Network Working Group
Internet Draft
Intended status: Standards Track
Expires: July 28, 2013

Paul E. Jones
Gonzalo Salgueiro
Cisco Systems
Joseph Smarr
Google

January 28, 2013

WebFinger
draft-ietf-appsawg-webfinger-09.txt

Abstract

This specification defines the WebFinger protocol, which can be used to discover information about people or other entities on the Internet using standard HTTP methods.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on July 28, 2013.

Copyright Notice

Table of Contents

1. Introduction

WebFinger is used to discover information about people or other entities on the Internet that are identified by a URI [6] or IRI [7] using standard Hypertext Transfer Protocol (HTTP) [2] methods over a secure transport [14]. A WebFinger server returns a JavaScript Object Notation (JSON) [5] object that describes a resource that is queried. The JSON object is referred to as the JSON Resource Descriptor (JRD).

For a person, the kinds of information that might be discoverable via WebFinger include a personal profile address, identity service, telephone number, or preferred avatar. For other entities on the Internet, a WebFinger server might return JRDs containing link relations that allow a client to discover, for example, the amount of toner in a printer or the physical location of a server.

Information returned via WebFinger might be for direct human consumption (e.g., looking up someone's phone number), or it might be used by systems to help carry out some operation (e.g., facilitate logging into a web site by determining a user's identity service).

Use of WebFinger is illustrated in the examples in Section 3 and described more formally in Section 4.

2. Terminology

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 RFC 2119 [1].

WebFinger makes heavy use of "Link Relations". Briefly, a Link Relation is an attribute and value pair used on the Internet wherein the attribute identifies the type of link to which the associated value refers. In HTTP and Web Linking [4], the attribute is a "rel" and the value is an "href". WebFinger also uses the "rel" attribute, where the "rel" value is either a single IANA-registered link relation type [10] or a URI [6].

3. Example Uses of WebFinger

This non-normative section shows a few sample uses of WebFinger.

3.1. Locating a User's Blog

Assume you receive an email from Bob and he refers to something he posted on his blog, but you do not know where Bob's blog is located. It would be simple to discover the address of Bob's blog if he makes that information available via WebFinger.

Assume your email client can discover the blog for you. After receiving the message from Bob (bob@example.com), you instruct your email client to perform a WebFinger query. It does so by issuing the following HTTPS [14] query to example.com:

```
GET /.well-known/webfinger?
                      resource=acct%3Abob%40example.com HTTP/1.1
Host: example.com
```

The server might then respond with a message like this:

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=UTF-8

{
```

```
      "expires" : "2012-11-16T19:41:35Z",
      "subject" : "acct:bob@example.com",
      "aliases" :
      [
        "http://www.example.com/~bob/"
      ],
      "properties" :
      {
          "http://example.com/ns/role/" : "employee"
      },
      "links" :
      [
        {
          "rel" : "http://webfinger.net/rel/avatar",
          "type" : "image/jpeg",
          "href" : "http://www.example.com/~bob/bob.jpg"
        },
        {
          "rel" : "http://webfinger.net/rel/profile-page",
          "href" : "http://www.example.com/~bob/"
        },
        {
          "rel" : "blog",
          "type" : "text/html",
          "href" : "http://blogs.example.com/bob/",
          "titles" :
          {
              "en-us" : "The Magical World of Bob",
              "fr" : "Le monde magique de Bob"
          }
        },
        {
          "rel" : "vcard",
          "href" : "https://www.example.com/~bob/bob.vcf"
        }
      ]
    }
```

The email client would take note of the "blog" link relation in the above JRD that refers to Bob's blog. This URL would then be presented to you so that you could then visit his blog. The email client might also note that Bob has published an avatar link relation and use that picture to represent Bob inside the email client. Lastly, the client might consider the vcard [16] link relation in order to update contact information for Bob.

In the above example, an "acct" URI [8] is used in the query, though any valid alias for the user might also be used. See section 4.5 for

more information on WebFinger and URIs.

An alias is a URI that is different from the "subject" URI that identifies the same entity. In the above example, there is one "http" alias returned, though there might have been more than one. Had the "http:" URI shown as an alias been used to query for information about Bob, the query would have appeared as:

```
GET /.well-known/webfinger?
         resource=http%3A%2F%2Fwww.example.com%2F~bob%2F HTTP/1.1
Host: www.example.com
```

Note that the host queried in this example is different than for the acct URI example, since the URI refers to a different host. Either this host would provide a response, or it would redirect the client to another host (e.g., redirect back to example.com). Either way, the response would have been substantially the same, with the subject and alias information changed as necessary. Other information, such as the expiration time might also change, but the set of link relations and properties would be the same with either response.

3.2. Identity Provider Discovery for OpenID Connect

Suppose Carol wishes to authenticate with a web site she visits using OpenID Connect [18]. She would provide the web site with her OpenID Connect identifier, say carol@example.com. The visited web site would perform a WebFinger query looking for the OpenID Connect Provider. Since the site is interested in only one particular link relation, the server might utilize the "rel" parameter as described in Section 4.3:

```
GET /.well-known/webfinger?
  resource=acct%3Acarol%40example.com&
  rel=http%3A%2F%2Fopenid.net%2Fspecs%2Fconnect%2F1.0%2Fissuer
  HTTP/1.1
Host: example.com
```

The server might respond with a JRD like this:

```
{
  "expires" : "2012-11-16T19:41:35Z",
  "subject" : "acct:carol@example.com",
  "links" :
  [
    {
      "rel" : "http://openid.net/specs/connect/1.0/issuer",
      "href" : "https://openid.example.com"
    }
  ]
}
```

Since the "rel" parameter only filters the link relations returned by the server, other name/value pairs in the response, including any aliases or properties, would be returned. Also, since support for the "rel" parameter is optional, the client must not assume the "links" array will contain only the requested link relation.

3.3. Auto-Configuration of Email Clients

WebFinger could be used to auto-provision an email client with basic configuration data. Suppose that sue@example.com wants to configure her email client. Her email client might issue the following query:

```
GET /.well-known/webfinger?
         resource=mailto%3Asue%40example.com HTTP/1.1
Host: example.com
```

The response from the server would contain entries for the various protocols, transport options, and security options. If there are multiple options, the server might return a link relation that for each of the valid options and the client or Sue might select which option to choose. Since JRDs list link relations in a specific order, then the most-preferred choices could be presented first. Consider this response:

```
{
  "subject" : "mailto:sue@example.com",
  "links" :
  [
    {
      "rel" : "http://example.net/rel/smtp-server",
      "properties" :
      {
        "http://example.net/email/host" : "smtp.example.com",
        "http://example.net/email/port" : "587",
        "http://example.net/email/login-required" : "yes",
        "http://example.net/email/transport" : "starttls"
      }
    },
    {
      "rel" : "http://example.net/rel/imap-server",
      "properties" :
      {
        "http://example.net/email/host" : "imap.example.com",
        "http://example.net/email/port" : "993",
        "http://example.net/email/transport" : "ssl"
      }
    }
  ]
```

```
}
```

In this example, you can see that the WebFinger server advertises an SMTP service and an IMAP service. In this example, the "href" entries associated with the link relation are absent. This is valid when there is no external reference that needs to be made.

3.4. Retrieving Device Information

As another example, suppose there are printers on the network and you would like to check the current toner level for a particular printer identified via the URI device:p1.example.com. While the "device" URI scheme is not presently specified, we use it here for illustrative purposes.

Following the procedures similar to those above, a query may be issued to get link relations specific to this URI like this:

```
GET /.well-known/webfinger?
                  resource=device%3Ap1.example.com HTTP/1.1
Host: p1.example.com
```

The link relations that are returned for a device may be quite different than those for user accounts. Perhaps we may see a response like this:

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=UTF-8

{
  "subject" : "device:p1.example.com",
  "links" :
  [
    {
      "rel" : "http://example.com/rel/tipsi",
      "href" : "http://192.168.1.5/npap/"
    }
  ]
}
```

While this example is fictitious, you can imagine that perhaps the Transport Independent, Printer/System Interface [17] may be enhanced with a web interface that allows a device that understands the TIP/SI web interface specification to query the printer for toner levels.

