

## Chapter 8c

# Qualified Electronic Verification

## Introduction

### i-effect® \*OCSP - At a Glance

- Secure Closed System Environment when used on IBM i
  - Legally Valid Verification
  - High Capacity Mass Verification of Invoices
  - Completely integrated into i-effect® V2R1 – the integrated solution IBM i
- 
- i-effect® \*OCSP (\*OCSP) is the signature verification module of i-effect® – the integrated solution for IBM i – (i-effect®); it can verify files in general and PDF or EDIFACT specifically according to the requirements of the German Signature ordinances (SigV) and German Signature Law (SigG). A manufacturers declaration has been registered for i-effect® \*OCSP, according to the requirements of SigV und SigG.
  - i-effect® \*OCSP's software is written in the Java programming language that requires a Java Runtime Edition of 5.0 or higher. The required PTFs/GroupPTFs and/or license programs must also be installed on the IBM i. System requirements can be viewed on our website <http://www.menten.com/com/i-effect/systemvoraussetzungen.php>.
  - i-effect® \*OCSP is the actual module that is responsible for generation of qualified verification reports in PDF format.
  - Bei i-effect® \*OCSP is a subsystem that runs independently from other i-effect® – the integrated solution for IBM System i – modules. It provides a service for the **"CRTOCSP"** command, in order to be able to receive and process verification jobs. The subsystem binds itself to a configurable IP Address (and Port-Number) on the IBM i-System.
  - i-effect® – the integrated solution for System i – creates a verification job using the **„CRTOCSP"** command and passes it to the i-effect® \*OCSP Module, which then

runs the signature verification in the form of a Service and/or Subsystems on the IBM i.

- i-effect® \*OCSP works to guarantee a high level of security in a closed system environment.

## i-effect® OCSP – Safe from Manipulation

To meet the requirements of German signature law, i-effect® \*OCSP has been equipped with a mechanism to detect manipulation to the software.

In addition, the program file of i-effect® \*OCSP can be tested for integrity as described in greater detail in the section „**Installation**“.

Successful verification guarantees that i-effect® \*OCSP's program file is an original and has not been manipulated.

## Installation

i-effect®'s installation instructions can be found in „**Kapitel 3**“.

### Testing the Integrity of the Program File

After successful installation of i-effect® – the integrated solution for IBM System i – i-effect® \*OCSP's program file must be tested for integrity.

For this purpose, we have provided a tool that tests the file's integrity. The program can be found under i-effect®'s – the integrated solution for IBM System i – installation directory in the sub folder OCSP/Tools, or in our download area on the i-effect® – Website.

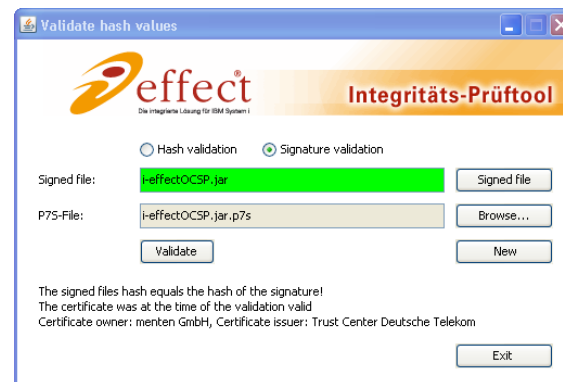
The tool is started by double clicking on “**i-effect\_Prueftool.jar**” and then select “**Signature Validation**” from within the program:



Open \*OCSP's program file by clicking on “**sign.file**”. It is located in the i-effect® -installation directory in the sub directory OCSP/LIB. The program file's name is “**i-effectOCSP.jar**”.

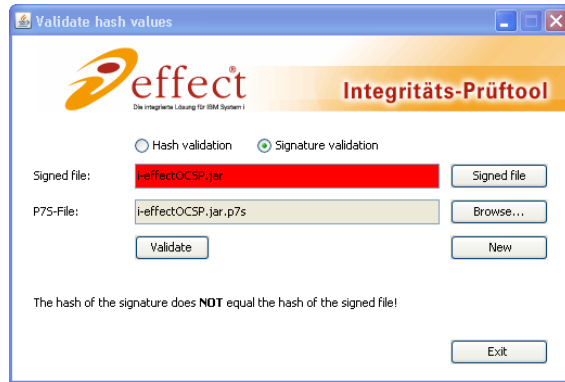
Using “**Browse...**” opens the signature file with the verification tool and click on “**Validate**”. The signature file has the same name as the program file and ends with “**.p7s**”.

