

Sterling B2B Integrator



# EBICS Banking Server Concepts

*Version 5.2.5*



Sterling B2B Integrator



# EBICS Banking Server Concepts

*Version 5.2.5*

**Hinweis**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen“ auf Seite 25 gelesen werden.

**Copyright**

Diese Ausgabe bezieht sich auf Version 5, Release 2, Modification 5 von Sterling B2B Integrator und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuauflage geändert wird.

© Copyright IBM Corporation 2000, 2015.

---

# Inhaltsverzeichnis

<b>EBICS Server Concepts (V5.2.5 oder höher)</b> . . . . .	<b>1</b>
Architektur des EBICS Banking Server. . . . .	2
Subscription Manager-Informationen verwalten. . .	6
EBICS-Transaktionen verwalten . . . . .	8
Von einem Abonnenten hochladen (FUL) . . . .	9
Vom EBICS-Server herunterladen (FDL) . . . .	10
Segmentation and Recovery . . . . .	11
VEU-Verarbeitung . . . . .	12

Schlüssel verwalten. . . . .	13
EBICS-Berichte generieren und abrufen . . . . .	15
EBICS-Server verwalten . . . . .	15
Systemauftrag verwalten . . . . .	16
Auftragsdaten verarbeiten . . . . .	19
Integration mit Sterling File Gateway vornehmen..	22

<b>Bemerkungen.</b> . . . . .	<b>25</b>
-------------------------------	-----------



---

## EBICS Server Concepts (V5.2.5 oder höher)

Der Electronic Banking Internet Communication Standard (EBICS) bezeichnet einen internetbasierten Kommunikations- und Sicherheitsstandard, der primär bei der fernen Datenübertragung zwischen Ihrer Organisation und einer Bank zur Ausführung unternehmensweiter Zahlungstransaktionen Anwendung findet.

EBICS ermöglicht den Datendateiaustausch unabhängig von Nachrichtenstandards und -formaten. EBICS verwendet etablierte Prozeduren für digitale Signaturen und die Verschlüsselung. Seine Funktionen basieren auf internationalen Standards für Internetkommunikation und verbesserte Sicherheit, wie etwa XML, HTTPS, TLS und SSL. EBICS besitzt darüber hinaus Multibank-Funktionalität, die Firmenkunden in denjenigen Ländern, die EBICS aktiv unterstützen, dazu befähigt, mit ein und derselben Software Transaktionen mit beliebigen Banken in diesen Ländern abzuwickeln.

Eine Reihe von Voraussetzungen müssen von einem Benutzer (der einem Partner zugeordnet ist) erfüllt werden, damit er banktechnische EBICS-Transaktionen mit einer bestimmten Bank implementieren kann. Die Grundvoraussetzung für die Implementierung von EBICS-Transaktionen ist die Unterzeichnung eines Vertrags zwischen dem Partner und der Bank. In diesem Vertrag werden die folgenden Details vereinbart:

- Die Art der Geschäftstransaktionen (banktechnischen Auftragsarten), die der Partner mit der Bank abwickeln wird
- Informationen zu den Bankkonten des Kunden
- Die Partner, die mit dem Banksystem arbeiten
- Die Autorisierungen und Berechtigungen, die der Benutzer besitzt

Der Partner empfängt die Bankzugriffsdaten (Bankparameter) nach der Unterzeichnung des Vertrages. Die Bank konfiguriert die Masterdaten für die Partner und Benutzer in Übereinstimmung mit den vertraglichen Vereinbarungen.

Weitere Voraussetzungen sind u. a. eine erfolgreiche Abonnenteninitialisierung, das erfolgreiche Herunterladen der öffentlichen Zertifikate der Bank durch den Benutzer und die erfolgreich ausgefallene Überprüfung der öffentlichen Zertifikate des Benutzers durch die Bank.

Der Sterling B2B Integrator EBICS Banking Server ist eine vollständige EBICS-Lösung, die eine Bank, einen Partner sowie die Benutzerverwaltung, die Zertifikatsverwaltung, sichere Dateitransaktionen, die Fehlerbehebung und die Berichterstellung einbezieht. Sterling B2B Integrator wird zum Senden und Empfangen von EBICS-Transaktionen verwendet.

Sterling B2B Integrator Banking Server unterstützt EBICS-Spezifikation V2.5 für Implementierungen in Französisch und Deutsch.

Sterling File Gateway operiert auf der Sterling B2B Integrator-Plattform und bietet eine sichere Dateiübertragung zwischen internen und externen Partnern mithilfe derselben oder anderer Kommunikationsprotokolle, Dateinamenskonventionen und Dateiformaten. Sterling File Gateway unterstützt die Übertragung großer Dateien und von Dateien mit großem Volumen durch die Anzeige der Dateiübertragung in

einem prozessorientierten und hoch skalierbaren Framework, der die Anforderungen an die Dateiübertragung bezüglich Protokoll- und Dateibrokering, Automatisierung und Datensicherheit reduziert.

## **Speicherbedarf des Dateisystems für FDL-Anforderungen**

Da der Auftragstyp FDL das Dateisystem zum Speichern der Nutzdaten verwendet, ist es wichtig das der Dateisystemspeicher entsprechend geplant wird. Große FDL-Nutzdaten erfordern bis zum 6 Mal soviel Dateibereich wie die eigentliche Nutzdatengröße. Beispiel: eine Nutzdatengröße von 5 GB erfordert über 30 GB an Dateibereich in Sterling B2B Integrator zum Verarbeiten der Anforderung.

Wenn Sie EBICS Banking Server In einer Clusterumgebung verwenden, müssen Sie das gemeinsam genutzte Dateisystem als Dokumentspeicher zwischen Knoten konfigurieren, auch wenn der standardmäßige Dokumentspeichertyp auf "Database" gesetzt ist. Die entsprechende Dokumentation zur *Installation* enthält weitere Anweisungen hierzu.

---

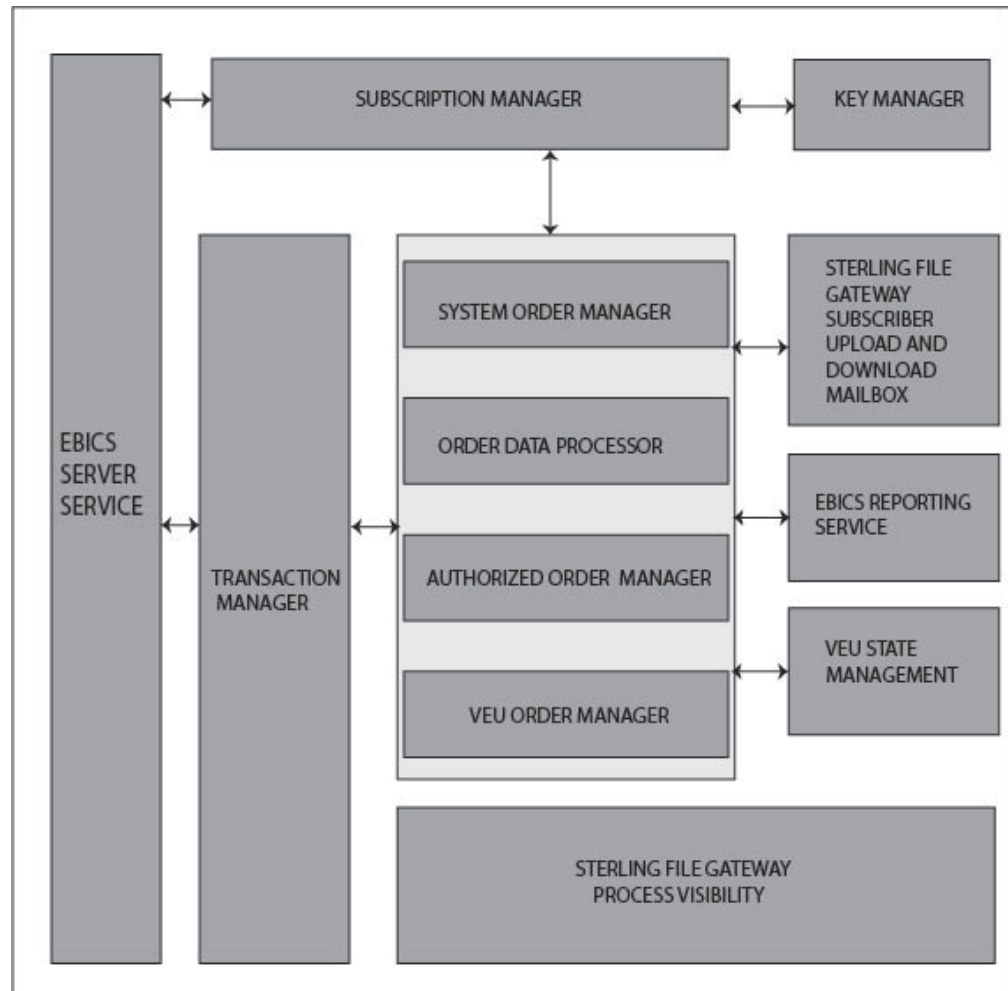
## **Architektur des EBICS Banking Server**

EBICS Banking Server ermöglicht Ihnen, Transaktionen mit Partnern und Benutzern unter Verwendung von EBICS auszuführen.

