Sterling B2B Integrator

# Concetti del server bancario EBICS

*Versione 5.2.5*

Sterling B2B Integrator

# Concetti del server bancario EBICS

*Versione 5.2.5*

**Nota**

Prima di utilizzare queste informazioni e il prodotto che supportano, leggere le informazioni in “Informazioni particolari” a pagina 23.

# Indice

**Concetti del server EBICS (V5.2.5 o versioni successive) . . . . . .. 1**
Architettura del server bancario EBICS . . . .. 2
Gestione delle informazioni del Gestore sottoscrizioni 6
Gestione delle transazioni EBICS . . . . . .. 8
Upload da un sottoscrittore (FUL) . . . . . .. 8
Download dal server EBICS (FDL). . . . .. 10
Segmentazione e recupero . . . . . .. 11
Elaborazione VEU . . . . . .. 11
Gestione delle chiavi . . . . . .. 12
Generazione e richiamo di report EBICS. . . . .. 14
Gestione del server EBICS . . . . . .. 15
Gestione dell'ordine di sistema . . . . . .. 15
Elaborazione dei dati di ordine . . . . . .. 18
Integrazione con Sterling File Gateway . . . .. 21

**Informazioni particolari. . . . . .. 23**

# Concetti del server EBICS (V5.2.5 o versioni successive)

EBICS (Electronic Banking Internet Communication Standard) è uno standard di sicurezza e per le comunicazioni basato su Internet utilizzato principalmente per il trasferimento di dati remoti tra la propria organizzazione e una banca per le transazioni di pagamento aziendali.

EBICS consente uno scambio di file di dati che non dipende dagli standard e dai formati dei messaggi. EBICS utilizza delle procedure stabilite di crittografia e di firma digitale. Le sue funzioni sono basate su standard internazionali per le comunicazioni via Internet e una maggiore sicurezza, ad esempio XML, HTTPS, TLS e SSL. EBICS ha anche una funzionalità multibanca che consente ai clienti aziendali nei paesi che hanno adottato EBICS di poter eseguire transazioni con qualsiasi banca di detti paesi con lo stesso software.

Per poter implementare le transazioni EBICS tecnico-bancarie con una particolare banca, l'utente (insieme con il partner) deve soddisfare una serie di prerequisiti. Il prerequisito di base per implementare le transazioni EBICS è la firma di un contratto tra il partner e la banca. I dettagli seguenti sono stati concordati in questo contratto:

- La natura delle transazioni di business (tipi di ordine tecnico-bancari) che il partner condurrà con la banca.
- Informazioni relative ai conti bancari dell'utente
- Gli utenti del partner che utilizzano il sistema della banca
- Le autorizzazioni di cui dispone l'utente

Il partner riceve i dati di accesso alla banca (parametri della banca) dopo avere firmato il contratto. La banca imposta i dati master dell'utente e nel partner nel sistema bancario in base agli accordi contrattuali.

Altri prerequisiti sono la corretta inizializzazione del sottoscrittore, il download dei certificati pubblici della banca da parte dell'utente e la positiva verifica dei certificati pubblici dell'utente da parte della banca.

Il server bancario EBICS di Sterling B2B Integrator rappresenta una soluzione EBICS completa che implica una banca, un partner, la gestione di utenti e certificati, le transazioni protette di file, il recupero da errori e la creazione di report. Utilizzare Sterling B2B Integrator per inviare e ricevere transazioni EBICS.

Il server bancario EBICS di Sterling B2B Integrator supporta la specifica EBICS V2.5 per le implementazioni francese e tedesca.

Sterling File Gateway opera sulla piattaforma Sterling B2B Integrator, abilitando il trasferimento protetto dei file tra partner interni ed esterni che utilizzano protocolli di comunicazione, convenzioni di denominazione dei file e formati di file uguali o differenti. Sterling File Gateway supporta lo spostamento di trasferimenti file di grandi dimensioni e volumi elevati, con la visibilità dello spostamento dei file in un framework orientato ai processi ed altamente scalabile che riduce i problemi relativi al trasferimento di file, come quelli relativi al brokering di file e protocolli, all'automazione ed alla sicurezza dei dati.

### Requisiti di spazio del file system per le richieste FDL

Poiché il tipo di ordine FDL utilizza il file system per archiviare il payload, è importante pianificare lo storage del file system. Un payload FDL di grandi dimensioni richiede uno spazio pari a circa 6 volte la dimensione del payload stesso. Ad esempio, un payload da 5 GB richiede più di 30 GB di spazio file in Sterling B2B Integrator per elaborare la richiesta.

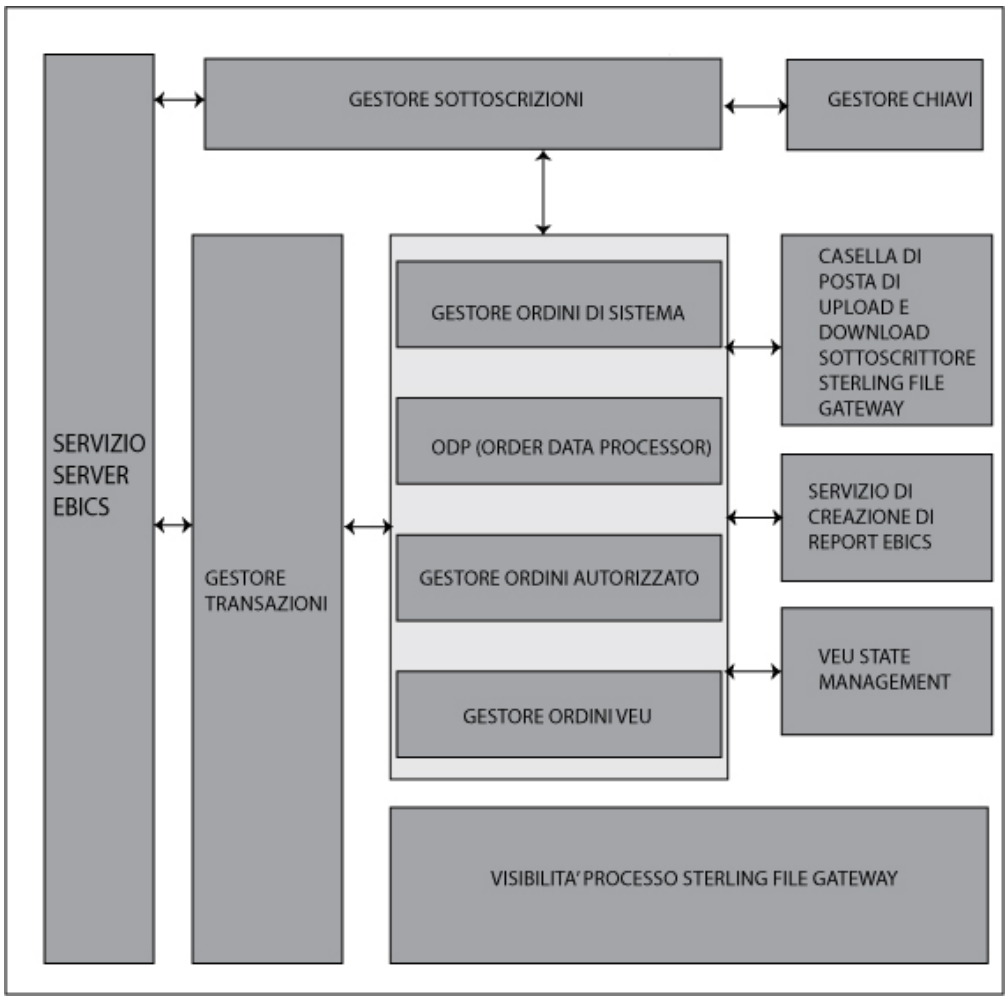
Quando si utilizza il server bancario EBICS in un ambiente cluster, è necessario configurare il file system condiviso come storage del documento tra i nodi, anche se il tipo di storage del documento predefinito è impostato su "Database". Per istruzioni, consultare la documentazione documentazione di *Installazione* appropriata.

## Architettura del server bancario EBICS

Il server bancario EBICS consente di eseguire transazioni con i partner e gli utenti utilizzando EBICS.

Le sue funzioni includono la creazione e la gestione di profili (banca, partner e utente), l'associazione di partner e utenti a tipi di ordine e formati file, l'assegnazione di autorizzazioni utente, la creazione e la gestione di certificati, l'elaborazione di dati di ordine, la memorizzazione e il richiamo di informazioni di profilo, certificati e messaggi, la gestione di flussi di messaggi e di flussi di transazioni, il trasferimento di file utilizzando i protocolli sicuri e così via.

