IBM Software Group

2006 B2B Customer Conference

B2B – Catch the Next Wave

C8: Using Applicability Statement (AS) within WPG

Rayne Anderson

WebSphere. software

ON DEMAND BUSINESS

Objectives

- Applicability Statement overview
  - Describe the background to Applicability Statement (AS)
  - What AS provides
  - Basic message flow and AS message structure
- AS within WPG
  - Features
  - Configuration (AS2)

Applicability Statement Background

- Defined by the Internet Engineering Task Force (IETF) EDIINT Work Group.
- A protocol to enable Electronic Data Interchange (EDI) over the Internet while maintaining a service level equivalent to the existing EDI exchanges over Value Added Networks (VAN).
- Objective was to profit from the advantages of Internet technologies without any negative impact on the installed EDI user base.
- VANs ensure the confidentiality, integrity and non-repudiation of the exchanged information as well as the authentication of the partners. Multiple technologies providing these functions for the Internet existed already and the approach of the EDIINT project was to evaluate these and to provide an integrated solution for the user community.
- The EDIINT protocols define an envelope for information to be transmitted over the Internet (or TCP-IP based networks) using HTTP, which is the foundation for the World Wide Web (WWW), SMTP, which is the common Internet mail protocol or FTP, File Transfer Protocol.

Applicability Statement Provides

- A standard for secure transmission of documents over SMTP (AS1), HTTP (AS2), FTP (AS3).
  - Provides a packaging wrapper for the payload document.
  - Documents can be EDI, XML, flat file, binary.
- A standard receipt protocol for non-repudiation.
  - A Message Disposition Notification (MDN) is used for the receipt.
  - The receipt is not specific to the payload.

Terminology

- Receipt - The functional message that is sent from a receiver to a sender to acknowledge receipt of an EDI/EC interchange. This message may be either synchronous or asynchronous in nature.
- Signed Receipt - A receipt with a digital signature.
- Synchronous Receipt - A receipt returned to the sender during the same HTTP session as the sender's original message.
- Asynchronous Receipt - A receipt returned to the sender on a different communication session than the sender's original message session.
- Message Disposition Notification (MDN) - The Internet messaging format used to convey a receipt. This term is used interchangeably with receipt. A MDN is a receipt.
- Non-repudiation of receipt (NRR) - A "legal event" that occurs when the original sender of an EDI/EC interchange has verified the signed receipt coming back from the receiver. NRR IS NOT a functional or a technical message.

Secure Transmission Loop

In the "secure transmission loop" for EDI/EC, one organization sends a signed and encrypted EDI/EC interchange to another organization and requests a signed receipt, and later the receiving organization sends this signed receipt back to the sending organization. In other words, the following transpires:

- The organization sending EDI/EC data signs and encrypts the data using S/MIME. In addition, the message will request that a signed receipt be returned to the sender. To support NRR, the original sender retains records of the message, message-ID, and digest (MIC) value.
- The receiving organization decrypts the message and verifies the signature, resulting in verified integrity of the data and authenticity of the sender.
- The receiving organization then returns a signed receipt to the sending organization in the form of a signed message disposition notification. This signed receipt will contain the hash of the received message, allowing the original sender to have evidence that the received message was authenticated and/or decrypted properly by the receiver.

AS Packaging Options

- Payload only (no encryption, signing, or payload compression).
- Payload only with compression (no encryption or signing).
- Sign and then payload compression.
- Payload compression and then sign.
- Encryption - on any of the above.
- Request MDN – on any of the above, which can be signed or unsigned, synchronous or asynchronous.

WPG Features

- AS messaging coming into WPG from partner
  - Unpackaging - Decryption, signature verification, decompression.
  - Business id resolution to defined partners.
  - Receipt (MDN) reply.
  - Non-repudiation – storage of the received documents.
- AS message going out of WPG to partner
  - Packaging – Encryption, signing, compression.
  - Retries when receipt not received.
- AS Document Viewer
  - Similar to the Document Viewer but specific to AS documents.
  - Can see the related MDN and status as relates to a document.

Configuration Summary

- AS
  - Configure business ids.
  - Decide if you want MDNs.
  - Decide if you want encryption or signing.
    - If yes then also configure certificates.
- Configure for the payload
  - Business Ids, Action to use, etc.

Configuration – AS B2B Capabilities

Package: AS (N/A)

Attribute	Description	Current Value	Inheritance	Update
Time To Acknowledge	Time To Acknowledge	30	Inherited from: **Scope:** Global **Type:** Time To Acknowledge	
Retry Count	Retry Count	3	Inherited from: **Scope:** Global **Type:** Retry Count	
AS Compress Before Sign	AS Compress Before Sign	Yes	Inherited from: **Scope:** Global **Type:** AS Compress Before Sign	Select one to update
AS Compressed	AS Compressed	No	Inherited from: **Scope:** Global **Type:** AS Compressed	Select one to update
AS Encrypted	AS Encrypted	Yes	Locally Assigned	Yes
AS MDN Http Url	AS MDN Http Url	http://localhost:57080/bcgreceiver/submit	Inherited from: **Scope:** Global **Type:** AS MDN Http Url	
AS MDN Email Address	AS MDN Email Address	emailto:xxx@xxx.xxx	Inherited from: **Scope:** Global **Type:** AS MDN Email Address	
AS MDN Asynchronous	AS MDN Asynchronous	Yes	Inherited from: **Scope:** Global **Type:** AS MDN Asynchronous	Select one to update
AS MDN Requested	AS MDN Requested	Yes	Inherited from: **Scope:** Global **Type:** AS MDN Requested	Select one to update
AS Message Digest Algorithm	AS Message Digest Algorithm	sha1	Inherited from: **Scope:** Global **Type:** AS Message Digest Algorithm	Select one to update
AS MDN Signed	AS MDN Signed	Yes	Locally Assigned	Yes
AS Signed	AS Signed	Yes	Locally Assigned	Yes
AS Business Id	AS Business Id	E11111111	Locally Assigned	E11111111

Configure Business IDs – Receiving documents

Yourself (i.e. Community Manager)

