

Sterling B2B Integrator



Visión general del Cliente EBICS

Versión 5.24

Sterling B2B Integrator



Visión general del Cliente EBICS

Versión 5.24

Nota

Antes de utilizar esta información y el producto al que da soporte, lea la información del apartado "Avisos" en la página 31.

Copyright

Este manual es la traducción del original en inglés *Sterling B2B Integrator EBICS Client Overview*. Esta edición se aplica a la Versión 5 Release 2 Modificación 4 de Sterling B2B Integrator y a todos los releases y modificaciones posteriores hasta que no se indique lo contrario en nuevas ediciones.

© Copyright IBM Corporation 2000, 2012.

Contenido

Capítulo 1. Visión general de EBICS . . . 1

Capítulo 2. Visión general del Cliente EBICS 3

Capítulo 3. Arquitectura y características esenciales del Cliente EBICS 5

Arquitectura del Cliente EBICS	5
Componentes del Cliente EBICS	7
Características esenciales del Cliente EBICS.	10
Tipos de usuario.	10
Certificados y claves	12
Tipos de orden	13
Firmas pendientes	16
Recuperación de órdenes	17
Búsqueda de órdenes y resumen de órdenes	17

Visor de sucesos.	19
Tablas de restauración.	20

Capítulo 4. Requisitos de configuración 21

Configuración necesaria en Sterling B2B Integrator	21
Configuración e inicialización del usuario	21
Configuración del banco	22
Configuración del formato de archivo	23
Configuración de la oferta	23
Configuración de permisos de usuario	24

Capítulo 5. Envío de órdenes 25

Índice 29

Avisos 31

Capítulo 1. Visión general de EBICS

Electronic Banking Internet Communication Standard (EBICS) es un estándar de comunicaciones y de seguridad basado en Internet. EBICS se utiliza principalmente para la transferencia remota de datos, tales como transacciones corporativas de pagos, entre una organización y un banco.

EBICS permite intercambiar archivos de datos con independencia de los estándares y formatos de los mensajes. EBICS utiliza procedimientos reconocidos de firma digital y cifrado. Las características de EBICS están basadas en estándares internacionales de comunicación por internet y seguridad mejorada, tales como XML, HTTPS, TLS y SSL. EBICS también permite que los clientes corporativos de países que han adoptado EBICS puedan efectuar transacciones con cualquier banco ubicado en esos países que haga uso del mismo software.

En las transacciones del Cliente EBICS intervienen las entidades siguientes:

Organización

Es la organización o compañía que utiliza el Cliente EBICS para realizar transacciones con el banco.

Banco Son las instituciones financieras con las que la organización realiza transacciones. EBICS Banking Server está instalado en el banco.

Socio Es el departamento o unidad de la organización que realiza transacciones con el banco.

Usuario o suscriptor

Es el personal del departamento que realiza las transacciones EBICS.

Una organización debe cumplir una serie de requisitos previos para poder utilizar transacciones EBICS con un banco determinado. El requisito básico para realizar transacciones EBICS es el establecimiento de un contrato entre el socio y el banco. En este contrato se acuerdan las cuestiones siguientes:

- Tipo de transacciones comerciales.
- Información sobre las cuentas bancarias del usuario.
- Información sobre los usuarios que trabajan con el sistema bancario.
- Autorizaciones y permisos de los usuarios.

El socio recibe los datos de acceso del banco (parámetros bancarios) después de firmado el contrato. El banco configura los datos maestros del socio y del usuario contenidos en el sistema bancario de acuerdo con los acuerdos contractuales. Otros requisitos previos son la inicialización del suscriptor, la descarga de los certificados públicos del banco por el usuario, la verificación de los certificados públicos del usuario por el banco y la verificación de los certificados del banco por el socio comercial.

IBM® Sterling B2B Integrator ofrece una solución EBICS completa al proporcionar una plataforma segura, flexible y eficiente a los bancos y organizaciones para realizar transacciones. La puesta en práctica de esta solución consta de dos componentes principales: EBICS Banking Server y el Cliente EBICS. EBICS Banking Server (servidor) representa un banco y el Cliente EBICS representa una organización. Tanto el servidor como el cliente se despliegan en Sterling B2B Integrator.

Capítulo 2. Visión general del Cliente EBICS

El Cliente EBICS de Sterling B2B Integrator es una aplicación cliente-servidor. Proporciona una solución EBICS completa para que una organización realice transacciones con bancos. Mediante el Cliente EBICS, un socio puede configurar y gestionar varios bancos, socios y usuarios. Varios usuarios pueden realizar transacciones con varios bancos (EBICS Banking Servers) sobre HTTP o HTTPS e intercambiar mensajes transaccionales de acuerdo con EBICS.

Los socios puede realizar las tareas siguientes en la interfaz de panel de instrumentos del Cliente EBICS:

- Configurar usuarios
- Configurar bancos
- Configurar valores de seguridad para usuarios
- Verificar valores de seguridad de un banco
- Crear y gestionar formatos de archivo
- Crear y gestionar permisos de usuario
- Crear y gestionar ofertas
- Configurar órdenes
- Enviar órdenes
- Ver sucesos e informes relacionados con órdenes

Nota: El Cliente EBICS permite la implementación en francés y alemán de EBICS versión 2.4.2.

Capítulo 3. Arquitectura y características esenciales del Cliente EBICS

La sección Arquitectura y características esenciales del Cliente EBICS proporciona una visión general de la arquitectura del Cliente EBICS y describe las características esenciales de ese producto.

Arquitectura del Cliente EBICS

El Cliente EBICS se despliega sobre Sterling B2B Integrator y reutiliza algunas de las funciones básicas siguientes de Sterling B2B Integrator:

- Creación y gestión de un socio comercial
- Gestión de certificados digitales
- Creación y gestión de buzones
- Creación de usuarios
- Ejecución de servicios y adaptadores
- Planificación de procesos de negocio

El diagrama siguiente muestra la arquitectura del Cliente EBICS.

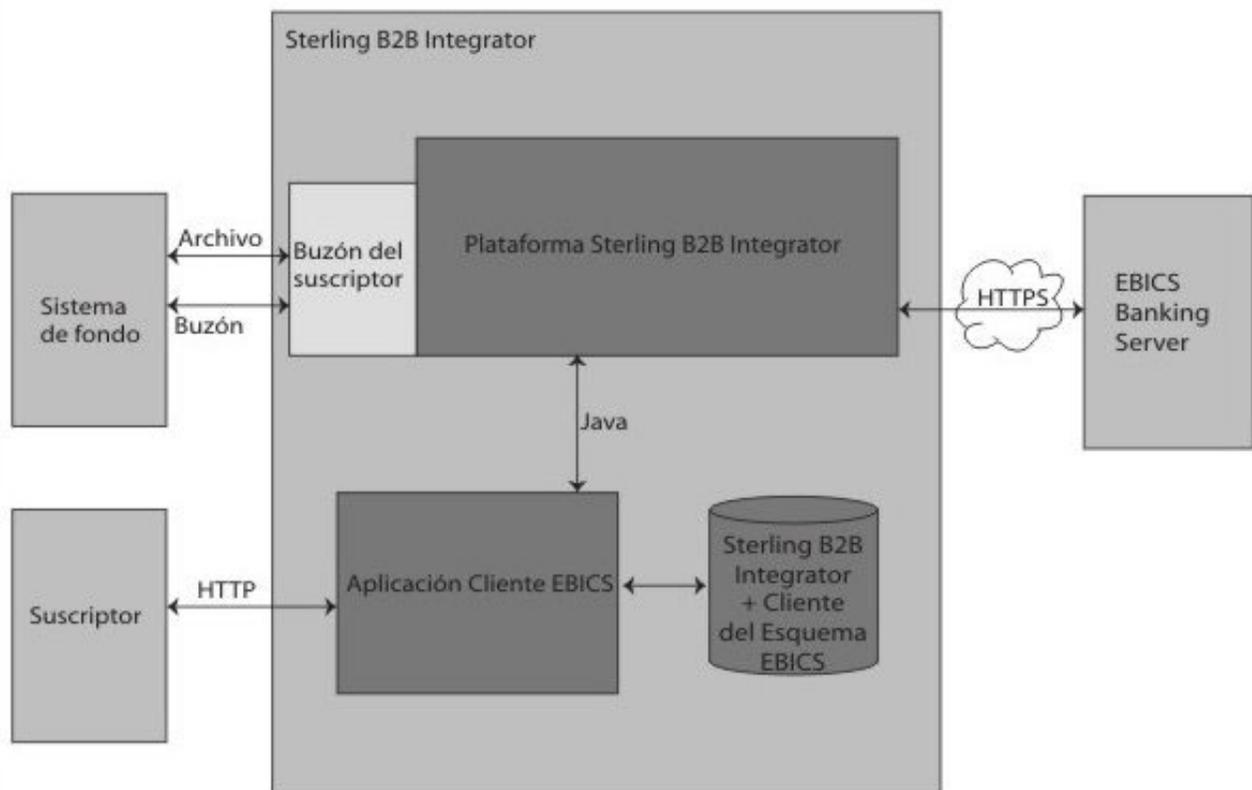


Figura 1. Arquitectura del Cliente EBICS

Las secciones siguientes describen los componentes de la arquitectura del Cliente EBICS.