If the test was successful the following display will appear:



Information regarding the owner and creator of the certificate will be provided in addition to information about the validity of the certificate and test results.

Unsuccessful validation looks as follows:



Verify that the correct files were used. If this is the case, contact us or one of our partners to receive a current, valid version of the program file.



**Note:**

The integrity of the program file can also be verified using the D-SIGN Reader from D-Trust. This tool can also be used to verify the online status of the certificate used for signatures.

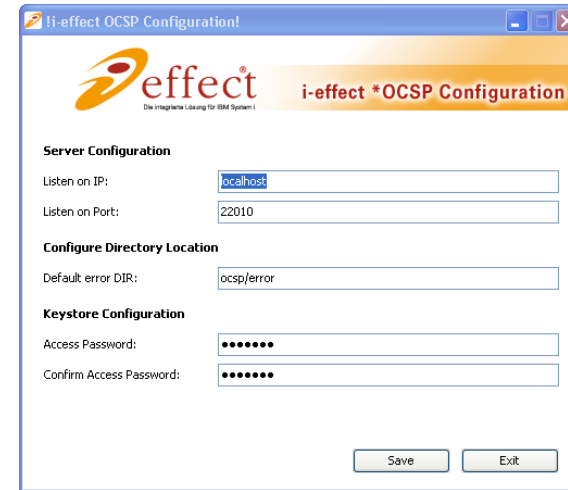
The software "D-SIGN Reader" can be found on D-Trust's website (<http://www.d-trust.net>). Click on "Service" and then the link "kostenlose Prüfsoftware".

## Configuration

i-effect® \*OCSP is setup using a configuration dialog. To open the configuration dialog open the installation directory of i-effect® – the integrated solution for IBM System i – and the sub directory OCSP.

In order to run the i-effect \*OCSP dialog Java Runtime Edition Version 5 or higher must be installed on the client PC.

The file "ocspConfigurationGUI.jar" is in the sub folder OCSP. Double clicking on it opens the configuration dialog:



## Program- Settings

The following explains the individual setting options in detail:

### Server Configuration

#### Bind to IP

This is the IP Address, to which i-effect® \*OCSP-Subsystem is bound, to receive incoming verification jobs. The default value "localhost" has been preset.

#### Bind to Port

The port, to which the i-effect® \*OCSP- Subsystem is bound, to receive incoming verification jobs. The default "22010" has been preset.

### Directory Configuration

#### Standard Error Directory

The directory where all files that could not be verified are stored.

### Keystore Configuration

#### Password

The password that allows access to the keystore by the subsystem. Changing the password does not change the existing password of the keystore!

## Confirm Password

Enter the password again to confirm that entry was correct.

## Setup

The operational environment must be set up according to the manufacturers declaration and the integrity of the program file must be guaranteed in order to run i-effect® \*OCSP. If the self test detects a change in the program file, the i-effect® \*OCSP-Subsystem cannot be started. In this case an entry in the (internal) logbook will be made (see „System monitoring“).

## OCSP Keystore

Is furnished with an empty keystore in which certificates required for verification can be stored.

Not all signatures of signed files contain the signing certificate (Public Certificate) that is required for verification, for example signed EDIFACT files. This is also the case with certificates that make up the certificate chain to the root certificate.

In these cases it is necessary to import the certificates and their corresponding certificate chain into the i-effect® \*OCSP-Keystore.

i-effect® \*OCSP's Keystore is located in the i-effect® -Installation directory in the sub folder "OCSP" and is named "2ocsp\_keystore.p12".

i-effect® \*OCSP's Keystore is managed using program "i-effectKeyManager.jar" that is also located in the sub folder "OCSP/Tools" of the installation directory.

This program can be used to import, delete and, if required, export certificates. It is also possible to change the keystore's password (the new password must be updated and the sub system restarted using the i-effect® \*OCSP-configuration dialog).

A detailed explanation of "i-effectKeyManager.jar" use can be found in the manual under „**Grafische Zusatzanwendungen**“.

i-effect®s- the integrated solution for IBM System i – manual can be downloaded from the website <http://www.i-effect.com>. Select the download area and then the sub category "manuals".

