

Secure Store & Forward / Digitale Signaturen (BC-SEC- SSF)



HELP.BCSECDISI

Release 4.6C



Copyright

© Copyright 2001 SAP AG. Alle Rechte vorbehalten.

Weitergabe und Vervielfältigung dieser Publikation oder von Teilen daraus sind, zu welchem Zweck und in welcher Form auch immer, ohne die ausdrückliche schriftliche Genehmigung durch SAP AG nicht gestattet. In dieser Publikation enthaltene Informationen können ohne vorherige Ankündigung geändert werden.

Die von SAP AG oder deren Vertriebsfirmen angebotenen Software-Produkte können Software-Komponenten auch anderer Software-Hersteller enthalten.

Microsoft[®], WINDOWS[®], NT[®], EXCEL[®], Word[®], PowerPoint[®] und SQL Server[®] sind eingetragene Marken der Microsoft Corporation.

IBM[®], DB2[®], OS/2[®], DB2/6000[®], Parallel Sysplex[®], MVS/ESA[®], RS/6000[®], AIX[®], S/390[®], AS/400[®], OS/390[®] und OS/400[®] sind eingetragene Marken der IBM Corporation.

ORACLE[®] ist eine eingetragene Marke der ORACLE Corporation.

INFORMIX[®]-OnLine for SAP und Informix[®] Dynamic Server[™] sind eingetragene Marken der Informix Software Incorporated.

UNIX[®], X/Open[®], OSF/1[®] und Motif[®] sind eingetragene Marken der Open Group.




HTML, DHTML, XML, XHTML sind Marken oder eingetragene Marken des W3C[®], World Wide Web Consortium, Massachusetts Institute of Technology.

JAVA[®] ist eine eingetragene Marke der Sun Microsystems, Inc.

JAVASCRIPT[®] ist eine eingetragene Marke der Sun Microsystems, Inc., verwendet unter der Lizenz der von Netscape entwickelten und implementierten Technologie.

SAP, SAP Logo, R/2, RIVA, R/3, ABAP, SAP ArchiveLink, SAP Business Workflow, WebFlow, SAP EarlyWatch, BAPI, SAPPHIRE, Management Cockpit, mySAP.com Logo und mySAP.com sind Marken oder eingetragene Marken der SAP AG in Deutschland und vielen anderen Ländern weltweit. Alle anderen Produkte sind Marken oder eingetragene Marken der jeweiligen Firmen.

Symbole

| Symbol | Bedeutung |
|---|------------|
|  | Achtung |
|  | Beispiel |
|  | Hinweis |
|  | Empfehlung |
|  | Syntax |

Typographische Konventionen

| Format | Beschreibung |
|---------------------------|---|
| <i>Beispieltext</i> | Wörter oder Zeichen, die vom Bildschirmbild zitiert werden. Dazu gehören Feldbezeichner, Bildtitel, Drucktastenbezeichner sowie Menünamen, Menüpfade und Menüeinträge. Querverweise auf andere Dokumentationen |
| Beispieltext | Hervorgehobene Wörter oder Ausdrücke im Fließtext, Titel von Grafiken und Tabellen |
| BEISPIELTEXT | Namen von Systemobjekten. Dazu gehören Reportnamen, Programmnamen, Transaktionscodes, Tabellennamen und einzelne Schlüsselbegriffe einer Programmiersprache, die von Fließtext umrahmt sind, z.B. SELECT und INCLUDE. |
| <code>Beispieltext</code> | Ausgabe auf dem Bildschirmbild. Dazu gehören Datei- und Verzeichnisnamen und ihre Pfade, Meldungen, Namen von Variablen und Parametern, Quelltext und Namen von Installations-, Upgrade- und Datenbankwerkzeugen. |
| Beispieltext | Exakte Benutzereingabe. Dazu gehören Wörter oder Zeichen, die Sie genau so in das System eingeben, wie es in der Dokumentation angegeben ist. |
| <Beispieltext> | Variable Benutzereingabe. Die Wörter und Zeichen in spitzen Klammern müssen Sie durch entsprechende Eingaben ersetzen, bevor Sie sie in das System eingeben. |
| BEISPIELTEXT | Tasten auf der Tastatur, z.B. Funktionstasten wie F2 oder die ENTER-Taste |

Inhalt

| | |
|--|-----------|
| Secure Store & Forward / Digitale Signaturen (BC-SEC-SSF) | 5 |
| Systemlandschaft bei Verwendung der SSF-Funktionen | 8 |
| Begriffe und Abkürzungen | 9 |
| SSF-Verwaltungsarbeiten | 12 |
| SSF mit externem Sicherheitsprodukt einsetzen | 13 |
| SSF installieren/konfigurieren: Frontends | 14 |
| SSF installieren/konfigurieren: Anwendungsserver | 15 |
| SSF-Benutzerinformationen pflegen | 17 |
| SSF-Benutzerinformationen pflegen: Release 4.6+ | 18 |
| Upgrade der SSF-Benutzerinformationen von Release 4.0/4.5 | 20 |
| Verwendung des SSF-Standardsicherheitsprodukts SAPSECULIB | 21 |
| SAP Security Library (SAPSECULIB) | 22 |
| Die System-PSE pflegen | 24 |
| SSF-Standardinformationen für Anwendungen definieren | 27 |
| Anwendungsspezifische Informationen pflegen | 28 |
| Die SSF-Installation testen | 31 |
| SSF-Parameter | 33 |
| SSF_LIBRARY_PATH | 36 |
| SSF_MD_ALG | 37 |
| SSF_SYMENCR_ALG | 38 |
| SSF_TRACE_LEVEL | 39 |
| SSF_NAME | 40 |
| Die SSF-Initialisierungsdatei | 41 |
| Information zu Release 4.0/4.5 | 43 |
| SSF-Benutzerinformationen pflegen: Release 4.0/4.5 | 44 |
| Die SSF-Initialisierungsdatei in Release 4.0 | 45 |

Secure Store & Forward / Digitale Signaturen (BC-SEC-SSF)

Einsatzmöglichkeiten

Die Mechanismen des [Secure Store & Forward \(SSF\) \[Extern\]](#) bieten Ihnen die Möglichkeit, Daten und Dokumente in SAP-Systemen als unabhängige Dateneinheiten zu sichern. Mit den SSF-Funktionen können Sie Daten und digitale Dokumente in sichere Formate "verpacken", bevor sie auf Datenträgern gesichert oder über (möglicherweise) unsichere Kommunikationsverbindungen übertragen werden. Wenn Sie Daten im SAP-System in einem sicheren Format speichern, bleiben sie in diesem gesicherten Format, selbst wenn Sie sie aus dem System exportieren.

SSF-Mechanismen verwenden [digitale Signaturen \[Seite 9\]](#) und [digitale Umschläge \[Seite 9\]](#), um digitale Dokumente zu sichern. Die **digitale Signatur** identifiziert den Unterzeichner eindeutig, läßt sich nicht fälschen und schützt die Integrität der Daten. Jede nach der Unterzeichnung vorgenommene Änderung der Daten führt dazu, daß die digitale Signatur für die geänderten Daten ungültig ist. Der **digitale Umschlag** stellt sicher, daß die Dateninhalte nur für die Empfänger einsehbar sind, für die sie bestimmt sind.

Die SSF-Mechanismen sind in Anwendungsgebieten nützlich, in denen ein erhöhtes Maß an Sicherheit besteht für:

- die spezifische und eindeutige Identifizierung von Personen oder Komponenten (z. B. bei Workflow-Prozessen)
- Unleugbarkeit oder Verbindlichkeit (z. B. beim Unterzeichnen nicht in gedruckter Form vorliegender Verträge)
- Authentizität und Integrität der Daten (z. B. Sichern der Audit-Logs)
- Senden und Ablegen vertraulicher Daten

Durch den Einsatz der SSF-Mechanismen in SAP-Anwendungen können Sie gedruckte Dokumente und handschriftliche Unterschriften durch automatisierte Workflow-Prozesse und digitale Dokumente ersetzen, die mittels digitaler Signaturen und digitaler Umschläge gesichert sind.

Einführungshinweise

Ab Release 4.0 stehen in den SAP-Systemen SSF-Mechanismen zur Verfügung.

Sie verwenden die SSF-Mechanismen, wenn Sie eine Anwendung im SAP-System benutzen, die digitale Signaturen oder digitale Umschläge enthält.

Derzeit verwenden zahlreiche Anwendungen zum Schutz der Daten SSF-Mechanismen beispielsweise:

- Produktionsplanung - Prozeßindustrie
- Produktdatenmanagement
- SAP ArchiveLink - Schnittstelle SAP Content Server HTTP 4.5

Mit der Zeit werden immer mehr Anwendungen SSF verwenden, um die Sicherheit zu erhöhen.

Einschränkungen

Externes Sicherheitsprodukt

Damit SSF seine Funktionen zur Verfügung stellen kann, benötigt es ein externes Sicherheitsprodukt. Als Standardprodukt liefern wir mit dem SAP-System die [SAP Security Library \(SAPSECULIB\) \[Seite 22\]](#). Die SAPSECULIB kann jedoch nur digitale Signaturen zur Verfügung stellen. Für die Unterstützung digitaler Umschläge, Verschlüsselung oder kryptografischer Hardware (z. B. Smartcards oder Sicherheitsboxen) benötigen Sie ein von SAP zertifiziertes externes Sicherheitsprodukt. Damit ein Produkt von SAP zertifiziert wird, muß es das Standarddatenformat PKCS#7 unterstützen. Informationen über die unterstützten Produkte finden Sie unter SAP Complementary Software Program (<http://www.sap.com/csp>).

Public-Key-Infrastruktur

Damit Sie die SSF-Mechanismen erfolgreich einsetzen können, muß eine [Public-Key-Infrastruktur \(PKI\) \[Seite 9\]](#) eingerichtet werden. Die PKI stellt sicher, daß Sie die digitalen Signaturen, Zertifikate und Zertifizierungsinstanzen (Certification Authorities, CAs) prüfen und ihnen vertrauen können. Eine PKI wird oftmals, allerdings nicht notwendigerweise, von den am Markt verfügbaren externen Sicherheitsprodukten unterstützt. Zwar bieten die SAP-Systeme nicht direkt eine PKI an, aber sie unterstützen die von verschiedenen Sicherheitsprodukten angebotenen PKIs.

