Internet Draft
draft-hoffman-rescap-mua-01.txt
April 20, 1999
Expires in six months

Paul Hoffman
Internet Mail Consortium

Rescap Profile for Mail User Agents

Status of this memo

1. Introduction

This document defines a profile of the rescap protocol for mail user agents (MUAs) and mail recipients. It describes the attributes that a mail sender might want or need to know about a particular mail recipient before sending a message.

The attributes are divided into four general categories:
- MIME handling
- S/MIME
- OpenPGP
- General

Note: this list is very preliminary. The process of defining the requirements for rescap has just begun. Because the rescap protocol has not even had a first draft, it is likely that there will be many significant changes to this draft in the future as rescap gets worked on.

In this document, "recipient" is used to indicate the user who can accept mail at the URL provided in the rescap request and "sender" is the person or process who requested the rescap information. Note that some of the attributes in this document apply to the MUA a recipient is using, while others apply directly to the mail recipient (which might be a human or a mail-processing program).

The attributes described in this document are those that a mail sender would want to know about a recipient or the recipient's MUA. Attributes about the mail recipient that have no relevance to a mail sender (such if the MUA uses IMAP to access its message store) are not included.

2. MIME Handling

The attributes in this section describe general MIME handling. They include some specific MIME profiles as well as more general MIME characteristics.

Identifier: PlainTextOnly
Value type: Boolean
Description: Can only read single-part text/plain messages. Put another way, cannot parse a MIME message.

Identifier: MIMEIntlHeaders
Value type: Boolean
Description: Conforms to [MIME-HEADER-EXTENSIONS], which describes many extensions for MIME headers, such as for non-ASCII characters.

Identifier: MIMEParamExtensions
Value type: Boolean
Description: Conforms to [MIME-PARAM], which describes many extensions for MIME parameter values and encoded words.

Identifier: DisplayableMedia
Value type: Conneg string
Description: A list of MIME types and subtypes that are natively displayed by the receiving MUA without falling back to a default media type. The string is in the format of [CONNEG], as extended by [CONNEG-MEDIA]. This string should contain only MIME types and subtypes, not additional media features.

Identifier: MediaFeatures
Value type: Conneg string
Description: A list of media features of the MUA. The string is in the format of [CONNEG].

Identifier: CharsetsDisplayed
Value type: List of strings
Description: The list of charset labels that describe the charsets [CHARSET] that can be displayed. Note that US-ASCII, and support for at least the US-ASCII subset of ISO-8859-*, is assumed regardless of the value of this attribute. The list is in order of preferred charsets, highest preference first. Note: this identifier may disappear in future versions of this document, or may be cast as a Conneg string, if there becomes a way to list charsets in the MediaFeatures identifier.

Identifier: PreferredLanguages
Value type: List of strings
Description: The lists of languages understandable to the recipient,

as described in [LANG]. The list is in order of preferred languages, highest preference first.

Identifier: HandlesMHTML
Value type: Boolean
Description: Handles MHTML content natively, as described in [MHTML].

Identifier: HandlesContentMD5
Value type: Boolean
Description: Handles Content-MD5 headers, as described in [CONTENT-MD5]. If the recipient does not handle Content-MD5 headers, as many don't, this the sender can save time by not constructing one.

Identifier: HandlesMailingListURLs
Value type: Boolean
Description: Handles mailing list URL headers, as described in [LIST-URLS].

Identifier: HandlesOnePassMultipart
Value type: Boolean
Description: Handles the "types" parameter for the multipart/alternative MIME type, as described in [MULTIPART-ONEPASS].

Identifier: RepliesToMDNs
Value type: Boolean
Description: Is able to reply to message disposition notification requests, as described in [MDN]. Note that this does not mean that the client will necessarily send an MDN back to a particular request, just that it is able to reply to such requests. This field helps a sending MUA decide whether or not to keep track of the MDNs sent to the recipient; if the recipient is known not to reply to MDNs, then the sender doesn't need to track them. This can also reduce the size of messages sent over bandwidth-restricted lines.

Identifier: CalendarClient
Value type: Boolean
Description: Can act as an iCalendar iMIP agent [IMIP].