Suscriptor

Un suscriptor utiliza el Cliente EBICS para realizar transacciones bancarias. El suscriptor o usuario se comunica con la aplicación Cliente EBICS mediante el protocolo HTTP para enviar y recibir mensajes.

Aplicación Cliente EBICS

La aplicación Cliente EBICS proporciona una interfaz de panel de instrumentos que le permite configurar y gestionar las entidades siguientes de EBICS:

- Usuario
- Banco
- Ofertas
- Formato de archivo
- Permisos de usuario
- Envío de órdenes
- Tareas pendientes
- Validación de clave de banco
- Claves

La aplicación Cliente EBICS interactúa con Sterling B2B Integrator y la base de datos de esquema de EBICS para recuperar y almacenar datos referentes a suscripciones y órdenes.

Sterling B2B Integrator y esquema del Cliente EBICS

Las tablas de esquema de Sterling B2B Integrator y el Cliente EBICS se almacenan en una base de datos común para permitir que la aplicación Cliente EBICS acceda a los datos siguientes:

- Datos nativos de Sterling B2B Integrator contenidos en tablas de esquema de Sterling B2B Integrator.
- Datos del Cliente EBICS contenidos en tablas de esquema de EBICS.

Plataforma Sterling B2B Integrator

La plataforma Sterling B2B Integrator en la que se despliega el Cliente EBICS.

Buzón Suscriptor

El buzón Suscriptor proporciona un mecanismo de acceso seguro para intercambiar mensajes entre el Cliente EBICS y EBICS Banking Server. Se configuran los buzones siguientes para cada usuario:

EBClientOrderMetadata

El buzón EBClientOrderMetadata es un buzón común asociado a todos los usuarios. Los metadatos de orden (OrderMetadata) asociados a una carga útil se colocan en el buzón EBClientOrderMetadata para procesar la carga útil enviada por un usuario técnico o no técnico.

Descarga (Bandeja de entrada)

El buzón Descarga se utiliza para colocar la respuesta descargada en el caso del tipo de orden HEV y datos desempaquetados en el caso de órdenes de descarga.

Carga (Bandeja de salida)

El buzón Carga se utiliza para colocar las cargas útiles.

Cuando se envía un tipo de orden de carga (FUL), la carga útil se encamina hacia el buzón Carga y los metadatos asociados a la orden se encaminan hacia el buzón EBClientOrderMetadata. La llegada de los metadatos de la orden al buzón EBClientOrderMetadata, ya sea para un tipo de orden de carga (FUL) o de descarga (FDL), desencadena un flujo de trabajo de solicitud del Cliente EBICS.

Sistema de fondo

Para enviar órdenes automáticamente desde el sistema de fondo se utiliza adaptador de Sterling B2B Integrator que puede desencadenar el proceso de negocio EBClientOrderPreProcess.

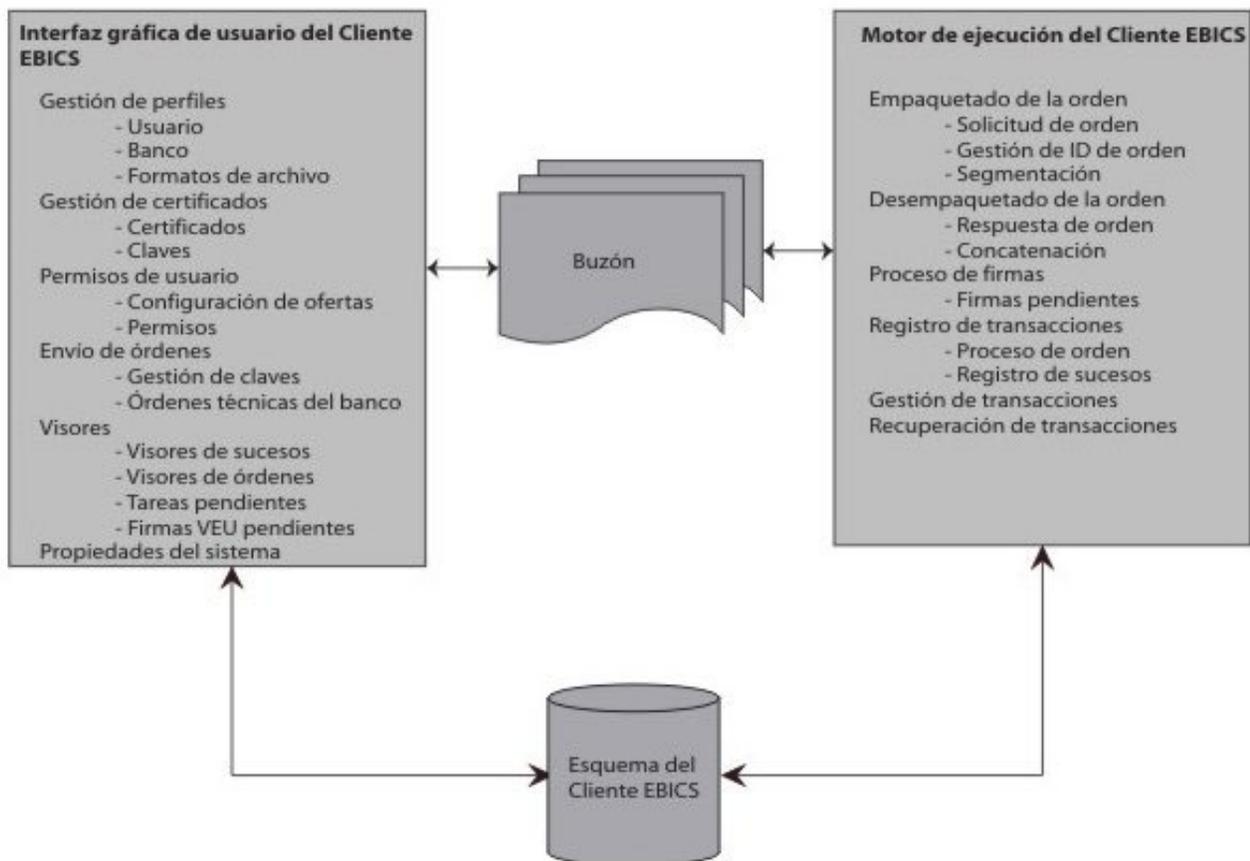
EBICS Banking Server

EBICS Banking Server está instalado en un banco. El Cliente EBICS se comunica con la aplicación EBICS Banking Server mediante el protocolo HTTP o HTTPS para intercambiar información sobre usuarios, socios comerciales, certificados digitales, datos de órdenes, formatos de archivo y tipos de orden. Para obtener más información sobre EBICS Banking Server, consulte la documentación de *Sterling B2B Integrator EBICS Banking Server*.

Componentes del Cliente EBICS

El Cliente EBICS consta de dos componentes principales: la interfaz gráfica de usuario del Cliente EBICS y el Motor de ejecución del Cliente EBICS. Ambos componentes utilizan buzones (Carga, Descarga y EBClientOrderMetadata) que se asignan a suscriptores individuales. Cuando un suscriptor envía una solicitud EBICS, el proceso de negocio del Cliente EBICS recoge la solicitud en los buzones Carga y EBClientOrderMetadata y entrega la solicitud a EBICS Banking Server de acuerdo con el tipo de orden. La respuesta recibida del servidor se procesa de acuerdo con el tipo de orden y se envía al buzón Descarga del suscriptor.

El diagrama siguiente muestra los componentes del Cliente EBICS.



Componentes del Cliente EBICS

Figura 2. Componentes del Cliente EBICS

Las secciones siguientes describen los componentes del Cliente EBICS.

Interfaz gráfica de usuario del Cliente EBICS

La interfaz gráfica de usuario del Cliente EBICS consta de los componentes siguientes:

Gestión de perfiles

Este componente le permite configurar y gestionar perfiles de banco, configurar usuarios existentes de Sterling B2B Integrator como usuarios del Cliente EBICS, y configurar formatos de archivo.

Gestión de certificados

Este componente es el encargado de la verificación de firmas electrónicas, y de la identificación, autenticación y cifrado de certificados o claves de bancos y usuarios.

Permisos de usuario

Este componente le permite configurar y gestionar ofertas y permisos de usuario.

Envío de órdenes

Este componente le permite procesar órdenes de gestión de claves y órdenes técnicas bancarias de carga y descarga.

Visores

Este componente proporciona una vista de resumen de órdenes seleccionadas o sucesos referentes a órdenes y permite a los usuarios firmar o enviar órdenes pendientes.

Propiedades del sistema

Este componente proporciona una vista de resumen de los valores de propiedades del sistema. Si es necesario, un administrador o super administrador del Cliente EBICS puede actualizar los valores.

Motor de ejecución del Cliente EBICS

El motor de ejecución del Cliente EBICS consta de los componentes siguientes:

Empaquetado de la orden

Este componente invoca los gestores de empaquetado apropiados y asegura que la orden se empaquete de acuerdo con las especificaciones. Este componente también se encarga de la segmentación de los datos de la orden.