Die Funktionen umfassen das Erstellen und Verwalten von Profilen (Bank-, Partner- und Benutzerprofil), Zuordnen von Partnern und Benutzern zu Auftragsarten und Dateiformaten, Zuordnen von Benutzerberechtigungen, Erstellen und Verwalten von Zertifikaten, Verarbeiten von Auftragsdaten, Speichern und Abrufen von Profilingformationen, Zertifikaten und Nachrichten, Verwalten von Nachrichten- und Transaktionsflüssen sowie Übertragen von Dateien mit sicheren Protokollen usw.

Das folgende Diagramm veranschaulicht die Architektur von EBICS Banking Server:





Der *Subscription Manager* umfasst die folgenden Funktionen:

- Profilverwaltung - Zum Erstellen und Verwalten von Bank-, Partner- und Benutzerprofilen
- Auftragsartkonfiguration - Zum Konfigurieren von Auftragsarten und Dateiformaten
- Angebotskonfiguration - Zum Gruppieren einer Menge von Auftragsarten und Dateiformaten zu einer Liste von Kunden
- Konfiguration für Benutzerberechtigung - Zum Zuweisen von Auftragsarten und Dateiformaten zu Benutzern
- Import von Subscription Manager-Informationen - Zum Importieren von Konfigurationsdetails, die sich auf Bank-, Partner-, Benutzer-, Angebots- und Benutzerberechtigungen, Auftragsarten und Dateiformate beziehen, aus einem externen Repository in den EBICS Banking Server
- Export von Subscription Manager-Informationen - Zum Exportieren von Konfigurationsdetails, die sich auf Bank-, Partner-, Benutzer-, Angebots- und Benutzerberechtigungen, Auftragsarten und Dateiformate beziehen, aus dem EBICS Banking Server in ein externes Repository

Die *Upload- und Download-Mailboxen des Subskribenten* werden bei der Einrichtung des Benutzerabonnements im Subscription Manager konfiguriert.

Die *Schlüsselverwaltung* bildet hauptsächlich zum Subscription Manager eine Schnittstelle zum Erstellen, Aktualisieren, Löschen und Abfragen von Zertifikaten.

Die Schlüsselverwaltung umfasst die folgenden Funktionen:

- Selbst signierte Zertifikate - Zum Generieren und Verwalten selbst signierter Zertifikate mit einer Schlüssellänge von 2048
- Zertifikate einer Zertifizierungsstelle (CA-Zertifikate) - Zum Verwalten der Zertifikate von Zertifizierungsstellen
- Schlüsselspeicher - Zum Bereitstellen der Keystores für die Zertifikate und Verwalten der Erneuerung und des Ablaufs von Zertifikaten
- Zertifikate importieren und exportieren - Zum Importieren und Exportieren von Zertifikaten
- Abonentenschlüsselvalidierung - Zum Validieren der Hashwerte von Benutzerzertifikaten
- Zertifikatshashwert - Zum Unterstützen der Erstellung von Zertifikatshashwerten mit SHA256

Der *EBICS-Server-Service* bildet eine Schnittstelle zum Subscription Manager, um die Profilinformationen von Banken, Partnern, Benutzern und Auftragsarten abzurufen, die für die Prüfung und Authentifizierung von Nachrichten und Transaktionen erforderlich sind. Er arbeitet bei der Verwaltung aller EBICS-Transaktionen (EBICS: Electronic Banking Internet Communication Standard) eng mit dem Transaction Manager zusammen.

Der EBICS-Server-Service umfasst die folgenden Funktionen:

- Anforderung und Antwort - Zum Abwickeln eingehender EBICS-Anforderungen (über HTTP und HTTPS) nach den EBICS-Protokollspezifikationen und zum Generieren einer entsprechenden Antwort zurück an den Anforderer
- Nachrichtenfluss - Zum Verwalten des Nachrichtenflusses für die Initialisierungs- und Dateiübertragungsphasen der EBICS-Transaktionen
- Authentifizierung und Autorisierung - Zum Ausführen von Nachrichtenauthentifizierungs- und Benutzerberechtigungsprüfungen

Der *Transaction Manager* arbeitet bei der Verwaltung des Upload- und Downloadflusses von Systemauftragsarten und banktechnischer Auftragsarten eng mit dem EBICS-Server-Service zusammen.

Der Transaction Manager umfasst die folgenden Funktionen:

- Asynchrone Transaktion - Zum Verwalten des asynchronen Transaktionsflusses für banktechnische Upload-Auftragsarten (FUL). Diese Funktion verwaltet den Verarbeitungsfluss autorisierter Aufträge in Zusammenarbeit mit dem Order Data Processor, um die Auftragsdaten zu entpacken und die entpackten Auftragsdaten der in den Benutzerprofileinstellungen definierten Zielmailbox für Uploads bereitzustellen.
- Synchroner Transaktion - Zum Verwalten des synchronen Transaktionsflusses für Upload- und Download-Systemauftragsarten und banktechnische Auftragsarten. Diese Funktion verwaltet die Flüsse für die Systemauftragsbearbeitung, die Berichtsverarbeitung (FDL, PSR) und die Verarbeitung banktechnischer Download-Aufträge (FDL).
- Segmentierung und Wiederherstellung - Zum Verwalten von Nullantworten, Segmentierung und Fehlerbehebung

Der *System Order Manager* ist verantwortlich für das Aktualisieren und Abfragen von Schlüsselverwaltungsinformationen und referenzieller Informationen für Benutzer.

Der *System Order Manager* arbeitet zum Aktualisieren und Abfragen der Schlüsselzertifikate und der referenziellen Informationen des Benutzers und zum Herunterladen von Bankparametern und Bankzertifikaten eng mit dem *Transaction Manager* und *Subscription Manager* zusammen.

Der *Authorized Order Manager* ist dafür verantwortlich, den *Order Data Processor* zum Entpacken der von der FUL-Auftragsartanforderung empfangenen Auftragsdaten, zum Routing (Weiterleiten) der entpackten Auftragsdaten an die Upload-Mailbox des Backend-Abonnenten und zum Umbenennen der entpackten Daten gemäß einer definierten Namenskonvention zu initialisieren.

*VEU Order Manager* ist für die Handhabung von VEU-Aufträgen (Auftragstypen HVD, HVE, HVS, HVT, HVU oder HVZ) verantwortlich.

Der *Order Data Processor* ist zum Packen und Entpacken von Auftragsdaten verantwortlich. Er bildet zum Abrufen der relevanten Informationen, die zum Packen und Entpacken der Auftragsdaten erforderlich sind, eine Schnittstelle zum *Subscription Manager* und *Transaction Manager*. Seine Funktionen umfassen die folgenden:

- Packen - Zum Packen von Auftragsdaten wie etwa Signieren, Komprimieren Verschlüsseln und Codieren gemäß Base64 je nach Anforderung der Auftragsart
- Entpacken - Zum Entpacken von Auftragsdaten wie etwa Überprüfung, Dekomprimierung, Entschlüsselung und Decodierung gemäß Base64 je nach der Anforderung der Auftragsart

Der *Berichtsdienst* ist dafür verantwortlich, den *Payment Status Report (PSR)* zu generieren, der dem Entpacken von Auftragsdaten bei einem asynchronen Hochladen eines banktechnischen Auftragstransaktionsflusses zugewiesen ist.

*VEU State Management* ist für die Verwaltung von Informationen zu VEU-Aufträgen verantwortlich, die nicht vollständig autorisiert wurden (z. B. noch fehlende Signaturen).

*Sterling File Gateway* verwendet Vorlagen für die Beschreibung, wie jede einzelne Transaktion interpretiert wird, um festzustellen, wie und wohin sie zugestellt werden soll und bietet eine Anzeige der Details der Übertragung zur Protokollierung und Fehlerbehebung.

*Sterling File Gateway* beinhaltet die folgenden Funktionen:

- Datei- oder Dateinamenstransformationen - Zum Zuordnen von Eingabe- zu Ausgabedateinamen, systemweiten, gruppenspezifischen und partnerspezifischen Richtlinien, allgemeinen Dateiverarbeitungstasks wie der Komprimierung und Dekomprimierung, PGP-Verschlüsselung und -Entschlüsselung sowie der Signierung
- Dateiübertragungssichtbarkeit - Ereignisse werden zwecks Überwachung und Berichterstellung aufgezeichnet; detaillierte Verfolgung (Tracking) zur Ermittlung der Eingabe-/Ausgabedateistrukturverarbeitung und zur dynamischen Routenermittlung; Fähigkeit der Einsicht in und Filterung von Datenflüssen für alle Benutzer
- Unterstützung einer Vielfalt von Übertragungsprotokollen - FTP, FTP/S, SSH/SFTP, SSH/SCP und *Sterling Connect:Direct* werden bei der Installation unter-

stützt; die Konfiguration zusätzlicher Protokolle (wie AS2, AS3 oder Odette FTP) ist durch Verwendung der Erweiterbarkeitsfunktion möglich

