DDDS Application for Metadata Services

The goal of a Dynamic Delegation Discovery System (DDDS) application for metadata service discovery is to find URLs of specific types of metadata services, by using a DNS query string that represents an identity of a person or organization. In other words, the goal is to retrieve one or more URLs from the DNS that will enable finding out more about an entity’s enabled metadata services available in some DNS resource records (RRs).

The framework for such a DDDS application sets out what kinds of information must be specified:

* A DNS query string which is a string of concatenated, dot-separated labels.
* Types of DNS records to be retrieved.
* Values for fields within DNS record types that are used.
* Processing steps to be taken.

Because the goal is to find URLs, the NAPTR (“u”) RR type provides the core framework for producing the desired DDDS application. The service field of a NAPTR can distinguish distinct kinds of metadata services, or supporting services such as a service for registration to obtain access authorization for metadata services. DNS domain names of organizations or persons provide the core solution for query strings that may be used when trying to locate metadata services for persons or organizations.

So when “example.com” wants to announce the URL for one of its metadata services, its IT services group can add a NAPTR record such as:

IN NAPTR 100 10 "U" "Meta:CPPA" "!^.\*$!https://example.com/cppa?s=orders!" .

The service name (Meta:CPPA) identifies a kind of metadata service for the organization with the domain name “example.com,” and the URL provides a secured endpoint to contact.

If a registration service is needed to arrange for authorized access, an additional NAPTR record can be added such as:

IN NAPTR 100 10 "U" "Register:CPPA" "!^.\*$!https://example.com/register!" .

In essence, the above approach provides a simple and general approach to retrieving URLs for an organization’s metadata and registration services that is usable for both programmatic and human access.

Before providing detailed specifications for service identifiers and conventions for URL queries, a number of special requirements need to be described.

# Complications

Although the preceding would be sufficient to define, at a high level, a basic DDDS application for obtaining URLs that provide endpoint information for metadata services , other special cases will require additional conventions. In particular, enhancements to query strings may be needed for special purposes, and for some situations, conventions for converting other (non-DNS) identification formats into DNS query strings may be useful.

The special situations and purposes include the following:

* Service providers may have agreed upon “special” domains within which all metadata service endpoints will be located. In this case, information encoding the specific person or organization may need to be prefixed to the special domain names to form the DNS query string. The motivation for this is to allow multiple hosts for metadata or registration services, and to allow specific persons or organizations to announce their service hosts by NAPTR records within the “special” domains. The PEPPOL and GS1 networks use special domains, within which DNS resource records for service hosts can be published.
* Identity may be symbolically represented in any number of naming authority formats and values. The ISO registered naming authorities have been mapped into URNs in ebXML’s **OASIS ebCore Party Id Type Technical Specification Version 1.0**. There is, additionally, a defined BCP (Best Current Practice) RFC that specifies how URNs can be mapped to query strings. The resulting conventions can define one way to store NAPTR RRs for metadata service information.
* Identity may be associated with other identifying addresses, such as email addresses. Privacy of information concerns may require a specialized registration service for converting email addresses in the email domain to URLs for metadata services of the email identified domain.
* If privacy concerns allow use of DNS RRs, nevertheless, authorization for access to the metadata services may be requested. In that case, additional prerequisite registration services may be required so that the seeker of metadata information may be authorized through an authorization request to the “owner” of the metadata information provided by a service.

Each of these more complex use cases will receive its own dedicated discussion.

# Common Service Provider Domain

There are two main sub cases: the customer of the service provider has its own DNS domain or the customer lacks a domain name and associated nameserver service.

In the first case, the customer can add NAPTR-u records that provide the URL for the customer’s metadata service provider (and registration service, if needed). The customer with a DNS name can, of course, manage its own name servers, or can hire service providers to manage its DNS resource records and name servers.

Example TBD.

In the second case, the common service provider domain can create a specialized DNS sub-domain for the customer, using an encoding of a name and naming authority identifier, as a prefix for the DNS path. Then NAPTR-u records can be retrieved for that prefixed DNS query string to retrieve the URL for the metadata (or other) service.

Example from PEPPOL using hexadecimal hash of name value and naming authority type.

Other examples?

# URN Resolution

Ways to provide standardized URNs for various registered or unregistered naming authorities and person or organization name values are developed in:

<http://docs.oasis-open.org/ebcore/PartyIdType/v1.0/PartyIdType-1.0.html>

Using the IETF/IANA registered NID format “urn:oasis:names:tc:ebcore:partyid-type:” a variety of ways to specify an organizational name are outlined. For example, the DUNS naming authority type can appear as

urn:oasis:names:tc:ebcore:partyid-type:DataUniversalNumberingSystem:0060

urn:oasis:names:tc:ebcore:partyid-type:iso6523:0060

urn:oasis:names:tc:ebcore:partyid-type:iso9735:1

For each of these types, a DUNS value would appear as a suffix and identity an organization or business.

The IETF has approved a Best Current Practice RFC 3405 “Dynamic Delegation Discovery System (DDDS) Part Five: URI.ARPA Assignment Procedures.” Top level domains have been established (“URN.ARPA”) within whose authority any registered NID may place NAPTR records that can be retrieved by queries using DNS label paths. URNs are converted to DNS query paths by appending the top level domain “urn.arpa” to the registered NID (“oasis”). [See RFC 3121 for URN syntax and the concepts of NID (Namespace ID) and NSS (Namespace Specific String).]

Then the URN’s NSS is prepended to obtain the full DNS query string:

myOrgIDValue:0060:iso6523:partyid-type:ebcore:tc:names.oasis.urn.arpa.

The registered NAPTRs for this string then provide URLs for metadata services when the metadata services have protected access, such as that enabled by HTTP basic authentication.

# User@Domain

The organization or person identifier formats for Email, IM, and SIP VOIP all make use of a format that links registered DNS names with a user name part (User@Domain).

When there are no concerns about publishing metadata service DNS records (which are intrinsically open and not access control protected), the user name can be prefixed (as a label) to the domain name to form a DNS query string that may be used to retrieve NAPTRs for registration and metadata services. Some technical limitations on label length, and overall DNS query length exist. And in practice, some limitations in octets allowed in labels probably exist.

For new deployments, technical and practical implementations may be worked around by restricting the strings allowed for the new “User” part to be acceptable as DNS labels. For workarounds for existing non-conforming user names, conforming aliases may be created for the non-conforming names, and then used when metadata service RRs are created.

# Registration Services Details

TBD, use-case and scenario driven.

Should each registration service leverage an internet-checkable identity/credential/anchor? Anchors such as a phone number for a SMS text or an email address or an IM account etc. with a link back to confirm receipt?

# DDDS Service Values and Detailed Processing

Names for metadata services defined in this document.

Adding new metadata or registration service names.

Detailed processing illustration.