TECHNICAL WHITE PAPER

COVAST AS2 ADAPTER
FOR
MICROSOFT BIZTALK SERVER 2004

MAY 2004

TABLE OF CONTENTS

INTRODUCTION

Historically, EDI (Electronic Data Interchange) transactions and other business documents have been exchanged using VANs (Value Added Networks) and various types of bilateral connections (leased lines and dial-up).

The main reason for exchanging documents using VANs and bilateral connections is that they guarantee certain agreed upon service levels. This means that the following things are guaranteed:

- Documents are always delivered (Guaranteed delivery);
- Documents are delivered on time (On time delivery);
- Documents cannot be disputed (Non-repudiation);
- Senders and Recipients are always known (Authentication).

Exchanging documents in this manner has one major disadvantage. The cost per transaction is quite high. This is because VANs charge not only a monthly fee, but also a per transaction fee. Leased lines and dial-up connections are expensive to setup and maintain as well.

Since the Internet has become available to almost everybody in the past decade, several efforts have been made to use Internet standard protocols to exchange those valuable business documents. They all failed.

Reasons for the failures were:

- The SMTP based protocols have no means to guarantee delivery;
- Messages sent via the Internet are easily intercepted and compromised;
- Because of the Internet's "anarchy model" nobody can prove authentication.

The Internet Engineering Task Force (IETF) has approved a standard for exchanging documents reliably using the Internet HTTP protocol. It guarantees all things provided by the traditional VANs and it is very cost effective because it uses the widely available Internet as its foundation. This standard is called AS2, which stands for Applicability Statement 2.

In order to certify compliance to the AS2 standard, the Drummond Group (www.drummondgroup.com) has been appointed to certify vendor's AS2 products.

Covast is working with Microsoft to provide certified AS2 technology as an adapter within their BizTalk Server product.

This product is called the "Covast AS2 Adapter for Microsoft BizTalk Server" and is described in more detail in this white paper. The Covast AS2 Adapter for Microsoft BizTalk Server is a fully integrated BizTalk Server adapter that has been certified by the Drummond Group.

The Covast AS2 Adapter is also available as the AS2 Adapter for EDI Accelerator.

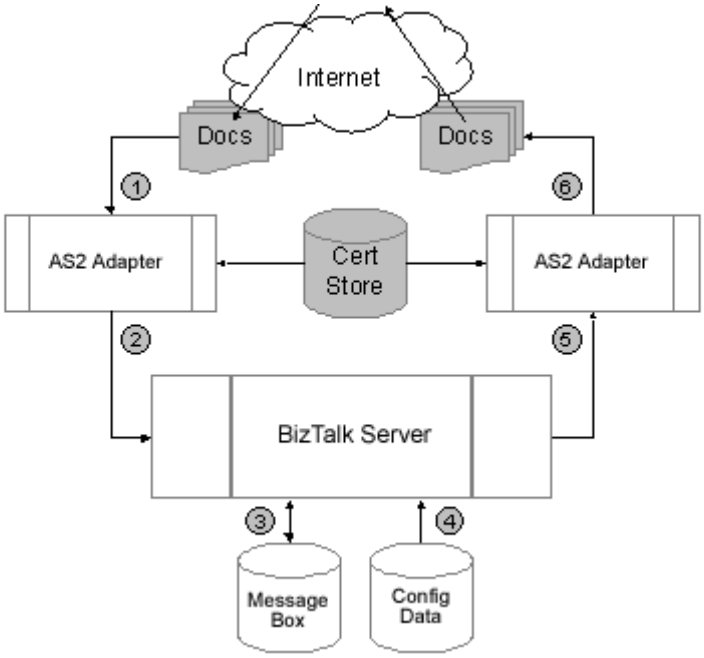
AS2 ADAPTER ARCHITECTURE

The Covast AS2 Adapter for Microsoft BizTalk Server has been implemented as a BizTalk Adapter.

The outbound AS2 traffic is handled by allocating the AS2 Adapter as a transport on any Send Port defined in Visual Studio in the BizTalk Explorer. This provides the signing, encrypting, compressing and sending of outbound messages to the AS2 recipient.

Inbound AS2 traffic is managed by a Windows 2000 \ 2003 Service that can handle multiple AS2 connections at a time. This Service is responsible for checking the digital signatures of the senders, decrypting, decompressing and submitting the received messages through a receive port / pipeline to the BizTalk Server Message Box for further processing. The Adapter also takes care of handling the Message Disposition Notifications (MDNs) to be sent back to the originator of the messages and correlation of received MDN's.

