

Kapitel 8a

Verschlüsselung & fortgeschrittene elektronische Signatur

Dieses Kapitel informiert Sie über die Konfiguration sowie verschiedenen Funktionen des *CRYPT Moduls in i-effect®. Entsprechend der möglichen Funktionen unterteilt sich das Kapitel in die Teile „**Signieren/Verifizieren von PDF's**“, „**Verschlüsselung/Entschlüsselung von Dateien**“ und „**Dateien qualifiziert signieren**“.

Um zu den Signatur- und Verschlüsselungsaufgaben zu gelangen geben Sie bitte die Auswahlziffer „12“ im i-effect® Hauptmenü ein. Diese Auswahl verzweigt in ein Menü, in dem alle Aufgaben des *CRYPT Moduls zusammengefasst sind. Von dort aus können die entsprechenden Funktionen ausgeführt werden.

Hier einige Definitionen zum Thema:

Keystore

Ein Keystore ist eine geschützte Datenbank, die Schlüssel und Zertifikate beinhaltet.

Der Zugriff auf den Keystore erfolgt über ein Passwort, das beim Anlegen eines neuen Keystore von der Person, die ihn erstellt, vergeben werden muss. Ein bereits vergebenes Passwort kann nur geändert werden, wenn es zuvor zur Authentifizierung eingegeben worden ist.

Schlüssel

Ein Schlüssel ist eine Zeichenkette von Bits, die in der Kryptographie Verwendung findet. Ein Schlüssel erlaubt es, Daten zu verschlüsseln, entschlüsseln sowie andere mathematische Operationen durchzuführen.

Private/Public Schlüsselpaar	<p>Ein Public/Private Schlüsselpaar ist eine mathematisch verwandte Zusammenstellung von zwei Zeichenketten, bei denen die eine „Privater Schlüssel“ und die andere „Öffentlicher Schlüssel“ genannt wird. Der öffentliche Schlüssel ist dabei der Teil des Schlüsselpaares, der typischer Weise allen Partnern zugänglich gemacht wird, mit denen man verschlüsselte Kommunikation betreiben will. Der private Schlüssel ist dagegen der sensible Teil des Schlüsselpaares und sollte nur für seinen Besitzer zugänglich sein.</p> <p>Daten, die mit einem öffentlichen Schlüssel verschlüsselt worden sind, können ausschließlich mit dem zum öffentlichen Schlüssel zugehörigen privaten Schlüssel entschlüsselt werden. Die Umkehrung gilt hier ebenfalls. Daten, die mit einem öffentlichen Schlüssel verschlüsselt worden sind, können nicht wieder mit dem gleichen öffentlichen Schlüssel entschlüsselt werden.</p>
Privater Schlüssel	<p>Unter geheimen Schlüsseln (private key) versteht man in asymmetrischen Kryptosystemen solche Schlüssel, die nur denjenigen bekannt sein dürfen, denen sie gehören. In symmetrischen Kryptosystemen ist ein solcher Schlüssel den vertrauten Kommunikationspartnern bekannt.</p>
Öffentlicher Schlüssel	<p>Unter einem öffentlichen Schlüssel (public key) versteht man in Kryptosystemen Schlüssel, die jedem bekannt sein dürfen und zur Verschlüsselung eines Klartextes in einen Geheimtext genutzt werden können, der für den Eigner des korrespondierenden geheimen Schlüssels bestimmt ist.</p>
Symmetrisches Kryptosystem	<p>Ein symmetrisches Kryptosystem ist ein Kryptosystem, das im Gegensatz zu einem asymmetrischen Kryptosystem denselben Schlüssel für Ver- und Entschlüsselung verwendet.</p>
Asymmetrisches Kryptosystem	<p>Ein asymmetrisches Kryptosystem ist ein Kryptosystem, das im Gegensatz zum symmetrischen Kryptosystem verschiedene Schlüssel zur Ver- und Entschlüsselung verwendet, nämlich den öffentlichen und den privaten Schlüssel.</p>

