Metadata Query Protocol

The Metadata Query Protocol is a REST-like API for requesting and receiving arbitrary metadata. The specification is currently broken into two parts: a base specification (draft-young-md-query) that makes no assumption about metadata format and a SAML profile of the base specification (draft-young-md-query-saml) that focuses on SAML metadata. This document (the one you are reading right now) gives a brief overview of the two specifications taken together.

Historically, section 4 of the OASIS SAML2 Metadata specification outlines two methods of SAML metadata publication and resolution, both of which rely on the SAML `entityID`, a globally unique URI. The first method resolves a metadata resource by mapping the `entityID` directly to the resource (by value) whereas the second method maps the `entityID` indirectly (by reference) via DNS. Both methods have inherent limitations, and hence the Metadata Query Protocol was created. The latter still uses the `entityID` as input to the resolution process but now a Metadata Query Server is responsible for mapping the `entityID` to the desired metadata resource.

By definition, a *Metadata Query Server* implements the Metadata Query Protocol. A reference implementation for the latter is Ian Young's Metadata Query Server (mdq-server) based on the Shibboleth Metadata Aggregator software. The InCommon Federation's metadata service is a real-world deployment instance of mdq-server.

Protocol Overview

As defined in the base specification, a metadata query request URL is constructed by concatenating the following four components (two of which are variable):

1. The Metadata Query Server's base URL
2. A single "/" character, unless the base URL already ends in a "/"
3. The string "entities/"
4. A single URL-encoded `entityID`

For example, if the base URL is http://mdq.example.com/public and the `entityID` is https://sso.example.org/idp, the request URL is

```
http://mdq.example.com/public/entities/https%3A%2F%2Fsso.example.org%2Fidp
```

A bash function to construct a request URL per the Metadata Query Protocol specification, and a command-line tool (called md_query.sh) based on that function, are stored on GitHub.

A Command-Line Tool for Testing a Metadata Query Server

You can experiment with the Metadata Query Protocol by using a shell script (called md_query.sh) to fetch SAML metadata at the command line. The script automatically URL-encodes an arbitrary `entityID` and uses that to construct a request URL to an instance of a Metadata Query Server. The bash function above is included in the shell script.