Figure 1: Schematic overview of the AS2 Adapter



1. The AS2 Service receives inbound documents and checks the sender signatures by using the appropriate certificates. These certificates have been stored upfront (the AS2 protocol does not exchange certificates in the HTTP session like with HTTPs). Then it decrypts and decompresses the documents. On failure the documents are rejected and the error is reported in Health and Activity Tracking (HAT) and the error information ends up in the Windows event log.
   When the document is successfully received and decrypted, the AS2 service will create and send back AS2 MDNs (Message Disposition Notification) to the originator of the documents;
2. The AS2 Adapter submits the inbound plain documents through the receive pipeline the Message Box.
3. The document is stored in the Message Box. From here any subscription for this document or Receive Location can consume the document for further processing;

4. When documents are destined for a trading partner that uses the AS2 protocol, the Send Port will retrieve the configuration data concerning the sender and recipient and pass that to the AS2 Transport Adapter;
5. The AS2 Transport Adapter will compress, encrypt and sign the documents and send them to the remote party according to the configuration defined;
6. On successful receipt, decryption and authentication, the remote party will send AS2 MDNs. On receipt of the MDNs the status in the BizTalk Tracking database will be updated. This status will be refelected in HAT as well.

MANAGING AS2 RELATED TRADING PARTNER INFORMATION

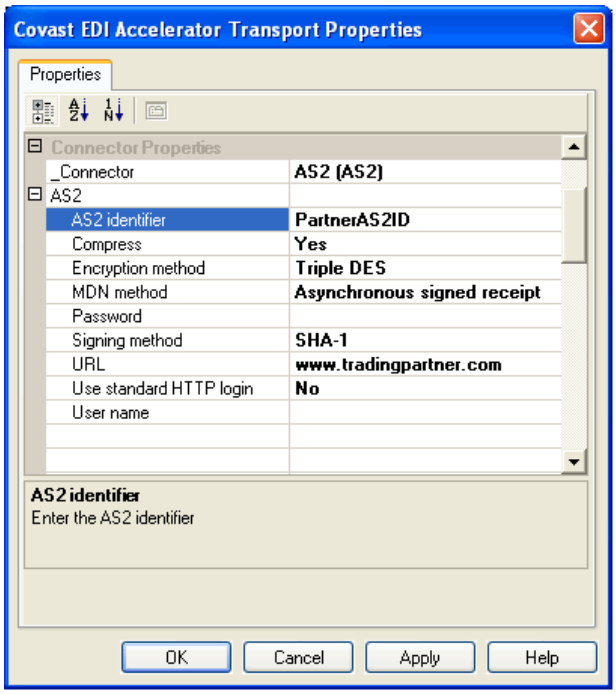
Communicating with a Trading Partner that uses the AS2 protocol needs about the same amount of configuration information as would communicating with a partner that uses HTTP/S to exchange S/MIME wrapped documents.

On the inbound, the AS2 Service needs only to be configured once during installation of the AS2 Adapter for BizTalk Server. Here you only need to specify details about which HTTP port should be used and some AS2 specific details about your own organization.

In order to be able to send information to an AS2 partner, you need to specify a destination URL (Uniform Resource Locator), the digital certificate of the recipient (your business partner) and some options with regard to signing, encrypting and compression of documents.

Configuration of AS2 partner details is accomplished on the Send Port.

Figure 2: AS2 Trading Partner Configuration



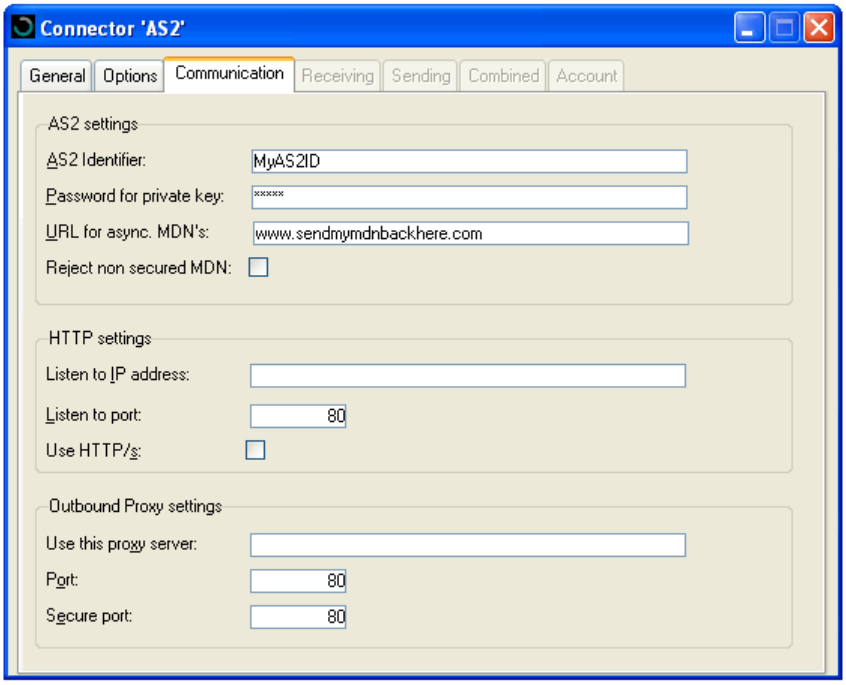
Configuration properties are:

- URL – This is the destination URL where the AS2 Adapter sends the messages to.
- AS2 Identifier – This is the identification by which this Trading Partner is identified in the AS2 community.
- Signing method – AS2 knows 3 different ways of signing: No signing, SHA-1 and MD5.
- Encryption method – AS2 knows 4 different ways of encryption: No encryption, Triple DES, RC2 40 and RC2 128.

