IETF RESCAP WG
Internet draft

G. Klyne, MIMEsweeper Group
9 January 2002
Expires: July 2002

RESCAP Scenarios
<draft-ietf-rescap-scenarios-01.txt>

Status of this memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC 2026.

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/1id-abstracts.html

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

Copyright Notice

Copyright (C) The Internet Society 2002. All Rights Reserved.

Abstract

This memo explores some scenarios for the resource capabaility discovery protocol (RESCAP). It is intended to provide some grounding in specific use-cases for decisions about RESCAP goals and design.

Table of contents

1. Introduction

This memo explores some scenarios for the resource capabaility discovery protocol (RESCAP). It is intended to provide some grounding in specific use-cases for decisions about RESCAP goals and design.

1.1 Structure of this document

Section 2 makes some general comments about expected RESCAP usage and deployment.

Section 3 describes a number of usage scenarios that motivate the design of RESCAP. In each case, the expected resource data and perceived security threats are listed.

Section 4 describes in greater detail the resource capability data elements that are noted in one of more of the scenarios.

Section 5 describes in greater detail the security threats that are noted in one of more of the scenarios.

1.2 Document terminology and conventions

RESCAP refers to the "Ressource Capability Discovery Protocol" that is being designed by the RESCAP working group.

> NOTE: Comments like this provide additional nonessential information about the rationale for parts of this document.

[[[Editorial comments and questions about outstanding issues are provided in triple brackets like this. These working comments should be resolved and removed prior to final publication.]]]

1.3 Discussion of this document

Discussion of this document should take place on the Resource Capability Protocol (RESCAP) mailing list. Please send comments regarding this document to:

<rescap@cs.utk.edu>

To subscribe to this list, send a message to "<rescap-request@cs.utk.edu>" containing the command "subscribe rescap" in the message body.

To see what has gone on before you subscribed, please see the mailing list archive at:

ftp://cs.utk.edu/pub/rescap

2. General issues

The RESCAP working group charter sets out the motivation and goals for the RESCAP protocol:

A variety of resource identifiers have been widely deployed on the Internet as a means of identifying various resources, services, and destinations. However, a means of attaching a set of attributes or characteristics to a given resource identifier and subsequently assessing those attributes or characteristics has not been specified and deployed.

A particularly important resolution service of this general type is one which, when given a mail address identifying a particular mail recipient, will return a series of attributes describing the capabilities of that recipient. This differs from a directory service in that no searching or other advanced query operations are involved.

RESCAP consists of two protocol parts:

- a general resolution protocol that will translate resource identifiers to a list of attributes.
- an administrative model and update protocol that can be used to set up and maintain the information the resolution protocol accesses.

The service resulting from the combination of these two protocols must meet the following goals:

(0) The resolution protocol must be highly scalable, as the intent is to deploy it very widely.

(1) Resolution protocol and server overhead must be very low, as some applications will make very heavy use of it.

(2) Identifiers input to the resolution service are to be formatted as Uniform Resource Identifiers (URIs) containing one or more DNS domains. Note that mail addresses can be presented as mailto: URIs to meet this requirement.

(3) Facilities to support inheritance within the attribute store will be essential, as the number of identifiers may be very large. Specifically, mechanisms are required for administrators to set default values for members of their administrative domains.

(4) Existing protocols will be profiled for use as part of this service whenever possible rather than developing new protocols. In particular:

(a) The DNS must be used as the first step in the resolution service. As the URIs under consideration here contain a DNS domain name, this provides for effective delegation of resolution activities.

(b) Existing DNS record types such as SRV and NAPTR will be used if feasible, to ease deployment.

(c) An existing administrative model and maintenance protocol will be used if feasible. Possible candidates for this include ACAP and LDAPv3. The protocol and security model by which a user can update his or her own attributes must be covered. The means to register and extend the set of attributes must be specified.

3. Scenarios

This section summarizes some intended uses for the RESCAP protocol. Resource metadata and security threats are simply listed here, with more extensive descrptions provided in the following sections.