Je nachdem welches Sicherheitsprodukt Sie verwenden, können Sie den Einsatz einer PKI auf eine vieler möglicher Arten einrichten. Entweder bauen Sie Ihre eigene PKI und CA auf und stellen dann eine Verbindung zu Ihren Kunden her oder Sie und Ihre Kunden einigen sich auf ein gemeinsames Trust Center. Ein gemeinsames Trust Center ist eine externe Instanz, der sowohl Sie als auch Ihre Kunden die Prüfung und Authentifizierung Ihrer PKI-Teilnehmer anvertrauen können. Die Nutzung eines gemeinsamen Trust Center kann viele der derzeit offenen Fragen bezüglich der Einrichtung einer PKI lösen.

Gesetze und Vorschriften

In einigen Ländern wird die Verwendung der Kryptografie und digitaler Signaturen gesetzlich geregelt. Diese Gesetze sind zur Zeit noch sehr unterschiedlich und können sich ändern. Sie sollten sich regelmäßig über die Auswirkungen dieser Gesetze auf Ihre Anwendungen informieren und sicherstellen, daß Ihnen alle weiteren Entwicklungen bekannt sind.

Beispiele von SAP-Anwendungen, die die SSF-Funktionen nutzen

Die folgenden SAP-Anwendungen sind Beispiele für Bereiche, die digitale Signaturen einsetzen, um ihren Anforderungen gerecht zu werden.

- **Qualitätsmanagement**
 - beim Ablegen von Prüfergebnissen für ein Prüflos
 - beim Erstellen oder Ändern des Verwendungsentscheids für ein Prüflos
- **Produktionsplanung für die Prozeßindustrie**
 - beim Abschließen eines Arbeitsschritts in der Herstellenweisung
 - bei der Annahme ungültiger Werte innerhalb der Eingabewertprüfungen
 - bei der Genehmigung eines Chargenprotokolls

- **Schnittstelle SAP ArchiveLink Content Server HTTP 4.5**
 - beim Authentifizieren einer Zugriffsanfrage auf das Archiv

Systemlandschaft bei Verwendung der SSF-Funktionen

Systemlandschaft bei Verwendung der SSF-Funktionen

SSF verwendet ein externes Sicherheitsprodukt, um die Funktionen ausführen zu können, die für die Verwendung digitaler Signaturen und Verschlüsselung in SAP-Systemen benötigt werden. Um mit dem externen Sicherheitsprodukt kommunizieren zu können, muß das SAP-System auf das Produkt und seine Informationen zugreifen können. Daher wird folgende Systemlandschaft für die Verwendung der SSF-Funktionen benötigt:

- Kommunikationsschnittstelle zum Sicherheitsprodukt:**

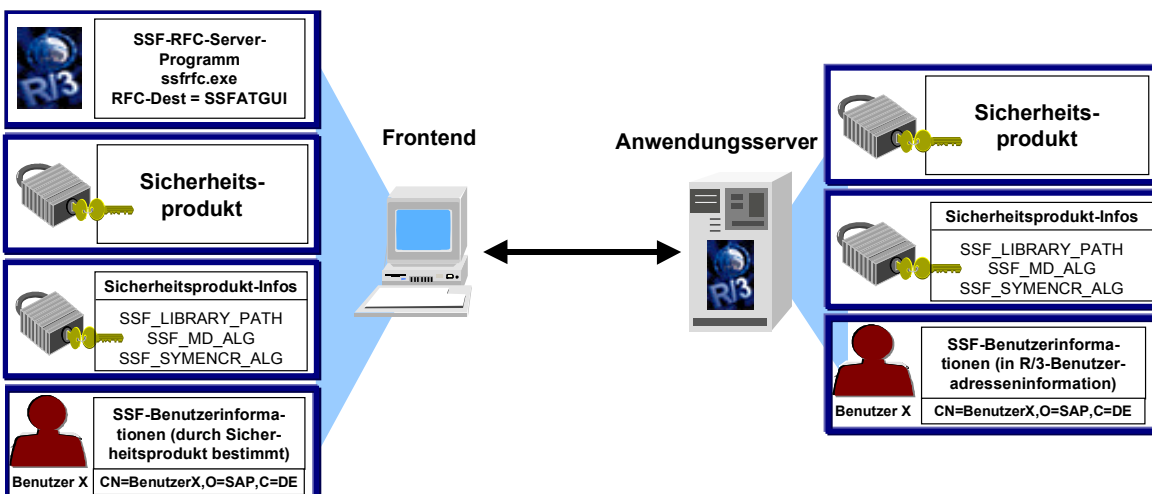
Für die Kommunikation mit dem externen Sicherheitsprodukt auf den Frontends verwendet das SAP-System das SSF-RFC-Serverprogramm `ssfrfc.exe` (RFC, Remote Function Call). Auf dem Anwendungsserver ist die Kommunikationsschnittstelle im SAP-Systemkernel enthalten.
- Zugriff auf produktspezifische Informationen:**

Das SAP-System muß auch auf die produktspezifischen Informationen (z. B. den Ort der Bibliothek und die vom Produkt verwendeten Algorithmen) zugreifen können. Auf den Frontend-Rechnern müssen sich diese Informationen entweder in Umgebungsvariablen oder in der SSF-Initialisierungsdatei `ssfrfc.ini` befinden. Auf den Anwendungsservern befinden sich diese Informationen entweder in Profilparametern oder Umgebungsvariablen.
- SSF-Informationen zum Benutzer**

Außerdem müssen die Benutzer, die an der Public-Key-Infrastruktur teilnehmen, auch im SAP-System korrekt gepflegt werden.

(Siehe Grafik unten.)

Komponenten der Systemlandschaft für die Verwendung von SSF



Die folgenden Abschnitte beschreiben die zur Einrichtung dieser Infrastruktur notwendigen Verwaltungsaufgaben.

Begriffe und Abkürzungen

Bevor Sie die SSF-Verwaltungsaufgaben durchführen, sollten Sie sich mit folgenden Begriffen und Abkürzungen vertraut machen:

- **Certification Authority (CA)**

Eine externe Instanz, die Public-Key-Zertifikate ausstellt. Die CA garantiert die Identität des Zertifikatbesitzers.

- **Credentials (Zugriffsberechtigung)**

Benutzer- oder komponentenspezifische Informationen, die es Benutzern oder Komponenten gestatten, auf die eigenen Sicherheitsinformationen zuzugreifen. Die Credentials können sich beispielsweise in einer geschützten Datei im Dateisystem befinden. Oftmals haben sie eine begrenzte Gültigkeitsdauer. Die Credentials der Benutzer können beispielsweise angelegt werden, wenn sie sich am Sicherheitsprodukt anmelden, und gelöscht werden, wenn sie sich abmelden.

- **digitale Signatur**

Sicherheitsmechanismus zum Schutz digitaler Daten.

Die digitale Signatur hat für die Verarbeitung digitaler Daten dieselbe Funktion wie eine handschriftliche Unterschrift für gedruckte Dokumente. Ihr Zweck ist sicherzustellen, daß Personen (oder Komponenten), die das digitale Dokument signieren, tatsächlich diejenigen sind, die zu sein sie vorgeben. Die digitale Signatur schützt auch die Integrität signierter Daten; sobald auch nur ein Bit der signierten Daten oder der Signatur geändert wird, ist die Signatur ungültig.

Die digitale Signatur basiert auf der Public-Key-Verschlüsselung. Jeder Unterzeichner erhält ein einzigartiges Schlüsselpaar aus einem privaten und einem dazugehörigen öffentlichen Schlüssel. Der Unterzeichner erstellt seine digitale Signatur mit seinem privaten Schlüssel. Er verteilt den öffentlichen Schlüssel nach Bedarf. Die Empfänger der signierten Daten prüfen mit dem öffentlichen Schlüssel des Unterzeichners dessen digitale Signatur.

Beispielsweise im elektronischen Handel (Electronic Commerce) werden nicht in gedruckter Form vorliegende Verträge ohne handschriftliche Unterschriften abgeschlossen.

- **digitaler Umschlag**

Diese Schutzmethode schützt eine Nachricht davor, von anderen als den Empfängern, für die sie bestimmt war, eingesehen zu werden.

Ein digitaler Umschlag wird mit hybrider Verschlüsselung erstellt. Zuerst wird die Nachricht selbst mittels symmetrischer Verschlüsselung verschlüsselt (d. h. für die Ver- und Entschlüsselung der Nachricht wird derselbe Schlüssel verwendet). Dann wird dieser Schlüssel mit der Public-Key-Verschlüsselung verschlüsselt und mit der verschlüsselten Nachricht versandt oder gesichert. Nur der Empfänger, für den die Nachricht bestimmt ist, kann den Schlüssel, der zur Verschlüsselung der Originalnachricht verwendet wurde, und somit die Nachricht entschlüsseln.

- **Persönliche Sicherheitsumgebung (Personal Security Environment, PSE)**

Begriffe und Abkürzungen

Sicherer Ort, an dem die Public-Key-Informationen eines Benutzers oder einer Komponente abgelegt werden. Die PSE eines Benutzers oder einer Komponente befindet sich normalerweise in einem geschützten Verzeichnis im Dateisystem oder auf einer Smartcard. Sie enthält sowohl die öffentlichen Informationen (Public-Key-Zertifikat und privates Adreßbuch) als auch die privaten Informationen (privater Schlüssel) des Besitzers. Daher sollte nur der Besitzer der Informationen auf seine PSE Zugriff haben.

Beispielsweise legt die **SAP Security Library** (SAPSECULIB) die Informationen des Anwendungsservers in einer PSE ab. In diesem Fall enthält die PSE sowohl das **private Adreßbuch** des SAP-Systems als auch das **SSF-Profil**.

- **Privates Adreßbuch**

Ort in der Public-Key-Infrastruktur, an dem die öffentlichen Schlüssel der Benutzer und Komponenten abgelegt werden. Je nachdem, welches Sicherheitsprodukt Sie verwenden, kann das private Adreßbuch mit dem SSF-Profil identisch sein.