Zertifikat	<p>In einem asymmetrischen Kryptosystem dient ein Zertifikat dem Nachweis, dass ein öffentlicher Schlüssel zu der angegebenen Person, Institution oder Maschine gehört. Dadurch können Authentizität, Vertraulichkeit und Integrität von Daten gegenüber Dritten garantiert werden.</p> <p>Ein Zertifikat enthält Informationen über den Namen des Inhabers, dessen öffentlichen Schlüssel, eine Seriennummer, die Gültigkeitsdauer und den Namen der Zertifizierungsstelle. Diese Daten sind in der Regel mit dem privaten Schlüssel der Zertifizierungsstelle signiert und können somit mit dem öffentlichen Schlüssel der Zertifizierungsstelle überprüft werden. Zertifikate für Schlüssel, die nicht mehr sicher sind, können über eine sogenannte Certificate Revocation List gesperrt werden.</p>
Zertifikatskette (certificate chain)	<p>Eine Zertifikatskette ist die Liste der Zertifikate vom Benutzerzertifikat bis hin zum Wurzel-Zertifikat (root-Certificate) einer CA (Certificate Authority). Mit der Prüfung der Zertifikatskette wird sichergestellt, dass ein Zertifikat von der jeweiligen Zertifizierungsstelle ausgestellt wurde und damit die Identität des Benutzers gesichert ist.</p>
Certificate Authority (CA)	<p>Eine Zertifizierungsstelle (engl. Certificate Authority, kurz CA) ist eine Organisation, die digitale Zertifikate herausgibt. Ein digitales Zertifikat ist das elektronische Äquivalent eines Personalausweises und dient dazu, einen bestimmten öffentlichen Schlüssel einer Person oder Organisation zuzuordnen. Diese Zuordnung wird von der Zertifizierungsstelle beglaubigt, indem sie diese mit ihrer eigenen digitalen Unterschrift versieht. Die Zertifikate enthalten „Schlüssel“ und Zusatzinformationen, die zur Authentifizierung sowie zur Verschlüsselung und Entschlüsselung sensibler oder vertraulicher Daten dienen, die über das Internet und andere Netze verbreitet werden. Als Zusatzinformationen sind zum Beispiel Lebensdauer, Verweise auf Sperrlisten, etc. enthalten, die durch die CA mit in das Zertifikat eingebracht werden.</p>

Standardkeystore von i-effect®

Den mitgelieferten Standard-Keystore von i-effect® finden Sie nach der erfolgreichen Installation im Verzeichnis `/i-effect/<version>/crypt` unter dem Namen `certificates.p12` (VERSION entspricht hierbei der von Ihnen installierten i-effect® Version, z.B. v1r4m0). Das Standardkennwort des Keystores lautet „**ieffect**“.

Es wird empfohlen dieses Kennwort vor der ersten Verwendung des Keystores zu ändern. Dazu können Sie das mitgelieferte Tool „**i-effectKeyManager**“ verwenden.

Das Tool befindet sich in Verzeichnis

`/i-effect/<version>/CRYPT/tools/i-effectKeyManager.jar`

Es bietet alle Funktionen zum Im- und Export von Schlüsseln und Zertifikaten, sowie weitere im Zusammenhang mit dem Keystore nützliche Funktionen.

Die genaue Verwendung des i-effectKeyManagers wird in Kapitel 14 „**Graphische Zusatzanwendungen**“ erklärt.

Grundkonfiguration des CRYPT Moduls

Die Grundkonfiguration des CRYPT Moduls entnehmen Sie bitte Kapitel 12 „**Verwaltung in i-effect®**“. Der dortige Unterpunkt „Erweiterte Parameter zum Modul *CRYPT“ erklärt die Grundeinstellungen für das CRYPT Modul.

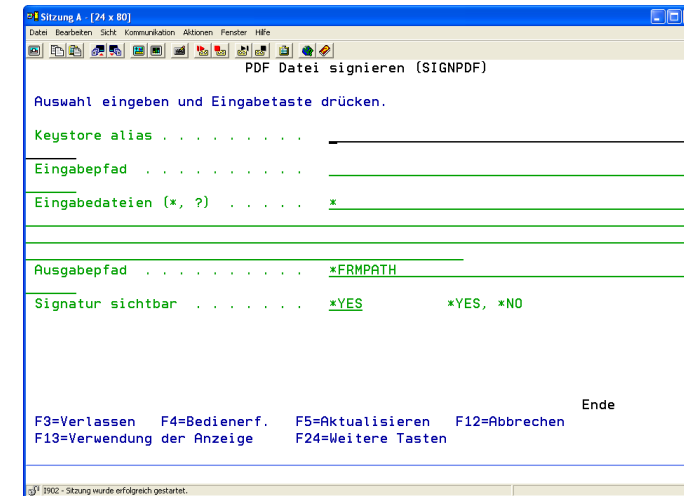
PDF Datei signieren (SIGNPDF)

Der Befehl **SIGNPDF** dient dazu beliebige PDF Dateien zu signieren. Dies können bereits vorhandene PDF Dokumente sein, oder solche, die mit i-effect® aus einer IBM Power Systems Spooldatei erzeugt wurden. Der Befehl verwendet die im *CRYPT Modul vorhandenen Funktionen zur Errechnung einer fortgeschrittenen elektronischen Signatur. Zur Anwendung dieses Befehls benötigen Sie die i-effect® Module *BASE und *CRYPT.

