0-9 und A-F um. Die Größe der kodierten Datenmenge verdoppelt sich gegenüber den eigentlichen Binärdaten.
- \*BASE64** Das BASE64-Encoding wandelt die Binärdaten in eine Kette druckbarer Zeichen um, die aus 64 Zeichen besteht: A-Z, a-z, 0-9, +, / (ohne Umlaute und ß). Die Größe der kodierten Datenmenge vergrößert sich um ca. 33% gegenüber der ursprünglichen Datenmenge.
- \*NONE** Es wird kein Encoding verwendet. Die Binärdaten werden unkodiert in die Datei übernommen.



Konfigurations-Seite 2 von ‚signqdata‘ (Nur bei Signatur-Typ \*EDIFACT sichtbar):

### Escape UNA Zeichen [EDIUNAESC]

Einstellen, ob innerhalb der neu eingefügten Signatur-Segmente der EDIFACT-Datei die UNA-Zeichen „escaped“ (entwertet) werden sollen.

#### Mögliche Werte:

- \*YES** (Voreingestellt) Vorhandene UNA Zeichen innerhalb der neuen Segmente werden mit dem im UNA-Segment definierten Escape-Zeichen entwertet (Standardseitig wird ‚?’ verwendet).
- \*NO** Vorhandene UNA Zeichen innerhalb der neuen Segmente werden nicht entwertet.

### Zeilenbruch [EDIBREAKL]

Über diesen Parameter kann eingestellt werden, ob EDIFACT-Dateien ein CRLF am Ende eines Segmentes angefügt bekommen sollen oder nicht. Je nach Einstellung wird dabei die Ursprungsdatei geändert und Zeilenbrüche hinzugefügt oder entfernt.

Alternativ kann die Voreinstellung verwendet werden, die die Datei hinsichtlich der Zeilenbrüche im Ursprungszustand belässt.

#### Mögliche Werte:

- \*DEFAULT** (Voreingestellt) Der Ursprungszustand der Datei wird belassen hinsichtlich vorhandener bzw. nicht vorhandener CRLF.
- \*YES** Sind in der Ursprungsdatei keine Zeilenbrüche vorhanden, werden CRLF hinzugefügt.

- \*NO** Sind in der Ursprungsdatei Zeilenbrüche enthalten, werden diese entfernt.

### Signatur Inhalt [EDISIGCONT]

Über diesen Parameter wird beim Signieren von EDIFACT-Messages eingestellt, über welchen Inhalt die Signatur gebildet werden soll.

#### Mögliche Werte:

- \*USHCONT** (Voreingestellt) Es wird der neu zu erzeugende Signatur-Header zusammen mit dem Inhalt der Message signiert. Bereits vorhandene Signatur-Segmente früherer Signaturprozesse werden nicht in die Berechnung für die Signatur mit einbezogen.
- \*USHTOUST** Der Message-Inhalt von Beginn des neuen Signatur-Headers bis hin zum Beginn der neuen Signatur-Tailer-Segment wird für die Berechnung der Signatur herangezogen. Vorangegangene in die Message eingebrachte Signaturen sind Teil der Signatur.

### Signatur Umfang [EDISIGRNG]

Mit diesem Parameter wird der zu signierende Umfang innerhalb eines EDIFACT-Interchanges (-Datei) festgelegt.

#### Mögliche Werte:

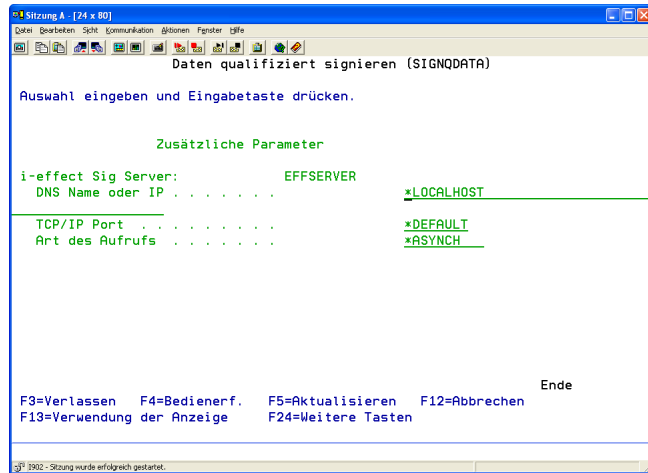
- \*MESSAGE** (Voreingestellt) Jede Message eines Interchanges wird signiert (sofern nicht mit EDITYPE der zu signierende Nachrichtentyp eingeschränkt wird).
- \*INTCHANGE** Der komplette EDIFACT-Datenstrom (-Datei) wird signiert. Es wird nur eine Signatur über die gesamten enthaltenen Daten erzeugt.
- \*GROUP** Jede Gruppe innerhalb eines EDIFACT-Interchange wird signiert.

