

Pieces of some puzzle

REFEDS / I2MM

A twisting ma(c)e of passages...

- entity categories
- mdx
- LoA Registry
- DiscoJuice+accountchooser.com?
- attribute type registry?

entity categories

entity categories

<http://macedir.org/>

```
<md:Extensions>
  <mdattr:EntityAttributes>
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
      <Attribute xmlns="urn:oasis:names:tc:SAML:2.0:assertion"
        NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
        Name="http://macedir.org/entity-category">
        <AttributeValue>http://example.org/category/dog</AttributeValue>
        <AttributeValue>urn:oid:1.3.6.1.4.1.21829</AttributeValue>
      </Attribute>
    </mdattr:EntityAttributes>
  </md:Extensions>
```

mdx spec

MDX

- Attempt to finalize draft-lajoie-md-query
 - <https://github.com/lajoie/md-query>
- Issues
 - tagged-based queries
 - capability discovery
 - multiple entities
 - 400 vs 500 error code
- Discuss on mdx-list
 - mdx@lists.iay.org.uk

LoA Registry

LoA Registry: The problem...

Applications need a way to discover trust frameworks and their published LoA definitions.

and the obvious solution...

Do an IANA registry of course!

draft-johansson-loa-registry

- IANA registry for Level of Assurance Profiles
- Status
 - Tim Polk (NIST and 800-63 author) document shepherd
 - In final IESG review
 - -06 will be mostly minor nits from -05

Experiences from the IETF process...

- Individual submissions process pretty easy
- Sensible (if non-trivial) IPR
- Results in stable referenceable documents
- Rough outline...
 - publish I-D
 - socialize in your communities
 - revise I-D based on feedback
 - find a shepherd
 - do PROTO write-up and do an IETF Last Call
 - wiggle through the IESG
 - \$done

Attribute Registry

Yes its a little bit crazy...

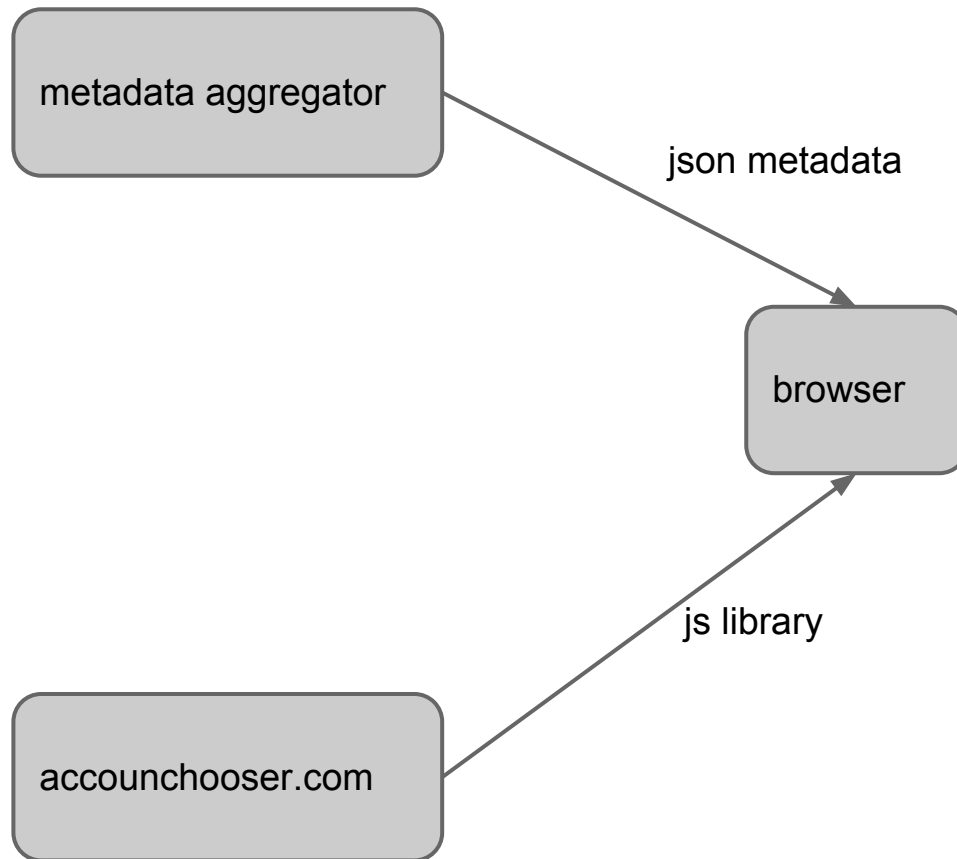
- IANA registry for attribute types?
- There is a requirements draft...
- Discussed at the ISOC identity ecosystem workshops
- Heather, Jamie and Leif are writing...

