Enriching Metadata

Improved Retrieval

- ETag & Last-Modified based conditional GETs
  - already supported by UK metadata servers
- Support for gzip compression
  - not yet supported by UK metadata servers
- Reloading of metadata in background thread
- All added in IdP 2.2 and SP 2.4

Improved Retrieval

- Dynamic Metadata Retrieval
  - just-in-time fetching of metadata by entity ID
    - less bandwidth and memory required by end entities
  - uses metadata query protocol
  - trust established via signature the same as today:
    - entity gets their metadata signed by trusted 3rd party and then serves it up
    - or, relying party must configure entity's certificate as trust anchor and vet the entity's processes themselves
  - in SP 2.1, to be added in IdP 2.3

Crypto Algorithm Selection

- Difficult to roll out new cryptographic algorithms
  - no idea what the relying party supports
  - no way to choose the strongest/best
  - leads to a least common denominator scenario
- Add algorithm information in to entity's metadata

```
<Extensions>
   <alg:DigestMethod
        Algorithm="http://www.w3.org/2001/04/xmldsig-more#sha384"/>
   <alg:DigestMethod
        Algorithm="http://www.w3.org/2001/04/xmlenc#sha256"/>

   <alg:SigningMethod MinKeySize="256" MaxKeySize="511"
     Algorithm="http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256"/>
   <alg:SigningMethod MinKeySize="2048" MaxKeySize="4096"
     Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256"/>
</Extensions>
```

Entity Attributes & Attribute Filters

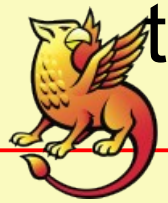
- Current mechanisms for attribute filtering rely either on user attributes, requester's entity ID or EntitiesDescriptor
- Use of EntitiesDescriptor to group entities with similar properties scales poorly
  - requires one group per permutation of grouping facets being tracked (n^2 problem)
  - based on misconception that EntitiesDescriptor groups are fixed and entities only appear in one group in one file
- Lacks mechanism to perform out of band checks and automatically using results during attribute filtering:
  - identify “safe” SPs to which PII can be sent

Entity Attributes & Attribute Filters

- Proposed solution:
  - annotate entities with entity attributes
    - e.g., UK section 6 compliance, located in EU
  - allow filtering based on entity attributes
- Support:
  - IdP 2.3 and SP 2.5 support simple string attributes
  - IdP 3.0 may support attributes w/ complex data
- Common attributes and values should be hashed out on REFEDs

Attribute Requirements

- Carry SP's attribute requirements in metadata
- Allows IdP operators to know what to release
- Can drive attribute consent mechanism
  - puts users in control of whether they release data
  - lowers overhead of working with new SPs
- Does not support boolean ORs
  - e.g., ePPN or ePTID is required
- Today, uApprove comes with IdP attribute filter that can release required or optional attribute



UI Customization

- Usability shows that current SSO flow lacks a coherent “story”
  - IdP “brand” doesn't show up in discovery service
  - SP “brand” doesn't show up on login pages
- Metadata has some fields that sorta seem right:
  - organization (IdP & SP) and service name/desc. (SP)
  - but different federations use wildly different info or don't populate them all
  - service name/description must also contain attribute requirements, what if you don't want to show them?

UI Customization

- Proposed solution: two metadata extensions
- UIInfo
  - display name, description, logo, keywords
  - information and privacy URLs
- DiscoHints
  - IP address ranges, domain names, geolocation
- UK currently collecting data for test
  - contact Rod or Nicole to participate

Interfederation

- Main Goal: ability to get metadata for entities, in multiple federations, to consumers
  - corollary: entities don't have to register with every federation in order to work with them
- eduGain is an attempt at such a system
  - still immature and buggy
  - questionable policies and after-project lifetime
- Using DNS as an analogy in this area is very useful
  - have /etc/hosts now; want an oracle instead

Interfederation

- Minimal technical approach:
  - concatenate metadata files and publish
  - not very efficient
- System probably needs more smarts
  - lots of data munging potential
  - single publishing endpoint that can hide ways in which data is found; think DNS stubs
- Also metadata extensions to carry information about registration and publication of data

Interfederation Issues

- Lots of self-imposed political issues
  - some want a playground where no kid can be bad
- Misconception: I can trust an entity because it's in a particular file
  - do you trust all servers in given a DNS domain?
- Misconception: I can release PII to an entity because it's in a file from my federation
  - do you give PII to any server in a given DNS domain?

Interfederation Preparation

- Deploy the embedded DS
- Keep IdP and SP up to date
- Don't release attributes to everyone
  - transient and ePTID are probably safe
- Don't release attributes to EntitiesDescriptors