RECOMMENDATION TO GISB EXECUTIVE COMMITTEE

Requester: Group 8760 **Request No.: R99035**

1. Recommended Action:

___Accept as requested
_X_Accept as modified below
___Decline

Effect of EC Vote to Accept Recommended Action:

_X_Change to Existing Practice
___Status Quo

2. TYPE OF MAINTENANCE

Per Request:

___Initiation
_X_Modification
___Interpretation
___Withdrawal

___Principle (x.1.z)
___Definition (x.2.z)
___Business Practice Standard (x.3.z)
___Document (x.4.z)
___Data Element (x.4.z)
___Code Value (x.4.z)
___X12 Implementation Guide
_X_Business Process Documentation

Per Recommendation:

___Initiation
_X_Modification
___Interpretation
___Withdrawal

___Principle (x.1.z)
___Definition (x.2.z)
___Business Practice Standard (x.3.z)
___Document (x.4.z)
___Data Element (x.4.z)
___Code Value (x.4.z)
___X12 Implementation Guide
_X_Business Process Documentation

3. RECOMMENDATION

SUMMARY: * Modify the Electronic Delivery Mechanism Implementation guide to support standards convergence with the Internet Engineering Taskforce "HTTP Transport for Secure EDI" (a.k.a.EDIINT standard AS2)

* Instruct the Contracts Subcommittee to review changes which may be needed in the GISB standard Trading partner Agreement which permit the trading partners to specify their mutual agreement to the use of signed receipts and the specific implementation of such use:

RECOMMENDATION TO GISB EXECUTIVE COMMITTEE

Requester: Group 8760 **Request No.: R99035**

DATA DICTIONARY (for new documents and addition, modification or deletion of data elements)

Document Name and No.:

Business Name (Abbreviation)	**Definition**	**Format**	**Usage**	**Condition**
version	*The GISB EDM version being used by the sender*	*numeric, decimal notation (e.g. 1.4)*	*in Request ; M*	*used in file transmittal and in posting error notifications*
receipt-disposition-to	*The party to receive receipts, the value should be the same as the "from"*	*Common Code Identifier format*	*in Request ; M*	*used in file transmittal and in posting error notifications*
receipt-report-type	*Type of receipt type being requested by sender*	*gisb-acknowledgement-receipt*	*in Request ; M*	*used in file transmittal and in posting error notifications*
receipt-security-selection	*Used to request signed receipts*	*signed-receipt-protocol=required, pgp-signature;signed-receipt-micalg=required, md5*	*In Request, MA*	*used in file transmittal and in posting error notifications*

* Indicates Common Code

BUSINESS PROCESS DOCUMENTATION (for addition, modification or deletion of business process documentation language)

Standards Book:

Language: Recommended changes to the EDM Implementation guide and Instruction to the Contracts Subcommittee (Start on next page)
Fully annoted pages of the EDM Implementation guide can be found on the GISB home page under the March 23, 2000 EDM meeting at www.gisb.org/edm.htm

Annotations from EdmAS2.pdf

Page 1

Annotation 1; Label: Carl P Caldwell; Date: 4/6/2000 1:21:09 PM
Proposed changes to section Executive Summary , subsection Open Standards Page 1, after the Security item

HTTP Transport for Secure EDI (a.k.a. IETF EDIINT AS2).

(after the sentence "The open standard technologies.....)
There are business benefits gained from adherence to "HTTP Transport for Secure EDI" such as :

- Allows potential to more readily, electronically trade with others (e.g., electric utilities, banks, suppliers, retail customers)

- Makes it more likely that packages can be purchased to replace custom written apps currently in place to support GISB EDM

- Strengthens the surety of receipt and error notification

HTTP Transport for Secure EDI (AS2) is an emerging standard, largely based on the original GISB EDM, that is being developed by the Internet Engineering Task Force, the Internet standards body. Adherence with a formal, international Internet standard, such as AS2 ensures that the specification will not change without due process and any changes that do occur will be the result of a broad consensus. Individual companies and entire industries are free to use as much or as little of AS2 as they see fit, providing the maximum flexibility to meet business needs.