- Partnerschnittstelle (myFileGateway) - Auf Web-Browser basierende Schnittstelle, die Partnern das Hochladen/Herunterladen von Dateien, Abonnieren von Ereignisbenachrichtigungen, Verwalten von Kennwörtern, Suchen und Anzeigen der Dateiübertragungsaktivität und Generieren von Berichten über die Dateiübertragungsaktivität ermöglicht
- Flexible Mailboxstrukturen - Möglichkeit der Angabe von Mailboxstrukturen, die den wirksamen Einsatz von Mustererkennungsrichtlinien ermöglichen, und der Angabe von Attributen, die für alle Partner oder eine Untermenge von Partnern zutreffen müssen
- Dynamisches Routing - Ableiten des Verbrauchers zur Laufzeit anhand von Mailboxstruktur, anhand von Dateiname, durch vom Geschäftsprozess abgeleiteten Verbrauchernamen oder anhand des von der Zuordnung (Map) abgeleiteten Verbrauchernamens

---

## Subscription Manager-Informationen verwalten

Das Subscription Manager-Menü in Sterling B2B Integrator ermöglicht Ihnen Folgendes:

- Erstellen und Verwalten von Bank-, Partner- und Benutzerprofilen in der Systemdatenbank
- Erstellen und Verwalten von Angeboten
- Zuweisen von Auftragsarten und Dateiformaten zu einem Auftrag
- Zuweisen von Berechtigungen zu Benutzern

Eine Bank kann nur ein Profil mit einer eindeutigen Bank-ID besitzen. Ein Bankprofil enthält die folgenden Informationen:

- Eindeutige ID der Bank

**Anmerkung:** Jede Bank-ID sollte eine eindeutige Portnummer besitzen.

- Name der Bank
- Adresse der Bank
- Öffentliche und private Verschlüsselungs-, Authentifizierungs- und Identifikationszertifikate
- HTTP-URL der Bank
- EBICS-Protokollversion

Eine Bank kann mehrere URLs haben. Die entsprechende Bank-URL wird einem Benutzer mitgeteilt, um Anforderungen an die Bank zu senden. Der URI (Uniform Resource Indicator) bzw. die einheitliche Referenz-ID wird im HTTP-Server-Adapter für die Empfangsbereitschaft am Port und zum Empfangen von EBICS-Anforderungen (sofern diese anfallen) konfiguriert.

Die folgenden Versionen von Bankprotokoll- und Prozesstypen werden unterstützt:

- EBICS-Protokollversion - H004, H003, H000
- Signaturversionen: A005, A006
- Authentifizierungsversion: X002
- Verschlüsselungsversion: E002

Jeder Partner kann über mehrere verschiedene Konteninformationen und Partner-IDs verfügen. Die Kontonummer muss entweder in nationalem (deutschem) oder

in internationalem Format (IBAN) angegeben werden. Sie können eine Partner-ID zu einem Angebot zuordnen. Das Partnerprofil enthält die folgenden Informationen:

- Eindeutige ID des Partners
- Organisationscode des Partners
- Name des Partners
- Adresse des Partners
- Konto-ID und Name des Kontoinhabers
- Währung, in der die Transaktion abgewickelt wird
- Kontonummer
- Bankleitzahl

Ein Benutzer kann einem oder mehreren Partnern untergeordnet sein. Eine Bank kann einen Benutzer erstellen und kann den Benutzer einem Partner zuordnen, muss dies jedoch nicht. Um den Austausch von EBICS-Nachrichten zwischen einem Partner und einem Benutzer zu ermöglichen, ist es erforderlich, eine Benutzer-ID einer Partner-ID zuzuordnen.

Die Übertragung von öffentlichen Zertifikaten an die Bank durch einen Benutzer erfolgt auf zwei voneinander unabhängigen Kommunikationspfaden:

- INI - Zuständig für den Versand des öffentlichen banktechnischen Schlüssels
- HIA - Zuständig für den Versand des öffentlichen Identifikations- und Authentifizierungsschlüssels und des öffentlichen Verschlüsselungsschlüssels

Wenn ein Benutzer erstmals einem Partner zugeordnet wird, lautet der Status des Benutzers 'Neu'. Wenn der Benutzer lediglich die INI-Anforderung an die entsprechende Bank sendet, wird der Status in 'Teilweise initialisiert' (INI) geändert. Sendet der Benutzer nur die HIA-Anforderung an die Bank, wird der Status in 'Teilweise initialisiert (HIA)' geändert. Hat der Benutzer sowohl die INI- als auch die HIA-Anforderung an die Bank gesendet, so ändert sich sein Status in 'Initialisiert'. Der Benutzer sendet die Initialisierungsschreiben der Schlüssel INI und HIA per E-Mail an die Bank. Nachdem die Bank die Initialisierungsschreiben zu INI und HIA erhalten hat, überprüft sie die Hashwerte in den Zertifikaten und gleicht diese mit ihrer Datenbank ab. Nach erfolgreich ausgefallener Überprüfung wird für den Benutzer der Status 'Bereit' festgelegt und dadurch angegeben, dass der Benutzer nun Transaktionen mit der Bank durchführen kann. Der Benutzer lädt dann die öffentlichen Zertifikate der Bank mit der HPB-Systemauftragsart herunter.

Sie können die Auftragsstypen HKD und HTD verwenden, um die Teilnehmerinformationen abzurufen, die von der Bank gespeichert wurden, nachdem für den Status des Benutzers *Bereit* festgelegt wurde.

Verwenden Sie den EBICS-Service 'Subscription Manager' zum Validieren der Schlüssel für die INI- und HIA-Initialisierungsschreiben. Nach erfolgreicher Validierung wird der Status des Benutzers z. B. in 'Bereit' aktualisiert, und dadurch angegeben, dass der Benutzer die HIA- und INI-Initialisierungsschreiben an die Bank gesendet hat. Mit diesem Service können Sie außerdem auch Subscription Manager-Daten die Systemdatenbank der Bank importieren bzw. aus ihr exportieren.

Das Benutzerprofil enthält die folgenden Informationen:

- Eindeutige ID des Benutzers
- Name des Benutzers
- Adresse des Benutzers

- Partner-ID, der der Benutzer zugeordnet ist
- Mailboxeinstellungen zur Ermöglichung des Hochladens, Herunterladens und Archivierens von Nachrichten

Anhand von EBICS-Auftragsarten wird angegeben, welche verschiedenen Transaktionen zwischen dem EBICS-Server und einem EBICS-Client ausgeführt werden können. Ein Auftragstyp kann null oder mehr Dateiformate aufweisen. Sie können Dateiformate zu den banktechnischen Upload- und Download-Auftragsarten zuordnen. Mit Upload-Auftragsarten können Sie Auftragsdaten von einem EBICS-Client auf einen EBICS-Server hochladen; mit Download-Auftragsarten hingegen können Sie Auftragsdaten von einem EBICS-Server auf einen EBICS-Client herunterladen. Eine Auftragsart enthält die folgenden Attribute:

- Auftragsart
- EBICS-Protokollversion
- Übertragungstyp - 'Upload' (Hochladen) oder 'Download' (Herunterladen)
- Auftragsdatenart - 'System' oder 'Technisch'

Ein Dateiformat enthält die folgenden Attribute:

- Dateiformat
- Ländercode des Dateiformats

Eine Bank kann ein oder mehrere Angebote erstellen. Ein Angebot stellt eine einfache Methode zur Gruppierung einer Menge von Auftragsarten und Dateiformaten und ihrer Zuordnung zu einer Liste von Partnern dar. Jedem Partner wird eine Liste von Auftragsarten zugeordnet, anhand der Transaktionen zwischen der Bank und dem Partner möglich werden. Ein Angebot stellt eine einfache Methode für die Bank dar, um eine vertragliche Vereinbarung mit dem Partner zu treffen. Ein Angebot enthält die folgenden Informationen:

- Bank-ID
- Name des Angebots
- Die Auftragsarten und Dateiformate, über die der Partner Nachrichten austauschen kann
- Autorisierungsebene für die Auftragsart
- Anzahl von Signaturen, die zum Autorisieren des Auftrags erforderlich sind

Ein Partner kann einem oder mehreren Benutzern zugeordnet werden. Eine Bank ordnet einem Benutzer die folgenden Berechtigungen zu:

- Die Auftragsarten und Dateiformate, über die der Partner Nachrichten austauschen kann
- Autorisierungsebene für die Auftragsart
- Der Höchstbetrag an Transaktionen (für ein bestimmtes Partnerkonto), die ein Benutzer ausführen kann. Sie können mehrere Partnerkonten mit unterschiedlichen Höchstbeträgen zuordnen.
- Die Währung, in der der Höchstbetrag für den Benutzer angegeben ist. Die Währung hängt vom Partnerkonto ab, das dem Höchstbetrag zugeordnet ist.

---

## EBICS-Transaktionen verwalten

Der Transaction Manager im EBICS-Server ist für die Verwaltung der Transaktionsstatus zuständig. Er ermittelt, welches Segment zum Generieren der XML-Antwortnachricht erforderlich ist.

Transaction Manager wickelt die Transaktionsflüsse für das Hoch- und Herunterladen ab und unterstützt die Segmentierung und Wiederherstellung von Auftragsdaten.

## Von einem Abonnenten hochladen (FUL)

Der Auftragstyp FUL wird zum Hochladen von Daten zu einer Bank verwendet.

Die Upload-Transaktion umfasst die folgenden Phasen:

- Initialisierung
- Datenübertragung

Der Benutzer sendet die Upload-Anforderung (FUL) an die Bank. FUL ist ein banktechnischer Upload-Auftragstyp.

