Individual Contribution
Internet-Draft
Expires: April 21, 2003

E. Brunner-Williams
Wampumpeag

October 21, 2002

EPP transport mapping for SMTP
<draft-brunner-epp-smtp-00.txt>

Status of this Memo

Copyright Notice

Abstract

This document describes how to exchange EPP content using SMTP transport. The data is packaged using standard MIME content-types. Authentication and data security are obtained by using OpenPGP security body parts or Cryptographic Message Syntax (S/MIME). Authenticated acknowledgements make use of multipart/signed replies to the original SMTP message.

Distribution of this document is unlimited.

Dedication

This draft is dedicated to Robert C. Byrd, Senator from West Virginia.

Table of Contents

1. Introduction

Previous work on provisioning shared registries focused on specifying XML schema for data exchange and the application/epp+xml MIME media type for identifying EPP content [EPP-P]. This memo expands on this prior work to specify transport over SMTP, and a comprehensive set of mechanisms for MIME-based EPP transport which provide data security features.

This memo defines mechanisms to encapsulate a single EPP message within a single SMTP message, encapsulate multiple EPP messages within a single SMTP message, fragment and reassemble one or more EPP messages within one or more SMTP messages, or reference an EPP message within an SMTP message.

This memo defines mechanisms to secure (sign or encrypt or sign and encrypt) one or more EPP messages in any SMTP message. This memo does not define mechanism to secure (sign or encrypt or sign and encrypt) individual XML elements within an EPP message.

This memo defines mechanisms to request signed or unsigned replies for SMTP messages, allowing the same synchronous blocking semantics of a EPP streams over a single, persistent TCP connection, albeit at a possibly slower pace.

Every example in this document has NOT been checked by two different implementors. This strongly indicates (but does not assure) that the examples are incorrect. All implementors must read the relevant document carefully before implementing from it. No one should use the examples in this document as stand-alone explanations of how to create MIME message bodies, or MIME message bodies to which security has been applied.

2. Background Summary

[Some language about these three registry protocols, and the applicability of SMTP as a transport protocol. Dave asked what purpose this serves. Answer TBD.]

This table compares the salient characteristics of EPP, RRP and SRS.

EPP	RRP	SRS
syntax:	syntax:	syntax:
XML	ABNF	keyword-value
encoding:	encoding:	encoding:
8-bit	7-bit	7-bit
MIME type:	MIME type:	MIME type:
app/epp+xml	n/a	mp/mixed
transport:	transport:	transport:
TCP	TCP	SMTP, TCP
OBJECTS:	OBJECTS:	OBJECTS:
domain	domain	domain
host	nameserver	host
contact	n/a	contact
OBJECTS:	OBJECTS:	OBJECTS:
check	check	inquire
info	status	status
create	add	create
update	mod	modify
delete	del	remove
transfer	transfer	transfer
renew	renew	renew

To Do:

Update SRS from Crispin's 11/98 I-D. Some things never really expire.

Indicate 2832bis extensions.

3. References Overview

MIME-based EPP transport over SMTP can be implemented by using specifications provided in the following RFCs:

-RFC 2821 SMTP
-RFC 2822 Text Message Formats
-RFC 2045 to 2049 MIME RFCs

MIME-based Secure EPP transport over SMTP can be implemented by using specifications provided in the following additional RFCs:

-RFC 1847 Security Multiparts for MIME
-RFC 2015, 3156, 2440 MIME/PGP
-RFC 2630, 2633 S/MIME v3 Specification

MIME-based Reliable EPP transport over SMTP can be implemented by using specifications provided in the following additional RFCs:

-RFC 1892 Multipart/Report
-RFC 2298 Message Disposition Notification

MIME-based Bulk EPP transport over SMTP can be implemented by by the specification provided in RFC 2046 for the following:

- message/partial subtype
- message/external-body subtype

4. MIME Fields

Content-Type == application/epp+xml

Content-Transfer-Encoding

1. 7bit -- this is the default, as is "us-ascii" for the charset parameter. This value is NOT RECOMMENDED if the encoding declaration of the XML document is NOT "us-ascii". Note that a line length limit and NUL and CRLF sequence semantics are absent in XML.

2. 8bit -- same as 7bit, with values above 127 allowed. This value is NOT RECOMMENDED if the participating MTAs are not known to support 8bit data.