Desempaquetado de la orden

Este componente es el encargado de desempaquetar la carga útil recibida de EBICS Banking Server. El desempaquetado incluye el proporcionar la respuesta apropiada a los usuarios para la orden y concatenar segmentos de datos de la orden en el caso de descargas.

Proceso de firmas

Este componente verifica si existen o no las firmas necesarias para una orden. Si no existen las firmas necesarias, la página Tareas pendientes del panel de instrumentos del Cliente EBICS se actualiza con los detalles de la orden pendiente. Cuando un usuario del Cliente EBICS con órdenes pendientes (firmar o enviar) inicia una sesión en el panel de instrumentos del Cliente EBICS, se abre la página Tareas pendientes para solicitar al usuario que firme o envíe la orden.

Registro de transacciones

Este componente es el encargado de registrar datos de transacciones en las tablas apropiadas de la base de datos.

Gestión de transacciones

Este componente inicia una sesión para establecer comunicación con EBICS Banking Server, gestiona transacciones entre el cliente y el servidor, y procesa las respuestas recibidas del servidor.

Recuperación de transacciones

Este componente recupera transacciones fallidas. El número de intentos de recuperación depende del valor especificado en la configuración del perfil del banco. EBICS Banking Server lleva un recuento de los intentos de recuperación. El servidor cancela la recuperación cuando se alcanza el número especificado de intentos.

Buzón

El componente Buzón proporciona una comunicación entre la interfaz gráfica de usuario del Cliente EBICS y el motor de ejecución del Cliente EBICS. El Cliente EBICS utiliza los buzones siguientes para almacenar y procesar solicitudes y respuestas de órdenes:

- EBClientOrderMetadata. Es un buzón común asociado a todos los usuarios.
- Descarga (Bandeja de entrada)

- Carga (Bandeja de salida)

Se crean buzones separados de carga y descarga y se asignan a cada usuario del Cliente EBICS.

Esquema del Cliente EBICS

Los datos referentes al Cliente EBICS se almacenan en las tablas de esquema del Cliente EBICS. La interfaz gráfica de usuario del Cliente EBICS y el motor de ejecución del Cliente EBICS acceden a las tablas para recuperar información sobre usuarios, bancos, ofertas, permisos de usuario y órdenes.

Características esenciales del Cliente EBICS

Esta sección describe algunas de las características esenciales del Cliente EBICS.

Tipos de usuario

Puede configurar los tipos de permiso siguientes para permitir que un usuario acceda a la interfaz de panel de instrumentos del Cliente EBICS:

Administrador del Cliente EBICS

Un administrador del Cliente EBICS puede configurar un usuario existente de Sterling B2B Integrator como usuario del Cliente EBICS o como operador del Cliente EBICS. El administrador puede también configurar las entidades siguientes en la interfaz de panel de instrumentos del Cliente EBICS:

- Perfil de banco
- Perfil de usuario
- Oferta
- Formato de archivo
- Claves
- Permiso de usuario
- Ver sucesos
- Buscar órdenes

Pero un administrador del Cliente EBICS no puede enviar órdenes.

Operador del Cliente EBICS

Un operador del Cliente EBICS puede ver información sobre perfiles de usuario y de banco, ver sucesos y buscar órdenes. Pero el operador del Cliente EBICS no puede realizar ninguna operación de creación, edición o supresión en la interfaz de panel de instrumentos del Cliente EBICS.

Usuario del Cliente EBICS

Un usuario del Cliente EBICS puede firmar y enviar órdenes, buscar órdenes enviadas por el usuario y ver sucesos para esas órdenes.

Usuario técnico

El Cliente EBICS también permite utilizar un usuario técnico. Un usuario técnico es un usuario del Cliente EBICS configurado para enviar órdenes en nombre de un usuario no técnico (usuario humano) del Cliente EBICS utilizando un sistema de fondo. El usuario técnico está asociado a un usuario no técnico. El campo **ID del sistema** contenido en la solicitud EBICS se llena con el ID de usuario del suscriptor técnico. Los certificados de firma electrónica, autorización y cifrado se asocian con el ID del sistema y se verifican de acuerdo con ello. Si se recibe una carga útil a

través de un adaptador del sistema de archivos, o cualquier otro adaptador técnico, tal como JSM o FTP, la aplicación Cliente EBICS utiliza el ID del usuario técnico especificado en el archivo XML y envía la orden. Si la carga útil se recibe a través del buzón de correo de un usuario del Cliente EBICS, se utiliza el ID del usuario para enviar la orden. Los permisos para el envío de órdenes se heredan del ID de usuario cuando una orden se envía a través de un buzón de correo de un usuario. Por ejemplo, si se envía un tipo de orden de carga con el formato de archivo pain.xxx.cfonb160, el Cliente EBICS verifica los permisos del usuario para enviar la combinación formada por el tipo de orden y el formato de archivo. Pero el Cliente EBICS verifica los certificados para firma electrónica, autenticación y cifrado especificados para el ID del sistema. La firma electrónica de un usuario técnico se define como Firma de transporte de tipo T.

Desde el sistema de fondo se cargan en el Cliente EBICS un archivo comprimido (.zip) que contiene un archivo XML, ordermetadata.xml, y opcionalmente la carga útil (para FUL y tipos de orden similares). Si el nombre de archivo de la carga útil contiene caracteres no ASCII, utilice el programa de utilidad jar, que se proporciona con el JDK (Java Development Kit) instalado, con Sterling B2B Integrator para crear un archivo comprimido. Ejecute jar desde el indicador de mandatos de Windows o el terminal de UNIX con los parámetros siguientes: jar cFM <nombre_archivo_zip> ordermetadata.xml <nombre_archivo_carga_útil con caracteres no ASCII>. Si el nombre de archivo de la carga útil solamente contiene caracteres ASCII, se puede utilizar el programa de utilidad jar o cualquier aplicación tal como WinZip o WinRAR para crear un archivo comprimido.

Nota: El directorio de inicio de Java se debe establecer en el JDK.

El Cliente EBICS recibe el archivo comprimido mediante un adaptador tal como el adaptador de sistema de archivos (FSA) configurado en Sterling B2B Integrator. Después de recibir el archivo comprimido, el proceso de negocio EBClientOrderPreProcess extrae el contenido del archivo XML y crea una solicitud EBICS de acuerdo con los valores especificados en el archivo XML. El archivo XML se debe ajustar al XSD siguiente. El usuario técnico se especifica en el campo ID del sistema.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="PartnerID" type="xsd:string"/>
  <xsd:element name="UserID" type="xsd:string"/>
  <xsd:element name="OrderType" type="xsd:string"/>
  <xsd:element name="SystemID" type="xsd:string"/>
  <xsd:element name="Parameter">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element ref="Name" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="Value" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="Type" minOccurs="0" maxOccurs="1"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="ParameterList">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element ref="Parameter" minOccurs="0" maxOccurs="unbounded"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="UserAuthNewPubKeyID" type="xsd:string"/>
  <xsd:element name="UserAuthNewPriKeyAlias" type="xsd:string"/>
  <xsd:element name="PAYLOADMSGID" type="xsd:string"/>
  <xsd:element name="Product" type="xsd:string"/>
</xsd:schema>
```

