Handbuch

OMS-Sign 1.2

profiforms

ProfiForms Projekt GmbH Hausener Str 6/1 D-71296 Heimsheim +49/7033 3012-0 www.profiforms.de

Rechtliche Hinweise

Inhalt

EINLEITUNG

Der OMS-Sign signiert PDF-Dokumente mit der qualifizierten elektronischen Signatur gemäß dem Verfahren der Massensignatur nach dem Deutschen Signaturgesetz (DSG). Die qualifizierte elektronische Signatur an einem Dokument dient dazu, die Identität des Erstellers des Dokumentes sicherzustellen. Weiterhin wird durch die Signatur gewährleistet, dass das Dokument nach der Signierung nicht mehr verändert wurde.

Gemäß dem deutschen Signaturgesetz wird für die qualifizierte elektronische Signatur eine Dreiecksbeziehung zwischen dem Ersteller, dem Empfänger und einer unabhängigen dritten Instanz, dem TrustCenter, realisiert. Der Ersteller weist sich gegenüber dem TrustCenter als natürliche Person aus und wird dort registriert. Im Gegenzug erhält der Empfänger vom TrustCenter eine oder mehrere Signatur-Karten mit einer ihn ausweisenden Zertifikatsliste, die als geheimer Schlüssel für die Signaturerstellung dient. Auf einer sicheren Signaturerstellungseinheit, die aus einer Kombination von Software, Hardware und der Signatur-Karte besteht, werden Signaturen für die Dokumente erstellt und ins PDF eingebettet.

Der Empfänger des PDF-Dokumentes kann die Unverändertheit des PDF-Dokumentes prüfen und die qualifizierte elektronische Signatur auf ihre Gültigkeit beim TrustCenter über eine OCSP-Anfrage (Online Certificate Status Protocol) feststellen. Dazu benötigt der Empfänger eine OCSP-fähige Software, die nicht Lieferbestandteil von OMS-Sign ist.

OMS-Sign ist in der Lage PDF-Dateien zu signieren, zu verifizieren oder beide Schritte zusammen durchzuführen.

Als sichere Signatureinheit arbeitet OMS-Sign mit den Produkten der Firma secunet Security Networks AG - multisignBox und multisignEnterprise - zusammen. Alternativ kann der Signaturservice „Signtrust Net“ der Deutschen Post AG Signtrust zur Anwendung kommen.

OMS-Sign ist vollständig in die Output Management Suite integriert und unterstützt deren Mechanismen des Accounting, Logging und Monitoring.

AUFRUFKONVENTIONEN SIGN

Verwendung

Der OMS-Sign kann zwei Parameter und eine Liste mit Optionen als Übergabeparameter verarbeiten:

sign [OptionenListe] Input-File [<Output-File>]

Erklärung

Input-File

Input-File ist ein PDF-File oder ein DocumentContainer-File. Ein DocumentContainer-File enthält einen oder mehrere PDF-File und Variablen zur Steuerung des Signaturvorganges. Unterstützt werden PDF-Dateien der PDF-Version 1.3 und 1.4.

Output-File

Der Output-File ist ein optionaler Parameter und gibt den Namen der zu erzeugenden Datei an. Ist kein Output-File angegeben, so wird der Input-File überschrieben.
Ist der Input-File ein einzelner PDF-File, so entsteht als Output-File wieder ein PDF-File. Ist der Input-File ein DocumentContainer-File, so entsteht als Output-File wieder ein DocumentContainer-File.

OptionenListe

Die OptionenListe enthält einzelne Optionen, die mit dem Zeichen ‚-' beginnen.

-all LogFile: Der Filename wird zum Logging aller Aktivitäten verwendet. ERR bedeutet Ausgabe auf STDERR. OUT bedeutet Ausgabe auf STDOUT.

-aip PATH: Pfad zu den Ini-Dateien

-aic CP: Codepage für Konfigurationsdateien, die über den LineReader gelesen werden

-per PERSON: Bezeichnet die unterzeichnende Person. Diese Person kann pro Dokument in einem ContainerFile durch die variable Person überschrieben werden.