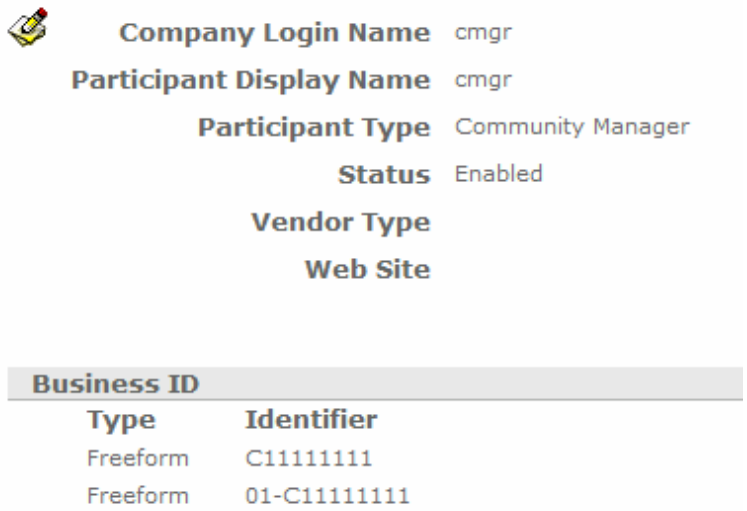
- Partner Profile – Used for receiving documents from partner
  - AS Business ID.
  - Payload Business ID (i.e. EDI Interchange)
    - Note: For EDI the business id consists of the EDI Qualifier-EDI business id.

Your partner (i.e. Community Participant)

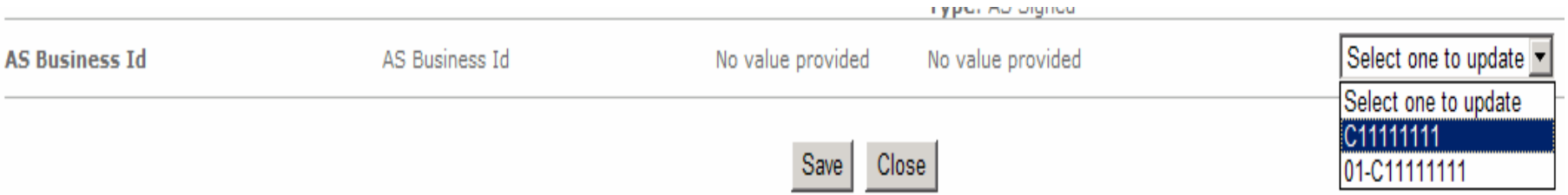
- Partner Profile – Used for receiving documents from partner
  - AS Business ID.
  - Payload Business ID (i.e. EDI Interchange).
    - Note: For EDI the business id consists of the EDI Qualifier-EDI business id.

Business IDs – Participants

Partner profile



Community Manager - B2B Capabilities or Document Flow Definition (Global) on the Source Document (from Backend)
Community Participant - B2B Capabilities on the Target Document



Configure Business IDs – Sending documents

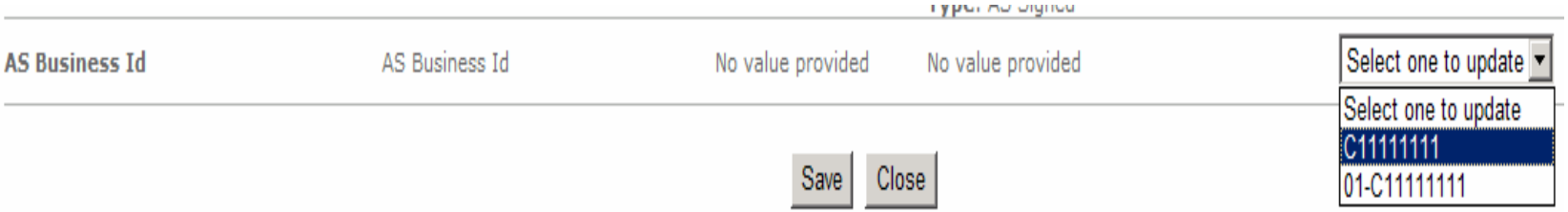
Yourself (i.e. Community Manager)

- B2B Capabilities – Used for sending documents to a partner.
  - AS Business ID – Note: this has to be set on the original source document from the backend, not the AS packaging.
  - If business id is not set then the source document sender business id will be used.

Your partner (i.e. Community Participant)

- B2B Capabilities – Used for sending documents to a partner.
  - AS Business ID – Set on the AS Package.
  - If business id is not set then the source document recipient business id will be used.

Community Manager - B2B Capabilities or Document Flow Definition (Global) on the Source Document (from Backend)
Community Participant - B2B Capabilities on the Target Document



Configuring MDNs

- Can configure in two different places:
  - On the target partners B2B Capabilities (specific to partner).
  - On the Document Flow Definition level (global).
- Set MDN
  - Asynchronous or Synchronous flag
  - HTTP response URL
    - For synchronous can be any value as long as valid HTTP URL format (i.e. http://xxx).
    - For asynchronous use the URL of a WPG HTTP Target (i.e. http://hostname:57080/bcgreceiver/submit).
  - Email address
    - For AS2 can be any value as long as valid email URL format (i.e. email:xxx@xxx.xxx).
  - Signed MDN requirement – Yes/No