```

<xsd:element name="Value" type="xsd:string"/>
<xsd:element name="UserEncrNewPubKeyAlias" type="xsd:string"/>
<xsd:element name="UserNewSignatureVersion" type="xsd:string"/>
<xsd:element name="UserSignNewPubKeyID" type="xsd:string"/>
<xsd:element name="Type" type="xsd:string"/>
<xsd:element name="UserEncrNewPubKeyID" type="xsd:string"/>
<xsd:element name="UserNewAuthVersion" type="xsd:string"/>
<xsd:element name="PreValidation" type="xsd:string"/>
<xsd:element name="UserAuthNewPriKeyID" type="xsd:string"/>
<xsd:element name="UserSignNewPriKeyAlias" type="xsd:string"/>
<xsd:element name="UserAuthNewPubKeyAlias" type="xsd:string"/>
<xsd:element name="HostID" type="xsd:string"/>
<xsd:element name="autoSubmit" type="xsd:string"/>
<xsd:element name="Name" type="xsd:string"/>
<xsd:element name="UserSignNewPriKeyID" type="xsd:string"/>
<xsd:element name="UserEncrNewPriKeyID" type="xsd:string"/>
<xsd:element name="UserNewEncVersion" type="xsd:string"/>
<xsd:element name="FileFormat" type="xsd:string"/>
<xsd:element name="DownloadDateRangeEnd" type="xsd:string"/>
<xsd:element name="SecurityMedium" type="xsd:string"/>
<xsd:element name="UserSignNewPubKeyAlias" type="xsd:string"/>
<xsd:element name="UserEncrNewPriKeyAlias" type="xsd:string"/>
<xsd:element name="orderIdPrefix" type="xsd:string"/>
<xsd:element name="DownloadDateRangeStart" type="xsd:string"/>
<xsd:element name="orderMetaData">
  <xsd:complexType>
    <xsd:all>
      <xsd:element ref="HostID" minOccurs="1" maxOccurs="1"/>
      <xsd:element ref="PartnerID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="PAYLOADMSGID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="PreValidation" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="Product" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="orderIdPrefix" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="SecurityMedium" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="OrderType" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="SystemID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="FileFormat" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="autoSubmit" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="DownloadDateRangeStart" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="DownloadDateRangeEnd" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserSignNewPubKeyAlias" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserSignNewPubKeyID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserSignNewPriKeyAlias" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserSignNewPriKeyID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserAuthNewPubKeyAlias" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserAuthNewPubKeyID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserAuthNewPriKeyAlias" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserAuthNewPriKeyID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserEncrNewPubKeyAlias" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserEncrNewPubKeyID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserEncrNewPriKeyAlias" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserEncrNewPriKeyID" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserNewSignatureVersion" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserNewAuthVersion" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="UserNewEncVersion" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="ParameterList" minOccurs="0" maxOccurs="1"/>
    </xsd:all>
  </xsd:complexType>
</xsd:element>
</xsd:schema>

```

Certificados y claves

El Cliente EBICS permite utilizar claves y tipos de certificado X.509 para la identificación y autenticación del usuario, cifrado y firmas electrónicas.

Certificados

X.509 es un estándar utilizado para definir certificados digitales. El Cliente EBICS permite utilizar X.509 para verificar firmas digitales. Los usuarios del Cliente EBICS pueden utilizar uno de los tipos de certificado siguientes:

- Certificados autofirmados con algoritmo de hash SHA256
- Certificados firmados por entidad emisora de certificados

Cuando se utiliza el tipo de certificado X.509 para la autenticación, el cifrado y la firma electrónica de un usuario del Cliente EBICS, un administrador del Cliente EBICS especifica claves públicas y privadas apropiadas al configurar el perfil de usuario. A continuación, el usuario del Cliente EBICS comparte las claves públicas de la firma electrónica con el banco mediante el tipo de orden INI (Inicialización), y las claves públicas de la identificación, autenticación y cifrado mediante el tipo de orden HIA.

Nota: No se pueden utilizar certificados autofirmados para firmas electrónicas, y por tanto para la inicialización del usuario (tipo de orden INI). Un usuario del Cliente EBICS que utilice certificados autofirmados para la identificación, autenticación y cifrado, debe utilizar certificados de entidad emisora de certificados para las firmas electrónicas.

El Cliente EBICS permite utilizar un almacén de claves de hardware para el certificado de firma digital. El almacén de claves de hardware se puede utilizar solamente para el tipo de clave de hardware 3SKey.

Claves

Cuando se utilizan claves para la autenticación, el cifrado y la firma electrónica de un usuario del Cliente EBICS, un administrador del Cliente EBICS genera o carga claves privadas al configurar el perfil de usuario. A continuación, el usuario del Cliente EBICS comparte las claves públicas de la firma electrónica con el banco mediante el tipo de orden INI y las claves públicas de la identificación, autenticación y cifrado mediante el tipo de orden HIA.

Nota: Utilice una herramienta externa para generar las claves.

Tipos de orden

El tipo de orden define la naturaleza de una transacción EBICS. El Cliente EBICS permite utilizar los tipos de orden siguientes:

Tipo de orden de gestión de claves

Este tipo de orden se utiliza para descargar información técnica, tal como clave bancaria, inicialización de usuario, gestión de claves, cancelación de órdenes, VEU, etc. El tipo de orden de gestión de claves también se denomina tipo de orden del sistema.

Tipo de orden técnica bancaria

Este tipo de orden se utiliza para diversas transacciones de carga y descarga que se producen entre un suscriptor y un banco. El contrato firmado entre un banco y un socio especifica los tipos de orden que los usuarios pueden enviar. El banco configura los tipos de orden utilizando EBICS Banking Server de Sterling B2B Integrator. Las órdenes técnicas bancarias pueden ser Órdenes de carga (FUL) y Órdenes de descarga

(FDL). Puede cargar una orden, es decir, emitir una orden a un banco, utilizando una orden de carga. Una orden de descarga le permite descargar un informe o extracto del banco.

Tipos de orden para el francés

La tabla siguiente muestra los tipos de orden de gestión de claves de carga que se pueden utilizar para la implementación en francés:

Tabla 1. Tipos de orden de gestión de claves de carga para la implementación en francés:

Tipo de orden de gestión de claves de carga	Descripción
INI	Se utiliza en la inicialización del suscriptor. Envía el certificado público técnico bancario de un cliente a EBICS Banking Server. Los datos de la orden se comprimen y codifican según Base64.
HIA	Se utiliza para transmitir certificados públicos de usuario con fines de identificación, autenticación y cifrado dentro del marco de la inicialización del suscriptor. Los datos de la orden se comprimen y codifican según Base64.
PUB	Se utiliza para actualizar certificados de cliente. Envía el certificado público técnico bancario del cliente para actualizar EBICS Banking Server. Los datos de la orden se firman, comprimen, cifran y codifican según Base64.
HCA	Se utiliza para actualizar certificados de cliente. Envía los certificados siguientes para actualizar EBICS Banking Server: <ul style="list-style-type: none"> • Certificado público de identificación y autenticación • Certificado público de cifrado Los datos de la orden se firman, comprimen, cifran y codifican según Base64.
HCS	Se utiliza para actualizar certificados de cliente. Envía los certificados siguientes para actualizar EBICS Banking Server: <ul style="list-style-type: none"> • Certificado público técnico bancario • Certificado público de identificación y autenticación • Certificado público de cifrado Los datos de la orden se firman, comprimen, cifran y codifican según Base64.
SPR	Se utiliza para suspender la autorización de acceso de un usuario. Solamente se envía la firma electrónica del usuario del Cliente EBICS. Los datos de la orden son un carácter en blanco. La firma se comprime, se cifra y codifica según Base64 como en una carga normal.

La tabla siguiente muestra los tipos de orden de gestión de claves de descarga que se pueden utilizar para la implementación en francés:

Tabla 2. Tipos de orden de gestión de claves de descarga para la implementación en francés:

Tipo de orden de gestión de claves de descarga	Descripción
HPB	Se utiliza para descargar certificados públicos bancarios desde EBICS Banking Server. Los datos de la orden se comprimen, cifran y codifican según Base64. El mensaje de respuesta y los datos de la orden no se firman.
HPD	Se utiliza para descargar parámetros bancarios desde EBICS Banking Server. Los datos de la orden se firman, comprimen, cifran y codifican según Base64.
HEV	Se utiliza para descargar información sobre versiones de EBICS soportadas.
HKD	Se utiliza para descargar información sobre un socio y suscriptores asociados. Los datos de la orden se comprimen y codifican según Base64.
HTD	Se utiliza para descargar información sobre un suscriptor y el socio asociado. Los datos de la orden se comprimen y codifican según Base64.

Tipos de orden para el alemán

