Draft G. Monroe
C. Howells
JanRain
December 6, 2006

OpenID DTP Messages 1.0 - Draft 03

Abstract

This document describes the process of creating and verifying DTP messages. A DTP message is a MIME message that includes the identifiers of the sender and recipients and is then signed and optionally encrypted using S/MIME.

Table of Contents

---

1. Requirements Notation

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] (Bradner, B., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).

---

2. Terminology

Identifier:
: An Identifier is a URL or XRI.

User:

Either a sender or recipient of messages. Users are represented within this protocol by Identifiers.

3. Introduction

Several applications require secure messaging between Users. This document describes a message format that includes sender and recipient information that allows for message verification. MIME [RFC2045] (Freed, N. and N. Borenstein, “Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies,” November 1996.) is used to encapsulate a payload and S/MIME [RFC3851] (Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” July 2004.) is used for signing and encryption.

This document defines the syntax for three MIME headers as well as how to use these headers to verify signatures and decrypt messages. How messages are delivered is beyond the scope of this document.

4. Syntactic Notation

This standard uses the Augmented Backus-Naur Form (ABNF) notation specified in [RFC2234] (Crocker, D. and P. Overell, “ABNF for Syntax Specifications,” November 1997.) for the formal definitions of the syntax of headers.

The following definition is used in the definition of the syntax of headers described in this document:

```
FWS     =     ([*WSP CRLF] 1*WSP)   ; Folding white space
```

5. Headers

5.1. The Dtp-Sender Header

In order to identify the User sending a message, the Dtp-Sender header is defined. The value of this header contains the Identifier of the sending user.

The syntax for the Dtp-Sender header is

```
dtp-sender  =  "Dtp-Sender:" [FWS] absoluteURI [FWS] CRLF
```

where absoluteURI is restricted to the syntax defined in [RFC2396] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifiers (URI): Generic Syntax,” August 1998.).

5.2. The Dtp-Recipients Header

In order to identifier the Users intended to receive a message, the Dtp-Recipients header is defined. The value of this header contains a list of the Identifiers of the recipients.

The syntax for the Dtp-Recipients header is

```
dtp-recipients   =  "Dtp-Recipients:" angle-identifier-list CRLF

angle-identifier =  [FWS] "<" absoluteURI ">" [FWS]

angle-identifier-list  = (angle-identifier *("," angle-identifier))
```

As in the Dtp-Sender header definition, absoluteURI is restricted to the syntax defined in [RFC2396] (Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifiers (URI): Generic Syntax,” August 1998.).

5.3. The Dtp-Recipient-Fingerprints Header

The encrypted message MUST have a Dtp-Recipient-Fingerprints MIME header which contains the SHA-1 fingerprint of each recipient's certificate. The value should be a series of colon-separated hex-encoded octets.

The syntax for the Dtp-Recipient-Fingerprints header is

```
dtp-recipient-fingerprints = "Dtp-Recipient-Fingerprints:" fplst CRLF
fplst                      = FWS fp *("," FWS fp) [FWS]
fp                         = 2HEXDIG 19(":" 2HEXDIG)
```

6. Messages

A DTP message is any MIME message containing both a Dtp-Sender header and a Dtp-Recipients header. Before a message is sent, it is signed and optionally encrypted using S/MIME as described in [RFC3851] (Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” July 2004.).

6.1. Message Signing

Before a DTP MIME message is signed, it must be canonicalized as per [RFC3851] (Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” July 2004.).Then it must be wrapped in a MIME message with a single header: "Content-Type: message/rfc822". This ensures that the Dtp-Signer and Dtp-Recipients headers are included in the S/MIME signature.

Here is a sample message after canonicalization but before signing:

```
Content-Type: message/rfc822
MIME-Version: 1.0
```

```
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Dtp-Sender: http://joe.example.com/
Dtp-Recipients: <http://bob.example.com/>, <xri://@Example=Sue>

Hello, world!
```

S/MIME allows for several ways to sign a MIME message. DTP implementations MUST use the "multipart/signed" format described in section 3.4.3 of [RFC3851] (Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” July 2004.).