Configuration MDN

Example with synchronous MDN

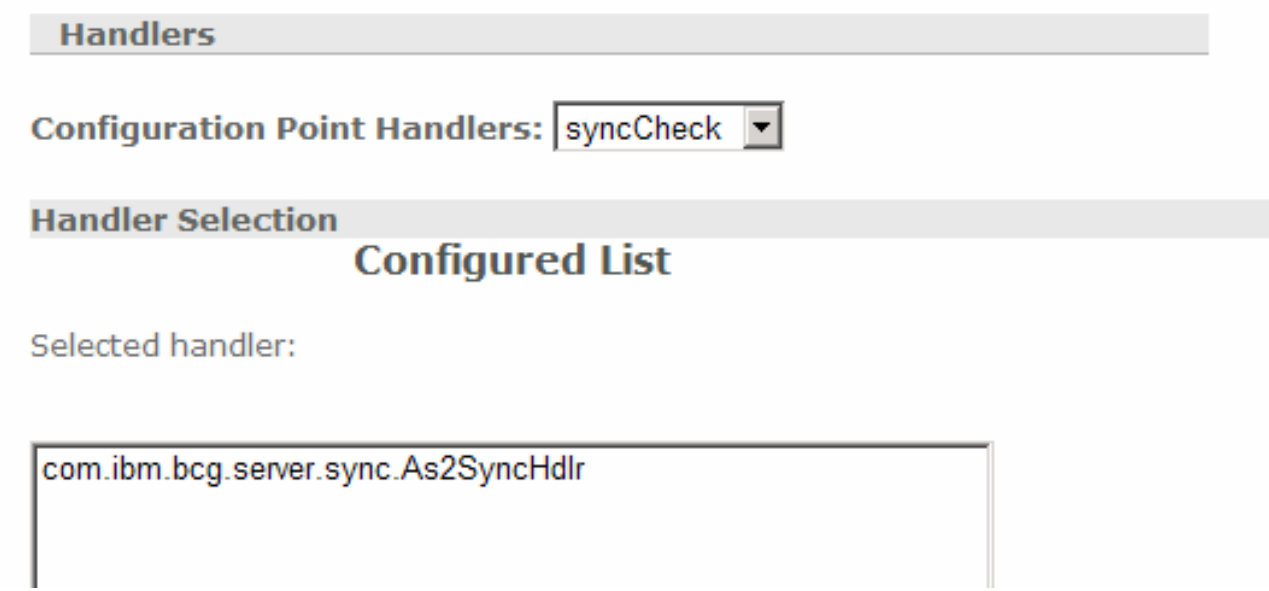
AS MDN Http Url	AS MDN Http Url	http://xxx	Locally Assigned	http://xxx
AS MDN Email Address	AS MDN Email Address	emailto:xxx@xxx.xxx	Locally Assigned	emailto:xxx@xxx.xxx
AS MDN Asynchronous	AS MDN Asynchronous	No	Locally Assigned	No
AS MDN Requested	AS MDN Requested	Yes	Locally Assigned	Yes

Example with asynchronous MDN

AS MDN Http Url	AS MDN Http Url	http://localhost:57080/bcgreceiver/submit	Locally Assigned	http://localhost:57080/bcgrecei
AS MDN Email Address	AS MDN Email Address	emailto:xxx@xxx.xxx	Locally Assigned	emailto:xxx@xxx.xxx
AS MDN Asynchronous	AS MDN Asynchronous	Yes	Locally Assigned	Yes
AS MDN Requested	AS MDN Requested	Yes	Locally Assigned	Yes

Configuring Synchronous MDNs – Receiver Target

- Some partners may request a synchronous MDN when they send you an AS2 document. The only required configuration is on the HTTP Receiver Target definition.
- Configure the Sync Check Handler: com.ibm.server.sy7nc.AS2SyncHdlr



Configuration - Signing

- Used for sending and receiving. For receiving WPG will enforce the signing requirement.
- Can configure in two different places:
  - On the target partners B2B Capabilities (specific to partner).
  - On the Document Flow Definition level (global)
- Set Signing
  - For payload
    - Will sign when sending to a partner.
    - Will require the payload to be signed when receiving from a partner.
  - For returned MDN
  - Optionally set signature hash algorithm
- Ensure that your signing private key (*.p12) is loaded (under Operator).
- For a returned signed MDN ensure the partners signing certificate (*.arm) is loaded.

Configuration - Encrypted

- Used for sending and receiving. For receiving WPG will enforce the encryption requirement.
- Can configure in two different places:
  - On the target partners B2B Capabilities (specific to partner).
  - On the Document Flow Definition level (global).
- Set Encryption for payload
  - Will encrypt when sending to a partner.
  - Will require the payload to be encrypted when receiving from a partner.
- Ensure that your partners encrypting certificate (*.arm) is loaded.
- For a returned encrypted MDN ensure the your private key (*.p12) is loaded (under Operator).

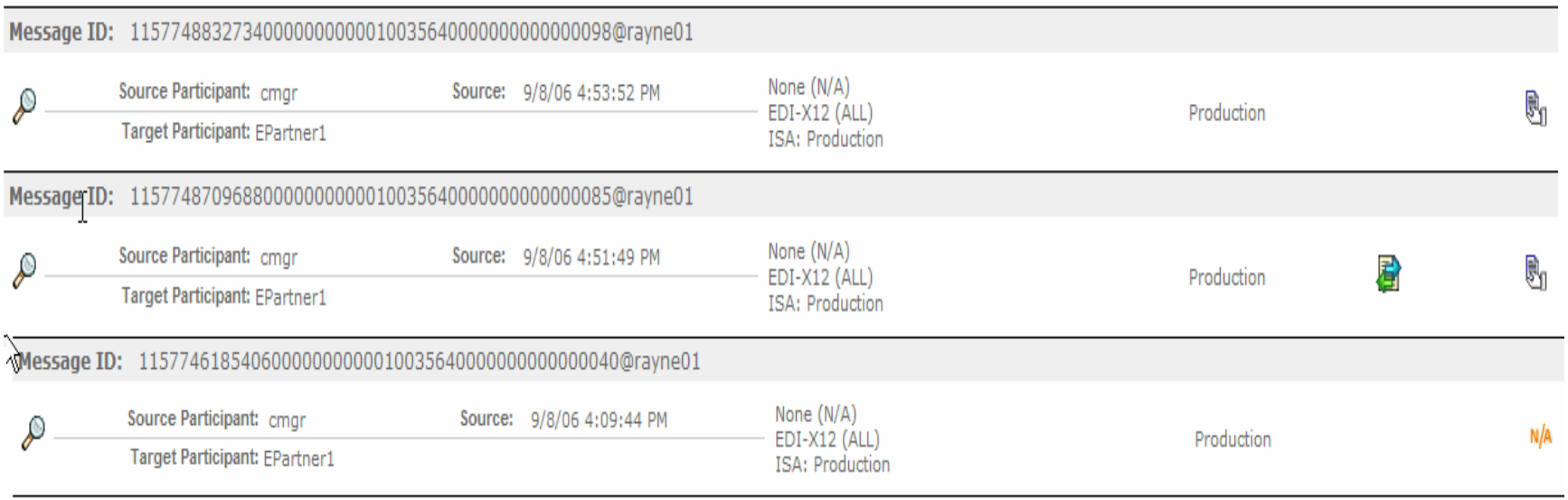
Configuration - Miscellaneous

- Compression – Compress before or after signing.
- Time to acknowledge – Time to wait (in minutes) for a returned MDN, if times out will resend the document.
- Retry Count – Number of resend tries.