### EDIFACT Nachrichtentyp [EDITYPE]

Es können entweder alle Nachrichtentypen (\*ALL) einer EDIFACT-Datei signiert werden oder ein bestimmter Nachrichtentyp (Bsp: ORDERS, INVOICE).

#### Voreinstellung:

- \*ALL** Alle Nachrichtentypen einer EDIFACT-Datei werden signiert.



Abschließende Konfigurations-Seite von ‚signqdata‘:

### i-effect \*SIGG Server [EFFSERVER]

#### DNS Name oder IP

Name oder IP-Adresse des Systems, auf dem der Signatur-Server ausgeführt wird.

#### Voreinstellung:

**\*LOCALHOST**



#### Anmerkung:

Die IP-Adresse des Servers muss mit angegeben werden, da der Signatur-Server nicht lokal ausgeführt wird

#### TCP/IP Port

TCP/IP Port des Signatur-Servers

#### Voreinstellung:

**\*DEFAULT** Bewirkt die Übernahme des im i-effect® System voreingestellten Ports (22005)

### Art des Aufrufs

Die Art wie der Server mit dem Aufruf verfahren soll.

- \*ASYNCH** Voreinstellung) - Der Signatur-Server veranlasst i-effect® nicht auf die Beendigung des Signatur-Jobs zu warten
- \*SYNCH** i-effect® wartet auf die Beendigung des Signatur-Jobs durch den Signatur-Server

## Überwachung und Kontrolle

### Übersicht laufender Programm-Aktivität

Die Übersicht Info informiert über die aktuellen und getätigten Aktivitäten von i-effect® \*SIGG.

Info	
Server:	<b>X</b>
Erledigte Jobs:	0
Fehlerhafte Jobs:	0
Jobs zu signieren:	0 (0)
Gesicherte Jobs:	0

#### Server

Das Feld Server zeigt an, ob der eigentliche Signaturserver läuft (grünes Häkchen) oder deaktiviert ist (rotes Kreuz).

#### Erledigte Jobs

Zeigt die Summe aller erfolgreich durchgeführten Signaturen einzelner Dateien seit dem Start des Programms an.

#### Fehlerhafte Jobs

Zeigt die Summe aller Signaturen an.

## Jobs zu signieren

Der erste Wert stellt die Anzahl der zu signierenden Jobs, die sich in der Warteschlange befinden, dar.

Der zweite Wert (in Klammern) steht für die Anzahl der Jobs, die aufgrund eines behebbaren Fehlers zwischengepuffert werden, bevor eine erneute Einreihung in die eigentliche Warteschlange erfolgt.

Anmerkung: Die Ansicht der Job-Warteschlange (Queue) zeigt sowohl die Jobs der eigentlichen Warteschlange, als auch die des Zwischenspeichers an, um diese löschen zu können.

## Gesicherte Jobs

Zeigt die Anzahl gesicherter Jobs an. Jobs werden gesichert/gespeichert sollte der Server gestoppt werden, obwohl noch Jobs in der Warteschlange sind. Beim nächsten Start des Servers werden diese Jobs wieder hergestellt.



Auch bei einem Systemabsturz/-ausfall bzw. Programmabsturz werden auf diese Weise alle noch gespeicherten Jobs wieder hergestellt.

Anmerkung: \*SIGG Jobs, die synchron gestartet worden sind, werden nicht gespeichert. Diese Jobs werden mit einem ABBRUCH beendet.

## Auftrags-Übersicht

In der Auftrags-Übersicht werden alle Aufträge angezeigt, die auf Basis der eingestellten Wahrscheinlichkeit in i-effect® \*SIGG hinterlegt wurden. Diese Übersicht dient als Kontroll-Mittel, um zumindest Stichprobenhaft die übergebenen zu signierenden Daten einsehen zu können.

Dieser Kontroll-Mechanismus dient der Überprüfung der Daten hinsichtlich möglicher Manipulationen durch Dritte bzw. unauthorisierter Personen und deckt die Anforderung des Signaturgesetzes, Daten vor der Signatur einsehen (bzw. die nicht signierte Fassung betrachten) zu können ab.

