Technical Comparison of EDIINT AS2 and GISB EDM

Introduction

In May of 1999 several representatives throughout the Gas, Electric, Automobile and Computer industries met in Dallas to discuss the convergence of their respective Internet EDI transport mechanisms into a single standard. The result of this "E-C" summit was an agreement by all parties to develop a new specification, which would be developed under the IETF, called EDIINT AS2.

EDIINT AS2 combines the core capabilities of existing Internet EDI transport mechanisms in a single specification. All of the GISB EDM, AIAG and EDIINT AS1 requirements have been addressed and are contained in AS2.

This document describes the technical similarities and differences between EDIINT AS2 and GISB EDM. The goal of this document is to provide the GISB FTTF with sufficient information to assess the impact of incorporating AS2 into GISB EDM. This report is not intended to compare all the features and functions of AS2 to GISB EDM, but rather focuses on the part of AS2 that most closely resembles GISB EDM, the multipart/form-data format. No coverage is given to the E-mail packaging and Message Delivery Notification options available within AS2.

EDIINT AS2 Overview

EDIINT AS2 defines a HTTP based protocol designed to support the reliable, secure transport of EDI data via the Internet. The original intent of AS2, prior to convergence, was to provide a HTTP facility for transporting EDI data packaged in an e-mail format, following the specifications defined in EDIINT AS1. This remains one of the primary requirements addressed by the current AS2 specification. As a direct result of AIAG and GISB inputs, the AS2 specification has been expanded to include a multipart/form-data alternative (following RFC 1867 and GISB EDM) for packaging EDI data. The addition of multipart/form-data to AS2 enables browser based clients the ability to POST EDI data to a web server, similar to GISB EDM.

AS2 contains 17 header level data elements to aid in the routing and processing of the EDI payload associated with each data exchange. All of the GISB EDM header data elements are supported (to, from, input-format, input-data and transaction-set) along with the full set of data elements requested by AIAG. In addition, several new header data elements are included which are used in the processing of acknowledgements.

In an effort to meet the needs of the broadest possible audience, AS2 includes support for both PGP and S/MIME cryptographic systems for privacy, authentication, integrity and non-repudiation. Both PGP and S/MIME have undergone extensive standardization by the IETF and open standards exist for both. These existing standards contain specifications describing the format, packaging and content-type identifiers for objects that have been encrypted/signed with PGP and S/MIME.

In anticipation of further developments with XML and its eventual adoption within the computer industry (e.g. RosettaNet), AS2 now includes support for XML in addition to the three EDI types defined in RFC1767 (EDI-X12, EDIFACT, EDI-consent).

Lastly, AS2 includes a robust, feature rich, set of real-time and asynchronous acknowledgements (a.k.a. timestamps). Acknowledgements within AS2 are based on IETF

standards for Multipart/Report messages (RFC 1892) and Message Disposition Notifications (RFC2298). These standards define a mechanism to provide a sending party with delivery status information and can be optionally signed by the “reporting” party.

Side-by-Side Comparison

Multipart/form-data Header Data Elements

GISB EDM	EDIINT AS2	PURPOSE
To	To	identical to GISB EDM
From	From	identical to GISB EDM
Input-format	Input-format	identical to GISB EDM
Input-data	Input-data	identical to GISB EDM
Transaction-set	Transaction-set	identical to GISB EDM
	Agent	network or agent where the data exchange originated
	Application	identifies the application used to process the data next
	DateTime	date and time the data was created
	RefNum	integer value used to uniquely identify the communication exchange
	UserParam	user defined parameter
	GISB-Version	EDM version number
	Receipt-disposition-to	DUNS number of party to receive acknowledgement, also used to request generalized receipt
	Receipt-delivery-option	indicates how the receipt is to be delivered. While the default mode of operation within HTTP transport is to return the receipt in the reply body, asynchronous reply is allowed through use of this data element
	Receipt-report-type	used to request a specific type of receipt (e.g. GISB-Acknowledgement-Receipt."
	Receipt-security-selection	indicates the protocol and algorithm choices for a digital signature over the receipt
	Disposition-notification-to	indicates that the MDN style of receipt is to be used. It may have values other than email addresses when it is found as a name parameter in a form-data body part, such as a D-U-N-S number
	Disposition-notification-options	identifies characteristics of message disposition notification in accordance with AS1

Packaging and Data Preparation

EDI Payload Packaging

EDIINT AS2 specifies an IETF standard mechanism for identifying EDI content, referred to as RFC1767. All payload data within AS2 is associated with one of the MIME media types specified in RFC1767 or any valid MIME media type specified in http://www.isi.edu/in-notes/iana/assignments/media-types/media-types, which includes text/xml.

Unlike GISB EDM where the "raw" EDI data is encrypted and signed, AS2 requires that EDI data be encapsulated in a MIME envelope, prior to performing any cryptographic functions on the data. The most appropriate choice for GISB being the MIME media type application/EDI-X12.

