Metadata Service Location using DDDS facilities

# Terminology:

Person – not entirely automated system entity!

Organization – potentially automated system.

* Both persons or organizations can have an identity registered/issued by a naming authority.
* DNS identifiers provide one example of a naming authority, where naming is delegated to other domain authorities over branches of the overall namespace. A single dot “.” is the namespace root. TLDs are top level domains delegated by root. ICANN (Internet Corporation for Assigned Names and Numbers defines the policies for naming authorities, TLD or otherwise.)

RR -- DNS Resource Record, returned in response to a DNS query.

DNS query -- A DNS query made to a DNS nameserver for specific or any RRs indexed by a query string. A query string is a “domain name consisting of one or more parts, technically called *labels*, that are conventionally concatenated, and delimited by dots, such as example.com.” A hostname is a domain name that “has at least one IP address associated with it.” The names allowed are specified by RFCs 1035, 1123, 2181 and updated by ICANN Internationalizing Domain Names in Applications (IDNA) which uses the Punycode mapping of UNICODE. Technically domain name labels are limited to 63 octets, and a full name is restricted to 253 octets. Supposedly any binary octet string is allowed as a label (RFC 2181, section 11). But for TLDs, the working rule has been case-independent “letters/digits/hyphens” in labels. RFCs do specify DNS labels using octets other than letters/digits/hyphens.

DNSSEC – pertains to RRs that enable signing of RRs.

DDDS -- Dynamic Delegation Discovery Service, whose core parts are specified in five RFCs 3401 through 3405. Specific DDDS applications are found in VOIP, SIP and many other specifications.

DDDS application -- the sequence of processing steps involved when using several DNS queries to produce a desired discovery result.

# Use cases:

Person with browser, person with email, person with IM, person with SMS, person with android/ios/etc. Specializations: business person, IT person.

* Discovery by web search, direct delivery of email, IM or SMS, included within this usage area. If standardization is needed, the effort could be reduced to set of requirements for a service that is exposed by underlying metadata-service locator application or even the metadata retrieval applications.
* Relevant naming authorities are from the DNS system and from telecommunications providers from the technical side. Governments, churches, business registries also provide naming or identifying authorities. Association of values in one system with values in another system is a tangled mess currently.

Person/Organization with DDDS-enabled application as a component of a metadata retrieval service.

* Case may show that an API over the DDDS component would be useful to define.
* Such an API could be exposed by a web server to a browser submission form, e.g.

Person/Organization requiring trust in the service that provides a location (URL) for a metadata service.

* Implementation could leverage DNSSEC over DNS RR used within a DDDS defined application; this trust requirement is concerned with the trust in the DNS information itself.
* Note that an ability to check that a metadata service is from the intended metadata server is to be provided by using a HTTPS URL for the service, and then relying on available checks within the TLS/SSL host identity checking process. This is a related, but distinct trust issue.

Person/Organization requiring trust that the contacted metadata service is actually the one referenced by the location information.

1. TLS/SSL (or in a URL format, the HTTPS scheme) is the primary means to implement this security requirement.

Person/Organization possessing a DDDS query string that consists of a hostname.domain pattern.

* NAPTR records can return URLs to be used to contact the metadata service(s). A service field within the NAPTR can be specified to indicate a type of service. If the service needs information identifying the organization/person involved, that can be specified in the path retrieved from the NAPTR. The hostname label can encode the individual identity.
* This mechanism can work for defining a DDDS way to retrieve metadata about an entity identified by an email address. For these cases, the email username is used as the hostname label. So the email address “user@example.com” becomes the query string “user.example.com.” [This solution would requires cooperation from the organizational domain controlling the email servers.]
* Other naming systems (such as VOIP) that have the user-at-domain format could use a similar map provided that collisions are avoided (perhaps by adding a prefix “\_email.user.example.com”).

Person/Organization possessing a DDDS query string consisting of a domain/subdomain value.

* Large organizations may directly identify locations (URLs) of metadata services using U-Naptr RRs. These may be hosted by service providers or the organization itself.
* The service field of the U-Naptr RRs can be used to distinguish different kinds of metadata services, such as SMP or CPP or RegRep and so forth.
* Multiple U-Naptr for a given service can “load balance”. (Probably not normally needed.)
* The above deployment assumes that location information is made available as a URL. Customization of the retrieved URL (by adding URL query parameters, for example) would need specification going beyond the specification needed for the DDDS application definition.

Organization requiring specialized naming authority identifiers.

* The PEPPOL SML pattern is one such solution.
* SML can be assimilated to a U-NAPTR DDDS application by using the hash encoding of the intended receiver name, combined with a DNS domain, to retrieve a U-NAPTR that has the URL for the metadata service of the intended receiver.
* Note that the SML mapping resembles the “user@domain” mapping, but where the SML domain replaces the email domain, and where a different encoding of the “prefix” is adopted.

Organization wishing to outsource DNS services

* If an organization wishes to outsource its domain, then the organization can ask that provider to add the relevant NAPTR RR. This situation is no different from the organization supplying MX RR to the DNS service provider, for example.

Organization managing its own DNS services.

* Will need to set up DNS RR as needed. NAPTR can point to either internal or hosted metadata services.

Organization using DDDS query string composed from the ARPA TLD subdomains for URI/URN fields

* RFC 3405 presents the “best current practice” for the DDDS application defined in 3404, which specifies URI resolution using DDDS. It is possible that the ebXML PartyID URI encodings can make use of the DDDS procedures to connect names within various naming authority schemes with metadata services using NAPTR RRs. The best approach to this is being researched.
* URN format is “urn:” <NID> “:” <NSS>, and BCP says that if the NID is registered, then retrieval domain suffix is “nid.urn.arpa” For the OASIS NID, the suffix would be “oasis.urn.arpa.”
* What about the prefix? The prefix would need to identify the partyid (and type). Should the NSS value be the prefix? Should it be a compact form of the NSS? There are many details and small issues to resolve before proposing a pattern. It seems likely that every NID would want to examine how NAPTR details were dealt with.
* A general issue is just how many patterns should be specified. IMO it is ok if there are several patterns for U-NAPTR conventions. In any specific interaction network, it will probably be known which pattern has been adopted for DNS identification and composition of query string. In practice, there will be little incentive to place identifiers in multiple systems. Probably three types of system:
  + A system type where the DNS name of the organization is queried for NAPTRs to metadata service(s).
  + A system type where naming authorities deploy NAPTR information and use a prefix of named organizations/persons.
  + A system type where service providers organize the NAPTR information of their customers and clients.

Organization requiring authorized metadata service access (registration service).

* Authorization service can be in a URL within a NAPTR, but with a registration service value in the NATPR service field. Specification would need to find enumerated values to identity registration service type(s) needed.

Any security or naming specializations needed for subtypes of organizations: military, government, education, healthcare, energy, and so forth.

* To be discovered during TC operation if possible!