Il seguente diagramma illustra l'architettura del server bancario EBICS:




Il *Gestore sottoscrizioni* include le seguenti funzioni:

- Gestione profili - per la creazione e la gestione di profili di banca, partner e utente
- Configurazione tipo di ordine - per configurare i tipi di ordine e i formati file
- Configurazione offerta - per il raggruppamento di un insieme di tipi di ordine e di formati file a un elenco di clienti
- Configurazione autorizzazioni utente - per assegnare tipi di ordine e formati file agli utenti
- Importazione di informazioni del Gestore sottoscrizioni - per importare i dettagli di configurazione relativi a banca, partner, utente, offerta, autorizzazioni utente, tipi di ordine e formati di file nel server bancario EBICS da un repository esterno
- Esportazione di informazioni del Gestore sottoscrizioni - per esportare i dettagli di configurazioni relativi a banca, partner, utente, offerta, autorizzazioni utente, tipi di ordine e formati di file in un repository esterno dal server bancario EBICS

Le *caselle di posta di upload e download del sottoscrittore* vengono configurate nel Gestore sottoscrizioni durante l'impostazione della sottoscrizione dell'utente.

*Gestione chiavi* si interfaccia principalmente con Gestore sottoscrizioni per creare, aggiornare, eliminare e interrogare certificati.

Gestione chiavi include le seguenti funzioni:

- Certificati autofirmati - per generare e gestire certificati autofirmati utilizzando la lunghezza di chiave 2048
- Certificati AC - per gestire i certificati di AC
- Storage di chiavi - per fornire gli archivi di chiavi per i certificati e gestire il rinnovo e la scadenza di certificati
- Importazione ed esportazione di certificati - per l'importazione e l'esportazione di certificati
- Convalida di chiavi sottoscrittore - per convalidare i valori hash dei certificati utente
- Valore hash certificato - per supportare la creazione del valore hash di certificato utilizzando SHA256

*Servizio server EBICS* si interfaccia anche con il Gestore sottoscrizioni per richiamare le informazioni di profilo di banche, partner, utenti e tipi di ordine occorrenti per la verifica e l'autenticazione di messaggi e transazioni. Opera in stretta collaborazione con Gestore transazioni per gestire tutte le transazioni EBICS.

Servizio server EBICS include le seguenti funzioni:

- Richiesta e risposta - per gestire le richieste EBICS in entrata (mediante HTTP e HTTPS) in base alle specifiche di protocollo EBICS e generando e inviando una risposta appropriata al richiedente
- Flusso di messaggi - per gestire il flusso di messaggi per le fasi di inizializzazione e di trasferimento file delle transazioni EBICS
- Autenticazione e autorizzazione - per eseguire i controlli di autorizzazione utente e autenticazione messaggi

*Gestore transazioni* si interfaccia strettamente con Servizio server EBICS per gestire il flusso di upload e di download dei tipi di ordine del sistema e dei tipi di ordine tecnico-bancario.

Gestore transazioni include le seguenti funzioni:

- Transazione asincrona - per la gestione del flusso di transazioni asincrone per il tipo di ordine tecnico-bancario (FUL) di upload. Gestisce il flusso di elaborazione ordini autorizzati in collaborazione con l'ODP (Order Data Processor) per spacchettare i dati di ordine e distribuire i dati di ordine spacchettati alla casella di posta di upload di destinazione come definito nelle impostazioni del profilo utente.
- Transazione sincrona - per gestire il flusso di transazioni sincrone per i tipi di ordine tecnico-bancari e di ordine di sistema di upload e download. Gestisce i flussi di elaborazione degli ordini di sistema, l'elaborazione dei report (FDL, PSR) e l'elaborazione degli ordini tecnico-bancari di download (FDL).
- Segmentazione e recupero - per la gestione di recupero da errore, segmentazione e nessuna riproduzione

*Gestore ordini di sistema* è responsabile dell'aggiornamento e dell'interrogazione delle informazioni di gestione chiave e delle informazioni di riferimento degli utenti.

Il Gestore ordini di sistema collabora con il Gestore transazioni ed il Gestore sottoscrizioni per aggiornare ed eseguire query delle informazioni di riferimento e dei certificati chiave dell'utente e per scaricare i parametri ed i certificati della banca.

Il *Gestore ordini autorizzato* è responsabile dell'avvio dell'ODP (Order Data Processor) per spacchettare i dati dell'ordine ricevuti dalla richiesta di tipo di ordine FUL, instradare i dati dell'ordine spacchettati verso la casella di posta di upload del sottoscrittore e per ridenominare i dati in base ad una convenzione di denominazione definita.

Il *Gestore ordini VEU* è responsabile della gestione degli ordini VEU (tipi di ordine HVD, HVE, HVS, HVT, HVU o HVZ).

L'*Order Data Processor* è responsabile dell'impacchettamento e dello spacchettamento dei dati di ordine. Si interfaccia con il Gestore sottoscrizioni e il Gestore transazioni per richiamare le informazioni pertinenti richieste per impacchettare e spacchettare i dati di ordine. Le sue funzioni includono:

- Impacchettamento - per l'impacchettamento di dati di ordine come la firma, la compressione, la crittografia e la codifica base64, a seconda del requisito del tipo di ordine.
- Spacchettamento - Per lo spacchettamento di dati di ordine come la verifica, la decompressione, la decrittografia e la decodifica base64, a seconda del requisito del tipo di ordine

Il *Servizio di creazione di report* è responsabile per la generazione del PSR (Payment Status Report) associato allo spacchettamento di dati di ordine durante un upload asincrono del flusso di transazioni dell'ordine tecnico-bancario.

La *Gestione stato VEU* è responsabile della gestione delle informazioni relative agli ordini VEU non completamente autorizzati (ad esempio, con firme in sospeso).

*Sterling File Gateway* utilizza dei template per descrivere il modo in cui viene interpretata ciascuna transazione EBICS per determinare come e dove eseguire la distribuzione e fornisce la visibilità dei dettagli dei trasferimenti per consentire la verifica e la risoluzione dei problemi.

Sterling File Gateway include le seguenti funzioni:

- Trasformazioni di nome file o file - per mappare nomi di file da input a nomi di file di output, politiche specifiche per partner, gruppi e a livello di sistema, attività di elaborazione file comuni come la compressione e la decompressione, crittografia e decrittografia PGP e firma
- Visibilità dei trasferimenti di file - vengono registrati gli eventi per il monitoraggio e la creazione di report; una traccia dettagliata per l'elaborazione della struttura di file di input-output e la determinazione dell'instradamento dinamico; capacità di visualizzare e filtrare i flussi di dati per tutti gli utenti
- Supporto completo dei protocolli di comunicazione - dopo l'installazione, sono supportati i protocolli FTP, FTP/S, SSH/SFTP, SSH/SCP e Sterling Connect:Direct; utilizzando la funzione di estendibilità, è possibile configurare ulteriori protocolli (come, ad esempio, AS2, AS3 oppure Odette FTP)
- Interfaccia partner (myFileGateway) - interfaccia basata sul browser Web che consente ai partner di caricare e scaricare file, effettuare la sottoscrizione a notifiche relative agli eventi, gestire le password, ricercare e visualizzare le attività di trasferimento dei file e generare report relativi tali attività
- Strutture di casella di posta flessibili - la capacità di specificare delle strutture di casella di posta che si avvalgono di politiche di corrispondenza di pattern e specificano attributi che devono essere "true" per tutti i partner o una serie secondaria di partner

- Instradamento dinamico - consumer derivato al runtime, mediante la struttura di casella di posta, il nome file, il nome consumer derivato dal processo business o il nome consumer derivato da mappe

## Gestione delle informazioni del Gestore sottoscrizioni

Il menu Gestore sottoscrizioni in Sterling B2B Integrator consente di:

- Creare e gestire profili di banche, partner e utenti nel database del sistema
- Creare e gestire le offerte
- Assegnare tipi di ordine e formati file a un'offerta
- Assegnare autorizzazioni agli utenti

Una banca può avere un solo profilo con un ID banca univoco. Un profilo di banca contiene le seguenti informazioni:

- ID univoco della banca

  **Nota:** Ogni ID banca deve avere un numero di porta univoco.
- Nome della banca
- Indirizzo della banca
- Certificati pubblici e privati di crittografia, autenticazione e identificazione
- URL HTTP della banca
- Versione del protocollo EBICS

Una banca può avere più URL. L'URL della banca corrispondente viene fornito a un utente per inviare richieste alla banca. L'URI (Uniform Resource Indicator) viene configurato nell'adattatore server HTTP per restare in attesa sulla porta e ricevere eventuali richieste EBICS.