Page 3

Annotation 1; Label: Carl P Caldwell; Date: 3/1/2000 7:18:56 PM
Proposed changes to section Business Process and Practices, subsection Overview: Where Internet EDM Fits..... Page 1, at the end of second paragraph

In Version 1.5 of the GISB Standards, the technical specifications of the   EDI/EDM method of communication have been modified to comply with a the broader "HTTP Transport for Secure EDI" standard being developed by the Internet Engineering Task force (IETF). These technical changes do not impact the underlying required business practices established by GISB. In addition, the security features of the EDI/EDM and batch FF/EDM communication method now includes mutually agreeable business practices to protect the sender of a document from non-repudiation and to digitally sign Error Notifications.

Page 8

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 7:54:20 PM
Proposed changes to section Business Process and Practices, subsection Receipt of Transactions (Server) . Page 6, before the last sentence on the page insert

If the transacting parties mutually agree to use signed receipts, then the application would additionally attach a digital signature to the response .

Page 34

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 7:55:55 PM
Page 2, Data Dictionary for Internet EDM – include the following:

Business Name: version

Definition: The GISB EDM version being used by the sender
Format: numeric, decimal notation (e.g. 1.4)
Usage: in Request; M
Condition: used in file transmittal and in posting error notifications

Business Name: receipt-disposition-to
Definition: the party to receive receipts, the value should be the same as the “from”
Format: Common Code Identifier format
Usage: in Request; M
Condition: used in file transmittal and in posting error notifications

Business Name: receipt-report-type
Definition: type of receipt type being requested by sender
Format: gisb-acknowledgement-receipt
Usage: in Request; M
Condition: used in file transmittal and in posting error notifications

Business Name: receipt-security-selection
Definition: Used to request signed receipts
Format:signed-receipt-protocol=required,pgp-signature;signed-receipt-micalg=required, md5
Usage: In Request, MA
Condition: Used in file transmittal and in posting error notifications

Page 37

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 7:58:17 PM
Proposed changes to section SENDING TRANSACTIONS, subsection GENERAL FLOW, Page 2, immediately following item 11:

If trading partners agree to implement signed receipts then the sending party must include the “receipt-security-selection” data element in the posted data. The receiving party must digitally sign the gisb-acknowledgement-receipt and encapsulate the gisb-acknowledgement-receipt and digital signature body parts within a MIME envelope with a Content-type of application/pgp-signature.

Page 39

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 7:59:29 PM
Proposed changes to section SENDING TRANSACTIONS, subsection Sample of HTML document with a form to perform a multipart post using an interactive browser:

Page 4, within the text of the example, following the To: <input …> line insert the following:

GISB EDM Version: <input TYPE=”text” NAME=”version” SIZE=5 VALUE=”1.4”><br>
Deliver Receipt To: <input TYPE=”text” NAME=”report-disposition-to” SIZE=20 VALUE=””><br>
Receipt Type: <input TYPE=”text” NAME=”receipt-report-type” SIZE=30 VALUE=”gisb-acknowledgement-receipt”><br>

IF requesting signed receipts also include:

Receipt Type: <input TYPE=”text” NAME=”receipt-security-selection” SIZE=30 VALUE=” signed-receipt-protocol=required, pgp-signature; signed-receipt-micalg=required, md5”><br>

Page 40

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:00:53 PM
Proposed changes to section SENDING TRANSACTIONS, subsection Server Response

Page 5, replace the first sentence with the following:

“The receiving server will send a gisb-acknowledgement-receipt as an HTTP response to the client before dropping the client’s connection. If the transacting parties agree to use signed receipts, then the receiving server applies a digital signature to the gisb-acknowledgement-receipt and encapsulates the entire package in a MIME envelope of Content-type: application/pgp-signature.”

Page 41

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:02:17 PM
Proposed changes to section SENDING TRANSACTIONS, subsection HTTP Request Data Elements

Page 6, insert the following rows into the Required Data Elements table, between the to and input-format rows:

version
The GISB EDM version being used by the sender, in decimal notation (e.g. 1.4) The sending of the “version” data element is intended to assist in the early identification of EDM configuration errors and will not in itself dictate the version which a receiving party will support.

receipt-disposition-to
Common Code Identifier of the party to receive the acknowledgement receipt

receipt-report-type Type of receipt requested “gisb-acknowledgement-receipt”

Annotation 2; Label: Carl P Caldwell; Date: 2/29/2000 8:44:13 AM
Page 6, insert into the last row of the Mutually Agreed to Data Elements table, the following:

receipt-security-selection
Used to request signed receipts from the party receiving a file upload.

