Trust & Identity Incubator - Pixie Dusting

REFEDS @TechEx2019
New Orleans, Dec 9 2019

Niels van Dijk
Trust & Identity Incubator lead
niels.vandijk@surfnet.nl
<table>
<thead>
<tr>
<th>Step</th>
<th>Team/Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collect proposals for incubator topics</td>
<td>Service Owners GEANT project T&amp;I community member</td>
</tr>
<tr>
<td>Review and prioritise the proposals</td>
<td>Main Incubator Board</td>
</tr>
<tr>
<td>Choose topics for the next cycle</td>
<td>Incubator Lead Team</td>
</tr>
<tr>
<td>Define goal, stakeholders, results</td>
<td>Incubator Topic Main Investigator</td>
</tr>
<tr>
<td>Work on topic, 6 sprints with demos</td>
<td>Incubator Topic Team</td>
</tr>
<tr>
<td>Finalize topic, handover the results</td>
<td>Incubator Topic Team</td>
</tr>
</tbody>
</table>
Community Trustmarks

How can research communities make statements on federation entities?
- For example sirtifi+
- Community trustmarks on top of RAF
- Leverage or share existing statements
- Protocol agnostic

Add to eduGAIN? Mmm, that’s really tricky because of the trusmodel

Local Trustmarks may be the answer
Local trustmarks

Makes statements in the context of a ‘local’ community
  • Nothing new: National federations have been doing this for ages

Take data from existing trust anchor and add on top of that
  • Similar to a VO adds VO attributes on top of IdP statement

Needed:
  • A CO trust anchor
  • Pixie dust
The plan: Pixie Dust

A place to consume existing trust
  • eduGAIN metadata

A place to add tags to these entities
  • A registry (Jagger, Janus, etc)

A place to publish enhanced metadata
  • Metadata signing by community

Community services (or a AARC BPA proxy) consume community signed metadata
A demonstrator

The Pixie-Dust collaboration wants to allow entities to assert SIRTFI+

1. Create metadata feed for the Pixie-Dust VO
   • Based on existing federation metadata

2. Allow Service controlled access to registry to tag it’s own entity

3. VO admin confirms tag validity for entity

4. Metadata with tag made available
A demonstrator

The Pixie-Dust collaboration wants to allow entities to assert SIRTFI+

1. Create metadata feed for the Pixie-Dust VO
   • Based on existing federation metadata

2. Allow Service controlled entry to registry it to tag it’s own entity

3. VO admin confirms tag validity for entity

4. Metadata with tag made available (part of movie #3)
Final thoughts

Pixie dusting technically works
  • may be based on existing tools
  • and a bit of glue

https://wiki.geant.org/pages/viewpage.action?pageId=120500327

Trusted place is still needed to hold the signed metadata
  • Perhaps a community AAI?
  • Holding multiple signing keys may become an issue
Questions