## i-effect® \*OCSP Start up

i-effect® – the integrated solution for IBM System i – has two ways to start the subsystem:

1. Start the subsystem using the i-effect-menu, **Option 85**

```

Sitzung B - [24 x 80]
Datei Bearbeiten Anzeige Kommunikation Aktionen Fenster Hilfe
IEFFECT i-effect - The integrated solution for IBM System i
System: H60B61DA

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

Automation:
40. Work with i-effect server
41. Start i-effect server
42. End i-effect server

Master data:
50. Work with EDI master data
51. Work with EDI originators
52. Work with EDI communication profiles
More...

Selection or command
==> 85

F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Logbook
  
```

Selecting **Option 85** from the i-effect-menu opens the overview for starting i-effect® subsystems (here is the second page of the i-effect-menu).

```

Sitzung B - [24 x 80]
Datei Bearbeiten Anzeige Kommunikation Aktionen Fenster Hilfe
Start i-effect subsystems (STREFFSBS)

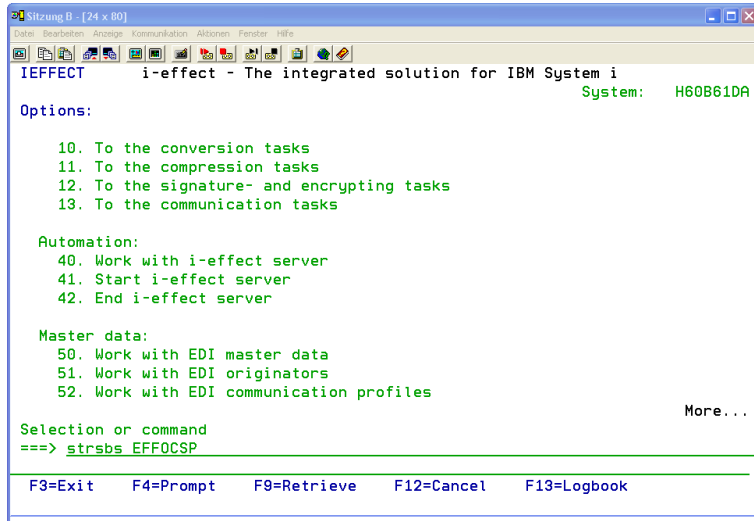
Type choices, press Enter.

Subsystem . . . . . > *OCSP *ALL, *AS2, *IEFFECT...
+ for more values

Bottom
F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
  
```

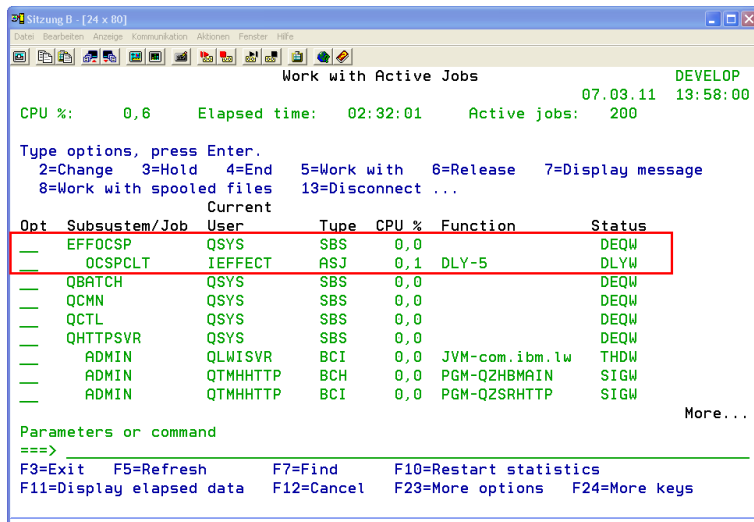
Entering \*OCSP and pressing enter starts the subsystem.

- Directly starting the subsystem.



i-effect®'s \*OCSP-Subsystem can be started directly using the **"STRSBS"** with the subsystem name **"EFFOCSP"** as a parameter.