Sitzung	Original	Signiert	Datei-Name	Signatur-Typ	Übergeben am
4418			TEST.PDF	PDF	2006-11-03 08:39:23:359

### Sitzung

Zeigt die Sitzungsnummer an, unter der der Auftrag im i-effect® Logbuch geführt wird.

## Original

Über einen Doppelklick mit der Maus auf das Symbol kann die Originaldatei in Abhängigkeit vom Typ im Adobe Acrobat Reader 6.0 oder im MS Windows Editor angezeigt werden.

## Signiert

Im Falle, dass es sich bei der Originaldatei um ein PDF-Dokument handelte und die Signatur in das Dokument eingebettet werden sollte, wird nach erfolgreichem Signieren eine entsprechendes Symbol in dieser Spalte angezeigt. Ein Doppelklick mit der Maus auf das Symbol öffnet die signierte Datei im Adobe Acrobat Reader 6.0.



## Datei-Name

Der Name der Datei, die es zu signieren gilt.

## Übergeben am

Zeitpunkt der Übergabe an den Signatur-Server.



Ansicht der Auftrags-Übersicht mit signiertem PDF-Dokument:

Sitzung	Original	Signiert	Datei-Name	Signatur-Typ	Übergeben am
4418			TEST.PDF	PDF	2006-11-03 08:39:23:359

Alternativ kann über einen Rechtsklick mit der Maus auf den gewünschten Auftrag das Kontextmenü aufgerufen werden.

Zum einen kann die Originaldatei über das Menü geöffnet werden und sofern vorhanden auch die signierte Datei.

Hier eine Beispielsicht des Menüs bei Vorhandensein eines signierten PDF-Dokuments:

Sitzung	Original	Signiert	Datei-Name	Signatur-Typ	Übergeben am
4418			TEST.PDF	PDF	2006-11-03 08:39:23:359

Zeige ausgewählte Originaldatei

Zeige ausgewählte signierte Datei

## Logging

i-effect® \*SIGG protokolliert alle wesentlichen Abläufe innerhalb des Programms und stellt diese Informationen zum Einigen in der „**Log Ansicht**“ zur Verfügung:

Datum	Log Typ	Name	Text
2006-11-07 09:37:31:156	INFO : Slot...	Slot ausgewählt	Slot ID:52481 ausgewählt zum Signieren
2006-11-07 09:37:19:890	INFO : SigG...	Starte SigGServer	Starte Server

Zum Anderen werden Log-Dateien gepflegt, die alle auftretenden Meldungen unterhalb des Installationsverzeichnis im Ordner **workspaceVogs** speichern.

Ein Rechtsklick mit der Maus öffnet das Kontextmenü, mit dessen Hilfe einzelne oder mehrere Logbucheinträge in die Zwischenablage kopiert werden können oder die Log-Datei - Übersicht geöffnet wird.

Datum	Log Typ	Name	Text
2006-11-07 09:28	INFO : Slot...	Slot ausgewählt	Slot ID:52481 ausgewählt zum Signieren
2006-11-07 09:28	INFO : SigG...	Starte SigGServer	Starte Server

### Kopiere in Zwischenablage

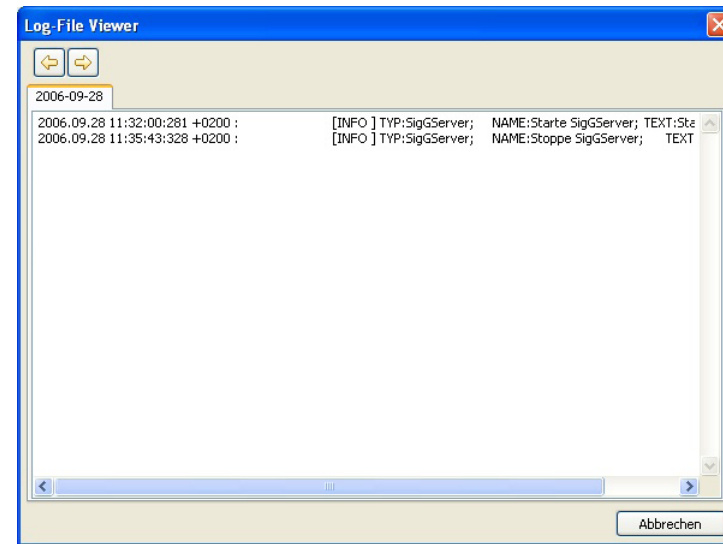
Kopiert den Inhalt der ausgewählten Zeilen in die Zwischenablage. Die Inhalte der einzelnen Zeilen der Tabelle werde im Format der Ausgaben in die Log-Datei umgewandelt.