Time To Acknowledge	Time To Acknowledge	30	Inherited from: **Scope:** Global **Type:** Time To Acknowledge	
Retry Count	Retry Count	3	Inherited from: **Scope:** Global **Type:** Retry Count	
AS Compress Before Sign	AS Compress Before Sign	Yes	Inherited from: **Scope:** Global **Type:** AS Compress Before Sign	Select one to update
AS Compressed	AS Compressed	No	Inherited from: **Scope:** Global **Type:** AS Compressed	Select one to update

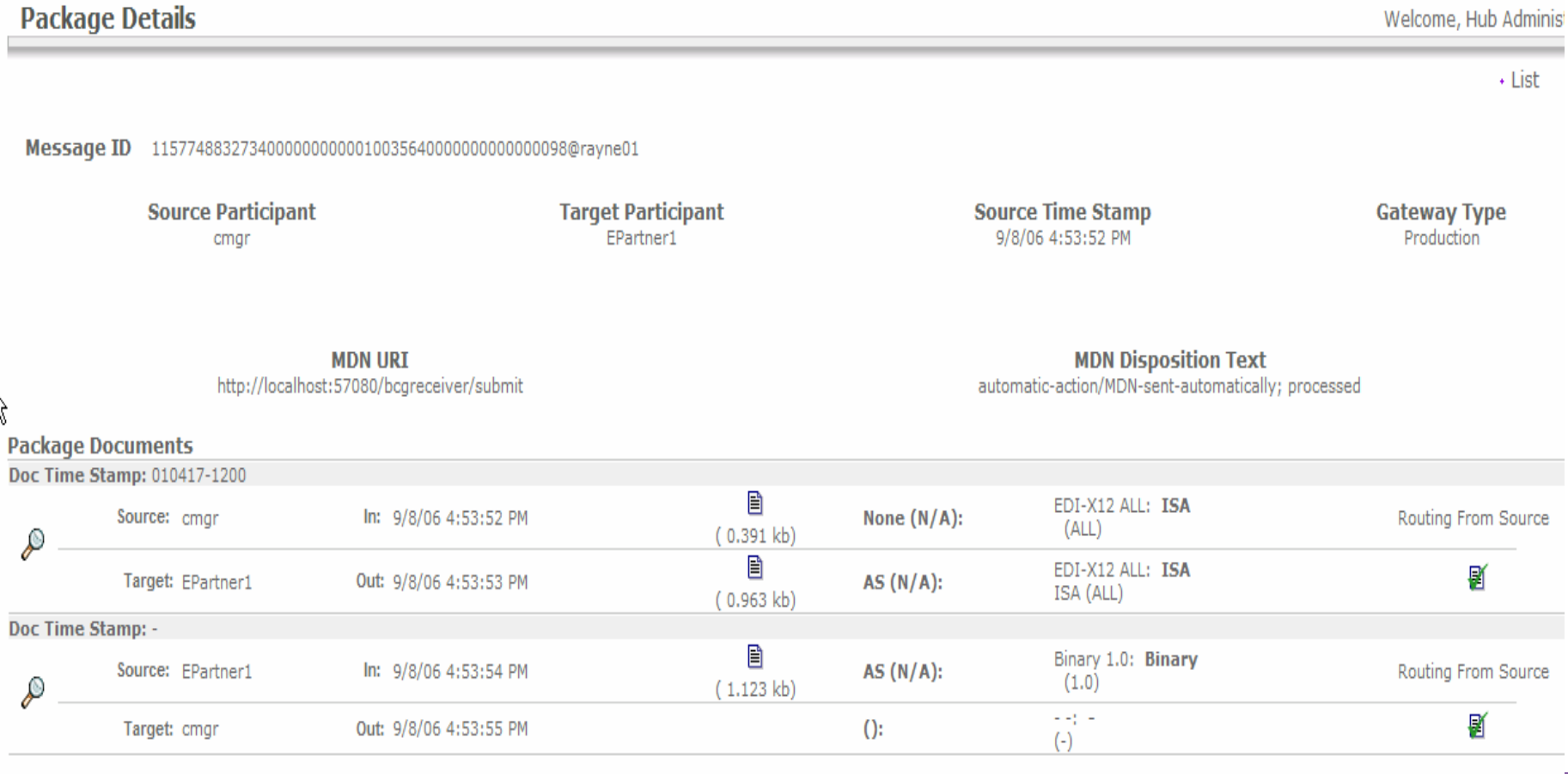
AS Document Viewer - List View

- Example showing:
  - Asynchronous MDN and status
  - Synchronous MDN and status
  - No MDN requested



AS Document Viewer - Details View

Drill down showing further details as well as both the original AS document and the MDN response



Summary

- AS is a payload agnostic envelope for sending documents via the internet.
- AS provides the conventions for signing, encryption, receipts, and non-repudiation.
- WPG will handle the AS requirements
  - Encryption, signing, MDNs (including correlation), non-repudiation, retries.
- We covered the AS semantics and how WPG configuration relates to those semantics.

