Sterling B2B Integrator

EBICS银行服务器概念

V 5.2.5

Sterling B2B Integrator

EBICS银行服务器概念

V 5.2.5

注

在使用本资料及其支持的产品之前，请阅读第 19 页的『声明』中的信息。

目录

EBICS 服务器概念（V5.2.5 或更高版本）

电子银行互联网通信标准 (EBICS) 是一项基于互联网的通信和安全标准，主要用于组织与银行间企业支付交易的远程数据传输。

EBICS 支持与消息标准和格式无关的数据文件交换功能。EBICS 使用了既定的数字签名和加密过程。其功能基于用于互联网通信和增强的安全性的国际标准，如 XML、HTTPS、TLS 和 SSL 等。EBICS 还具有多银行功能，其中，已采用 EBICS 的国家或地区中的企业客户可以与使用相同软件的国家或地区中的任何银行进行交易。

用户（与伙伴关联）必须符合一系列先决条件，才能与特定银行进行银行技术类 EBICS 交易。执行 EBICS 交易的基本先决条件是伙伴与银行之间签订合同。在此合同中，双方必须就以下详细信息达成一致:

- 伙伴与银行间的业务交易（银行技术类订单类型）的性质
- 有关用户银行帐户的信息
- 使用银行系统的伙伴用户
- 用户具有的权限和许可权

签订合同后，伙伴会收到银行的访问数据（银行参数）。银行会根据合同协议的规定，在银行系统中设置伙伴与用户主数据。

其他先决条件包括：订户成功进行初始化，用户下载银行公用证书，以及银行成功验证用户公用证书。

Sterling B2B Integrator EBICS 银行服务器是完整的 EBICS 解决方案，涉及银行、伙伴和用户管理、证书管理、安全文件交易、错误恢复及报告。使用 Sterling B2B Integrator 发送和接收 EBICS 交易。

Sterling B2B Integrator EBICS 银行服务器支持以法语和德语实现的 EBICS 规范 V2.5。

Sterling File Gateway 在 Sterling B2B Integrator 平台上运行，使用相同或不同的通信协议、文件命名约定和文件格式，在内部和外部伙伴之间启用安全文件传输。Sterling File Gateway 支持高容量的大型文件传输操作，在面向流程的高度可扩展框架中实现文件移动可视性，该框架能够缓解文件传输方面的难点，如协议和文件代理、自动化以及数据安全。

针对 FDL 请求的文件系统空间需求

由于 FDL 订单类型使用文件系统存储有效内容，因此相应规划文件系统存储很重要。大型 FDL 有效内容需要的文件空间为有效内容大小本身的 6 倍。例如，5 GB 有效内容需要 Sterling B2B Integrator 中具有超过 30 GB 文件空间以处理请求。

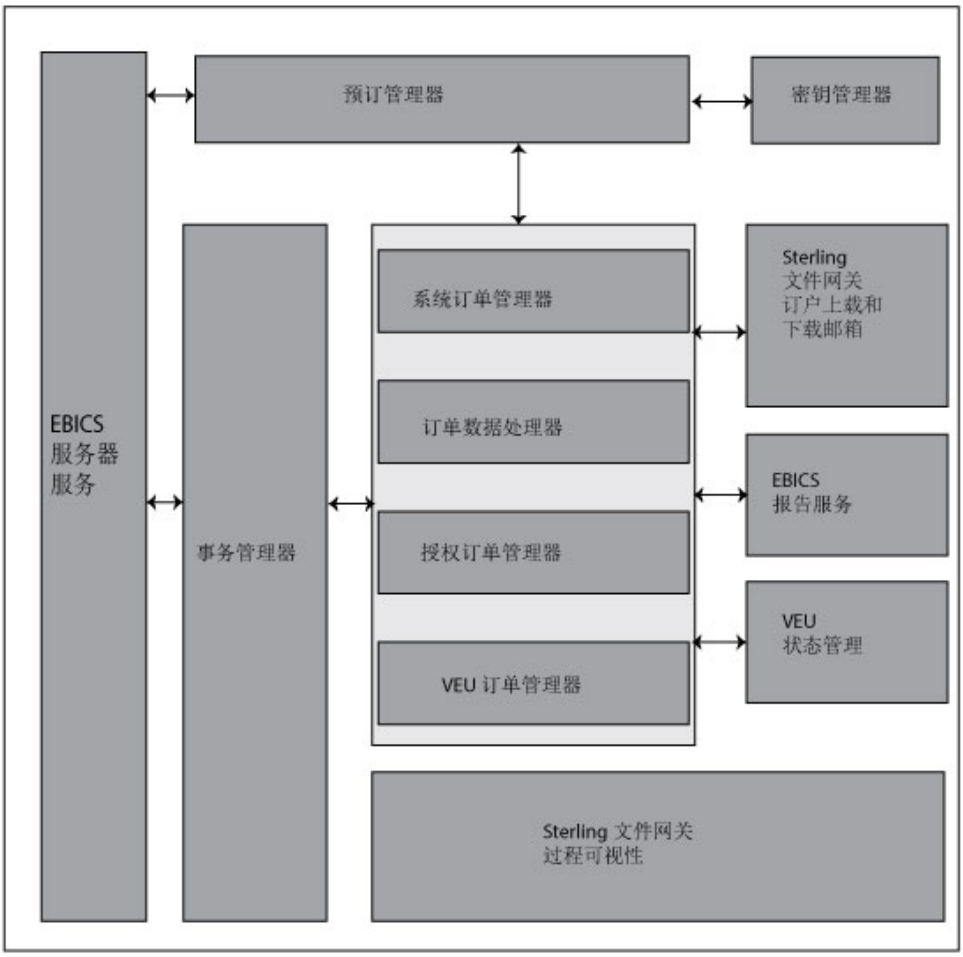
在集群环境中使用 EBICS 银行服务器时，必须将共享文件系统配置为节点之间的文档存储器，即使缺省文档存储器类型设置为“数据库”。请参阅相应“安装”文档，以获取指示信息。

