

Internet Draft
draft-hoffman-rescap-mua-03.txt
August 8, 2000
Expires in six months

Paul Hoffman
Internet Mail Consortium

Rescap Profile for Mail User Agents

Status of this memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Abstract

This document defines a profile of the rescap protocol [[RESCAP-MAIN](#)] 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.

1. Introduction

The attributes described in this document are divided into four general categories:

- MIME handling
- S/MIME
- OpenPGP
- General

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 as if the MUA uses IMAP to access its message store) are not included.

[1.1](#) Value types

This document specifies a list of request-type items for rescap. Each item specifies an identifier and associated tag, a value type which describes the format of the response-type associated with the request, and a description.

The value types described in this document are:

Boolean: a one-octet value. x00 indicates false, and x01 indicates true.

Integer: a two-octet value that indicates an integer between 0 and 65535.

List of strings: a structure for strings. Each element of the structure consists of a two-octet length, followed by a string of octets.

String: a string of octets.

[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: 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: String

Description: A list of media features of the MUA. The string is in the format of [[CONNEG](#)].

Identifier: CharsetsDisplayed

Value type: String

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 string is in the format of [[CONNEG](#)], using the tags defined in [[CONNEG-CHARLANG](#)].

Identifier: PreferredLanguages

Value type: List of strings

Description: The lists of languages understandable to the recipient, as described in [[LANG](#)]. The string is in the format of [[CONNEG](#)], using the tags defined in [[CONNEG-CHARLANG](#)].

Identifier: LineLength

Value type: Integer

Description: The width, in characters, of a line in the display of the MUA. For variable-width displays, this should be an estimate of the number of characters per line (probably in "em widths") for a typical mail message. For systems that have no line limitations, this value should be set to 0.

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: 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 strings
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 strings
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 strings
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 strings
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 strings

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 strings

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 strings

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: `UBEPrefrences`

Value type: List of strings

Description: Specifies the preferences of the recipient for receiving unsolicited bulk email (UBE). Each entry in the list consists of two sub-strings that are separated by a vertical bar character ("|", ASCII 0x7C). The first substring is a tag indicating the law or policy being referred to, and the second substring 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: 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 strings

Description: Lists the email addresses used by this recipient. Each entry in the list consists of two sub-strings that are separated by a vertical bar character ("|", ASCII 0x7C). The first sub-string is an email address, and the second sub-string 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. Note that this attribute could be used by an unscrupulous marketer to obtain additional addresses to which they can send UBE.

6. Security Considerations

The rescap protocol will control the security of the passing the values for the attributes described here. If authentication is 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 2533](#).

[CONNEG-CHARLANG] "Registration of Charset and Languages Media Features Tags", [draft-hoffman-char-lang-media](#).

[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](#).

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

[RESCAP-MAIN] "The rescap Resolution Protocol", [draft-ietf-rescap-proto-main](#).

[SMIME-CERT] "S/MIME Version 3 Certificate Handling", [RFC 2632](#).

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

[SMIME-ESS] "Enhanced Security Services for S/MIME",
[RFC 2634](#).

[SMIME-MSG] "S/MIME Version 3 Message Specification",
[RFC 2633](#).

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

[A. IANA Registrations](#)

[A.1 Attribute Identifier Registrations](#)

[[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 -02 and -03](#)

Added [section 1.1](#).

Added sentence about UBE to AssociatedEmailAddresses.

Added the note about em widths in LineLength.

Got rid of list of pairs of strings for simplicity.

[D. Author's Address](#)

Paul Hoffman
Internet Mail Consortium
[127 Segre Place](#)
Santa Cruz, CA 95060
phoffman@imc.org