El Cliente EBICS se puede utilizar con los tipos de orden para el alemán definidos en el Anexo 2 del documento de especificaciones de EBICS (*EBICS_Annex2_OrderTypes-File_Formats_01_11_2010.pdf*). El atributo Formato de archivo identifica el tipo de archivo que se carga o descarga. El atributo Formato de archivo es necesario como parte de los detalles de la orden. En la implementación de EBICS para el alemán, los tipos de orden definen la naturaleza de la transacción financiera, por ejemplo, un tipo de orden se utiliza para la transferencia de crédito, otro tipo de orden se utiliza para el cargo directo, etc. Los identificadores de tipo de orden para la implementación en alemán siguen el protocolo de transferencia de archivos existente (BCS FTAM). Un usuario del Cliente EBICS puede cargar o descargar tipos de orden del alemán de forma similar a como se utilizan los tipos de orden genéricos FUL (carga) y FDL (descarga).

Distributed Electronic Signature (VEU) es una característica que permite que varios suscriptores autoricen órdenes. De acuerdo con la implementación de EBICS, es obligatorio que un banco permita la utilización de VEU.

La tabla siguiente muestra los tipos de orden de VEU de carga que se pueden utilizar para la implementación en alemán:

Tabla 3. Tipos de orden de VEU de carga para la implementación en alemán

Tipos de orden de VEU de carga	Descripción
HVU	Se utiliza para descargar una visión general de VEU. Los datos de la orden se comprimen y codifican según Base64.
HVD	Se utiliza para recuperar el estado de VEU. Los datos de la orden se comprimen y codifican según Base64.
HVZ	Se utiliza para descargar una visión general de VEU junto con información adicional. Los datos de la orden se comprimen y codifican según Base64.
HVT	Se utiliza para recuperar detalles de transacción de VEU. Los datos de la orden se comprimen y codifican según Base64.

La tabla siguiente muestra los tipos de orden de VEU de descarga que se pueden utilizar para la implementación en alemán.

Tabla 4. Tipos de orden de VEU de descarga para la implementación en alemán

Tipos de orden de VEU de descarga	Descripción
HVE	Se utiliza para añadir la firma de VEU. Los datos de la orden se comprimen y codifican según Base64.
HVS	Se utiliza para añadir la cancelación de VEU. Los datos de la orden se comprimen y codifican según Base64.

Firmas pendientes

Dependiendo de los valores de configuración definidos en una oferta, podría ser necesario que varios firmantes firmasen la orden para poder procesar los datos de la orden. Si se envía una orden para procesar sin todas las firmas necesarias, el Cliente EBICS no procesará la orden. Se envían notificaciones de firma pendiente a los buzones de los firmantes implicados para solicitarles que se ocupen de la orden. Se abre la página Firma pendiente para un usuario que tenga órdenes pendientes de enviar o firmar cuando el usuario entra en la interfaz de panel de instrumentos del Cliente EBICS. Se muestran los estados siguientes para una orden:

Pendiente, Firmar

La orden está pendiente y necesita que se firme.

Pendiente, Enviar

Se han obtenido todas las firmas necesarias y es necesario enviar la orden.

Hardware Signature Module

El Cliente EBICS permite la utilización de Hardware Signature Module para firmas electrónicas (ES). Si la clave de seguridad de hardware para firmas electrónicas está configurada para un usuario, se abre la ventana Firma electrónica cuando el usuario pulsa **Firmar**. El usuario debe proporcionar la clave de seguridad de hardware apropiada para firmar la orden. En este momento, el Cliente EBICS sólo permite utilizar Hardware Signature Module mediante 3SKey. Debe habilitar la

versión 1.6_24 de Java, o superior, en el navegador para poder abrir el applet de Hardware Signature Module.

Recuperación de órdenes

La recuperación de órdenes es una característica importante del Cliente EBICS. Para una transacción de carga, se podría producir un error de proceso de orden en el banco. Para las transacciones de descarga, se podría producir un error de proceso de respuesta en el suscriptor o cliente. Además de los errores de proceso, también se podrían producir errores de transporte.

El mecanismo de recuperación necesita el ID de la transacción EBICS afectada y está basado en la definición de puntos de recuperación de transacciones:

- Para las transacciones de carga, el punto de recuperación es el último paso de la transacción cuya solicitud EBICS se ha enviado satisfactoriamente al sistema bancario y cuya respuesta EBICS se ha transmitido satisfactoriamente. El punto de recuperación está determinado por el estado de la transacción en el sistema bancario.
- Para las transacciones de descarga, podrían existir varios puntos de recuperación. Los puntos de recuperación son los pasos de la transacción cuya solicitud EBICS ha sido recibida satisfactoriamente por el banco y cuya respuesta EBICS se ha transmitido satisfactoriamente.

Cuando se produce un error de transporte o proceso, se utiliza un punto de recuperación para continuar la transacción a partir del paso de transacción que sigue a continuación del punto de recuperación en la secuencia.

Recuperación de transacciones

Cuando se transmiten datos de transacción, se podrían producir cualquiera de los errores siguientes:

- Error de transporte
- Error de proceso
- Error de tiempo de espera excedido

El Cliente EBICS almacena el estado de cada segmento que se ha enviado o recibido satisfactoriamente del banco. Cuando se produce un error después de haber enviado o recibido satisfactoriamente 'n' segmentos, el cliente inicia la recuperación a partir del segmento que ocupa la posición (n+1).

EBICS Banking Server mantiene un contador de recuperaciones y también hace un seguimiento del número máximo de intentos de recuperación permitidos. El contador se incrementa después de cada intento. Si se alcanza el número máximo de intentos y la recuperación es infructuosa, el servidor cancela el proceso de recuperación y suspende la transacción completa.

Búsqueda de órdenes y resumen de órdenes

Los usuarios pueden buscar órdenes y ver el resumen de las ordenes en la interfaz de panel de instrumentos del Cliente EBICS, utilizando uno de los parámetros siguientes o una combinación de ellos:

- Ubicación de búsqueda: tablas activas, tablas de archivo

Nota: Las órdenes recientes se almacenan en tablas activas y las órdenes archivadas se almacenan en tablas de restauración.

- Fecha de inicio y finalización de la orden

- Hora de inicio y finalización de la orden
- ID de banco (ID de host)
- Nombre de socio
- ID de orden
- Estado: Todos, Satisfactorio, Erróneo, En curso, Pendiente en servidor, Pendiente en cliente
- Tipo de orden
- Formato de archivo
- Tipo de permiso: Emisor, Firmante
- ID de usuario: este parámetro solamente puede ser utilizado por un administrador del Cliente EBICS y un operador del Cliente EBICS

Cuando un administrador del Cliente EBICS realiza la búsqueda, se muestran las órdenes enviadas por todos los usuarios del sistema. Cuando un usuario del Cliente EBICS realiza la búsqueda, en los resultados de la búsqueda se muestran las órdenes enviadas por el usuario. El resultado de la búsqueda se muestra en formato tabular y se puede ordenar por orden ascendente o descendente. El resultado de la búsqueda también se puede renovar periódicamente especificando un tiempo de renovación. Puede pulsar el enlace del ID de orden para ver información sobre la orden. La página Detalles de resumen de orden está dividida en dos secciones: **Datos de orden** y **Detalles de orden**.

La sección Datos de orden proporciona la información siguiente sobre la orden seleccionada:

- ID de orden
- Tipo de orden
- Formato de archivo
- Número de firmas (Firmas necesarias para enviar la orden)
- Fecha y hora de inicio
- Fecha y hora de última actividad
- Fecha y hora de terminación
- Nombre de socio
- ID de usuario
- ID de banco (ID de host)
- Estado de la orden
- Documento (carga útil de la orden) - El enlace del documento de la orden sólo se muestra para el usuario del Cliente EBICS. Pulse en el enlace para ver la carga útil (para cargar y descargar órdenes técnicas) o el XML de la solicitud de orden (para otros tipos de orden).

La sección Detalles de orden tiene tres pestañas:

Suceso de orden

Proporciona información sobre sucesos referentes a una orden, tales como datos comprimidos, datos codificados, tareas pendientes creadas por el emisor, etc.

Actividades

Proporciona información sobre actividades referentes a una orden, tales como Pendiente de firma en el cliente, Enviar acción por remitente, etc. Las actividades pueden estar en uno de los estados siguientes:

- En curso

- Completado
- Fallido

No se generan actividades para los tipos de orden INI, HIA y HPB.

Firmas pendientes

Lista los usuarios cuyas firmas están pendientes para la orden seleccionada.

Visor de sucesos

El Cliente EBICS genera sucesos relacionados con órdenes. Todos los sucesos están predefinidos y se proporcionan metadatos al sistema. Un usuario no puede definir los sucesos. Los sucesos se registran para un ID de orden y no existen sucesos autónomos en el Cliente EBICS.

Los usuarios pueden buscar sucesos y ver los detalles del suceso relacionados con las órdenes en la interfaz de panel de instrumentos del Cliente EBICS, utilizando uno de los parámetros siguientes o una combinación de ellos:

- Ubicación de búsqueda: tablas activas, tablas de archivo

Nota: Las órdenes recientes se almacenan en tablas activas y las órdenes archivadas se almacenan en tablas de archivo.

- Fecha de inicio y finalización del suceso
- Hora de inicio y finalización del suceso
- Tipo de suceso: Todos, Información, Aviso, Error, Crítico

