

操作手册

一、产品简介

(一) 基本概念

1. 什么是AS2

AS2 (Applicability Statement 2) 是一种基于互联网的安全数据交换协议，主要用于企业之间的电子数据交换 (EDI)。它定义了一种通过 HTTP 或 HTTPS 传输 EDI 数据的标准方式，并提供了“加密、数字签名和确认回执 (MDN)”等安全机制。

AS2 的关键特性：

- 数据加密：确保数据在传输过程中不会被窃取。
- 数字签名：确保数据来源的真实性，并防止数据被篡改。
- MDN (Message Disposition Notification)：类似于“已读回执”，确保数据正确送达。
- 基于 HTTP/HTTPS：可以利用现有的互联网基础设施进行数据交换，无需专门的专线连接。
- 实时传输：相较于传统的 EDI 传输方式 (如 FTP、VAN)，AS2 更加实时和高效。

AS2 由 IETF (Internet Engineering Task Force) 在 RFC 4130 中定义，并广泛应用于零售、制造、物流、医疗等行业。例如，沃尔玛 (Walmart) 强制供应商使用 AS2 进行 EDI 交易。

2. 什么是EDI

EDI (Electronic Data Interchange, 电子数据交换) 是一种企业间以电子方式交换商业文件的标准，取代了传统的纸质文件传输方式。EDI 允许企业之间以结构化格式 (如 EDIFACT、X12 等) 交换订单、发票、发货通知等信息。

EDI 的关键特性：

- 标准化：EDI 使用标准格式 (如 ANSI X12、EDIFACT) 来确保不同企业之间的系统兼容性。
- 自动化：减少人工干预，提高业务处理效率。
- 减少错误：避免手工输入错误，提高数据准确性。
- 降低成本：减少纸张、邮寄、人工处理的成本。

EDI 的常见应用场景：

- 零售行业：订单（PO）、发票（Invoice）、发货通知（ASN）。
- 制造业：生产计划、库存管理、供应链协作。
- 物流行业：运输单据、货运通知。
- 医疗行业：电子病历、医疗保险报销。

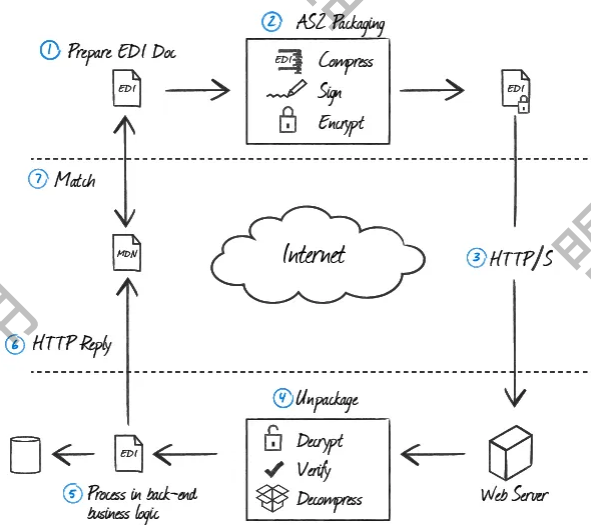
3. AS2 和 EDI 的关系

AS2 只是 EDI 数据交换的一种传输方式，而 EDI 是更广泛的商业数据交换标准。两者的关系可以类比为：

- EDI 是“内容”（即要传输的业务数据，如订单、发票）。
- AS2 是“管道”（即用于传输 EDI 数据的通信协议）。

AS2 在 EDI 传输中的作用：

1. 企业 A 生成 EDI 文件（如使用 ANSI X12 标准的订单 850）。
2. EDI 文件通过 AS2 进行加密、签名，并通过 HTTP/HTTPS 发送给企业 B。
3. 企业 B 接收 AS2 消息，解密、验证签名，确认完整性。
4. 企业 B 解析 EDI 数据，并在 ERP 或 SCM 系统中处理。
5. 企业 B 发送 MDN（回执）确认企业 A 收到数据。