- **Public-Key-Infrastruktur (PKI)**

Ein System, das die an der Verwendung der Public-Key-Technologie beteiligten Vertrauensbeziehungen verwaltet. Die PKI hat die Aufgabe sicherzustellen, daß Public-Key-Zertifikate und CAs geprüft werden können und vertrauenswürdig sind. Die Sammlung der Dienste und Komponenten, die am Aufbau und der Pflege dieser Vertrauensbeziehungen beteiligt sind, heißt PKI.

- **Public-Key-Technologie**

Technologie zum Sichern digitaler Dokumente.

Die Public-Key-Technologie verwendet Schlüsselpaare. Jeder Teilnehmer erhält ein einzigartiges Schlüsselpaar, das aus einem öffentlichen und einem privaten Schlüssel besteht. Die beiden Schlüssel haben folgende Eigenschaften:

- Die Schlüssel sind Paare und gehören zusammen.
- Der private Schlüssel kann nicht aus dem öffentlichen Schlüssel abgeleitet werden.
- Wie der Name schon sagt, wird der öffentliche Schlüssel veröffentlicht. Der Besitzer der Schlüssel verteilt den öffentlichen Schlüssel nach Bedarf. Der Empfänger eines signierten Dokuments muß diesen Schlüssel kennen, um die digitale Signatur prüfen zu können. Um ein verschlüsseltes Dokument versenden zu können (digitaler Umschlag), muß der Absender außerdem den öffentlichen Schlüssel des Empfängers kennen.
- Der private Schlüssel muß geheimgehalten werden. Der Schlüsselbesitzer verwendet den privaten Schlüssel zum Generieren seiner digitalen Signatur sowie zum Entschlüsseln von Nachrichten, die mit einem digitalen Umschlag geschützt sind. Daher muß der Schlüsselbesitzer sicherstellen, daß **kein** Unbefugter auf den privaten Schlüssel zugreifen kann.

- **Public-Key-Zertifikat**

Ein digitales Dokument, das die notwendigen Informationen zur Identifizierung seines Besitzers sowie zur Prüfung von dessen Signatur enthält. Ein Public-Key-Zertifikat enthält normalerweise folgende Informationen:

- Allgemeine Informationen
 - Version
 - Seriennummer

- Gültigkeitsdauer
- Information über den Zertifikataussteller
 - Distinguished Name der CA
- Informationen über den Zertifikatbesitzer
 - Distinguished Name des Besitzers
 - öffentlicher Schlüssel des Besitzers
 - verwendeter asymmetrischer, kryptografischer Algorithmus
- digitale Signatur der CA
 - verwendeter asymmetrischer, kryptografischer Algorithmus
 - digitale Signatur der CA
- **SAP Security Library (SAPSECULIB)**

Standardsicherheitsprodukt, das mit dem SAP-System geliefert wird. Die SAPSECULIB ist eine Dynamic Link Library, die sich auf jedem Anwendungsserver befindet. Die SAPSECULIB bietet die Funktionen für den Einsatz digitaler Signaturen in SAP-Systemen. Funktionen für die Verwendung digitaler Umschläge und Verschlüsselung unterstützt sie nicht.
- **SSF-Profil**

Informationen im SAP-System über den Ort, an dem der private Teil der Public-Key-Informationen eines Benutzers oder einer Komponente (der private Schlüssel) abgelegt ist. Das SSF-Profil kann eine Datei oder eine beliebige Information sein, die die Public-Key-Informationen angibt. Die exakte Form des Profils hängt von dem von Ihnen verwendeten Sicherheitsprodukt ab.
- **System-PSE**

Die Persönliche Sicherheitsumgebung (Personal Security Environment, PSE) des SAP-Systems. Die System-PSE wird während des Installationsvorgangs von der SAPSECULIB erstellt und enthält das private Adreßbuch sowie das SSF-Profil für das SAP-System. In Release 4.5A erhält jeder Anwendungsserver seine eigene System-PSE, ab Release 4.5B erstellt das System eine einzige System-PSE, die es an alle Anwendungsserver verteilt.

Siehe auch:

SAP-Bibliothek:

- [BC - Basis → Sicherheit → Secure Store & Forward / Digitale Signaturen → Public-Key-Technologie \[Extern\]](#)

SSF-Verwaltungsarbeiten

SSF-Verwaltungsarbeiten

Bei der Verwendung der SSF-Funktionen fallen gewisse Verwaltungsarbeiten an. Wenn Sie beispielsweise ein externes Sicherheitsprodukt einsetzen, müssen Sie das Produkt auf allen Komponenten installieren, wo die SSF-Informationen benötigt werden. Sie müssen auch die Benutzer pflegen, die die digitalen Signaturen und die digitalen Umschläge benutzen sollen.

Die in diesem Abschnitt genannten Themen beschreiben die Verwaltungsarbeiten, die mit dem Einsatz von SSF in SAP-Systemen anfallen. Auch die Verwaltungs- und Pflegeaufgaben bezüglich der SAPSECULIB sind darin enthalten. Informationen über Aufgaben in Verbindung mit einem externen Sicherheitsprodukt finden Sie in der Dokumentation des Sicherheitsprodukts.

Lesen Sie dazu

- über die Standardinstallationsarbeiten bei Verwendung eines externen Sicherheitsprodukts die Abschnitte unter [SSF mit externem Sicherheitsprodukt einsetzen \[Seite 13\]](#):
 - [SSF installieren/konfigurieren: Frontends \[Seite 14\]](#)
 - [SSF installieren/konfigurieren: Anwendungsserver \[Seite 15\]](#)
 - [SSF-Benutzerinformationen pflegen \[Seite 17\]](#)
- falls Sie in Release 4.0 oder 4.5 SSF-Benutzerinformationen gepflegt haben und ein Upgrade auf ein neueres Release vorgenommen haben: [Upgrade der SSF-Benutzerinformationen von Release 4.0/4.5 \[Seite 20\]](#).
- falls Sie für die verschiedenen Anwendungen unterschiedliche Sicherheitsprodukte einsetzen: [SSF-Standardinformationen für Anwendungen definieren \[Seite 27\]](#) und [Anwendungsspezifische Informationen pflegen \[Seite 28\]](#).
- falls Sie das Standardsicherheitsprodukt SAPSECULIB (nur digitale Signaturen) verwenden, brauchen Sie keine Installations- oder Konfigurierungsarbeiten vorzunehmen. Informationen über die SAPSECULIB finden Sie unter [Verwendung des SSF-Standardsicherheitsprodukts SAPSECULIB \[Seite 21\]](#).
- zum Testen der SSF-Installation: [Die SSF-Installation testen \[Seite 31\]](#).

SSF mit externem Sicherheitsprodukt einsetzen

Wenn Sie ein externes Sicherheitsprodukt verwenden, um digitale Signaturen und Verschlüsselung in SAP-Systemen zu unterstützen, müssen Sie an jedem der Frontend-Rechner (siehe [SSF installieren/konfigurieren: Frontends \[Seite 14\]](#)) und auf den Anwendungsservern (siehe [SSF installieren/konfigurieren: Anwendungsserver \[Seite 15\]](#)) SSF installieren und konfigurieren. Auf den Frontends können Sie die SSF-Parameterwerte entweder in Umgebungsvariablen oder in der SSF-Initialisierungsdatei `ssfrfc.ini` angeben. Auf den Anwendungsservern können Sie entweder Profilparameter oder Umgebungsvariablen benutzen.



Erst ab Release 4.5 können Sie Umgebungsvariablen verwenden, um die SSF-Parameter zu definieren.

Auch auf dem Anwendungsserver müssen Sie [SSF-Benutzerinformationen pflegen \[Seite 17\]](#).

Informationen zum Testen der SSF-Installation finden Sie unter [Die SSF-Installation testen \[Seite 31\]](#).

SSF installieren/konfigurieren: Frontends

SSF installieren/konfigurieren: Frontends

1. Installieren Sie das Sicherheitsprodukt auf jedem Frontend-Rechner, auf dem die SSF-Funktionen verwendet werden sollen. Schreiben Sie den Namen und den Ort der Bibliothek des Sicherheitsprodukts auf.



Die Installationsanweisungen finden Sie in der Dokumentation des externen Sicherheitsprodukts.

2. Wenn Sie die Vorschlagswerte der folgenden SSF-Parameter ändern wollen, geben Sie deren Werte entweder in der entsprechenden Umgebungsvariablen (ab Release 4.5) oder in der Datei `ssfrfc.ini` an. Weitere Informationen über die Verwendung der Datei finden Sie unter [Die SSF-Initialisierungsdatei \[Seite 41\]](#).

Die folgende Tabelle zeigt die SSF-Parameter.

SSF-Parameter

| Parameter | Vorschlagswert | Mögliche Werte |
|---|--|--|
| SSF_LIBRARY_PATH [Seite 36] | Die Standardbibliothek ist die SAPSECULIB-Bibliothek <code>libssfso.<ext></code> . Standardmäßig sucht das System diese Datei in dem Verzeichnis, in dem sich das ausführbare Programm <code>ssfrfc.exe</code> befindet. | Zeichenfolge von bis zu 255 Zeichen Namen und Ort der Datei finden Sie in Ihrem Sicherheitsprodukt. |
| SSF_MD_ALG [Seite 37] | MD5 | MD2, MD4, MD5, SHA1, RIPEMD160 Andere mögliche Werte finden Sie in Ihrem Sicherheitsprodukt. |
| SSF_SYMENCR_ALG [Seite 38] | DES-CBC | DES-CBC, TRIPLE-DES, IDEA Andere mögliche Werte finden Sie in Ihrem Sicherheitsprodukt. |
| SSF_TRACE_LEVEL [Seite 39] | 0 | 0, 1, 2, 3 |



Beachten Sie, daß der Parameter `SSF_LIBRARY_PATH` sowohl den Pfad als auch den Dateinamen der SSF-Bibliothek enthalten muß.

SSF installieren/konfigurieren: Anwendungsserver

1. Installieren Sie das Sicherheitsprodukt auf jedem der Anwendungsserver. Schreiben Sie den Namen und den Ort der Bibliothek des Sicherheitsprodukts auf.



Die Installationsanweisungen finden Sie in der Dokumentation des externen Sicherheitsprodukts.