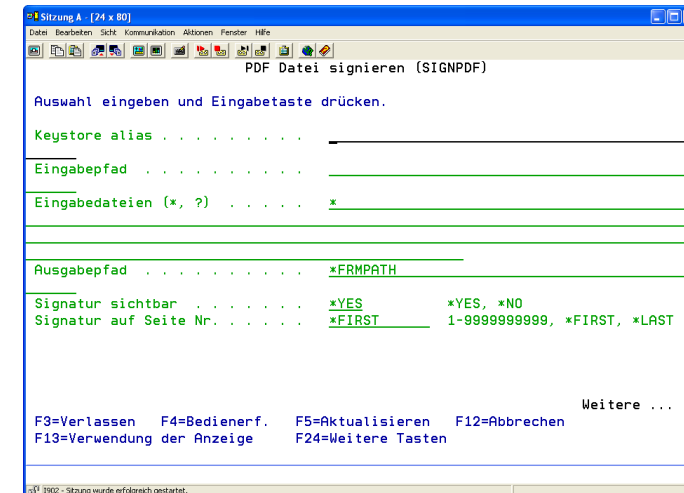
In das Menü für die Signatur von PDF Dateien gelangen Sie, indem Sie im i-effect® Menü Auswahl 12 aufrufen und danach **Menüpunkt 1 „PDF Datei(en) signieren“**.

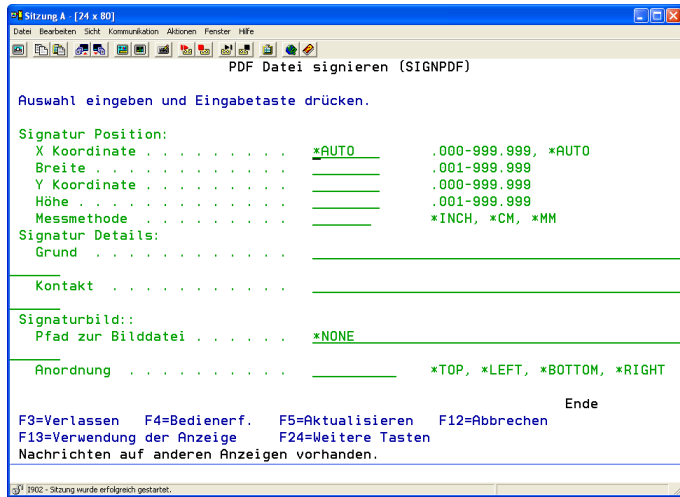
Alternativ dazu können Sie auch direkt im i-effect® Menü den Befehl „**SIGNPDF**“ gefolgt von **F4** eingeben.

Folgendes Dialogprogramm wird angezeigt:



Die möglichen Parameter für die Signatur von PDF Dateien verteilen sich auf zwei Seiten. Um alle verfügbaren Parameter anzuzeigen drücken Sie bitte **F9**. Mittels den Tasten Bild-auf und Bild-ab können Sie zwischen den zwei Seiten des Menü wechseln und die benötigten Werte eintragen.





Erläuterung der Parameter:

Keystore Alias (ALIAS)

Der Alias im i-effect® Keystore, der zur Erstellung der Signatur verwendet werden soll. Unter dem Alias muss im Keystore ein privater Schlüssel abgelegt sein.

Eingabepfad (FRMPATH)

Angabe des Pfades im IFS Dateisystem, aus dem PDF Dateien für die Erstellung einer digitalen Signatur gelesen werden sollen.

Eingabedatei(en) (FRMIFSDATE)

Angabe der aus dem im Parameter FRMPATH angegebene Pfad zu lesenden PDF Dokumente. Durch Verwendung der Wildcard Symbole „*“ und „?“ können eine beliebige, dem Suchmuster entsprechende Anzahl an Dateien für die Verarbeitung ausgewählt werden.

*	Alle Dateien des ausgewählten Verzeichnis werden verarbeitet.
generisch*	Sie können mit einem Stern (*) einen Teil eines Dateinamens ersetzen. Geben Sie nur den ersten Teil des Namens, gefolgt von (*) ein, um eine Liste aller Dateien zu erhalten, deren Name mit diesem ersten Wortteil beginnt.

Für generische Namen sind folgende Formate möglich:

ABC*	Alle Dateien werden verarbeitet, deren Namen mit den Zeichen ABC beginnen, z.B. ABC, ABCD oder ABCTEST.
a*	Alle Dateien werden verarbeitet, deren Namen in Anführungszeichen eingeschlossen sind und mit a beginnen, z.B. „a“, „aB“, „aD“.
*.pdf	Alle Dateien werden verarbeitet, deren Namensendung „.pdf“ lauten.

Ausgabepfad (TOPATH)

Name des Ausgabepfades für die signierten PDF Dokumente. Die Dateinamen entsprechen der Originaldateiname aus dem gelesenen Eingabepfad. Sollten Dateien unter dem Namen im Zielverzeichnis bereits existieren, so werden die Namen durch Anhängen einer Namensendung (Zahl) eindeutig gehalten.

Signatur sichtbar (VISIBLE)

Die im PDF eingebettete Signatur kann durch ein visuelles Abbild, z.B. die Grafik einer Unterschrift, visualisiert werden. Hier wird bestimmt, ob ein solches visuelles Abbild in die PDF Datei eingebettet werden soll.

*YES	Die Signatur wird im PDF Dokument visualisiert.
*NO	Die Signatur ist zwar im PDF Dokument enthalten, es wird jedoch kein visuelles Abbild erzeugt.