Sono supportate le seguenti versioni del protocollo della banca e dei tipi di processo:

- Versione del protocollo EBICS - H004, H003. H000
- Versioni della firma - A005, A006
- Versione dell'autenticazione - X002
- Versione della crittografia - E002

Ogni partner può avere uno o più ID partner e informazioni sul conto. È necessario specificare il numero di conto, in formato nazionale (tedesco) o internazionale (IBAN). È possibile associare un ID partner a un'offerta. Il profilo di partner contiene le seguenti informazioni:

- ID univoco del partner
- Codice organizzazione del partner
- Nome del partner
- Indirizzo del partner
- ID conto e nome dell'intestatario del conto
- Valuta in cui viene eseguita la transazione
- Numero del conto
- Codice della banca

Un utente può trovarsi sotto uno o più partner. Una banca può creare un utente associandolo o meno a un partner. Per abilitare lo scambio di messaggi EBICS tra un partner e un utente, è necessario associare un ID utente a un ID partner.

Un utente trasmette i certificati pubblici alla banca tramite due percorsi di comunicazione indipendenti:

- INI - invia la chiave tecnico-bancaria pubblica
- HIA - invia la chiave di autenticazione e di identificazione pubblica e la chiave di crittografia pubblica

Quando viene inizialmente assegnato a un partner, lo stato dell'utente è Nuovo. Se l'utente invia solo la richiesta INI alla banca corrispondente, lo stato viene modificato in Parzialmente inizializzato (INI). Se l'utente invia solo la richiesta HIA alla banca, il suo stato diventa Parzialmente inizializzato (HIA). Dopo che l'utente ha inviato sia la richiesta INI sia la richiesta HIA alla banca, lo stato viene modificato in Inizializzato. L'utente invia per posta elettronica le lettere di inizializzazione delle chiavi INI e HIA alla banca. Quando la banca riceve le lettere di inizializzazione relative a INI e HIA, verifica i valori hash nei certificati rispetto al suo database. Dopo una verifica eseguita con esito positivo, lo stato dell'utente viene impostato su Pronto, indicando che l'utente può ora svolgere transazioni con la banca. L'utente scarica quindi i certificati pubblici della banca utilizzando il tipo di ordine del sistema HPB.

È possibile utilizzare i tipi di ordine HKD e HTD per richiamare le informazioni sul sottoscrittore memorizzate dalla banca dopo che lo stato dell'utente è impostato su *Pronto*.

Utilizzare il servizio Gestore sottoscrizioni EBICS per convalidare le chiavi nelle lettere di inizializzazione INI e HIA. Dopo una verifica eseguita con esito positivo, lo stato dell'utente viene aggiornato, ad esempio su Pronto, indicando che l'utente ha inviato le lettere di inizializzazione HIA e INI alla banca. È anche possibile utilizzare questo servizio per importare/esportare i dati del Gestore sottoscrizioni nel/dal database del sistema bancario.

Il profilo utente contiene le seguenti informazioni:

- ID univoco dell'utente
- Nome dell'utente
- Indirizzo dell'utente
- ID partner cui è associato l'utente
- Impostazioni della casella di posta per abilitare upload, download e archiviazione di messaggi

I tipi di ordine EBICS specificano le diverse transazioni che possono verificarsi tra il server EBICS e un client EBICS. Un tipo di ordine può avere zero o più formati file. È possibile associare i formati file ai tipi di ordine di upload e download tecnico-bancari. È possibile utilizzare i tipi di ordine di upload per eseguire l'upload dei dati di ordine da un client EBICS a un server EBICS e i tipi di ordine di download per eseguire il download di dati di ordine da un server EBICS a un client EBICS. Un tipo di ordine contiene i seguenti attributi:

- Il tipo di ordine
- Versione del protocollo EBICS
- Tipo di trasferimento - Upload o Download
- Tipo di dati di ordine - Sistema o Tecnico

Un formato file contiene i seguenti attributi:

- Il formato file
- Codice paese del formato file

Una banca può creare una o più offerte. Un'offerta fornisce un facile metodo di raggruppamento di una serie di tipi di ordine e formati file per un elenco di partner. A ogni partner viene allocato un elenco di tipi di ordine per abilitare le transazioni tra la banca e il partner. Un'offerta fornisce a una banca un modo facile per impostare un contratto con il partner. Un'offerta contiene le seguenti informazioni:

- ID banca
- Nome dell'offerta
- Tipi di ordine e i formati file con i quali il partner può scambiare messaggi
- Livello di autorizzazione per il tipo di ordine
- Numero di firme richieste per autorizzare l'ordine

Un partner può essere associato a uno o più utenti. Una banca assegna le seguenti autorizzazioni a un utente:

- Tipi di ordine e i formati file con i quali l'utente può scambiare messaggi
- Livello di autorizzazione per il tipo di ordine
- L'importo massimo (per un conto partner specifico) di cui un utente può eseguire la transazione. È possibile associare più conti partner a importi massimi differenti.
- La valuta in cui viene specificato l'importo massimo per l'utente. La valuta dipende dal conto partner associato all'importo massimo.

## Gestione delle transazioni EBICS

Gestore transazioni nel server EBICS è responsabile della gestione degli stati delle transazioni. Determina il segmento richiesto per generare il messaggio di risposta XML.

Gestore transazioni gestisce i flussi della transazione di upload e download e supporta la segmentazione ed il recupero dei dati dell'ordine.

### Upload da un sottoscrittore (FUL)

Il tipo di ordine FUL viene utilizzato per caricare i dati in una banca.

La transazione di upload si articola nelle seguenti fasi:

- Inizializzazione
- Trasferimento dei dati

L'utente invia la richiesta di upload (FUL) alla banca. FUL è un tipo di ordine di upload tecnico-bancario.

**Importante:** Per i payload FUL di grandi dimensioni, è necessario incrementare il valore dell'impostazione Tempo massimo di inattività (MaxIdleTime) nel Servizio server EBICS. Se il valore dell'impostazione MaxIdleTime è troppo basso, la transazione potrebbe essere annullata prima di essere completata. Un valore dell'impostazione appropriato per i payload FUL di grandi dimensioni è 300 minuti.

Il servizio di autorizzazione dell'ordine EBICS gestisce le richieste di ordine in entrata per il tipo di ordine di upload tecnico-bancario. Se un ordine ha ottenuto il numero di firme richiesto, questo servizio inoltre l'ordine alla casella di posta di upload del sottoscrittore. Altrimenti, questo servizio conserva i dati dell'ordine nel database finché non sarà stato ottenuto il numero di firme richiesto.

Il processo di business handleEBICSRequest riceve una richiesta dell'utente. Se la richiesta dell'utente contiene l'ultimo segmento dei dati dell'ordine, richiama in modo asincrono il processo di business EBICSOrderAuthorizationProcessing per spacchettare i dati dell'ordine e generare i seguenti file:

**Nota:** lo spacchettamento dei dati di ordine include la decodifica, la decrittografia e la decompressione dei dati di ordine.

- .DAT - contiene i dati dell'ordine spacchettati nella casella di posta di upload di un utente
- .SIG - contiene la firma dei dati dell'ordine nella casella di posta di upload di un utente
- .PRM - contiene i parametri dell'ordine nella casella di posta di upload di un utente
- .PSR - contiene un report di stato dell'elaborazione asincrona nella casella di posta di download dell'utente

## Elaborazione dell'inizializzazione

Un utente avvia una transazione inoltrando le richieste che contengono informazioni sull'ordine in entrata. In base a queste informazioni, il server EBICS verifica il tipo di ordine, esegue il test di riproduzione del messaggio, verifica l'autenticazione del messaggio e controlla l'autorizzazione dell'utente prima di accettare la richiesta.

Dopo una corretta verifica dei dati di ordine, la banca genera un ID transazione e include l'ID nella sua risposta all'utente.

## Elaborazione del trasferimento di dati

Quando è richiesto più di un segmento per trasferire i dati di ordine, la banca esegue l'autenticazione del messaggio, verifica la transazione e verifica il numero e la dimensione dei segmenti. Dopo che il server EBICS riceve l'ultimo segmento dei dati di ordine, i dati di ordine completi vengono inoltrati al processo di business EBICSOrderAuthorizationProcessing in modo asincrono e la transazione termina.