Header Name	AS2 Message	MDN	使用/示例值
AS2-Version	强制性	强制性	1.0 / 1.1 或 1.2

AS2-From	强制性	强制性	发送者的 AS2 标识符
AS-To	强制性	强制性	接收者的 AS2 标识符
Message-Id	强制性	强制性	唯一的消息 ID
Disposition-Notification-To	强制性	N/A	MDN 同步/异步？例如，email@org.com 用于同步或 URL，如 http://org.com/async_mdn 用于异步
Disposition-Notification-Options	强制性	N/A	MDN 选项，例如：signed-receipt-protocol=optional,pkcs7-signature; signed-receipt-micalg=optional,sha1
Receipt-Delivery-Option	可选	N/A	异步 MDN URL，例如 http://org.com/async_mdn
Content-Type	强制性	强制性	依赖于消息 'application/pkcs7-mime' 进行加密，'multipart/signed' 进行签名 AS2 或 MDN
Content-Transfer-Encoding	可选	N/A	usually present with encrypted AS2 messages 通常与加密的 AS2 消息一起出现
Content-Disposition	可选	N/A	通常包含加密的 AS2 消息
MIME-Version	可选	可选	通常为 1.0
Subject	可选	可选	例如，来自 MFT 网关的 AS2 消息（如电子邮件中所述）
From	可选	可选	例如，发件人的电子邮件（如电子邮件中所述）
Date	可选	可选	例如，Thu, 19 Dec 2002 15:03:38 GMT（如电子邮件中所示）
EDIINT-Features	可选	N/A	例如：多个附件或 CEM

4. AS2 和其他 EDI 传输方式的对比

传输方式	传输协议	安全性	传输速度	适用场景
------	------	-----	------	------

AS2	HTTP/HTTPS	高（加密 & 签名）	快（实时）	B2B 电子商务、零售供应链
FTP/SFTP	FTP/SFTP	中（需额外加密）	中	传统 EDI 传输
VAN（增值网络）	专有网络	高	慢（批量传输）	传统 EDI 业务
API (REST/SOAP)	HTTP/HTTPS	高	快	现代 B2B 集成

(二) 产品亮点

“盟接之桥”：让EDI报文传递更简单、更灵活、更安全。还在为复杂的EDI对接头疼吗？传统EDI方案开发周期长、维护成本高、数据格式僵化，而“盟接之桥”正是为解决这些问题而生！我们基于AS2协议，为您提供灵活、高效、安全的EDI报文传递服务，助您轻松打通企业间的数据桥梁。

为什么选择“盟接之桥”？

1. 灵活取数，适配任意业务场景

无论是SQL数据库还是API接口，“盟接之桥”都能轻松对接，按需提取数据，并组装成客户指定的EDI报文格式（如X12、EDIFACT等）。再也不用为不同客户的特殊需求反复开发，一套系统，灵活适配！

2. 基于AS2协议，安全可靠

AS2（Applicability Statement 2）是当前最主流的EDI传输协议之一，支持数据加密、数字签名和MDN回执，确保报文在传输过程中防篡改、防泄露、可追溯。“盟接之桥”完美兼容AS2，让您的数据交换既高效又安全。

3. 降低技术门槛，减少开发成本

传统EDI对接往往需要专业团队长期投入，而“盟接之桥”提供开箱即用的解决方案，大幅减少开发和维护成本。无论是初次接触EDI的新手，还是需要高效扩容的老手，都能快速上手，省时省力。

4. 高稳定性，保障业务连续性

我们深知EDI报文传递对业务的重要性，因此“盟接之桥”采用高可用架构，支持断点续传、自动重试和实时监控，确保每一份报文都能准确送达，避免因网络波动或系统故障导致的业务中断。

适用场景：

- 1) 供应链协同：与供应商、物流商高效交换订单、发货通知、发票等数据。
- 2) 零售电商：快速对接各大平台，自动化处理订单、库存、结算信息。
- 3) 金融服务：安全传输对账、支付指令等敏感数据，符合行业合规要求。