Signatur auf Seite Nr. (SIGPAGE)

Im Falle der Einbettung eines visuellen Abbildes der erzeugten Signatur kann bestimmt werden, auf welcher Seite diese Signatur angezeigt werden soll.

*FIRST	Das visuelle Abbild wird auf der ersten Seite des PDF Dokuments eingefügt.
*LAST	Das visuelle Abbild wird auf der letzten Seite des PDF Dokuments eingefügt.
1-999999999	Das visuelle Abbild wird auf der angegebenen Seite eingefügt.

(POSITION)

Der POSITION Parameter (Signatur Position) erscheint nur, wenn VISIBLE(*YES) ausgewählt wurde.

Dieser Parameter ermöglicht Ihnen die Position festzulegen, an der die Signatur im PDF Dokument visualisiert werden soll. Die Angabe erfolgt durch Festlegung von Koordinaten, und zwar die Seite herunter von oben nach unten und von links nach rechts.

Beispiel:

```
SIGNPDF      ALIAS(,as2.menten.com')
             FRMPATH(,/tmp')
             FRMIFSFILE(*.pdf')
             TOPATH(*FRMPATH)
             VISIBLE(*YES)
             SIGPAGE(*FIRST)
             POSITION(0 100 0 100 *MM)
```

Hier wird mit dem Zertifikat von „as2.menten.com“ eine digitale Signatur für alle PDF Dateien im Verzeichnis „/tmp“ erstellt. Ein visuelles Abbild der Signatur erscheint auf der ersten Seite links oben in der Größe 100x100 mm.

Es gibt fünf Elemente zu diesem Parameter.

X Koordinate

Das erste Element ist die Spaltenposition oder X-Koordinate, d.h. die Position von linken Seitenrand an, wo das Abbild der Signatur positioniert werden soll. Es wird angegeben entweder in Zoll, Millimeter oder Zentimeter abhängig von Wert der Messmethoden-Option (beachten Sie unten das fünfte Element).

Breite

Das zweite Element ist die Breite des visuellen Signaturbereichs. Es wird angegeben entweder in Zoll, Millimeter oder Zentimeter abhängig von Wert der Messmethoden-Option (beachten Sie unten das fünfte Element).

Y Koordinate

Das dritte Element ist die Zeilennummer bzw. y-Koordinate, d.h. die Position auf der Seite von oben herab gemessen, wo das Abbild der Signatur positioniert werden soll. Es wird angegeben entweder in Zoll, Millimeter oder Zentimeter abhängig von Wert der Messmethoden-Option (beachten Sie unten das fünfte Element).

Höhe

Das vierte Element ist die Höhe des visuellen Signaturbereichs. Es wird angegeben entweder in Zoll, Millimeter oder Zentimeter abhängig von Wert der Messmethoden-Option (beachten Sie unten das fünfte Element).

Messmethode

Das fünfte Element ist die Messmethode und gibt die Einheiten an, in denen die vier vorhergehenden Elemente angegeben werden.

Möglich sind folgende Sonderwerte:

*INCH	Die vertikale und horizontale Position so wie die Länge oder Breite werden in Zoll angegeben.
*MM	Die vertikale und horizontale Position so wie die Länge oder Breite werden in Millimeter angegeben.
*CM	Die vertikale und horizontale Position so wie die Länge oder Breite werden in Zentimeter angegeben.

Signatur Details (DETAILS)

Zusammen mit der Signatur können in die PDF Datei weitere Angaben eingebunden werden, die der Empfänger beim Anzeigen der Details zur Signatur angezeigt bekommt.

Der Parameter besteht aus zwei Elementen**Grund**

Das erste Element erlaubt die Angabe eines Grundes zur Signaturerstellung. Dies kann eine beliebige Zeichenfolge sein, die bei der Anzeige der Signaturdetails im Feld „Grund“ wiedergegeben wird.

Kontakt

Das zweite Element erlaubt die Angabe eine Kontaktinformation. Dies kann eine beliebige Zeichenfolge sein, die bei der Anzeige der Signaturdetails im Feld „Kontakt“ wiedergegeben wird.

Signaturgrafik (PICTURE)

Zusammen mit der Signatur kann auch eine Grafik in die PDF Datei eingebunden werden, die der Empfänger bei Ansicht der PDF-Datei angezeigt bekommt. Diese Grafik kann z. B. eine persönliche Unterschrift oder auch ein Passbild sein.

Möglich sind folgende Sonderwerte:

*NONE	Es wird keine Grafikdatei eingebunden.
--------------	--

Der Parameter besteht aus zwei Elementen**Pfad zur Bilddatei.**

Geben Sie hier den vollständigen IFS-Pfad zur Grafikdatei an.

Anordnung

Geben Sie hier die Stelle an, an der die Grafik im Signaturfeld erscheinen soll.

Mögliche Sonderwerte:

*TOP	Die Grafik erscheint oben im Signaturfeld (und die Signatur darunter).
*LEFT	Die Grafik erscheint links im Signaturfeld (und die Signatur rechts).
*BOTTOM	Die Grafik erscheint unten im Signaturfeld (und die Signatur darüber).
*RIGHT	Die Grafik erscheint rechts im Signaturfeld (und die Signatur links).