4. WebFinger Protocol

WebFinger is a simple HTTP-based web service that returns a JSON Resource Descriptor (JRD) to convey information about an entity on

the Internet and the Cross-Origin Resource Sharing (CORS) [9] specification to facilitate queries made via a web browser.

4.1. Constructing a WebFinger Query

This specification defines URI parameters that are passed from the client to the server when issuing a request. These parameters, "resource" and "rel", and the parameter values are included in the "query" component of the URI (see Section 3.4 of RFC 3986). To construct the "query" component, the client performs the following steps. First, each parameter value is percent-encoded as per Section 2.1 of RFC 3986. Next, the client constructs a string to be placed in the query component by concatenating the name of the first parameter together with an equal sign ("=") and the percent-encoded parameter value. For any subsequent parameters, the client appends an ampersand ("&") to the string, the name of the next parameter, an equal sign, and percent-encoded parameter value. The client MUST NOT insert any spaces while constructing the string. The order in which the client places each parameter and its corresponding parameter value is unspecified.

4.2. Performing a WebFinger Query

A WebFinger client issues a query to the well-known [3] resource /.well-known/webfinger. A query MUST include the "resource" parameter exactly once and set to the value of the URI for which information is being sought. If the "resource" parameter is absent or malformed, the WebFinger server MUST indicate that the request is bad as per Section 10.4.1 of RFC 2616 [2].

A client MUST query the WebFinger server using HTTPS only. If the client determines that the server has an invalid certificate, the server returns a 4xx or 5xx status code, or the HTTPS connection cannot be established for any reason, the client MUST accept that the WebFinger query has failed and MUST NOT attempt to reissue the WebFinger request using HTTP over a non-secure connection.

A WebFinger server MUST return a JRD as the representation for the resource if the client requests no other supported format explicitly via the HTTP "Accept" header. The client MAY include the "Accept" header to indicate a desired representation, though no other representation than JRD is defined in this specification. The media type used for the JSON Resource Descriptor (JRD) is "application/json" [5].

A WebFinger server MAY redirect the client, but MUST only redirect the client to an HTTPS URI.

A WebFinger server can include cache validators in a response to enable conditional requests by the client and/or expiration times as per Section 13 of RFC 2616.

4.3. The "rel" Parameter

When issuing a request to the server, the client MAY utilize the "rel" parameter to request only a subset of the information that would otherwise be returned without the "rel" parameter. When the "rel" parameter is used, only the link relations that match the link relations provided via "rel" are included in the array of links returned in the JRD. All other information normally present in a resource descriptor is present in the resource descriptor, even when "rel" is employed.

The "rel" parameter MAY be transmitted to the server multiple times in order to request multiple types of link relations.

The purpose of the "rel" parameter is to return a subset of resource's link relations. Use of the parameter might reduce processing requirements on either the client or server, and it might also reduce the bandwidth required to convey the partial resource descriptor, especially if there are numerous link relation values to convey for a given resource.

Support for the "rel" parameter is OPTIONAL, but RECOMMENDED on the server. Should the server not support the "rel" parameter, it MUST ignore it and process the request as if no "rel" parameter values were present.