Annotation 3; Label: Carl P Caldwell; Date: 3/7/2000 8:18:28 PM
Page 6 Under section SENDING TRANSACTIONS, sub-section Writing a Batch Brower
replace the line in the example containing
"POST C:\execute HTTP/1.0"
with
"POST /cgi-bin/AS2dispatcher HTTP/1.0"

Page 43

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:22:46 PM
Proposed changes to section SENDING TRANSACTIONS, subsection Writing a Batch Browser , (example includes request for signed receipt)

Page 8, replace the example with the following:

```
-----------------------------87453838942833
Content-Disposition: form-data; name="from"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="to"
```

```
234567890
-----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.4
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
-----------------------------87453838942833
Content-Disposition: form-data; name="input-format"

x12
-----------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename=”c:\temp\smallnom.bin”
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"

--8760
Content-Type: application/pgp-encrypted

Version: 1

--8760
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHs
z0e8sb7ErC340MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG
lQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/43fkB+al
ATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1E
h785zC03UAw0qg0ugMt86dPeyd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8O
cp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RQbeN
aqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cV
zpb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9
UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZySaRO8Vtff+
4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
--8760--
-----------------------------87453838942833--
```

Annotation 2; Label: Carl P Caldwell; Date: 3/7/2000 10:19:00 PM
Proposed changes to section SENDING TRANSACTIONS, subsection Writing a Batch Browser

Page 8, replace the last bulleted paragraph on the page with the following:

The data field containing the GISB standard file has two extra identifiers: first the name of the file sent from the source computer, filename=”c:\temp\smallnom.bin”, and second a content type identifier on a separate line. This line should always be constructed to reflect the content-type of the data being transmitted, in accordance with accepted Internet standards. If the data file contains clear text, X12 data, as shown in the above example, the content-type identifier follows the recommendations of RFC 1767, “MIME Encapsulation of EDI Data”, and the “Content-Type:application/EDI-X12” is used. However, for security purposes it is recommended that all data be encrypted and digitally signed prior to transmission over the Internet. There are IETF standards for describing and packaging encrypted data files, most notably, “MIME Security with Pretty Good Privacy (PGP)”, RFC 2015 and “MIME-based Secure EDI”, RFC TBD.

When the sender of a file intends to use encryption and digital signature functions to secure the contents of a data file the file must be prepared in accordance with the above mentioned IETF standards. ASC X12 data must first be prepared in canonical form as specified in RFC 1767. The ASC X12 data file would be concatenated with the MIME Content-type of application/EDI-X12 as the first line of the file.

For example below is a file before encryption:

```
Content-type: application/EDI-X12
ISA~00~ ~01~AAA6300300~14~1234567890000 ~14~2345678900000
... more data from the X12 file…
IEA~1~000003616
```

This file is encrypted, signed and packaged, which follows EDIINT AS1 and RFC 2015, which produces a file containing MIME headers and encrypted content as follows.

Below is the file after encryption:

```
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"


--8760
Content-Type: application/pgp-encrypted


Version: 1


--8760
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5
```

```
hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHs
z0e8sb7ErC340MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG
lQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/43fkB+al
ATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1E
h785zC03UAw0qg0ugMt86dPeyd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8O
cp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RQbeN
aqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cV
zpb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9
```

```
UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZySaRO8Vtff+
4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
--8760--
```

This file is associated with the “input-data” data element of the multipart-form-data and is sent to the recipient using the HTTP POST method.