EBICS 银行服务器体系结构

EBICS 银行服务器支持您使用 EBICS 与伙伴和用户进行交易。

其功能包括: 创建和管理概要文件（银行、伙伴和用户），将伙伴和用户与订单类型和文件格式相关联，指定用户许可权，创建和管理证书，处理订单数据，存储和检索概要文件信息、证书和消息，管理消息流和事务流，以及使用安全协议传输文件，等等。

下图显示了 EBICS 银行服务器体系结构:



*预订管理器*包含以下功能:

- 概要文件管理 - 用于创建和管理银行、伙伴和用户概要文件
- 订单类型配置 - 用于配置订单类型和文件格式
- 报价配置 - 用于将一组订单类型和文件格式分组到客户列表中
- 用户许可权配置 - 用于为用户指定订单类型和文件格式
- 导入预订管理器信息 - 用于将与银行、伙伴、用户、报价、用户许可权、订单类型和文件格式相关的配置详细信息从外部存储库导入 EBICS 银行服务器中

- 导出预订管理器信息 - 用于将与银行、伙伴、用户、报价、用户许可权、订单类型和文件格式相关的配置详细信息从 EBICS 银行服务器导出到外部存储库中

设置用户预订期间，预订管理器中会配置*订户上载和下载邮箱*。

*密钥管理*主要与预订管理器相结合，以创建、更新、删除和查询证书。

密钥管理包含以下功能:

- 自签名证书 - 用于使用 2048 密钥长度生成和管理自签名证书
- CA 证书 - 用于管理 CA 证书
- 密钥存储 - 用于为证书提供密钥存储，并管理证书的更新和到期
- 导入和导出证书 - 用于导入和导出证书
- 订户密钥验证 - 用于验证用户证书散列值
- 证书散列值 - 用于支持使用 SHA256 创建证书散列值

*EBICS 服务器服务*与预订管理器相结合，以检索在验证和认证消息与事务时所需的银行、伙伴、用户和订单类型的概要文件信息。它与交易管理器紧密协作，以管理所有的 EBICS 交易。

EBICS 服务器服务包含以下功能:

- 请求和响应 - 用于根据 EBICS 协议规范处理入局 EBICS 请求（通过 HTTP 和 HTTPS），并生成合适的响应以回送至请求者
- 消息流 - 用于针对 EBICS 交易的初始化和文件传输阶段来管理消息流
- 认证和授权 - 用于执行消息认证和用户授权检查

*交易管理器*与 EBICS 服务器服务紧密结合，以管理系统订单类型和银行技术类订单类型的上载和下载流。

交易管理器包含以下功能:

- 异步事务 - 用于管理上载银行技术类订单类型 (FUL) 的异步事务流。它与订单数据处理器进行协作来管理授权订单处理流，以解压订单数据，并将解压后的订单数据传送至用户概要文件设置中所定义的目标上载邮箱。
- 同步事务 - 用于管理上载和下载系统订单和银行技术类订单类型的同步事务流。它会管理系统订单处理、报告处理 (FDL, PSR) 并下载银行技术类订单 (FDL) 处理流。
- 分段和恢复 - 用于管理无重放、分段和错误恢复

*系统订单管理器*负责更新和查询密钥管理信息和用户参考信息。

系统订单管理器与交易管理器和预订管理器紧密合作，以更新和查询用户的密钥证书和参考信息，并下载银行参数和银行证书。

*授权订单管理器*负责启动订单数据处理器，以解压通过 FUL 订单类型请求收到的订单数据、将解压订单数据路由至后端订户的上载邮箱，并根据定义的命名约定对其进行重命名。

*VEU 订单管理器*负责处理 VEU 订单（订单类型 HVD、HVE、HVS、HVT、HVU 或 HVZ）。

*订单数据处理器*负责压缩和解压订单数据。它与预订管理器和交易管理器相结合，以检索在压缩和解压订单数据时所需的相关信息。其功能包括:

- 压缩 - 用于根据订单类型的需求压缩订单数据，如签名、压缩、加密和基本 64 位编码
- 解压 - 用于根据订单类型的需求解压订单数据，如验证、解压、解密和基本 64 位解码

*报告服务*负责在异步上载银行技术类订单事务流期间，生成与解压订单数据相关联的支付状态报告 (PSR)。

*VEU 状态管理*负责维护与未完全授权（例如，具有暂挂签名）的 VEU 订单相关的信息。

Sterling File Gateway 使用模板来描述如何解释每个 EBICS 交易以确定该交易的传递方式和目的地，并提供传输详细信息的可视性以用于审计和故障诊断。

Sterling File Gateway 包含以下功能:

- 文件或文件名变换 - 用于将输入映射至输出文件名，系统范围的特定于组、伙伴的策略，常规文件处理任务（如压缩和解压、PGP 加密和解密以及签名）
- 文件传输可视性 - 将记录事件以供监控和报告；详细跟踪输入/输出文件结构处理和动态路由确定过程；能够查看和过滤所有用户的数据流
- 广泛的通信协议支持 - 安装时支持 FTP、FTP/S、SSH/SFTP、SSH/SCP 和 Sterling Connect:Direct，另外可使用可扩展性功能来配置其他协议（如 AS2、AS3 或 Odette FTP）
- 伙伴界面 (myFileGateway) - 基于 Web 浏览器的界面，支持伙伴上载和下载文件、预订有关事件的通知、管理密码、搜索和查看文件传输活动，以及生成有关文件传输活动的报告
- 灵活的邮箱结构 - 能够指定利用模式匹配策略的邮箱结构，并指定其值必须对所有伙伴或伙伴子集为 true 的属性
- 动态路由选择 - 通过邮箱结构、文件名、从业务流程派生的使用者名称或从映射派生的使用者名称而在运行时派生的使用者

管理预订管理器信息

通过 Sterling B2B Integrator 中的“预订管理器”菜单，您可以:

- 创建和管理系统数据库中的银行、伙伴和用户概要文件
- 创建和管理报价
- 向报价指定订单类型和文件格式
- 向用户分配许可权

银行只能拥有一份具有唯一银行标识的概要文件。银行概要文件包含以下信息:

- 银行的唯一标识

  注: 每个银行标识都应具有唯一的端口号。
- 银行名称
- 银行地址

- 公用和专用加密、认证和识别证书
- 银行 HTTP URL
- EBICS 协议版本

银行可以具有多个 URL。将为用户提供相应的银行 URL，以便用户向银行发送请求。在 HTTP 服务器适配器中配置了统一资源标识符 (URI)，以侦听端口并接收 EBICS 请求（如存在）。

以下版本的银行协议和过程类型受支持:

- EBICS 协议版本 - H004、H003 和 H000
- 签名版本 - A005、A006
- 认证版本 - X002
- 加密版本 - E002

每个伙伴都可以拥有多个帐户信息和伙伴标识。您必须指定帐号，格式可以为国家（德国）或国际 (IBAN) 格式。您可以将伙伴标识与报价相关联。伙伴概要文件包含以下信息:

- 伙伴的唯一标识
- 伙伴的组织代码
- 伙伴名称
- 伙伴地址
- 帐户标识和帐户持有者名称
- 交易所用币种
- 帐号
- 银行代码

用户可以在多个伙伴之下。银行在创建用户时，可以将用户与伙伴相关联，也可以不关联。要启用伙伴与用户之间的 EBICS 消息交换功能，必须将用户标识与伙伴标识相关联。

用户通过两条独立的通信路径将公用证书传输至银行:

- INI - 发送公用银行技术类密钥
- HIA - 发送公用识别和认证密钥及公用加密密钥

初次向伙伴分配用户时，用户状态为“新建”。如果用户只将 INI 请求发送至相应的银行，那么状态会更改为“部分初始化 (INI)”。如果用户只将 HIA 请求发送至银行，那么状态会更改为“部分初始化 (HIA)”。在用户将 INI 和 HIA 请求发送至银行后，状态会更改为“已初始化”。用户会将 INI 和 HIA 密钥的初始化信件以邮件形式发送至银行。银行收到有关 INI 和 HIA 的初始化信件后，会根据自己的数据库验证证书中的散列值。成功验证后，用户状态会设置为“就绪”，表明用户现在可以与银行进行交易。接下来，用户可以使用 HPB 系统订单类型来下载银行公用证书。

您可以使用 HKD 和 HTD 订单类型来检索用户状态设置为*就绪*后银行存储的订户信息。

使用 EBICS 预订管理器服务来验证 INI 和 HIA 初始化信件上的密钥。成功验证后，用户状态会得到更新，如更新为“就绪”，这表明用户已将 HIA 和 INI 初始化信件发送至银行。您还可以使用此服务将预订管理器数据导入银行系统数据库或从中导出该数据。

用户概要文件包含以下信息:

- 用户的唯一标识
- 用户名称
- 用户地址
- 与用户相关联的伙伴标识
- 用于支持上载、下载和归档消息的邮箱设置

EBICS 订单类型会指定 EBICS 服务器和 EBICS 客户端之间可执行的各项交易。订单类型可以无文件格式，也可以具有多个文件格式。您可以将文件格式与银行技术类上载和下载订单类型相关联。您可以使用上载订单类型将订单数据从 EBICS 客户端上载至 EBICS 服务器，并使用下载订单类型将订单数据从 EBICS 服务器下载至 EBICS 客户端。订单类型包含以下属性:

- 订单类型
- EBICS 协议版本
- 传输类型 - 上载或下载
- 订单数据类型 - 系统或技术类

文件格式包含以下属性:

- 文件格式
- 文件格式的国家或地区代码

银行可以创建一个或多个报价。报价会提供一种简易的方法来将一组订单类型和文件格式分组到伙伴列表中。将向每个伙伴分配一份订单类型列表，以支持银行与伙伴之间的交易。通过报价，银行可轻松与伙伴订立合同。报价包含以下信息:

- 银行标识
- 报价名称
- 伙伴可用于交换消息的订单类型和文件格式
- 订单类型的授权级别
- 授权订单时所需的签名数

伙伴可与一个或多个用户相关联。银行会向用户分配以下许可权:

- 用户可用于交换消息的订单类型和文件格式
- 订单类型的授权级别
- 用户可以交易的最大金额（针对特定的伙伴帐户）。您可以将多个伙伴帐户与不同的最大金额关联。
- 为用户指定最大金额时所用币种。币种取决于与最大金额关联的伙伴帐户。

管理 EBICS 交易

EBICS 服务器中的交易管理器负责维护交易状态。它会确定在生成 XML 响应消息时所需的段。

交易管理器会处理上载和下载事务流，并支持对订单数据进行分段和恢复。

从订户上载 (FUL)

FUL 订单类型用于将数据上载到银行。

上载交易包含以下阶段:

- 初始化
- 数据传输

用户将上载 (FUL) 请求发送给银行。FUL 是银行技术类上载订单类型。

要点: 针对大型 FUL 有效内容，应该增大“EBICS 服务器服务”中的“最大空闲时间 (MaxIdleTime)”设置。如果 MaxIdleTime 设置过低，那么交易在完成之前可能被取消。针对大型 FUL 有效内容的相应设置为 300 分钟。

EBICS 订单授权服务处理银行技术类上载订单类型的入局订单请求。如果订单获得所需签名数，那么该服务会把订单转发到订户上载邮箱。否则，该服务会将订单数据保留在数据库中，直到获得所有必需数目的签名。

handleEBICSRequest 业务流程接收用户请求。如果用户请求包含订单数据的最后一个分段，那么它会异步调用 EBICSOrderAuthorizationProcessing 业务流程，以解压缩订单数据并生成以下文件:

注: 解压缩订单数据包含解码、解密和解压缩订单数据。

- .DAT - 在用户上载邮箱中包含解压缩的订单数据
- .SIG - 在用户上载邮箱中包含订单数据的签名
- .PRM - 在用户上载邮箱中包含订单参数
- .PSR - 在用户下载邮箱中包含异步处理的状态报告

处理初始化

用户通过提交包含有关入局订单的信息的请求来启动交易。基于该信息，EBICS 服务器在接受请求前会验证订单类型、执行消息重放测试、验证消息认证，并检查用户权限。

订单数据验证成功后，银行会生成交易标识，并在其提供给用户的响应中包含此标识。

处理数据传输

当传输订单数据需要多个分段时，银行会执行消息认证、验证交易并验证分段的数目和大小。在 EBICS 服务器接收订单数据的最后一个分段后，会将完整的订单数据异步转发到 EBICSOrderAuthorizationProcessing 业务流程，从而终止该交易。

