AS2 file transfer for EDI - practical implementation guide

IN THIS ARTICLE:

SOLVEDI

www.solvedi.eu

Author: Wojtek Kazimierczak

2023-12-12

AS2 server: Which Option to Choose and How to Implement It?

This article discusses EDIINT AS2 (Applicability Statement 2) protocol from practical point of view. It is designed for managers and specialists responsible for implementing EDI, particularly those without prior experience with this protocol. A comprehensive understanding of AS2 will help to select the right approach and ease the process of choosing the software package or an EDI service provider.

1. What is AS2?

AS2 is a protocol designed for the secure transfer of data files over the Internet.

Main features:

- Data is encrypted and signed, ensuring clear identification of the sender and recipient while preventing unauthorized viewing and modification of data during transport.
- The server receiving data automatically sends a receipt confirmation (MDN) to the sender.

This second feature distinguishes AS2 from other file transfer methods, making it an ideal protocol for the transfer of electronic business documents between trading partners (EDI). MDNs allow for a clear **identification of responsibilities** and can serve as **legal proof** that a given organization received a document with specific content (e.g., an order for goods at a specific price).

Due to its cost-effectiveness, the AS2 protocol has almost completely replaced the previously used X.400 protocol, especially given that the fee for the X.400 protocol was often related to the amount of data transferred.

2. Self-Managed AS2 Server or Managed EDI Service?

Before choosing an implementation method, it is important to consider that a self-managed AS2 server may not be the best choice for everyone. This is because EDI requires an upfront generation of the documents (data files) in a specific format. I have already discussed this topic in detail in the article: How to Implement EDI - Practical Tips.

For this reason most of the companies opt for a service of a specialized EDI service provider, encompassing both **translation** and **transport**. With large-scale operations, an EDI service provider is able to offer a more favorable price for an AS2 link, as it may be shared by multiple customers. Nevertheless, this is not always true, so it’s important to carefully analyze and compare different offers.

The other option: self-managed AS2 server is less common. It represents approximately 10% of the partners we have collaborated with. This option is typically considered by two distinct groups:

1. Large corporations that possess the necessary skills and resources for integrating IT systems. Their objective is to establish a competitive edge by seamlessly integrating their IT systems with partners.
2. Medium-sized companies with a small number of partners that have fairly good IT support that can handle the setup of translation and transport software on their own, saving them from recurring expenses.

3. Choice of AS2 Software

When considering a self-managed AS2 server, two options are available:

1. **On-Premise**: This involves installing the software in your own IT environment.

- Generally higher setup cost, but lower maintenance cost.
- Server requires typical day-to-day administration (availability, security).
- Static IP address is required.

2. **Cloud AS2**: This option utilizes AS2 software provided as a service.

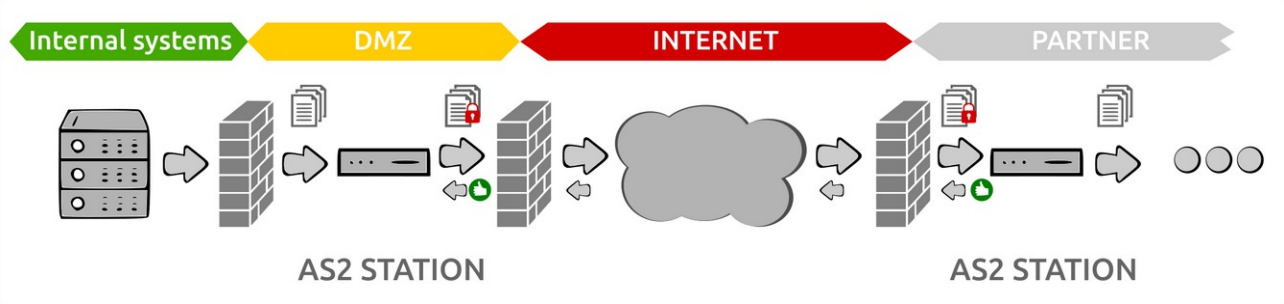
- No upfront costs, but there is a monthly fee, which can be quite significant and may dependent on the amount of data transferred.
- The service provider is responsible for the day-to-day administration.

In both cases, adding new partners should be done in-house, so it requires an understanding of how the AS2 protocol works (I explain it later in this article). Smaller organizations can use external consultants to setup the environment and add new partners, and then take over the day-to-day administration by internal IT team.

Before making any decisions, it is always a good idea to evaluate the features of the existing data and application integration software. Many Managed File Transfer (MFT) or Enterprise Service Bus (ESB) packages offer support for AS2. Otherwise, you can use free software under an Open Source license - some examples are provided in the footnotes[1].