-vol: Für den Output-File generiert OMS-Sign zusätzlich noch eine *.vol-Datei. Eine *.vol-Datei ist eine xml-Datei, welche die Ausgabedatei näher beschreibt. Die Option –vol ist von besonderem Interesse bei der Integration in den OMS-Spooler.

-sno SNO: Alternativ zur Angabe der Seriennummer in der reportw.ini kann diese auch als Kommandozeilenparameter übergeben werden. Die Seriennummer in der sign.ini wird ignoriert.

-h: Bei der Angabe von –h, -?, -help oder --help erfolgt nur die Ausgabe einer Kurzbeschreibung zu den Aufrufkonventionen des OMS-Sign.

-v: Bei der Angabe von -v erfolgt nur die Ausgabe der Versionsnummer auf den Bildschirm. Danach beendet OMS-Sign seine Arbeit.

-mod MODE: Arbeitsmodus:

SIGN	signieren
VERIFY	verifizieren
SIGNVERIFY	signieren und anschließend verifizieren

-adv: Mit -adv werden alle Variablen definiert, die in allen Dokumenten des Datenstroms gesetzt werden. Der Parameter -adv kann in der Kommandozeile mehrfach vorkommen, so dass unterschiedliche Variablen definiert werden können.

Syntax

-adv VARNAME=VOLUME

Beispiel:

```
sign –adv PRN=OFFICEPRN1 –adv PRNSERVER=RW1 x.pdf
```

SIGN.INI

Alle Zeilen und Objekte werden über den LineReader als Preprozessor gelesen und unterstützen Includes und das Lesen aus Sections.

Verwendung

Die sign.ini speichert generelle Informationen zu den Laufeigenschaften des OMS-Sign. Folgende Schlüsselwörter und Objekte sind in der sign.ini zulässig:

SerNo Value

SerNo beinhaltet die Seriennummer bzw. den Produkt-Autorisierungs-Schlüssel des OMS-Sign. Alternativ zur Angabe in der sign.ini kann die Seriennummer auch als Parameter der Kommandozeile gesetzt werden. Ist beides angegeben, so hat der Parameter der Kommandozeile den Vorrang vor dem Eintrag in der sign.ini.

Syntax

SerNo XXXXX-XXXXX-XXXXX-XXXXX

CommonSettings

CommonSettings ist eine Aufzählung von Schlüsselwörtern, die allgemeine Einstellungen definieren.

Syntax

CommonSettings {
OutFileDocRefFields List
OutFileSAPRefFields List
CancelOnVerificationFailure Value
}

OutFileDocRefFields List

OUTFILEDOCREFFIELDS ist eine Komma-separierte Liste von Variablen-Namen oder Fix-Strings, die in der angegebenen Reihenfolge als CSV-Zeile in einen DocRef-File geschrieben werden. Fix-Strings beginnen und enden mit Anführungszeichen. Die hier aufgeführten Variablen sollten entweder am Dokument vorhanden sein oder aus der Liste der Standard DocRef-Fields kommen, die unter "Zusätzliche Ausgabevariablen/DocRef" weiter hinten beschrieben sind. OutFileDocRef-Files haben denselben Namen wie die Dat-Files. Die Endung ist allerdings ".docref".

OutFileSAPRefFields List

OUTFILESAPREFFIELDS ist eine Komma-separierte Liste von Variablen-Namen oder Fix-Strings, die in der angegebenen Reihenfolge als CSV-Zeile in einen SAPRef-File geschrieben werden. Fix-Strings beginnen und enden mit Anführungszeichen. Die hier aufgeführten Variablen sollten entweder am Dokument vorhanden sein oder aus der Liste der Standard DocRef-Fields kommen, die unter "Zusätzlichen Ausgabevariablen/DocRef" weiter hinten beschrieben sind. OutFileSAPRef-Files haben denselben Namen wie die Dat-Files. Die Endung ist allerdings ".sapref".

CancelOnVerificationFailure Value

CANCELONVERIFICATIONFAILURE ist ein Schalter mit den Werten 0 und 1, wobei 0 der Standardwert ist. Eine Verifiaktion erzeugt einen Prüfbeleg, anhand dem die Gültigkeit der Signatur bestimmt werden kann. Eine Prüfbeleg mit dem Ergebnis einer ungültigen Signatur ist kein Abbruchgrund für das Programm. Soll der Prozess beim Feststellen einer ungültigen Signatur abgebrochen werden, so ist der Schalter einzuschalten.