Example of MIME encapsulation of EDI data following AS2 standard:

```
Content-Type: application/EDI-X12

ISA*……...
…
…
IEA
```

After the payload data has been "packaged" cryptographic functions may be applied.

Cryptographic Processing and Packaging

This section will focus on the options and procedures appropriate when using PGP.

EDIINT AS2 specifies IETF standard mechanisms for preparing and identifying data processed with PGP encryption and digital signatures. The standards referenced by AS2 are; RFC1847, Security Multiparts for MIME and RFC2015, MIME Security with Pretty Good Privacy (PGP).

Unlike GISB, which only supports encapsulated signatures, two options exist within AS2 for digital signatures, detached and encapsulated. Encapsulated signatures refer to the way in which PGP can include the digital signature integrally within the encryption function essentially making the signature part of the encrypted output. Detached signatures refer to the separation of the actual digital signature data from the encrypted object, making creation of the digital signature a separate and distinct process from encryption.

Detached signatures are created by processing the EDI payload through a secure hashing function, such as MD5 or SHA1, resulting in a message digest, which is then signed using the sending party's private key. The detached signature data is then enveloped with a MIME media type of application/pgp-signature. The digital signature part is then appended to the EDI payload (created above), using a multipart/signed format, for example:


```
Content-Type: multipart/signed; micalg=pgp-md5
protocol="application/pgp-signature"; boundary=bar

--bar
Content-Type: application/EDI-X12

ISA*……
IEA……

--bar
Content-Type: application/pgp-signature

-----BEGIN PGP MESSAGE-----
Version: 2.6.2

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/LC//
jJV5bNvkZIGPIcEmI5iFd9boEgvpirHtIREEqLQRkYNoBActFBZmh9GC3C041WGq
uMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfolT9Brn
HOxEa44b+EI=
=ndaj
-----END PGP MESSAGE-----

--bar--
```

This multipart signed object is then encrypted using PGP’s encryption function, the same as within GISB EDM (excluding the signature option). This results in the creation of a PGP encrypted object, which must have MIME enveloping applied. AS2 specifies that PGP encrypted data must be packaged following the specifications in RFC2015. This requires that encrypted objects be enveloped in a Content-type: multipart/encrypted envelope, for example:

```
Content-Type: multipart/encrypted;
       protocol="application/pgp-encrypted"; boundary=foo

--foo
Content-Type: application/pgp-encrypted

Version: 1

--foo

Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: 2.6.2

Content-Type: multipart/signed; micalg=pgp-md5
protocol="application/pgp-signature"; boundary=bar

--bar
Content-Type: application/EDI-X12

ISA*……
```


```
IEA……

--bar
Content-Type: application/pgp-signature

-----BEGIN PGP MESSAGE-----
Version: 2.6.2

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/LC//
jJV5bNvkZIGPIcEmI5iFd9boEgvpirHtIREEqLQRkYNoBActFBZmh9GC3C041WGq
uMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfolT9Brn
HOxEa44b+EI=
=ndaj
-----END PGP MESSAGE-----

--bar--
-----END PGP MESSAGE-----

--foo--
```

As in the case with GISB EDM, the multipart/encrypted payload is associated with the Input-data header element and packaged in multipart/form-data, following RFC 1867, with other associated header data elements (To, From, Input-format, Report-disposition-to, Receipt-report-type, Receipt-security-selection and GISB-Version) and the entire package is sent over the Internet using HTTP POST.

Receipt Processing

AS2 receipt processing is similar to GISB in that a receipt is immediately returned to the sender in the same session as the HTTP POST operation that was used to send an EDI file. There are multiple receipt types supported by AS2, however only the GISB-Acknowledgement-receipt will be described here.

Upon a successful receipt of a data exchange the receiving server is required to issue a receipt to the sender in the format requested by the sender in the Receipt-report-type header. The GISB-Acknowledgement-receipt is identical to the GISB timestamp in all characteristics except for an additional level of enveloping.

Because AS2 is required to follow IETF standards the GISB acknowledgement must be packaged in a multipart/report format as specified in RFC 1892, The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages. A Multipart/Report content-type that contains a GISB-Acknowledgement-receipt consists of two sub-parts. The first body part, which is intended for human consumption, contains a standard GISB EDM timestamp in html format. The second body part contains the same information however it is intended for “machine processing”. Here is an example of a GISB-Acknowledgement-receipt:

```
Content-Type: multipart/report;  report-type="GISB-
Acknowledgement-Receipt"; boundary="GISB7867"

--GISB7867
Content-type: text/html
```


```
<HTML><HEAD><TITLE>Acknowledgement Receipt Success</TITLE></HEAD>
<BODY><P>
time-c=19960619082855*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>

--GISB7867
Content-type: text/plain

time-c=19960619082855*
request-status=ok*
server-id=coolhost*
trans-id=234423897*
--GISB7867--
```

In addition to the above description of receipt processing a sending host can request that the “receiving” host sign the receipt with a digital signature, making the receipt non-repuditable. Signed receipts, using PGP, are packaged in a multipart/signed MIME envelope as defined in RFC 2015.