3. S/MIME

The attributes in this section indicate the S/MIME capabilities of the recipient as described in [SMIME-MSG], [SMIME-CERT], and associated documents.

Note that some S/MIME public keys are used for both encrypting and signing. This means that there may be duplicated certificates in the SMIMESigningCertsBasic and SMIMEEncryptingCerts lists.

Identifier: SMIMEVerifiesSigned
Value type: List of strings
Description: Indicates that the recipient can verify the signatures on

S/MIME signed messages. The strings in the list indicate the type of signatures accepted. The values currently are limited to "id-dsa" and "rsaEncryption". The list is in decreasing order of preference.

Identifier: SMIMESigningCertsBasic
Value type: List of binary
Description: Provides the S/MIME certificates for public signing keys of the recipient. The list is in decreasing order of preference.

Identifier: SMIMESigningCertsExtended
Value type: List of binary
Description: Provides the S/MIME certificates for public signing keys of the recipient, including additional signed attributes, as described in [SMIME-CERTDIST]. The list is in decreasing order of preference.

Identifier: SMIMEEncryptingCerts
Value type: List of binary
Description: Provides the S/MIME certificates for public encrypting keys of the recipient. The list is in decreasing order of preference.

Identifier: SMIMEHigherCerts
Value type: List of binary
Description: Provides the S/MIME certificates for certificate authorities that have signed the recipient's signing and encrypting certificates. These higher-level certificates can be used by the sender to validate the recipient's certificates. The list is in no particular order.

Identifier: SMIMESignedReceipts
Value type: Boolean
Description: Responds to requests for S/MIME signed receipts described in [SMIME-ESS].

Identifier: SMIMESecurityLabels
Value type: Boolean
Description: Acts on S/MIME security labels, or is behind a gateway that does security label handling, as described in [SMIME-ESS].

Identifier: SMIMESecureMailingList
Value type: Boolean
Description: Is a mailing list that uses secure mailing list handling described in [SMIME-ESS].

Identifier: SMIMEHandlesSigningCert
Value type: Boolean
Description: Handles the signed SigningCertificate attribute described in [SMIME-ESS].

4. OpenPGP

The attributes in this section indicate the OpenPGP capabilities of the recipient as described in [OPEN-PGP] and associated documents.

Identifier: OpenPGPVerifiesSigned
Value type: List of strings
Description: Indicates that the recipient can verify the signatures on OpenPGP signed messages. The strings in the list indicate the type of signatures accepted. The values currently are limited to "DSA" and "RSA". The list is in decreasing order of preference.

Identifier: OpenPGPSigningCertsBasic
Value type: List of binary
Description: Provides the OpenPGP certificates for public signing keys of the recipient. The list is in decreasing order of preference.

Identifier: OpenPGPEncryptingCerts
Value type: List of binary
Description: Provides the OpenPGP certificates for public encrypting keys of the recipient. The list is in decreasing order of preference.

Identifier: OpenPGPHigherCerts
Value type: List of binary
Description: Provides the OpenPGP certificates for users and certificate authorities that have signed the recipient's signing and encrypting certificates. These higher-level certificates can be used by the sender to validate the recipient's certificates. The list is in no particular order.

5. General

User agent and recipient attributes that don't fit into the other categories appear in this section.

Identifier: UBEPrefernces
Value type: List of pairs of strings
Description: Specifies the preferences of the recipient for receiving unsolicited bulk email (UBE). Each entry in the list is a pair of strings. The first entry in the pair is a tag indicating the law or policy being referred to, and the second entry is the value specified for that law or policy. The identities of the laws and policies must be registered with IANA.

Identifier: MailingListInfo
Value type: String
Description: Gives information about a mailing list. The format of the information is single string consisting of RFC 822 headers, as described in [MAILLIST]. If the recipient is not a mailing list and this attribute is included in the rescap response, the string should be empty.

Identifier: GeneralInfo
Value type: vCard string

Description: Gives information about the person or system that is associated with the recipient. The information is returned in the vCard format described in [VCARD]. Note that any information in this attribute that can also be represented in other attributes in this profile should also be delivered in the other attributes. No client should have to retrieve the value for this attribute in order to get information that is also available in other attributes.