Il processo di business EBICSOrderAuthorizationProcessing spacchetta i dati di ordine e li inoltra alla casella di posta di upload dell'utente. Il processo di business EBICSOrderAuthorizationProcessing genera un report PSR (post processing report) e lo invia alla casella di posta di download dell'utente. Questo processo di business genera anche i file .SIG e .PRM da inoltrare alla casella di posta di upload dell'utente. Quando il processo di business EBICSOrderAuthorizationProcessing rileva un errore, ad esempio una firma elettronica non valida, viene generato un file .err. Utilizzare il file .err per ispezionare un file di dati di ordine non valido, se necessario.

# Download dal server EBICS (FDL)

Il tipo di ordine FDL viene utilizzato per scaricare i dati da una banca.

La transazione di download si articola nelle seguenti fasi:

- Inizializzazione
- Trasferimento dei dati
- Riconoscimento

Un utente inoltra il tipo di ordine FDL alla banca. L'utente richiede il download del report .PSR per ottenere lo stato della richiesta FUL. L'utente può anche richiedere di scaricare dei formati file validi diversi da .PSR utilizzando il tipo di ordine FDL.

**Importante:** Per i payload FDL di grandi dimensioni, è necessario incrementare il valore dell'impostazione Tempo massimo di inattività (MaxIdleTime) nel Servizio server EBICS. Se il valore di questa impostazione è troppo basso, la transazione potrebbe essere annullata prima di essere completata. Un valore dell'impostazione appropriato per i payload FDL di grandi dimensioni è 300 minuti.

## Elaborazione dell'inizializzazione

La banca verifica il messaggio dall'utente. Dopo aver verificato la richiesta dell'utente, la banca raccoglie i dati di ordine dalla casella di posta di download dell'utente in base alle informazioni sul formato file nella richiesta.

Se più di un messaggio corrisponde al formato file, la banca unisce il contenuto di ciascun messaggio in una singola aggregazione di dati di ordine e richiama il processore di dati di ordine in modo sincrono per impacchettare i dati di ordine.

Se il formato codificato dei dati di ordine supera 1 MB, i dati di ordine vengono separati in segmenti. Il primo segmento dei dati di ordine e l'ID transazione sono inclusi nella risposta all'utente.

## Elaborazione del trasferimento di dati

L'utente invia la richiesta per il successivo segmento di dati. La banca autentica il messaggio e verifica la transazione e il numero e la dimensione del segmento.

In ogni fase del trasferimento, la banca trasferisce tutti i segmenti fino all'inclusione dell'ultimo segmento dei dati di ordine nella sua risposta all'utente.

## Elaborazione del riconoscimento di dati

Dopo aver ricevuto l'ultimo segmento dei dati di ordine dalla banca, l'utente avvia l'ultima fase, la richiesta di riconoscimento, per indicare che il trasferimento di dati è stato eseguito correttamente.

Se riceve un riconoscimento positivo (codice ricevuta=0) dall'utente, la banca sposta i messaggi scaricati dalla casella di posta di download dell'utente alla casella di posta di archivio dell'utente. Se riceve un riconoscimento negativo dall'utente, la banca conserva i messaggi scaricati nella casella di posta di download dell'utente.

Se desidera scaricare dei formati file validi diversi dai report .PSR dalla casella di posta di archivio dell'utente, l'utente deve specificare un intervallo di date nella

richiesta EBICS. L'utente deve assicurarsi che l'intervallo di date corrisponda alla data di consegna del file .DAT quando vengono spostati dalla casella di posta di download a quella di archivio dell'utente.

## Segmentazione e recupero

La richiesta di dati di ordine (upload o download) non può superare 1 MB in formato compresso, crittografato, con codifica base64. Se la richiesta di dati di ordine supera 1 MB, il formato codificato deve essere separato in segmenti. Il server bancario EBICS è responsabile della combinazione di tutti questi segmenti per ripristinare il formato originale dei dati dell'ordine.

Se si verifica un errore durante la distribuzione dei segmenti di dati di ordine, è possibile eseguire il ripristino. L'utente può eseguire il download o l'upload del segmento appropriato in base al punto di ripristino inviato in risposta dal server.

Il ripristino consente la continuazione della trasmissione di un ordine nonostante il verificarsi di un errore, senza che sia necessario ritrasmettere tutti i segmenti di dati di ordine che sono stati trasmessi correttamente.

Un punto di ripristino può essere utilizzato per continuare le transazioni dal passo di transazione successivo a questo punto di ripristino nella sequenza dei passi di transazione. I punti di ripristino devono essere impostati durante il processo di ripristino:

- Per le transazioni di caricamento, il punto di ripristino è l'ultimo passo di transazione in cui la banca ha ricevuto correttamente il messaggio di richiesta e ha trasmesso una risposta all'utente. Il punto di ripristino è determinato dallo stato della transazione nel sistema bancario.
- Per le transazioni di download, possono esistere diversi punti di ripristino. Tutti i passi di transazione precedenti della transazione in cui la banca ha ricevuto correttamente il messaggio di richiesta e ha trasmesso una risposta all'utente.

## Elaborazione VEU

Il server bancario EBICS supporta la firma VEU (Distributed Electronic Signature), che consente a più partner (o sottoscrittori) di autorizzare un ordine.

VEU è un'abbreviazione tedesca che significa Distributed Electronic Signature (firma elettronica distribuita). Con la VEU, più partner (o sottoscrittori) possono autorizzare un ordine. Partner differenti da clienti differenti o dallo stesso cliente possono firmare un particolare ordine. I partner possono richiedere i propri ordini con firme in sospeso e firmarli o annullarli. Il sistema di gestione VEU nel server bancario EBICS salva gli ordini per cui le firme sono in sospeso da partner differenti fino a quando non si verifica uno dei casi riportati di seguito:

- È stato ricevuto il numero necessario di firme autorizzate.
- L'ordine viene annullato.

VEU utilizza i seguenti tipi di ordine:

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

I firmatari autorizzati di un cliente possono utilizzare diversi processi di firma che possono supportare processi hash differenti che hanno come risultato valori hash differenti. Nel processo VEU, il valore hash dei dati dell'ordine viene fornito quando vengono eseguiti i tipi di ordine HVD e HVZ. Tale valore hash deriva dalla versione della firma utilizzata dal sottoscrittore che esegue HVZ e HVD. Il valore hash viene fornito con la versione della firma utilizzata come attributo.

Di seguito è riportato un riepilogo di un processo VEU tipico:

1. Un cliente EBICS (PartnerA) avvia un ordine trasmettendo i dati dell'ordine in una transazione EBICS con l'attributo dell'ordine `OZHNN` e firmando con la classe di firma `E` o `T`.
2. Quando viene ricevuto dal sistema bancario EBICS, il sistema di gestione VEU analizza il tipo di ordine e le firme già inoltrate, inclusa la relativa classe. Se sono necessarie ulteriori firme per l'elaborazione dell'ordine, vengono memorizzate a livello intermedio per il processo VEU insieme al relativo valore hash.
3. Un altro cliente EBICS (Partner B) che dispone di una firma in sospeso e deve firmare un ordine archiviato esegue un'interrogazione utilizzando il tipo di ordine HVU o HVZ per individuare gli ordini che è autorizzato a firmare. La risposta include informazioni relative ai seguenti elementi:
   - tipo di ordine
   - numero dell'ordine
   - numero delle firme richieste e delle firme già fornite (inclusa l'indicazione che specifica se la propria firma è ancora richiesta o è già stata fornita)
   - parte dell'ordine originale
   - dimensione dei dati dell'ordine non compressi
   - (solo per il tipo di ordine HVZ) valore hash dei dati dell'ordine

   Se è stato utilizzato il tipo di ordine HVZ, ignorare il passo successivo.
4. Il partner B utilizza il tipo di ordine HVD per controllare l'ordine ed acquisire il valore hash di tale ordine.
5. Facoltativo. Se il tipo di ordine HVT è supportato dalla banca, il partner B può scaricare ulteriori dettagli dell'ordine utilizzando il tipo di ordine HVT. In base ai parametri della richiesta, vengono ricevute informazioni relative alle transazioni del singolo ordine (dati del conto, informazioni sull'importo, data di elaborazione, dati di utilizzo ed altre descrizioni) oppure i dati dell'ordine completo.
6. Una volta ricevute tutte le informazioni richieste, il partner B può firmare l'ordine utilizzando il tipo di ordine HVE. Il sistema di gestione VEU nel server bancario EBICS esegue la convalida ed aggiunge la firma all'ordine.
7. Il Partner B può decidere di annullare l'ordine utilizzando il tipo di ordine HVS.
8. Una volta completate tutte le firme, il server bancario EBICS elabora completamente l'ordine.

## Gestione delle chiavi

È possibile inserire, aggiornare e richiamare i certificati presenti nel repository di Sterling B2B Integrator.