EBICSOrderAuthorizationProcessing 业务流程会解压缩订单数据，并将其转发到用户上载邮箱。EBICSOrderAuthorizationProcessing 业务流程会生成后处理报告 (PSR)，并将其路由至用户的下载邮箱。该业务流程还会生成 .SIG 和 .PRM 文件，以转发到用户的上载邮箱。当 EBICSOrderAuthorizationProcessing 业务流程遇到错误（例如，无效的电子签名）时，会生成 .err 文件。如果需要，使用该 .err 文件检查无效的订单数据文件。

从 EBICS 服务器 (FDL) 下载

FDL 订单类型用于从银行下载数据。

下载事务由以下几个阶段组成:

- 初始化
- 数据传输
- 确认

用户会向银行提交 FDL 订单类型。用户会请求下载 .PSR 报告，以获得 FUL 请求的状态。用户还可以使用 FDL 订单类型，请求下载 .PSR 之外的其他有效文件格式。

要点: 针对大型 FDL 有效内容，应该增大“EBICS 服务器服务”中的“最大空闲时间 (MaxIdleTime)”设置。如果此设置过低，那么交易在完成之前可能被取消。针对大型 FDL 有效内容的相应设置为 300 分钟。

处理初始化

银行会验证用户的消息。银行在验证用户的请求后，会根据请求中的文件格式信息，从用户下载邮箱中收集订单数据。

如果有多条消息与文件格式相符，银行会将每条消息的内容合并到同一订单数据中，并同步调用订单数据处理器以压缩订单数据。

如果订单数据的编码格式超出 1 MB，那么订单数据会分隔成几段。订单数据的第一段和交易标识会包含在针对用户的响应中。

处理数据传输

用户会为下一数据段发送请求。银行会认证消息，验证交易、段号和大小。

在每个传输阶段中，银行都会传输所有的段，直至订单数据的最后一段包含在针对用户的响应中。

处理数据确认

在从银行收到订单数据的最后一段后，用户会启动最后一个阶段（即确认请求），以表明数据传输成功。

如果银行从用户收到肯定的确认（接收代码=0），那么银行会将下载的消息从用户下载邮箱移至用户归档邮箱。如果银行从用户收到否定的确认，那么银行会将下载的消息保留在用户下载邮箱中。

如果用户要从其归档邮箱中下载 .PSR 报告之外的有效文件格式，那么用户必须在 EBICS 请求中指定日期范围。用户必须确保日期范围与 .DAT 文件在从用户下载邮箱移至用户归档邮箱时的删除日期相匹配。

分段和恢复

订单数据请求（上载或下载）的压缩、加密和基本 64 位编码格式不能超过 1 MB。如果订单数据请求超过 1 MB，那么编码格式必须分割为多个段。EBICS 银行服务器负责组合所有这些分段，以将订单数据恢复为原始格式。

如果在传送订单数据分段期间发生错误，可以执行恢复。用户可根据由服务器作为响应发送的恢复点下载或上载适当的分段。

恢复允许在发生错误的情况下继续传输订单，而无需重新传输已成功传输的所有订单数据段。

恢复点可用于从交易步骤顺序中该恢复点之后的交易步骤继续交易。在恢复过程期间，必须设置恢复点:

- 对于上载交易，恢复点是银行成功接收消息请求并向用户传输响应中的最后一个交易步骤。恢复点是由银行系统中的交易状态确定的。
- 对于下载交易，可能存在多个恢复点。银行成功接收消息请求并向用户传输响应的交易之前的所有交易步骤。

VEU 处理

EBICS 银行服务器支持分布式电子签名 (VEU)，此签名允许多个合作伙伴（或订户）授权订单。

VEU 是德语缩写词，表示分布式电子签名。使用 VEU，多个合作伙伴（或订户）可授权订单。来自不同客户或相同客户的不同合作伙伴可对特定订单签名。合作伙伴可请求其具有暂挂签名的订单，对其进行签名或取消。EBICS 银行服务器中 VEU 管理系统保存来自合作伙伴中签名处于暂挂的订单，直至发生以下其中一种情况:

- 已收到必需数目的授权签名。
- 已取消订单。

VEU 使用以下订单类型:

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

客户的授权签名可使用不同签名过程，这些过程可支持生成不同散列值的不同散列过程。在 VEU 过程中，执行订单类型 HVD 和 HVZ 时，提供了订单数据的散列值。此散列值派生自执行 HVZ 和 HVD 的订户使用的签名版本。用作属性的签名版本中随附了散列值。

以下是典型 VEU 过程的摘要:

1. EBICS 客户（合作伙伴 A）通过使用订单属性 OZHNN 在 EBICS 交易中传输订单数据并使用签名类 E 或 T 进行签名来发起订单。

2. EBICS 银行服务器接收时，VEU 管理系统会分析订单类型和已提交的签名（包括其类）。如果需要更多签名以处理订单，那么会立即针对 VEU 过程对签名及其散列值进行中间存储。
3. 具有暂挂签名且需要对存储订单签名的其他 EBICS 客户（合作伙伴 B）将使用订单类型 HVU 或 HVZ 进行查询，以找到有权签名的订单。响应包含有关以下相关信息:
   - 订单类型
   - 订单号
   - 所需的签名数以及已提供的数目（包含是否仍需要其自己的签名或是否已提供此签名）
   - 原始订单方
   - 未压缩订单数据的大小
   - （仅订单类型 HVZ）订单数据的散列值

   如果使用了订单类型 HVZ，那么会跳过下一个步骤。
4. 合作伙伴 B 使用订单类型 HVD 检查订单，并获取此订单的散列值。
5. 可选。如果银行支持订单类型 HVT，那么合作伙伴 B 可使用订单类型 HVT 下载更多订单详细信息。根据请求参数，他们接收有关单个订单交易（帐户数据、金额信息、处理日期、利用率数据和其他描述）或完整订单数据的信息。
6. 收到所有必需信息后，合作伙伴 B 可使用订单类型 HVE 对订单进行签名。 EBICS 银行服务器中 VEU 管理系统验证签名并将签名添加到订单。
7. 合作伙伴 B 可选择使用订单类型 HVS 取消订单。
8. 完成所有签名后，EBICS 银行服务器将完成订单处理。

