Independent Submission
Request for Comments: 5402
Category: Informational
ISSN: 2070-1721

T. Harding, Ed.
Axway

February 2010

Compressed Data within an Internet Electronic Data Interchange (EDI) Message

Abstract

This document explains the rules and procedures for utilizing compression (RFC 3274) within an Internet EDI (Electronic Data Interchange) 'AS' message, as defined in RFCs 3335, 4130, and 4823.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This is a contribution to the RFC Series, independently of any other RFC stream. The RFC Editor has chosen to publish this document at its discretion and makes no statement about its value for implementation or deployment. Documents approved for publication by the RFC Editor are not a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5402.

IESG Note

The content of this RFC was at one time considered by the IETF, and therefore it may resemble a current IETF work in progress or a published IETF work. This RFC is not a candidate for any level of Internet Standard. Readers of this RFC should exercise caution in evaluating its value for implementation and deployment.

Copyright Notice

carefully, as they describe your rights and restrictions with respect to this document.

1. Introduction

Historically, electronic messages produced by systems following the guidelines as outlined in the IETF EDIINT Working Group specifications AS1 [AS1], AS2 [AS2], and AS3 [AS3] did not have a way to provide a standardized transport neutral mechanism for compressing large payloads. However, with the development of RFC 3274, "Compressed Data Content Type for Cryptographic Message Syntax (CMS)", we now have a transport-neutral mechanism for compressing large payloads.

A typical EDIINT 'AS' message is a multi-layered MIME message, consisting of one or more of the following: payload layer, signature layer, and/or encryption layer. When an 'AS' message is received, a Message Integrity Check (MIC) value must be computed based upon defined rules within the EDIINT 'AS' RFCs and must be returned to the sender of the message via a Message Disposition Notification (MDN).

The addition of a new compression layer will require this document to outline new procedures for building/layering 'AS' messages and computing a MIC value that is returned in the MDN receipt.

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 [RFC2119].

2. Compressed Data MIME Layer

The compressed-data CMS (Cryptographic Message Syntax) MIME entity as described in [COMPRESSED-DATA] may encapsulate a MIME entity that consists of either an unsigned or signed business document.

Implementers are to follow the appropriate specifications identified in the "MIME Media Types" registry [MIME-TYPES] maintained by IANA for the type of object being packaged. For example, to package an XML object, the MIME media type of "application/xml" is used in the Content-Type MIME header field and the specifications for enveloping the object are contained in [XMLTYPES].

MIME entity example:

```
Content-type: application/xml; charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<!-- sample xml document -->
```

The MIME entity will be compressed using [ZLIB] and placed inside a CMS compressed-data object as outlined in [COMPRESSED-DATA]. The compressed-data object will be MIME encapsulated according to details outlined in [S/MIME3.1], RFC 3851, Section 3.5.

Example:

```
Content-Type: application/pkcs7-mime; smime-type=compressed-data;
name=smime.p7z
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7z

MIAGCyqGSIb3DQEJEAEJoIAwgAIBADANBgsqhkiG9w0BCRADCDCABgkqhkiG9w0BBwGg
Hnic7ZRdb9owFIbvK/k/5PqVYPFXGK12YYyboVFASSp1vQtZGiLRACZE49/XHoUW7S/0
fU5ivWnasml72XFb3gb5druui7ytN803M570nii7C5r8tfwR281hy/p/KSM3+jzH5s3+
P3VT3QbLusnt8WPIuN5vN/vaA2+DulnXTXkXvNTr8j8ouZmkCmGI/UW+ZS/C8zP0bz2d
UEk2M8mlaxjRMByAhZTj0RGYg4TvogiRASROsZgjpVcJCb1KV6QzQeDJ1XkoQ5Jm+C5P
v+ORAcshOGeCcdFJyfgFxdtCdEcmOrbinc/+BBMzRThEYpwl+jEBpciSGWQkI0TSlREm
SGLuESm/iKUFt1y4XHBO2a5oq0IKJKWLS9kUZTA7vC5LSxYmgVL46SIWxIfWBQd6Adrn
vGxVibLqRCtIpp4g2qpdtqK1LiOeolpVK5wVQ5P7+QjZAlrh0cePYTx/gNZuB9Vhndtg
W9ogK+3rnmg3YWygnTuF5GDS+Q/jIVLnCcYZFc6Kk/+c80wKwZjwdZIqDYWRH68MuBQS
3CAaYOBNJMliTl0X7eV5DnoKIFSKYdj3cRpD/cK/JWTHJRe76MUXnfBW8m7Hd5zhQ4ri
+kV1/3AGSlJ32bFPd2BsQD8uSzIx6lObkjdz95c0AAAAAAAAAAAAAAAA
```

Note: Content-Transfer-Encoding of base64 would only be required if the compressed-data MIME bodypart is transferred via a 7-bit protocol like SMTP and is visible in the outer layer of the MIME message. If the compressed-data MIME bodypart is placed inside of an encrypted MIME bodypart, content-transfer-encoding would not be required on the compressed-data MIME bodypart, but would be required on the encrypted MIME bodypart.

3. Structure of an EDI MIME Compressed Message

When compressing a document that will be signed, the application MAY compress the innermost MIME body before signing (see Sections 3.2 and 3.5), or it MAY compress the outer multipart/signed MIME body (see Sections 3.3 and 3.6), but it MUST NOT do both within the same document. The receiving application MUST support both methods of compression when unpackaging an inbound document.

Note: The following sections (3.1 - 3.6) show the individual layers of a properly formatted EDI MIME message with a compressed data layer. Please refer to the appropriate RFCs for the proper construction of the resulting MIME message. "application/xxxxxxx" is used to indicate an application media subtype.