3.1 Mail user agent capability discovery

It can be very useful for a mail sender to have some knowledge of a receiver's user agent before a message is sent. This kind of information is difficult to discover by any other means, and mail users are often forced to resort to ad-hoc out-of-band means to learn how to best prepare a message for a given recipient.

Type of resource:

- a mailbox, identified by a 'mailto:' URL [1, 2].

Type of metadata:

- Media feature expression

- Security options

- MIME handling options
- General capabilities and preferences

Security threats:

- Unauthorized access or disclosure
- Response spoofing
- Data mining

3.2 Resource metadata access

Web and other data resources may have associated metadata (URCs?). A combination of DNS and RESCAP protocols might be used to access this resource metadata.

HTTP might be used instead of RESCAP, but the RESCAP goals suggest two possible advantages over HTTP: lightweight access for small items of information that are accessed frequently, and the RESCAP administrative model suggests a possibility for easier administration of metadata for metadata about a family of related resources.

Following this line, RESCAP may find a role in efficient URN resolution (using DNS NAPTR and related records [22] to locate a suitable RESCAP server).

Type of resource:

- Web and ftp data
- [[[Others?]]]

Type of metadata:

- Resource URLs
- Media feature expressions

[[[List other kinds of metadata returned]]]

Security threats:

- Unauthorized access
- Response spoofing

- Firewall configuration disclosure

3.3 Resource replica locations

Popular web and FTP resources are often replicated on different servers for fault tolerance and load sharing. Given a URL for one copy of a resource, RESCAP might be used to find another copy.

[[[NOTE: DNS NAPTR, etc., might be better used for this purpose]]]

Type of resource:

- Anything with a URL or URI.

Type of metadata:

- Resource location information

Security threats:

- Unauthorized access
- Response spoofing
- Firewall configuration disclosure

3.4 Alternative or associated URLs

A network resource may have associated or alternative URLs. For example, to access the resource using a different protocol, to access different versions of a resource or to access associated information about a resource.

Type of resource:

- Anything with a URL or URI.

Type of metadata:

- Resource location information

Security threats:

- Unauthorized access
- Response spoofing
- Firewall configuration disclosure

3.5 Capabilities at a telephone number

Convergence between the Internet and telephone networks is leading to resources and endpoints accessed from the Internet being identified by telephone numbers. A simple telephone number does little to indicate the kinds of service available at that endpoint, or the protocols that may be used to access the facilities provided.

In some cases, communication with an endpoint identified by a telephone number may take place entirely over the Internet, in which case it is necessay to know which Internet protocols should be employed (e.g. H.323, SIP, Internet fax, VPIM, etc.).

Type of resource:

- Communication service endpoints tradtionally associated with the telephone network: voice, voice messaging, fax, etc.

Type of metadata:

- Media feature expression
- Security options
- MIME handling options
- General capabilities and preferences
- [[[Access billing information???]]]

Security threats:

- Unauthorized access or disclosure
- Response spoofing
- Data mining
- Traffic analysis

3.6 Public key distribution

To conduct secure communications with a given endpoint, a suitable public key for that endpoint may be needed. RESCAP could be one useful way to publish public key information.

Type of resource:

- Any communication endpoint

Type of metadata:

- Security options

Security threats:

- The usual issues associated with public key distribution.

3.7 Recognized certification authorities

In the absence of an X.509 style global root for authorizing public keys, one of the challenges to securing communication with public key cryptography is to find a certification authority (CA) that is directly or indirectly trusted by both parties.

Having each party publish details of the CAs that it recognizes may help in establishing a chain of trust between the communicating parties.

Type of resource:

- Any communication endpoint

Type of metadata:

- X.509 Certification Authorities

[[[What is PGP equivalent?]]]

Security threats:

- The usual issues associated with public key distribution.