È possibile inserire un certificato con codifica base64 (pubblico o privato) ed importare ed esportare i certificati nel repository di Sterling B2B Integrator.

È anche possibile eseguire le seguenti attività in Sterling B2B Integrator:

- Creare un certificato autofirmato con una lunghezza di chiave 2048 per EBICS
- Gestire certificati AC
- Memorizzare certificati e gestire rinnovo e scadenza dei certificati
- Accettare un certificato pubblico di un utente
- Convalidare le seguenti chiavi sottoscrittore utilizzando SHA256 come algoritmo hash:
  - Valore hash chiavi di autenticazione e identificazione (in formato esadecimale)
  - Valore hash chiave di crittografia (in formato esadecimale)
  - Valore hash chiave firma elettronica (in formato esadecimale)

Utilizzare il servizio di esportazione certificato EBICS per esportare in un sistema esterno i certificati presenti in Sterling B2B Integrator. Utilizzare questo servizio quando si desidera sincronizzare i certificati presenti in Sterling B2B Integrator con un sistema o un database esterno.

Utilizzare il servizio di importazione certificati EBICS per aggiungere i certificati da un repository esterno a Sterling B2B Integrator. È anche possibile eliminare i certificati scaduti o non validi.

## Funzioni del gestore chiavi

Il servizio di gestione ed archiviazione delle chiavi esegue le funzioni riportate di seguito:

- Convalida delle chiavi duplicate - Il certificato utilizzato per l'autenticazione o la crittografia non può essere uguale al certificato ES. Utilizzare una serie univoca di chiavi per l'autenticazione o la crittografia e la firma.
- Estensione di utilizzo della chiave X.509 – Il server bancario EBICS supporta l'utilizzo di X.509 come estensione di utilizzo della chiave.
- Verifica dei certificati CRL e OCSP

Il gestore chiavi gestisce i certificati nel repository di Sterling B2B Integrator. Esso inserisce, aggiorna e richiama i certificati nel repository di Sterling B2B Integrator ed esegue alcune funzioni sui certificati, come, ad esempio, il calcolo del valore hash del certificato.

Il gestore chiavi convalida i certificati client di cui è stato eseguito il check-in nel server prima che possano essere utilizzati. È necessario ottenere i certificati firmati da una autorità di certificazione (CA, Certificate Authority). In un certificato firmato dalla CA, l'emittente firma il certificato. Per verificare l'autenticità del certificato utente, il server bancario EBICS esegue la verifica della firma concatenata fino al certificato CA root.

Prima di iniziare le transazioni EBICS, l'amministratore EBICS deve eseguire il check-in dei certificati firmati dalla CA e dalla CA intermedia nell'archivio dei certificati CA di Sterling B2B Integrator.

Il client deve fornire tre tipi di certificati:

- Certificato di autenticazione
- Certificato di crittografia
- Certificato ES (Electronic Signature - firma elettronica)

La chiave pubblica del certificato di autenticazione viene utilizzata per la verifica delle firme digitali. I certificati di autenticazione possono essere autofirmati o firmati dalla CA. Il valore del campo Utilizzo chiave per un certificato di autenticazione è Firma digitale. Una firma digitale viene utilizzata per l'autenticazione dell'entità e l'autenticazione dell'origine dati con integrità.

La chiave pubblica del certificato di crittografia viene utilizzata per crittografare i dati dell'ordine. I certificati di crittografia possono essere autofirmati o firmati dalla CA. Il valore del campo Utilizzo chiave per un certificato di crittografia è Cifratura chiave. In EBICS, viene utilizzata una chiave simmetrica per inviare dati dell'ordine crittografati o decrittografati. La chiave simmetrica viene crittografata con il valore della chiave pubblicare del certificato di crittografia per il trasporto. La cifratura della chiave viene utilizzata quando esiste un certificato con un protocollo che crittografa le chiavi.

La chiave pubblica del certificato ES (Electronic Signature) viene utilizzata per verificare la firma dei dati dell'ordine. Il valore della chiave pubblica di un certificato della firma elettronica non deve essere uguale a quello di un certificato di crittografia o di autenticazione. Il valore del campo Utilizzo chiave per un certificato ES è Non rifiuto. Il non rifiuto protegge dalle entità di firma che negano falsamente un'azione, escludendo il certificato o la firma CRL. Le firme elettroniche sono di due tipi:

- Firma trasporto – può essere autofirmata o firmata dalla CA
- Firma personale – deve essere firmata dalla CA

## Generazione e richiamo di report EBICS

Utilizzare il servizio di creazione di report EBICS per generare un report sullo stato del pagamento (o PSR, acronimo di payment status report) con ogni richiesta di ordine di upload. Il report .PSR è in un formato XML e rispetta lo schema pain.002.001.02. Dopo essere stato generato correttamente, il report .PSR viene inserito nella casella di posta di download dell'utente EBICS.

Un report .PSR viene generato dopo l'elaborazione di ordine asincrona di ogni FUL. Un utente può inviare una richiesta FDL con il formato file pain.002.001.02.ack per richiamare il report .PSR. Se nella richiesta EBICS non è specificato alcun intervallo di date, la banca concatena i report PSR nella casella di posta di download dell'utente ed impacchetta i dati dell'ordine nella risposta EBICS.

Quando la banca riceve un riconoscimento positivo dall'utente in base al valore del parametro fornito nell'elemento FDLOrderParams della richiesta FDL, i report.PSR nella casella di posta di download dell'utente vengono spostati nella casella di posta di archivio dell'utente. Se non viene ricevuto alcun riconoscimento positivo dopo un periodo di tempo specificato, l'utilità di pianificazione del servizio server EBICS imposta nuovamente il Conteggio estraibile su 1 per i report .PSR nella casella di posta di download dell'utente, consentendo all'utente di scaricare nuovamente i report .PSR.

Se l'utente desidera scaricare i report .PSR dalla propria casella di posta di archivio, deve specificare un intervallo di date nella richiesta EBICS. L'utente deve verificare che l'intervallo di date corrisponda alla data di consegna dei report .PSR quando viene eseguito lo spostamento dalla casella di posta di download dell'utente alla casella di posta di archivio dell'utente.

## Gestione del server EBICS

Il server EBICS è implementato come servizio in Sterling B2B Integrator. Il servizio server EBICS è responsabile della gestione delle richieste EBICS in entrata (mediante HTTP e HTTPS) in base alle specifiche di protocollo EBICS e generando e inviando l'appropriata risposta agli utenti.

Il server EBICS elabora la generazione e la verifica della firma elettronica (o ES, ossia electronic signature) e l'identificazione e l'autenticazione di messaggi EBICS. Si interfaccia anche con il Gestore sottoscrizioni per richiamare le informazioni di profilo di banche, partner, utenti e tipi di ordine occorrenti per la verifica e l'autenticazione di messaggi e transazioni. I flussi di elaborazione (asincroni e sincroni) di richieste, come ad esempio FUL e FDL, sono anch'essi gestiti dal servizio. È possibile configurare il servizio per aggiornare il repository EBICS e inviare le notifiche di eventi a un'applicazione esterna durante una transazione sincrona. La gestione del flusso di messaggi per le fasi di inizializzazione e trasferimento delle transazioni EBICS è anche una delle responsabilità chiave del servizio. Il ciclo di vita delle transazioni EBICS nel sistema bancario e lo stato delle transazioni aperte sono gestiti dal server EBICS, che funge anche da storage intermedio per le firme elettroniche e i segmenti dati di ordine trasmessi.

Durante il download dei dati dell'ordine tecnico-bancari, il server EBICS raccoglie tutti i dati dell'ordine disponibili nella casella di posta dell'utente, li raggruppa in un singolo documento ed invia il documento al processore dei dati dell'ordine per impacchettare il documento, ovvero eseguire le operazioni di firma, compressione, crittografia e codifica.

Per informazioni relative alla configurazione del servizio server EBICS, consultare *Servizio server EBICS*.

## Gestione dell'ordine di sistema

Il Gestore ordini di sistema collabora con il Gestore transazioni ed il Gestore sottoscrizioni per aggiornare ed eseguire una query delle informazioni di riferimento e dei certificati chiave di un utente e per scaricare i parametri ed i certificati bancari. Genera e richiama dati di ordine XML in base alle informazioni sul profilo.