The following example presents the same example as found in Section 3.1, but uses the "rel" parameter in order to select two link relations:

```
GET /.well-known/webfinger?
          resource=acct%3Abob%40example.com&
          rel=http%3A%2F%2Fwebfinger.net%2Frel%2Fprofile-page&
          rel=vcard HTTP/1.1
Host: example.com
```

In this example, the client requests the link relations of type "http://webfinger.net/rel/profile-page" and "vcard". The server then responds with a message like this:

```
HTTP/1.1 200 OK
Access-Control-Allow-Origin: *
Content-Type: application/json; charset=UTF-8

{
```

```
      "expires" : "2012-11-16T19:41:35Z",
      "subject" : "acct:bob@example.com",
      "aliases" :
      [
        "http://www.example.com/~bob/"
      ],
      "properties" :
      {
          "http://example.com/ns/role/" : "employee"
      },
      "links" :
      [
        {
          "rel" : "http://webfinger.net/rel/profile-page",
          "href" : "http://www.example.com/~bob/"
        },
        {
          "rel" : "vcard",
          "href" : "http://www.example.com/~bob/bob.vcf"
        }
      ]
    }
```

As you can see, the server returned only the link relations requested by the client, but also included the other parts of the JRD.

In the event that a client requests links for link relations that are not defined for the specified resource, a resource descriptor MUST be returned. In the returned JRD, the "links" array MAY be absent, empty, or contain only links that did match a provided "rel" value.

4.4. The JSON Resource Descriptor (JRD)

The JSON Resource Descriptor (JRD), originally introduced in RFC 6415 [19] and based on the Extensible Resource Descriptor (XRD) format [20], is a JSON object that is comprised of the following name/value pairs:

- expires
- subject
- aliases
- properties
- links

The members "expires" and "subject" are name/value pairs whose value are strings, "aliases" is an array of strings, "properties" is an object comprised of name/value pairs whose values are strings, and "links" is an array of objects that contain link relation

information.

When processing a JRD, the client MUST ignore any unknown member and not treat the presence of an unknown member as an error.

Below, each of these members of the JRD is described in more detail.

4.4.1. expires

The value of the "expires" member is a string that indicates the date and time after which the JRD SHOULD be considered expired and no longer utilized.

This format is formally defined in RFC 3339 [15].

The "expires" member MUST NOT use fractional seconds and MUST express time only Universal Coordinate Time via the "Z" designation on the end of the string.

An example of the "expires" member is:

```
"expires" : "2012-11-16T19:41:35Z"
```

The "expires" member is optional in a JRD, but SHOULD be honored if present.

4.4.2. subject

The value of the "subject" member is a URI that identifies the entity that the JRD describes.

The "subject" value returned by a WebFinger server MAY differ from the value of the "resource" parameter used in the client's request. This may happen, for example, when the subject's identity changes (e.g., a user moves his or her account to another service) or when the server prefers to express URIs in canonical form.

The "subject" member MUST be present.

4.4.3. aliases

The "aliases" array is an array of zero or more URI strings that identify the same entity as the "subject" URI. Each URI must be an absolute URI.

The "aliases" array is optional.

4.4.4. properties

The "properties" object is comprised of zero or more name/value pairs whose names are absolute URIs and whose values are strings or null.

Properties are used to convey additional information about the subject of the JRD. As an example, consider this use of "properties":

```
"properties" : { "http://webfinger.net/ns/name" : "Bob Smith" }
```

The "properties" member is optional.

4.4.5. links

The "links" array contains zero or more elements that contain the link relation information. Each element of the array is an object comprised of the following name/value pairs:

- rel
- type
- href
- titles
- properties

The members "rel", "type", and "href" are a name/value pairs whose values are strings, "titles" and "properties" are objects comprised of name/value pairs whose values are strings.

The order of elements in the "links" array indicates an order of preference. Thus, if there are two or more link relations having the same "rel" value, the first link relation would indicate the user's preferred link relation.

The "links" array is optional in the JRD.

Below, each of the members of the objects found in the "links" array is described in more detail. Each object in the "links" array, referred to as a "link relation object", is completely independent from any other object in the array; any requirement to include a given member in the link relation object refers only to that particular object.

