Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2018

V. Bertola
Open-Xchange
M. Sanz
DENIC eG
October 18, 2017

OpenID Connect DNS-based Discovery
draft-sanz-openid-dns-discovery-00

Abstract

The following document describes a DNS-based mechanism for a client to discover an OpenID Identity Provider given an Identifier of the End-User, as a complementary alternative to the existing WebFinger-based mechanism.

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 https://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 April 21, 2018.

Copyright Notice

1. Introduction

"OpenID Connect Discovery 1.0" [OpenID.Discovery] uses WebFinger [RFC7033] to locate the OpenID Provider for an End-User in a process called "issuer discovery". While this mechanism has been in place for quite some time now and it has proven to work, it presents some operational inconveniences: A (dedicated) WebFinger service has to be setup and operated on top of an HTTPS server. Furthermore: in an OpenID deployment with distributed resources, each resource would have to be running its own WebFinger service to point to its issuer. This presents scaling/operating challenges, especially in a scenario where the deployment happens at Internet scale and each resource may use a different, personal domain name.

This document presents a lightweight discovery mechanism based on top of DNS (and DNS has to be setup anyway for the WebFinger approach to work). This so-called "DNS-based discovery" does not disrupt the existing discovery specification and is presented as an alternative discovery process, compatible to the existing issuer discovery process described in "OpenID Connect Discovery 1.0" [OpenID.Discovery] if interpreted as a so-called "out-of-band" mechanism.

Additionally the mechanisms described in this document enrich the discovery process by allowing to discover not only the issuer, but also potential Claims Providers [OpenID.Core] available for a given End-User identifier.

2. Requirements Notation and Conventions

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 [RFC2119].

Throughout this document, values are quoted to indicate that they are to be taken literally. When using these values in protocol messages, the quotes MUST NOT be used as part of the value.

3. DNS-based Discovery Resource Record

The format defined here has been inspired by the DMARC [RFC7489] and DKIM [RFC6376] specifications and some text passages have been directly copied from those standards to allow for a reading without following references.

DNS-based discovery metadata are stored as DNS TXT records in subdomains named "_openid". The underscore construct is used to define a semantic scope for DNS records that are associated with the

parent domain (s. "DNS Scoped Data Through Global '_Underscore' Naming of Attribute Leaves" [I-D.ietf-dnsop-attrleaf]).

For example, the domain owner of "myname.example.com" would post OpenID configuration in a TXT record at "_openid.myname.example.com". This DNS-located OpenID metadata will hereafter be called the "OpenID record".

To allow for the use of e-mail addresses as resources, the following additional rules are defined:

- In case the resource identifier contains at least one "@" character, the rightmost "@" character is replaced by the string "._openidemail.", which introduces an additional DNS subdomain inside the identifier's domain name.

- If any character in the resulting resource identifier is disallowed from use in domain names as per [RFC1035] section 2.3.1, the punycoding algorithm defined in [RFC3492] is applied.

Per [RFC1035] a TXT record can comprise several "character-string" objects. Where this is the case, the evaluator of the OpenID record must concatenate these strings by joining together the objects in order and parsing the result as a single string.

Content of OpenID records follow the extensible "tag=value" syntax for DNS-based key records defined in [RFC6376] and definition there applies. Specifically:

- Values are a series of strings containing either plain text or "base64" text (as defined in [RFC2045], Section 6.8). The definition of the tag will determine the encoding of each value.

- Unencoded semicolon (";") characters must not occur in the value, since that separates tag-value pairs.

- Whitespaces are allowed anywhere around tags. In particular, any whitespace after the "=" and any whitespace before a terminating ";" is not part of the value; however, whitespace inside the value is significant.

- Tags must be interpreted in a case-sensitive manner. Values must be processed as case sensitive unless the specific tag description of semantics specifies case insensitivity. Host and domain names in this context are to be compared in a case insensitive manner, per [RFC4343].

- Tags with duplicate names must not occur within a single tag-list; if a tag name does occur more than once, the entire tag-list is invalid.

- Tag=value pairs that represent the default value for optional records may be included to aid legibility.

- Unrecognized tags must be ignored.

- Tags that have an empty value are not the same as omitted tags. An omitted tag is treated as having the default value; a tag with an empty value explicitly designates the empty string as the value.

Only tags defined in this document or in later extensions are to be processed; note that given the rules of the previous paragraph, addition of a new tag into the registered list of tags does not itself require a new version of OpenID record to be generated (with a corresponding change to the "v" tag's value, see later), but a change to any existing tags does require a new version.

The following tags are introduced as the initial valid OpenID tags:

- v: Version (plain-text; REQUIRED). Identifies the record retrieved as a OpenID record. It must have the value of "OID1". The value of this tag must match precisely; if it does not or it is absent, the entire record must be ignored. It must be the first tag in the list.