SIGNERS.INI

Alle Zeilen und Objekte werden über den LineReader als Preprozessor gelesen und unterstützen Includes und das Lesen aus Sections.

Verwendung

Die signers.ini enthält alle Informationen über die zeichnenden Personen und ihre Anmelde-informationen bei der sicheren Signatureinheit.

Es werden drei Objektarten unterstützt:

DefaultConnection
DefaultPerson
Persons

Alle drei Objektarten setzen sich aus den Basis-Objekten Connection und Person zusammen.

DefaultConnection

DefaultConnection definiert Standardwerte für die Connections einzelner Personen. Einstellungen, die die Connections aller Personen gemeinsam haben, können in die DefaultConnection abgespeichert werden. Die Connection einer Person kann die einzelnen Default-Werte dann trotzdem noch überschreiben.

```
DefaultConnection {
    siehe Connection
}
```

DefaultPerson

DefaultPerson definiert eine Person mit dem Namen DEFAULT in der Liste der Personen. Dies bedeutet, dass eine Person mit dem Namen DEFAULT in der Personen-Tabelle angelegt wird. Ist beim Aufruf von OMS-Sign keine Person angegeben und auch im Dokument keine variable Person definiert, so signiert OMS-Sign das Dokument auf die Person mit dem Namen DEFAULT.

```
DefaultPerson {
    siehe Person
}
```

Persons

Persons ist eine Liste von Personen-Objekten, wie diese weiter unten beschrieben wird.

```
Persons {
    PersonName1 {
     siehe Person
    }
    PersonName2 {
     siehe Person
    }
    ...
}
```

Die Connection speichert Anmeldeinformationen für eine Person an einer sicheren Signatureinheit.

Syntax

Connection {

DualServer	Val
ServerAddress	Val
ServerAddress2	Val
ServerPort	Val
Trials	Val
UserName	Val
Password	Val
ProxiAddress	Val
ProxiPort	Val
ProxiUserName	Val
ProxiPassword	Val
CA_Certificate	Val
ConnectTimeOut	Val
OperationTimeOut	Val
HashType	Val
ProtocolType	Val
Revocation	Val

}

DualServer Value

FieldOrValue und NVC
DualServer bestimmt beim Vorhandensein einer zweiten sicheren Signatureinheit, ob die zweite Box im Modus Fail-Over oder Lastverteilung läuft. Standardwert ist Failover.

Werte für DualServer sind:

0 oder FAILOVER	für Fail Over
1 oder LOADBALANCING	für Lastverteilung

Lastverteilung bedeutet nicht, dass jedes Dokument zu einer anderen sicheren Signatureinheit gesendet wird, sondern beim Aufbau einer Verbindung wird die Verbindung zu einer sicheren Signatureinheit für den gesamten Lauf nach einem Zufallskriterium gewählt.

ServerAddress Value

FieldOrValue und NVC
IP-Adresse oder DNS-Name der ersten sicheren Signatureinheit.

ServerAddress2 Value

FieldOrValue und NVC
IP-Adresse oder DNS-Name der zweiten sicheren Signatureinheit.

ServerPort Value

FieldOrValue und NVC
Port auf dem die sichere Signatureinheit Verbindungen akzeptiert.

Trials Value

FieldOrValue und NVC
Trials gibt die Anzahl der Versuche an, die bei der Kommunikation mit der sicheren Signatureinheit unternommen werden, bevor bei Nichterfolg abgebrochen wird. Standardwert ist 3.

UserName Value

FieldOrValue und NVC
Benutzername zur Authentifizierung gegenüber der sicheren Signatureinheit.

Password Value

FieldOrValue und NVC
Passwort zur Authentifizierung gegenüber der sicheren Signatureinheit.

ProxiAddress Value

FieldOrVaule und NVC
IP-Adresse oder DNS-Name des Proxi-Servers. Die Angabe ist optional.

ProxiPort Value

FieldOrValue und NVC
Port auf dem der Proxi-Server die Verbindungen erwartet. Die Angabe ist optional.