Here is the sample message above after signing:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
  protocol="application/x-pkcs7-signature";
  micalg=sha1; boundary="----5B3A27555DFD2976DF0FD80CE5810DCE"

This is an S/MIME signed message

------5B3A27555DFD2976DF0FD80CE5810DCE
Content-Type: message/rfc822
MIME-Version: 1.0

Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Dtp-Sender: http://joe.example.com/
Dtp-Recipients: <http://bob.example.com/>, <xri://@Example=Sue>

Hello, world!

------5B3A27555DFD2976DF0FD80CE5810DCE
Content-Type: application/x-pkcs7-signature; name="smime.p7s"
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="smime.p7s"

MIIEGAYJKoZIhvcNAQcCoIIECTCCBAU...UCWswF07WtoMPdd+xsdjJXUgM=

------5B3A27555DFD2976DF0FD80CE5810DCE--
```

6.2. Message Encryption

Encrypted DTP messages are S/MIME Enveloped-only messages, as described in section 3.3 of [RFC3851] (Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” July 2004.). DTP implementations must support AES as described in [RFC3565] (Schaad, J., “Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS),” July 2003.) for encryption and decryption.

An additional Dtp-Recipient-Fingerprints header, as described above, MUST be added to S/MIME envelope. This header MUST include the SHA-1 fingerprints of the certificates for all message recipients.

Sample message after encryption.

```
MIME-Version: 1.0
Content-Disposition: attachment; filename="smime.p7m"
Content-Type: application/x-pkcs7-mime;
   smime-type=enveloped-data; name="smime.p7m"
Content-Transfer-Encoding: base64
Dtp-Recipient-Fingerprints:
   1A:C0:5A:8E:DE:BD:41:83:38:05:CD:97:16:E0:72:93:D2:70:31:83,
   03:3F:CC:CC:CA:9F:C0:B5:62:BC:44:FD:1C:E9:3E:14:06:83:27:9B

MIIK0AYJKoZIhvcNAQcDoIIKwTCC...a/uiPg65KdkSajemd
```

7. Handling Received Messages

When a messages is received, it should be decrypted and validated. After that, use is application-specific.

7.1. Message Decryption

DTP Messages are S/MIME Enveloped-only messages. The Dtp-Recipient-Fingerprints header contains the fingerprints of the certificates to which the message is encrypted. Each certificate fingerprint listed can be used to identify a private key that can be used to decrypt the message.

7.2. Signature Verification

Once a message is decrypted the senders signature must be verified. Since the signed message is in "multipart/signed" format, the Dtp-Sender header can be easily retrieved. The sender's identifier is used to discover the sender's X.509 certificate from an application specific XRDS Service element as described in [KeyDiscovery] (Monroe, G. and C. Howells, “OpenID Service Key Discovery 1.0 - Draft 01,” December 2006.). The certificate is then used to verify the S/MIME signature over the DTP MIME message.

8. Normative References

[KeyDiscovery] Monroe, G. and C. Howells, “OpenID Service Key Discovery 1.0 - Draft 01,” December 2006 (HTML, TXT).

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

[RFC2119] Bradner, B., “Key words for use in RFCs to Indicate Requirement Levels,” RFC 2119, March 1997.

[RFC2234] Crocker, D. and P. Overell, “ABNF for Syntax Specifications,” RFC 2234, November 1997.

[RFC2396] Berners-Lee, T., Fielding, R., and L. Masinter, “Uniform Resource Identifiers (URI): Generic Syntax,” RFC 2396, August 1998.

[RFC3565] Schaad, J., “Use of the Advanced Encryption Standard (AES) Encryption Algorithm in Cryptographic Message Syntax (CMS),” RFC 3565, July 2003.

[RFC3851] Ramsdell, B., “Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification,” RFC 3851, July 2004.

Authors' Addresses

Grant Monroe
JanRain, Inc.
5331 SW Macadam Avenue
Suite #375
Portland, OR 97239
USA
Email: grant@janrain.com

Carl Howells
JanRain, Inc.
5331 SW Macadam Avenue
Suite #375
Portland, OR 97239
USA
Email: chowells@janrain.com