**Wichtig:** Bei großen FUL-Nutzdaten sollte die Einstellung für die maximale Leerlaufzeit (MaxIdleTime) im EBICS Server Service erhöht werden. Wenn die Einstellung MaxIdleTime zu niedrig ist, könnte die Transaktion vor der Beendigung abgebrochen werden. Die passende Einstellung für große FUL-Nutzdaten ist 300 Minuten.

Der EBICS-Service für Auftragsautorisierung wickelt eingehende Auftragsanforderungen für die banktechnische Upload-Auftragsart ab. Wenn ein Auftrag die Anzahl der erforderlichen Signaturen bezogen hat, leitet dieser Service den Auftrag an die Upload-Mailbox des Abonnenten weiter. Andernfalls bewahrt dieser Service die Auftragsdaten in der Datenbank so lange auf, bis der Auftrag die erforderliche Anzahl von Signaturen vorweisen kann.

Der Geschäftsprozess 'handleEBICSRequest' empfängt die Anforderung eines Benutzers. Wenn die Benutzeranforderung das letzte Segment der Auftragsdaten enthält, wird der Geschäftsprozess EBICSOrderAuthorizationProcessing asynchron aufgerufen, um die Auftragsdaten zu entpacken und die folgenden Dateien zu generieren:

**Anmerkung:** Zum Entpacken von Auftragsdaten gehört das Decodieren, Entschlüsseln und Dekomprimieren der Auftragsdaten.

- .DAT - Enthält die nicht gepackten Auftragsdaten in einer Upload-Mailbox des Benutzers
- .SIG - Enthält die Signatur der Auftragsdaten in einer Upload-Mailbox des Benutzers
- .PRM - Enthält die Auftragsparameter in der Upload-Mailbox des Benutzers
- .PSR - Enthält einen Statusbericht der asynchronen Verarbeitung in der Download-Mailbox des Benutzers

### Initialisierung verarbeiten

Ein Benutzer leitet durch die Übergabe der Anforderungen, die Informationen zum eingehenden Auftrag enthalten, eine Transaktion ein. Ausgehend von diesen Informationen überprüft der EBICS-Server die Auftragsart, führt den Nachrichtenwidergabetest durch, überprüft die Nachrichtenauthentifizierung und prüft die Benutzerautorisierung, bevor er die Anforderung annimmt.

Nach erfolgreich ausgefallener Überprüfung der Auftragsdaten generiert die Bank eine Transaktions-ID und bindet die ID in ihre Antwort an den Benutzer ein.

## Datenübertragung verarbeiten

Wenn für die Übertragung von Auftragsdaten mehr als nur ein Segment erforderlich ist, führt die Bank die Nachrichtenauthentifizierung aus, überprüft die Transaktion und überprüft die Segmentnummer und -größe. Nachdem der EBICS-Server das letzte Segment der Auftragsdaten empfangen hat, werden die nun vollständigen Auftragsdaten an den Geschäftsprozess 'EBICSOrderAuthorizationProcessing' asynchron weitergeleitet und die Transaktion endet.

Der Geschäftsprozess 'EBICSOrderAuthorizationProcessing' entpackt die Auftragsdaten und leitet sie an die Upload-Mailbox des Benutzers weiter. Der Geschäftsprozess 'EBICSOrderAuthorizationProcessing' generiert einen Bericht nach der Verarbeitung (PSR) und leitet diesen an die Download-Mailbox des Benutzers weiter. Dieser Geschäftsprozess generiert auch die SIG- und PRM-Dateien, die an die Upload-Mailbox des Benutzers weitergeleitet werden. Wenn der Prozess 'EBICSOrderAuthorizationProcessing' einen Fehler feststellt, wie zum Beispiel eine ungültige elektronische Signatur, so wird eine ERR-Datei (Fehlerdatei) generiert. Verwenden Sie diese ERR-Datei, um bei Bedarf eine ungültige Auftragsdatendatei zu untersuchen.

## Vom EBICS-Server herunterladen (FDL)

Der Auftragstyp FDL wird zum Herunterladen von Daten von einer Bank verwendet.

Die Download-Transaktion umfasst die folgenden Phasen:

- Initialisierung
- Datenübertragung
- Bestätigung

Ein Benutzer reicht die FDL-Auftragsart bei der Bank ein. Der Benutzer fordert den Download des Berichts (Format .PSR) an, um den Status der FDL-Anforderung abzurufen. Der Benutzer kann durch Verwendung der FDL-Auftragsart auch das Herunterladen anderer gültiger Dateiformate außer PSR anfordern.

**Wichtig:** Bei großen FDL-Nutzdaten sollte die Einstellung für die maximale Leerlaufzeit (MaxIdleTime) im EBICS Server Service erhöht werden. Wenn diese Einstellung zu niedrig ist, könnte die Transaktion vor der Beendigung abgebrochen werden. Die passende Einstellung für große FDL-Nutzdaten ist 300 Minuten.

## Initialisierung verarbeiten

Die Bank überprüft die Nachricht vom Benutzer. Nach erfolgter Überprüfung der Anforderung des Benutzers durch die Bank erfasst die Bank auf der Grundlage der Dateiformatangaben in der Anforderung die Auftragsdaten aus der Download-Mailbox des Benutzers.

Wenn mehr als eine Nachricht mit dem Dateiformat übereinstimmt, verknüpft die Bank den Inhalt der einzelnen Nachrichten zu einem einzelnen Auftragsdatensatz und ruft synchron den Auftragsdatenprozessor (ODP) zum Packen der Auftragsdaten auf.

Wenn das verschlüsselte Format der Auftragsdaten die Größe von 1 MB überschreitet, so werden die Auftragsdaten in Segmente aufgeteilt. Das erste Segment der Auftragsdaten und die Transaktions-ID sind in der Antwort an den Benutzer enthalten.



## Datenübertragung verarbeiten

Der Benutzer sendet die Anforderung für das nächste Datensegment. Die Bank authentifiziert die Nachricht, überprüft die Transaktion und prüft die Segmentnummer und -größe.

In jeder Übertragungsphase überträgt die Bank sämtliche Segmente, bis das letzte Segment der Auftragsdaten in ihrer Antwort an den Benutzer enthalten ist.

## Bestätigung für Daten verarbeiten

Nachdem der Benutzer das letzte Segment der Auftragsdaten von der Bank empfangen hat, leitet er die letzte Phase ein: Anhand einer Bestätigungsanforderung wird angegeben, dass die Datenübertragung erfolgreich durchgeführt wurde.

Wenn die Bank vom Benutzer eine positive Bestätigung (Empfangscode=0) erhält, verschiebt die Bank die heruntergeladenen Nachrichten aus der Download-Mailbox des Benutzers in seine Archivmailbox. Wenn die Bank hingegen eine negative Bestätigung vom Benutzer erhält, so bewahrt die Bank die heruntergeladenen Nachrichten weiterhin in der Download-Mailbox des Benutzers auf.

Wenn ein Benutzer aus seiner Archivmailbox gültige Dateiformate herunterladen möchten, bei denen es sich nicht um PSR-Berichte handelt, so muss er in der EBICS-Anforderung einen Datumsbereich angeben. Der Benutzer muss sicherstellen, dass der Datumsbereich mit dem Versanddatum der DAT-Datei übereinstimmt, an dem sie aus der Download-Mailbox in die Archivmailbox des Benutzers verschoben wurde.

## Segmentation and Recovery

The order data request (upload or download) cannot exceed 1 MB in compressed, encrypted, base64 encoded form. If the order data request exceeds 1 MB, the encoded form must be separated into segments. EBICS Banking Server is responsible for combining all these segments in order to reinstate the order data to its original form.

If an error occurs during the delivery of the order data segments, recovery can be performed. The user can download or upload the appropriate segment according to the recovery point sent in response by the server.

Recovery allows the transmission of an order to continue despite the occurrence of an error, without necessitating the retransmission of all order data segments that have been transmitted successfully.

A recovery point can be used to continue transactions from the transaction step that follows this recovery point in the transaction step sequence. Recovery points must be set during the recovery process:

- For upload transactions, the recovery point is the last transaction step wherein the bank has successfully received the request message and transmitted a response to the user. The recovery point is determined by the state of the transaction in the bank system.
- For download transactions, several recovery points may exist. All the previous transaction steps of the transaction wherein the bank has successfully received the request message and transmitted a response to the user.

## VEU-Verarbeitung

EBICS Banking Server unterstützt die verteilte elektronische Unterschrift (VEU), die es mehreren Partnern (oder Abonnenten) ermöglicht, einen Auftrag zu autorisieren.

VEU ist die Abkürzung für Verteilte Elektronische Unterschrift. Mit VEU können mehrere Partner (oder Abonnenten) einen Auftrag autorisieren. Unterschiedliche Partner von verschiedenen Kunden oder desselben Kunden können einen bestimmten Auftrag signieren. Partner können ihre Aufträge mit ausstehenden Signaturen anfordern und diese signieren oder stornieren. Das VEU-Managementsystem im EBICS Banking Server speichert die Aufträge unterschiedlicher Partner, für die Signaturen ausstehen, bis eine der folgenden Situationen auftritt:

- Die erforderliche Anzahl an rechtsverbindlichen Unterschriften wurde empfangen.
- Der Auftrag wurde abgebrochen.