管理密钥

您可以插入、更新和检索 Sterling B2B Integrator 存储库中存在的证书。

您可以插入基本 64 位编码证书（公用或专用），将证书导入 Sterling B2B Integrator 存储库中以及从中导出证书。

您还可以在 Sterling B2B Integrator 中执行以下任务:

- 使用 EBICS 的密钥长度 2048 创建自签名证书
- 管理 CA 证书
- 存储证书并管理证书的更新和到期
- 接受用户的公用证书
- 使用 SHA256 作为散列算法来验证以下订户密钥:
  - 识别和认证密钥散列值（十六进制格式）
  - 加密密钥散列值（十六进制格式）
  - 电子签名密钥散列值（十六进制格式）

使用 EBICS 导出证书服务将 Sterling B2B Integrator 中存在的证书导出到外部系统。要将 Sterling B2B Integrator 中存在的证书与外部数据库或系统进行同步，请使用此服务。

使用 EBICS 导入证书服务将外部存储库中的证书添加至 Sterling B2B Integrator 中。您还可以删除到期或无效的证书。

密钥管理器的功能

密钥管理和存储将执行以下功能:

- 重复密钥验证 - 用于认证或加密的证书不能与 ES 证书相同。对认证或加密和签名使用唯一的密钥集。
- X.509 密钥使用扩展 - EBICS 银行服务器支持使用 X.509 作为密钥使用扩展。
- OCSP 和 CRL 证书验证

密钥管理器将管理 Sterling B2B Integrator 存储库中的证书。它会在 Sterling B2B Integrator 存储库中插入、更新和检索证书，并对证书运行相关功能，如计算证书的散列值。

密钥管理器将先验证检入服务器的客户机证书，之后才可以使用这些证书。您必须从认证中心获取 CA 签名的证书。在 CA 签名的证书中，颁发者会对证书进行签名。为验证用户证书的真实性，EBICS 银行服务器会执行链式签名验证直至根 CA 证书。

在开始 EBICS 交易之前，EBICS 管理员必须检入 Sterling B2B Integrator CA 证书存储库中 CA 签名的证书和中间 CA 签名的证书。

客户机必须提供三种类型的证书:

- 认证证书
- 加密证书
- 电子签名 (ES) 证书

认证证书的公用密钥用于验证数字签名。认证证书可以是 CA 签名的证书或自签名证书。认证证书的密钥使用字段的值是“数字签名”。数字签名用于实体认证和具有完整性的数据源认证。

加密证书的公用密钥用于加密订单数据。加密证书可以是 CA 签名的证书或自签名证书。加密证书的密钥使用字段的值是“密钥加密”。在 EBICS 中，对称密钥用于对加密或解密的订单数据分流。使用用于传输的加密证书的公用密钥值对对称密钥进行加密。当存在的证书具有对密钥进行加密的协议时，将使用密钥加密。

电子签名 (ES) 证书的公用密钥用于验证订单数据的签名。电子签名证书的公用密钥值不应与认证或加密证书相同。电子签名证书的密钥使用字段的值为“不可抵赖”。不可抵赖将防止签名实体错误地拒绝某个操作、排除证书或 CRL 签名。电子签名具有两种类型:

- 传输签名 - 可以是 CA 签名或自签名
- 个人签名 - 必须是 CA 签名

生成和检索 EBICS 报告

使用 EBICS 报告服务对每个上载订单 (FUL) 请求生成支付状态报告 (PSR)。.PSR 报告为 XML 格式，并遵循 pain.002.001.02 模式。成功生成 .PSR 报告后，会将该报告置于 EBICS 用户下载邮箱中。

对每个 FUL 进行异步订单处理后，会生成 .PSR 报告。用户可以发送具有 pain.002.001.02.ack 文件格式的 FDL 请求，以检索 .PSR 报告。如果未在 EBICS 请求中指定任何日期范围，那么银行会连接用户下载邮箱中的 PSR 报告，并打包 EBICS 响应中的订单数据。

当银行根据 FDL 请求中的 FDLOrderParams 元素下提供的参数值从用户收到肯定的确认时，用户下载邮箱中的 .PSR 报告将移至用户归档邮箱。如果在指定的超时周期后未收到任何肯定的确认，那么 EBICS 服务器服务调度程序会针对用户下载邮箱中的 .PSR 报告将“可提取计数”恢复为 1，支持用户重新下载 .PSR 报告。

如果用户要从用户的归档邮箱中下载 .PSR 报告，那么用户必须在 EBICS 请求中指定日期范围。用户必须确保日期范围与 .PSR 报告在从用户下载邮箱移至用户归档邮箱时的删除日期相匹配。

管理 EBICS 服务器

EBICS 服务器已实施为 Sterling B2B Integrator 中的一项服务。EBICS 服务器服务负责根据 EBICS 协议规范来处理入局 EBICS 请求（通过 HTTP 和 HTTPS），生成正确的响应并将其回送至用户。

EBICS 服务器会处理电子签名 (ES) 的生成和验证过程，以及 EBICS 消息的识别和认证过程。它还与预订管理器相结合，以检索在验证和认证消息与事务时所需的银行、伙伴、用户和订单类型的概要文件信息。请求（如 FUL 和 FDL）的处理流（异步和同步）也由该服务管理。您可以配置服务以更新 EBICS 存储库，并在同步事务期间将事件通知发送至外部应用程序。针对 EBICS 交易的初始化和传输阶段来管理消息流，这也是该服务的关键职责之一。银行系统中的 EBICS 交易生命周期和公开事务状态由 EBICS 服务器进行管理，该服务器还充当传输的订单数据段和电子签名 (ES) 的中间存储器。

在下载银行技术类订单数据时，EBICS 服务器会收集用户邮箱中的所有可用订单数据，将其连接到一个文档中，并将该文档发送至订单数据处理器以将该文档打包，即，对文档进行签名、压缩、加密和编码。