Cuando un administrador del Cliente EBICS realiza la búsqueda, se muestran los sucesos relacionados con todas las órdenes. Cuando un usuario del Cliente EBICS realiza la búsqueda, se muestran los sucesos relacionados con las órdenes enviadas por el usuario. El resultado de la búsqueda se muestra en formato tabular y se puede ordenar por orden ascendente o descendente. El resultado de la búsqueda también se puede renovar periódicamente especificando un intervalo de tiempo para mostrar la lista actualizada de órdenes. Puede pulsar el enlace del ID de suceso deseado para ver información completa sobre el suceso. La página Detalles de resumen de suceso está dividida en dos secciones: **Detalles de suceso** y **Detalles de orden**.

La sección Detalles de suceso proporciona la información siguiente sobre el suceso seleccionado:

- Código de suceso
- Nombre de suceso
- Descripción del suceso
- Tipo de suceso
- ID de usuario
- Indicación de fecha y hora

La sección Detalles de orden proporciona la información siguiente sobre la orden asociada al suceso:

- ID de orden
- Tipo de orden
- Documento (Pulse el icono de documento para ver el documento de carga útil)
- Nombre de socio
- ID de usuario

- ID de banco (ID de host)

Tipos de suceso

Los sucesos puede ser de estos tipos:

Información

Proporciona información sobre sucesos. Por ejemplo: cifrado realizado satisfactoriamente.

Aviso Un mensaje de aviso. Por ejemplo: orden recibida con avisos.

Error Suceso que indica la existencia de una condición de error. Por ejemplo: la entrega al banco ha fallado.

Crítico

Suceso que indica la existencia de una condición crítica. Por ejemplo: La base de datos del Cliente EBICS no funciona.

Tablas de restauración

El archivado de datos de transacción, tales como datos de órdenes, sucesos y datos relacionados con firma pendiente protege datos críticos. El archivado ahorra espacio de disco en la base de datos y espacio de disco en el sistema de archivos (cuando se utilizan documentos almacenados en disco), lo cual a su vez mejora la eficiencia del Cliente EBICS.

Un administrador del Cliente EBICS puede configurar un tiempo de vida para los datos de transacción en Sterling B2B Integrator. Cuando los datos de transacción sobrepasan su tiempo de vida, el servicio de proceso de negocio Backup traslada los datos a un soporte físico. Más tarde los datos se pueden restaurar en las tablas de restauración. El servicio de proceso de negocio Backup se puede ejecutar de forma manual o planificada. El archivado de datos de transacción es una actividad que consume muchos recursos. Por tanto, es recomendable realizar esa tarea durante las horas de menor actividad.

El servicio de proceso de negocio Restore restaura datos de transacción archivados desde un soporte físico a una ubicación de datos restaurados, donde los datos se pueden buscar y ver.

Capítulo 4. Requisitos de configuración

El capítulo Requisitos de configuración define los elementos que se deben configurar en el Cliente EBICS para realizar transacciones con un banco. Para obtener información de configuración detallada, consulte la *Guía del usuario del Cliente EBICS*.

Configuración necesaria en Sterling B2B Integrator

Antes de utilizar el Cliente EBICS, configure las entidades siguientes en Sterling B2B Integrator.

1. Cree un registro de identidad para el socio, que defina el socio como identidad base.
2. Cree una cuenta de usuario.
3. Configure un adaptador que le permite enviar y recibir archivos e invoca el proceso de negocio EBClientOrderPreProcess. Por ejemplo, configure un adaptador de sistema de archivos para invocar el proceso de negocio EBClientOrderPreProcess. El proceso de negocio EBClientOrderPreProcess se utiliza para validar la carga útil recibida de un usuario técnico y extraer la carpeta donde reside la carga útil o metadatos y enviar los datos de la carga útil a los buzones apropiados.
4. Configure los buzones siguientes y asícelos a cada usuario:
 - EBClientOrderMetadata (preconfigurado)
 - Descarga (Bandeja de entrada)
 - Carga (Bandeja de salida)
5. Verifique que el proceso de negocio EBClientMailboxArrivedMessage esté asociado con el buzón EBClientOrderMetadata. La regla de direccionamiento automático hace que el proceso de negocio ejecute funciones automatizadas, tales como notificar la entrada de mensajes en el buzón de un usuario.
6. Asegúrese de que planificación MailboxEvaluateAllAutomaticRulesSubMin esté habilitada. La planificación evalúa periódicamente la regla de direccionamiento para asegurar su correcto funcionamiento.
7. Registre las claves públicas compartidas por el banco en el almacén de claves de la entidad emisora de certificados o cree un certificado autofirmado con el algoritmo de hash SHA256.

Configuración e inicialización del usuario

El primer paso para iniciar una transacción con el banco es configurar un usuario existente de Sterling B2B Integrator como usuario del Cliente EBICS. Esto incluye especificar valores para atributos, tales como tipo de usuario, tipo de certificado, etc. Se pueden configurar tres tipos de usuarios en el Cliente EBICS: administrador de EbicsClient, operador de EbicsClient y usuario de EbicsClient. También se puede configurar un usuario técnico en el cliente. El Cliente EBICS permite utilizar los estándares para claves X.509 y RSA para definir certificados digitales. Para obtener más información sobre tipos de usuario, consulte el tema *Tipos de usuario*. Los atributos de configuración de usuario varían según el tipo de usuario y tipo de certificado. No es necesario configurar información sobre certificados y claves para un administrador de EBICS u operador del Cliente EBICS.

Después de configurar un usuario existente como usuario de EBICS, el usuario transmite los certificados públicos a la institución financiera utilizando dos vías de comunicación independientes:

INI Envía la clave pública técnica bancaria.

HIA Envía la clave pública de identificación y autenticación, y la clave pública de cifrado.

Cuando se configura el usuario y se asigna a un socio, el estado del usuario es Nuevo. Si el usuario envía solamente la solicitud INI al banco, el estado se cambia a Inicializado parcialmente (INI). Si el usuario envía solamente la solicitud HIA al banco, el estado se cambia a Inicializado parcialmente (HIA). Después de que el usuario envíe las solicitudes INI y HIA al banco, el estado se cambia al estado Inicializado en el sistema del banco, y al estado Preparado en el Cliente EBICS. El usuario crea las cartas de inicialización de INI y HIA con el valor de hash de las claves utilizando la interfaz de panel de instrumentos del Cliente EBICS, firma manualmente las cartas y las envía al banco. Cuando el banco recibe las cartas de inicialización de INI y HIA, el banco compara los valores de hash contenidos en las cartas con la base de datos del banco. Una vez realizada satisfactoriamente la validación, el estado del usuario se establece en Preparado, que indica que el usuario puede ahora hacer transacciones con el banco.

Configuración del banco

Un banco es la entidad primaria de una transacción EBICS. El banco contiene el servidor con el que un socio y usuarios asociados pueden realizar transacciones EBICS. Los detalles de la configuración del banco incluyen:

- ID de banco (ID de host)
- Nombre del banco
- URL del banco
- Se prefiere RSA
- Información de contacto del banco
- Dirección de correo electrónico
- Claves públicas de certificados de autenticación y cifrado
- Versiones de clave de certificados de autenticación y cifrado

Una parte esencial de la configuración del banco es el ID de banco o ID de host. Después de firmar un contrato, el banco comparte el ID de banco o ID de host, junto con el URL del banco, con el socio. Un administrador del Cliente EBICS crea un perfil de banco utilizando la información compartida por el banco con el socio. Si el URL del banco utiliza un protocolo HTTP seguro, es necesario un certificado HTTPS. El certificado HTTPS del banco se crea en Sterling B2B Integrator y se configura utilizando el Cliente EBICS.

El estado del banco se establece en Nuevo hasta que se validan las claves públicas de identificación, autenticación y cifrado del banco. La validación de las claves del banco incluye los pasos siguientes:

1. Un usuario del Cliente EBICS envía un tipo de orden HPB para descargar las claves públicas del banco.
2. Después de la validación satisfactoria de las claves de autenticación e identificación del usuario, el banco envía una respuesta HPB. La respuesta HPB contiene las claves públicas del banco. Las claves se almacenan en la base de datos del Cliente EBICS y se genera un valor de hash de las claves.

3. El banco proporciona al usuario valores de hash para la parte pública de las claves mediante un canal independiente de EBICS. Por ejemplo, un portal, correo o sitio web del banco.
4. El usuario copia los valores de hash a partir del portal y valida las claves del banco utilizando la interfaz de panel de instrumentos del Cliente EBICS.
5. Los valores de hash compartidos por el banco se comparan con los valores de hash generados internamente. Si los valores de hash coinciden, el estado del banco se establece en Activado. Si los valores de hash del banco y el usuario no coinciden, se solicita al usuario que revalide las claves del banco.

Una vez realizada satisfactoriamente la validación, el estado del banco se establece en Activado, que indica que el socio y sus usuarios asociados pueden ahora hacer transacciones con el banco.

Configuración del formato de archivo

El formato o tipo de archivo que se carga o descarga se identifica mediante el atributo Formato de archivo. Un tipo de orden puede tener varios o ningún formato de archivo. Un formato de archivo contiene los atributos siguientes:

Código de país

Código del país donde se puede utilizar el formato de archivo.

Tipos de orden admitidos

FUL (Upload), FDL (Download), y otros tipos de orden.

Los formatos de archivo para FUL y FDL están basados en el tipo de solicitud SWIFTNet. Para obtener más información sobre SWIFTNet, consulte <http://www.swift.com/>. La primera parte del nombre de formato de archivo debe ser uno de los elementos listados en la tabla siguiente. Los elementos indican el tipo de transacción.