3. binary -- same as 8bit.

4. quoted-printable -- This value is RECOMMENDED if the encoding declaration of the XML document is NOT "us-ascii". This value (or base64) is REQUIRED if data is signed, or encrypted.

5. base64 -- This value is RECOMMENDED if the encoding declaration of the XML document is NOT "us-ascii". This value (or quoted-printable) is REQUIRED if data is signed, or encrypted.

charset -- Processors generating XML MIME entities MUST NOT label conflicting charset information between the MIME Content-Type and the XML declaration.

[This list is incomplete.]

5. Sender Message Structures

The message structures in this section are presented hierarchically in terms of which RFC's and Internet-Drafts are applied to form the specific structure.

Common Structure

```
No Encryption, No Signature
-RFC822/2045
   -EPP-P (application/epp+xml)
```

PGP/MIME Structure

```
No Encryption, Signature
-RFC822/2045
   -RFC1847 (multipart/signed)
      -EPP-P (application/epp+xml)
      -RFC2015/2440/3156 (application/pgp-signature)

Encryption, No Signature
-RFC822/2045
   -RFC1847 (multipart/encrypted)
      -RFC2015/2440/3156 (application/pgp-encrypted)
         -"Version: 1"
      -RFC2015/2440/3156 (application/octet-stream)
         -EPP-P (application/epp+xml) (encrypted)

Encryption, Signature
-RFC822/2045
   -RFC1847 (multipart/encrypted)
      -RFC2015/2440/3156 (application/pgp-encrypted)
         -"Version: 1"
      -RFC2015/2440/3156 (application/octet-stream)
         -RFC1847 (multipart/signed)(encrypted)
            -EPP-P (application/epp+xml) (encrypted)
            -RFC2015/2440/3156 (application/pgp-signature)(encrypted)
```

S/MIME Structure

```
No Encryption, Signature
-RFC822/2045
   -RFC1847 (multipart/signed)
      -EPP-P (application/epp+xml)
   -RFC2633 (application/pkcs7-signature)
```

```
Encryption, No Signature
-RFC822/2045
   -RFC2633 (application/pkcs7-mime)
      -EPP-P (application/epp+xml) (encrypted)

Encryption, Signature
-RFC822/2045
   -RFC2633 (application/pkcs7-mime)
      -RFC1847 (multipart/signed) (encrypted)
         -EPP-P (application/epp+xml) (encrypted)
         -RFC2633 (application/pkcs7-signature) (encrypted)
```

6. Example: Unsigned, Unencrypted, No Receipt Requested

Sender sends unencrypted data, does NOT request a receipt. The MIME fields of interest are:

1. Mime-Version: 1.0 REQUIRED

2. Content-Type: application/epp+xml REQUIRED

3. Content-Transfer-Encoding: OPTIONAL

In this example, the encoding declaration of both the XML document and MIME entity is "us-ascii", and the Content-Transfer-Encoding is 7bit.

```
   From: epp+smtp@utterly-bogus.nld
   To: epp+smtp@pseudo-random.nld
   Date: whenever
   Subject: test 1: domain-create unsigned, unencrypted, no receipt
requested
   Message-Id: <200210081114.HAA06361@utterly-bogus.nld>
   Mime-Version: 1.0

   Content-Type: application/epp+xml; charset="us-ascii"
   Content-Transfer-Encoding: 7bit

   <?xml version="1.0" encoding="us-ascii" standalone="no"?>
   <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
        epp-1.0.xsd">
     <command>
       <create>
         <domain:create
          xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
          xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
          domain-1.0.xsd">
           <domain:name>example.tld</domain:name>
           <domain:period unit="y">2</domain:period>
           <domain:ns>ns1.example.tld</domain:ns>
           <domain:ns>ns1.example2.tld</domain:ns>
           <domain:registrant>jd1234</domain:registrant>
           <domain:contact type="admin">sh8013</domain:contact>
           <domain:contact type="tech">sh8013</domain:contact>
           <domain:authInfo type="pw">2fooBAR</domain:authInfo>
         </domain:create>
       </create>
       <clTRID>ABC-12345</clTRID>
```

```
    </command>
  </epp>
```

7. Example: Signed, Unencrypted, No Receipt Requested

Sender sends signed unencrypted data, does NOT request a receipt.
The MIME fields of interest are:

1. Mime-Version: 1.0 REQUIRED

2. Content-Type: multipart/signed

3. Content-Type: application/epp+xml REQUIRED

4. Content-Transfer-Encoding: quoted-printable RECOMMENDED

In this example, the encoding declaration of both the XML document
and MIME entity is "sjis", and the Content-Transfer-Encoding is
quoted-printable.

```
From: epp+smtp@utterly-bogus.nld
To: epp+smtp@pseudo-random.nld
Date: whenever
Subject: test 2: domain-create signed, unencrypted, no receipt requested
Message-Id: <200210081114.HAA06362@utterly-bogus.nld>
Mime-Version: 1.0
Content-Type: multipart/signed; micalg=pgp-md5;
        protocol="application/pgp-signature"; boundary="42"
Content-Disposition: inline

--42
& Content-Type: application/epp+xml; charset="sjis"
& Content-Transfer-Encoding: quoted-printable
&
& <?xml version="1.0" encoding="sjis" standalone="no"?>
& <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
&      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
&      xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
&      epp-1.0.xsd">
&   <command>
&     <create>
&       <domain:create
&        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
&        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
&        domain-1.0.xsd">
&         <domain:name>example.tld</domain:name>
&         <domain:period unit="y">2</domain:period>
&         <domain:ns>ns1.example.tld</domain:ns>
&         <domain:ns>ns1.example2.tld</domain:ns>
&         <domain:registrant>jd1234</domain:registrant>
```

```
&         <domain:contact type="admin">sh8013</domain:contact>
&         <domain:contact type="tech">sh8013</domain:contact>
&         <domain:authInfo type="pw">2fooBAR</domain:authInfo>
&       </domain:create>
&     </create>
&     <clTRID>ABC-12345</clTRID>
&   </command>
& </epp>
--42

Content-Type: application/pgp-signature
Content-Disposition: inline

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.0.7 (FreeBSD)

iD8CBQE85tUtWry0BWjoQKURAtV1AJoC7/RCMhS86o2RS53zcx2gdZroYACg0xj6
VPugCOXxguA/yd9VF6qoNsM=
=ApJ4
-----END PGP SIGNATURE-----

--42
```

The signature is calculated over lines beginning with a "&".

8. Example: Unsigned, Encrypted, No Receipt Requested

Sender sends unsigned encrypted data, does NOT request a receipt.
The MIME fields of interest are:

1. Mime-Version: 1.0 REQUIRED

2. Content-Type: multipart/encrypted

3. Content-Transfer-Encoding: quoted-printable RECOMMENDED

4. Content-Type: application/epp+xml REQUIRED

In this example, the encoding declaration of both the XML document and MIME entity is "iso-8859-1", and the Content-Transfer-Encoding is quoted-printable.

```
From: epp+smtp@utterly-bogus.nld
To: epp+smtp@pseudo-random.nld
Date: whenever
Subject: test 3: domain-create signed, unencrypted, no receipt requested
Message-Id: <200210081114.HAA06363@utterly-bogus.nld>
Mime-Version: 1.0
Content-Type: multipart/encrypted;
        protocol="application/pgp-encrypted"; boundary="42"

--42

Content-Type: application/pgp-encrypted

Version: 1

--42
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
E Content-Type: application/epp+xml; charset="iso-8859-1"
E Content-Transfer-Encoding: quoted-printable
E
E <?xml version="1.0" encoding="iso-8859-1" standalone="no"?>
E <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
E      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
E      xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
E      epp-1.0.xsd">
E   <command>
E     <create>
E       <domain:create
```

```
E        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
E        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
E        domain-1.0.xsd">
E         <domain:name>example.tld</domain:name>
E         <domain:period unit="y">2</domain:period>
E         <domain:ns>ns1.example.tld</domain:ns>
E         <domain:ns>ns1.example2.tld</domain:ns>
E         <domain:registrant>jd1234</domain:registrant>
E         <domain:contact type="admin">sh8013</domain:contact>
E         <domain:contact type="tech">sh8013</domain:contact>
E         <domain:authInfo type="pw">2fooBAR</domain:authInfo>
E       </domain:create>
E     </create>
E     <clTRID>ABC-12345</clTRID>
E   </command>
E </epp>
-----END PGP MEESAGE-----

--42
```

Lines beginning with a "E" are Encrypted. Decryption is left as an exercise for the reader.