- iss: The designated hostname for the Issuer (plain-text; REQUIRED). Internationalized domain names must be encoded as A-labels, as described in Section 2.3 of [RFC5890]. That hostname can be used as the issuer location of an OpenID Connect Discovery 1.0 (Section 4) Configuration Request to discover its relevant OpenID endpoints. The issuer can contain path components (e.g. "issuer.example.com/path").

- clp: The designated hostname for the Claims Provider (plain-text; OPTIONAL). Internationalized domain names must be encoded as A-labels, as described in Section 2.3 of [RFC5890]. That hostname can be used by Identity Providers as a claim source for aggregated or distributed claims. Support for Aggregated Claims and Distributed Claims is OPTIONAL in the OpenID Core specification, so is the usage of this tag. The value of this tag can contain path components (e.g. "provider.example.com/path").

The following is an example of a valid OpenID record for the domain example.com according to this specification:

```
_openid IN TXT "v=OID1;iss=auth.freedom-id.de;clp=identityagent.de"
```

Figure 1: Example OpenID record

4. DNS-based Issuer Discovery Process

DNS-based OpenID Provider Issuer discovery is the process of determining the location of the OpenID Provider with this specification.

DNS-based issuer discovery requires the following information to make a discovery request:

- resource - Identifier for the target End-User that is the subject of the discovery request
- host - Hostname target of the discovery DNS query

To start discovery of OpenID endpoints, the End-User supplies an Identifier to the Relying Party. The RP applies the same normalization rules to the Identifier as described in "OpenID Connect Discovery 1.0" [OpenID.Discovery] to determine the Resource and Host. It is worth mentioning that as result of those rules the resource could exactly match the host (e.g. resource is "example.com" and host is "example.com").

The RP will then follow the following lookup scheme:

1. The RP queries the DNS for an OpenID record at host. A possibly empty set of records is returned.
2. Records that do not start with a "v=" tag that identifies the current version of this document, or an older version of this document supported by the RP, are discarded. If a tag identifying the current version is found, all records identifying other versions are discarded. If no tag identifying the current version is found, but other tags identifying older versions are, the records using the latest supported version are kept, and all others are discarded.
3. If the remaining set contains multiple records or no records, the DNS-based discovery process terminates.
4. If the retrieved OpenID record does not contain a valid iss tag, the process terminates.

5. Once the Issuer has been extracted from the iss tag, the regular dynamic discovery process can be resumed in Section 4 "Obtaining OpenID Provider Configuration Information" of [OpenID.Discovery].

As already mentioned in [OpenID.Discovery] it is also worth noting that no relationship can be assumed between the user input Identifier string and the resulting Issuer location.

5. Security Considerations

DNS-based discovery depends directly on the security of the DNS. OpenID records must be ignored if not deployed in parallel with DNSSEC [RFC4033]. DNSSEC validation of OpenID records MUST be performed at all time before using them for any purpose. DNSSEC-validation errors must result in abortion of this DNS-based discovery process.

6. IANA Considerations

tbd

7. References

7.1. Normative References

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/info/rfc1035>.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC3492] Costello, A., "Punycode: A Bootstring encoding of Unicode for Internationalized Domain Names in Applications (IDNA)", RFC 3492, DOI 10.17487/RFC3492, March 2003, <https://www.rfc-editor.org/info/rfc3492>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005, <https://www.rfc-editor.org/info/rfc4033>.

[RFC4343] Eastlake 3rd, D., "Domain Name System (DNS) Case Insensitivity Clarification", RFC 4343, DOI 10.17487/RFC4343, January 2006, <https://www.rfc-editor.org/info/rfc4343>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/info/rfc5890>.

7.2. Informative References

[I-D.ietf-dnsop-attrleaf]
Crocker, D., "DNS Scoped Data Through Global '_Underscore' Naming of Attribute Leaves", draft-ietf-dnsop-attrleaf-02 (work in progress), March 2017.

[OpenID.Core]
Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., and C. Mortimore, "OpenID Connect Core 1.0", November 2014, <http://openid.net/specs/openid-connect-core-1_0.html>.

[OpenID.Discovery]
Sakimura, N., Bradley, J., Jones, M., and E. Jay, "OpenID Connect Discovery 1.0", November 2014, <http://openid.net/specs/openid-connect-discovery-1_0.html>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/info/rfc6376>.

[RFC7033] Jones, P., Salgueiro, G., Jones, M., and J. Smarr, "WebFinger", RFC 7033, DOI 10.17487/RFC7033, September 2013, <https://www.rfc-editor.org/info/rfc7033>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/info/rfc7489>.

Authors' Addresses

Vittorio Bertola
Open-Xchange

Email: vittorio.bertola@open-xchange.com
URI: https://www.open-xchange.com

Marcos Sanz
DENIC eG
Kaiserstrasse 75 - 77
Frankfurt am Main 60329
Germany

Email: sanz@denic.de
URI: https://www.denic.de