References

- Document references
- AS Packaging references
- AS Message examples

References - Documents

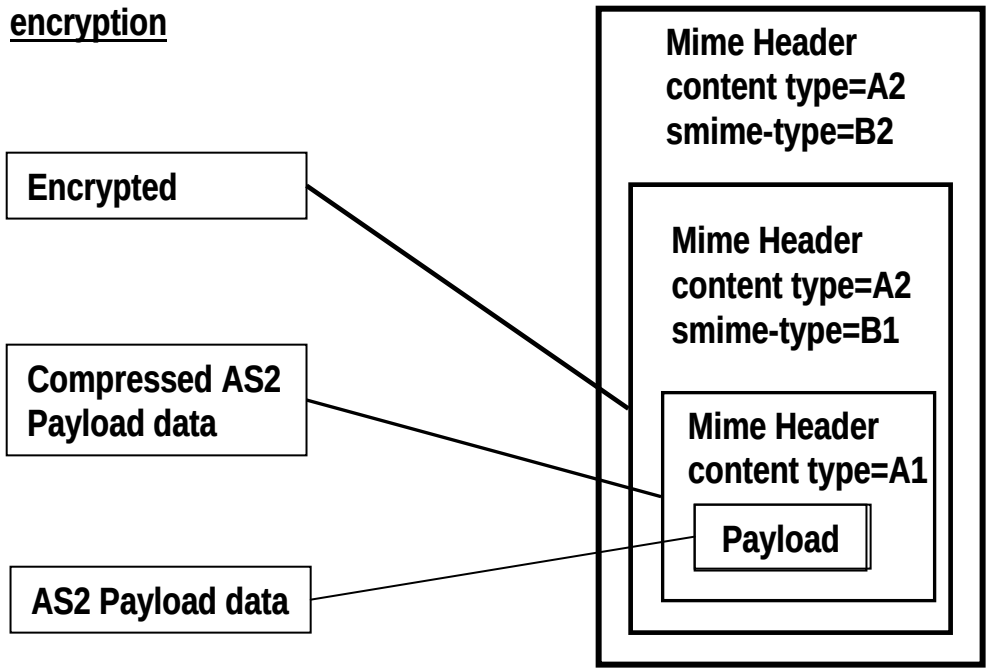
- Specifications
  - AS1 (SMTP) - RFC3335 - MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet
  - AS2 (HTTP) - RFC4130 - MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2
  - AS3 (FTP) - draft-ietf-ediint-as3-04.txt - FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet – submitted for RFC approval
  - MDN (Message Disposition Notification) – RFC3798
- WPG Product Documentation
  - Hub Configuration Guide

References – AS Packaging

- Following three slides show a picture representation of AS packaging
  - Compression and Encryption.
  - Signature on uncompressed payload, compression, encryption.
  - Signature on compressed payload, encryption.

AS2 Mime With Compression/Encryption

AS2 Mime with compression and encryption



A1 = application/xml,
*application/edifact,
*application/edix12
* - indicates binary