ProxiUserName Value

FieldOrValue und NVC
Benutzername zur Authentisierung gegenüber dem Proxi-Server. Die Angabe ist optional.

ProxiPassword Value

FieldOrValue und NVC
Passwort zur Authentisierung gegenüber dem Proxi-Server. Die Angabe ist optional.

CA_Certificate Value

FieldOrValue und NVC
Speicherort und Name der lokalen CA-Zertifikatsdatei. Für den sicheren Verbindungsaufbau wird ein Zertifikat benötigt. Standardmäßig wird das Zertifikat aus der Datei cacert.pem gelesen, die im Ini-Path stehen muss. Soll das Zertifikat aus einer anderen Datei gelesen werden, so kann es mit CA_Certificate angegeben werden. CA_Certificate ist optional.

ConnectTimeOut Value

FieldOrValue und NVC
Timeout in Sekunden für den Verbindungsaufbau zur sicheren Signatureinheit. Ist ConnectTimeOut nicht gesetzt, so wird ein Standardwert verwendet. ConnectTimeOut ist optional.

HashType Value

FieldOrValue und NVC
Die Berechnung des Hash-Wertes eines PDFs kann über unterschiedliche Algorithmen realisiert werden. Die Bundesnetzagentur gibt vor, welcher Algorithmus im Moment verwendet werden darf. Der Algorithmus wird als HashType definiert und kennt folgende Werte:

SHA1	
SHA2_224	
SHA2_256	
SHA2_384	
SHA2_512	
RIPEMD160	StandardWert
AUTO	

ProtocolType Value

FieldOrValue und NVC
Ist ein Schalter mit den Werten XML, PDF und EMBED, wobei EMBED der Standardwert ist. PROTOCOLTYPE bestimmt bei der Verifikation die Art des Prüfberichtes:

XML	Prüfbericht als externe XML-Datei
PDF	Prüfbericht als externe PDF-Datei
EMBED	Prüfbericht als anhängende Seitengruppe eingebettet in das zu prüfende PDF

Revocation Value

FieldOrValue und NVC
REVOCATION ist ein Schalter mit den Werten NONE, OCSP und CRL, wobei OCSP der Standardwert ist. REVOCATION bestimmt bei der Verifikation wie der Sperrstatus einer Karte ermittelt werden soll:

OCSP	Verwendung des Online Certification Status Protokolls (über das Internet)
CRL	Verwendung des Certificat Revocation List (lokal über Liste)
NONE	Keinen Sperrstatus überprüfen

OperationTimeOut Value

FieldOrValue und NVC
Timeout in Sekunden für Übertragungsoperationen zur sicheren Signatureinheit. Ist OperationTimeOut nicht gesetzt, so wird ein Standardwert verwendet. OperationTimeOut ist optional.

Person speichert alle Informationen zu einer signierenden Person:


Syntax

```
PersonName {
    FullName      Val
    Location      Val
    Reason        Val
    SignConnection {
    ...
    }
    VerifyConnection {
    ...
    }
}
```

PersonName

PersonName ist der Name der Person. Dabei sind keine Leerzeichen im Namen erlaubt.

FullName Value

FieldOrValue und NVC
FullName beinhaltet den vollständigen Namen der signierenden Person. Der FullName kann Leerzeichen und Umlaute beinhalten. HTML-Entities und Zeichen des lokalen Zeichensatzes werden unterstützt. Die Angabe ist optional.

Location Value

FieldOrValue und NVC
Location ist der Ort der Unterzeichnung. Ist die Angabe länger als 255 Zeichen, so wird sie gekürzt. Location kann Leerzeichen und Umlaute beinhalten. Entities und Zeichen des lokalen Zeichensatzes werden unterstützt. Die Angabe ist optional.

Reason Value

FieldOrValue und NVC
Reason ist der Grund oder Anlass des Unterzeichnens. Ist die Angabe länger als 255 Zeichen, so wird sie gekürzt. Reason kann Leerzeichen und Umlaute beinhalten. Entities und Zeichen des lokalen Zeichensatzes werden unterstützt. Die Angabe ist optional.

SignConnection

SignConnection ist die Connection, die zur Signierung verwendet wird. Ist das Objekt gar nicht oder nicht vollständig definiert, so werden die fehlenden Angaben aus dem Objekt DefaultConnection ergänzt. SignConnection ist ein Objekt vom Typ Connection und dort beschrieben.

