Individual Submission
Internet-Draft
Intended status: Informational
Expires: December 31, 2011

K. Meadors, Ed.
Drummond Group Inc.

June 29, 2011

Multiple Attachments for EDI-INT
draft-meadors-multiple-attachments-ediint-14

Abstract

The EDI-INT AS1, AS2 and AS3 messages were designed specifically for the transport of EDI documents. Since multiple interchanges could be placed within a single EDI document, there was not a need for sending multiple EDI documents in a single message. As adoption of EDI-INT grew, other uses developed aside from single EDI document transport. Some transactions required multiple attachments to be interpreted together and stored in a single message. This informational draft describes how multiple documents, including non-EDI payloads, can be attached and transmitted in a single EDI-INT transport message. The attachments are stored within the MIME Multipart/Related structure. A minimal list of content-types to be supported as attachments is provided.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on December 31, 2011.

Table of Contents

1. Introduction

The primary work of EDI-INT was to develop a secure means of transporting EDI documents over the Internet. This was described in the three working group developed standards for secure transport over SMTP AS1 [RFC3335], HTTP AS2 [RFC4130] and FTP AS3 [RFC4823]. For most uses of EDI, all relevant information to complete a single business transaction could be stored in a single document. As adoption of EDI-INT grew, new industries and businesses began using AS2 and needing to include multiple documents in a single message to complete a trading partner transaction. These documents were a variety of MIME media types. This informational draft describes how to use the MIME multipart/related body structure within EDI-INT messages to store multiple document attachments. Details of computing the MIC value over this body are covered. A minimum listing of MIME media types to support within the multipart/related body is given along with information on extracting these documents.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Using Multiple-Attachments in EDI-INT

2.1. Multipart/Related Structure

Multiple payload attachments for EDI-INT messages are stored within a multipart/related MIME body [RFC2387]. The multipart/related structure allows an multiple number of MIME attachments or message payloads to be communicated in a single structure and message.

The attached payloads can be of any MIME content-type depending on the trading partner agreement, but section 2.4 lists the content-types which MUST be supported. The use and format of the multipart/related body follows the rules in RFC 2387, including the required type parameter to determine the root body part. The use of the optional start parameter is RECOMMENDED.

2.2. EDI-INT Features Header

To indicate support for multiple-attachments (MA), an EDI-INT application MUST use the EDI-INT Features header [RFC6017]. The Feature Header indicates the instance application can support various features, such as certification exchange. The header is present in all messages from the instance application, not just those which

feature certification exchange.

For applications implementing multiple attachments, the MA-Feature-Name MUST be used within the EDI-INT Features header as listed in this ABNF [RFC5234] syntax:

```
MA-Feature-Name = "multiple-attachments"
```

An example of the EDI-INT Features header in a message from an application supporting MA:

```
EDIINT-Features: multiple-attachments
```

2.3. MIC Calculation

MIC calculation in an EDI-INT message with multiple attachments is performed in the same manner as for a single EDI payload. The only difference is calculating the message integrity check (MIC) over the whole multipart/related body rather than a single EDI payload. Section 5.2.1 of AS1 [RFC3335] and section 2 of EDIINT COMPRESSION [RFC5402] describe the MIC calculations used for single payload document within an EDI-INT message. The approach is summerized below for multipart/related. Refer to stated sections above for more details.

For a compressed but unsigned message, regardless of encryption, the MIC is calculated over the uncompressed multipart/related body including any applied Content-Transfer-Encoding. The body MUST be canonicalized according to the procedure described in the underlying transport protocol (e.g. HTTP AS2 [RFC4130]) before the MIC is calculated.

For an encrypted but unsigned and uncompressed message, the MIC is calculated on the decrypted multipart/related body, including header and all attached documents. The body MUST be canonicalized according to the procedure described in the underlying transport protocol (e.g. HTTP AS2 [RFC4130]) before the MIC is calculated.

For an unsigned and unencrypted message, the MIC is calculated over the data inside the multipart/related boundaries prior to Content-Transfer-Encoding. However, unsigned and unencrypted messages SHOULD NOT be sent due to lack of security.