4. AS2 in Practice

In order to send and receive documents through AS2, both parties need to continuously maintain a server, often referred to as an “AS2 station”. Each station is identified by a unique name, known as the AS2 ID. To limit security risks, such a server is most often placed behind a firewall, in the DMZ (demilitarized zone), to limit access to authorized partners only.



1 There are several AS2 servers that are available on an Open Source license. One of the most mature and popular ones, based on my experience, is Mendelson AS2. It offers two types of licenses: community and commercial. Other options include Java-based OpenAS2, or django-pyas2, which is written in Python. Apache Camel framework has also a component supporting AS2.

Without going into too much detail, sending of a document via AS2 may look like following:

- The internal ERP system sends to the AS2 station a file designated for a specific partner (company). If the ERP system is not able to use the format expected on the other side (for example EDIFACT), an additional translating software do the conversion before the file is received by AS2 station.
- The AS2 server encrypts and signs the file, ensuring it can only be deciphered by the intended partner.
- The encrypted file is transmitted to the partner through the Internet.
- The receiving AS2 server authenticates the sender using his public certificate and document's digital signature, then it decrypts the file.
- Upon successful completion of the process, the recipient's AS2 server sends back to the sender a file with an acknowledgment of receipt (MDN).

The MDN may also be "negative," for example when the file is received, but the sender's authenticity cannot be confirmed due to an expired certificate. A transmission with negative MDN should be considered as failed, so the file should be resend when the issue is solved.

For further details on the AS2 protocol, you can refer to the RFC 4130[2] standard. It's worth noting that the approved standard encompasses AS2 versions 1.0 and 1.1. There's also a draft of version 1.2 and several extensions[3], though none of those proposals had received an official approval.

Speaking of different versions: there is a whole family of protocols collectively called EDIINT (Electronic Data Interchange - Internet Integration). In addition to the most popular AS2 protocol (transport via HTTP/HTTPS), there are also: AS1 (email) and AS3 (FTP). The newest one - AS4 - is based on web services.

5. AS2 Certificates Management

While comprehensive information about how public key cryptography works is readily available (see footnote[4] for my recommended reading), let's focus on practical guidelines related to AS2:

- Most commonly self-generated X.509 certificates are used.
- The validity period is usually set between 2 to 5 years. A longer validity period minimizes disruptive changes for partners. If necessary (private key compromised), the certificate can be simply replaced with a new one.
- A certificate with a public key should be sent to the partner alongside the AS2 configuration (details explained below).

2 The AS2 standard is described in RFC 4130.

3 One of such AS2 features (extentions) is CEM, which facilitates the updates of certificates. It has been describedd in the (now expired) IETF draft Certificate Exchange Messaging for EDIINT.

4 For those who want to further understand how AS2 works and learn best practices, I especially recommend a series of three great articles by Todd Gould, published by Loren Data: ① **AS2: What Is It**, ② **AS2: Best Practices**, ③ **AS2: Certificates**.

- The same set of keys is utilized for both encryption and signing.
- If HTTPS is employed (although not mandatory, as it implies double encryption), the SSL certificate associated with the URL should be procured from one of the widely accepted certificate providers (CA). This eliminates the need for partners to update it.

I must admit that while AS2 administration isn't problematic, renewing certificates with multiple partners is a challenge. Therefore, this operation require careful planning and precise communication. Just picture the scenario where (lets say) 100 individuals need to update certificates simultaneously, with AS2 support being just a side task for most of them.

Procedure for Changing Your Own Certificate:

- Set the date of certificate renewal at least two weeks before its expiry, to ley yourself a reserve in case of unexpected situations. Opt for a business day, preferably around noon.
- Inform your partners at least one month before the selected renewal date. Send an email containing the new certificate and the following information:
    - Date, time, and time zone of the planned renewal.
    - Clarification that the old certificate will cease to function after this date.
    - Details of the AS2 ID and URL affected by the change.
    - Serial numbers of both the old and new certificates.
    - Request to acknowledge or forward your email to the right person.
    - Tip: Don't use the expiry date of the old certificate in your communication, as it may be confused with the date of the certificate renewal.

One more thing: it's crucial to maintain an up-to-date list of email addresses of AS2 administrators on the partner side.

6. AS2 Server Setup and Documentation - Best Practices

Setting up AS2 can be a challenging task, especially for those without prior experience. It is somehow similar to an IPSec VPN setup, where many parameters should be set the same way on both sides. The following tips are aimed at making the process smoother.

Base configuration parameters:

- **AS2 station URL and port**: For example, http://example.com:8080/as2.
    - The AS2 standard does not specify the TCP port to be used for communication. Commonly used ports include 80, 8080, 4080, or for HTTPS (with SSL): 443, 8443. However, in practice, the port number unfortunately may differ for each partner, requiring firewall adjustments.
    - HTTP protocol is sufficient, as the transmitted data are already encrypted by AS2 protocol. Some partners may require HTTPS anyway.