4.4.5.1. rel

The value of the "rel" member is a string that is either an absolute URI or a registered relation type [10] (see RFC 5988 [4]). The value of the "rel" member MUST contain exactly one URI string or registered relation type and MUST NOT contain a space-separated list of URIs or registered relation types. The URI or registered relation type identifies the type of the link relation. The other members of the object have meaning only once the type of link relation is understood. In some instances, the link relation will have associated semantics that allow a client to query for other resources

on the Internet. In other instances, the link relation will have associated semantics that allow the client to utilize the other members of the link relation object without fetching additional external resources.

The "rel" member MUST be present in the link relation object.

4.4.5.2. type

The value of the "type" member is a string that indicates the media type [11] of the linked resource (see RFC 4288 [12]).

The "type" member is optional in the link relation object.

4.4.5.3. href

The value of the "href" member is a string that contains a URI pointing to the linked resource.

The "href" member is optional in the link relation object.

4.4.5.4. titles

The "titles" object is comprised of zero or more name/value pairs whose name is a language tag [13] or the string "default". The string is human-readable and describes the link relation. More than one title for the link relation MAY be provided for the benefit of users who utilize the link relation and, if used, a language identifier SHOULD be duly used as the name. If the language is unknown or unspecified, then the name is "default".

A JRD SHOULD NOT include more than one title identified with the same language tag (or "default") within the link relation object. Meaning is undefined if a link relation object includes more than one title named with the same language tag (or "default"), though this MUST NOT treat this as an error. A client MAY select whichever title or titles it wishes to utilize.

Here is an example of the titles object:

```
"titles" :
{
  "en-us" : "The Magical World of Bob",
  "fr" : "Le monde magique de Bob"
}
```

The "titles" member is optional in the link relation object.

4.4.5.5. properties

The "properties" object within the link relation object is comprised of zero or more name/value pairs whose names are absolute URIs and whose values are strings or null. Properties are used to convey additional information about the link relation. As an example, consider this use of "properties":

```
"properties" : { "http://example.net/mail/port" : "993" }
```

The "properties" member is optional in the link relation object.

4.5. WebFinger and URIs

WebFinger requests can include a parameter specifying the URI of an account, device, or other entity. WebFinger is agnostic regarding the scheme of such a URI: it could be an "acct" URI [7], an "http" or "https" URI, a "mailto" URI [21], or some other scheme.

For resources associated with a user account at a host, use of the "acct" URI scheme is RECOMMENDED, since it explicitly identifies an account accessible via WebFinger. Further, the "acct" URI scheme is not associated with other protocols as, by way of example, the "mailto" URI scheme is associated with email. Since not every host offers email service, using the "mailto" URI scheme is not ideal for identifying user accounts on all hosts. That said, use of the "mailto" URI scheme would be ideal for use with WebFinger to discover mail server configuration information for a user.

5. Cross-Origin Resource Sharing (CORS)

WebFinger resources might not be accessible from a web browser due to "Same-Origin" policies. The current best practice is to make resources available to browsers through Cross-Origin Resource Sharing (CORS) [9], and servers MUST include the Access-Control-Allow-Origin HTTP header in responses. Servers SHOULD support the least restrictive setting by allowing any domain access to the WebFinger resources:

```
Access-Control-Allow-Origin: *
```

There are cases where defaulting to the least restrictive setting is not appropriate, for example a WebFinger server on an intranet that provides sensitive company information should not allow CORS requests from any domain, as that could allow leaking of that sensitive information. A WebFinger server that wishes to restrict access to information from external entities SHOULD use a more restrictive Access-Control-Allow-Origin header.

6. Access Control

As with all web resources, access to the /.well-known/webfinger resource MAY require authentication. Further, failure to provide required credentials MAY result in the server forbidding access or providing a different response than had the client authenticated with the server.

Likewise, a server MAY provide different responses to different clients based on other factors, such as whether the client is inside or outside a corporate network. As a concrete example, a query performed on the internal corporate network might return link relations to employee pictures, whereas link relations for employee pictures might not be provided to external entities.