The HTTP POST data stream used to send this file would appear as follows:

```
-----------------------------87453838942833
Content-Disposition: form-data; name="from"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="to"

234567890
-----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.4
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-security-selection"

signed-receipt-protocol=required, pgp-signature; signed-receipt-micalg=required, md5
-----------------------------87453838942833
Content-Disposition: form-data; name="input-format"

X12
-----------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename=”c:\temp\smallnom.bin”
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"


--8760
Content-Type: application/pgp-encrypted

Version: 1


--8760
```

```
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHs
z0e8sb7ErC340MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG
lQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/43fkB+al
ATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1E
h785zC03UAw0qg0ugMt86dPeyd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8O
cp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RQbeN
aqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cV
zpb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9
UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZySaRO8Vtff+
4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----

--8760--

-----------------------------87453838942833--
```

Page 44

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:33:45 PM

Proposed changes to section SENDING TRANSACTIONS, subsection Writing a Batch Browser

Page 9, replace the example with the following:

```
POST /cgi-bin/AS2dispatcher HTTP/1.0
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Content-type: multipart/form-data; boundary=---------------------------87453838942833
Content-Length: 5379

-----------------------------87453838942833
Content-Disposition: form-data; name="from"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="to"

234567890
-----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.4
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
```

```
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
-----------------------------87453838942833
Content-Disposition: form-data; name="input-format"

X12
-----------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename=”c:\temp\smallnom.bin”
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"

--8760
Content-Type: application/pgp-encrypted

Version: 1

--8760
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHs
z0e8sb7ErC340MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG
lQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/43fkB+al
ATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1E
h785zC03UAw0qg0ugMt86dPeyd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8O
cp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RQbeN
aqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cV
zpb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9
UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZySaRO8Vtff+
4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
--8760--
-----------------------------87453838942833—
```

Page 45

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 10:21:21 PM
Proposed changes to section RECEIVING TRANSACTIONS, subsection General Flow

Page 10, replace list items 5 and 6 with the following:

5. Create gisb acknowledgement receipt
5.1 If using signed receipts: 5.1.1 Produce a digital signature over the gisb acknowledgement receipt created in step 5 5.1.2 Encapsulate the gisb acknowledgement receipt and Digital Signature body parts in a content-type of application/multipart/signed envelope
6. Return HTTP response, the gisb acknowledgement receipt object, back to server

Page 46

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:19:47 PM
Page 11, Under section RECEIVING TRANSACTIONS, sub-section Writing the CGI Process replace

the line containing "POST C:\execute HTTP/1.0" with "POST /cgi-bin/AS2dispatcher HTTP/1.0"

Page 47

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:37:10 PM
Proposed changes to section RECEIVING TRANSACTIONS, subsection Writing the CGI Process

Page 12, replace the example with the following:

```
-----------------------------87453838942833
Content-Disposition: form-data; name="from"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="to"

234567890
-----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.4
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
-----------------------------87453838942833
Content-Disposition: form-data; name="input-format"

X12
-----------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename=”c:\temp\smallnom.bin”
Content-Type: multipart/encrypted; boundary=8760; protocol="application/pgp-encrypted"

--8760
Content-Type: application/pgp-encrypted

Version: 1

--8760
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
Version: PGP 6.5

hQCMAzRG1pEOIOvdAQP+JMr0m/9+8yOL60Z9Vr6fFV81FCExB/o0xmwiMkiwYsHs
z0e8sb7ErC340MrNA/dw3taGMjmI+CXYRF/PLEdg1NZE1ZCtNeL4YdIHAMLWwODG
lQxhSucz8rMSgQ5mZzcOJwBdWLW70efgsu/9UljuJjYc1uZ6C03eFQv/43fkB+al
ATtgydxX4g8QK664ad+Jo/XUICSmWBL66fqJR1KLeLf4wTaqGy174Aq48Wpwvg1E
h785zC03UAw0qg0ugMt86dPeyd91e2JigqwDYEf/DYEKD0J9BGiGpS/uAupNKj8O
cp2IWClxKOGUbxpVNOnNTqWHS/GntegvDE/7/ewCxDxsnmQS95pOl141QZ1RQbeN
```

```
aqx2Dq/ra9g65HNchOCzjul5Vi8HHf6Yhg2WnROe+npByyCue6rihqgNVOJwj0cV
zpb4JE+gMDf3q4ISUb1Fv7/+SSFHDdnhdC5YTpqf1Bc3B07hiLmtTXqNit31EbX9
UVElObzSa9ZhxbC6/eSl7Nuf5ZTDsh9nrk+QQJ6FeC9W4cqXLj7IZySaRO8Vtff+
4ktqeuhYusT4kSpnk027aw4O/5jomUkfb22CAe4=
=Oiuo
-----END PGP MESSAGE-----
--8760--
-----------------------------87453838942833—
```