3.1. No Encryption, No Signature

```
-RFC5322/2045
  -[COMPRESSED-DATA](application/pkcs7-mime)
    -[MIME-TYPES](application/xxxxxxx)(compressed)
```

This section shows the layers of an unsigned, unencrypted compressed message. The first line indicates that the MIME message conforms to [RFC5322] and [RFC2045] with a Content-Type of application/pkcs7-mime. Within the pkcs7-mime entity is a compressed MIME entity containing the electronic business document.

3.2. No Encryption, Signature

```
-RFC5322/2045
  -[RFC1847] (multipart/signed)
    -[COMPRESSED-DATA](application/pkcs7-mime)
      -[MIME-TYPES](application/xxxxxxx)(compressed)
    -RFC3851 (application/pkcs7-signature)
```

This section shows the layers of a signed, unencrypted compressed message where the payload is compressed before being signed.

3.3. No Encryption, Signature

```
-RFC5322/2045
  -[COMPRESSED-DATA](application/pkcs7-mime)
    -[RFC1847] (multipart/signed)(compressed)
      -[MIME-TYPES](application/xxxxxxx)(compressed)
      -RFC3851 (application/pkcs7-signature)(compressed)
```

This section shows the layers of a signed, unencrypted compressed message where a signed payload is compressed.

3.4. Encryption, No Signature

```
-RFC5322/2045
  -RFC3851 (application/pkcs7-mime)
    -[COMPRESSED-DATA](application/pkcs7-mime) (encrypted)
      -[MIME-TYPES](application/xxxxxxx)(compressed)(encrypted)
```

This section shows the layers of an unsigned, encrypted compressed message where the payload is compressed before it is encrypted.

3.5. Encryption, Signature

```
-RFC5322/2045
  -RFC3851 (application/pkcs7-mime)
    -[RFC1847] (multipart/signed) (encrypted)
      -[COMPRESSED-DATA](application/pkcs7-mime) (encrypted)
        -[MIME-TYPES](application/xxxxxxx) (compressed)(encrypted)
      -RFC3851 (application/pkcs7-signature) (encrypted)
```

This section shows the layers of a signed, encrypted compressed message where the payload is compressed before being signed and encrypted.

3.6. Encryption, Signature

```
-RFC5322/2045
  -RFC3851 (application/pkcs7-mime)
    -[COMPRESSED-DATA](application/pkcs7-mime) (encrypted)
      -[RFC1847] (multipart/signed) (compressed)(encrypted)
        -[MIME-TYPES](application/xxxxxxx) (compressed)(encrypted)
        -RFC3851 (application/pkcs7-signature)(compressed)(encrypted)
```

This section shows the layers of a signed, encrypted compressed message where the payload is signed before being compressed and encrypted.

4. MIC Calculations for Compressed Messages Requesting Signed Receipts

4.1. MIC Calculation for Signed Message

For any signed message, the MIC to be returned is calculated over the same data that was signed in the original message as per [AS1]. The signed content will be a MIME bodypart that contains either compressed or uncompressed data.

4.2. MIC Calculation for Encrypted, Unsigned Message

For encrypted, unsigned messages, the MIC to be returned is calculated over the uncompressed data content including all MIME header fields and any applied Content-Transfer-Encoding.

4.3. MIC Calculation for Unencrypted, Unsigned Message

For unsigned, unencrypted messages, the MIC is calculated over the uncompressed data content including all MIME header fields and any applied Content-Transfer-Encoding.

5. Error Disposition Modifier

For a received message where a receipt has been requested and decompression fails, the following disposition modifier will be returned in the signed MDN.

"Error: decompression-failed" - the receiver could not decompress the message

6. EDIINT Version Header Field

Any application that supports the compression methods outlined within this document MUST use a version identifier value of "1.1" or greater within the AS2 or AS3 Version header field as describe in [AS2] and [AS3].

7. Compression Formats

Implementations MUST support ZLIB [ZLIB], which utilizes DEFLATE [DEFLATE].

8. Security Considerations

This document is not concerned with security, except for any security concerns mentioned in the referenced RFCs.

9. Normative References

[AS1] Harding, T., Drummond, R., and C. Shih, "MIME-based Secure Peer-to-Peer Business Data Interchange over the Internet", RFC 3335, September 2002.

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

[AS3] Harding, T. and R. Scott, "FTP Transport for Secure Peer-to-Peer Business Data Interchange over the Internet", RFC 4823, April 2007.

[ZLIB] Deutsch, P. and J-L. Gailly, "ZLIB Compressed Data Format Specification version 3.3", RFC 1950, May 1996.

[DEFLATE] Deutsch, P., "DEFLATE Compressed Data Format Specification version 1.3", RFC 1951, May 1996.

[MIME-TYPES] IANA, "MIME Media Types" registry, available from http://www.iana.org.

[RFC1847] Galvin, J., Murphy, S., Crocker, S., and N. Freed, "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, November 1996.

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

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, October 2008.

[S/MIME3.1] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, January 2010.

[XMLTYPES] Murata, M., St. Laurent, S., and D. Kohn, "XML Media Types", RFC 3023, January 2001.

[COMPRESSED-DATA] Gutmann, P., "Compressed Data Content Type for Cryptographic Message Syntax (CMS)", RFC 3274, June 2002.

10. Acknowledgments

A number of the members of the EDIINT Working Group have also worked very hard and contributed to this document. The following people have made direct contributions to this document:

David Fischer, Dale Moberg, Robert Asis, and everyone involved in the AS1, AS2 Interop testing during 2002.

Author’s Address

Terry Harding
Axway
Scottsdale, Arizona
USA

EMail: tharding@us.axway.com