9. Example: Signed, Encrypted, No Receipt Requested

Sender sends signed encrypted data, does NOT request a receipt. The MIME fields of interest are:

1. Mime-Version: 1.0 REQUIRED

2. Content-Type: multipart/encrypted

3. Content-Transfer-Encoding: quoted-printable RECOMMENDED

4. Content-Type: application/epp+xml REQUIRED

In this example, the encoding declaration of both the XML document and MIME entity is "ibm037" (EBCDIC), and the Content-Transfer-Encoding is quoted-printable.

```
From: epp+smtp@utterly-bogus.nld
To: epp+smtp@pseudo-random.nld
Date: whenever
Subject: test 4: domain-create signed, unencrypted, no receipt requested
Message-Id: <200210081114.HAA06364@utterly-bogus.nld>
Mime-Version: 1.0
Content-Type: multipart/encrypted;
        protocol="application/pgp-encrypted"; boundary="42"

--42

Content-Type: application/pgp-encrypted

Version: 1

--42
Content-Type: application/octet-stream

-----BEGIN PGP MESSAGE-----
E Content-Type: multipart/signed;
E         protocol="application/pgp-signature"; boundary="24"
E Content-Disposition: inline
E
E --24
E &  Content-Type: application/epp+xml; charset="ibm037"
E &  Content-Transfer-Encoding: quoted-printable
E &
E &  <?xml version="1.0" encoding="ibm037" standalone="no"?>
E &  <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
E &       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
```

```
E &       xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
E &       epp-1.0.xsd">
E &    <command>
E &      <create>
E &        <domain:create
E &         xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
E &         xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
E &         domain-1.0.xsd">
E &          <domain:name>example.tld</domain:name>
E &          <domain:period unit="y">2</domain:period>
E &          <domain:ns>ns1.example.tld</domain:ns>
E &          <domain:ns>ns1.example2.tld</domain:ns>
E &          <domain:registrant>jd1234</domain:registrant>
E &          <domain:contact type="admin">sh8013</domain:contact>
E &          <domain:contact type="tech">sh8013</domain:contact>
E &          <domain:authInfo type="pw">2fooBAR</domain:authInfo>
E &        </domain:create>
E &      </create>
E &      <clTRID>ABC-12345</clTRID>
E &    </command>
E &  </epp>
E &  --24
E
E Content-Type: application/pgp-signature
E Content-Disposition: inline
E
E -----BEGIN PGP SIGNATURE-----
E Version: GnuPG v1.0.7 (FreeBSD)
E
E iD8CBQE85tUtWry0BWjoQKURAtV1AJoC7/RCMhS86o2RS53zcx2gdZroYACg0xj6
E VPugCOXxguA/yd9VF6qoNsM=
E =ApJ4
E -----END PGP SIGNATURE-----
E
E --24
-----END PGP MESSAGE-----

--42
```

The signature is calculated over lines beginning with a "&". Lines begining with a "E" are Encrypted. Decryption is left as an exercise for the reader.

10. Example: Signed, Unencrypted, No Receipt Requested

Sender sends signed unencrypted data, does NOT request a receipt.
The MIME fields of interest are:

1. Mime-Version: 1.0 REQUIRED

2. Content-Type: multipart/signed

3. Content-Type: application/epp+xml REQUIRED

4. Content-Transfer-Encoding: base64 RECOMMENDED

In this example, the encoding declaration of both the XML document
and MIME entity is "big5", and the Content-Transfer-Encoding is
base64.

```
From: epp+smtp@utterly-bogus.nld
To: epp+smtp@pseudo-random.nld
Date: whenever
Subject: test 5: domain-create signed, unencrypted, no receipt requested
Message-Id: <200210081114.HAA06365@utterly-bogus.nld>
Mime-Version: 1.0
Content-Type: multipart/signed; micalg=sha1;
        protocol="application/pkcs7-signature"; boundary="42"
Content-Disposition: inline

--42
& Content-Type: application/epp+xml; charset="big5"
& Content-Transfer-Encoding: base64
&
& <?xml version="1.0" encoding="big5" standalone="no"?>
& <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
&      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
&      xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
&      epp-1.0.xsd">
&   <command>
&     <create>
&       <domain:create
&        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
&        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
&        domain-1.0.xsd">
&         <domain:name>example.tld</domain:name>
&         <domain:period unit="y">2</domain:period>
&         <domain:ns>ns1.example.tld</domain:ns>
&         <domain:ns>ns1.example2.tld</domain:ns>
&         <domain:registrant>jd1234</domain:registrant>
```

```
&         <domain:contact type="admin">sh8013</domain:contact>
&         <domain:contact type="tech">sh8013</domain:contact>
&         <domain:authInfo type="pw">2fooBAR</domain:authInfo>
&       </domain:create>
&     </create>
&     <clTRID>ABC-12345</clTRID>
&   </command>
& </epp>
--42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VCpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--42
```