VEU verwendet die folgenden Auftragsstypen:

- HVU
- HVD
- HVZ
- HVE
- HVS
- HVT (Optional)

Berechtigte Zeichnungsberechtigte eines Kunden können unterschiedliche Signaturprozesse verwenden, die möglicherweise unterschiedliche Hashprozesse unterstützen. Dies führt zu unterschiedlichen Hashwerten. Im VEU-Prozess wird der Hashwert der Auftragsdaten bereitgestellt, wenn die Auftragsstypen HVD und HVZ ausgeführt werden. Dieser Hashwert wird von der Signaturversion abgeleitet, die vom Abonnenten verwendet wird, der HVZ und HVD ausführt. Der Hashwert wird mit der Signaturversion bereitgestellt und als Attribut verwendet.

Hier finden Sie eine Zusammenfassung eines typischen VEU-Prozesses:

1. Ein EBICS-Kunde (Partner A) initiiert einen Auftrag, indem er Auftragsdaten in einer EBICS-Transaktion mit dem Auftragsattribut 0ZHNN überträgt und mit der Signaturklasse E oder T unterzeichnet.
2. Beim Empfang durch den EBICS Banking Server analysiert das VEU-Managementsystem den Auftragsstyp und die Signaturen, die bereits übertragen wurden, einschließlich der zugehörigen Klassen. Falls weitere Signaturen für die Verarbeitung des Auftrags erforderlich sind, wird dieser für den VEU-Prozess zusammen mit seinem Hashwert zwischengespeichert.
3. Ein anderer EBICS-Kunde (Partner B) mit ausstehenden Signaturen, der einen gespeicherten Auftrag unterzeichnen will, stellt mithilfe des Auftragsstyps HVU oder HVZ eine Abfrage, um herauszufinden, für welche Aufträge er zeichnungsberechtigt ist. Die Antwort enthält Informationen über:
  - Auftragsstyp
  - Auftragsnummer
  - Anzahl der erforderlichen Signaturen und Anzahl der bereits bereitgestellten Signaturen (einschließlich der Angabe, ob die eigene Signatur noch erforderlich ist oder bereits geleistet wurde)
  - Ursprünglicher Auftraggeber

- Größe der nicht komprimierten Auftragsdaten
- (Nur bei Auftragstyp HVZ) Hashwert der Auftragsdaten

Falls der Auftragstyp HVZ verwendet wurde, überspringen Sie den nächsten Schritt.

4. Partner B verwendet den Auftragstyp HVD, um den Auftrag zu überprüfen und um den Hashwert dieses Auftrag abzurufen.
5. Optional. Falls der Auftragstyp HVT von der Bank unterstützt wird, kann Partner B weitere Auftragsdetails mithilfe des Auftragstyps HVT herunterladen. Abhängig von den Anforderungsparametern empfangen Sie entweder Informationen zu einzelnen Auftragstransaktionen (Kontodaten, Betragsdaten, Verarbeitungsdaten, Verwendungsdaten und andere Beschreibungen) oder die vollständigen Auftragsdaten.
6. Wenn alle erforderlichen Informationen empfangen wurden, kann Partner B den Auftrag mithilfe von Auftragstyp HVE unterzeichnen. Das VEU-Verwaltungssystem in EBICS Banking Server überprüft die Signatur und fügt sie dem Auftrag hinzu.
7. Partner B könnte den Auftrag auch stornieren, indem er Auftragstyp HVS verwendet.
8. Wenn alle Signaturen vollständig sind, wird der EBICS Banking Server den Auftrag vollständig verarbeiten.

---

## Schlüssel verwalten

Sie können Zertifikate in das Sterling B2B Integrator-Repository einfügen sowie die im Sterling Integrator-Repository vorhandenen Zertifikate aktualisieren und abrufen.

Sie können ein mit Base64 codiertes (öffentliches oder privates) Zertifikat einfügen und Zertifikate in das Sterling B2B Integrator-Repository importieren bzw. von dort exportieren.

Sie können ferner die folgenden Tasks in Sterling B2B Integrator ausführen:

- Selbst signiertes Zertifikat mit der Schlüssellänge 2048 für EBICS erstellen
- Zertifikate von Zertifizierungsstellen (CA-Zertifikate) verwalten
- Zertifikate speichern sowie Erneuerung und Ablauf von Zertifikaten verwalten
- Öffentliches Zertifikat eines Benutzers akzeptieren
- Folgende Abonentenschlüssel durch Verwendung von SHA256 als Hashalgorithmus validieren:
  - Hashwert für den Identifikations- und den Authentifizierungsschlüssel (in Hex-Format)
  - Hashwert für den Verschlüsselungsschlüssel (in Hex-Format)
  - Hashwert für elektronische Signatur (in Hex-Format)

Verwenden Sie den EBICS-Service für Zertifikatexport, um die in Sterling B2B Integrator vorhandenen Zertifikate in ein externes System zu exportieren. Verwenden Sie diesen Service, wenn Sie die in Sterling B2B Integrator vorhandenen Zertifikate mit einer externen Datenbank oder einem internen System synchronisieren möchten.

Verwenden Sie den EBICS-Service zum Importieren von Zertifikaten, um Zertifikate aus einem externen Repository zu Sterling B2B Integrator hinzuzufügen. Sie haben außerdem die Möglichkeit, die abgelaufenen oder ungültigen Zertifikate zu löschen.

## Funktionen der Schlüsselverwaltung

Schlüsselverwaltung und -speicher führen folgende Funktionen aus:

- Doppelte Schlüsselüberprüfung - Das Zertifikat, das für die Authentifizierung und Verschlüsselung verwendet wird, kann nicht auch für das ES-Zertifikat verwendet werden. Verwenden Sie jeweils einen eindeutigen Schlüsselsatz für die Authentifizierung bzw. Verschlüsselung und für die Vertragsunterzeichnung.
- X.509-Erweiterung für Schlüsselnutzung – EBICS Banking Server unterstützt die Verwendung von X.509 als Erweiterung der Schlüsselnutzung.
- OCSP- und CRL-Zertifikatsüberprüfung

Der Schlüsselmanager verwaltet die Zertifikate im Sterling B2B Integrator-Repository. Zertifikate werden im Sterling B2B Integrator-Repository eingefügt, aktualisiert und abgerufen und es werden Funktionen wie beispielsweise die Berechnung des Hashwerts für das Zertifikat durchgeführt.

Die Schlüsselverwaltung überprüft die Clientzertifikate und checkt diese in den Server ein, bevor sie verwendet werden können. Sie müssen die CA-signierten Zertifikate von einer Zertifizierungsstelle anfordern. In einem CA-signierten Zertifikat unterzeichnet der Aussteller das Zertifikat. Um die Authentizität des Benutzerzertifikats zu überprüfen, führt der EBICS Banking Server eine verkettete Signaturprüfung bis zum Zertifikat der Stammzertifizierungsstelle durch.

Der EBICS-Administrator muss die von der Zertifizierungsstelle signierten Zertifikate und die temporären von der Zertifizierungsstelle signierten Zertifikate in den CA-Zertifikatspeicher von Sterling B2B Integrator einchecken, bevor die EBICS-Transaktionen ausgeführt werden.

Der Client muss drei Typen von Zertifikaten zur Verfügung stellen:

- Authentifizierungszertifikat
- Verschlüsselungszertifikat
- Zertifikat für elektronische Signatur (ES)

Der öffentliche Schlüssel des Authentifizierungszertifikats wird verwendet, um digitale Signaturen zu überprüfen. Die Authentifizierungszertifikate können entweder CA-signiert oder selbst signiert sein. Der Wert des Schlüsselnutzungsfelds für ein Authentifizierungszertifikat ist die digitale Signatur. Eine digitale Signatur wird für die Entitätsauthentifizierung und die Authentifizierung der Datenherkunft mit Integrität verwendet.

Der öffentliche Schlüssel des Verschlüsselungszertifikats wird verwendet, um Auftragsdaten zu verschlüsseln. Die Verschlüsselungszertifikate können entweder CA-signiert oder selbst signiert sein. Der Wert des Schlüsselnutzungsfelds für ein Verschlüsselungszertifikat ist die Schlüsselverschlüsselung. In EBICS wird ein symmetrischer Schlüssel verwendet, um verschlüsselte oder entschlüsselte Auftragsdaten im Datenstrom zu übertragen. Der symmetrische Schlüssel wird für den Transport mit dem öffentlichen Schlüsselwert des Verschlüsselungszertifikats verschlüsselt. Die Schlüsselverschlüsselung wird verwendet, wenn ein Zertifikat mit einem Protokoll vorhanden ist, das Schlüssel verschlüsselt.

Der öffentliche Schlüssel des Zertifikats für elektronische Signaturen (ES) wird verwendet, um die Signatur der Auftragsdaten zu überprüfen. Der öffentliche Schlüsselwert eines ES-Zertifikats darf nicht mit dem Wert eines Authentifizierungs- oder Verschlüsselungszertifikats übereinstimmen. Der Wert des Schlüsselnutzungsfelds für ein Zertifikat für elektronische Signatur ist der fälschungssichere Herkunftsnachweis. Der fälschungssichere Herkunftsnachweis schützt die unterzeichnende Entität davor, eine Aktion fälschlicherweise zurückzuweisen. Eine Ausnahme davon bildet das Unterzeichnen von Zertifikaten und CRLs. Es gibt zwei Typen elektronischer Signaturen:

- Transportsignatur – kann CA-signiert oder selbst signiert sein
- Persönliche Signatur – muss CA-signiert sein

---

## EBICS-Berichte generieren und abrufen

Sie verwenden den EBICS-Berichtsservice, um mit jeder Upload-Auftragsanforderung (FUL) einen Payment Status Report (PSR: Zahlungsstatusbericht) zu generieren. Der PSR-Bericht liegt in XML-Format vor und entspricht dem Schema 'pain.002.001.02'. Nachdem der .PSR-Bericht erfolgreich generiert wurde, wird er in der Download-Mailbox des EBICS-Benutzers abgelegt.