VerifyConnection

VerifyConnection ist die Connection, die zur Verifikation verwendet wird. Ist das Objekt gar nicht oder nicht vollständig definiert, so werden die fehlenden Angaben aus dem Objekt DefaultConnection ergänzt. VerfyConnection ist ein Objekt vom Typ Connection und dort beschrieben.

Beispiel:

```
DefaultConnection {
  ServerAddress 192.168.2.244
  ServerPort    443
}

Persons {
 Achim {
  FullName    Achim Hubenduebel
  Location    Stuttgart
  Reason      @Reason
  SignConnection {
   UserName   AHudbl
   Password   %NVC%woLCkcORw5HvvKjvvZXvvb/vvJLvvIHvvYHvvYHCsw==
  }
 }
 Thomas {
  FullName    Thomas Pantoffel
  Location    Berlin
  Reason      Gutschrift
  SignConnection {
   UserName   TPanto
   Password   %NVC%woLCicOLw5HvvKnvvZ3vvbnvvJ3vvJg=
  }
 }
}

DefaultPerson {
 FullName     Klaus Kinsky
 Location     Bonn
 SignConnection {
  UserName    KKinsky
  Password    %NVC%woLCjMOOw5LvvKTvvY/vvavvvIA=
 }
}
```

NVC – NON VISIBLE CODE-ANGABEN

NVC ist eine einfache Kodierungstechnik zur Abspeicherung von Text in einer Datei, die verhindert, dass der Text mit einem Editor gelesen werden kann. OMS-Sign erkennt NVC-kodierten Text und ist in der Lage, diesen beim Lesen wieder zu dekodieren. Schlüsselwörter, die NVC-kodierten Text lesen können, sind im Handbuch mit NVC gekennzeichnet.

Zur Konvertierung von normalen Strings in NVC-Strings kann das Programm String verwendet werden, das Bestandteil der Output Management Suite ist.

Die NVC-Kodierung gilt nicht als sichere Kodierung wie z. B. die RSA128-Kodierung. Obwohl die Passwörter in der signer.ini NVC-kodiert abgelegt werden können, ist es notwendig, die signer.ini vor fremdem Zugriff und krimineller Analyse zu schützen.

```
Bsp.: Password    %NVC%woLCjMOOw5LvvKTvvY/vvavvvIA=
```

FIELDORVALUE-ANGABEN

Zu den wichtigsten internen Mechanismen gehören FieldOrValue-Berechnungen. Diese Mechanismen stehen mit fast allen Basisobjekten in Verbindung und sind deshalb von besonderer Bedeutung.

FieldOrValue-Angaben bringen große Variabilität in die Konfiguration, da die Steuerung wichtiger Parameter entweder fest vorgegeben ist oder aus einem Feld des Datenstroms gelesen wird. FieldOrValue versetzt Sie in die Lage, wichtige Werte zur Ablaufsteuerung dynamisch aus dem Datenstrom ermitteln zu können. Parameter, die FieldOrValue-fähig sind, können

fix festgelegt werden

```
Bsp.: Reason Rechnung
```

aus einem Feld des Dokumentes gelesen werden

```
Bsp.: Reason @BELEG_ART
```

ZUSÄTZLICHE AUSGABEVARIABLEN

DocRef-Variablen:

PERSON	Unterzeichnende Person
DOCREF	Dokument-Referenz aus dem DocDef
DATETIME	Datum und Uhrzeit der Unterzeichnung
FULLNAME	Vollständiger Name der unterzeichnenden Person
REASON	Grund der Unterzeichnung
LOCATION	Ort der Unterzeichnung
VERIFICATIONSUCCSESS	Erfolg der Verifikation mit den Werten true oder false
VERIFICATIONMESSAGE	Informeller Text über den Erfolg der Verifikation oder Gründe des Misserfolgs
PROTOCOLCONTENTTYPE	Dateitype des Prüfprotokolls mit den Werten: application/pdf oder text/xml
SIGNMODE	Modus in dem sign betrieben wurde: SIGN|VERIFY|SIGNVERIFY

INDEX