Page 48

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:42:50 PM
Proposed changes to section RECEIVING TRANSACTIONS, subsection Writing the CGI Process

Page 13, replace the last paragraph on the page with the following:

Immediately after the CGI validates (as above), parses, and saves the data, the CGI should record the time and construct a gisb acknowledgement receipt described in the following section. This gisb acknowledgement receipt is usually sent from the CGI by writing to the standard output (stdout) of the CGI process. If using signed receipts, the receiving party must produce a digital signature of the gisb acknowledgement receipt and send both the gisb acknowledgement receipt and digital signature body parts within a multipart/signed MIME envelope.

Page 49

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:43:35 PM
Proposed changes to section URL/CGI Implementation Guidelines

Page 14, replace the first sentence in the paragraph starting with “Error Notifications” with the following:

Error notifications include errors that occur some time after the gisb acknowledgement receipt is sent (such as a file decryption error) as well as errors on the transactions.

Page 50

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:44:49 PM
Proposed changes to section URL/CGI Implementation Guidelines, subsection Server Specifications

Page 15, replace the sentence starting with “The HTTP response must be enveloped” with the following:

The gisb acknowledgement receipt must be enveloped in a multipart/report, as specified in EDIINT AS2 following the rules for Generalized Receipts. If signed receipts are used, the gisb acknowledgement receipt (including the multipart/report envelope) is digitally signed, producing a application/pgp-encrypted body part. Both the multipart/report (gisb acknowledgement receipt) and the application/pgp-signature body parts are placed in a multipart/signed envelope and the entire package is returned to the sender.

Annotation 2; Label: Carl P Caldwell; Date: 2/29/2000 8:50:53 AM
Proposed changes to section URL/CGI Implementation Guidelines, subsection Server Specifications

Page 15, remove the sentence “The HTTP response must be no more than 2048 characters

Annotation 3; Label: Carl P Caldwell; Date: 3/7/2000 8:45:24 PM
The HTTP response must be no more than 2048 characters.

Page 51

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 8:46:00 PM
Proposed changes to section URL/CGI Implementation Guidelines, subsection HTTP Response Data Elements

Page 16, replace the example given under “successful, plain text format:” with the following:

```
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--
```

Annotation 2; Label: Carl P Caldwell; Date: 3/7/2000 8:46:21 PM
Proposed changes to section URL/CGI Implementation Guidelines, subsection HTTP Response Data Elements

Page 16, replace the example given under “error, plain text format:” with the following:

```
Content-Type: multipart/report;  report-type="gisb-acknowledgement-receipt";  boundary="GISB7866"

--GISB7866
Content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Error</TITLE></HEAD> <BODY><P>
time-c=19960619082855*
request-status=EEDM106: Invalid To Common Code Identifier*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>
--GISB7866
Content-type: text/plain

time-c=19960619082855*
request-status=EEDM106: Invalid To Common Code Identifier*
server-id=coolhost*
trans-id=234423897*
--GISB7866--
```

Annotation 3; Label: Carl P Caldwell; Date: 3/7/2000 8:46:45 PM
Proposed changes to section URL/CGI Implementation Guidelines, subsection HTTP Response Data Elements

Page 16, replace the example given under “warning, plain text format:” with the following:

```
Content-Type: multipart/report;  report-type="gisb-acknowledgement-receipt";  boundary="GISB7866"

--GISB7866
Content-type: text/html

<HTML><HEAD><TITLE>Acknowledgement Receipt Warning</TITLE></HEAD> <BODY><P>
time-c=19960619082855*
request-status=WEDM100: Transaction Set Sent, Not Mutually Agreed*
server-id=coolhost*
trans-id=234423897*
</P> </BODY></HTML>
--GISB7866
Content-type: text/plain

time-c=19960619082855*
request-status= WEDM100: Transaction Set Sent, Not Mutually Agreed *
server-id=coolhost*
trans-id=234423897*
--GISB7866--
```

Annotation 4; Label: Carl P Caldwell; Date: 3/7/2000 9:03:28 PM
or, as a more elaborate response to a successful transmittal,