Tabla 5. Elemento de nombre de formato de archivo

Elemento	Descripción
pain.	Iniciación de pagos
camt.	Gestión de efectivo
tsrv.	Servicios comerciales
tsmt.	Gestión de servicios comerciales

Configuración de la oferta

Una oferta es un superconjunto de tipos de orden y formatos de archivo. Las ofertas se asocian a un ID de banco para especificar los posibles tipos de orden y formatos de archivo que se pueden utilizar al realizar transacciones con el banco. Las ofertas proporcionan la ventaja de agrupar muchas transacciones bancarias y gestionárselas juntas. Una oferta contiene los atributos siguientes:

- Nombre: nombre de la oferta
- ID de banco: ID de banco al que está asociada la oferta
- Tipo de orden: tipo de orden admitido
- Formato de archivo: formato de archivo admitido

Nota: Solamente un administrador del Cliente EBICS puede configurar formatos de archivos y ofertas.

Configuración de permisos de usuario

Los permisos de usuario definen las ofertas, tipos de orden y formatos de archivo que un usuario del Cliente EBICS puede procesar en el Cliente EBICS. Se puede asignar uno de los tipos de permiso siguientes a un usuario:

Firmante

Un firmante solamente puede firmar una orden, pero no puede emitirla.

Emisor

Un emisor puede emitir una orden después de que el firmante o firmantes designados firmen la orden.

La tabla siguiente proporciona información sobre los niveles de autorización que se pueden especificar para un usuario del Cliente EBICS.

Tabla 6. Niveles de autorización

Nivel de autorización	Tipo de permiso	Descripción
E	Firmante	Firma individual. Es el nivel de autorización más alto.
A	Firmante	Firma primaria.
B	Firmante	Firma secundaria
T	Emisor	Firma de transporte. Las firmas de transporte no se utilizan para la autorización de órdenes técnicas bancarias, sino para el envío autorizado al sistema del banco.

Si el valor de firma electrónica se establece en 1, es necesaria una firma individual con un nivel de autorización E o A para procesar una orden. Si el valor de firma electrónica se establece en 2, es necesaria una combinación de los niveles E o A y B para procesar la orden. El valor de firma electrónica se establece en 0 para órdenes de gestión de claves.

Nota: De acuerdo con la especificación EBICS, no es posible utilizar una combinación de dos niveles de autorización secundarios de firma electrónica (nivel de autorización B) para procesar una orden.

Capítulo 5. Envío de órdenes

El envío de órdenes implica la transmisión de órdenes al sistema del banco desde el Cliente EBICS. Según si la orden se carga en el sistema del banco o se descarga de él, las órdenes pueden ser de Carga o Descarga. Cada orden debe pasar por varias fases de transacción durante su proceso.

Orden de carga

Un usuario envía un solicitud de carga (FUL) al banco. FUL es un tipo de orden técnica bancaria de carga. La transacción de carga consta de las etapas siguientes:

- Inicialización de la orden
- Proceso de la orden

Inicialización de la orden

Un usuario inicia una transacción de carga con el banco enviando una solicitud de orden de carga (FUL). El componente Motor de ejecución del Cliente EBICS verifica el nivel de autorización del usuario y el número de firmas necesarias para procesar la orden. Si se cumplen los criterios necesarios, se procesa la orden y se envía al sistema del banco. En otro caso, la orden se almacena en la base de datos y la página Tareas pendientes del panel de instrumentos del Cliente EBICS se actualiza con los detalles de la orden pendiente. Cuando un usuario del Cliente EBICS con órdenes pendientes (firmar o enviar) inicia una sesión en el panel de instrumentos del Cliente EBICS, se abre la página Tareas pendientes para solicitar al usuario que firme o envíe la orden.

Proceso de la orden

Estos son los pasos para procesar un envío de orden que incluye el tipo de orden técnica bancaria de carga (FUL) y el tipo de orden de gestión de claves:

1. Se invoca el Módulo de empaquetado de órdenes para el cifrado, firmas de autenticación, firmas de autorización, codificación y compresión.
2. Se genera el ID de orden.
3. Si los datos de la orden son mayores que el tamaño especificado de 1 MB, se segmentan los datos de la orden. Se mantiene un registro de transacciones para registrar la segmentación.
4. Se invoca el módulo XML para construir la solicitud EBICS.
5. Se genera el registro de actividad para actualizar el estado de la orden.
6. Se invoca espacio de buzón apropiado para almacenar los datos de la orden.
7. Se recogen y registran sucesos en la base de datos durante cada actividad.
8. Se envían los datos de la orden al sistema del banco.
9. La respuesta de postproceso recibida del banco se almacena en el buzón de descarga del usuario.

Orden de descarga

Un usuario envía la orden de descarga (FDL) al banco. La orden FDL es un tipo de orden técnica bancaria de descarga. La transacción de descarga consta de las etapas siguientes:

- Inicialización de la orden
- Proceso de la orden
- Acuse de recibo

Inicialización de la orden

Un usuario inicia una transacción de descarga con el banco enviando una solicitud de orden de descarga (FDL). El componente Motor de ejecución del Cliente EBICS verifica el nivel de autorización del usuario. Si se cumplen los criterios necesarios, se procesa la orden y se envía al sistema del banco.

Proceso de la orden

La respuesta recibida del sistema del banco para la orden se procesa de acuerdo con estos pasos:

1. La respuesta recibida del banco se almacena en el buzón de descarga del usuario.
2. Se invoca el componente Procesador de respuesta de orden para procesar la respuesta.
3. El Procesador de respuesta realiza las tareas siguientes:
 - a. Invoca el Módulo de desempaquetado de orden para la descompresión, decodificación y descifrado.
 - b. Invoca la Concatenación de orden si la respuesta está segmentada.
 - c. Invoca el Registro de actividad para actualizar el estado de la orden.
 - d. Recoge y registra sucesos en la base de datos del Cliente EBICS durante cada actividad.

Acuse de recibo

Después de recibir del banco el último segmento de los datos de la orden, el cliente inicia la última fase (solicitud de acuse de recibo) para indicar que la transferencia de datos ha sido satisfactoria. Si el banco recibe del cliente un acuse de recibo positivo (código de recepción=0), el banco traslada los mensajes descargados desde el buzón de descarga del usuario al buzón de archivado del usuario. Si el banco recibe del cliente un acuse de recibo negativo, el banco conserva los mensajes descargados en el buzón de descarga del usuario.

Empaquetado de la orden

Los datos de la orden se empaquetan de acuerdo con los valores especificados de firma, compresión, cifrado y codificación. Por ejemplo, si el tipo de orden es FUL, se invoca FULPackingHandler.

El empaquetado de la orden también comprende la creación de identificadores de orden inequívocos. El Cliente EBICS asigna un ID de orden exclusivo de acuerdo con el banco, ID de usuario y tipo de orden. El cliente genera el ID de orden según especificaciones de EBICS.

- El ID de orden es un identificador alfanumérico de cuatro caracteres.
- El primer carácter es una letra. Un usuario del Cliente EBICS puede especificar el primer carácter del ID de la orden.
- Los caracteres segundo, tercero y cuarto del ID de orden son letras y números en orden ascendente (A-Z o 0-9).

Segmentación de los datos de la orden

De acuerdo con las especificaciones de EBICS para la transferencia de datos, el tamaño de los datos de la orden una vez comprimidos, cifrados y codificados no debe ser mayor que 1 MB. Si el tamaño es mayor que 1 MB después de la compresión, cifrado y codificación, los datos de la orden se segmentan de forma que cada segmento no sobrepase el tamaño fijo de 1 MB. A continuación, los segmentos se transmiten secuencialmente en orden consecutivo en forma de mensajes individuales de EBICS.

Desempaquetado de la orden

El desempaquetado de la orden comprende la decodificación, descifrado, descompresión y verificación de los datos de la orden. También comprende registrar las ordenes para las que han fallado las operaciones de seguridad y las razones del fallo.

Concatenación de segmentos

El sistema receptor (servidor o cliente) ejecuta los cálculos algorítmicos en orden inverso para recuperar los datos originales de la orden. Los segmentos de datos se concatenan, decodifican, descifran y desempaquetan secuencialmente para obtener los datos originales de la orden.

Índice

A

Actividades 19
Administrador del Cliente EBICS 10
Aplicación Cliente EBICS 6
Arquitectura del Cliente EBICS 5

B

Banco 1
Buzón 9, 10
Buzón Suscriptor 6

C

Carga (Bandeja de salida) 7
Certificados 13
Claves 13
Código de país 23
Componentes del Cliente EBICS 7
Concatenación de segmentos 27

D

Descarga (Bandeja de entrada) 7
Desempaquetado de la orden 9, 27

E

EBClientOrderMetadata 6
EBICS, visión general 1
EBICS Banking Server 7
Emisor 24
Empaquetado de la orden 9, 26
Envío de órdenes 8
Esquema de Sterling B2B Integrator y Cliente EBICS 6
Esquema del Cliente EBICS 10

F

Firmante 24
Firmas pendientes 19

G

Gestión de certificados 8
Gestión de perfiles 8
Gestión de transacciones 9

H

Hardware Signature Module 16
HIA 22
HPB 22

I

INI 22
Interfaz de panel de instrumentos del Cliente EBICS 3
Interfaz gráfica de usuario del Cliente EBICS 8

M

Motor de ejecución del Cliente EBICS 9

N

Niveles de autorización de permisos de usuario 24

O

Operador del Cliente EBICS 10
Orden de carga 25
Orden de descarga 25
Organización 1

P

Permisos de usuario 8
Plataforma Sterling B2B Integrator 6
Proceso de firmas 9
Propiedades del sistema 9

R

Recuperación de transacciones 9, 17
Registro de transacciones 9

S

Segmentación de los datos de la orden 27
Sistema de fondo 7
Socio 1
Suceso de orden 18