二、帮助手册

(一) 证书管理

1. 证书定义

在 AS2 (Applicability Statement 2) 协议中，证书的“签名”和“加解密”是两个不同的安全功能，分别用于保证消息的完整性（[防篡改](#)）和机密性（[防窃听](#)）。

以下是对这两个概念的详细解析：

(一) 签名

通常使用发送方的[私钥证书](#)对数据进行签名，以确保发送方作为文件创建者的身份（通常使用 SHA-1 签名算法）。

1. 为什么签名需要私钥？

数字签名的核心目的是证明数据的完整性和发送方的身份。以下是签名过程的工作原理：

签名生成：

- 1) 发送方（你）用自己的私钥对数据进行签名。
- 2) 签名的本质是用私钥加密一个基于数据计算出的哈希值（例如 SHA-256 哈希值）。这个过程确保只有你（持有私钥的一方）能够生成有效的签名。

签名验证：

- 1) 接收方（交易伙伴）使用你的公钥来验证签名。
- 2) 验证的过程是检查签名是否与数据匹配，并确认签名是由你的私钥生成的。

因此，签名需要私钥的原因是：只有私钥的持有者才能生成有效的签名，而任何人都可以使用公钥来验证签名的真实性。

2. 私钥的安全性如何保证？

虽然签名过程中确实使用了私钥，但请注意以下几点：

- 1) 私钥仅用于签名：在 AS2 协议中，私钥仅用于生成签名，而不会被共享或传输给任何第三方（包括交易伙伴）。交易伙伴只需要你的公钥证书（从 `.pem` 文件中提取的部分）来验证签名，而不是你的私钥。
- 2) 私钥存储安全：私钥应存储在安全的地方，例如服务器上的受保护文件系统、硬件安全模块（HSM）或密钥管理服务（KMS）。私钥不应该硬编码到代码中，也不应该暴露给未经授权的人员。
- 3) 签名和加密分离：签名使用的是你自己的私钥，而加密使用的是交易伙伴的公钥。这意味着，即使攻击者获得了交易伙伴的公钥，他们也无法伪造你的签名，因为只有你持有私钥。

（二）加密

通常使用接收方(Company A)的**公钥证书**进行加密（使用 3DES 加密算法），因此只有正确的接收方才能解密文件。AS2 使用安全/多用途网络邮件扩展 (S/MIME) 协议将邮件包装在安全信封中。

这是一个很好的问题！让我来详细解释一下为什么在签名过程中需要使用私钥，以及为什么这并不违反安全性原则。

2. 证书格式

证书格式	特点	用途
pfx、p12	包含证书和私钥，有密码保护	服务器和客户端软件证书配置
p7b	通常只含证书链，无私钥，Base64 编码	传输证书链或存储证书集合
pem、crt、cer	文本形式，可包含证书、私钥或 CSR，可编辑	开源软件和命令行工具
jks	由 Java 的 <code>keytool</code> 管理，专门用于 Java 应用程序。既可以存储证书，也可以存储私钥。需要密码保护。	

3. 证书合成

“盟接之桥”使用到的证书格式为P12。因此，首先需要合成P12证书。合成方法是用OpenSSL工具，如下是合成命令：

合成P12证书

Plain Text

```
1 openssl pkcs12 -export \  
2 -out acig.bocady.com.p12 \  
3 -inkey acig_bocady_com.key \  
4 -in acig_bocady_com_integrated.pem \  
5 -name "takstar_hp_cer" \  
6 -password pass:prod
```

命令行解释：

- `-export` 表示你要创建一个 PKCS#12 文件。
- `-out acig.bocady.com.p12` 指定输出文件名，在此例中为 `acig.bocady.com.p12`。
- `-inkey acig_bocady_com.key` 是指定你的私钥文件的位置和名称。
- `-in acig_bocady_com_integrated.pem` 是你的证书文件的位置和名称。
- `-name` 是你合成证书的别名。
- `-password` 是你合成证书的密码。