    - The URL should be supplemented, if necessary, with a list of public IP addresses, expected to send and receive (for firewall configuration).
- **AS2 ID**: a unique server name, composed of up to 128 printable ASCII characters, excluding quotation marks and backslashes, case sensitive. Hints:
    - Typically, names are written in capital letters and include an abbreviation of the company name or contain company's GLN number.
    - The AS2 identifier determines which certificate is to be used in communication with the partner.
    - Assign a unique AS2 ID to each link, such as COMPANY-TEST or COMPANY-PROD, to facilitate the segregation of messages for different environments. This approach eliminates the necessity of inspecting the message content to determine the destination system.
- **AS2 certificate**: use meaningful file name and send as zipped attachment or provide a download link, to avoid some restrictive email servers.
- **Encryption algorithm**: for example, 3DES.
- **Signing algorithm** (message and MDN): for instance, SHA-256 (note: if possible, SHA-1 should no longer be used).
- **MDN type**: synchronous or asynchronous (doesn't matter, change to the other in case of issues).

Additional Parameters and Commonly Used Values:

- **Message Encryption**: yes.
- **Message Signature**: yes.
- **MDN Required**: yes.
- **MDN Signature**: yes.
- **Compression**: no.
- **Content Transfer Encoding**: binary or base64; usually doesn't matter, unless requested by the partner.
- **Payload Content Type**: doesn't matter, leave the default of your application (example: "application/EDIFACT").
- **Delivery Retry**: yes, 3 attempts (depending on your software).

It is recommended to establish two separate AS2 links, one for testing purposes and one for production. This approach will prevent sending trucks full of goods due to accidental test messages being sent to the production system.

All parameters should be summarized in the form of a clear table, saved as a PDF and sent along with the certificate to the partner, before initiating the configuration. Below is an example of such documentation, as found of the web page of an EDI provider[5]:

5 Babelway: AS2 specification example.

AS2 Specification

Environment	account of jeff_demo / Environment 1
Identity	BABELWAY_AS2_29329
Sending protocol	HTTP
Receiving protocol	HTTP
HTTP AS2 URL	http://us1.babelway.net/corvus/httpd/as2/inbound
List of potential listening IP (for firewall configuration)	52.5.32.55 52.5.32.186
Listening port	80
List of potential sending IP (for firewall configuration)	52.5.32.55 52.5.32.186
Endpoint type	All purposes
Receipt Type	MDN
Receipt Signature Type	SHA1
Delivery Mode	Synchronous or Asynchronous
Data compression	None
Signing Algorithm	SHA1
Encryption Algorithm	3DES
AS2 certificate	See attached file as2.babelway_legacy.crt
AS2 certificate chain	See attached files : root.babelway_legacy.crt
Bundled certificate & Certificate Authority	See attached file as2.babelway_legacy.p7b

Frequently, AS2 specifications that you'll receive may not explicitly define certain parameters and use different names (above: "Identity" means "AS2 ID"). Additionally, some partners will specify all possible values supported by their software for a given parameter, such as "Encryption algorithm: 3DES, RC2, AES-128, AES-192, AES-256". In such cases, you may propose one specific value for each parameter, to prevent any confusion.

7. Setting Up and Testing the Connection

In the best circumstances, setting up an AS2 connection can be done in under an hour. However, in practice, all agreements and tests usually take about a week. We've seen some instances where it has taken several weeks to do the setup, but those should be considered extreme cases.

Common challenges are mostly related to communication and coordination. Typical issues include errors in the URL or port, incorrect firewall configuration, incorrect certificate, typos in AS2 ID names, or differences in the configuration of both stations. As always, accurate documentation and precise communication are crucial.

AS2 Link Setup Steps

1. Both parties exchange their AS2 documentation and public certificates and agree on common AS2 parameters.
2. After finishing the setup, make a simple test: send any file (like a text document), separately in both directions, and check if a positive MDN is received.
3. In case of issues, conduct comprehensive diagnostics, starting from double-checking the configuration and certificate serial numbers, reviewing firewall configurations, and, if necessary, continue with a detailed analysis of the network traffic.
4. Upon successful completion of the test, the link is ready for sending the real EDI documents.

8. After Go-Live: AS2 Server Administration

Ongoing supervision involves:

- Automated monitoring that the server is running.
- Periodic updates of certificates, as described above.
- Reaction to any alerts, such as negative/missing MDNs. These alerts can be managed by the person responsible for the overall EDI supervision.

Summary

As you can see from the length of this article, implementing AS2 communications requires some effort. The positive aspect is that once the link is established, it rarely causes any issues.

➽ Original article: https://www.solvedi.eu/blog/as2-implementation/