### Zeige Inhalt der Log-Datei

Öffnet die Log-Datei - Übersicht mit der Log-Datei, in der sich der Inhalt der ausgewählten Zeile befindet. Bei einer Auswahl mehrere Einträge in der Tabelle werden ggfs. mehrere Reiter in der Log-Datei - Übersicht geöffnet (abhängig davon, ob die Einträge in verschiedenen Dateien vorkommen).

Die Log-Datei - Übersicht ermöglicht das Durchwandern aller verfügbaren Log-Dateien mit Hilfe der Pfeiltasten im oberen Bereich des Fensters.

Je Kalendertag, den das Programm läuft, wird eine entsprechende Log-Datei nach dem Muster siggserver-JAHR-MONAT-TAG.log angelegt.



## Auftrags-Logging in i-effect®

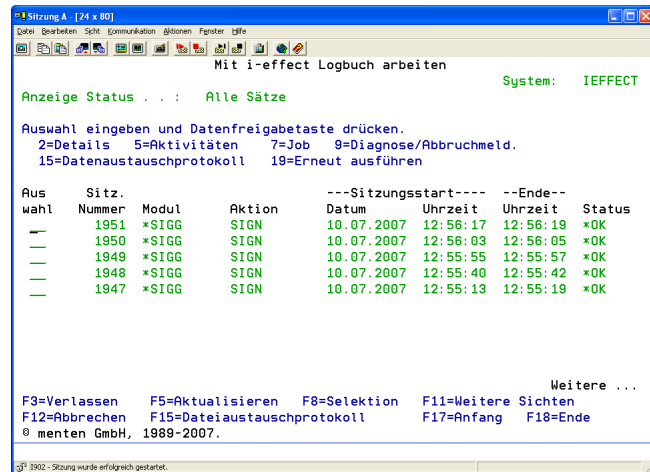
Die vom i-effect® – die integrierte Lösung für IBM Power Systems – erstellten und an den Signatur-Server übergebenen Signaturaufträge tragen ihre Meldungen über erfolgte Zwischenschritte und Ereignisse in das i-effect® Log-Buch ein.

Im i-effect® Logbuch kann der aktuelle Status eines erstellten Signatur-Auftrags eingesehen werden.

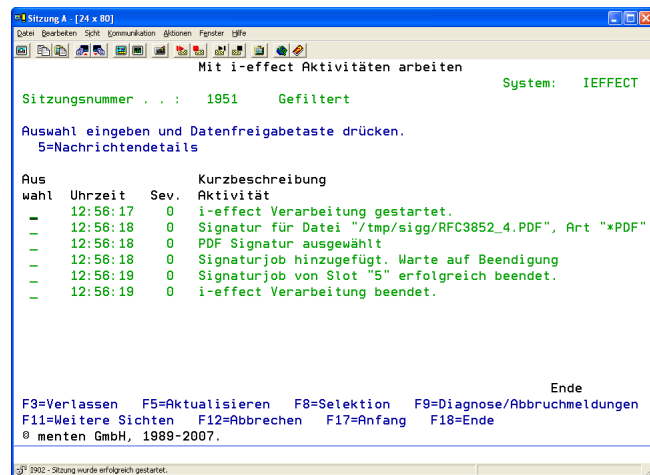
Solange sich ein Auftrag im ACTIVE-Status befindet, ist er vom i-effect® \*SIGG noch nicht abgearbeitet und an i-effect® zurückgegeben worden.

Ein Auftrag kann mit dem Status **\*OK**, **\*DIAG** oder **\*ERROR** abgeschlossen werden.

Ist ein Auftrag erfolgreich signiert worden, sendet der Signatur-Server ein \*OK an i-effect® zurück.



Die Einsicht in die Nachrichten eines Auftrages zeigt den Werdegang an: welche Datei(en) mit welchem Slot auf welche Art von i-effect® \*SIGG bearbeitet wurden.



Ein Abschluss eines Auftrages mit \*DIAGNOSE bedeutet, dass nicht alle mit dem Auftrag übergebenen Dateien erfolgreich signiert werden konnten. Eine Durchsicht der Meldungen sollte die Ursache der einzelnen Probleme erkennen lassen.

Ein Abschluss mit \*ERROR kann verschiedenste Ursachen haben. Auch hier hilft nur die Durchsicht der Meldungen, die zu diesem Auftrag im Job-Log hinterlegt wurden.

## Logging im ‚internal‘-Verzeichnis von i-effect®

Im „internal“-Verzeichnis einer i-effect®-Installation werden detailliert Informationen über die Abläufe der einzelnen i-effect® Module protokolliert und unterstützt die Suche und Behebung möglicher Probleme.