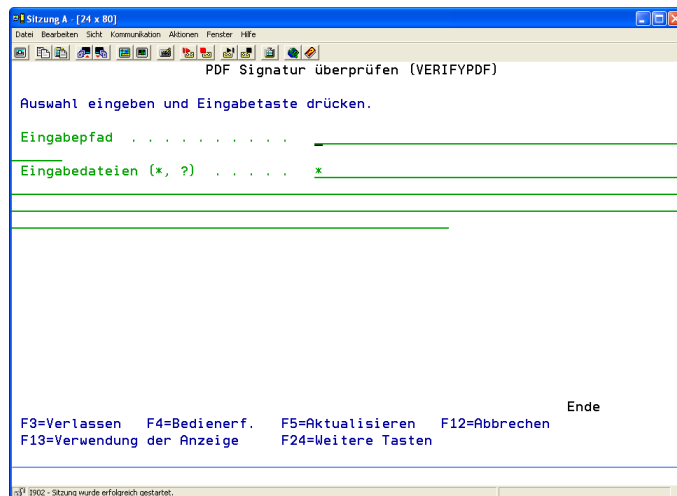
PDF Signatur prüfen (VERIFYPDF)

Der Befehl **VERIFYPDF** dient dazu, beliebige signierte PDF Dateien zu überprüfen. Dazu werden die in den PDF Dateien vorhandenen elektronischen Signaturen gegen die im i-effect® Keystore abgelegten öffentlichen Schlüssel geprüft. Ist ein Eintrag im Keystore vorhanden, und konnte die Signatur erfolgreich überprüft werden ist damit sichergestellt, dass sowohl die Authentizität als auch die Integrität des Dokuments gewährleistet ist.

Zur Verwendung dieses Befehls sind Lizenzen der i-effect® Module *BASE und *CRYPT notwendig.

In das Menü für die Verifizierung von PDF Dateien gelangen Sie, indem Sie im i-effect® Menü **Auswahl 12** aufrufen und danach **Menüpunkt 2 „PDF Datei(en) verifizieren“**.

Alternativ dazu können Sie auch direkt im i-effect® Menü den Befehl „**VERIFYPDF**“ gefolgt von **F4** eingeben.

Folgendes Dialogprogramm wird angezeigt.**Erläuterung der Parameter:****Eingabepfad (FRMPATH)**

Angabe des Pfades im IFS Dateisystem, aus dem PDF Dateien für die Überprüfung der digitalen Signatur gelesen werden sollen.

Eingabedatei(en) (FRMIFSFIL)

Angabe der aus dem im Parameter FRMPATH angegebene Pfad zu lesenden PDF Dokumente. Durch Verwendung der Wildcard Symbole „*“ und „?“ können eine beliebige, dem Suchmuster entsprechende Anzahl an Dateien für die Verarbeitung ausgewählt werden.

*	Alle Dateien des ausgewählten Verzeichnis werden verarbeitet.
generisch*	Sie können mit einem Stern (*) einen Teil eines Dateinamens ersetzen. Geben Sie nur den ersten Teil des Namens, gefolgt von (*) ein, um eine Liste aller Dateien zu erhalten, deren Name mit diesem ersten Wortteil beginnt.

Für generische Namen sind folgende Formate möglich:

ABC*	Alle Dateien werden verarbeitet, deren Namen mit den Zeichen ABC beginnen, z.B. ABC, ABCD oder ABCTEST.
a*	Alle Dateien werden verarbeitet, deren Namen in Anführungszeichen eingeschlossen sind und mit a beginnen, z.B. „a“, „aB“, „aD“.
*.pdf	Alle Dateien werden verarbeitet, deren Namenserweiterung „pdf“ lauten.

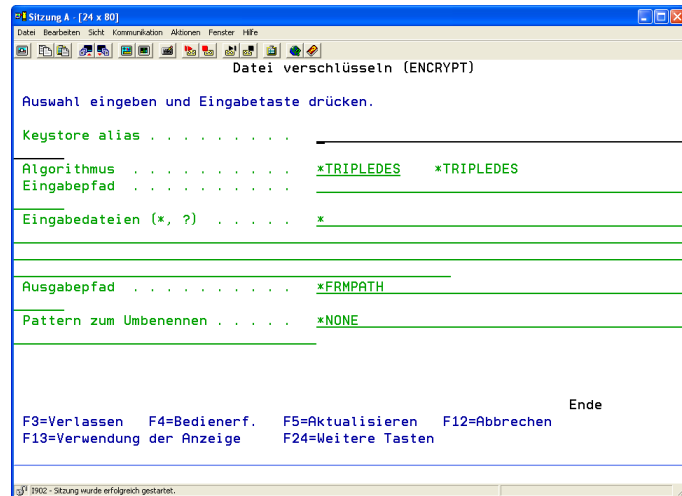
Datei verschlüsseln (ENCRYPT)