The signature is calculated over lines beginning with a "&".

11. Example: Unsigned, Encrypted, No Receipt Requested

Sender sends unsigned encrypted data, does NOT request a receipt.
The MIME fields of interest are:

1. Mime-Version: 1.0 REQUIRED

2. Content-Type: application/pkcs7-mime

3. Content-Type: application/epp+xml REQUIRED

4. Content-Transfer-Encoding: base64 RECOMMENDED

In this example, the encoding declaration of both the XML document
and MIME entity is "euc-jp", and the Content-Transfer-Encoding is
base64.

```
From: epp+smtp@utterly-bogus.nld
To: epp+smtp@pseudo-random.nld
Date: whenever
Subject: test 6: domain-create signed, unencrypted, no receipt requested
Message-Id: <200210081114.HAA06367@utterly-bogus.nld>
Mime-Version: 1.0
Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
    name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename=smime.p7m

E Content-Type: application/epp+xml; charset="euc-jp"
E Content-Transfer-Encoding: base64
E
E <?xml version="1.0" encoding="euc-jp" standalone="no"?>
E <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
E      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
E      xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
E      epp-1.0.xsd">
E   <command>
E     <create>
E       <domain:create
E        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
E        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
E        domain-1.0.xsd">
E         <domain:name>example.tld</domain:name>
E         <domain:period unit="y">2</domain:period>
E         <domain:ns>ns1.example.tld</domain:ns>
E         <domain:ns>ns1.example2.tld</domain:ns>
```

```
E         <domain:registrant>jd1234</domain:registrant>
E         <domain:contact type="admin">sh8013</domain:contact>
E         <domain:contact type="tech">sh8013</domain:contact>
E         <domain:authInfo type="pw">2fooBAR</domain:authInfo>
E       </domain:create>
E     </create>
E     <clTRID>ABC-12345</clTRID>
E   </command>
E </epp>
```

Lines beginning with a "E" are Encrypted. Decryption is left as an exercise for the reader.

12. Example: Signed, Encrypted, No Receipt Requested

Sender sends signed encrypted data, does NOT request a receipt. The MIME fields of interest are:

1. Mime-Version: 1.0 REQUIRED

2. Content-Type: multipart/signed

3. Content-Type: application/epp+xml REQUIRED

4. Content-Transfer-Encoding: base64 RECOMMENDED

In this example, the encoding declaration of both the XML document and MIME entity is "bjecree", and the Content-Transfer-Encoding is base64.

```
From: epp+smtp@utterly-bogus.nld
To: epp+smtp@pseudo-random.nld
Date: whenever
Subject: test 8: domain-create signed, encrypted, no receipt requested
Message-Id: <200210081114.HAA06368@utterly-bogus.nld>
Mime-Version: 1.0

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
    name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
    filename=smime.p7m
    boundary="42"

--42
E Content-Type: multipart/signed; micalg=sha1;
E         protocol="application/pkcs7-signature"; boundary="42"
E Content-Disposition: inline
E
E & Content-Type: application/epp+xml; charset="bjecree"
E & Content-Transfer-Encoding: base64
E &
E & <?xml version="1.0" encoding="bjecree" standalone="no"?>
E & <epp xmlns="urn:ietf:params:xml:ns:epp-1.0"
E &      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
E &      xsi:schemaLocation="urn:ietf:params:xml:ns:epp-1.0
E &      epp-1.0.xsd">
E &   <command>
E &     <create>
E &       <domain:create
```

```
E &        xmlns:domain="urn:ietf:params:xml:ns:domain-1.0"
E &        xsi:schemaLocation="urn:ietf:params:xml:ns:domain-1.0
E &        domain-1.0.xsd">
E &         <domain:name>example.tld</domain:name>
E &         <domain:period unit="y">2</domain:period>
E &         <domain:ns>ns1.example.tld</domain:ns>
E &         <domain:ns>ns1.example2.tld</domain:ns>
E &         <domain:registrant>jd1234</domain:registrant>
E &         <domain:contact type="admin">sh8013</domain:contact>
E &         <domain:contact type="tech">sh8013</domain:contact>
E &         <domain:authInfo type="pw">2fooBAR</domain:authInfo>
E &       </domain:create>
E &     </create>
E &     <clTRID>ABC-12345</clTRID>
E &   </command>
E & </epp>
E --42
E Content-Type: application/pkcs7-signature; name=smime.p7s
E Content-Transfer-Encoding: base64
E Content-Disposition: attachment; filename=smime.p7s
E
E ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
E 4VCpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
E n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
E 7GhIGfHfYT64VQbnj756
E
--42
```