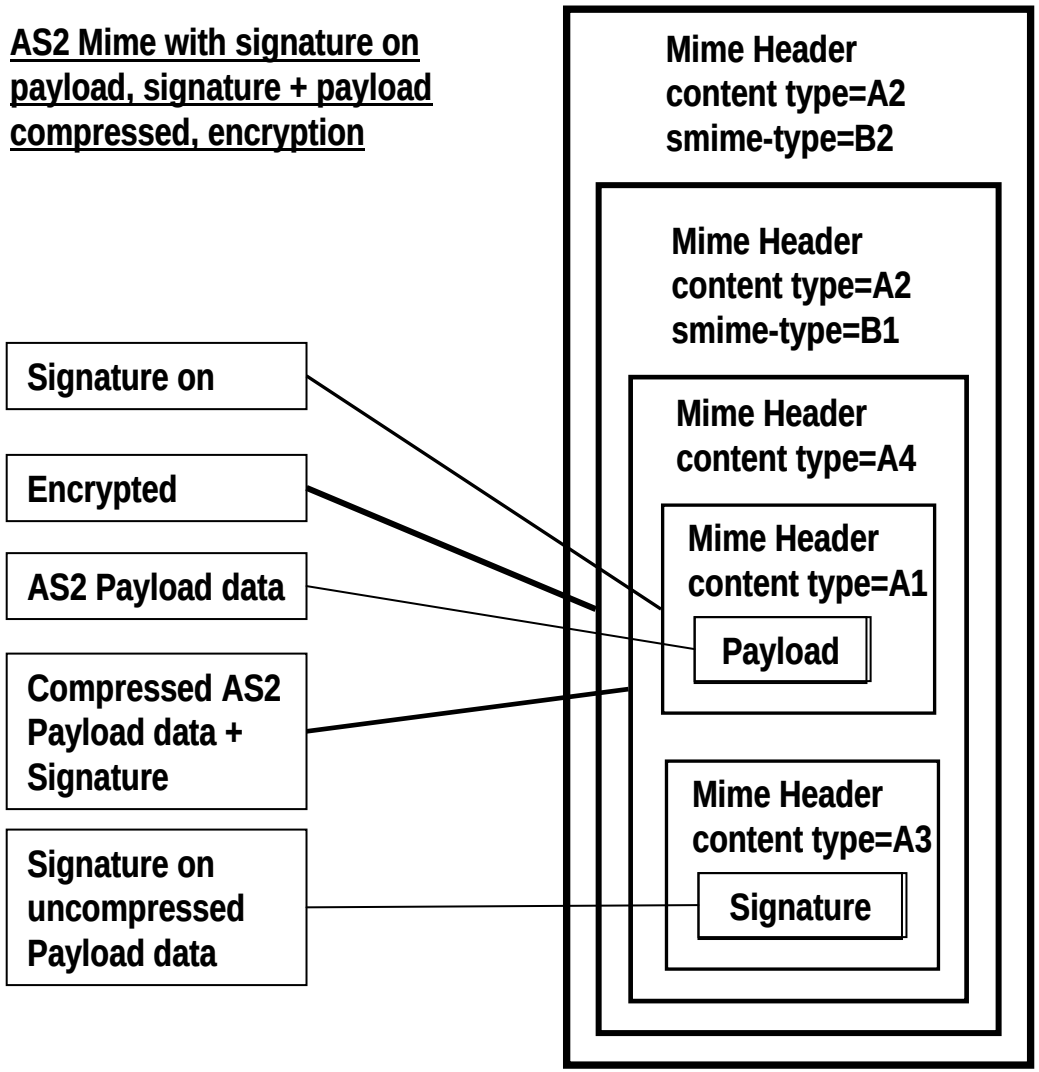
A2 = application/pkcs7-mime

B1 = compressed-data

B2 = enveloped-data

AS2 Mime With Signature/Compression/Encryption 1

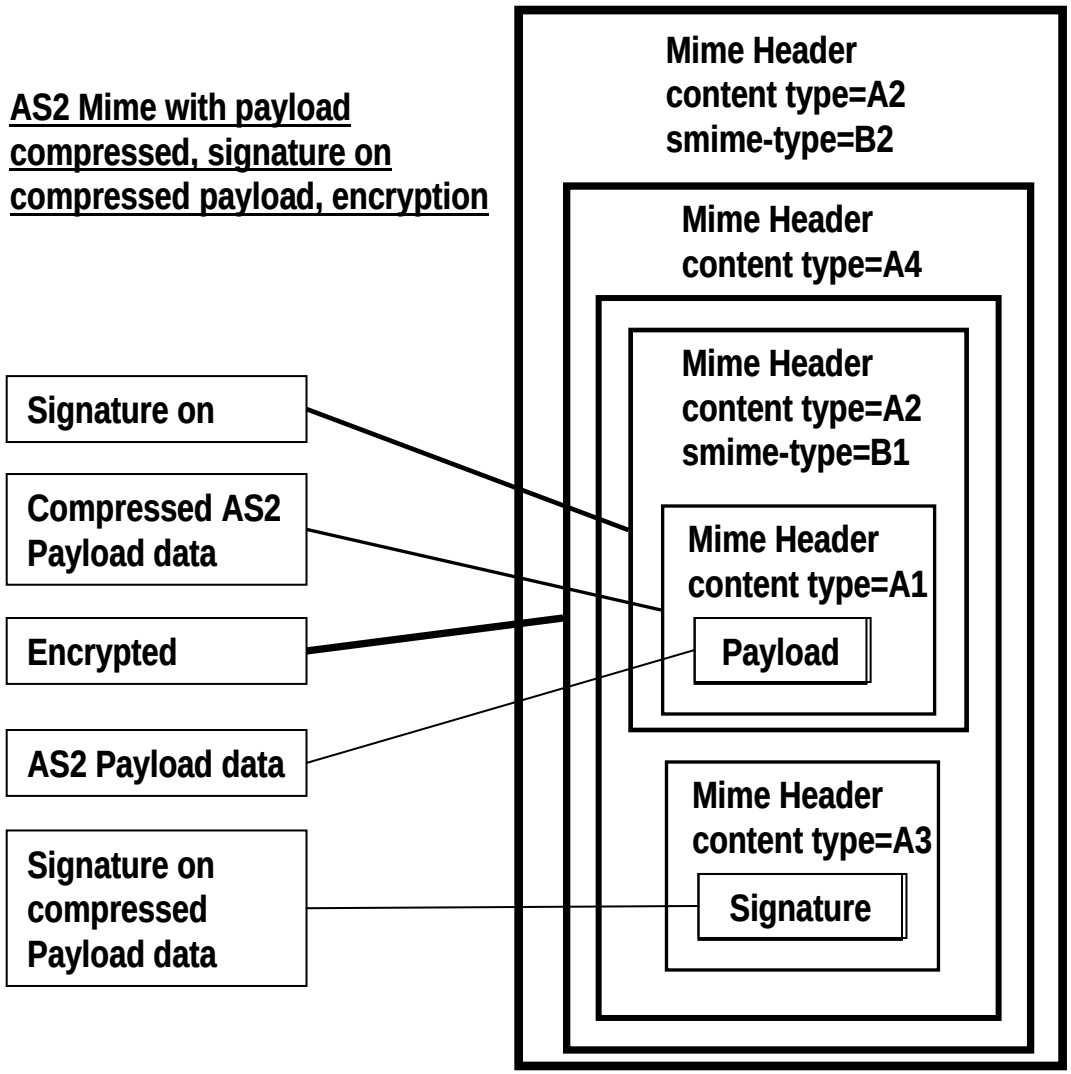
AS2 Mime with signature on payload, signature + payload compressed, encryption



A1 = application/xml,
*application/edifact,
*application/edix12
* - indicates binary
A2 = application/pkcs7-mime
A3 = application/pkcs7-signature
A4 = multipart/signed
B1 = compressed-data
B2 = enveloped-data

AS2 Mime With Signature/Compression/Encryption 2

AS2 Mime with payload compressed, signature on compressed payload, encryption



A1 = application/xml,
*application/edifact,
*application/edix12
* - indicates binary
A2 = application/pkcs7-mime
A3 = application/pkcs7-signature
A4 = multipart/signed
B1 = compressed-data
B2 = enveloped-data

Example of AS messages

Examples show:

- Plain message
- Message requesting synchronous MDN
- Message requesting asynchronous MDN
- Message requesting asynchronous MDN and is Signed.
- Message requesting asynchronous signed MDN, is signed and encrypted.
- Example MDN
- Example MDN that is signed.

Example: No MDN, Signing, Or Encryption

Transport Header

POST /input/AS2 HTTP/1.1
Connection: close
Host: localhost:59080
Date: Fri, 08 Sep 2006 20:09:45 UTC

Translated Document

Content-Length:391
Content-Type: application/edi-x12
AS2-From: C11111111
AS2-To: E11111111
AS2-Version: 1.1
Message-ID: <115774618540600000000000100356400000000000000040@rayne01>
Mime-Version: 1.0
Recipient-Address: http://localhost:59080/input/AS2
Subject: E11111111;C11111111
Content-Disposition: attachment; filename=edi-cmgr-to-EPartner1.inp

ISA~00~ ~00~ ~01~C11111111 ~01~E11111111 ~010417~1200~U~00401~000000001~0~T~:!
GS~QG~6116630000~004236241~20010417~1200~1~X~004010!
ST~879~0001!
G91~W!
N1~BY~BUYER NAME~9~004236241!
N1~VN~VENDOR~9~123456780!
G62~07~20010419!
G28~012345000621~012345000621~UP~123456789012~VN~30108!
G62~61~20010419!
G40~~10.50~~~1350!
SE~9~0001!
GE~1~1!
IEA~1~000000001!

Example: Sync MDN, No Signing Or Encryption

Transport Header

POST /input/AS2 HTTP/1.1
Connection: close
Host: localhost:59080
Date: Fri, 08 Sep 2006 20:28:54 UTC

Translated Document

Content-Length:391
Content-Type: application/edi-x12
AS2-From: C11111111
AS2-To: E11111111
AS2-Version: 1.1
Message-ID: <115774733448400000000001003564000000000000059@rayne01>
Mime-Version: 1.0
Recipient-Address: http://localhost:59080/input/AS2
Subject: E11111111;C11111111
Content-Disposition: attachment; filename=edi-cmgr-to-EPartner1.inp
Disposition-Notification-To: xxx@xxx.xxx

ISA~00~ ~00~ ~01~C11111111 ~01~E11111111 ~010417~1200~U~00401~000000001~0~T~:!
GS~QG~6116630000~004236241~20010417~1200~1~X~004010!
ST~879~0001!
G91~W!
N1~BY~BUYER NAME~9~004236241!
N1~VN~VENDOR~9~123456780!
G62~07~20010419!
G28~012345000621~012345000621~UP~123456789012~VN~30108!
G62~61~20010419!
G40~~10.50~~~1350!
SE~9~0001!
GE~1~1!
IEA~1~000000001!