Der Befehl **ENCRYPT** dient dazu beliebige Dateien zu verschlüsseln. Dabei werden die im i-effect® System innerhalb des *CRYPT Moduls vorhandenen Funktionen zum Verschlüsseln mit Hilfe einer PKI Infrastruktur verwendet. Das Ergebnis dieses Vorgangs ist eine vom System erstellte Ausgabedatei, die im Standard PK7 Format bereit gestellt wird. Diese kann zum einen von beliebigen PKI Systemen wieder entschlüsselt werden, und stellt zum anderen einen Standardisierten Weg der Darstellung verschlüsselter Inhalte dar. Voraussetzung für die Nutzung dieser Funktionen ist, dass im i-effect® Keystore der öffentliche Schlüssel des Empfängers hinterlegt ist, und der Alias dieses Schlüsseleintrags bekannt ist. Zur Anwendung dieses Befehls werden die i-effect® Module *BASE und *CRYPT benötigt.

In das Menü für die Verschlüsselung von Dateien gelangen Sie, indem Sie im i-effect® Menü **Auswahl 12** aufrufen und danach **Menüpunkt 4 „Datei(en) verschlüsseln“**.

Alternativ dazu können Sie auch direkt im i-effect® Menü den Befehl „**ENCRYPT**“ gefolgt von **F4** eingeben.

Folgendes Dialogprogramm wird angezeigt.



Erläuterung der Parameter;

Keystore Alias (ALIAS)

Der Alias im i-effect® Keystore, der zur Verschlüsselung der Daten der Eingabedatei verwendet werden soll. Unter dem Alias muss im Keystore ein öffentlicher Schlüssel (Zertifikat) abgelegt sein.

Algorithmus der Verschlüsselung (ENCRYPT)

Mit diesem Parameter kann angegeben werden, welche Art der Verschlüsselung für die angegebene Eingabedatei angewendet werden soll.

***TRIPLEDES** 3DES Verschlüsselung

Der Data Encryption Standard (Abkürzung:DES) ist ein weit verbreiteter symmetrischer Verschlüsselungsalgorithmus. Die Schlüssellänge von 3DES ist mit 168 Bit drei mal so groß wie bei DES (56 Bit), wodurch die Schlüsselkomplexität um den Faktor 2^{112} gesteigert wird.

Eingabepfad (FRMPATH)

Angabe des Pfades im IFS Dateisystem, aus dem Dateien für die Verschlüsselung gelesen werden sollen.

Eingabedatei(en) (FRMIFSFIL)

Angabe der aus dem im Parameter FRMPATH angegebene Pfad zu lesenden Dateien. Durch Verwendung der Wildcard Symbole „*“ und „?“ können eine beliebige, dem Suchmuster entsprechende Anzahl an Dateien für die Verarbeitung ausgewählt werden.

* Alle Dateien des ausgewählten Verzeichnis werden verarbeitet

generisch*

Sie können mit einem Stern (*) einen Teil eines Dateinamens ersetzen. Geben Sie nur den ersten Teil des Namens, gefolgt von (*) ein, um eine Liste aller Dateien zu erhalten, deren Name mit diesem ersten Wortteil beginnt.

Für generische Namen sind folgende Formate möglich:

ABC*	Alle Dateien werden verarbeitet, deren Namen mit den Zeichen ABC beginnen, z.B. ABC, ABCD oder ABCTEST
a*	Alle Dateien werden verarbeitet, deren Namen in Anführungszeichen eingeschlossen sind und mit a beginnen, z.B. „a“, „aB“, „aD“
*.pdf	Alle Dateien werden verarbeitet, deren Namensweiterung „pdf“ lauten

Ausgabepfad (TOPATH)

Name des Ausgabepfades für die verschlüsselten Dateien. Die Dateinamen entsprechen dem Originaldateinamen aus dem gelesenen Eingabepfad. Zusätzlich wird an den Namen die Endung „.pk7“ angehängt. Sollten Dateien unter dem Namen im Zielverzeichnis bereits existieren, so werden die Namen durch Anhängen einer Namensweiterung (Zahl) eindeutig gehalten.

Neuer Name zum Umbenennen (RENAME)

Geben Sie hier an, ob die erstellten verschlüsselten Dateien umbenannt werden sollen sowie ggf einen neuen Namen bzw. Namensmuster. Mit diesem Parameter kann flexibel die Standardvorgabe der Benennung von verschlüsselten Dateien verändert werden.

Folgende Optionen stehen zur Auswahl:

***NONE** Die verschlüsselten Dateien werden nicht umbenannt. Sie erhalten einen Namen, der aus dem Namen der Originaldatei plus angehängter neuer Erweiterung (pk7) gebildet wird.

Name

Hier kann ein neuer Name oder ein Namens-Muster angegeben werden. Das Namensmuster enthält jeweils einen „*“ als Platzhalter für den Original Dateinamen VOR der Erweiterung, und einen weiteren „*“ für die Erweiterung im Originaldateinamen.