2. Geben Sie die SSF-Parameter auf dem Anwendungsserver entweder in den Profilparametern `ssf<x>/...` oder (ab Release 4.5) in den Umgebungsvariablen `SSF<x>_...` an.



Ab Release 4.5B können Sie bis zu drei verschiedene Sicherheitsprodukte installieren. Dies könnte notwendig sein, wenn verschiedene Anwendungen unterschiedliche Sicherheitsprodukte verwenden. Daher verwendet jedes Produkt einen eigenen Satz Profilparameter. Definieren Sie die Parameter für die Anzahl Ihrer Sicherheitsprodukte. Siehe auch [Anwendungsspezifische Informationen pflegen \[Seite 28\]](#).

Die Tabelle zeigt die Profilparameter des Anwendungsservers.

SSF-Profilparameter

| Parameter | Vorschlagswert | Mögliche Werte |
|---|--|--|
| Produkt 1: <code>ssf/ssfapi_lib</code> Produkt 2: <code>ssf2/ssfapi_lib</code> Produkt 3: <code>ssf3/ssfapi_lib</code> | Leer – d. h. das System verwendet die SAPSECULIB. (Siehe Hinweis unten.) | Zeichenfolge von bis zu 255 Zeichen Namen und Ort der Datei finden Sie in Ihrem Sicherheitsprodukt. |
| Produkt 1: <code>ssf/ssf_md_alg</code> Produkt 2: <code>ssf2/ssg_md_alg</code> Produkt 3: <code>ssf3/ssg_md_alg</code> | MD5 | MD2, MD4, MD5, SHA1, RIPEMD160 Andere mögliche Werte finden Sie in Ihrem Sicherheitsprodukt. |
| Produkt 1: <code>ssf_symencr_alg</code> Produkt 2: <code>ssf2_symencr_alg</code> Produkt 3: <code>ssf3_symencr_alg</code> | DES-CBC | DES-CBC, TRIPLE-DES, IDEA Andere mögliche Werte finden Sie in Ihrem Sicherheitsprodukt. |

SSF installieren/konfigurieren: Anwendungsserver

| | | |
|-----------------------------------|-----------------|--|
| Produkt 1: <code>ssf/name</code> | Produkt 1: SSF | Zeichenfolge von bis zu 10 Zeichen (Groß- und Kleinschreibung wird berücksichtigt) |
| Produkt 2: <code>ssf2/name</code> | Produkt 2: SSF2 | |
| Produkt 3: <code>ssf3/name</code> | Produkt 3: SSF3 | |



Beim Start eines Anwendungsservers lädt das System stets das Sicherheitsprodukt SAPSECULIB und ordnet die SAPSECULIB-Informationen dem nächsten verfügbaren Parametersatz `ssf<x>/...` zu.

Standardmäßig sucht das System die SAPSECULIB-Bibliothek (`libssfso`) in dem in Profilparameter `DIR_LIBRARY` angegebenen Verzeichnis. Falls notwendig, können Sie in dem entsprechenden Parameter `ssf<x>/ssfapi_lib` (oder in der Umgebungsvariablen `SSF<x>_LIBRARY_PATH`) einen anderen Dateinamen und -ort der SAPSECULIB-Bibliothek angeben. Wenn Sie davon Gebrauch machen, vergewissern Sie sich, daß der entsprechende Parameter `ssf<x>/name` (oder die Umgebungsvariable `SSF<x>_NAME`) den Namen SAPSECULIB enthält.

- Um SSF-Aktivitäten für Trace-Funktionen aufzuzeichnen, setzen Sie die Umgebungsvariable `SSF_TRACE_LEVEL` auf einen der folgenden Werte:

SSF-Trace-Stufen

| Trace-Stufe | Das System zeichnet folgendes auf: |
|-------------|---|
| 0 | <ul style="list-style-type: none"> den Start des SSF-RFC-Servers das Laden der SSF-Bibliothek die Installation der RFC-fähigen SSF-Funktionen |
| 1 | <ul style="list-style-type: none"> Informationen wie in Trace-Stufe 0 den Namen und Rückgabewert der aufgerufenen SSF-Funktionen |
| 2 | <ul style="list-style-type: none"> Informationen wie in Trace-Stufe 0 und 1 Informationen über den Unterzeichner und den Empfänger, wenn SSF-Funktionen aufgerufen werden |
| 3 | <ul style="list-style-type: none"> Informationen wie in Trace-Stufe 0, 1 und 2 alle Eingabe- und Ausgabedaten, wenn SSF-Funktionen aufgerufen werden |

Das System zeichnet die Trace-Informationen in der Datei `dev_ssf<#>` auf (wobei # die Nummer ist, die jeder Trace-Datei zugewiesen wird).

- Führen Sie alle möglicherweise erforderlichen anwendungsspezifischen Aufgaben durch. Weitere Informationen finden Sie in der Dokumentation der Anwendung.

SSF-Benutzerinformationen pflegen

Auf welche Art und Weise Sie die SSF-Benutzerinformationen pflegen müssen, hängt von Ihrem Release ab.

- **Release 4.0/4.5**

In Release 4.0 müssen Sie die Customizing-Aktivität *SSF-Information zum Benutzer pflegen* (Transaktion O07C) zur Eingabe der SSF-Benutzerinformationen verwenden.

Siehe auch:

- [Besondere Information zu Release 4.0/4.5 \[Seite 43\]](#)

- **Ab Release 4.6**

Ab Release 4.6 pflegen Sie die Informationen in der Standardtabelle für Benutzeradressinformationen.

Informationen finden Sie unter

- [SSF-Benutzerinformationen pflegen: Release 4.6+ \[Seite 18\]](#)

- **Upgrade von Release 4.0/4.5**

Wenn Sie ein Upgrade auf Release 4.6 vorgenommen haben und zuvor die SSF-Benutzerinformationen mit Transaktion O07C gepflegt haben, müssen Sie nun die Customizing-Aktivität *Upgrade der SSF-Benutzerinformationen von Release 4.0/4.5* benutzen, um die SSF-Informationen in die Benutzeradressinformationen zu migrieren.

Siehe auch:

- [Upgrade der SSF-Benutzerinformationen von Release 4.0/4.5 \[Seite 20\]](#)

SSF-Benutzerinformationen pflegen: Release 4.6+

SSF-Benutzerinformationen pflegen: Release 4.6+

Verwendung

Ab Release 4.6 sind die SSF-Informationen in der Standardtabelle für Benutzeradreßinformationen enthalten.

Zur Pflege der SSF-Informationen der Benutzer verwenden Sie die entsprechende in der folgenden Tabelle angegebene Transaktion.

Pflegeaktionen für die Benutzeradreßinformationen

| Transaktion | Verantwortlicher | Aufgabe |
|-------------|------------------|---|
| SU01 | Systemverwalter | Anlegen und Pflegen der Benutzerstammsätze aller Benutzer, einschließlich der SSF-Informationen zum Benutzer. |
| SO12 | Office-Verwalter | Pflege der Office-Informationen der Benutzer, einschließlich der SSF-Benutzerinformationen für die Verwendung digitaler Signaturen. |
| SU3 | Benutzer | Pflegen der eigenen Adreßinformationen, einschließlich der SSF-Informationen für das Empfangen verschlüsselter Daten. |

Voraussetzungen

Das Sicherheitsprodukt wurde installiert und SSF wurde auf dem Anwendungsserver konfiguriert (siehe [SSF installieren/konfigurieren: Anwendungsserver \[Seite 15\]](#)).

Der Ort des SSF-RFC-Serverprogramms `ssrfrc` muß auch als RFC-Destination `SAP_SSFATGUI` in Transaktion SM59 definiert werden.

Vorgehensweise

1. Rufen Sie eine der Pflegeaktionen für Benutzeradressen auf.
2. Wählen Sie in den Benutzeradreßinformationen *Weitere Kommunikation*.
3. Markieren Sie den *Kommunikationstyp SSF*.
4. Geben Sie in den entsprechenden Feldern die folgenden SSF-Informationen ein:

SSF-Informationen zum Benutzer

SSF-Benutzerinformationen pflegen: Release 4.6+

| Feld | Verfügbar über Transaktion | | | Beschreibung | Kommentar |
|--------------------|----------------------------|------|-----|--|---|
| | SU01 | SO12 | SU3 | | |
| <i>SSF-ID</i> | X | X | X | SSF-Benutzername | Die Syntax des SSF-Benutzernamens wird von dem von Ihnen verwendeten Sicherheitsprodukt bestimmt. |
| <i>Profil</i> | X | | X | Profilname | Gibt das Profil an, in dem die Sicherheitsinformationen des Benutzers abgelegt sind. Der Wert dieses Parameters wird ebenfalls von dem von Ihnen verwendeten Sicherheitsprodukt bestimmt. |
| <i>Destination</i> | X | | X | Die RFC-Destination (logische Destination), wo das SSF-RFC-Serverprogramm definiert wurde. | Siehe Eingabehilfe (F4). Vorschlagswert = SAP_SSFATGUI (SSF für digitale Signaturen an den Frontends) |



Sie können nur Felder pflegen, die in der speziellen Pflgetransaktion zur Verfügung stehen (siehe Spalte *Verfügbar über Transaktion* in der obigen Tabelle). Unzutreffende Felder werden nicht angezeigt. Beispielsweise kann der Office-Verwalter mit Transaktion SO12 nicht das individuelle SSF-Profil eines Benutzers ändern.

5. Sichern Sie Ihre Eingabe.

Upgrade der SSF-Benutzerinformationen von Release 4.0/4.5

Upgrade der SSF-Benutzerinformationen von Release 4.0/4.5

Ab Release 4.6 befindet sich die Pflege der SSF-Benutzerinformationen in der Standardtabelle für die Benutzeradressenpflege. In Release 4.0 und 4.5 wurden die SSF-Benutzerinformationen in Tabelle TC70 abgelegt, ab Release 4.6 sind diese Informationen in Tabelle ADR11 abgelegt.

Wenn Sie die SSF-Benutzerinformationen in Release 4.0 oder 4.5 gepflegt haben und ein Upgrade auf ein neueres Release vornehmen wollen, finden Sie Informationen dazu unter der Customizing-Aktivität in *BC - Basis* → *Sicherheit* → *Digitale Signaturen* → *Upgrade der SSF-Benutzerinformationen von Release 4.0/4.5*.