要了解有关配置 EBICS 服务器服务的信息，请参阅 *EBICS 服务器服务*。

管理系统订单

系统订单管理器与交易管理器和预订管理器紧密合作，以更新和查询用户的密钥证书和参考信息，并下载银行参数和银行证书。它会根据概要文件信息生成并检索 XML 订单数据。

系统订单管理器还能用于上载和下载系统订单。下表列出了 EBICS 交易所支持的上载系统订单类型:

上载系统订单类型	描述
INI	在订户初始化过程中使用。将客户的银行技术类公用证书发送给 EBICS 银行服务器。订单数据会进行压缩和基本 64 位编码。

上载系统订单类型	描述
HIA	用于传输用户公用证书，以在订户初始化框架内进行识别、认证和加密。订单数据会进行压缩和基本 64 位编码。
PUB	用于更新客户证书。发送客户的银行技术类公用证书来更新 EBICS 银行服务器。订单数据会进行签名、压缩、加密和基本 64 位编码。
HCA	用于更新客户的证书。发送以下证书来更新 EBICS 银行服务器: • 识别和认证公用证书 • 加密公用证书 订单数据会进行签名、压缩、加密和基本 64 位编码。
HCS	用于更新客户的证书。发送以下证书来更新 EBICS 银行服务器: • 银行技术类公用证书 • 识别和认证公用证书 • 加密公用证书 订单数据会进行签名、压缩、加密和基本 64 位编码。
SPR	用于暂挂用户的访问授权。订单数据会进行签名、压缩、加密和基本 64 位编码。

下表列出了 EBICS 交易所支持的下载系统订单类型:

下载系统订单类型	描述
HPB	用于从 EBICS 银行服务器下载银行公用证书。订单数据会进行压缩、加密和基本 64 位编码。将使用认证证书通过 XML 数字签名对响应消息进行签名。不会对订单数据进行签名。
HPD	用于从 EBICS 银行服务器下载银行参数。订单数据会进行压缩、加密和基本 64 位编码。将使用认证证书通过 XML 数字签名对响应消息进行签名。不会对订单数据进行签名。
HEV	用于下载有关所支持的 EBICS 版本的信息。响应消息是明文。HEV 响应中没有订单数据。
HKD	用于下载客户和订户数据。当用户处于“就绪”状态时，可以使用。检索银行存储的与订户公司和关联订户相关的信息（包括银行自己的信息）。订单数据会进行压缩、加密和基本 64 位编码。将使用认证证书通过 XML 数字签名对响应消息进行签名。不会对订单数据进行签名。

下载系统订单类型	描述
HTD	用于下载客户和订户数据。当用户处于“就绪”状态时，可以使用。检索银行存储的与订户公司相关的信息或银行自己的信息。订单数据会进行压缩、加密和基本 64 位编码。将使用认证证书通过 XML 数字签名对响应消息进行签名。不会对订单数据进行签名。

系统订单管理器会检索银行存储的与订户公司相关的信息。用户状态设置为“就绪”（表明用户可以与银行交易）后，订户可以使用 HKD 和 HTD 订单类型，检索银行存储的与订户公司及所有关联订户相关的信息。银行的响应包含客户帐户列表。

如果至少满足以下一个条件，帐户信息将包含在 HKD 响应中:

- 在与银行签订的合同协议中，指定将与客户共享对帐单
- 至少授权客户的一个订户对帐户签名

订户可以使用 HTD 订单类型检索银行存储的与订户公司相关的信息或银行自己的信息。但是，不会在该订单类型中共享与公司关联订户相关的信息。您必须使用 HKD 订单类型检索与公司和关联订户相关的信息（包括银行自己的信息）。 HKD 和 HTD 响应将列出订户有权访问的伙伴的关联帐户。

HKD 下载系统订单的响应消息包含以下参数:

- HostID
- PartnerInfo - 包含伙伴的详细信息，如地址、订户有权访问的帐户信息以及伙伴有权使用的订单类型。
- UserInfo - 包含订户的详细信息，如用户标识、订户状态以及用户许可权信息。用户许可权信息包含订单类型列表的授权级别、关联帐户以及金额阈值限制。

处理订单数据

为确保订单数据的安全传输，订单数据必须进行压缩。压缩订单数据包含根据订单类型需求进行签名、压缩、加密和基本 64 位编码。接收方必须解压缩订单数据才能查看属性。解压订单数据包含根据订单类型需求进行验证、解压、解密和基本 64 位解码。

订单数据处理器负责压缩和解压缩订单数据。它与预订管理器和交易管理器相结合，以检索在压缩和解压缩订单数据时所需的相关信息。例如，概要文件信息可能包含交易标识、流的方向（上载或下载）、响应类型（同步或异步）、所需流程的类型、加密密钥的对象标识以及电子签名 (ES) 的对象标识。EBICS 订单处理服务执行 EBICS 交易和用户检索，以及加密对称密钥的压缩和解压缩。基于检索的配置文件信息，EBICS 订单处理服务会确定是否需要压缩或解压缩订单数据，并调用适当的压缩或解压缩服务。

授权订单管理器负责启动订单数据处理器，以解压通过 FUL 订单类型请求收到的订单数据、将解压订单数据路由至后端订户的上载邮箱，并根据定义的命名约定对其进行重命名。

除 EBICS 订单处理服务以外，以下服务在 Sterling B2B Integrator 中可用于处理订单数据:

- EBICS 订单授权服务处理银行技术类上载订单类型 (FUL) 的入局订单请求。如果订单满足需要的签名数，该服务会将订单转发至订户上载邮箱。否则，该服务会将订单转发给暂挂订单邮箱。
- EBICS 订单流式方法服务使用 Sterling B2B Integrator 中的流水线功能压缩和解压缩订单数据。
- EBICS ES 打包服务可压缩或解压缩签名并验证 ES 时使用的密钥信息。
- EBICS 压缩服务使用流水线方式的 zlib 压缩和解压订单数据。
- EBICS 加密服务使用流水线方式的 AES-128 算法执行订单数据的加密和解密。支持 E002 加密算法。
- EBICS 编码服务使用流水线方式的基本 64 位方法执行订单数据的编码和解码。
- EBICS 签名服务使用以流水线计算的 SHA-256 摘要执行订单数据的签名和验证。支持 A005 和 A006 签名算法。