Gestore ordini di sistema gestisce anche l'implementazione di ordini di sistema di upload e di download. La seguente tabella elenca i tipi di ordine di sistema di upload supportati per le transazioni EBICS:

| Tipo di ordine di sistema di upload | Descrizione |
|---|---|
| INI | Utilizzato nell'inizializzazione sottoscrittore. Invia il certificato pubblico tecnico-bancario di un cliente al server bancario EBICS. I dati di ordine sono compressi e codificati su base64. |
| HIA | Utilizzato per trasmettere i certificati pubblici dell'utente per l'identificazione, l'autenticazione e la crittografia nel framework dell'inizializzazione del sottoscrittore. I dati di ordine sono compressi e codificati su base64. |

| Tipo di ordine di sistema di upload | Descrizione |
|---|---|
| PUB | Utilizzato per aggiornare i certificati del cliente. Invia il certificato pubblico tecnico-bancario del cliente per l'aggiornamento al server bancario EBICS. I dati dell'ordine vengono firmati, compressi, crittografati e codificati base64. |
| HCA | Utilizzato per aggiornare il certificato del cliente. Invia i seguenti certificati per l'aggiornamento del server bancario EBICS:<br>• Certificato pubblico di identificazione e autenticazione<br>• Certificato pubblico di crittografia<br>I dati dell'ordine vengono firmati, compressi, crittografati e codificati base64. |
| HCS | Utilizzato per aggiornare il certificato del cliente. Invia i seguenti certificati per l'aggiornamento del server bancario EBICS:<br>• Certificato pubblico tecnico-bancario<br>• Certificato pubblico di identificazione e autenticazione<br>• Certificato pubblico di crittografia<br>I dati dell'ordine vengono firmati, compressi, crittografati e codificati base64. |
| SPR | Utilizzato per sospendere l'autorizzazione di accesso di un utente. I dati dell'ordine vengono firmati, compressi, crittografati e codificati base64. |

La seguente tabella elenca i tipi di ordine di sistema di download supportati per le transazioni EBICS:

| Tipo di ordine di sistema di download | Descrizione |
|---|---|
| HPB | Utilizzato per eseguire il download dei certificati pubblici della banca dal server bancario EBICS. I dati di ordine vengono compressi, crittografati, e codificati su base64. Il messaggio di risposta viene firmato con una firma digitale XML utilizzando il certificato di autenticazione. I dati dell'ordine non vengono firmati. |
| HPD | Utilizzato per eseguire il download dei parametri bancari dal server bancario EBICS. I dati di ordine vengono compressi, crittografati, e codificati su base64. Il messaggio di risposta viene firmato con una firma digitale XML utilizzando il certificato di autenticazione. I dati dell'ordine non vengono firmati. |

| Tipo di ordine di sistema di download | Descrizione |
|---|---|
| HEV | Utilizzato per scaricare le informazioni sulle versioni EBICS supportate. Il messaggio di risposta è in testo non crittografato. In una risposta HEV non sono presenti dati dell'ordine. |
| HKD | Utilizzato per scaricare i dati del cliente e del sottoscrittore. Può essere utilizzato quando l'utente è nello stato Pronto. Richiama le informazioni memorizzate dalla banca relative all'azienda del sottoscrittore ed ai sottoscrittori associati (incluse le informazioni della banca). I dati di ordine vengono compressi, crittografati, e codificati su base64. Il messaggio di risposta viene firmato con una firma digitale XML utilizzando il certificato di autenticazione. I dati dell'ordine non vengono firmati. |
| HTD | Utilizzato per scaricare i dati del cliente e del sottoscrittore. Può essere utilizzato quando l'utente è nello stato Pronto. Richiama le informazioni memorizzate dalla banca relative all'azienda del sottoscrittore o le informazioni della banca. I dati di ordine vengono compressi, crittografati, e codificati su base64. Il messaggio di risposta viene firmato con una firma digitale XML utilizzando il certificato di autenticazione. I dati dell'ordine non vengono firmati. |

Il Gestore ordini di sistema richiama le informazioni memorizzate dalla banca relative all'azienda del sottoscrittore. I sottoscrittori possono richiamare le informazioni memorizzate dalla banca relative all'azienda del sottoscrittore ed a tutti i sottoscrittori associati utilizzando i tipi di ordine HKD e HTD dopo che lo stato dell'utente è impostato su 'Pronto', ad indicare che l'utente può eseguire transazioni con la banca. La risposta della banca contiene un elenco dei conti del cliente.

Le informazioni relative al conto sono incluse nella risposta HKD se è soddisfatta almeno una delle seguenti condizioni:

- Negli accordi contrattuali con la banca, è specificato che gli estratti conto verranno condivisi con il cliente
- Almeno uno dei sottoscrittori del cliente è autorizzato alla firma per il conto

I sottoscrittori possono richiamare le informazioni memorizzate dalla banca relative all'azienda del sottoscrittore o le informazioni della banca utilizzando il tipo di ordine HTD. Tuttavia, le informazioni relative ai sottoscrittori associati dell'azienda non sono condivise in questo tipo di ordine. È necessario utilizzare il tipo di ordine HKD per richiamare le informazioni relative all'azienda ed ai sottoscrittori associati (incluse le informazioni della banca). La risposta HKD ed HTD elenca i conti associati del partner per i quali il sottoscrittore dispone di autorizzazione di accesso.

Il messaggio di risposta dell'ordine di sistema di download HKD include i seguenti parametri:

- HostID
- PartnerInfo - Include i dettagli del partner, come l'indirizzo, le informazioni sul conto per cui il sottoscrittore dispone dell'autorizzazione di accesso ed i tipi di ordine che il partner è autorizzato ad utilizzare.
- UserInfo - Include i dettagli del sottoscrittore, come l'ID utente, lo stato del sottoscrittore e le informazioni sulle autorizzazioni utente. Le informazioni sulle autorizzazioni utente includono il livello di autorizzazione dell'elenco dei tipi di ordine, i conti associati ed il limite di soglia dell'importo.

## Elaborazione dei dati di ordine

È necessario impacchettare i dati di ordine per garantirne un trasferimento protetto. L'impacchettamento dei dati dell'ordine include la firma, la compressione, la crittografia e la codifica in base64, in base ai requisiti del tipo di ordine. Il destinatario deve spacchettare i dati di ordine per visualizzare gli attributi. Lo spacchettamento dei dati dell'ordine include la verifica, la decompressione, la decrittografia e la decodifica in base64, in base ai requisiti del tipo di ordine.

L'ODP (Order Data Processor) è responsabile dell'impacchettamento e dello spacchettamento dei dati di ordine. Si interfaccia con il Gestore sottoscrizioni e il Gestore transazioni per richiamare le informazioni pertinenti richieste per impacchettare e spacchettare i dati di ordine. Ad esempio, le informazioni sul profilo possono includere l'ID transazione, la direzione del flusso (upload o download), il tipo di risposta (sincrona o asincrona), il tipo di processi richiesto, l'ID oggetto della chiave crittografata e l'ID oggetto della firma elettronica (o ES, ossia Electronic Signature). Il servizio di elaborazione ordini EBICS esegue il richiamo di utenti e transazioni EBICS e l'impacchettamento e lo spacchettamento di chiavi simmetriche crittografate. In base alle informazioni sul profilo richiamate, il servizio di elaborazione ordini EBICS determina se è necessario l'impacchettamento o lo spacchettamento dei dati e richiama il servizio di impacchettamento o spacchettamento appropriato.

Il Gestore ordini autorizzato è responsabile dell'avvio dell'ODP (Order Data Processor) per spacchettare i dati dell'ordine ricevuti dalla richiesta del tipo di ordine FUL, dell'invio dei dati dell'ordine spacchettati alla casella di posta di upload del sottoscrittore di backend e della relativa ridenominazione in base ad una convenzione di denominazione definita.

Oltre al servizio di elaborazione ordini EBICS, in Sterling B2B Integrator sono disponibili i seguenti servizi per elaborare i dati dell'ordine:

- Il servizio di autorizzazione dell'ordine EBICS gestisce le richieste di ordine in entrata per il tipo di ordine di upload tecnico-bancario (FUL). Se un ordine ha ottenuto il numero di firme richiesto, questo servizio inoltra l'ordine alla casella di posta di upload del sottoscrittore. Altrimenti, il servizio inoltra l'ordine alla casella di posta degli ordini in sospeso.
- Il servizio di flusso di ordini EBICS esegue l'impacchettamento e lo spacchettamento dei dati dell'ordine utilizzando la funzionalità pipeline in Sterling B2B Integrator.
- Il servizio di packaging della firma elettronica (o ES, Electronic Signature) EBICS impacchetta o spacchetta le informazioni chiave utilizzate quando si firma o si verifica la firma elettronica.
- Il servizio di compressione EBICS esegue la compressione e la decompressione di dati di ordine utilizzando zlib in modalità pipeline.