Diese Aktivität führt den Report RSADR7C70TOADR11 aus, der die SSF-Benutzerinformationen von Tabelle TC70 in Tabelle ADR11 verschiebt.

Beachten Sie, daß diese Aktivität mandantenunabhängig ist. Damit werden die SSF-Informationen der Benutzer in allen Mandanten des SAP-Systems übernommen.

Verwendung des SSF-Standardsicherheitsprodukts SAPSECULIB

Wir liefern SAP-Systeme mit dem SSF-Standardsicherheitsprodukt SAPSECULIB. Die SAPSECULIB bietet Funktionen zum Erstellen und Prüfen digitaler Signaturen, die innerhalb des SAP-Systems verwendet werden. Sie bietet keine Unterstützung für digitale Umschläge, Smartcard-Authentifizierung oder kryptografische Hardware. Wenn Sie eine vollständige SSF-Unterstützung wünschen, benötigen Sie ein externes Sicherheitsprodukt.

Normalerweise brauchen Sie keine Verwaltungsarbeiten vornehmen, wenn Sie SAPSECULIB als Sicherheitsprodukt verwenden. Allerdings könnten die Informationen in den nachfolgenden Abschnitten bei Problemen oder bei der Überwachung des Status der SAPSECULIB-Komponenten hilfreich sein.

SAP Security Library (SAPSECULIB)

SAP Security Library (SAPSECULIB)

Definition

Die SAP Security Library (SAPSECULIB) ist das Standardsicherheitsprodukt für die SSF-Mechanismen.

Verwendung

Die SAPSECULIB bietet die Funktionen, mit denen innerhalb der SAP-Systeme digitale Signaturen erstellt und geprüft werden können.

Integration

Die SAPSECULIB ist Teil der Standardinstallation des SAP-Systems. Während des Installationsvorgangs generiert das System mit der SAPSECULIB für jeden Anwendungsserver eine [Persönliche Sicherheitsumgebung \(Personal Security Environment, PSE\) \[Seite 9\]](#), die [System-PSE \[Seite 9\]](#). Der Anwendungsserver kann dann die in der PSE enthaltenen Informationen verwenden, um Dokumente digital zu signieren und die digitalen Signaturen anderer Komponenten zu prüfen.



In Release 4.5A generiert das System für jeden Anwendungsserver eine individuelle System-PSE.

Ab Release 4.5B generiert das System eine einzige System-PSE und verteilt sie an alle Anwendungsserver.

Die System-PSE wird während des Installationsvorgangs erzeugt und befindet sich in der folgenden Datei in Verzeichnis `<Instanzverzeichnis>/sec`:

- Release 4.5A `SAPSECU.pse`
- ab Release 4.5B `SAPSYS.pse`



Wenn Sie ein Upgrade von Release 4.5A auf ein neueres Release durchführen, legt das System eine neue System-PSE namens `SAPSYS.pse` an, die Datei `SAPSECU.pse` wird jedoch nicht entfernt oder umbenannt. Denken Sie daran, daß das System eventuell auf die alte PSE zugreifen muß, um digitale Signaturen zu prüfen, die vor dem Upgrade erzeugt wurden.

Bei jedem Neustart eines Anwendungsservers stellt das System automatisch sicher, daß das Unterverzeichnis `sec` vorhanden ist und die System-PSE des Servers enthält. In Release 4.5 generiert das System automatisch eine neue System-PSE, wenn es beim Systemstart keine PSE vorfindet. Ab Release 4.6 vergibt das System, falls eine System-PSE vorhanden ist, diese an den Anwendungsserver. Ist in der Datenbank keine System-PSE vorhanden, generiert das System eine neue, die von allen Anwendungsservern verwendet wird.

Wenn Sie für einen Anwendungsserver eine neue PSE anlegen müssen, nachdem der Installationsvorgang bereits abgeschlossen ist, finden Sie Informationen dazu unter [System-PSE pflegen \[Seite 24\]](#).

**Nur für UNIX-Plattformen:**

Damit das System die SAP Security Library beim Start des Anwendungsservers laden kann, müssen Sie sicherstellen, daß die UNIX-Umgebungsvariable für das Laden gemeinsam genutzter Bibliotheken den im Profilparameter `DIR_LIBRARY` des SAP-Systems genannten Pfad enthält (z. B. `/usr/sap/<SID>/SYS/exe/run`). Stellen Sie sicher, daß die Umgebungsvariable in der Benutzerumgebung für das Benutzerkonto gesetzt ist, unter dem der Anwendungsserver läuft (z. B. `<sid>adm`). Die entsprechenden UNIX-Umgebungsvariablen sind:

- `LD_LIBRARY_PATH`: Solaris, Sinix, OSF/1, Reliant UNIX, Digital UNIX
- `SHLIB_PATH`: HP-UX
- `LIBPATH`: AIX

Die System-PSE pflegen

Die System-PSE pflegen

Verwendung

Die Pflege der System-PSE ist ab Release 4.5B verfügbar.

Mit der PSE-Pflege pflegen und überwachen Sie die System-PSEs.

Sie können

- eine neue System-PSE generieren und an die Anwendungsserver verteilen
- eine lokale PSE importieren und als System-PSE an alle Anwendungsserver verteilen
- die PIN (Personal Identification Number) ändern, die die System-PSE schützt
- [Credentials \[Seite 9\]](#) (Zugriffsberechtigung) für die System-PSE erstellen

Vorgehensweise

1. Mit Transaktion PSEMAINT greifen Sie auf die PSE-Pflege zu.

Das Bild *PSE-Management* zeigt die Status aller Anwendungsserver-PSEs.

Es gibt folgende Status:

– RFC

Es gibt folgende Status der RFC-Verbindung zum Anwendungsserver:

- ok
- fehlerhaft
- warte ...

– PSE-Status

Es gibt folgende SSF- und PSE-Status:

- PSE & SSF OK
Dieser Status zeigt an, daß die System-PSE für den Anwendungsserver installiert wurde und zugreifbar ist.
- SSF fehlerhaft
Dieser Status zeigt an, daß auf dem Anwendungsserver ein externes Sicherheitsprodukt installiert wurde und eine System-PSE vorhanden ist; allerdings kann auf die System-PSE nicht zugegriffen werden. Die häufigste Ursache für diesen Fehler ist, daß auf dem Anwendungsserver keine Credentials (Zugriffsberechtigung) vorliegen. Mit der Funktion *Credentials erzeugen* beheben Sie diesen Fehler.
- Kein Sicherheitsprodukt
Dieser Status zeigt an, daß die SAPSECULIB nicht installiert wurde.
- lokale PSE fehlt

Die System-PSE pflegen

Dieser Status zeigt an, daß auf dem Anwendungsserver keine System-PSE vorhanden ist. Mit *PSE erzeugen* oder *PSE importieren* beheben Sie diesen Fehler.

- PSE fehlerhaft

Dieser Fehler zeigt an, daß die PSE-Version auf dem Anwendungsserver nicht mit der in der Datenbank abgelegten Version übereinstimmt. Mit *PSE erzeugen* oder *PSE importieren* beheben Sie diesen Fehler.

2. Plazieren Sie den Cursor auf dem Anwendungsserver, auf dem Sie die jeweilige Funktion ausführen wollen, und wählen Sie den entsprechenden Menüeintrag.

Die nachfolgende Tabelle zeigt, welche Funktionen Sie ausführen können.

PSE-Pflegefunktionen

| Funktion | Menüpfad | Wissenswertes |
|--|--|---|
| Generieren einer neuen System-PSE, die an die Anwendungsserver verteilt wird | → <i>PSE</i> → <i>Erzeugen</i> | Diese Funktion legt auf dem ausgewählten Anwendungsserver eine neue PSE an, importiert sie in die Datenbank und verteilt sie an alle übrigen Anwendungsserver. Bereits vorhandene PSEs werden überschrieben. |
| Importieren einer lokalen PSE, die als System-PSE an alle Anwendungsserver verteilt wird | → <i>PSE</i> → <i>Importieren</i> | Diese Funktion importiert eine lokale PSE in die Datenbank und verteilt sie an alle Anwendungsserver. Bereits vorhandene PSEs werden überschrieben. |
| Ändern der PIN, die die System-PSE schützt | → <i>PSE</i> → <i>PIN ändern</i> | Die Standardsystem-PSE wird nicht über eine PIN geschützt. Wir empfehlen, daß Sie zum Schutz der PSE eine PIN zuweisen. |
| Credentials (Zugriffsberechtigung) für die System-PSE erstellen | → <i>PSE</i> → <i>Credentials erzeugen</i> | Der Anwendungsserver benötigt Credentials, um auf seine System-PSE zugreifen zu können. Obwohl normalerweise für einen Anwendungsserver Credentials vorhanden sind, müssen Sie gelegentlich neue anlegen, z. B. für einen neu konfigurierten Anwendungsserver, der noch nicht auf seine System-PSE zugegriffen hat. |
| Funktion | Drucktaste | Wissenswertes |

Die System-PSE pflegen

Ändern der Liste, der für die Verifikation zu verwendenden Zertifikate

 *Zertifikatsliste*

Mit dieser Funktion können Sie eine Liste der Public-Key-Zertifikate pflegen, die vom System zur Verifikation der digitalen Signatur anderer Benutzer oder anderer Systemkomponenten verwendet werden können.

Exportieren einer Version der System-PSE, die von anderen zur Verifikation der digitalen Signatur des Systems verwendet werden kann

 *Verifikations-PSE*

Diese PSE enthält nur die öffentlichen Informationen der System-PSE (z. B. das Public-Key-Zertifikat und den öffentlichen Schlüssel des Systems). Diese Informationen können an andere verteilt werden, um die digitalen Signaturen des Systems zu verifizieren.

Ausstellen einer Zertifikatanforderung an die SAP-CA

 *Zertifikatsrequest*

Mit dieser Funktion werden das Public-Key-Schlüsselpaar und ein Public-Key-Zertifikat erzeugt. Das Public-Key-Zertifikat wird dann zum Signieren an die SAP-CA gesendet.