Ein PSR-Bericht wird nach der synchronen Auftragsverarbeitung eines jeden FUL generiert. Ein Benutzer kann eine FDL-Anforderung mit dem Dateiformat 'pain.002.001.02.ack' senden, um den .PSR-Bericht abzurufen. Wenn in der EBICS-Anforderung kein Datumbereich angegeben ist, so verknüpft die Bank die PSR-Berichte in der Download-Mailbox des Benutzers und packt die Auftragsdaten in die EBICS-Antwort.

Wenn die Bank vom Benutzer auf der Grundlage des Parameterwertes unter dem Element 'FDLOrderParams' in der FDL-Anforderung eine positive Bestätigung erhält, so werden die PSR-Berichte in der Download-Mailbox des Benutzers in seine Archivmailbox verschoben. Geht nach einer zuvor angegebenen Zeitspanne keine positive Bestätigung ein, so ändert die Planungsfunktion des EBICS-Server-Service für die PSR-Berichte in der Download-Mailbox des Benutzers den Wert für die Extraktionsanzahl zurück in 1 und ermöglicht dem Benutzer dadurch das erneute Herunterladen der PSR-Berichte.

Wenn ein Benutzer aus seiner Archivmailbox die PSR-Berichte herunterladen möchte, so muss er in der EBICS-Anforderung einen Datumbereich angeben. Der Benutzer muss sicherstellen, dass der Datumbereich mit dem Versanddatum des .PSR-Berichts übereinstimmt, an dem sie aus der Download-Mailbox in die Archivmailbox des Benutzers vorschoben wurde.

---

## EBICS-Server verwalten

Der EBICS-Server ist als Service in Sterling B2B Integrator integriert. Der EBICS-Server-Service ist für die Abwicklung eingehender EBICS-Anforderungen (über HTTP und HTTPS) nach den EBICS-Protokollspezifikationen sowie für die Generierung und das Senden der entsprechenden Antwort zurück an Benutzer zuständig.

Der EBICS-Server verarbeitet die Generierung und die Überprüfung der elektronischen Signatur (ES) sowie die Identifikation und Authentifizierung von EBICS-Nachrichten. Er bildet außerdem eine Schnittstelle zum Subscription Manager, um die Profilinformationen von Banken, Partnern, Benutzern und Auftragsarten abzurufen, die für die Prüfung und Authentifizierung von Nachrichten und Transaktio-

nen erforderlich sind. Die (synchronen und asynchronen) Verarbeitungsflüsse von Anforderungen wie etwa FUL und FDL werden ebenfalls von dem Service gehandhabt. Sie können den Service so konfigurieren, dass er bei einer synchronen Transaktion das EBICS-Repository aktualisiert und Ereignisbenachrichtigungen an eine externe Anwendung sendet. Die Verwaltung des Nachrichtenflusses für die Initialisierungs- und Übertragungsphasen von EBICS-Transaktionen zählt ebenso zu den Schlüsselzuständigkeiten des Service. Der Lebenszyklus der EBICS-Transaktionen im Banksystem und der Status offener Transaktionen werden vom EBICS-Server verwaltet, der außerdem auch als Zwischenspeicher für übertragene Auftragsdatensegmente und elektronische Signaturen (ES) fungiert.

Wenn banktechnische Auftragsdaten heruntergeladen werden, sammelt der EBICS-Server alle verfügbaren Auftragsdaten in der Mailbox des Benutzers und verknüpft diese zu einem einzelnen Dokument, das er dann an den Auftragsdatenprozessor (ODP) sendet, damit dort das Dokument gepackt wird, d. h. signiert, komprimiert, verschlüsselt und codiert.

Informationen zum Konfigurieren des EBICS-Server-Service finden Sie unter dem Thema *EBICS-Server-Service*.

---

## Systemauftrag verwalten

Der System Order Manager arbeitet zum Aktualisieren und Abfragen der Schlüsselzertifikate und der referenziellen Informationen eines Benutzers und zum Herunterladen von Bankparametern und Bankzertifikaten eng mit dem Transaction Manager und Subscription Manager zusammen. Er generiert und ruft XML-Auftragsdaten auf der Grundlage der Profilinformatoren ab.

Der System Order Manager wickelt außerdem die Implementierung von Upload- und Download-Systemaufträgen ab. Die folgende Tabelle enthält eine Auflistung der unterstützten Upload-Systemauftragsarten für EBICS-Transaktionen:

Upload-Systemauftragstyp	Beschreibung
INI	Wird in der Abonnenteninitialisierung verwendet. Sendet das banktechnische öffentliche Zertifikat eines Kunden an den EBICS Banking Server. Die Auftragsdaten werden komprimiert und mit Base64 verschlüsselt.
HIA	Wird zum Übertragen von öffentlichen Benutzerzertifikaten zur Identifikation, Authentifizierung und Verschlüsselung innerhalb des Frameworks der Abonnenteninitialisierung verwendet. Die Auftragsdaten werden komprimiert und mit Base64 verschlüsselt.
PUB	Wird zum Aktualisieren der Zertifikate von Kunden verwendet. Sendet das banktechnische öffentliche Zertifikat des Kunden zum Aktualisieren des EBICS Banking Server. Die Auftragsdaten werden unterzeichnet, komprimiert, verschlüsselt und mit Base64 codiert.

Upload-Systemauftragstyp	Beschreibung
HCA	<p>Wird zum Aktualisieren des Zertifikats eines Kunden verwendet. Sendet die folgenden Zertifikate zum Aktualisieren des EBICS Banking Server:</p> <ul style="list-style-type: none"> <li>• Öffentliches Zertifikat für Identifikation und Authentifizierung</li> <li>• Öffentliches Zertifikat für Verschlüsselung</li> </ul> <p>Die Auftragsdaten werden unterzeichnet, komprimiert, verschlüsselt und mit Base64 codiert.</p>
HCS	<p>Wird zum Aktualisieren des Zertifikats eines Kunden verwendet. Sendet die folgenden Zertifikate zum Aktualisieren des EBICS Banking Server:</p> <ul style="list-style-type: none"> <li>• Öffentliches banktechnisches Zertifikat</li> <li>• Öffentliches Zertifikat für Identifikation und Authentifizierung</li> <li>• Öffentliches Zertifikat für Verschlüsselung</li> </ul> <p>Die Auftragsdaten werden unterzeichnet, komprimiert, verschlüsselt und mit Base64 codiert.</p>
SPR	<p>Wird zum Aussetzen der Zugriffsberechtigung eines Benutzers verwendet. Die Auftragsdaten werden unterzeichnet, komprimiert, verschlüsselt und mit Base64 codiert.</p>

Die folgende Tabelle enthält eine Auflistung der für EBICS-Transaktionen unterstützten Download-Systemauftragsarten:

Download-Systemauftragsart	Beschreibung
HPB	<p>Wird zum Herunterladen öffentlicher Bankzertifikate vom EBICS Banking Server verwendet. Die Auftragsdaten werden komprimiert, verschlüsselt und mit Base64 codiert. Die Antwortnachricht wird mithilfe des Authentifizierungszertifikats mit einer digitalen XML-Signatur signiert. Die Auftragsdaten werden nicht signiert.</p>
HPD	<p>Wird zum Herunterladen von Bankparametern vom EBICS Banking Server verwendet. Die Auftragsdaten werden komprimiert, verschlüsselt und mit Base64 codiert. Die Antwortnachricht wird mithilfe des Authentifizierungszertifikats mit einer digitalen XML-Signatur signiert. Die Auftragsdaten werden nicht signiert.</p>
HEV	<p>Wird zum Herunterladen von Informationen zu unterstützten EBICS-Versionen verwendet. Die Antwortnachricht enthält Klartext. Es sind keine Auftragsdaten in einer HEV-Antwort enthalten.</p>

Download-Systemauftragsart	Beschreibung
HKD	Wird zum Herunterladen von Kunden- und Abonentendaten verwendet. Kann verwendet werden, wenn der Benutzer sich im Status 'Bereit' befindet. Ruft Informationen ab, die von der Bank gespeichert wurden, und das Unternehmen des Abonnenten und die zugehörigen Abonnenten (einschließlich der bankeigenen Informationen) betreffen. Die Auftragsdaten werden komprimiert, verschlüsselt und mit Base64 codiert. Die Antwortnachricht wird mithilfe des Authentifizierungszertifikats mit einer digitalen XML-Signatur signiert. Die Auftragsdaten werden nicht signiert.
HTD	Wird zum Herunterladen von Kunden- und Abonentendaten verwendet. Kann verwendet werden, wenn der Benutzer sich im Status 'Bereit' befindet. Ruft Informationen ab, die von der Bank gespeichert wurden, und das Unternehmen des Abonnenten oder die bankeigenen Informationen betreffen. Die Auftragsdaten werden komprimiert, verschlüsselt und mit Base64 codiert. Die Antwortnachricht wird mithilfe des Authentifizierungszertifikats mit einer digitalen XML-Signatur signiert. Die Auftragsdaten werden nicht signiert.