Annotation 5; Label: Carl P Caldwell; Date: 3/7/2000 10:24:20 PM
Signed Receipt

```
Content-Type:multipart/signed; micalg=pgp-md5; protocol="application/pgp-signature";
boundary=8760

--8760

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--
--8760
Content-Type: application/pgp-signature

-----BEGIN PGP MESSAGE-----

Version: 2.6.2

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/LC//
JV5bNvkZIGPIcEmI5iFd9boEgvpirHtIREEqLQRkYNoBActFBZmh9GC3C041WGq
uMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfolT9Brn
HOxEa44b+EI=
=ndaj

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

--8760—
```

Page 52

Annotation 1; Label: Carl P Caldwell; Date: 2/29/2000 8:53:42 AM
Proposed changes to section URL/CGI Implementation Guidelines, subsection HTTP Response Data Elements

Page 17, remove the example given under “HTML format”.

Annotation 2; Label: Carl P Caldwell; Date: 3/7/2000 8:48:24 PM
HTML format (this example is for a successful transmittal): <html> <head> <title> Upload OK</ title> </ head> <!-- time- c= 19960123203618*-->_ <!-- request- status= ok* --> <!-- server- id= coolhost* --> <!-- trans- id= 232323897*--> <h1> Upload OK </ h1>< br> <body> <B> File Saved at (time- c): </ B> 19960123203618< br> <B> Status (request- status): </ B> ok< br> <B> Server (server- id): </ B> coolhost< br> <B> Transaction ID (trans- id): </ B> 232323897< br> </ body> </ html>

Page 54

Annotation 1; Label: Carl P Caldwell; Date: 3/1/2000 7:33:53 PM
Proposed changes to section Security , subsection Encryption / Digital Signature . Page 19, new paragraph after the second paragraph

Digital signatures may also be applied, on a mutually agreeable basis, to the HTTP response by the receiver of the transacation.

Annotation 2; Label: Carl P Caldwell; Date: 3/1/2000 7:37:00 PM
Proposed changes to section Security , subsection Decryption / Signature Verification . Page 19, new paragraph after the second paragraph

When digital signatures are applied the HTTP response, on a mutually agreeable basis, the HTTP response received by the sender the transacation may be verified to ensure non-repudiation of receipt of the transaction.

Page 56

Annotation 1; Label: Carl P Caldwell; Date: 2/29/2000 8:55:05 AM
Proposed changes to section Sending Error Notification Transactions, subsection Error Notification

Page 21, insert the following as the last paragraph of the subsection:

“Additionally, trading partners are permitted to utilize digitally signed error notifications, if both parties mutually agree to do so.”

Page 57

Annotation 1; Label: Carl P Caldwell; Date: 2/29/2000 8:55:37 AM
Proposed changes to section Sending Error Notification Transactions, subsection Error Notification Data Elements

Page 22, remove the sentence containing “The entire error notification must be no more than 2048 characters.”

Annotation 2; Label: Carl P Caldwell; Date: 2/29/2000 8:56:13 AM
Proposed changes to section Sending Error Notification Transactions, subsection Error Notification Data Elements

Page 22, replace the paragraph starting with “If an HTML response is given” with the following:

If an error notification is given, a GISB Error Notification contains two body parts nested within a multipart/report outer envelope. The first body part contains human readable content in HTML. The second body part contains machine readable content in HTML. Additionally, consenting trading partners can mutually agree to digitally sign error notifications. If digital signatures are used, the multipart/report containing the GISB Error Notification is used to create a digital signature body part, identified by a content-type of application/pgp-signature. Both the multipart/report GISB Error Notification and application/pgp-encrypted digital signature body parts are combined in a multipart/signed envelope.

Annotation 3; Label: Carl P Caldwell; Date: 3/7/2000 8:49:40 PM
The entire error notification must be no more than 2048 characters.