Einfügen der Antwort der SAP-CA auf die Zertifikatanforderung

 *Zertifikatsrequest*

Mit dieser Funktion importieren Sie die erhaltene Antwort (unterzeichnetes Public-Key-Zertifikat) in das System.

SSF-Standardinformationen für Anwendungen definieren

Verwendung

Mit diesem Verfahren definieren Sie einen Vorschlagssatz SSF-Informationen, die Anwendungen anstelle der Vorschlagswerte des Systems verwenden sollen.

Die nachfolgende Tabelle zeigt die Systemvorschlagswerte.

Systemvorschlagswerte für SSF-Informationen

| SSF-Information | Vorschlagswert | Kommentar |
|-----------------------------|--|---|
| Sicherheitsprodukt | Das Produkt, dessen Bibliothek im SSF-Profilparameter <code>ssf/ssfapi_lib</code> enthalten ist. | Der Vorschlagswert dieses Parameters ist die SAPSECULIB-Bibliothek <code>libssfso</code> . Während des Konfigurierens von SSF können Sie den Wert dieses Parameters ändern. Siehe SSF installieren/konfigurieren: Anwendungsserver [Seite 15] . |
| Name des Sicherheitsprodukt | Der in Profilparameter <code>ssf/name</code> angegebene Name des Sicherheitsprodukts. | <code>ssf/name</code> entspricht dem in <code>ssf/ssfapi_lib</code> angegebenen Produkt. |
| SSF-Format | PKCS#7 | Derzeit wird nur das Format PKCS#7 unterstützt. |
| Privates Adreßbuch | <Instanzverzeichnis>/ <code>sec/SAPSYS.pse</code> | Dies ist der Ort, an dem sich die mit SAPSECULIB gelieferte PSE befindet, wobei das <Instanzverzeichnis> durch Profilparameter <code>DIR_INSTANCE</code> definiert ist. |

Voraussetzungen

In Profilparameter `ssf<x>/ssfapi_lib` muß der Name und der Ort der Bibliothek des Produkts angegeben werden. Geben Sie den Namen des Produkts in Profilparameter `ssf<x>/name` an.

Vorgehensweise

In der Vorgehensweise [Anwendungsspezifische Informationen pflegen \[Seite 28\]](#), legen Sie den **Standardwerte**-Eintrag in der Dropdown-Liste *Anwendung* an oder ändern ihn dort.

Ergebnis

Das System verwendet anstelle der Systemvorschlagswerte die Werte, die Sie im Eintrag **Standardwerte** als Vorschlagswerte für die SSF-Informationen angeben.

Anwendungsspezifische Informationen pflegen

Anwendungsspezifische Informationen pflegen

Verwendung

Mit diesem Verfahren geben Sie anwendungsspezifische Informationen an, z. B. wenn Sie für die Verwendung der SSF-Funktionen mehr als ein Sicherheitsprodukt benutzen oder wenn Sie zwar dasselbe Produkt aber für verschiedene Anwendungen unterschiedliche [SSF-Profil](#) [Seite 9] oder [private Adreßbücher](#) [Seite 9] verwenden.



Wenn Sie beispielsweise die Schnittstelle ArchiveLink II HTTP Content Server 4.5 verwenden, die als Sicherheitsprodukt die SAPSECULIB zum Signieren von Ablageaufträgen benutzt, und Sie zum Erstellen digitaler Signaturen in einer anderen Anwendung ein externes Sicherheitsprodukt einsetzen, müssen Sie für jede Anwendung SSF-Informationen angeben.

Voraussetzungen

Die Sicherheitsprodukte wurden auf allen Anwendungsservern installiert.

Die SSF-Profilparameter (oder Umgebungsvariablen) `ssf<x>/name` und `ssf<x>/ssfapi_lib` enthalten die Namen der Sicherheitsprodukte sowie die Namen und Orte der Bibliotheken der Sicherheitsprodukte.

Vorgehensweise

- Um auf die SSF-Informationen bestimmter Anwendungen zuzugreifen, rufen Sie Transaktion SSFA auf.
 - Ist nur ein Eintrag vorhanden, zeigt das System ihn an. Ansonsten zeigt es eine Tabelle aller vorhandenen Einträge an.
- Ist schon ein Eintrag für die Anwendung vorhanden und Sie wollen ihn ändern, markieren Sie ihn und wählen Sie *Springen* → *Detail*. Ansonsten können Sie folgendermaßen einen Eintrag anlegen:
 - Wählen Sie *Bearbeiten* → *Neue Einträge*.
 - Wählen Sie den Anwendungsnamen aus der Dropdown-Liste und drücken Sie die *Return*-Taste. (Wählen Sie den Eintrag **Standardwerte** oder legen Sie ihn an, um einen Vorschlagseintrag für Anwendungen zu erstellen. Weitere Informationen finden Sie unter [SSF-Standardinformationen für Anwendungen definieren](#) [Seite 27].)
 - Sie gelangen auf das Bild zur Pflege des Eintrags.
- Geben Sie in den entsprechenden Feldern die folgenden Informationen ein.

Anwendungsspezifische SSF-Pflegefelder

Anwendungsspezifische Informationen pflegen

| Feld | Wert | Kommentar |
|-------------------------|--------------------------------------|---|
| <i>Sicherheitsprod.</i> | Name des Sicherheitsprodukts | Der Name des Produkts muß dem in einem der Profilparameter <code>ssf<x>/name</code> angegebenen Namen entsprechen. Das System verwendet dann die im entsprechenden Profilparameter <code>ssf<x>/ssfapi_lib</code> angegebene Bibliothek für die Anwendung. |
| <i>SSF-Format</i> | PKCS#7 | Derzeit wird nur dieses Format unterstützt. |
| <i>Priv.Adr.Buch</i> | Name und Ort des privaten Adreßbuchs | Das private Adreßbuch enthält die öffentlichen Schlüssel der Benutzer und der Komponenten. Der Name und Ort des privaten Adreßbuchs wird von dem Sicherheitsprodukt bestimmt, das Sie verwenden. |
| <i>Profilname</i> | Name und Ort des SSF-Profiles | Das SSF-Profil enthält die gesamten Sicherheitsinformationen der Benutzer und der Komponenten (z. B. die privaten Schlüssel). Der Name und Ort des SSF-Profiles wird von dem Sicherheitsprodukt bestimmt, das Sie verwenden. |



Die Anwendung legt fest, welche Informationen Sie für diese Anwendung pflegen können. Daher werden nur die für die Anwendung benötigten Felder angezeigt.



Wenn Sie ein Eingabefeld frei lassen, verwendet die Anwendung den Vorschlagswert. Der Vorschlagswert wird entweder im Vorschlagseintrag festgelegt oder, falls kein Vorschlagseintrag definiert wurde, werden die Systemvorschlagswerte verwendet. (Weitere Informationen finden Sie unter [SSF-Standardinformation für Anwendungen definieren \[Seite 27\]](#).) Die derzeit definierten Vorschlagswerte werden im unteren Abschnitt des Pflegebildes angezeigt.

4. Wählen Sie *Zertifikate bei Daten*, falls
 - a. den digitalen Signaturen der Benutzer oder Komponenten deren Zertifikate beigefügt werden sollen oder
 - b. Zertifikate zur Überprüfung digitaler Signaturen verwendet werden sollen

Anwendungsspezifische Informationen pflegen

5. Wählen Sie *nur dig. Signatur*, falls die signierten Daten nicht der digitalen Unterschrift beigefügt werden sollen.
6. Sichern Sie Ihre Eingabe.

Die SSF-Installation testen

Verwendung

Nach der Installation von SSF können Sie mit den Reports SSF01 und SSF02 sicherstellen, daß das Sicherheitsprodukt korrekt installiert wurde. Mit SSF01 testen Sie die Installation auf dem Frontend und mit SSF02 die Installation auf dem Anwendungsserver.

Vorgehensweise

1. Rufen Sie Transaktion SE38 auf.
2. Um die SSF-Installation auf den Frontends zu testen, geben Sie im Feld *Programm* **SSF01** ein; um SSF auf dem Anwendungsserver zu testen, geben Sie **SSF02** ein.
3. Wählen Sie *Programm* → *Ausführen* → *Direkt*.

Das System zeigt ein Funktionsauswahlfeld mit den Funktionen, die Sie testen können.

4. Wählen Sie die Funktion *Version ermitteln*.
5. Wenn Sie die Version für ein bestimmtes Sicherheitsprodukt testen wollen, geben Sie dessen Namen (wie in Profilparameter `ssf<x>/name` angegeben) in das Feld *Sicherheitsprodukt* der Gruppe *Weitere Optionen* ein.



Die anderen Optionen und Felder sind für diesen Test ohne Bedeutung.

6. Wählen Sie *Programm* → *Ausführen*.

Das System zeigt die Testergebnisse an. Sofern der Test erfolgreich war, zeigt es den Rückgabewert `SSF_API_OK` sowie die Versionsinformationen des Sicherheitsprodukts an. Am Frontend gibt es außerdem noch die Version des SSF-RFC-Serverprogramms an. Wenn das System auf einen Fehler stieß, zeigt es eine Fehlermeldung.



Falls Sie als Sicherheitsprodukt die SAPSECULIB verwenden, führt der Test am Frontend (Report SSF01) zu einem Fehlercode. (SAPSECULIB ist nur auf dem Anwendungsserver installiert.)