(二) 操作指南

1. 系统登录

系统部署之后，在浏览器中输入：<http://localhost:12315/login?redirect=%2Findex>。备注：地址以实际的部署地址为准。



登录成功后，进入首页，如下所示：



2. 环境配置

环境配置主要是初始化证书以及AS2的配置信息，操作界面如下：

环境配置

环境信息

环境 dev

证书信息

证书地址

证书名称 testaciq.bocady.com

证书密码 bocady

AS2信息

Owner AS2 Id TakstarThailand_QA

Owner AS2 Name TakstarThailand

AS2 Id PSEumoriBTP_QA

AS2 Name Parther

AS2 URL https://shpiq.8-cpi003-rt.cfapps.us10.hana.ondemand.com:443/as2/as2

AS2 Subject Master Data from Takstar Thailand

AS2 sign SHA256

AS2 encrypt AES256

AS2 retries 5

连接状态 测试

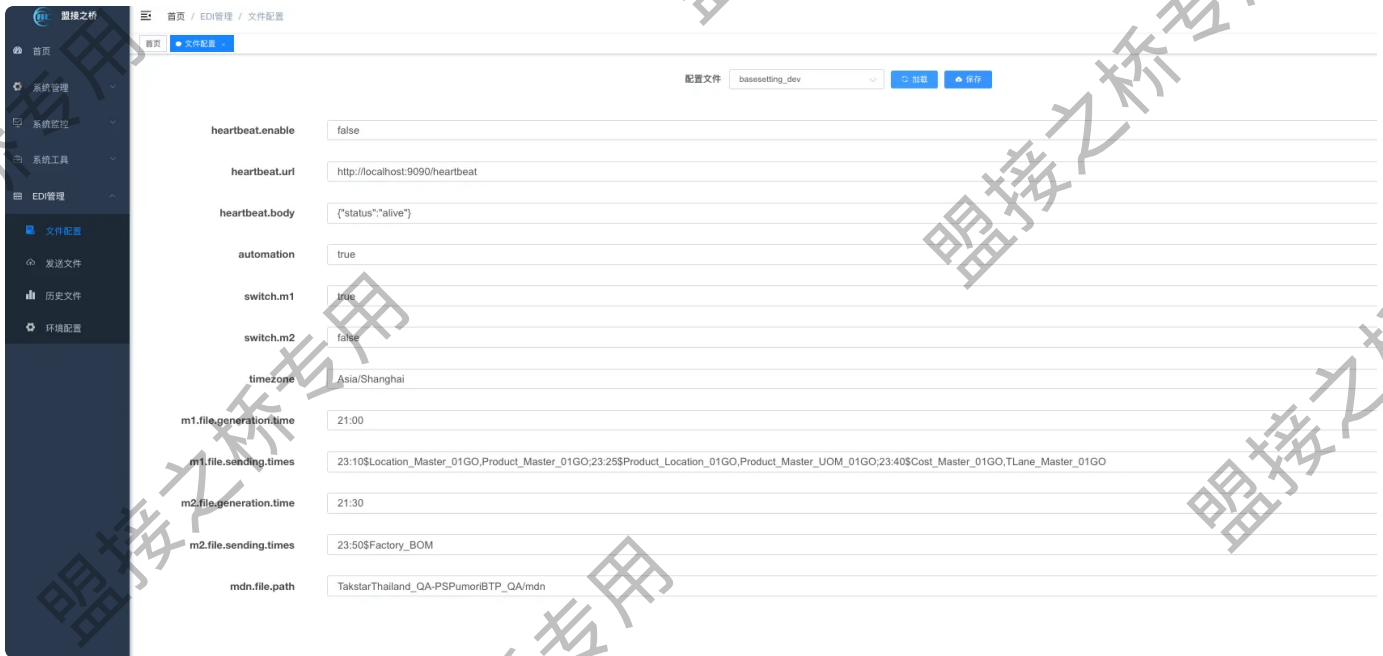
保存

详细描述：

- 环境：有2个选项（dev, prod），分别代表开发环境和生产环境。
- 证书地址：这个就是需要将2.1.3章节准备好的P12证书上传到系统的证书库，系统会自动读取证书库的证书文件。
- 证书名称：这里自动生成上传证书的名称。
- 证书密码：这里就是合成证书的时候填写的密码。
- Owner AS2 Id：这个代表发送方的AS2 Id。
- Owner AS2 Name：这个代表发送方的AS2名称。
- AS2 Id：这个代表交易伙伴的AS2 Id。
- AS2 Name：这个代表交易伙伴的AS2名称。
- AS2 URL：这个代表交易伙伴的AS2地址，EDI报文就是推送到这个地址。
- AS2 Subject：这个表示主题，作用就是区分推送过来的报文来自哪里。
- AS2 sign：这个表示签名算法，常用的有：SHA256，SHA128等。
- AS2 encrypt：这个表示加密算法，常用的有：AES256，3DES等。
- AS2 retries：这个表示重试次数。如果推送失败，可以再次推送。

3. 配置文件

这个配置文件的作用是业务配置，比如：取数、定时发送设置。操作界面如下：



配置项	值
heartbeat.enable	false
heartbeat.url	http://localhost:9090/heartbeat
heartbeat.body	{"status": "alive"}
automation	true
switch.m1	true
switch.m2	false
timezone	Asia/Shanghai
m1.file.generation.time	21:00
m1.file.sending.times	23:10\$Location_Master_01GO,Product_Master_01GO;23:25\$Product_Location_01GO,Product_Master_UOM_01GO;23:40\$Cost_Master_01GO,TLane_Master_01GO