必须解压缩订单数据才能上载交易，必须压缩订单数据才能下载交易。

压缩过程包含以下顺序。但是，基于订单类型，以下一个或多个过程可能并非必需:

1. 签名
2. 压缩
3. 加密
4. 基本 64 位编码

以下示例说明了订单类型的加密。业务流程会调用加密服务。如果订单数据已签名，那么业务流程会将对称密钥传递给加密服务。如果订单数据未签名，那么加密服务会生成对称密钥并将其返回给业务流程。如果对称密钥已创建，那么业务流程会调用 EBICS 订单处理服务，并将输出消息类型设置为 setEncryptedKey。

解压缩过程包含以下顺序。但是，基于订单类型，以下一个或多个过程可能并非必需:

1. 基本 64 位解码
2. 解密
3. 解压
4. 验证签名

以下示例说明了订单类型的解密。业务流程会调用 EBICS 订单处理服务，并将输出消息类型设置为 getEncryptedKey。在流程数据中会检索并设置基本 64 位编码密钥，以供加密服务使用。

电子签名

电子签名 (ES) 确保对订单数据进行认证。签名确保客户机发送至银行服务器的订单数据具有完整性和不可抵赖性。

EBICS 指定 ES 的两类签名:

- 个人签名
  - 类型为 E 的单个签名
  - 类型为 A 的首个签名

  - 类型为 B 的第二个签名
- 类型为 T 的传输签名

Sterling B2B Integrator 支持以下签名类型:

- 类型为 T 的传输签名
- 个人签名或类型为 E 的银行技术类 ES - 单个签名

传输签名可以是自签名证书或 CA 签名的证书。个人签名必须由 CA 签名，并且由银行识别。使用传输签名提交订单和个人签名以授权订单。

在个人签名中，您必须在合同中为每种订单类型或文件格式指定签名数，以处理订单数据。允许的最大个人签名数为 2。类型为 E 的个人签名可以包含以下签名:

- 单个
- 可选两个
- 必需两个

预验证

当使用银行技术类上载订单类型时，订户可以在第一个交易步骤中向银行发送信息。银行可以预验证订单数据。预验证订单数据包含以下内容:

- 数据摘要验证
- 帐户授权
- 金额限制验证

在预验证订单数据成功之后，银行系统会收到 FUL 文件。如果满足以下先决条件，银行就可以使用预验证来处理订单数据:

- 银行支持预验证功能
- 预验证节点存在于入局请求中

预验证数据摘要

如果满足以下先决条件，银行就可以验证数据摘要:

- 银行支持预验证功能。
- 预验证或数据摘要节点存在于入局请求中。
- 将订单类型设置为 SPR 请求之外的任何上载订单类型。

预验证帐户授权和金额限制

如果满足以下先决条件，银行就可以验证帐户授权和金额限制:

- 银行支持预验证功能。
- 预验证或帐户授权节点存在于入局请求中。
- 在入局请求中，未将 OrderAttribute 属性设置为 DZHNN。
- 在入局请求中，将订单类型设置为技术上载订单类型 (FUL)。
- 在合同许可权中，签署者的签名类至少为 B。

如果定义了授权订单所需个人签名的最小数量和最大数量，预验证功能将会验证签署者指定的帐户信息和金额限制。 “帐户授权”下列出的帐户必须是有效的伙伴帐户。必须

配置所有签署者，以对“预验证”中列出的所有帐户具有用户许可权。所指定货币值的金额不得超出任何签署者的“用户许可权”配置中设置的最大金额。

与 Sterling File Gateway 集成

Sterling File Gateway 使用相同或不同的通信协议、文件命名约定和文件格式，在内部和外部伙伴之间启用安全文件传输。Sterling File Gateway 支持 EBICS 执行高容量的大型文件传输操作，在面向流程的高度可扩展框架中实现端到端的文件移动可视性，该框架能够缓解文件传输方面的难点，如协议和文件代理、自动化以及数据安全。

文件通过共享邮箱和伙伴在 EBICS 服务器和 Sterling File Gateway 之间移动。预订管理器会在创建伙伴的过程中，在用户/伙伴/收件箱的结构中创建邮箱。

Sterling File Gateway 使用“供应事实”作为“路由通道模板”定义的一部分。 EBICS 场景中使用的路由通道模板必须包含供应事实配置。使用模板的路由通道必须包含供应事实的值的规范。

对于入站场景，EBICS 订单数据处理器 (ODP) 会将 EBICS 订单文件上载 (FUL) 从 EBICS 客户端移至 EBICS 服务器，再解压有效内容并存入用户/伙伴/收件箱邮箱结构中。Sterling File Gateway 可配置为从该邮箱进行路由，以进行下游处理并最终传送至使用者。

在出站场景中，Sterling File Gateway 配置为在使用者邮箱中存放消息，该消息将路由并存储到用户/伙伴/发件箱中。在进行 EBICS 订单文件下载 (FDL)（从 EBICS 客户端至 EBICS 服务器）时，EBICS 订单数据处理器 (ODP) 会将消息打包，并提供给客户端。

Sterling File Gateway 支持操作员搜索交易，并查看路径和传送过程的详细信息。

需要某些过程才能启动与 Sterling File Gateway 的集成。有关与 Sterling File Gateway 集成的更多信息，请参阅“Sterling File Gateway 与 EBICS 的集成”（网址为 http://www.ibm.com/support/knowledgecenter/SS4TGX_2.2.0/com.ibm.help.sfg_ebics.doc/SFGEB_IntegrationwEBICS.html）。

声明

本信息是为在美国提供的产品和服务编写的。

IBM® 可能在其他国家或地区不提供本文档中讨论的产品、服务或功能特性。有关您当前所在区域的产品和服务的信息，请向您当地的 IBM 代表咨询。任何对 IBM 产品、程序或服务的引用并非意在明示或暗示只能使用 IBM 的产品、程序或服务。只要不侵犯 IBM 的知识产权，任何同等功能的产品、程序或服务，都可以代替 IBM 产品、程序或服务。但是，评估和验证任何非 IBM 产品、程序或服务，将由用户自行负责。

IBM 公司可能已拥有或正在申请与本文档内容有关的各项专利。提供本文档并未授予用户任何使用这些专利的任何许可。您可以用书面方式将许可查询寄往:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

有关双字节字符集（DBCS）信息的许可查询，请与您所在国家或地区的 IBM 知识产权部门联系，或用书面方式将查询寄往:

Intellectual Property Licensing

Legal and Intellectual Property Law

IBM Japan Ltd.