Example: Async MDN, No Signing Or Encryption

Transport Header

POST /input/AS2 HTTP/1.1
Connection: close
Host: localhost:59080
Date: Fri, 08 Sep 2006 20:53:53 UTC

Translated Document

Content-Length:391
Content-Type: application/edi-x12
AS2-From: C11111111
AS2-To: E11111111
AS2-Version: 1.1
Message-ID: <115774883273400000000000100356400000000000000098@rayne01>
Mime-Version: 1.0
Recipient-Address: http://localhost:59080/input/AS2
Subject: E11111111;C11111111
Content-Disposition: attachment; filename=edi-cmgr-to-EPartner1.inp
Disposition-Notification-To: xxx@xxx.xxx
Receipt-Delivery-Option: http://localhost:57080/bcgreceiver/submit

ISA~00~ ~00~ ~01~C11111111 ~01~E11111111 ~010417~1200~U~00401~000000001~0~T~:!
GS~QG~6116630000~004236241~20010417~1200~1~X~004010!
ST~879~0001!
G91~W!
N1~BY~BUYER NAME~9~004236241!
N1~VN~VENDOR~9~123456780!
G62~07~20010419!
G28~012345000621~012345000621~UP~123456789012~VN~30108!
G62~61~20010419!
G40~~10.50~~~1350!
SE~9~0001!
GE~1~1!
IEA~1~000000001!

Example: Async MDN And Signing, No Encryption

```
Content-Type: multipart/signed; micalg=sha1;  protocol="application/pkcs7-signature";  boundary="----
=_Part_0_154876699.1157750500891"
AS2-From: C11111111
AS2-To: E11111111
AS2-Version: 1.1
Message-ID: <1157750500875000000000001003564000000000000110@rayne01>
Mime-Version: 1.0
Recipient-Address: http://localhost:59080/input/AS2
Subject: E11111111;C11111111
Disposition-Notification-To: xxx@xxx.xxx
Receipt-Delivery-Option: http://localhost:57080/bcgreceiver/submit
Content-Length: 1586

------=_Part_0_154876699.1157750500891
Content-Type: application/edi-x12
Content-Disposition: attachment; filename=edi-cmgr-to-EPartner1.inp

ISA~00~ ~00~ ~01~C11111111 ~01~E11111111 ~010417~1200~U~00401~000000001~0~T~:!
GS~QG~6116630000~004236241~20010417~1200~1~X~004010!
ST~879~0001!
G91~W!
N1~BY~BUYER NAME~9~004236241!
N1~VN~VENDOR~9~123456780!
G62~07~20010419!
G28~012345000621~012345000621~UP~123456789012~VN~30108!
G62~61~20010419!
G40~~10.50~~~1350!
SE~9~0001!
GE~1~1!
IEA~1~000000001!
------=_Part_0_154876699.1157750500891
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: binary

0_− * ┌•┐└P0L┐┌┌1 0 −|+♯└┐→|0 − * ┌•┌┌J┐┌┐┘E┌0 − * ┌┌┘|051 0 −└U┘−‼┐US1◀0¢−└U┘
‼¤IBM test1‼0◀−└U┘└‼
9.49.189.00┤ 0609082108192┤ 090603210819Z051 0 −└U┘−‼┐US1◀0¢−└U┘
‼¤IBM test1‼0◀−└U┘└‼
9.49.189.000 − * ┌ ┌ ┌ | └ 0┐ Ok<#□&  []4Q61Q_┬ r♯ ← |□r↑ ¿B├ M↔ ?s_4D¤ | 'l╩  jG*) Q┐ └ ┌ ┌ 0 − * ┌ ┌ ┘ | └ A(t37NX♯3
'‼(|
└ ¶ `→ K¤ LLC□i□&□EB0>┐ ┌ ┌ 0=051 0 − └ U┘ − ‼ ┐ US1◀ 0¢ − └ U┘
‼¤IBM test1‼0◀−└U┘└‼
9.49.189.0┐ ┘ E┌ 0 − | +♯ └ ┐ → | 0↑ − * ┌ └ 1 − * ┌ • ┌ 0  − * ┌ | 1¢ ┤ 060908212140Z0#− * ┌ ┘ 1┬ ┘ ¶ − %¶ a/s.5- − *
┌ ┌ ┌ | ┘ 9RK♯ R 8□dM¤ mJhwL¶ k*┴ mE2E*~)Ra\@3ɔ,o e♯ 5h+iGADO.┘ 8┘ ]9
------=_Part_0_154876699.1157750500891--
```

Example: Async Signed MDN, Signing, And Encryption

Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name=smime.p7m
AS2-From: C11111111
AS2-To: E11111111
AS2-Version: 1.1
Message-ID: <11577530672500000000000010035640000000000000136@rayne01>
Mime-Version: 1.0
Recipient-Address: http://localhost:59080/input/AS2
Subject: E11111111;C11111111
Disposition-Notification-To: xxx@xxx.xxx
Disposition-Notification-Options: signed-receipt-protocol=optional, pkcs7-signature; signed-receipt-micalg=optional, sha1
Receipt-Delivery-Option: http://localhost:57080/bcgreceiver/submit
Content-Length: 2031