Discovery (again)

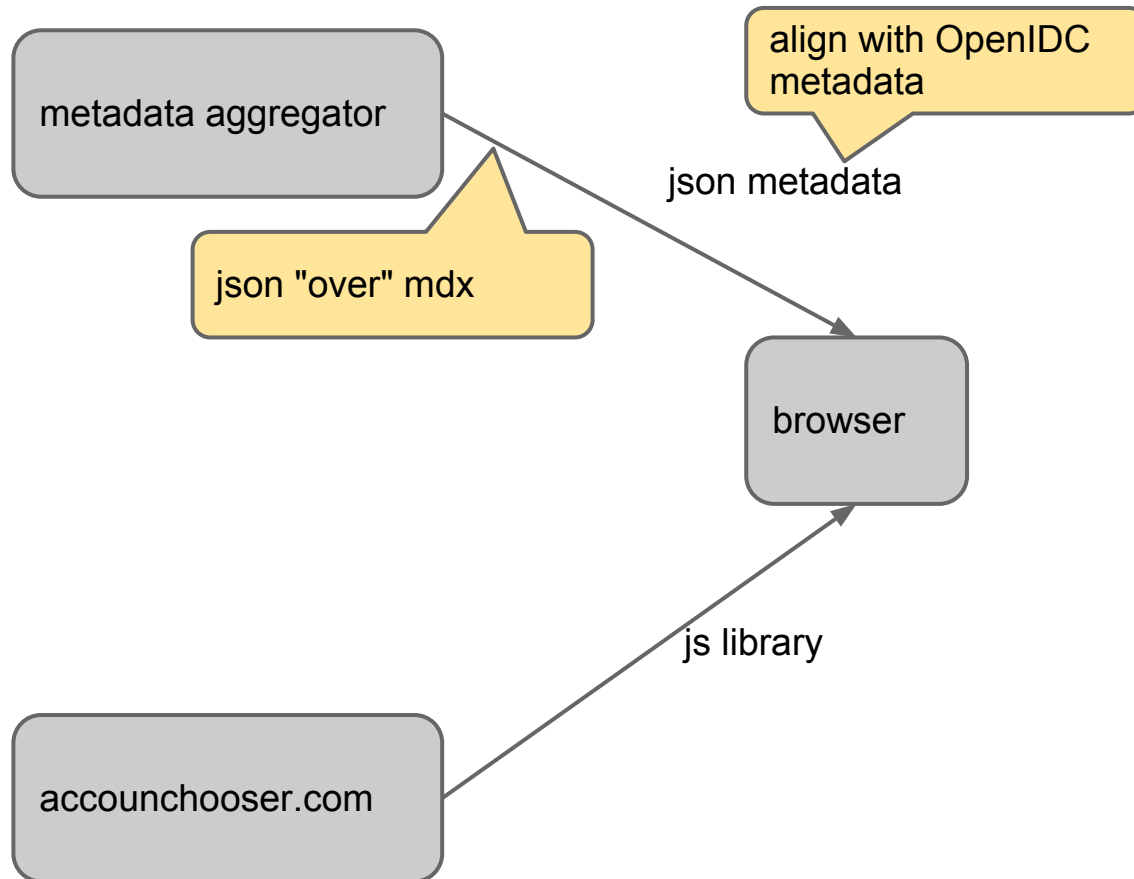
DiscoJuice+accountchooser = ?

- DiscoJuice
 - common domain + javascript + cookie
- accountchooser.com
 - common domain + javascript + html5 local store

conceptually...



conceptually...



issues for accountchooser@OIDF...

- relax ties to email address
metadata format for discovery
- discovery hints from SP
 - eg "must be LoA3 and in edugain"
- must be possible to run on own domain

Proposal

The R&E community should engage with the accountchooser WG @ OIF to make accountchooser + an optional DJ backend a viable option for (interfederation) discovery.

LEGO update

The fun-with-branding activity...

- A couple of mappings to OIX FICAM LoA1 have been published
- SWAMID is working on Kantara mapping

Preliminary conclusions...

Few gotchas

- Insurance requirements
- Specific jurisdictional requirements

Nothing really bad...

Q&A