Ruft Informationen ab, die von der Bank gespeichert wurden, und das Unternehmen des Abonnenten betreffen. Die Abonnenten können Informationen abrufen, die von der Bank gespeichert wurden und das Unternehmen des Abonnenten sowie alle zugehörigen Abonnenten betreffen, indem die Auftragstypen HKD und HTD verwendet werden, sobald der Benutzerstatus 'Bereit' lautet und so angibt, dass der Benutzer Transaktionen mit der Bank ausführen kann. Die Antwort der Bank enthält eine Liste der Konten der des Kunden.

Die Kontoinformationen sind in der HKD-Antwort enthalten, wenn mindestens eine der folgenden Bedingungen zutrifft:

- In der vertraglichen Vereinbarung mit der Bank ist angegeben, dass die Kontoauszüge für dieses Konto mit dem Kunden gemeinsam genutzt werden.
- Mindestens ein Abonnent des Kunden ist für dieses Konto zeichnungsberechtigt.

Die Abonnenten können Informationen abrufen, die von der Bank gespeichert wurden und das Unternehmen des Abonnenten oder bankeigene Informationen betreffen, indem Sie den Auftragstyp HTD verwenden. Informationen zu den zugehörigen Abonnenten des Unternehmens werden bei diesem Auftragstyp nicht gemeinsam genutzt. Sie müssen den Auftragstyp HKD verwenden, um Informationen abzurufen, die zu dem Unternehmen und den zugehörigen Abonnenten (einschließlich der bankeigenen Informationen) gehören. Die HKD- und HTD-Antwort listet die zugehörigen Konten der Partner auf, zu denen der Subskribent zugangsberechtigt ist.

Die Antwortnachricht des HKD-Download-Systemauftrags umfasst die folgenden Parameter:



- HostID
- PartnerInfo - Umfasst Details der Partner wie deren Adresse, die Kontoinformationen, für die der Abonnent zugangsberechtigt ist, und die Auftragsstypen, die der Partner verwenden darf.
- UserInfo - Umfasst Details des Abonnenten wie die Benutzer-ID, den Status des Abonnenten und Informationen zur Benutzerberechtigung. Die Informationen zur Benutzerberechtigung enthalten die Berechtigungsstufe der Liste der Auftragsstypen, zugehörige Konten und den Höhe des Schwellenwerts.

---

## Auftragsdaten verarbeiten

Zur Sicherstellung der sicheren Übertragung von Auftragsdaten müssen die Auftragsdaten gepackt werden. Das Packen der Auftragsdaten umfasst das Signieren, Komprimieren Verschlüsseln und Codieren gemäß Base64 je nach Anforderungen der Auftragsart. Der Empfänger muss die Auftragsdaten entpacken, um die Attribute anzeigen zu können. Das Entpacken der Auftragsdaten umfasst das Überprüfen, Dekomprimieren, Entschlüsseln und Decodieren gemäß Base64 je nach der Anforderungen der Auftragsart.

Der Order Data Processor (ODP) ist für das Packen und Entpacken der Auftragsdaten zuständig. Er bildet zum Abrufen der relevanten Informationen, die zum Packen und Entpacken der Auftragsdaten erforderlich sind, eine Schnittstelle zum Subscription Manager und Transaction Manager. Die Profilinformatoren können zum Beispiel die Transaktions-ID, die Richtung des Datenflusses (Upload oder Download), den Antworttyp (synchron oder asynchron), die Art der erforderlichen Prozesse, die Objekt-ID des verschlüsselten Schlüssels und die Objekt-ID der elektronischen Signatur (ES) umfassen. Der EBICS-Service für Auftragsverarbeitung nimmt EBICS-Transaktionen und den Abruf von Benutzern vor und führt das Packen und Entpacken verschlüsselter symmetrischer Schlüssel aus. Auf der Basis der abgerufenen Profilinformatoren ermittelt der EBICS-Service für Auftragsverarbeitung, ob ein Packen oder Entpacken der Auftragsdaten erforderlich ist, und ruft den entsprechenden Service zum Packen bzw. Entpacken auf.

Der Authorized Order Manager ist dafür verantwortlich, den Order Data Processor zum Entpacken der von der FUL-Auftragsartanforderung empfangenen Auftragsdaten, zum Routing (Weiterleiten) der entpackten Auftragsdaten an die Upload-Mailbox des Backend-Abonnenten und zum Umbenennen der entpackten Daten gemäß einer definierten Namenskonvention zu initialisieren.

Abgesehen vom EBICS-Service für Auftragsverarbeitung stehen in Sterling B2B Integrator die folgenden Services zur Verarbeitung von Auftragsdaten zur Verfügung:

- Der EBICS-Service für Auftragsautorisierung wickelt eingehende Auftragsanforderungen für die banktechnische Upload-Auftragsart (FUL) ab. Wenn ein Auftrag die Anzahl der erforderlichen Signaturen vorweisen kann, leitet dieser Service den Auftrag an die Upload-Mailbox des Abonnenten weiter. Andernfalls leitet dieser Service den Auftrag an die Mailbox für anstehende Aufträge weiter.
- Der EBICS-Service für Auftragsstreaming packt und entpackt Auftragsartdaten anhand der Pipelinefunktionalität in Sterling B2B Integrator.
- Der EBICS-Service zum Packen von elektronischen Signaturen (ES) packt oder entpackt Schlüsselinformationen, die beim Signieren und Überprüfen der elektronischen Signatur (ES) verwendet werden.
- Der EBICS-Service für Komprimierung führt die Komprimierung und Dekomprimierung von Auftragsdaten mit zlib im Pipelinemodus aus.

- Der EBICS-Service für Verschlüsselung führt die Verschlüsselung und Entschlüsselung von Auftragsdaten anhand des Algorithmus AES-128 im Pipelinemodus aus. Der Verschlüsselungsalgorithmus E002 wird unterstützt.
- Der EBICS-Service für Codierung führt die Codierung und Decodierung von Auftragsdaten anhand der Methode Base64 im Pipelinemodus aus.
- Der EBICS-Service für Signierung nimmt die Signierung und Überprüfung von Auftragsdaten für im Pipelinemodus berechneten Digest SHA-256 vor. Die Signaturalgorithmen A005 und A006 werden unterstützt.

Auftragsdaten müssen für Upload-Transaktionen entpackt und für Download-Transaktionen gepackt werden.

Der Prozess des Packens setzt sich aus den folgenden Einzelprozessen zusammen. Abhängig von der Auftragsart sind jedoch unter Umständen ein oder mehrere der folgenden Prozesse nicht erforderlich:

1. Signieren
2. Komprimieren
3. Verschlüsseln
4. Codieren gemäß Base64

Das folgende Beispiel veranschaulicht, wie die Verschlüsselung einer Auftragsart erfolgt. Ein Geschäftsprozess ruft den Service für die Verschlüsselung auf. Wenn die Auftragsdaten bereits signiert worden sind, übergibt der Geschäftsprozess den symmetrischen Schlüssel an den Verschlüsselungsservice. Wenn die Auftragsdaten noch nicht signiert worden sind, generiert der Service für die Verschlüsselung den symmetrischen Schlüssel und gibt diesen an den Geschäftsprozess zurück. Nachdem der symmetrische Schlüssel erstellt worden ist, ruft der Geschäftsprozess den EBICS-Service für Auftragsverarbeitung auf, wobei als Ausgabenachrichtentyp der Wert 'setEncryptedKey' festgelegt ist.

Der Prozess des Entpackens setzt sich aus den folgenden Einzelprozessen zusammen. Abhängig von der Auftragsart sind jedoch unter Umständen ein oder mehrere der folgenden Prozesse nicht erforderlich:

1. Decodieren gemäß Base64
2. Entschlüsseln
3. Entkomprimieren
4. Signatur überprüfen

Das folgende Beispiel veranschaulicht die Entschlüsselung einer Auftragsart. Ein Geschäftsprozess ruft den EBICS-Service für Auftragsverarbeitung auf, wobei für den Ausgabenachrichtentyp der Wert 'getEncryptedKey' festgelegt ist. Der gemäß Base64 verschlüsselte geheime Schlüssel wird abgerufen und wird dann in den Verarbeitungsdaten zur Verwendung durch den Service für Verschlüsselung angegeben.

## Elektronische Signaturen

Die elektronische Signatur (ES) stellt die Authentifizierung der Auftragsdaten sicher. Die Signatur stellt die Integrität und den fälschungssicheren Herkunftsnachweis der Auftragsdaten sicher, die vom Bankserver gesendet wurden.

EBICS gibt zwei Signaturklassen für ES an:

- Persönliche Signatur

- Einzelne Signatur vom Typ E
- Erste Signatur vom Typ A
- Zweite Signatur vom Typ B
- Transportsignatur vom Typ T

Sterling B2B Integrator unterstützt die folgenden Signaturtypen:

- Transportsignatur vom Typ T
- Persönliche Signatur oder banktechnische ES vom Typ E – Einzelsignatur

Transportsignaturen können entweder selbst signierte oder CA-signierte Zertifikate sein. Persönliche Signaturen müssen CA-signiert und von der Bank anerkannt sein. Verwenden Sie die Transportsignatur, um den Auftrag und die persönliche Signatur zu übergeben, um die Bestellung zu autorisieren.