- MDN Method – The AS2 Adapter is capable of handling 3 different types of Message Disposition Notifications: No receipt, Plain receipt and Signed receipt.
- Compress – It is possible to have messages compressed before sending them.

In addition to the Trading Partner information, it is also necessary to configure your company's details with regard to the AS2 adapter. This can be done during installation of the AS2 Adapter, but can also be altered at a later time.

Figure 3: Configuring the AS2 Adapter



The settings configured here will be used for incoming AS2 sessions and contain:

- AS2 Identifier – Your company's AS2 identifier.
- Private key password – The password needed to access your private key.
- URL for asynchronous MDNs – Your company's URL where asynchronous Message Disposition Notifications should be sent to.
- Listen to IP address – This enables the AS2 Adapter to listen for inbound AS2 requests on a Virtual IP number, thus enabling Network Load Balancing.
- Listen to port – The HTTP port on which the AS2 adapter will listen for incoming calls.
- Use this proxy server – The (optional) proxy server via which outbound HTTP sessions will be set up.
- Port – The port on the proxy server to be used for HTTP connections.
- Secure port – The port on the proxy server to be used for HTTP/S connections.

MANAGING CERTIFICATES

Certificates can be imported in the Windows Certificate store and be exported from there to the appropriate format for the AS2 adapter. The AS2 protocol is based on the Public Key Infrastructure (PKI) and heavily relies on Digital Certificates.

In an AS2 configuration a couple of items are needed concerning certificates:

- Your own certificate. This can be from a “Certificate Authority” (like Verisign) but with AS2 it is also allowed to use “self signed” certificates (self generated certificates, there are different tools available for this). Between trading partners there should be agreements on the type of certificates used.
- A Certificate can contain a private key; The private key is your own key from which your certificate for signatures and your public key is derived. You always keep your private key yourself.
- A public key. The public key is exchanged with your trading partners. The public key is used to encrypt messages sent to you and for authentication by your trading partner.

In order to be able to exchange messages between your company and one trading partner using the AS2 protocol, you need at least two digital certificates: 1 for your own company and 1 for your partner issued to them. The AS2 standard allows for self-signed certificates as well, that’s why the “issued to” can be equal to the “issued by”. A higher level of security can be reached when the certificates are issued by one of the well-known Certificate Authorities.

The friendly name of the certificates is used as the AS2 Identifier referred to in the previous chapter. Using the AS2 Identifier, the AS2 Adapter can retrieve the appropriate certificates from the certificate store and sign and encrypt the outbound documents according to the settings.

MANAGING OPERATIONS

The Covast AS2 Adapter for Microsoft BizTalk Server is implemented as a BizTalk Server adapter. It is not only from a configuration point of view fully integrated into BizTalk Server, but also from an operational point of view.

The AS2 Adapter fully relies on the BizTalk Messaging foundation, i.e. using the BizTalk Management databases to store configuration information and the Tracking database to keep track of the inbound and outbound traffic.

As soon as errors occur, they will be recorded in the Tracking database and errors will be visible in Health and Activity Tracking. Besides that, error are written in the Windows event log, where they also could be monitored MOM or by operators themselves.

SUMMARY

Exchanging EDI (Electronic Data Interchange) and XML documents reliably via the cost effective Internet instead of via the expensive Value Added Networks (VANs) *and* providing all the service levels traditionally guaranteed by the VANs can today be done by using the AS2 standard.

The Covast AS2 Adapter for Microsoft BizTalk Server is a fully integrated BizTalk Server adapter that has been certified every year by the Drummond group. This provides users the ability to exchange documents with business partners using the AS2 standard seamlessly.

Managing your business partners that exchange documents with you using the AS2 standard protocol requires exactly the same effort as managing all your other partners that connect to you through BizTalk Server. This is made possible by using the same Messaging Manager user interface you, as a BizTalk Server user are already accustomed to.

Implementing the AS2 protocol has never been so easy!

CONTACT INFORMATION

North American Headquarters

Covast
3340 Peachtree Road, NE
Tower Place, Suite 2280
Atlanta, Georgia 30326
USA

Tel: 1.866.COVAST1 or +1 404.812.7150
Fax: +1 404.812.7155

European Headquarters

Covast
Rivium Quadrant 151
2909 LC Capelle a.d. lJssel
P.O. Box 8738
3009 AS Rotterdam
The Netherlands

Tel: +31 10.235.10.22
Fax: +31 10.288.92.47

E-mail

info@covast.com

URL

http://www.covast.com