Using **"WRKACTJOB"** will display if the subsystem is running or was started correctly:

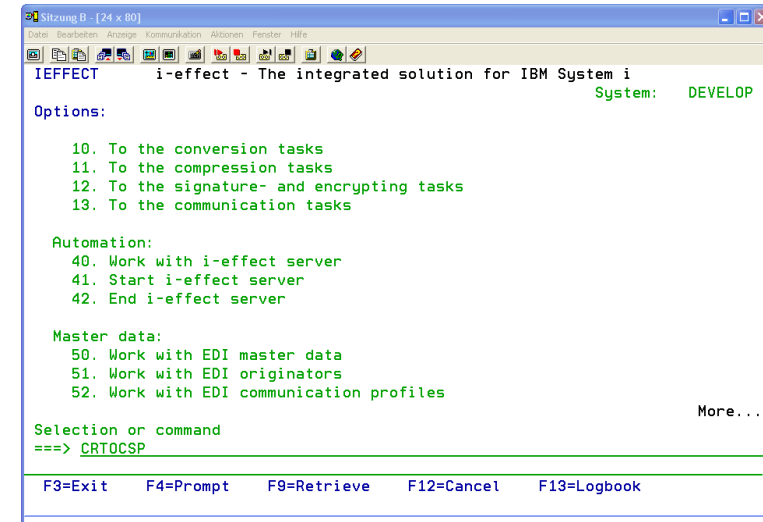


## Creating a Verification Job

Entering the command **"CRTOCSP"** and pressing the **Function key <F4>** are used to create a verification job.

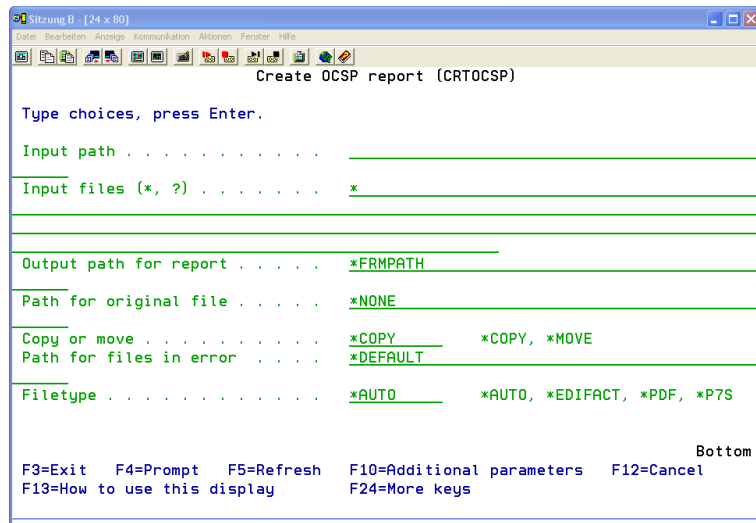
If i-effect®'s \*OCSP subsystem is not already running it will be started when this command is entered.

Pressing **<F4>** opens a overview of the command's possible parameters



### Note:

The **"CRTOCSP"** command only creates verification jobs. The verification job sends the information regarding the files for verification and where required in which format the signed files are in. IBM i's security concept can define who has the authority to run the **"CRTOCSP"** command to prevent misuse of i-effect® \*OCSP.



The parameter settings of the verification job are made on the first page, as well as file path specifications and the type of verification.

### Input Path [FRMPATH]

The absolute directory path, where the files for verification are located.

### Input Files (\*,?) [FRMIFSFIL]

File name or file pattern of the files for verification.

### Output Report Path [REPORTPATH]

Optional: absolute path for the output directory of the report.

#### Default Setting:

**\*FRMPATH** The input path will be used to store the report.

### Original File Path [OFILEPATH]

Optional: specifies an absolute path for storage of the original file. The verified file will either be copied or moved from its original location to the directory defined here.

#### Default Setting:

**\*NONE** The original file will remain at its original location.

#### Further Special Value:

**\*REPORTPATH** The directory specified as the report path will be used.

### Copy or Move [COPYMOVE]

#### Possible Values:

**\*COPY** (Default) Copies the verified file into the path entered in OFILEPATH, if \*NONE was not entered to prevent copying.  
**\*MOVE** The verified file will be moved into the path entered in OFILEPATH, if \*NONE was not entered to prevent copying.

### Error Path [ERRPATH]

Optional: Path where files will be moved that could not be verified.