In persönlichen Signaturen müssen Sie die Anzahl der Signaturen für jeden Auftragsstyp oder für jedes Dateiformat im Vertrag angeben, um die Auftragsdaten zu verarbeiten. Die maximale zulässige Anzahl der persönlichen Signaturen beträgt 2. Die persönliche Signatur vom Typ E kann die folgenden Signaturen enthalten:

- Einzel
- Optional Dual
- Obligatorisch Dual

## **Vorabvalidierung**

Bei der Verwendung von banktechnischen Upload-Auftragstypen, kann der Abonent im ersten Transaktionsschritt Informationen an die Bank senden. Die Bank kann die Auftragsdaten vorab validieren. Die Vorabvalidierung von Auftragsdaten umfasst Folgendes:

- Verifizierung des Datenauszugs
- Kontoberechtigung
- Überprüfung des Grenzwertbetrags

Nach der erfolgreichen Vorabvalidierung der Auftragsdaten empfängt das System die FUL-Datei. Die Bank kann die Vorabvalidierung zur Verarbeitung von Auftragsdaten verwenden, wenn die folgenden Voraussetzung erfüllt sind:

- Die Bank unterstützt die Funktion zur Vorabvalidierung
- Der Vorabvalidierungsknoten ist in der eingehende Anforderung vorhanden

### **Vorabvalidierung des Datenauszugs**

Die Bank kann den Datenauszug überprüfen, wenn die folgenden Voraussetzungen erfüllt sind:

- Die Bank unterstützt die Funktion zur Vorabvalidierung.
- Die Vorabvalidierung oder der Datenauszugsknoten (DataDigest) sind in der eingehenden Anforderung enthalten.
- Der Auftragstyp ist ein beliebiger Upload-Auftragstyp, jedoch nicht die SPR-Anforderung.

### **Die Vorabvalidierung der Kontoberechtigung und des Grenzwertbetrags**

Die Bank kann die Kontoberechtigung und den Grenzwertbetrag überprüfen, wenn die folgenden Voraussetzungen erfüllt sind:

- Die Bank unterstützt die Funktion zur Vorabvalidierung.
- Die Vorabvalidierung oder der Kontoberechtigungsknoten (AccountAuthorization) sind in der eingehenden Anforderung enthalten.
- Das Attribut OrderAttribute ist in der eingehenden Anforderung nicht auf DZHNN festgelegt.
- Der Auftragstyp ist in der eingehenden Anforderung auf einen technischen Upload-Auftragstyp (FUL) festgelegt.
- Die Signaturklasse des Unterzeichners in der Vertragsgenehmigung ist mindestens B.

Die Vorabvalidierung überprüft die für die Signatur vorgesehenen Kontoinformationen und den Grenzwertbetrag, falls die minimale und maximale Anzahl persönlicher Signaturen definiert ist, die für die Berechtigung des Auftrags definiert sind. Das Konto, das unter AccountAuthorization aufgelistet ist, muss ein gültiges Partnerkonto sein. Alle Unterzeichner müssen mit der Benutzerberechtigung für alle in der Vorabvalidierung aufgelisteten Konten konfiguriert sein. Die Menge der angegebenen Währungswerte darf den Höchstbetrag nicht überschreiten, der in der Konfiguration der Benutzerberechtigung für eine beliebige Signatur festgelegt wurde.

---

## Integration mit Sterling File Gateway vornehmen

Sterling File Gateway bietet eine sichere Dateiübertragung zwischen internen und externen Partnern mithilfe derselben oder anderer Kommunikationsprotokolle, Dateinamenskonventionen und Dateiformaten. Sterling File Gateway unterstützt EBICS bei der Ausführung umfangreicher und großvolumiger Dateiübertragungen mit End-to-End-Sichtbarkeit der Dateibewegung in einem prozessorientierten und hochgradig skalierbaren Framework, das die bei Dateiübertragungen anfallenden Herausforderungen wie etwa Protokoll- und Dateibrokering, Automation und Datensicherheit entschärft.

Die Bewegung von Dateien zwischen dem EBICS-Server und Sterling File Gateway erfolgt über gemeinsam genutzte Mailboxen und Partner. Der Subscription Manager erstellt während der Erstellung von Partnern Mailboxen in der Benutzer-/Partner-/Posteingangsstruktur.

Sterling File Gateway verwendet die Bereitstellungsfakten als Teil der Definition der Routingkanalvorlage. In EBICS-Szenarien verwendete Routingkanalvorlagen müssen die Konfiguration von Bereitstellungsfakten enthalten. Routingkanäle, die die Vorlagen verwenden, müssten die Spezifikation von Werten für Bereitstellungsfakten enthalten.

Bei eingehenden Szenarien verwendet der EBICS Order Data Processor (ODP) einen EBICS-Auftragsdateiupload (FUL) von einem EBICS-Client an einen EBICS-Server, entpackt die Nutzdaten und legt diese in einer Benutzer-/Partner-/Posteingangsstruktur ab. Sterling File Gateway ist für das Routing von dieser Mailbox für die Downstream-Verarbeitung und die letztendliche Zustellung zu einem Verbraucher konfiguriert.

Beim ausgehenden Szenario ist Sterling File Gateway zum Ablegen einer Nachricht in einer Verbrauchermailbox konfiguriert, die dann weitergeleitet und in Benutzer/Partner/Postausgang gespeichert wird. Bei einem EBICS-Auftragsdateidownload (FDL) von einem EBICS-Client zu einem EBICS-Server packt der EBICS Order Data Processor (ODP) die Nachricht und macht sie dem Client verfügbar.

Sterling File Gateway ermöglicht Operatoren die Suche nach Transaktionen und die Anzeige von Routen und Zustellungen.

Bestimmte Prozeduren sind erforderlich, um die Integration mit Sterling File Gateway einzuleiten. Weitere Informationen zur Integration von Mit Sterling File Gateway finden Sie unter dem Thema *Sterling File Gateway Integration mit EBICS* unter [http://www.ibm.com/support/knowledgecenter/SS4TGX\\_2.2.0/com.ibm.help.sfg\\_ebics.doc/SFGEB\\_IntegrationwEBICS.html](http://www.ibm.com/support/knowledgecenter/SS4TGX_2.2.0/com.ibm.help.sfg_ebics.doc/SFGEB_IntegrationwEBICS.html).



---

## Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM® die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

*IBM Director of Licensing*

*IBM Europe, Middle East Africa*

*Tour Descartes 2, avenue Gambetta*

*92066 Paris La Defense*

*France*

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

*IBM Corporation*

*J46A/G4*

*555 Bailey Avenue*

*San Jose, CA 95141-1003*

*U.S.A.*

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

COPYRIGHTLIZENZ:



Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellsprache geschrieben sind und Programmier Techniken in verschiedenen Betriebsumgebungen veranschaulichen. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, zu verwenden, zu vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle für die Betriebsumgebung konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten. Die Beispielprogramme werden ohne Wartung (auf "as-is"-Basis) und ohne jegliche Gewährleistung zur Verfügung gestellt. IBM übernimmt keine Haftung für Schäden, die durch die Verwendung der Beispielprogramme entstehen.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© IBM 2015. Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. 2015.

Wird dieses Buch als Softcopy (Book) angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

## **Marken**

IBM, das IBM Logo und ibm.com sind eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicennamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

IT Infrastructure Library ist eine eingetragene Marke der Central Computer and Telecommunications Agency. Die Central Computer and Telecommunications Agency ist nunmehr in das Office of Government Commerce eingegliedert worden.

Intel, das Intel-Logo, Intel Inside, das Intel Inside-Logo, Intel Centrino, das Intel Centrino-Logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium und Pentium sind Marken oder eingetragene Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA oder anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

ITIL ist eine eingetragene Marke, eine eingetragene Gemeinschaftsmarke des Office of Government Commerce und eine eingetragene Marke, die beim U.S. Patent and Trademark Office eingetragen ist.

UNIX ist eine eingetragene Marke von The Open Group in den USA und anderen Ländern.

Java™ und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Cell Broadband Engine wird unter Lizenz verwendet und ist eine Marke der Sony Computer Entertainment, Inc. in den USA und/oder anderen Ländern.

Linear Tape-Open, LTO, das LTO-Logo, Ultrium und das Ultrium-Logo sind Marken von HP, der IBM Corporation und von Quantum in den USA und/oder anderen Ländern.

Connect Control Center®, Connect:Direct®, Connect:Enterprise, Gentran®, Gentran:Basic®, Gentran:Control®, Gentran:Director®, Gentran:Plus®, Gentran:Realtime®, Gentran:Server®, Gentran:Viewpoint®, Sterling Commerce™, Sterling Information Broker®, und Sterling Integrator® sind Marken oder eingetragene Marken der Sterling Commerce, Inc., einer IBM Company.

Weitere Unternehmens-, Produkt- und Servicennamen können Marken oder Servicemarken anderer Hersteller sein.





Gedruckt in Deutschland