- Il servizio di crittografia EBICS esegue la crittografia e la decrittografia dei dati di ordine utilizzando l'algoritmo AES-128 in modalità pipeline. È supportato l'algoritmo di crittografia E002.
- Il servizio di codifica EBICS esegue la codifica e la decodifica dei dati di ordine utilizzando il metodo base64 in modalità pipeline.
- Il servizio di firma EBICS esegue la firma e la verifica EBICS dei dati di ordine sul digest SHA-256 calcolato in modalità pipeline. È supportato l'algoritmo di firma A005 e A006.

I dati di ordine devono essere spacchettati per le transazioni di upload e impacchettati per le transazioni di download.

Il processo di impacchettamento comporta la seguente sequenza. Tuttavia, in base al tipo di ordine, uno o più dei seguenti processi potrebbero non essere richiesti:

1. Firma
2. Compressione
3. Crittografia
4. Codifica Base64

Il seguente esempio illustra la crittografia di un tipo di ordine. Un processo di business richiama il servizio di crittografia. Se i dati di ordine sono stati firmati, il processo di business passa la chiave simmetrica al servizio di crittografia. Se i dati di ordine non sono stati firmati, il servizio di crittografia genera e restituisce la chiave simmetrica al processo di business. Se è stata creata la chiave simmetrica, il processo di business richiama il servizio di elaborazione ordini EBICS con il tipo di messaggio di output impostato su setEncryptedKey.

Il processo di spacchettamento comporta la seguente sequenza. Tuttavia, in base al tipo di ordine, uno o più dei seguenti processi potrebbero non essere richiesti:

1. Decodifica Base64
2. Decrittografia
3. Decompressione
4. Verifica della firma

Il seguente esempio illustra la decrittografia di un tipo di ordine. Un processo di business richiama il servizio di elaborazione ordini EBICS con il tipo di messaggio di output impostato su getEncryptedKey. La chiave segreta con codifica base64 viene richiamata e impostata nei dati processo per essere utilizzata dal servizio di crittografia.

## Firme elettroniche

La firma elettronica garantisce l'autenticazione dei dati dell'ordine. Le firme garantiscono l'integrità ed il non rifiuto dei dati dell'ordine inviati dal client al server bancario.

EBICS specifica due classi di firma della firma elettronica:

- Firma personale
  - Firma singola di tipo E
  - Prima firma di tipo A
  - Seconda firma di tipo B
- Firma trasporto di tipo T

Sterling B2B Integrator supporta i seguenti tipi di firma:

- Firma trasporto di tipo T
- Firma personale o firma elettronica tecnico-bancaria di tipo E – Firma singola

Le firme trasporto possono essere certificati autofirmati o firmati dalla CA. Le firme personali devono essere firmate dalla CA e riconosciute dalla banca. Utilizzare la firma trasporto per inoltrare l'ordine e la firma personale per autorizzare l'ordine.

Nelle firme personali, è necessario specificare il numero di firme per ciascun tipo di ordine o formato file nel contratto per elaborare i dati dell'ordine. Il numero massimo di firme personali consentite è 2. La firma personale di tipo E può contenere le seguenti firme:

- Singola
- Duale facoltativa
- Duale obbligatoria

## Pre-convalida

Quando si utilizzano i tipi di ordine di upload tecnico-bancari, il sottoscrittore può inviare le informazioni nel primo passo di transazione alla banca. La banca può preconvalidare i dati dell'ordine. La preconvalida dei dati dell'ordine include quanto riportato di seguito:

- Verifica del digest dei dati
- Autorizzazione del conto
- Verifica del limite dell'importo

Una volta eseguita correttamente la preconvalida dei dati dell'ordine, il sistema bancario riceve il file FUL. La banca può utilizzare la preconvalida per elaborare i dati dell'ordine se sono soddisfatti i seguenti prerequisiti:

- La banca supporta la funzionalità di preconvalida
- Nella richiesta in entrata è presente il nodo di preconvalida

### Preconvalida del digest di dati

La banca può verificare il digest di dati se sono soddisfatti i seguenti prerequisiti:

- La banca supporta la funzionalità di preconvalida.
- Nella richiesta in entrata è presente il nodo DataDigest o di preconvalida.
- Il tipo di ordine è impostato su qualsiasi tipo di ordine di upload ad eccezione della richiesta SPR.

### Preconvalida dell'autorizzazione del conto e del limite dell'importo

La banca può verificare l'autorizzazione del conto ed il limite dell'importo se sono soddisfatti i seguenti prerequisiti:

- La banca supporta la funzionalità di preconvalida.
- Nella richiesta in entrata esiste il nodo AccountAuthorization o di preconvalida.
- L'attributo OrderAttribute non è impostato su DZHNN nella richiesta in entrata.
- Il tipo di ordine è impostato sul tipo di ordine di upload tecnico (FUL) nella richiesta in entrata.
- La classe di firma del firmatario è almeno B nell'autorizzazione del contratto.

La preconvalida verifica le informazioni sul conto indicato dal firmatario ed il limite dell'importo se è definito il numero minimo e massimo di firme personali richieste per autorizzare l'ordine. Il conto elencato in AccountAuthorization deve essere un conto partner valido. Tutti i firmatari devono essere configurati con l'autorizzazione utente per tutti i conti elencati nella preconvalida. L'importo di un valore di valuta specificato non deve superare l'importo massimo impostato nella configurazione delle autorizzazioni utente per tutti i firmatari.

## Integrazione con Sterling File Gateway

Sterling File Gateway abilita il trasferimento sicuro dei file tra partner interni ed esterni che utilizzano protocolli di comunicazione, convenzioni di denominazione dei file e formati di file uguali o differenti. Sterling File Gateway supporta EBICS per lo spostamento di trasferimenti file di grandi dimensioni e volumi elevati, con la visibilità end-to-end dello spostamento dei file in un framework orientato ai processi ed altamente scalabile, che riduce i problemi relativi al trasferimento di file, come quelli relativi al brokering di file e protocolli, all'automazione ed alla sicurezza dei dati.

I file vengono spostati dal server EBICS a Sterling File Gateway e viceversa mediante partner e caselle di posta condivise. Il Gestore sottoscrizioni crea delle caselle di posta nella struttura di Utente/Partner/Posta in entrata durante la creazione dei partner.

Sterling File Gateway utilizza i Fact di provisioning come parte della definizione di Template del canale di instradamento. I template del canale di instradamento utilizzati negli scenari EBICS devono includere la configurazione dei fact di provisioning. I canali di instradamento che utilizzano i template devono includere la specifica di valori per i fact di provisioning.

Per gli scenari in ingresso, l'ODP (Order Data Processor) EBICS porta un upload del file (FUL) di ordine EBICS dal client EBICS a un server EBICS, spacchetta il payload e lo deposita in una struttura di casella di posta Utente/Partner/Posta in entrata. Sterling File Gateway è configurato per eseguire l'instradamento da tale casella di posta per l'elaborazione downstream e la distribuzione finale ad un consumer.

Nello scenario in uscita, Sterling File Gateway è configurato in modo da depositare un messaggio nella casella di posta del consumer, che viene instradato ed archiviato in Utente/Partner/Posta in uscita. Su un download del file (FDL) di ordine EBICS da un client EBICS a un server EBICS, l'ODP (Order Data Processor) EBICS impacchetta il messaggio e lo rende disponibile al client.

Sterling File Gateway consente agli operatori di ricercare le transazioni e visualizzare i dettagli degli instradamenti e delle distribuzioni.

Alcune procedure sono necessarie per avviare l'integrazione con Sterling File Gateway. Per ulteriori informazioni relative all'integrazione con Sterling File Gateway, consultare *Sterling File Gateway Integration with EBICS* all'indirizzo http://www.ibm.com/support/knowledgecenter/SS4TGX_2.2.0/com.ibm.help.sfg_ebics.doc/SFGEB_IntegrationwEBICS.html.

# Informazioni particolari

Queste informazioni sono state sviluppate per prodotti e servizi offerti negli Stati Uniti.

IBM® può non offrire i prodotti, i servizi o le funzioni presentati in questo documento in altri paesi. Consultare il proprio rappresentante locale IBM per informazioni sui prodotti ed i servizi attualmente disponibili nella propria zona. Qualsiasi riferimento ad un prodotto, programma o servizio IBM non implica o intende dichiarare che solo quel prodotto, programma o servizio IBM può essere utilizzato. Qualsiasi prodotto funzionalmente equivalente al prodotto, programma o servizio che non violi alcun diritto di proprietà intellettuale IBM può essere utilizzato. Tuttavia, è responsabilità dell'utente valutare e verificare il funzionamento di qualsiasi prodotto, programma o servizio non IBM.