#### Default Setting:

**\*DEFAULT** The standard error path is used. It is located in the i-effect installation directory under ocsf/error.

### File Type [FILETYPE]

#### Possible Values:

**\*AUTO** (Default) The system will attempt to determine the type of signature based on the file extension and then select the correct verification procedure.  
**\*EDIFACT** Verifies a signed EDIFACT file. The EDI file must be in the format EANCOM 2002 Syntax Level 4.  
**\*PDF** Verifies a signed PDF file, the signature should be in the PDF file.  
**\*P7S** Verification based on an external signature P7S/CMS file (SignedData). It is required that the signed file have the same name as the separate signature file without the ending 'p7s' and/or ',.cms'.

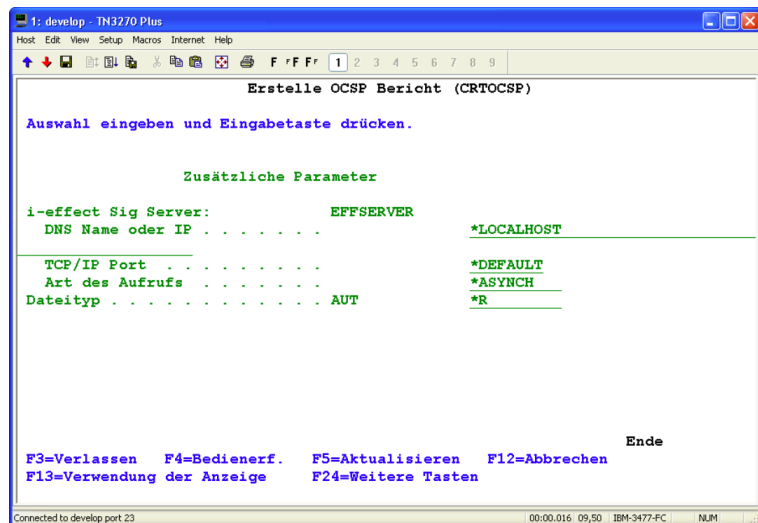
After the required parameters are specified, job generation must be confirmed by using the enter key. It is assumed that the i-effect® \*OCSP subsystem is configured with the default values (IP = „localhost“, Port = 22010).

If the configuration was changed and the subsystem uses a different IP address or a different port the command must also be configured to reflect this configuration.

If a job is sent to the wrong IP address or port an error message will occur. The verification job will not be carried out in this case.

To reach the second page of command configuration, the **Function Key <F9>** must be pressed within the first configuration page of the CRTOCSP command. By **<F9>** all parameters of the command can be edited. It is then possible to use the **<PAGE-UP>** or **<PAGE-DOWN>** - keys to switch between the pages.

On the second page the settings for the subsystem can be edited:



The Second configuration page of „CRTOCSP“:

### i-effect® \*OCSP Server [EFFSERVER]

#### DNS Name or IP

Name or IP-Address of the OCSP-Subsystem, to which it will bind itself.

#### Default Setting:

\*LOCALHOST

#### TCP/IP Port

TCP/IP Port of the OCSP Subsystems

#### Default Setting:

\*DEFAULT Uses the default i-effect® System Ports (22010)

### Type of Call

The way the server will handle the call.

<b>*ASYNCH</b>	(Default) The OCSP subsystem tells i-effect® not to wait until the verification job has ended.
<b>*SYNCH</b>	i-effect will wait until the verification job is ended by the OCSP-subsystem.

### File Type [AUT]

Optional: Specification of access rights to the report. Determines the data rights for \*PUBLIC for the report file.

<b>*R</b>	Read Only
<b>*RX</b>	Read and execute
<b>*RW</b>	Read and write
<b>*RWX</b>	Read, write and execute (all)
<b>*X</b>	Execute only
<b>*W</b>	Write only
<b>*WX</b>	Write and execute
<b>*NONE</b>	No authority

## i-effect \*OCSP Shutdown

There are two ways to shutdown the subsystem:

1. End the subsystem using the i-effect-menu with **option 86**

```

Sitzung B - [24 x 80]
Datei Bearbeiten Anzeige Kommunikation Aktionen Fenster Hilfe
IEFFECT i-effect - The integrated solution for IBM System i
System: DEVELOP

Options:
  53. Work with EDI communication resources

Administration:
  80. Work with program modules
  81. Work with logbook

  83. Reorganize logbook content

  85. Start i-effect subsystems
  86. End i-effect subsystems

Selection or command
==> 86

F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Logbook
Bottom
  