Identifier: AssociatedEmailAddresses
Value type: List of lists
Description: Lists the email addresses used by this recipient. The list contains items that contain a pair of string items. The pairs consist of an email address and a description. The description should be the strings "home", "work", "all", "unused". The "unused" term indicates an email address that is no longer valid for the recipient.

6. Security Considerations

The rescap protocol will control the security of the passing the values for the attributes described here. If digital signatures are not used, an attacker can alter the values that the client receives from the server, thereby causing false values or no values to be received. For example, an attacker can change the legal notices sent, which can cause damage to the named recipient. If encryption is not used, an attacker can watch the values of the attributes as they are transmitted over the Internet.

7. References

[CHARSET] "IANA Charset Registration Procedures", RFC 2278

[CONNEG] "A Syntax for Describing Media Feature Sets", RFC 2553.

[CONNEG-MEDIA] "MIME content types in media feature expressions", draft-ietf-conneg-feature-type.

[CONTENT-MD5] "The Content-MD5 Header Field", RFC 1864.

[IMIP] "iCalendar Message-Based Interoperability Protocol (iMIP)", RFC 2447.

[LANG] "Tags for the Identification of Languages", RFC 1766.

[LIST-URLS] "The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields", RFC 2369.

[MAILLIST] "The Use of URLs as Meta-Syntax for Core Mail List Commands and their Transport through Message Header Fields", RFC 2369.

[MDN] "An Extensible Message Format for Message Disposition

Notifications", RFC 2298.

[MHTML] "MIME E-mail Encapsulation of Aggregate Documents, such as HTML (MHTML)", RFC 2110.

[MIME-HEADER-EXTENSIONS] "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", RFC 2047.

[MIME-PARAM] "MIME Parameter Value and Encoded Word Extensions: Character Sets, Languages, and Continuations", RFC 2231.

[MULTIPART-ONEPASS] "One Pass Multipart/Alternative Processing", draft-lundblade-1pass-mult-alt.

[OPEN-PGP] "OpenPGP Message Format", RFC 2440.

[SMIME-CERT] "S/MIME Version 3 Certificate Handling", draft-ietf-smime-cert.

[SMIME-CERTDIST] "Certificate Distribution Specification", draft-ietf-smime-certdist.

[SMIME-ESS] "Enhanced Security Services for S/MIME", draft-ietf-smime-ess.

[SMIME-MSG] "S/MIME Version 3 Message Specification", draft-ietf-smime-msg.

[VCARD] "vCard MIME Directory Profile", RFC 2426.

A. IANA Registrations

A.1 Attribute Identifier Registrations

[[It is likely that all the attribute identifiers in this document will need to be registered.]]

A.2 Additional Registrations

[[Registration of UCE law and policy identifiers]]

B. Acknowledgments

The following people have contributed changes and additions to this document:

Chris Newman
Graham Klyne
Larry Masinter
Tony Hansen

C. Changes between versions of the draft

C.1 Changes between -00 and -01

Changed "HandlesMIME" to "PlainTextOnly" to avoid making it sound like a compliance setting. Removed reference to [MIME-CONFORM].

Changed "MIMEHeaderExtensions" to "MIMEIntlHeaders".

Added note in "CharsetsDisplayed" about US-ASCII. Also added note that this might go away in the future if charsets can be defined in conneg.

Added notes in HandlesContentMD5 and RepliesToMDNs about the logic of using these identifiers.

Got rid of HandlesContentDisposition and HandlesPlainFormat (and the references to [CONTENT-DISP] and [PLAIN-FORMAT]). Both of these are for characteristics that can be included in messages regardless of whether or not the recipient understands them, and including the features involves very low overhead for the sender.

Removed FaxSimpleClient and FaxExtendedClient because the relevant parts of both of these features can be determined from the MediaFeatures identifier.

Added MailingListInfo, AssociatedEmailAddresses, and GeneralInfo in section 5.

D. Author's Address

Paul Hoffman
Internet Mail Consortium
127 Segre Place
Santa Cruz, CA 95060
phoffman@imc.org