If the expected MIC value differs from the calculated MIC value, all attachments MUST be considered invalid and retransmitted.

2.4. Document Processing

Upon receipt of an EDI-INT message with multiple attachments, the receiving user agent MUST be able to extract the attached payloads from the message rather than only removing the multipart/related body from the message. The storing or processing of the documents as they relate to the pending transaction is implementation dependent.

2.5. Content-Types to Support

Documents of the following MIME media types MAY be found in a multipart/related body and MUST be accepted by the user agent. However, any media type can be used depending upon industry need, and other media types MAY be accepted depending upon trading partner agreement.

application/xml

application/pdf

application/msword

application/vnd.ms-excel, application/x-msexcel

application/rtf

application/octet-stream

application/zip

image/bmp

image/gif

image/tiff

image/jpeg

text/plain

text/html

text/rtf

text/xml

3. Example Message

Here is an example AS2 message which uses two attachments. The first attachment is an XML document which is the root attachment, and the second attachment is a PDF document. For both the XML and PDF documents as well as the applied digital signature, their content has been omitted for size consideration. This example is provided as an illustration only and is not considered part of the specification. If the example conflicts with the definitions specified above or in the other referenced RFCs, the example is considered invalid.

```
POST /as2 HTTP/1.1
Host: www.example.com:8080
Connection: Close, TE
Message-ID: <1109712943488@10.65.122.242>
Subject: Multiple Attachment Example
Date: Tue, 01 Mar 2005 21:37:03 GMT
AS2-To: TradingPartner
AS2-From: User
AS2-Version: 1.2
EDIINT-Features: multiple-attachments
Disposition-Notification-To: http://www.example.com/as2
Disposition-Notification-Options:
   signed-receipt-protocol=optional,pkcs7-signature;
   signed-receipt-micalg=optional,sha1
Content-type: multipart/signed;
   protocol="application/pkcs7-signature"; micalg=sha1;
   boundary="OUTER-BOUNDARY"
Content-length: 207440

--OUTER-BOUNDARY
Content-Type: Multipart/Related; boundary="INNER-BOUNDARY";
   start="<root.attachment>"; type="application/xml"

--INNER-BOUNDARY
Content-Type: application/xml
Content-ID: <root.attachment>

[XML DOCUMENT]

--INNER-BOUNDARY
Content-Type: application/pdf
Content-ID: <2nd.attachment>

[PDF DOCUMENT]

--INNER-BOUNDARY--

--OUTER-BOUNDARY
Content-Type: application/pkcs7-signature

[DIGITAL SIGNATURE]

--OUTER-BOUNDARY--
```

4. Security Considerations

Multiple attachments have very similar security concerns to what is described in the three EDI-INT transport standards. This includes the importance of using strong cryptography and the necessity of using valid certificates and chaining to a trusted CA. Please refer to these standards SMTP AS1 [RFC3335], HTTP AS2 [RFC4130] and FTP AS3 [RFC4823] for details of their security considerations.

The only additional security consideration is that if the MIC calculation by user agent differs from expected MIC calculation, all the attached documents MUST be considered invalid. Because the MIC calculation is over the multipart/related body, the MIC validates the content-integrity of all the documents.

5. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2387] Levinson, E., "The MIME Multipart/Related Content-type", RFC 2387, August 1998.

[RFC3335] Harding, T., Drummond, R., and C. Shih, "MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet", RFC 3335, September 2002.

[RFC4130] Moberg, D. and R. Drummond, "MIME-Based Secure Peer-to-Peer Business Data Interchange Using HTTP, Applicability Statement 2 (AS2)", RFC 4130, July 2005.

[RFC4823] Harding, T. and R. Scott, "FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet", RFC 4823, April 2007.

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[RFC5402] Harding, T., "Compressed Data within an Internet Electronic Data Interchange (EDI) Message", RFC 5402, February 2010.

[RFC6017] Meadors, K., "Electronic Data Interchange - Internet Integration (EDIINT) Features Header Field", RFC 6017, September 2010.

Author's Address

Kyle Meadors (editor)
Drummond Group Inc.
Nashville, Tennessee 37221
US

Phone: +1 (817) 709-1627
Email: kyle@drummondgroup.com