```

**Option 86** confirmed by enter opens the menu for subsystem shutdown.

```

Sitzung B - [24 x 80]
Datei Bearbeiten Anzeige Kommunikation Aktionen Fenster Hilfe
Finish i-effect subsystems (ENDEFFSBS)

Type choices, press Enter.

Subsystem . . . . . *OCSP *ALL, *AS2, *IEFFECT...
+ for more values
Controlled end delay time . . . *NOLIMIT Number, *NOLIMIT

F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display
F24=More keys
Bottom
  
```

Entering **"\*OCSP"** and confirming with the **"enter key"** shuts down the i-effect® \*OCSP subsystem.

2. Direct shutdown of the subsystems

```

Sitzung B - [24 x 80]
Datei Bearbeiten Anzeige Kommunikation Aktionen Fenster Hilfe
IEFFECT i-effect - The integrated solution for IBM System i
System: DEVELOP

Options:
  53. Work with EDI communication resources

Administration:
  80. Work with program modules
  81. Work with logbook

  83. Reorganize logbook content

  85. Start i-effect subsystems
  86. End i-effect subsystems

Selection or command
==> endsbs EFFOCSP

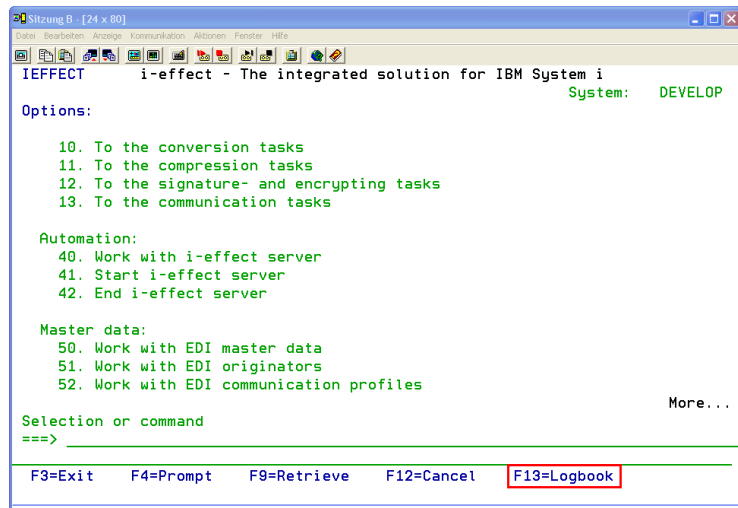
F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Logbook
Bottom
  
```

The i-effect® \*OCSP subsystem can also be directly shutdown using the **"ENDSBS"** command and the subsystem **"EFFOCSP"** as its parameter.

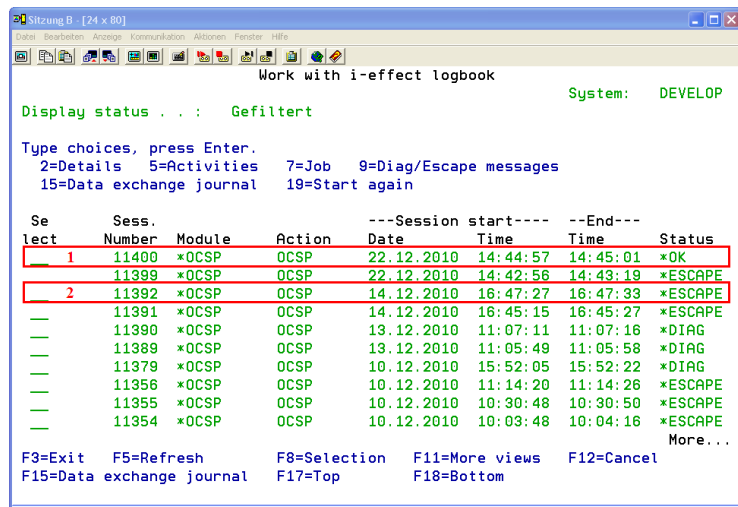
## System Monitoring

### Job Logging in i-effect®

The individuals processing steps of commands in use can be recorded and followed in the i-effect® Logbook. Every registered command (or a command chain using \*SERVER) has its own session number under which all logging entries are saved within the logbook.