Suscriptor 6

T

Tipo de orden de gestión de claves 13
Tipo de orden técnica bancaria 14
Tipos de orden admitidos 23
Tipos de orden para el alemán 15
Tipos de orden para el francés 14
Tipos de suceso 20

U

Usuario del Cliente EBICS 10
Usuario o suscriptor 1

Usuario técnico 10

V

visión general de EBICS 1
Visores 9

Avisos

Esta información se ha desarrollado para productos y servicios ofrecidos en los Estados Unidos.

IBM no puede ofrecer en otros países los productos, servicios o funciones tratadas en el presente documento. Consulte al representante local de IBM para obtener información acerca de los productos y servicios disponibles actualmente en su área. Las referencias a un producto, programa o servicio de IBM no pretenden establecer ni implicar que sólo pueda utilizarse dicho producto, programa o servicio de IBM. En su lugar se puede utilizar cualquier producto, programa o servicio funcionalmente equivalente que no vulnere ningún derecho de propiedad de intelectual de IBM. No obstante, es responsabilidad del usuario evaluar y verificar el funcionamiento de cualquier producto, programa o servicio que no sea de IBM.

IBM puede tener patentes o solicitudes de patente pendientes que afecten a los temas tratados en este documento. La posesión de este documento no le otorga ninguna licencia sobre dichas patentes. Puede enviar sus consultas sobre licencias, por escrito, a la dirección siguiente:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

Estados Unidos

Para realizar consultas sobre licencias relativas a la información de doble byte (DBCS), póngase en contacto con el Departamento de propiedad intelectual de IBM de su país o envíe sus consultas, por escrito, a:

Licencia de propiedad intelectual

Legal and Intellectual Property Law

IBM Japan Ltd.

1623-14, Shimotsuruma, Yamato-shi

Kanagawa 242-8502 Japón

El siguiente párrafo no se aplica en el Reino Unido ni en cualquier otro país en el que tales disposiciones sean incompatibles con la legislación local:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROPORCIONA ESTA PUBLICACIÓN "TAL CUAL" SIN GARANTÍAS DE NINGUNA CLASE, EXPLÍCITAS O IMPLÍCITAS, INCLUIDAS, PERO SIN LIMITARSE A ELLAS, LAS GARANTÍAS IMPLÍCITAS DE NO VULNERABILIDAD, COMERCIALIZACIÓN O IDONEIDAD PARA UN PROPÓSITO DETERMINADO. Algunos países no permiten la renuncia a garantías explícitas o implícitas en determinadas transacciones, por lo que puede que esta declaración no sea aplicable en su caso.

La presente publicación puede contener inexactitudes técnicas o errores tipográficos. Periódicamente se efectúan cambios en la información aquí incluida; dichos cambios se incorporarán en nuevas ediciones de esta publicación. IBM puede realizar mejoras y/o cambios en el/los producto(s) y/o el/los programa(s) descrito(s) en esta publicación, en cualquier momento y sin previo aviso.

Las referencias en esta información a sitios web que no son de IBM se proporcionan sólo para su comodidad y de ninguna manera constituyen una aprobación de estos sitios web. El material de dichos sitios web no forma parte del material correspondiente a este producto IBM y el uso de estos sitios web se realiza a cuenta y riesgo del usuario.

IBM puede utilizar o distribuir la información que suministre el usuario del modo que considere adecuado sin incurrir por ello en ninguna obligación con el usuario.

Los propietarios de licencias de este programa que deseen recibir información acerca de éste con el fin de permitir: (i) el intercambio de información entre programas creados independientemente y otros programas (incluido éste) y (ii) el uso mutuo de la información que se ha intercambiado, deben ponerse en contacto con el departamento siguiente:

IBM Corporation

J46A/G4

555 Bailey Avenue

San José, CA 95141-1003

Estados Unidos

Dicha información puede estar disponible, sujeta a los términos y condiciones adecuados, incluido, en algunos casos, el pago de una tasa.

El programa bajo licencia que se describe en este documento y todo el material bajo licencia disponible los proporciona IBM bajo los términos de las Condiciones Generales de IBM, Acuerdo Internacional de Programas Bajo Licencia de IBM o cualquier acuerdo equivalente entre las partes.

Los datos de rendimiento contenidos aquí se han determinado en un entorno controlado. Por lo tanto, los resultados obtenidos en otros entornos operativos podrían variar de forma notable. Algunas mediciones se han realizado en sistemas en desarrollo y no existe ninguna garantía de que éstas sean iguales en los sistemas disponibles generalmente. Además, algunas medidas se pueden haber estimado mediante extrapolación. Los resultados reales pueden variar. Los usuarios de este documento deben verificar los datos aplicables a su entorno específico.

La información relativa a productos que no son de IBM se ha obtenido de los proveedores de dichos productos, de los anuncios publicados o de otras fuentes disponibles para el público. IBM no ha probado esos productos y no puede confirmar la precisión del rendimiento, la compatibilidad ni ninguna otra afirmación relacionada con productos que no son de IBM. Las consultas relacionadas con productos no desarrollados por IBM deben dirigirse a los proveedores de dichos productos.

Todas las declaraciones concernientes a la dirección futura de IBM u objetivos están sujetos a cambio o cancelación sin aviso previo y sólo representan metas y objetivos.

Todos los precios de IBM que se muestran en este documento son precios al por mayor recomendados por IBM, vigentes y están sujetos a cambios sin previo aviso. Los precios de los distribuidores pueden variar.

Esta información está pensada sólo a efectos de planificación. La información aquí contenida puede cambiar antes de que se comercialicen los productos descritos.

Esta información contiene ejemplos de datos e informes utilizados en operaciones comerciales diarias. Para ilustrarlos de la forma más completa posible, los ejemplos incluyen nombres de particulares, empresas, marcas y productos. Todos estos nombres son ficticios y cualquier parecido con nombres y direcciones utilizadas por una empresa de negocios real es mera coincidencia.

LICENCIA DE COPYRIGHT:

Esta información contiene programas de aplicaciones de ejemplo en código fuente, que ilustran técnicas de programación en las distintas plataformas operativas. El usuario puede copiar, modificar y distribuir estos programas de ejemplo como desee, sin tener que efectuar ningún pago a IBM, con la finalidad de desarrollar, utilizar, realizar marketing o distribuir programas de aplicaciones según la interfaz de programación de las aplicaciones para la plataforma operativa en la que se han escrito tales programas de ejemplo. Estos ejemplos no se han probado exhaustivamente bajo todas las condiciones. Por lo tanto, IBM no puede garantizar ni certificar la fiabilidad, la utilidad o el funcionamiento de estos programas. Los programas de ejemplo se ofrecen "TAL CUAL", sin garantía de ningún tipo. IBM no se hará responsable de los daños derivados de la utilización que haga el usuario de los programas de ejemplo.

Cada copia de cualquier parte de estos programas de ejemplo o de cualquier trabajo que derive de éstos, debe incluir un aviso de copyright, tal como se indica a continuación:

© IBM 2012. Algunas partes de este código proceden de los programas de ejemplo de IBM Corp. © Copyright IBM Corp. 2012.

Si está viendo esta información en copia software, es posible que las fotografías y las ilustraciones en color no aparezcan.

Marcas registradas

IBM, el logotipo de IBM e [ibm.com](http://www.ibm.com) son marcas comerciales o marcas registradas de International Business Machines Corp., registradas en muchas jurisdicciones en todo el mundo. Otros nombres de productos y servicios pueden ser marcas registradas de IBM o de otras empresas. Puede encontrar una lista actualizada de las marcas registradas de IBM en la web bajo "Copyright and trademark information" en <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, el logotipo de Adobe, PostScript y el logotipo de PostScript son marcas registradas de Adobe Systems Incorporated en los Estados Unidos o en otros países.

IT Infrastructure Library es una marca registrada de la Agencia Central de Telecomunicaciones y Computación (CCTA, UK), actualmente parte de la OGC (Office of Government Commerce, UK).

Intel, el logotipo de Intel, Intel Inside, el logotipo de Intel Inside, Intel Centrino, el logotipo de Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium y Pentium son marcas comerciales o marcas registradas de Intel Corporation o sus sucursales en los Estados Unidos y en otros países.

Linux es una marca registrada de Linus Torvalds en los Estados Unidos y en otros países.

Microsoft, Windows, Windows NT y el logotipo de Windows son marcas registradas de Microsoft Corporation en los Estados Unidos y en otros países.

ITIL es una marca registrada, una marca registrada comunitaria de la OGC británica (Office of Government Commerce), y está registrada en la Oficina de Patentes y Marcas de Estados Unidos.

UNIX es una marca registrada de The Open Group en los Estados Unidos y en otros países.

Java y todas las marcas registradas y logotipos basados de Java son marcas registradas o marcas comerciales registradas Oracle y/o sus afiliados.

Cell Broadband Engine es una marca registrada de Sony Computer en los Estados Unidos y en otros países y se utiliza bajo licencia.

Linear Tape-Open, LTO, el logotipo de LTO, Ultrium el logotipo de Ultrium son marcas registradas de HP, IBM Corp. y Quantum en los Estados Unidos y en otros países.

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[®] y Sterling Integrator[®] son marcas comerciales o marcas registradas de Sterling Commerce, Inc., una empresa de IBM.

Otros nombres de empresas, productos y servicios pueden ser marcas registradas o de servicios de otras empresas.