19-21, Nihonbashi-Hakozakicho, Chuo-ku

Tokyo 103-8510, Japan

本条款不适用英国或任何这样的条款与当地法律不一致的国家或地区: International Business Machines Corporation“按现状”提供本出版物，不附有任何种类的（无论是明示的还是暗含的）保证，包括但不限于暗含的有关非侵权、适销和适用于某种特定用途的保证。某些国家或地区在某些事务中不允许免除明示或暗含的保证。因此本条款可能不适用于您。

本信息中可能包含技术方面不够准确的地方或印刷错误。此处的信息将定期更改；这些更改将编入本资料的新版本中。IBM 可以随时对本资料中描述的产品和/或程序进行改进和/或更改，而不另行通知。

本信息中对非 IBM Web 站点的任何引用都只是为了方便起见才提供的，不以任何方式充当对那些 Web 站点的保证。那些 Web 站点中的资料不是 IBM 产品资料的一部分，使用那些 Web 站点带来的风险将由您自行承担。

IBM 可以按它认为适当的任何方式使用或分发您所提供的任何信息而无须对您承担任何责任。

本程序的被许可方如果要了解有关程序的信息以达到如下目的: (i) 允许在独立创建的程序和其他程序（包括本程序）之间进行信息交换，以及 (ii) 允许对已经交换的信息进行相互使用，请与下列地址联系:

IBM Corporation

J46A/G4

555 Bailey Avenue

San Jose, CA 95141-1003

U.S.A.

只要遵守适当的条件和条款，包括某些情形下的一定数量的付费，都可获得这方面的信息。

本资料中描述的许可程序及其所有可用的许可资料均由 IBM 依据 IBM 客户协议、IBM 国际软件许可协议或任何同等协议中的条款提供。

此处包含的任何性能数据都是在受控环境中测得的。因此，在其他操作环境中获得的数据可能会有明显的不同。有些测量可能是在开发级的系统上进行的，因此不保证与一般可用系统上进行的测量结果相同。此外，有些测量是通过推算而估计的，实际结果可能会有差异。本文档的用户应当验证其特定环境的适用数据。

涉及非 IBM 产品的信息可从这些产品的供应商、其出版说明或其他可公开获得的资料中获取。IBM 没有对这些产品进行测试，也无法确认其性能的精确性、兼容性或任何其他关于非 IBM 产品的声明。有关非 IBM 产品性能的问题应当向这些产品的供应商提出。

所有关于 IBM 未来方向或意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

所有 IBM 的价格均是 IBM 当前的建议零售价，可随时更改而不另行通知。经销商的价格可能会有差异。

本信息仅用于规划的目的。在所描述的产品上市之前，此处的信息会有更改。

本信息包含在日常业务操作中使用的数据和报告的示例。为了尽可能完整地说明这些示例，示例中可能会包括个人、公司、品牌和产品的名称。所有这些名称纯属虚构，如与实际商业企业使用的名称及地址雷同，纯属巧合。

版权许可:

本信息包括源语言形式的样本应用程序，这些样本说明不同操作平台上的编程方法。如果是为按照在编写样本程序的操作平台上的应用程序编程接口 (API) 进行应用程序的开发、使用、经销或分发为目的，您可以任何形式对这些样本程序进行复制、修改、分发，而无须向 IBM 付费。这些示例并未在所有条件下进行完全测试。因此，IBM 不能担保或暗示这些程序的可靠性、可维护性或功能。样本程序“按现状”提供，不附有任何种类的保证。对于因使用样本程序而引起的损害赔偿，IBM 不承担责任。

凡这些样本程序的每份拷贝或其任何部分或任何演绎作品，都必须包括如下版权声明:

如果您是以软拷贝的形式查看本信息，照片和彩色插图可能不会出现。

商标

IBM、IBM 徽标和 ibm.com® 是 International Business Machines Corp. 在全球许多司法区域注册的商标或注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 站点 http://www.ibm.com/legal/copytrade.shtml 上“Copyright and trademark information”部分中提供了 IBM 商标的最新列表。

Adobe、Adobe 徽标、PostScript 和 PostScript 徽标是 Adobe Systems Incorporated 在美国和/或其他国家或地区的注册商标或商标。

IT Infrastructure Library 是 Central Computer and Telecommunications Agency（它现在是 Office of Government Commerce 的一部分）的注册商标。

Intel、Intel 徽标、Intel Inside、Intel Inside 徽标、Intel Centrino、Intel Centrino 徽标、Celeron、Intel Xeon、Intel SpeedStep、Itanium 和 Pentium 是 Intel Corporation 或其子公司在美国和其他国家或地区的商标或注册商标。

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。

Microsoft、Windows、Windows NT 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他国家或地区的商标。

ITIL 是一个注册商标，是 Office of Government Commerce 的共同体注册商标，并且已在 U.S. Patent and Trademark Office 进行注册。

UNIX 是 The Open Group 在美国和其他国家或地区的注册商标。

Java™ 和所有基于 Java 的商标和徽标是 Oracle 和/或其附属公司的商标或注册商标。

Cell Broadband Engine 是 Sony Computer Entertainment, Inc. 在美国和/或其他国家或地区的商标，并根据当地许可进行使用。

Linear Tape-Open、LTO、LTO 徽标、Ultrium 和 Ultrium 徽标是 HP、IBM Corp. 和 Quantum 在美国和其他国家或地区的商标。

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® 和 Sterling Integrator® 是 Sterling Commerce®, Inc., 和 IBM 公司的商标或注册商标。

其他公司、产品和服务名称可能是其他公司的商标或服务标记。

Printed in China