- Exposure of potentially weak security

3.8 Internet fax capabilities

Internet fax uses e-mail protocols to emulate a fax-like service within the Internet e-mail environment. One problem with this is that the endpoint identification and capability exchange associated with traditional facsimile is not provided by the e-mail protocols. RESCAP may provide an alternatuve way to access such information, particularly with respect to receiver capabilities.

Even if the proposed content negotiation framework is deployed, using RESCAP to obtain capability information cam optimize the process by reducing the number of occasions on which additional message round trips will be needed.

Type of resource:

- a mailbox, identified by a 'mailto:' URL [1, 2].

Type of metadata:

- Level of Internet fax support (e.g. "simple", "extended", "full", "none").
- Media feature expression
- Security options
- MIME handling options
- General capabilities and preferences

Security threats:

- Unauthorized access or disclosure
- Response spoofing
- Data mining

3.9 VPIM voice messagiong capabilities

VPIM uses e-mail protocols to transfer voice messages within the Internet e-mail environment. RESCAP may provide a way to access vital information about VPIM receiver caabilities.

Type of resource:

- a mailbox, identified by a 'mailto:' URL [1, 2].

Type of metadata:

- Level of VPIM support (e.g. "V2", "IVM", support for message privacy options such as "do not forward").
- Media feature expression (especially for indicating supported audio codecs).
- Security options
- MIME handling options
- General capabilities and preferences

Security threats:

- Unauthorized access or disclosure
- Response spoofing
- Data mining

3.10 IPP printer capabilities

IPP uses a protocol modeled on HTTP to transfer print images for remote printing, and to control the print process.

Although IPP allows printer capabilities to be interrogated, RESCAP might be used as a more efficient way to find such information, particularly in a phase of printer discovery.

Type of resource:

- IPP printer, identified by an 'ipp:' URL (String)

Type of metadata:

- IPP capability informaton
- Other resource metadata

Security threats:

- Unauthorized access
- Response spoofing
- Firewall configuration disclosure

3.11 Presence protocol supplementary information

There has been much discussion both within and outside the IMPP working group about the use of a presence protocol to distribute capability information. A problem is that it cxan be difficult to know how far it is reasonable to go in adding supplementary information to what should be a very lightweight indication of "available/not-available" presence informaton.

One way to address this problem is to restrict the presence information to genuine dynamic status information, and to use RESCAP to access any (less dynamic) supplementary information about a contact point described by presence information.

Type of resource:

- Presence information contact address -- as a URL.

Type of metadata:

- General preference and capability information (esp. vCard)
- Media feature expression

Security threats:

- Unauthorized access
- Response spoofing
- Firewall configuration disclosure
- Data mining

4. Resource capability data

Try to draw line between a capability resolution service and a content deivery service.

4.1 Media feature expression

4.2 Security options

4.2.1 S/MIME capabilities

S/MIME related capabilities [3,4,5, and associated documents].

- S/MIME signature types that can be verified (list of strings; e.g. "id-dsa", "rsaEncryption").
- S/MIME public signing key certificates (list of arbitrary binary values).
- S/MIME public encrypting key certificates (list of arbitrary binary values).
- S/MIME public key-certificaton key certificates - used by agents acting in a certifying authority (CA) role (list of arbitrary binary values).
- Resonds to requests for S/MIME signed receipts? (Boolean).

- Recognizes and interprets S/MIME security labels? (Boolean).

- Acts as an S/MIME secure mailing list? (Boolean).

- Handles signed 'SigningCertificate' attribute? (Boolean).

4.2.2 OpenPGP

OpenPGP related capabilities [6, and associated documents].

- OpenPGP signature types that can be verified (list of strings; e.g. "DSA", "RSA").

- OpenPGP public signing key certificates (list of arbitrary binary values).

- OpenPGP public encrypting key certificates (list of arbitrary binary values).

- OpenPGP public key-certificaton key certificates (list of arbitrary binary values).

4.2.3 Channel security

[[[Details of keys, etc., applicable to channel security mechanisms, such as TLS]]]

4.2.4 Network security

[[[Details of keys, etc., applicable to channel netwrk mechanisms, such as IPSEC]]]

4.2.5 X.509 certification authority

- List of X.509 certification authorities directly trusted by a party (List of strings containing X.509 distinguished names).