Use the **Function Key <F13>** to reach the logbook from the i-effect® menu.

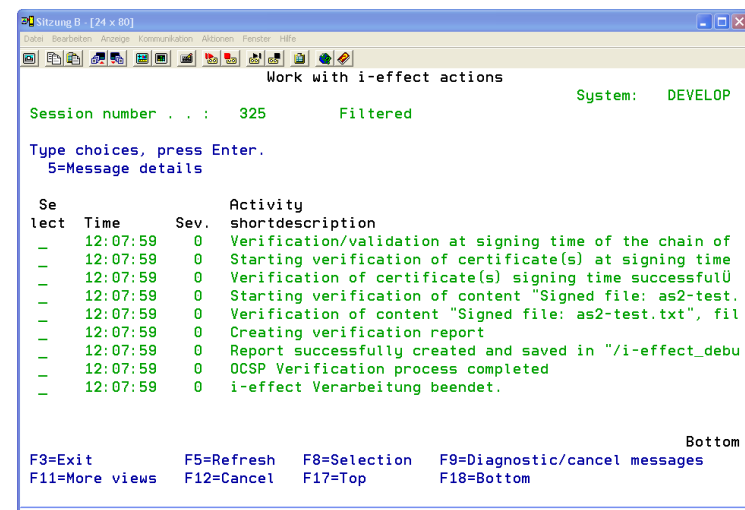
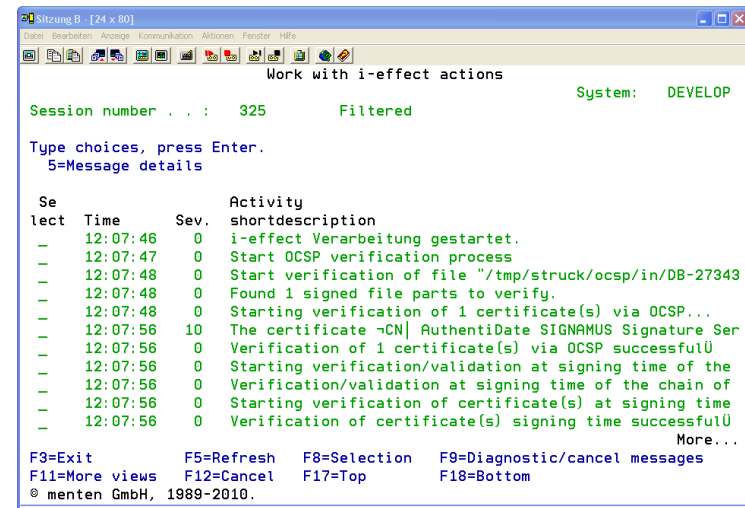


The first page of the logbook will be displayed. Using the **<PAGE-UP>** or **<PAGE-DOWN>**-keys will page through the logbook.

In the status column of the logbook, the current processing status or the status in which the command ended can be seen.

With \*OCSP, verification can basically only be ended with a correct **(1)** or an error **(2)** result.

To display the details of a finished verification job, move the cursor by using the arrow keys to the desired entry. Enter **Option 5** and press enter to reach the detail view (Here \*OK):



The detail view displays over two pages of processing steps that the verification job generated. Using **Option 5** will display the individual processing steps completely.

The report of a successful verification lists the details in the area called **"Test Results"** of the results of the individual processing steps:

Test Results	
File's Signature Test	*OK
Certificate Test incl. Path at Time of Signature	*OK
Certificate Status at Time of Signature	*OK
OCSP-Certificate Status at signing time	*OK
Qualified Certificate	*OK
<b>Total Results</b>	<b>*OK</b>

If an error occurred at least one of the steps will have an error status:

Work with i-effect actions		System:
Session number . . . :	325	DEVELOP
	Filtered	
Type choices, press Enter.		
5=Message details		
Se	Activitu	

With a message severity of 40, the error status and the text description will be displayed and the entire processing will be set to \*ABORT.

In the case displayed here, the certificate could not be verified by OCSP. In this case, the processing will not be stopped, but rather verification of the signed file will be continued.