Es kann folgende Rückgabewerte geben:

Fehlercodes im SSF-Testprogramm

| Fehlercode | Betrifft* | Definition | Vorgehen |
|------------|-----------|--------------------------|----------|
| SSF_API_OK | FE / AS | Es trat kein Fehler auf. | |

Die SSF-Installation testen

| | | | |
|------------------|---------|--|--|
| SSF_RFC_ERROR | FE | RFC-Destination ist nicht korrekt definiert oder das System kann das SSF-RFC-Serverprogramm <code>ssfrfc.exe</code> nicht starten. | <p>Verwenden Sie Transaktion SM59. Vergewissern Sie sich, daß die RFC-Destination <code>SAP_SSFATGUI</code> als TCP/IP-Destination definiert ist. Testen Sie die Verbindung in SM59.</p> <p>Vergewissern Sie sich, daß die Datei <code>ssfrfc.exe</code> am richtigen Ort liegt. (Bei einer Standardinstallation sollte sie sich im SAP-GUI-Verzeichnis befinden.)</p> |
| SSF_API_NO_SECTK | FE / AS | Das Sicherheitsprodukt wurde nicht korrekt installiert. | <p>Stellen Sie sicher, daß der <code>SSF_LIBRARY_PATH</code> (oder <code>ssf/ssfapi_lib</code>) korrekt eingestellt ist.</p> <p>Setzen Sie die Trace-Stufe auf 1 und prüfen Sie den Inhalt der Trace-Datei <code>dev_ssf</code>.</p> |

*FE = Frontend-Rechner; AS = Anwendungsserver

SSF-Parameter

Die folgenden Parameter definieren die SSF-Konfiguration an den Frontends und den Anwendungsservern:

SSF-Parameter

| Parameter | Beschreibung |
|---|---|
| SSF_LIBRARY_PATH [Seite 36] | Pfad und Dateiname der SSF-Bibliothek |
| SSF_MD_ALG [Seite 37] | kryptografischer Hash-Algorithmus |
| SSF_SYMCNCR_ALG [Seite 38] | symmetrischer Verschlüsselungsalgorithmus |
| SSF_TRACE_LEVEL [Seite 39] | Trace-Stufe zum Aufzeichnen der SSF-Aktivitäten |
| SSF_NAME [Seite 40] (ab Release 4.5B) | Name des Sicherheitsprodukts (nur für Anwendungsserver) |

Eine vollständige Beschreibung und die Standardwerte der einzelnen Parameter finden Sie in der Dokumentation dieser Parameter.

SSF-Parameter an Frontend-Rechnern definieren

An den Frontends können Sie die SSF-Parameter entweder in Umgebungsvariablen (ab Release 4.5A) oder in der SSF-Initialisierungsdatei `ssfRFC.ini` angeben. Weitere Informationen über die Verwendung von `ssfRFC.ini` finden Sie unter [Die SSF-Initialisierungsdatei \[Seite 41\]](#).

Die Einträge in der SSF-Initialisierungsdatei setzen die der Umgebungsvariablen außer Kraft. Falls weder in den Umgebungsvariablen noch in der Datei `ssfRFC.ini` Einträge vorhanden sind, verwendet das System die Vorschlagswerte.

SSF-Parameter auf den Anwendungsservern definieren

Auf den Anwendungsservern können Sie SSF-Informationen entweder über Umgebungsvariable (ab Release 4.5A) oder Profilparameter angeben. Die Werte der Profilparameter setzen die der Umgebungsvariablen außer Kraft. Wenn Sie keine der beiden Möglichkeiten nutzen, verwendet das System die Vorschlagswerte.

SSF-Parameter bei Verwendung mehrerer Sicherheitsprodukte definieren (nur für Anwendungsserver)

Ab Release 4.5B können Sie für unterschiedliche Anwendungen bis zu drei verschiedene Sicherheitsprodukte verwenden. Um zwischen den SSF-Parametern der einzelnen Anwendungen zu unterscheiden, gibt es drei Sätze SSF-Parameter, die Sie auf den Anwendungsservern definieren können. Die Parametersätze haben folgende Syntax:

- **Umgebungsvariable:**
 - Produkt 1: SSF_...
 - Produkt 2: SSF2_...
 - Produkt 3: SSF3_...
- **Profilparameter:**

SSF-Parameter

- Produkt 1: ssf/...
- Produkt 2: ssf2/...
- Produkt 3: ssf3/...



Allerdings können Sie nur auf den Anwendungsservern mehrere Sicherheitsprodukte installieren. Auf den Frontends können Sie nur ein einziges Produkt konfigurieren.



Zur Erstellung digitaler Signaturen verwendet die Schnittstelle SAP ArchiveLink II HTTP Content Server 4.5 als Sicherheitsprodukt SAPSECULIB. Im Qualitätsmanagement wird zum Signieren der Prüflose ein externes Sicherheitsprodukt <Produkt> verwendet, das zum Erstellen digitaler Signaturen auch einen anderen Hash-Algorithmus als die SAPSECULIB verwendet. Die folgenden Definitionen für die Profilparameter der Anwendungsserver geben für jede dieser Anwendungen andere Werte an.

Beispiel für Profilparameter der Anwendungsserver bei Verwendung unterschiedlicher Produkte**Anwendung: Schnittstelle SAP ArchiveLink II HTTP Content Server 4.5****Produkt: SAPSECULIB**

| Parameter | Wert |
|----------------|---|
| ssf/ssfapi_lib | Name und Ort der SAPSECULIB-Bibliothek libssfso |
| ssf/name | SAPSECULIB |
| ssf/ssf_md_alg | MD5 |

Anwendung: Qualitätsmanagement**Produkt: <Produkt>**

| Parameter | Wert |
|-----------------|--|
| ssf2/ssfapi_lib | Name und Ort der Bibliothek des Produkts |
| ssf2/name | <Produkt> |
| ssf2/ssf_md_alg | SHA1 |

Verwenden Sie außerdem Transaktion SSFA, um das <Produkt> für die Anwendung **Qualitätszeugnisabwicklung** anzugeben. Weitere Informationen finden Sie unter [Anwendungsspezifische Informationen pflegen \[Seite 28\]](#).

Die einzelnen Parameter werden in den folgenden Abschnitten beschrieben.

SSF_LIBRARY_PATH

SSF_LIBRARY_PATH

| | |
|---|---|
| Umgebungsvariablen- oder Initialisierungsdateieintrag: | Produkt 1: SSF_LIBRARY_PATH Produkt 2: SSF2_LIBRARY_PATH Produkt 3: SSF3_LIBRARY_PATH |
| Profilparameter des Anwendungsservers: | Produkt 1: ssf/ssfapi_lib Produkt 2: ssf2/ssfapi_lib Produkt 3: ssf3/ssfapi_lib |
| Kurzbeschreibung: | Pfad und Dateiname der SSF-Bibliothek |
| Gültig für Release: | alle |
| Beschreibung: | Dieser Parameter enthält den vollständigen Pfad und Dateinamen einer externen Funktionsbibliothek für die Secure-Store-&-Forward-Funktionen. Name und Ort der Bibliothek werden von dem von Ihnen verwendeten Sicherheitsprodukt bestimmt. |
| Vorschlagswert: | libssfso.<ext> (<ext> ist die entsprechende plattformabhängige Erweiterung. Unter Windows NT ist die Erweiterung z. B. dll. Mit .XXX lassen Sie das System automatisch die richtige Erweiterung festlegen.) libssfso.<ext> ist die SAPSECULIB-Bibliothek, also das Standardsicherheitsprodukt. Bei den Frontends sucht das System libssfso.<ext> standardmäßig in dem Verzeichnis, in dem sich das ausführbare Programm ssfrfc.exe befindet. Bei einer Standardinstallation ist dies das SAP-GUI-Verzeichnis (unter Windows NT ist das z. B. C:\Programme\sappc\sapgui). Auf dem Anwendungsserver ist der Vorschlagswert für ssf/ssfapi_lib nicht ausgefüllt, d. h. das System sucht die SAPSECULIB-Bibliothek libssfso.<ext> in dem in Profilparameter DIR_LIBRARY angegebenen Verzeichnis. |
| Gültige Einträge, Formate: | Zeichenfolge von bis zu 255 Zeichen |



Die Parameter zusätzlicher Produkte können Sie nur auf den Anwendungsservern definieren.

SSF_MD_ALG

**Umgebungsvariablen-
oder
Initialisierungsdateiein-
trag:**

Produkt 1: SSF_MD_ALG
Produkt 2: SSF2_MD_ALG
Produkt 3: SSF3_MD_ALG

**Profilparameter des
Anwendungsservers:**

Produkt 1: ssf/ssf_md_alg
Produkt 2: ssf2/ssf_md_alg
Produkt 3: ssf3/ssf_md_alg

Kurzbeschreibung:

kryptografischer Hash-Algorithmus für SSF

Gültig für Release:

alle

Beschreibung:

Dieser Parameter enthält den kryptografischen Hash-Algorithmus, der zusammen mit den SSF-Funktionen zu verwenden ist. Der Algorithmus des kryptografischen Hash-Werts wird z. B. zum Erstellen digitaler Signaturen verwendet.

Sie müssen einen Algorithmus angeben, der von dem von Ihnen verwendeten Sicherheitsprodukt unterstützt wird.

Vorschlagswert:

MD5

**Gültige Einträge,
Formate:**

MD2, MD4, MD5, SHA1, RIPEMD160

Angaben zu weiteren unterstützten Algorithmen finden Sie in der Dokumentation Ihres Sicherheitsprodukts.



Die Parameter zusätzlicher Produkte können Sie nur auf den Anwendungsservern definieren.

SSF_SYMENCNCR_ALG

SSF_SYMENCNCR_ALG

| | |
|---|---|
| Umgebungsvariablen- oder Initialisierungsdateiein- trag: | Produkt 1: SSF_SYMENCNCR_ALG Produkt 2: SSF2_SYMENCNCR_ALG Produkt 3: SSF3_SYMENCNCR_ALG |
| Profilparameter des Anwendungsservers: | Produkt 1: ssf/ssf_symencnrcr_alg Produkt 2: ssf2/ssf_symencnrcr_alg Produkt 3: ssf3/ssf_symencnrcr_alg |
| Kurzbeschreibung: | Symmetrischer Verschlüsselungsalgorithmus für SSF |
| Gültig für Release: | alle |
| Beschreibung: | <p>Dieser Parameter enthält den symmetrischen Verschlüsselungsalgorithmus, der zusammen mit den SSF-Funktionen zu verwenden ist. Der symmetrische Verschlüsselungsalgorithmus wird z. B. zum Erstellen digitaler Umschläge verwendet.</p> <p>Sie müssen einen Algorithmus angeben, der von dem von Ihnen verwendeten Sicherheitsprodukt unterstützt wird.</p> |
| Vorschlagswert: | DES-CBC |
| Gültige Einträge, Formate: | DES-CBC, TRIPLE-DES, IDEA |
| | Informationen über weitere unterstützte Algorithmen finden Sie in der Dokumentation Ihres Sicherheitsprodukt. |



Die Parameter zusätzlicher Produkte können Sie nur auf den Anwendungsservern definieren.