Page 58

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 10:27:48 PM
Proposed changes to section Sending Error Notification Transactions, subsection Error Notification Data Elements

Page 23, replace the example given under Error Notification Example with the following:

```
POST /cgi-bin/AS2dispatcher HTTP/1.0
Referer: http://www.get.a.life/upl.htm
Connection: Keep-Alive
User-Agent: brow v0.1 XYZ Corp.
Host: localhost
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, */*
Content-type: multipart/form-data; boundary=---------------------------87453838942833
Content-Length: 1958
-----------------------------87453838942833
Content-Disposition: form-data; name="from"
```

```
234567890
-----------------------------87453838942833
Content-Disposition: form-data; name="to"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="version"

1.4
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-disposition-to"

123456789
-----------------------------87453838942833
Content-Disposition: form-data; name="receipt-report-type"

gisb-acknowledgement-receipt
-----------------------------87453838942833
Content-Disposition: form-data; name="input-format"

error
-----------------------------87453838942833
Content-Disposition: form-data; name="input-data"; filename=”c:\temp\error.not”
Content-Type: multipart/report;  report-type="gisb-error-notification";  boundary="GISB7868"

--GISB7868
Content-type: text/html

<HTML><HEAD><TITLE>Error Notification</TITLE></HEAD> <BODY><P>
orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*
</P> </BODY></HTML>

--GISB7868
Content-Type: text/plain

orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*
--GISB7868--
-----------------------------87453838942833--
```

Annotation 2; Label: Carl P Caldwell; Date: 3/7/2000 10:26:51 PM

Signed Error Notification

```
Content-Type:multipart/signed; micalg=pgp-md5; protocol="application/pgp-signature";
boundary=8760

--8760

Content-Type: multipart/report;  report-type="gisb-error-notification";  boundary="GISB7868"

--GISB7868
Content-type: text/html

<HTML><HEAD><TITLE>Error Notification</TITLE></HEAD> <BODY><P>
orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*

</P> </BODY></HTML>

--GISB7868
Content-Type: text/plain

orig-from=123456789*
orig-to=234567890*
orig-input-format=X12*
resp-time-c=19960619102855*
resp-server-id=coolhost*
resp-trans-id=234423897*
request-status=EEDM601: Public Key Invalid*
comments=Please contact 1-800-555-1212 for correct public key*

--GISB7868--
--8760

Content-Type: application/pgp-signature
-----BEGIN PGP MESSAGE-----

Version: 2.6.2

iQCVAwUBMJrRF2N9oWBghPDJAQE9UQQAtl7LuRVndBjrk4EqYBIb3h5QXIX/LC//
JV5bNvkZIGPIcEmI5iFd9boEgvpirHtIREEqLQRkYNoBActFBZmh9GC3C041WGq
uMbrbxc+nIs1TIKlA08rVi9ig/2Yh7LFrK5Ein57U/W72vgSxLhe/zhdfolT9Brn
HOxEa44b+EI=
=ndaj

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

--8760--
```

Page 63

Annotation 1; Label: Carl P Caldwell; Date: 3/7/2000 9:43:52 PM
Proposed changes to Table A - Internet EDM Standard Error Codes and Messages, subsection Internet EDM Standard Error Codes and Messages

Pages 27-28, add the following error codes and messages to the Internet EDM Standard Error Codes and Messages table:

Validation Code: EEDM110
Description: Invalid “version”
Data Element: version
Required vs. Mutually Agreed: required

Validation Code: EEDM111
Description: Missing "version"
Data Element: version
Required vs. Mutually Agreed: required

EEDM112 "receipt-security-selection" not mutually agreed
receipt-security-selection
mutually agreed
WEDM102 "receipt-security-selection" not mutually agreed
receipt-security-selection
mutually agreed
EEDM113
Invalid "receipt-security-selection"
receipt-security-selection
mutually agreed

EEDM114
Missing "receipt-disposition-to"
receipt-disposition-to
required

EEDM115
Invalid "receipt-disposition-to"
receipt-disposition-to
required

EEDM116
Missing "receipt-report-type"
receipt-report-type
required
EEDM117
Invalid "receipt-report-type"
receipt-report-type
required

EEDM118
Missing "receipt-security-selection"

receipt-security-selection
mutually agreed
WEDM103
Missing "receipt-security-selection"
receipt-security-selection
mutually agreed