Z.B. :

***.DONE** macht aus „file1.txt“ „file1.DONE“
_DONE. macht aus „file1.txt“ „file1_DONE.txt“
***_1055am** macht aus „file1.txt“ „file1.txt_1055am“

Datei entschlüsseln (DECRYPT)

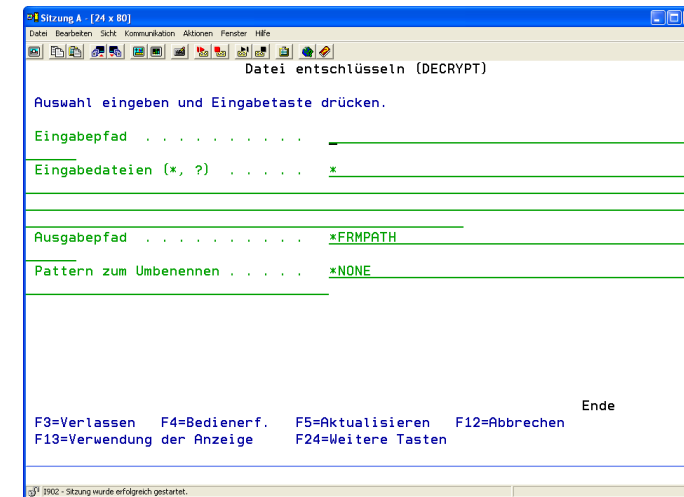
Der Befehl **DECRYPT** dient dazu beliebige Dateien zu entschlüsseln. Dabei werden die im i-effect® System innerhalb des *CRYPT Moduls vorhandenen Funktionen zum Entschlüsseln mit Hilfe einer PKI Infrastruktur verwendet. Das Ergebnis dieses Vorgangs ist eine vom System erstellte Ausgabedatei, die, sofern entsprechende Schlüssel im Keystore gefunden wurden, nach der Entschlüsselung wieder die Originaldaten enthält.

Voraussetzung für die Nutzung dieser Funktionen ist, dass im i-effect® Keystore der private Schlüssel hinterlegt ist, der zu dem öffentlichen Schlüssel passt, mit dem die Daten verschlüsselt wurde. Zur Anwendung dieses Befehls werden Lizenzen der i-effect® Module *BASE und *CRYPT benötigt.

In das Menü für die Verschlüsselung von Dateien gelangen Sie, indem Sie im i-effect® Menü **Auswahl 12** aufrufen und danach **Menüpunkt 5 „Datei(en) entschlüsseln“**.

Alternativ dazu können Sie auch direkt im i-effect® Menü den Befehl „**DECRYPT**“ gefolgt von **F4** eingeben.

Folgendes Dialogprogramm wird angezeigt.



Erläuterung der Parameter:

Eingabepfad (FRMPATH)

Angabe des Pfades im IFS Dateisystem, aus dem verschlüsselten Dateien für die Entschlüsselung gelesen werden sollen.

Eingabedatei(en) (FRMIFSFILE)

Angabe der aus dem im Parameter FRMPATH angegebenen Pfad zu lesenden Dateien. Durch Verwendung der Wildcard Symbole „*“ und „?“ können eine beliebige, dem Suchmuster entsprechende Anzahl an Dateien für die Verarbeitung ausgewählt werden.

* Alle Dateien des ausgewählten Verzeichnis werden verarbeitet

generisch*

Sie können mit einem Stern (*) einen Teil eines Dateinamens ersetzen. Geben Sie nur den ersten Teil des Namens, gefolgt von (*) ein, um eine Liste aller Dateien zu erhalten, deren Name mit diesem ersten Wortteil beginnt.

Für generische Namen sind folgende Formate möglich:

ABC* Alle Dateien werden verarbeitet, deren Namen mit den Zeichen ABC beginnen, z.B. ABC, ABCD oder ABCTEST
a* Alle Dateien werden verarbeitet, deren Namen in Anführungszeichen eingeschlossen sind und mit a beginnen, z.B. „a“, „aB“, „aD“
***.pdf** Alle Dateien werden verarbeitet, deren Namensendung „pdf“ lauten

Ausgabepfad (TOPATH)

Name des Ausgabepfades für die entschlüsselten Dateien. Die Dateinamen entsprechen dem Originaldateinamen aus dem gelesenen Eingabepfad. Zusätzlich wird eine eventuell vorhandene Endung „.pk7“ entfernt. Sollten Dateien unter dem Namen im Zielverzeichnis bereits existieren, so werden die Namen durch Anhängen einer Namens-erweiterung (Zahl) eindeutig gehalten.

Neuer Name zum Umbenennen (RENAME)

Geben Sie hier an, ob die erstellten entschlüsselten Dateien umbenannt werden sollen sowie ggf einen neuen Namen bzw. Namensmuster.

Mit diesem Parameter kann flexibel die Standardvorgabe der Benennung von entschlüsselten Dateien verändert werden.