Die Log-Datei wird nach dem Muster „JAHR-MONAT-TAG-sigg.log“ für das \*SIGG-Modul angelegt.

Dieses Logging ist in gewisser Hinsicht eine Ergänzung zum i-effect® Logbuch und nimmt nur Informationen auf, die mit dem Server-Dienst und der Signaturlogik des \*SIGG Signaturserver in Zusammenhang stehen.

## Update von i-effect® \*SIGG

Um eine neue Version von i-effect® \*SIGG zu installieren muss die ursprünglich installiert Version deinstalliert werden.

Sie können i-effect® \*SIGG entweder über die Systemsteuerung -> Software deinstallieren oder über das Windows-Menü:



Anschließend könne Sie die neue Version von i-effect® \*SIGG wie unter „Installation von i-effect® \*SIGG“ beschrieben installieren.

### WICHTIG:

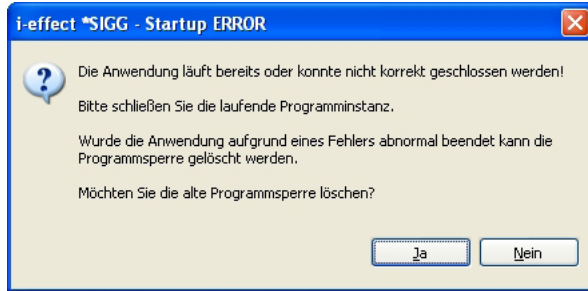
*Haben Sie vor ein Update von i-effect® – die integrierte Lösung für IBM Power Systems – auf eine neue Version zu machen, ist auch ein Update auf die passende Version des i-effect® \*SIGG Moduls erforderlich!*

# Fehlerbehebung

## Fehlermeldung während Programmstart

Um zu Verhindern, dass aus Versehen mehrere Instanzen des \*SIGG Signaturservers parallel laufen, wird ein Sperrmechanismus aktiviert.

Wird der \*SIGG Signaturserver ein weiteres Mal gestartet, erhalten Sie folgende Meldung:



Der Start des \*SIGG Signaturservers wird unterprohen.

Für den Fall, dass diese Anzeige erscheint obwohl definitive keine weitere Instanz geöffnet ist, kann die Sperre aufgehoben werden. Es könnte sein, dass durch einen Programmabsturz die Sperre nicht mehr aufgehoben werden konnte.

In diesem Fall können Sie bedenkenlos die Sperre löschen.



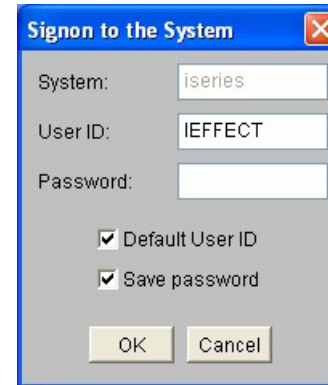
### Anmerkung:

**WICHTIG !!!** Das Löschen der Sperre würde auch durchgeführt werden können, wenn eine weitere Instanz des Programm läuft! Sollten Sie dennoch die Sperre löschen, startet der Signaturserver. Die Folge: Datenverlust, Schädigung der Programmkonfiguration, Fehler bei der Durchführung von Signaturen.

## Eingetragenes Benutzerpasswort fehlerhaft



Wurde ein falsches Passwort in die Programm-Einstellungen für den Benutzer der IBM Power Systems eingetragen, wird ein Dialog von dem Framework erzeugt, welches den Zugriff auf die Ressourcen der IBM Power Systems ermöglicht.



Das Schließen dieses ersten Fensters öffnet einen weiteren Dialog, der zur Eingabe des korrekten Passwortes für den eingetragenen Benutzer auffordert.

Bitte das Passwort hier nicht eintragen und den Dialog über **CANCEL** schließen! Ein Eintrag des Passwortes an dieser Stelle kann nicht vom SigG Signaturserver gespeichert werden!

## Löschen von nicht abgearbeiteten Jobs

An den Server bereits übergebene Jobs können auch manuell gelöscht werden, in dem die Warteschlangen-Übersicht geöffnet wird. Gelöschte Jobs werden im Job-Log des i-effect® - Systems mit Status **ABBRUCH** geführt.



### Anmerkung:

Solange diese Übersicht geöffnet ist, können keinen weiteren Jobs der Warteschlange abgearbeitet werden (Die Warteschlange wird geblockt)!