13. Receiver Message Structures

This section is intentionally blank, pending implementation.

14. Bulk Transport

Large EPP message bodies may be fragmented by message transfer agents. A subtype of message/partial is defined in [RFC2046] to allow large objects to be delivered as fragments in separate pieces of mail and to be reassembled by the receiving user agent. If the message/partial subtype is used, three parameters must be specified in the Content-Type field: a unique identifier, a sequence identifier, and a sequence terminator. Note that sequence identifiers begin with 1, not 0.

```
Content-Type: Message/Partial; number=2; total=3;
              id="200210081114.HAA06360@utterly-bogus.nld"

Content-Type: Message/Partial;
              id="200210081114.HAA06360@utterly-bogus.nld";
              number=2
```

But the third piece MUST specify the total number of fragments:

```
Content-Type: Message/Partial; number=3; total=3;
              id="200210081114.HAA06360@utterly-bogus.nld"
```

It is possible that a piece of a partial message, upon re-assembly, contains a partial message as well.

Large EPP message body transport may also be accomplished without fragmentation. A subtype of external-body is defined in [RFC2046] to indicate that the actual body data are referenced by the message, but not included in the message. The access-type parameter values for the external-body subtype includes FTP, to indicate that the message body is accessible as a file using the FTP [RFC959] protocol. For this access-type, the following additional parameters are mandatory:

NAME -- The name of the file that contains the actual body data,

SITE -- A machine from which the file may be obtained,

MODE -- MUST be IMAGE if the encoding declaration of MIME entity (and presumably the XML document) is NOT us-ascii, otherwise this parameter is optional

Note: A login id and password for the machine named by the SITE parameter are not specified as content-type parameters, and must be obtained from the user. The use of the external-body subtype and an access-type of FTP are RECOMMENDED for large messages between limited size sets of EPP peers, for which the EPP authentication mechanism is

adequate, e.g., escrow messaging, and inter-registry messaging. The use of the external-body subtype and an access-type of ANON-FTP are RECOMMENDED for messages which do not require authentication, e.g., public escrow messaging.

In this example, the encoding declaration of both the XML document and MIME entity is "gb2312", and the MODE is IMAGE.

```
From: epp+smtp@utterly-bogus.nld
To: epp+smtp@pseudo-random.nld
Date: whenever
Subject: test bulk B: external body reference
Message-Id: <200210101118.HAA2853@utterly-bogus.nld>
Mime-Version: 1.0
Content-Type: Multipart/Mixed; Boundary="42"

--42

[This is an optional inline summary of the referenced body.]

--42
Content-Type: Message/External-body;
        name="sufficiently-useful-identifier.xml";
        site="ftp.utterly-bogus.nld";
        access-type="ftp";
        directory="registry-Y/posted"
        mode="image"

Content-Type: application/epp+xml; charset="gb2312"
Content-ID:     <2002-10-9150009@utterly-bogus.nld>

--42
```

15. Security Considerations

Most of this memo is concerned with secure transport of EPP data, and considers endpoint authentication, data security, data integrity and [in its next revision] non-repudiation of origin and non-repudiation of receipt.

Early reviewer's comments and author's nigglings:

1. are there EPP-unique bits not MIME-generic? (Dave),

2. "man-in-the-middle" attacks (Dave),

3. denial-of-service" attacks (Dave),

4. the locus of authority for EPP data is variable, see "thick" vs "thin" registry design considerations, elsewhere (Eric),

5. extending message-level mechanisms to message fragments (Eric),

6. other

[More closing mumble.]