Folgende Optionen stehen zur Auswahl:

*NONE	Die entschlüsselten Dateien werden nicht umbenannt. Ihr Name wird aus dem Namen der Originaldatei gebildet. Sollte bei der Verschlüsselung die Erweiterung „pk7“ angehängt worden sein, so wird sie hier abgeschnitten
--------------	--

Name

Hier kann ein neuer Name oder ein Namens-Muster angegeben werden. Das Namensmuster enthält jeweils einen „*“ als Platzhalter für den Original Dateinamen VOR der Erweiterung, und einen weiteren „*“ für die Erweiterung im Originaldateinamen.

Z.B. :

*.DONE	macht aus „file1.txt“ „file1.DONE“
_DONE.	macht aus „file1.txt“ „file1_DONE.txt“
*_1055am	macht aus „file1.txt“ „file1.txt_1055am“

Allgemeine Befehle & Werkzeuge

In diesem Abschnitt werden allgemeine Befehle und Werkzeuge, die für das *CRYPT Module zur Verfügung stehen, erläutert.

Keystore Tools

Bei den Keystore Tools handelt es sich um zusätzliche JAVA Programme für den i-effect® Keystore. Sie befinden sich im Verzeichnis `/i-effect/<version>/CRYPT/tools` unter dem Namen `KeystoreTools.jar`. JAR Dateien sind JAVA Archive welche die JAVA Programme enthalten.

Ausführen können Sie die Keystore Tools mit dem Systembefehl `RUNJAVA` plus der für die jeweils gewünschte Funktionalität erforderlichen Parameter. Im folgenden werden die Funktionen und die jeweils zu verwendenden Parameter erläutert.

Der Basisaufruf der KeystoreTools sieht wie folgt aus

`RUNJAVA CLASS(/i-effect/<version>/CRYPT/tools/KeystoreTools.jar) PARM(...)`

gefolgt von einem oder mehreren Parametern die innerhalb des PARM Parameters, durch Komma getrennt, angegeben werden.

Bitte beachten Sie, dass die Parameter innerhalb des PARM Parameters in einfache Hochkommata gesetzt werden müssen (,param1, param2,...')

*CHECK – Überprüft die Gültigkeit der Zertifikate im i-effect® Keystore

Bei Angabe des *CHECK Parameters gefolgt von einer Zahl (beides durch Komma getrennt), wird die Gültigkeitsdauer der im Keystore befindlichen Zertifikate überprüft. Die Zahl entspricht dabei der Anzahl an Tagen, die zu prüfen sind, bis ein Zertifikat die Gültigkeit verliert.

Das Ergebnis dieser Prüfung wird in der Textdatei

`/i-effect/<version>/internal/YYYY-MM-DD-certificates_to_check.list`

gespeichert. In dieser Datei sind alle betreffenden Zertifikate mit dem jeweiligen Alias und Zertifikatsinformationen aufgelistet.

Wenn Sie beispielsweise alle Zertifikate gelistet haben möchten, die innerhalb der nächsten 30 Tage ablaufen, sieht der Aufruf wie folgt aus:

`RUNJAVA CLASS(/i-effect/<version>/CRYPT/tools/KeystoreTools.jar) PARM(*CHECK,30)`

Darüber hinaus werden auch immer automatisch alle Zertifikate gelistet, die noch nicht gültig oder schon abgelaufen sind. Wurden weder noch nicht gültige, abgelaufene oder innerhalb der angegebenen Tage ablaufende Zertifikate gefunden, so ist die Ausgabedatei leer.

Hinweis für die automatisierte Verwendung in i-effect® *SERVER

Sie können die Ausführung KeystoreTools *CHECK automatisieren, z. B. als wöchentlichen ***SCHEDULE** Servertask, und haben somit die Möglichkeit frühzeitig zu reagieren wenn das eigene Zertifikat oder das eines Partners ausläuft. Die in diesem Fall zu verwendende Art der *SERVER Verarbeitung ist ***USERDEFINED**, bei Dateiar ist *NONE anzugeben.



*Voraussetzung für den Einsatz ist eine gültige Lizenz des *SERVER Moduls.*

Für die Verwendung im Servertask muss jedoch ein weiterer Parameter mit an den Aufruf übergeben – die *SERVER spezifische Variable „%SESSIONNUMBER%“. Diese Variable enthält die vom Servertask zur Laufzeit verwendete Sitzungsnummer. Wird diese Nummer an KeystoreTools *CHECK übergeben, so werden die Logbuchnachrichten von KeystoreTools in die Sitzung mit der angegebene Nummer geschrieben.

Bezogen auf den vorherigen Beispielaufruf sieht der Aufruf für den Einsatz im Servertask dann folgendermaßen aus:

```
RUNJAVA CLASS(/i-effect/<version>/CRYPT/tools/KeystoreTools.jar) PARM(*CHECK, 30,%SESSIONNUMBER%)
```

Diesen Aufruf geben Sie dann als auszuführende Verarbeitung an.

Wie Sie einen Servertask und dessen Verarbeitung definieren wird ausführlich in Kapitel 8 „Prozessautomatisierung“ beschrieben.