4.3 MIME handling options

The attributes in this section describe MIME handling capabilities [7,8].

- Plain text only - MIME not recognized (Boolean).

- Supports MIME header extensions [9] (Boolean).

- Supports MIME parameter extensions [10] (Boolean).

- Character sets [11] displayed (String, containing CONNEG media feature expression [12], containg character set feature tags [13] in simple disjunctive form).

- Preferred languages [14] (String, containing CONNEG media feature expression [12], containg language feature tags [13] in simple disjunctive form).

- Display line length in characters (Integer).

- Can handle MHTML [15]? (Boolean).

- Can handle Content-MD5 [16]? (Boolean).

- Can handle mailing list URLs? (Boolean).

- Can recognize and respond to MDN requests [18]? (Boolean)

- Can act as an iCalendar and iMIP agent [19]? (Boolean)

4.4 General capabilities and preferences

This section lists some general capabilities that may be significant to a message sender.

Unsolicited bulk e-mail preferences. (List of pairs of strings, each of which is a policy name and an associated value).

Mailing list information. (String containing a list of RFC 822 headers [20]).

vCard information [21]. (String containing information in vCard format.)

Associated e-mail addresses. (List of pairs of strings; each pair is an e-mail address and description of that address, such as "home", "work", etc.).

4.5 Resource location information

Resource location(s) can be described using a URL or a list of URLs:

- Single location: URL (String)

- Multiple locations: list of URLs (List of strings).

5. RESCAP security threats

In considering security for RESCAP, note that the general presumtpion is that the information being provided is public. But completely unrestricted access may be inappropriate because that would create an exposure to privacy invasion through data mining activities. Also, there may be requirements to disclose some information only within a closed community.

[[[The rest of this section has yet to be fleshed out]]]

5.1 Unauthorized access or disclosure

Access controls

5.2 Response spoofing

5.3 Traffic analysis

5.4 Data mining (privacy)

5.5 Firewall configuration disclosure

5.6 Denial of service

6. Security considerations

[[[Additional points?]]]

6.1 Authentication

Note that there are a number of diferent authentication cases to be considered:

- Server to client
- Client to server
- Request to server
- Response to client

7. Acknowledgements

The initial list of scenarios was largely culled from an informal meeting of RESCAP working group participants, and from Paul Hoffman's RESCAP profile for mail user agents.

8. References

[[[Full citations to be supplied]]]

[1] RFC 821, "Simple Mail Transfer Protocol"

[2] "mailto: URL"

[3] SMIME-MSG

[4] SMIME-CERT

[5] SMIME-ESS

[6] OpenPGP

[7] RFC 2045, MIME

[8] RFC 2046, MIME

[9] RFC 2047, MIME extensions

[10] MIME parameter extensions

[11] Charset registry

[12] RFC 2533, Media feature expressions

[13] CONNEG charset/language tags

[14] Language code registry

[15] MHTML

[16] Content-MD5

[17] Mailing list URLs

[18] RFC 2298, MDNs

[19] iCalendar/iMIP

[20] Mailing list headers

[21] vCard format

[22] RFC 2168, URN resolution and DNS NAPTR record

[xx] "xxx"
xxx, yyy
Internet draft: <xxx>
Work in progress, xxx yyyy

8. Author's address

Graham Klyne,
MIMEsweeper Group,
1310 Waterside,
Arlington Business Park
Theale
Reading, RG7 4SA
United Kingdom.
Telephone: +44 118 930 1300
Facsimile: +44 118 930 1301
E-mail: GK-ResCap@ninebynine.org

Appendix A: Amendment history

00a	30-Mar-2000	Memo initially created.
01a	09-Jan-2002	Reissued to Internet-drafts, without significant change.

TODO

Full copyright statement

Copyright (C) The Internet Society 2002. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assigns.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.