SSF_TRACE_LEVEL

| | |
|---|--|
| Umgebungsvariablen- oder Initialisierungsdateieintrag: | Produkt 1: SSF_TRACE_LEVEL Produkt 2: SSF2_TRACE_LEVEL Produkt 3: SSF3_TRACE_LEVEL |
| Profilparameter des Anwendungsservers: | nicht als Profilparameter eines Anwendungsservers definiert |
| Kurzbeschreibung: | Trace-Stufe zum Aufzeichnen der SSF-Aktivitäten |
| Gültig für Release: | alle |
| Beschreibung: | In Abhängigkeit von der Trace-Stufe zeichnet das System Informationen über SSF-Funktionsaufrufe in Datei <code>dev_ssf</code> auf. |
| Vorschlagswert: | 0 (niedrigste Trace-Stufe) |
| Gültige Einträge, Formate: | 0 : Das System zeichnet folgendes auf: <ul style="list-style-type: none"> • den Start des SSF-RFC-Servers • das Laden der SSF-Funktionsbibliothek • die Installation der RFC-fähigen SSF-Funktionen 1 : Zusätzlich zeichnet das System folgendes auf: <ul style="list-style-type: none"> • Namen und Rückgabewerte der aufgerufenen SSF-Funktionen 2 : Zusätzlich zeichnet das System folgendes auf: <ul style="list-style-type: none"> • Informationen über den Unterzeichner und den Empfänger beim Aufruf von SSF-Funktionen 3 : Zusätzlich zeichnet das System folgendes auf: <ul style="list-style-type: none"> • alle Eingabe- und Ausgabedaten beim Aufruf von SSF-Funktionen |



Die Parameter zusätzlicher Produkte können Sie nur auf den Anwendungsservern definieren.

Außerdem ist der `SSF_TRACE_LEVEL` auf dem Anwendungsserver nicht als Profilparameter definiert. Sie können den Wert der SSF-Trace-Stufe nur mit der Umgebungsvariablen angeben.

SSF_NAME

SSF_NAME

| | | |
|---|---|-----------|
| Umgebungsvariable: | Produkt 1: | SSF_NAME |
| | Produkt 2: | SSF2_NAME |
| | Produkt 3: | SSF3_NAME |
| Profilparameter des Anwendungsservers: | Produkt 1: | ssf/name |
| | Produkt 2: | ssf2/name |
| | Produkt 3: | ssf3/name |
| Kurzbeschreibung: | Name des Sicherheitsprodukts | |
| Gültig für Release: | Ab Release 4.5B | |
| Beschreibung: | Dieser Parameter enthält den Namen des Sicherheitsprodukts. | |
| Vorschlagswert: | Produkt 1: | SSF |
| | Produkt 2: | SSF2 |
| | Produkt 3: | SSF3 |
| Gültige Einträge, Formate: | Zeichenfolge von bis zu 255 Zeichen | |



Die Parameter zusätzlicher Produkte können Sie nur auf den Anwendungsservern definieren.

Auch `SSF_NAME` wird nur auf dem Anwendungsserver definiert.



Beim Start eines Anwendungsservers lädt das System automatisch die SAPSECULIB und ordnet die SAPSECULIB-Informationen dem nächsten verfügbaren Parametersatz `ssf<x>/...` zu. Falls beispielsweise kein anderes Produkt in den SSF-Parametern angegeben wurde, wird der Parameter `ssf/name` beim Start des Anwendungsservers auf den Wert SAPSECULIB gesetzt.

Die SSF-Initialisierungsdatei

Definition

Datei, die die SSF-Konfiguration für die Frontend-Rechner enthält.

Verwendung

Sie können die SSF-Initialisierungsdatei zum Konfigurieren der SSF-Parameter an den Frontend-Rechnern benutzen.



Ab Release 4.5 können Sie entweder die SSF-Initialisierungsdatei oder die Umgebungsvariablen verwenden.

Name und Ort

Der Standardname der SSF-Initialisierungsdatei lautet `ssfrfc.ini`. Sie befindet sich im selben Verzeichnis wie das SSF-RFC-Serverprogramm `ssfrfc.exe`. (Bei einer Standardinstallation ist dies das SAP-GUI-Verzeichnis.) Mit der Umgebungsvariablen `SSF_INI_FN` können Sie einen anderen Namen und Ablageort angeben.

Syntax

Das Format für die Eingabe der einzelnen Parameter in die Datei ist eine Zeileneingabe mit folgender Syntax:

`<SSF-Parameter>=<Parameterwert>`

Beachten Sie folgendes:

- Mit einem Stern (*) beginnende Zeilen sowie Leerzeilen werden als Kommentar interpretiert.
- Stößt der SSF-Prozeß der Dateianalyse auf einen Fehler, bricht er ab. Die Zeile mit dem Fehler wird in der SSF-Trace-Datei `dev_ssf` aufgezeichnet.



Hier sehen Sie ein Beispiel der Datei `ssfrfc.ini` aus Release 4.5.

ssfrfc.ini

```
*****
* Secure Store & Forward (SSF) Initialization File *
*****
SSF_LIBRARY_PATH=c:\Program Files\SAPpc\SAPgui\libssf.dll
SSF_MD_ALG=MD5
SSF_SYMENCNCR_ALG=DES-CBC
SSF_TRACE_LEVEL=0
```

Die SSF-Initialisierungsdatei

Information zu Release 4.0/4.5

Bestimmte Pflegeaufgaben und SSF-Informationen haben sich zwischen den Releases 4.0, 4.5 und 4.6 geändert. Die Pflege der SSF-Informationen zum Benutzer befindet sich nun in der Benutzeradressenpflege und die Verwendung sowie die Syntax der SSF-Initialisierungsdatei wurden geändert. Weitere Informationen finden Sie unter

- [SSF-Benutzerinformationen pflegen: Release 4.0/4.5 \[Seite 44\]](#)
- [Die SSF-Initialisierungsdatei in Release 4.0 \[Seite 45\]](#)

SSF-Benutzerinformationen pflegen: Release 4.0/4.5

SSF-Benutzerinformationen pflegen: Release 4.0/4.5

Voraussetzungen

Das Sicherheitsprodukt wurde installiert und SSF wurde auf dem Anwendungsserver konfiguriert (siehe [SSF installieren/konfigurieren: Anwendungsserver \[Seite 15\]](#)).

Der Ort des SSF-RFC-Serverprogramms `ssfrfc` muß auch als RFC-Destination `SAP_SSFATGUI` in Transaktion SM59 definiert werden.

Vorgehensweise

1. Im Customizing für *Systemadministration* wählen Sie *Verwaltung externer Sicherheitssysteme* → *Sichere Speicherung und Datenexport (SSF)* → *SSF-Informationen für Benutzer verwalten* (Transaktion O07C).
2. Ändern Sie einen vorhandenen Eintrag, indem Sie ihn markieren und *Springen* → *Detail* wählen oder legen Sie einen neuen Eintrag an, indem Sie *Neue Einträge* wählen.
Sie gelangen auf die Sicht "Digitale Signatur: SSF-Informationen zum Benutzer" ändern: *Details*.
3. Geben Sie die erforderlichen Daten ein:

SSF-Benutzerinformation pflegen

| Feld | Beschreibung | Kommentar |
|---|--|---|
| <i>Destination</i> | Die RFC-Destination (logische Destination), wo das SSF-RFC-Serverprogramm definiert wurde. | SAP_SSFATGUI Siehe Eingabehilfe (F4). |
| <i>U/E Name</i> | Name des SSF-Unterzeichners /-Empfängers | Die Syntax des Namens hängt von dem Sicherheitsprodukt ab, das Sie verwenden. |
| <i>Namensraum</i> (nur in Release 4.0) | Namensraum, in dem die Benutzerinformationen gültig sind. | Die Benutzerinformationen können beispielsweise auf einer Smartcard, in einem lokalen Verzeichnis oder in einem X.500-Verzeichnis abgelegt sein. Mit der Eingabehilfe (F4) können Sie mögliche Eingaben anzeigen. |
| <i>Profilname</i> | Profilname | Gibt das Profil an, in dem die Sicherheitsinformationen des Benutzers abgelegt sind. Der Wert dieses Parameters hängt von dem Sicherheitsprodukt ab, das Sie verwenden. |

4. Sichern Sie Ihre Eingabe.

Die SSF-Initialisierungsdatei in Release 4.0

Dieser Abschnitt erklärt die geringfügigen Unterschiede, die Sie bei der Verwendung der SSF-Initialisierungsdatei in Release 4.0 beachten müssen. Allgemeine Informationen zur Verwendung der Datei finden Sie unter [Die SSF-Initialisierungsdatei \[Seite 41\]](#).

Kein Support der Umgebungsvariablen in Release 4.0

In Release 4.0 müssen Sie die SSF-Parameter zum Konfigurieren der SSF-Initialisierungsdatei auf den Frontend-Rechnern benutzen.

Syntax für ssrfc.ini in Release 4.0

In Release 4.0 ist das Format für die Eingabe der einzelnen Parameter in die Datei eine Zeileneingabe mit folgender Syntax:

<SSF-Parameterbeschreibung> = <Parameterwert>

Beachten Sie folgendes:

- Bei den SSF-Parameterbeschreibungen in Release 4.0 ist die Groß- und Kleinschreibung zu berücksichtigen. Vor und nach dem Gleichheitszeichen (=) müssen Sie genau ein Leerzeichen einfügen. Es gibt folgende Beschreibungen:
 - SSF Library Path
 - SSF Hash Algorithm
 - SSF Symmetric Encryption Algorithm
 - SSF Trace Level
- Die letzte Zeile der Datei muß durch Drücken der *Return*-Taste abgeschlossen werden.



Hier sehen Sie ein Beispiel der Datei `ssrfc.ini` aus Release 4.0.

ssrfc.ini

```
*****
* Secure Store & Forward (SSF) Initialization File *
*****
SSF Library Path = c:\Program Files\SAPpc\SAPgui\libssf.dll
SSF Hash Algorithm = MD5
SSF Symmetric Encryption Algorithm = DES-CBC
SSF Trace Level = 0
<Return>
```