Further, link relations provided in a WebFinger server response MAY point to web resources that impose access restrictions. For example, the aforementioned corporate server may provide both internal and external entities with URIs to employee pictures, but further authentication might be required in order for the client to access the picture resources if the request comes from outside the corporate network.

The decisions made with respect to what set of link relations a WebFinger server provides to one client versus another and what resources require further authentication, as well as the specific authentication mechanisms employed, are outside the scope of this document.

7. Hosted WebFinger Services

As with most services provided on the Internet, it is possible for a domain owner to utilize "hosted" WebFinger services. By way of example, a domain owner might control most aspects of their domain, but use a third-party hosting service for email. In the case of email, mail servers for a domain are identified by MX records. An MX record points to the mail server to which mail for the domain should be delivered. It does not matter to the sending mail server whether those MX records point to a server in the destination domain or a different domain.

Likewise, a domain owner might utilize the services of a third party to provide WebFinger services on behalf of its users. Just as a domain owner was required to insert MX records into DNS to allow for hosted email serves, the domain owner is required to redirect HTTP queries to its domain to allow for hosted WebFinger services.

When a query is issued to /.well-known/webfinger, the web server MUST return a response with a redirection status code that includes a

Location header pointing to the location of the hosted WebFinger service URL. The WebFinger service URL does not need to point to /.well-known/* on the hosting service provider server.

As an example, assume that example.com's WebFinger services are hosted by example.net. Suppose a client issues a query for acct:alice@example.com like this:

```
GET /.well-known/webfinger?
              resource=acct%3Aalice%40example.com HTTP/1.1
Host: example.com
```

The server might respond with this:

```
HTTP/1.1 307 Temporary Redirect
Access-Control-Allow-Origin: *
Location: https://wf.example.net/example.com/webfinger?
                  resource=acct%3Aalice%40example.com HTTP/1.1
```

The client can then follow the redirection, re-issuing the request to the URL provided in the Location header. Note that the server will include any required URI parameters in the Location header value, which could be different than the URI parameters the client originally used.

8. Security Considerations

Since this specification utilizes Cross-Origin Resource Sharing (CORS) [9], all of the security considerations applicable CORS are also applicable to this specification.

The required use of HTTPS is to ensure that information is not modified during transit. It should be appreciated that in environments where a web server is normally available, there exists the possibility that a compromised network might have its WebFinger server operating on HTTPS replaced with one operating only over HTTP. As such, clients MUST NOT issue queries over a non-secure connection.

Clients MUST verify that the certificate used on an HTTPS connection is valid and accept a response only if the certificate is valid.

Service providers and users should be aware that placing information on the Internet accessible through WebFinger means that any user can access that information. While WebFinger can be an extremely useful tool for allowing quick and easy access to one's avatar, blog, or other personal information, users should understand the risks, too. If one does not wish to share certain information with the world, do not allow that information to be freely accessible through WebFinger and do not use any service supporting WebFinger. Further, a

WebFinger server MUST NOT be used to provide any personal information to any party unless explicitly or implicitly authorized by the person whose information is being shared. Implicit authorization can be determined by the user's voluntary utilization of a service as defined by that service's relevant terms of use or published privacy policy.

The aforementioned word of caution is perhaps worth emphasizing again with respect to dynamic information one might wish to share, such as the current location of a user. WebFinger can be a powerful tool used to assemble information about a person all in one place, but service providers and users should be mindful of the nature of that information shared and the fact that it might be available for the entire world to see. Sharing location information, for example, would potentially put a person in danger from any individual who might seek to inflict harm on that person.

The easy access to user information via WebFinger was a design goal of the protocol, not a limitation. If one wishes to limit access to information available via WebFinger, such as a WebFinger server for use inside a corporate network, the network administrator must take measures necessary to limit access from outside the network. Using standard methods for securing web resources, network administrators do have the ability to control access to resources that might return sensitive information. Further, a WebFinger server can be employed in such a way as to require authentication and prevent disclosure of information to unauthorized entities.