m2.file.generation.time	21:30
m2.file.sending.times	23:50\$Factory_BOM
mdn.file.path	TakstarThailand_QA-PSPumoriBTP_QA/mdn

配置界面一

详细描述：

- heartbeat.enable：是否启用健康检查。
- heartbeat.url：健康检查监控端地址。
- heartbeat.body：健康检查发送报文。
- automation：是否启用自动取数。
- switch.m1：M1业务是否开启（备注：根据具体实际业务）
- switch.m2：M2业务是否开启（备注：根据具体实际业务）
- timezone：时区
- m1.file.generation.time：M1业务文件自动生成时间（备注：根据实际业务）
- m1.file.sending.times：M1业务文件自动发送时间（备注：根据实际业务）
- m2.file.generation.time：M2业务文件自动生成时间（备注：根据实际业务）
- m2.file.sending.times：M2业务自动发送时间（备注：根据实际业务）
- mdn.file.path：MDN文件生成文件路径（相对路径）

配置文件: testsetting_dev

加载 保存

m1.file.generation.time	21:00
m1.file.sending.times	23:10\$Location_Master_01GO,Product_Master_01GO;23:25\$Product_Location_01GO,Product_Master_UOM_01GO;23:40\$Cost_Master_01GO,TLane_Master_01GO
m2.file.generation.time	21:30
m2.file.sending.times	23:50\$Factory_BOM
mdn.file.path	...
mail.host	smtp.exmail.qq.com
mail.port	465
mail.attach.enable	false
mail.subject	...
mail.username	...
mail.password	...
mail.to	...

配置界面二（上接配置界面一）

详细描述：

- mail.host：邮件服务器
- mail.port：邮件服务器端口
- mail.attach.enable：是否包含附件
- mail.subject：邮件主题
- mail.username：发件人
- mail.password：发件人密码
- mail.to：收件人

4. 发送文件

这里是实时发送的功能，主要是发送文件，界面如下：



功能描述：这里主要是发送EDI文件的，如果有提前准备好的文件并且需要实时发送，可以在这里操作。

5. 历史文件

文件发送完成后，可以查询发送历史，界面如下：



文件发送列表根据时间查询，并且支持文件下载。