IBM può avere applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La fornitura del presente documento non concede alcuna licenza a tali brevetti. È possibile inviare per iscritto richieste di licenze a:

*IBM Director of Licensing*

*IBM Corporation*

*North Castle Drive*

*Armonk, NY 10504-1785*

*U.S.A.*

Per richieste di licenze relative ad informazioni su double-byte character set (DBCS), contattare il Dipartimento di Proprietà Intellettuale IBM nel proprio paese o inviare richieste per iscritto a:

*Intellectual Property Licensing*

*Legal and Intellectual Property Law*

*IBM Japan Ltd.*

*19-21, Nihonbashi-Hakozakicho, Chuo-ku*

*Tokyo 103-8510, Japan*

**Il seguente paragrafo non si applica al Regno Unito o a qualunque altro paese in cui tali dichiarazioni sono incompatibili con le norme locali:** IBM (INTERNATIONAL BUSINESS MACHINES CORPORATION) FORNISCE LA PRESENTE PUBBLICAZIONE "NELLO STATO IN CUI SI TROVA" SENZA GARANZIE DI ALCUN TIPO, ESPRESSE O IMPLICITE, IVI INCLUSE, A TITOLO DI ESEMPIO, GARANZIE IMPLICITE DI NON VIOLAZIONE, DI COMMERCIABILITÀ E DI IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcuni stati non consentono la rinuncia ad alcune garanzie espresse o implicite in determinate transazioni, pertanto, la presente dichiarazione può non essere applicabile.

Queste informazioni potrebbero includere inesattezze tecniche o errori tipografici. Le modifiche alle presenti informazioni vengono effettuate periodicamente; tali modifiche saranno incorporate nelle nuove pubblicazioni della pubblicazione. IBM può effettuare miglioramenti e/o modifiche ai prodotti e/o ai programmi descritti nella presente pubblicazione in qualsiasi momento senza preavviso.

Qualsiasi riferimento in queste informazioni a siti Web non IBM sono fornite solo per convenienza e non servono in alcun modo da approvazione di tali siti Web. I materiali presenti in tali siti Web non sono parte dei materiali per questo prodotto IBM e l'utilizzo di tali siti Web è a proprio rischio.

IBM può utilizzare o distribuire qualsiasi informazione fornita in qualsiasi modo ritenga appropriato senza incorrere in alcun obbligo verso l'utente.

I licenziatari di questo programma che desiderano avere informazioni allo scopo di abilitare: (i) lo scambio di informazioni tra i programmi creati indipendentemente e gli altri programmi (incluso il presente) e (ii) il reciproco utilizzo di informazioni che sono state scambiate, dovrebbero contattare:

*IBM Corporation*

*J46A/G4*

*555 Bailey Avenue*

*San Jose, CA 95141-1003*

*U.S.A.*

Tali informazioni possono essere disponibili, in base ad appropriate clausole e condizioni, includendo in alcuni casi, il pagamento di una tassa.

Il programma concesso in licenza descritto nel presente documento e tutto il materiale concesso in licenza disponibile sono forniti da IBM in base alle clausole dell'Accordo per Clienti IBM (IBM Customer Agreement), dell'IBM IPLA (International Program License Agreement) o qualsiasi altro accordo equivalente tra le parti.

Qualsiasi dato sulle prestazioni qui contenuto è stato determinato in un ambiente controllato. Pertanto, i risultati ottenuti in altri ambienti operativi possono notevolmente variare. Alcune misurazioni possono essere state effettuate su sistemi del livello di sviluppo e non vi è alcuna garanzia che tali misurazioni resteranno invariate sui sistemi generalmente disponibili. Inoltre, alcune misurazioni possono essere state stimate tramite estrapolazione. I risultati reali possono variare. Gli utenti del presente documento dovranno verificare i dati applicabili per i propri ambienti specifici.

Le informazioni relative a prodotti non IBM sono ottenute dai fornitori di quei prodotti, dagli annunci pubblicati o da altre fonti disponibili al pubblico. IBM non ha testato quei prodotti e non può confermarne l'accuratezza della prestazione, la compatibilità o qualsiasi altro reclamo relativo ai prodotti non IBM. Le domande sulle capacità dei prodotti non IBM dovranno essere indirizzate ai fornitori di tali prodotti.

Tutte le dichiarazioni relative all'orientamento o alle intenzioni future di IBM sono soggette a modifica o a ritiro senza preavviso e rappresentano solo mete e obiettivi.

Tutti i prezzi IBM mostrati, sono i prezzi al dettaglio suggeriti da IBM, sono attuali e soggetti a modifica senza preavviso. I prezzi al fornitore possono variare.

Queste informazioni sono solo per scopi di pianificazione. Le presenti informazioni sono soggette a modifiche prima che i prodotti descritti siano resi disponibili.

Queste informazioni contengono esempi di dati e report utilizzati in quotidiane operazioni aziendali. Per illustrarle nel modo più completo possibile, gli esempi includono i nomi di individui, società, marchi e prodotti. Tutti questi nomi sono fittizi e qualsiasi somiglianza con nomi ed indirizzi utilizzati da gruppi aziendali realmente esistenti è puramente casuale.

LICENZA SUL DIRITTO D'AUTORE:

Queste informazioni contengono programmi applicativi di esempio in linguaggio sorgente, che illustrano tecniche di programmazione su varie piattaforme operative. È possibile copiare, modificare e distribuire questi programmi di esempio sotto qualsiasi forma senza alcun pagamento alla IBM, allo scopo di sviluppare, utilizzare, commercializzare o distribuire i programmi applicativi in conformità alle API (application programming interface) a seconda della piattaforma operativa per cui i programmi di esempio sono stati scritti. Questi esempi non sono stati testati approfonditamente tenendo conto di tutte le condizioni possibili. IBM, quindi, non può garantire o sottintendere l'affidabilità, l'utilità o il funzionamento di questi programmi. I programmi di esempio sono forniti "NELLO STATO IN CUI SI TROVANO" e senza alcun tipo di garanzia. IBM non intende essere responsabile per alcun danno derivante dal vostro uso dei programmi di esempio.

Ogni copia o qualsiasi parte di questi programmi di esempio o qualsiasi lavoro derivato, devono contenere le seguenti informazioni relative alle leggi sul diritto d'autore:



Se si visualizzano tali informazioni come softcopy, non potranno apparire le fotografie e le illustrazioni a colori.

## Marchi

IBM, il logo IBM e ibm.com sono marchi di International Business Machines Corp., registrati in molte giurisdizioni nel mondo. Altri nomi di prodotti o servizi possono essere marchi di IBM o di altre società. Un elenco aggiornato di marchi IBM è disponibile sul Web alla pagina “Copyright and trademark information” all'indirizzo http://www.ibm.com/legal/copytrade.shtml.

Adobe, il logo Adobe, PostScript ed il logo PostScript sono marchi registrati o marchi di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.

IT Infrastructure Library è un marchio registrato di Central Computer and Telecommunications Agency che ora fa parte dell'Office of Government Commerce.

Intel, il logo Intel, Intel Inside, il logo Intel Inside, Intel Centrino, il logo Intel Centrino, Celeron, Intel Xeon, Intel SpeedStep, Itanium e Pentium sono marchi o marchi registrati di Intel Corporation o di sue consociate negli Stati Uniti e in altri paesi.

Linux è un marchio registrato di Linus Torvalds negli Stati Uniti, in altri paesi o entrambi.

Microsoft, Windows, Windows NT ed il logo Windows sono marchi di Microsoft Corporation negli Stati Uniti, in altri paesi o entrambi.

ITIL è un marchio registrato e un marchio comunitario registrato dell'Office of Government Commerce ed è registrato nell'U.S. Patent and Trademark Office.

UNIX è un marchio registrato di The Open Group negli Stati Uniti e in altri paesi.

Java™ e tutti i marchi e i logo basati su Java sono marchi di Oracle e/o sue affiliate.

Cell Broadband Engine è un marchio di Sony Computer Entertainment, Inc. negli Stati Uniti, in altri paesi o entrambi ed è usato in base ad una licenza.

Linear Tape-Open, LTO, il Logo LTO, Ultrium ed il Logo Ultrium sono marchi di HP, IBM Corp. e Quantum negli Stati Uniti e in altri paesi.

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® e Sterling Integrator® sono marchi o marchi registrati di Sterling Commerce, Inc., una società IBM.

Nomi di altre società, prodotti o servizi possono essere marchi di altre società.

Stampato in Italia