Test Results	
File's Signature Test	*OK
Certificate Test incl. Path at Time of Signature	*OK
Certificate Status at Time of Signature	*OK
OCSP-Certificate Status at signing time	*OK
Qualified Certificate	*FAILED
<b>Total Results</b>	<b>*FAILED</b>

The result created a test report that is displayed in the **"Test Result"** area, and contains a detailed list of which processing steps were completed successfully and which were not.

Test Results	
File's Signature Test	*FAILED
Certificate Test incl. Path at Time of Signature	*OK
Certificate Status at Time of Signature	*OK
OCSP-Certificate Status at signing time	*OK
Qualified Certificate	*FAILED
<b>Total Results</b>	<b>*FAILED</b>

In this example of a failed test, the verification of the signed data shows a manipulation of the original document.

\*DIAGNOSE is an additional status, in conjunction with test report creation.

Work with i-effect logbook		System:		
Display status . . . :		DEVELOP		
Type choices, press Enter.				
2=Details 5=Activities 7=Job 9=Diag/Escape messages				
15=Data exchange journal 19=Start again				
Se	Sess.	---Session start---	---End---	Status
lect	Number	Date	Time	Time
---	11400	*OCSP	OCSP	22.12.2010 14:44:57 14:45:01 *OK
---	11399	*OCSP	OCSP	22.12.2010 14:42:56 14:43:19 *ESCAPE
---	11392	*OCSP	OCSP	14.12.2010 16:47:27 16:47:33 *ESCAPE
---	11391	*OCSP	OCSP	14.12.2010 16:45:15 16:45:27 *ESCAPE
---	11390	*OCSP	OCSP	13.12.2010 11:07:11 11:07:16 *DIAG
---	11389	*OCSP	OCSP	13.12.2010 11:05:49 11:05:58 *DIAG
---	11379	*OCSP	OCSP	10.12.2010 15:52:05 15:52:22 *DIAG
---	11356	*OCSP	OCSP	10.12.2010 11:14:20 11:14:26 *ESCAPE
---	11355	*OCSP	OCSP	10.12.2010 10:30:48 10:30:50 *ESCAPE
---	11354	*OCSP	OCSP	10.12.2010 10:03:48 10:04:16 *ESCAPE
More...				
F3=Exit		F5=Refresh		F8=Selection
F15=Data exchange journal		F17=Top		F11=More views
		F18=Bottom		F12=Cancel

\*DIAGNOSE generally means that verification was successfully completed. However, verification indicated, that either the hash-algorithm or the RSA key length (or both) are (were) no longer adequately secure at the time of verification (more information can be found at the German Federal Network Agency's website) Link: [http://www.bundesnetzagentur.de/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen\\_node.html](http://www.bundesnetzagentur.de/DE/Sachgebiete/QES/Veroeffentlichungen/Algorithmen/algorithmen_node.html).

The report will also contain a marker regarding the algorithm verification status:

Signature Details	
Signature Description	PDF-Signatur Signature-Bez.: Unterschrift Revision der PDF: 1
Signature Algorithm	RSA (2048) with SHA-1
Signature Time	2007-12-11T13:06:42.000+0100
Content's Hash Value (SHA-1)	1B 48 7C A1 EB C1 91 22 9D CC 54 FF 66 E9 8F 0E 0A C4 03 E1
Attribute Hash Value (SignedData) (SHA-1)	D1 54 45 FC E6 D5 85 E0 A7 40 18 D5 F6 5E A8 A1 E8 D5 DC BE
Signature Hash Value (SHA-1)	D1 54 45 FC E6 D5 85 E0 A7 40 18 D5 F6 5E A8 A1 E8 D5 DC BE
State of the signatures hash algorithm:	The hash algorithm SHA-1 at verification time is considered as not sufficiently secure since 2008-08-01.

## Logging in the 'internal'-Directory of i-effect®

In the **„internal“**-directory of an i-effect®-Installation detailed information regarding the processes of individual i-effect® modules are logged, which helps find and correct possible problems.

The log file for the \*OCSP module will be generated using the pattern **"yearmonthday-ocsp.log"**.

This logging is an expansion of the i-effect® logbook and records further information that was generated by the i-effect \*OCSP-Subsystem.

## Update of i-effect® \*OCSP

To install a new version of i-effect® \*OCSP, i-effect® – the integrated solution for IBM System i – must be updated.

After which, the integrity of the i-effect® \*OCSP program file must be tested (see „*Installation*“).