0 * ┌•└•┌10┐┌0G0?1 0 –└U┘–╢┐US1←0├–└U┘
╢↕IBM Test EPartner11╢0◄–└U┘└╢
0.49.189.0┐┘E┌0 – * ┌┌┌┤┘i=k↕┤'!{gtN[va┌5=Po1|4U┤^H`UUU{YKC/?1[OWkp(5SJ–1|! * ┌•┌0¶╌◘*
└ • ┘ ◘ na ☐eKO┬ 'F☐E↑ N┼ qX┤ ┼ 27Q6♬ v^/;☐F:cJ6KC*>\ /VMq`4в♬ 62⁹Z 英← - oi;t}(jzU AmMkM┴ x Rt2T
yEK☐ b+Qs9Q#✡ @AdG&ka✡ 5{cA k♭.┌ -A|v^ n? ↕ ☐b_z{z☐H/✡ qض|y╢ 4j k/@;}viL)R↑ | X:6Sy▯ • ¿z ¶ 6T@☐a},▒D5
┬ Vh7$M┌ y9I±┴ ← A┴ ? ă ┤ ?♬ V[X]☐^(☐uEu¸z&) (i ◘ B
V▯▯ E>-?3rjv1↑ '*┼ >9← 2*]i◄ | ┼ 4r9Z,¶ <7&STuSi└ ▯ ┴ SYP+b(A.d/\• ;↑ 1/┤ ┬ ↕ {6US`┌ k▯ y?}__k← D^f~t8▯ ☐6be ┘
◘&c qi b• ▯ ☐Rp :Ckǫ ↕ S"fd<u{k'k9☐3☐₀L♬ !A?ZO┐ =☐ɯWX+↕ /%©A`┐ al↑ 5┘ ~ – /↕ k'^ JCm┬ H{dG☐J┴
{xx`☐b← ☐MnVÏ{A↕ rS¶ • .E↑ N^T[OD*-✡ "Y ℰ{– g• ☐x6?zK3t^D → ?DN↑ ┴ 0}B~)↕ ⌠ \yK*┴ ◘ b,e2z┤ ┘ L Yw`BoC+┤
C┘ <↕ O pg,HY7r◘ n└ ♬ ┘ {3‹ ← ◘ `u+♬ '└ KwufrI^^"`¶ R ┬ ┬ q┘ =Fp WhaI^☐nz71☐ↀ ↕;9aip _H◄ \hq?d☐$GTED&2
←uQG┤3◘:┤Mi╢%GP KáP^XM%¶╤TM]Yza8

Example: MDN

Transport Header

Connection:
Content-Length: 711
Host:
AS2-Version: 1.1
Recipient-Address: http://localhost:59080/input/AS2
Subject: C11111111; E11111111
Mime-Version: 1.0
Content-Type: multipart/report; Report-Type=disposition-notification; boundary="----=_Part_40_298968702.1157748834688"
AS2-To: C11111111
AS2-From: E11111111
ReferenceId: 11577488348280000000000010040760000000000000026
Message-ID: <E11111111@1157748833109C0A8016537cb61f8f3397d8602291e678010d8ef53e6a097ff6>

Initial Document

------=_Part_40_298968702.1157748834688
Content-Type: text/plain
Content-Transfer-Encoding: 7bit

This MDN response message is for:

Message id: <11577488327340000000000010035640000000000000098@rayne01>
From: C11111111

------=_Part_40_298968702.1157748834688
Content-Type: message/disposition-notification
Content-Transfer-Encoding: 7bit

Reporting-UA: WBI_Connect-Express
Original-Recipient: rfc822; E11111111
Final-Recipient: rfc822; E11111111
Original-Message-ID: <11577488327340000000000010035640000000000000098@rayne01>
Disposition: automatic-action/MDN-sent-automatically; processed
Received-Content-MIC: 2u6ZhFf/oeJ+N0LlaHWJwx4bfBM=, sha1

------=_Part_40_298968702.1157748834688

Example: MDN With Signature

Transport Header

Connection:
Content-Length: 1968
Host:
AS2-Version: 1.1
Recipient-Address: http://localhost:59080/input/AS2
Subject: C11111111; E11111111
Mime-Version: 1.0
Content-Type: multipart/signed; micalg=sha1; protocol="application/pkcs7-signature"; boundary="----=_Part_102_1108813426.1157751327016"
AS2-To: C11111111
AS2-From: E11111111
ReferenceId: 1157751328188000000000001004076000000000000035
Message-ID: <E11111111@1157751324469C0A8016537cb61f8f3397d8602291e678010d8ef53e6a097ff2>

Initial Document

------=_Part_102_1108813426.1157751327016
Content-Type: multipart/report; Report-Type=disposition-notification;
boundary="----=_Part_101_762685042.1157751327016"

------=_Part_101_762685042.1157751327016
Content-Type: text/plain
Content-Transfer-Encoding: 7bit

This MDN response message is for:

Message id: <1157751324078000000000001003564000000000000121@rayne01>
From: C11111111

------=_Part_101_762685042.1157751327016
Content-Type: message/disposition-notification
Content-Transfer-Encoding: 7bit

Reporting-UA: WBI_Connect-Express
Original-Recipient: rfc822; E11111111
Final-Recipient: rfc822; E11111111
Original-Message-ID: <1157751324078000000000001003564000000000000121@rayne01>
Disposition: automatic-action/MDN-sent-automatically; processed
Received-Content-MIC: 2FcBrtclFKOOYS9z/cUuNf5dLaE=, sha1

------=_Part_101_762685042.1157751327016--

------=_Part_102_1108813426.1157751327016
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: binary

0}– * ┌•┐└n0j┐┌┌1 0 –|+ƒ└┐¬|0 – * ┌•┌┌^┐┌┐┘E┌0 – * ┌┌|0?1 0 –└U┘–╢┐US1┐0├└U┘
╢‡IBM Test EPartner11╢0◄└U┘└╢
9.49.189.00┤ 060908211254Z┤ 090603211254Z0?1 0 –└U┘–╢┐US1┐0├└U┘
╢‡IBM Test EPartner11╢0◄└U┘└╢
9.49.189.000 – * ┌┌┌|└0┐‡`z_)X|^,ya┐M
o):□ ⁄*‖{mt]╢ a1&?¶ 0>0>a– h Tj† ├ ┐ └ ┌ ┌ 0 – * ┌ ┌ ┘ | └ @j└ Oc□qu┐ 燮m38P6GwP‡ f9 >RG┬ ├ LoIo9%comF┤ R'qV‡ :/‡ R□┐1L0H┐ ┌ ┌
1 0 –└U┘–╢┐US1┐0├└U┘
╢‡IBM Test EPartner11╢0◄└U┘└╢