Finally, a WebFinger server has no means of ensuring that information provided by a user is accurate. Likewise, neither the server nor the client can be absolutely guaranteed that information has not been manipulated either at the server or along the communication path between the client and server. Use of HTTPS helps to address some concerns with manipulation of information along the communication path, but it clearly cannot address issues where the server provided incorrect information, either due to being provided false information or due to malicious behavior on the part of the server administrator. As with any information service available on the Internet, users should wary of information received from untrusted sources.

9. IANA Considerations

This specification registers the "webfinger" well-known URI in the Well-Known URI Registry as defined by [3].

URI suffix: webfinger

Change controller: IETF

Specification document(s): RFC QQQ

Related information: The response from WebFinger server will be a JSON Resource Descriptor (JRD) as described in section 4.4 of RFC QQQ.

[RFC EDITOR: Please replace "QQQ" references in this section with the number for this RFC.]

10. Acknowledgments

The authors would like to acknowledge Eran Hammer-Lahav, Blaine Cook, Brad Fitzpatrick, Laurent-Walter Goix, Joe Clarke, Michael B. Jones, Peter Saint-Andre, Dick Hardt, Tim Bray, and Joe Gregorio for their invaluable input.

11. References

11.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999.

[3] Nottingham, M., Hammer-Lahav, E., "Defining Well-Known Uniform Resource Identifiers (URIs)", RFC 5785, April 2010.

[4] Nottingham, M., "Web Linking", RFC 5988, October 2010.

[5] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)", RFC 4627, July 2006.

[6] Berners-Lee, T., Fielding, R., and Masinter, L., "Uniform Resource Identifier (URI): Generic Syntax", STD 66, RFC 3986, January 2005.

[7] Duerst, M., "Internationalized Resource Identifiers (IRIs)", RFC 3987, January 2005.

[8] Saint-Andre, P., "The 'acct' URI Scheme", draft-ietf-appsawg-acct-uri-02, December 2012.

[9] Van Kesteren, A., "Cross-Origin Resource Sharing", W3C CORS http://www.w3.org/TR/cors/, July 2010.

[10] IANA, "Link Relations", http://www.iana.org/assignments/link-relations/.

[11] IANA, "MIME Media Types", http://www.iana.org/assignments/media-types/index.html.

[12] Freed, N., Klensin, J., "Media Type Specifications and Registration Procedures", RFC 4288, December 2005.

[13] Phillips, A., Davis, M., "Tags for Identifying Languages", RFC 5646, January 2001.

[14] Rescorla, E., "HTTP Over TLS", RFC 2818, May 2000.

[15] Klyne, G., Newman, C., "Date and Time on the Internet: Timestamps", RFC 3339, July 2002.

11.2. Informative References

[16] Perreault, S., "vCard Format Specification", RFC 6350, August 2011.

[17] "Transport Independent, Printer/System Interface", IEEE Std 1284.1-1997, 1997.

[18] Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., Mortimore, C., and E. Jay, "OpenID Connect Messages 1.0", June 2012, http://openid.net/specs/openid-connect-messages-1_0.html.

[19] Hammer-Lahav, E. and Cook, B., "Web Host Metadata", RFC 6415, October 2011.

[20] Hammer-Lahav, E. and W. Norris, "Extensible Resource Descriptor (XRD) Version 1.0", http://docs.oasis-open.org/xri/xrd/v1.0/xrd-1.0.html.

[21] Duerst, M., Masinter, L., and J. Zawinski, "The 'mailto' URI Scheme", RFC 6068, October 2010.

Author's Addresses

Paul E. Jones
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA

Phone: +1 919 476 2048
Email: paulej@packetizer.com
IM: xmpp:paulej@packetizer.com

Gonzalo Salgueiro
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA

Phone: +1 919 392 3266
Email: gsalguei@cisco.com
IM: xmpp:gsalguei@cisco.com

Joseph Smarr
Google

Email: jsmarr@google.com