16. Internationalization Considerations

Since the publication of [RFC1766], now [RFC3066][BCP47], meta-data taging, restricted to the repitoires defined in [ISO639] and [ISO3166], have been widely (mis)understood to exhaust this subject. With the publication of [RFC2130] and its sequela [RFC2277][BCP18] and [RFC2279], universal code-set dependency, restricted to the repitoires defined in [UNICODE], have also been widely (mis)understood to exhaust this subject.

The astute reader of this memo will have observed that neither of these classes of restrictions has been observed here. Encoding has been signaled between the EPP peers, consistent with the normative texts defining TCP, SMTP, MIME, XML, and EPP, using meta-data, without dependency upon [ISO639], [ISO3166], or an IETF-defined post-hoc repository of meta-data [RFC2978], nor upon [UNICODE], or any encoding strictly-extending ASCII.

The encodings used outside the limits imposed by [RFC1766] et seq., and by [UNICODE] are:

1. ibm037 (aka "EBCDIC"), first implemented in OS/360, April 1964

2. big5, first defined in 1984 by the Taipei Computer Association

3. euc-jp, first defined in 1987 by XPG/3, see also: euc-cn, euc-kr, euc-tw. Note Bene: EUC has no requirement that code set 0 be ASCII.

4. sjis, see also JIS X 0208:1997

5. bjecree, first defined by Bill Jancewicz (SIL), and adopted by the Naskapi Cree First Nation, and other Cree First Nations

Other POSIX Locale Condisderations This memo introduces no string collation, character case mapping or equivalence classing, message cataloging, monetary, numeric, or date/time formatting considerations beyond those introduced in [EPP-P].

References

[1] Bradner, S., "The Internet Standards Process -- Revision 3", RFC 2026, BCP 9, October 1996.

[2] Klensin, J., "Simple Mail Transfer Protocol", RFC 2821, April 2001.

[3] Resnick, P., "Internet Message Format", RFC 2822, April 2001.

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

[5] Freed, N., "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", RFC 2046, November 1996.

[6] Moore, K., "Multipurpose Internet Mail Extensions (MIME) Part Three: Message Header Extensions for Non-ASCII Text", RFC 2047, November 1996.

[7] Freed, N., "Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures", RFC 2048, November 1996.

[8] Freed, N., "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples", RFC 2049, November 1996.

[9] Galvin, J., "Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted", RFC 1847, October 1995.

[10] Elkins, M., "MIME Security with Pretty Good Privacy (PGP)", RFC 2015, October 1996.

[11] Elkins, M., "MIME Security with OpenPGP", RFC 3156, August 2001.

[12] Callas, J., "OpenPGP Message Format", RFC 2440, November 1998.

[13] Housley, R., "Cryptographic Message Syntax", RFC 2630, June 1999.

[14] Ramsdell, B., "S/MIME Version 3 Message Specification", RFC 2633, June 1999.

[15] Vaudreuil, G., "The Multipart/Report Content Type for the Reporting of Mail System Administrative Messages", RFC 1892, January 1996.

[16] Fajman, R., "An Extensible Message Format for Message Disposition Notifications", RFC 2298, March 1998.

[17] Hollenbeck, S., "Extensible Provisioning Protocol", , August 2002.

[18] Hollenbeck, S., "Extensible Provisioning Protocol Contact Mapping", , August 2002.

[19] Hollenbeck, S., "Extensible Provisioning Protocol Domain Name Mapping", , August 2002.

[20] Hollenbeck, S., "Extensible Provisioning Protocol Host Mapping", , August 2002.

Author's Address

Eric Brunner-Williams
Wampumpeag, LLC
1415 Forest Avenue
Portland, Maine 04103
United States

EMail: brunner@nic-naa.net

Appendix A. Acknowledgements

Many thanks go to the authors of MIME-based Secure EDI IETF Draft, who's work is shamelessly expropriated, and to many of the contributors to the IETF EPP drafts. In addition the author thanks Marshall Rose who provided the extremely useful [RFC2629] document type description and xml2rfc tool used to edit this specification. The author may yet learn how to use this tool.

The author especially thanks the National Cooperative Business Association, and the Swiss Education and Research Network, without who's generous funding this work would not have been possible.

Full Copyright Statement