TO: GISB Contracts Subcommittee

FROM: GISB EDM Subcommittee

Date: March 23, 2000

Re: AS2 affect on the TPA

As a result of processing Request No. R99035 from Group 8760 the EDM subcommittee is recommending the adoption of certain changes in order to address the business needs for privacy, authentication, integrity and non-repudiation of Origin and Receipt as specified in “HTTP Transport for Secure EDI” (a.k.a. EDIINT AS2). The EDIINT AS2 modifications to the GISB EDM protocol allow trading partners to mutually agree to implement signed receipts. To implement signed receipts the receiving party must digitally sign the gisb-acknowledgement-receipt and encapsulate the gisb-acknowledgement-receipt and digital signature body parts within a MIME envelope with a content-type of application/pgp-signature. Additionally the GISB EDM recommended changes permit trading partners to utilize digitally signed error notifications, if both parties mutually agree to do so. If digital signatures are used, the multipart/report containing the gisb error notification is used to create a digital signature body part, identified by a content-type of application/pgp-signature. Both the multipart/report gisb error notification and application/pgp-encrypted digital signature body parts are combined in a multipart/signed envelope.

When reviewing these proposed changes the EDM subcommittee raised the issue of whether the adoption of EDIINT AS2 requires modification to the Trading Partner Agreement, GISB Standard No. 6.3.3 (TPA). The following areas of the TPA may need to be revised to permit the trading partners to specify their mutual agreement to the use of signed receipts and the specific implementation of such use:

1. Review of terminology throughout the TPA (for example HTTP response, time-c, etc.)
2. Section 2.2 Digital Signature Verification and Decryption
3. Section 2.3 Functional Acknowledgement and Response Document
4. Exhibit (Transaction Set Exhibit), Section 4.

The above list is not intended to be an inclusive list.

4. SUPPORTING DOCUMENTATION

a. Description of Request:

Review and recommend changes to the existing body of EDM standards to support standards convergence across other standards setting groups, such as AIAG, UIG, and EDI-INT.

b. Description of Recommendation:

Electronic Delivery Mechanism Subcommittee

Motion: The AS2 convergence work paper will be sent to the FTTF for their meeting on February 16th. The FTTF will review the work paper to verify the technical specification and examples. In addition, FTTF should review the work paper to verify that the changes do not require any mandatory changes to business practices between trading partners.

Sense of the Room: **1/21/2000** 16 In Favor 0 Opposed

Future Technology Taskforce

Motion: Based of FTTF's review, version 2.1 (will become version 2.2 with changes), the AS2 document is technically acceptable.

Sense of the Room: **2/16/2000** 15 In Favor 0 Opposed

Electronic Delivery Mechanism Subcommittee

Motion: Adopt the AS2 work paper, as posted and with above changes, as a the EDM Subcommittee recommendation to the Executive Committee as to support standards convergence with the Internet Engineering Taskforce EDIINT standard AS2.

Sense of the Room: **3/23/2000** 10 In Favor 0 Opposed

Motion: Adopt the instruction, as modified, to the Contracts Subcommittee regarding the changes which may be needed in the GISB standard Trading partner Agreement.

Sense of the Room: **3/23/2000** 11 In Favor 0 Opposed

c. Business Purpose:

There are business benefits gained from adherence to "HTTP Transport for Secure EDI" (a.k.a. IETF EDIINT AS2) such as allowing potential to more readily, electronically trade with others (e.g., electric utilities, banks, suppliers, retail customers), making it more likely that packages can be purchased to replace custom written apps currently in place to support GISB EDM and strengthening the surety of receipt and error notification

HTTP Transport for Secure EDI (AS2) is an emerging standard, largely based on the original GISB EDM, that is being developed by the Internet Engineering Task Force, the Internet standards body. Adherence with a formal, international Internet standard, such as AS2 ensures that the specification will not change without due process and any changes that do occur will be the result of a broad consensus. Individual companies and entire industries are free to use as much or as little of AS2 as they see fit, providing the maximum flexibility to meet business needs.

d. Commentary/Rationale of Subcommittee(s)/Task Force(s):

The technical specifications of the EDI/EDM method of communication have been modified to comply with a the broader "HTTP Transport for Secure EDI" standard being developed by the Internet Engineering Task force (IETF). These technical changes do not impact the underlying required business practices established by GISB. In addition, the security features of the EDI/EDM and batch FF/EDM communication method now includes mutually agreeable business practices to protect the sender of a document from non-repudiation and to digitally sign Error Notifications.