



Authentication and Authorisation for Research and Collaboration

Sirtfi Update

Authentication and Authorisation for Research and Collaboration

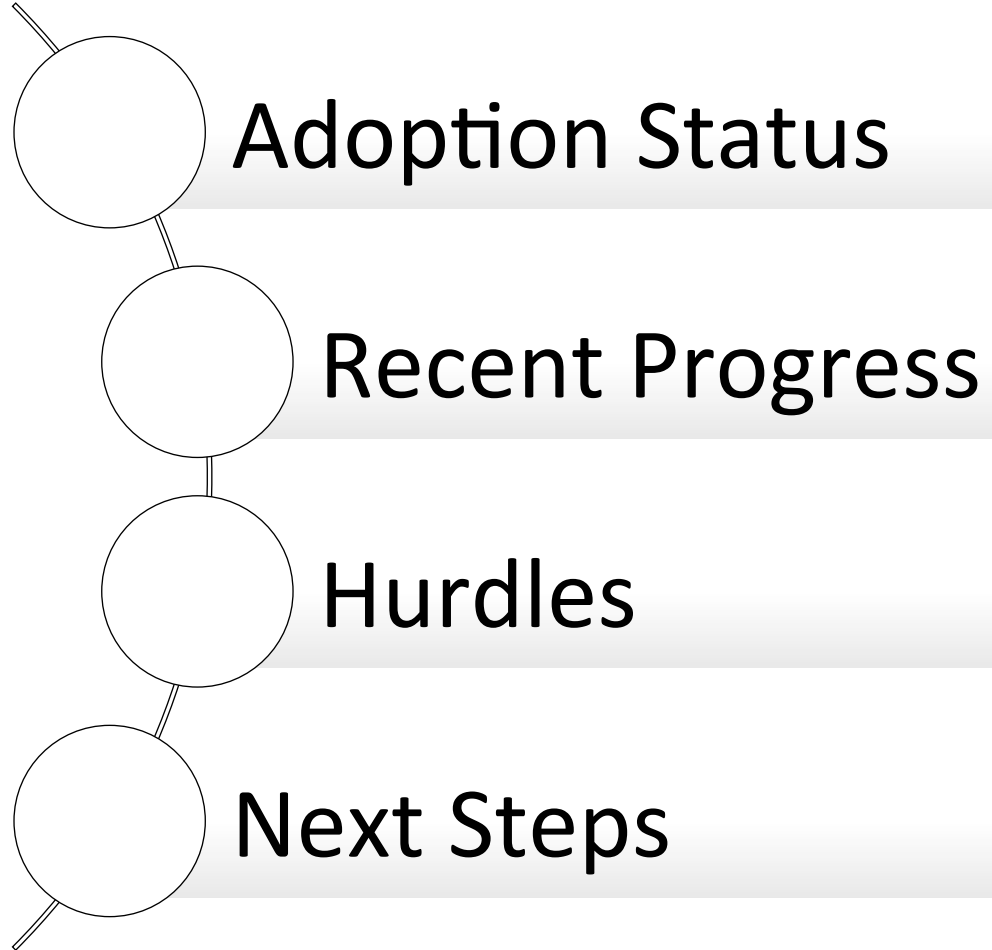
Hannah Short, CERN

AARC NA3

CERN, Computer Security

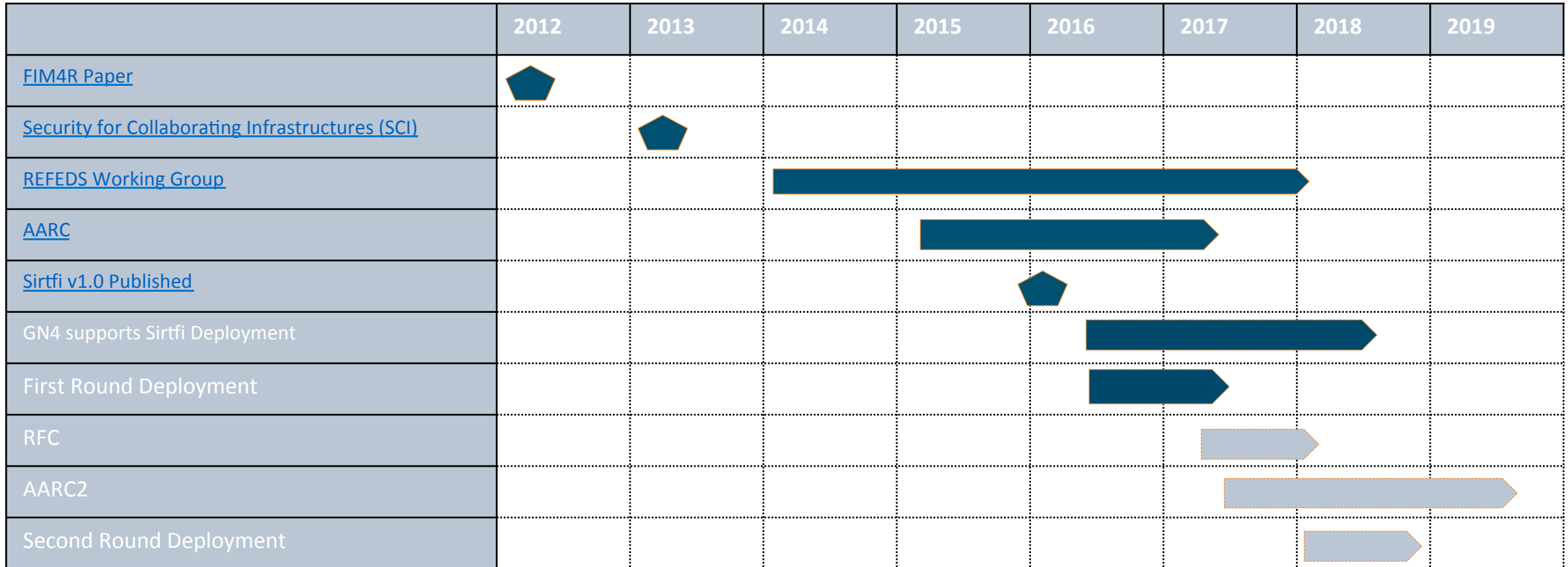
REFEDS, Miami

25 September 2016

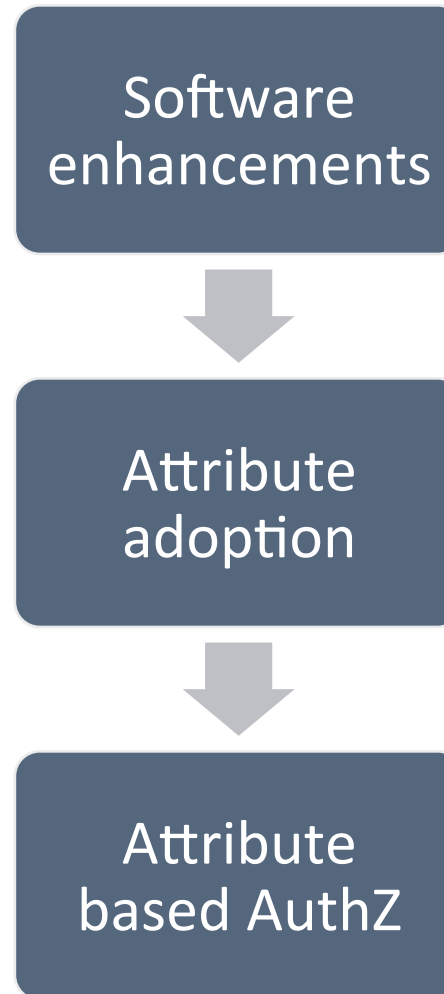


Sirtfi

A timeline



What is Sirtfi Deployment?



Software enhancements

- Jagger

- Janusz made necessary changes (super quickly!)
- Impacts GARR, HEAnet, GN4's Federation as a Service...
- Once enabled for a deployment, entity owners need to apply for Sirtfi via entityedit and add their security contact

- DFN

- Wolfgang is pushing update for Sirtfi changes
- Entity owners will be able to apply for Sirtfi via a checkbox



hannahshort commented 27 days ago

As discussed with Janusz, the Sirtfi REFEDS Working Group has recently defined 2 metadata additions to show adoption of Sirtfi (the Security Incident Response Trust Framework for Federated Identity). Please could you add support to Jagger for handling these two metadata additions (1 attribute profile extension and one custom contactPerson)? Info on the wiki: <https://wiki.refeds.org/display/SIRTFI/Guide+for+Federation+Participants>



janul added the **feature request** label 27 days ago



janul added a commit that closed this issue 17 days ago



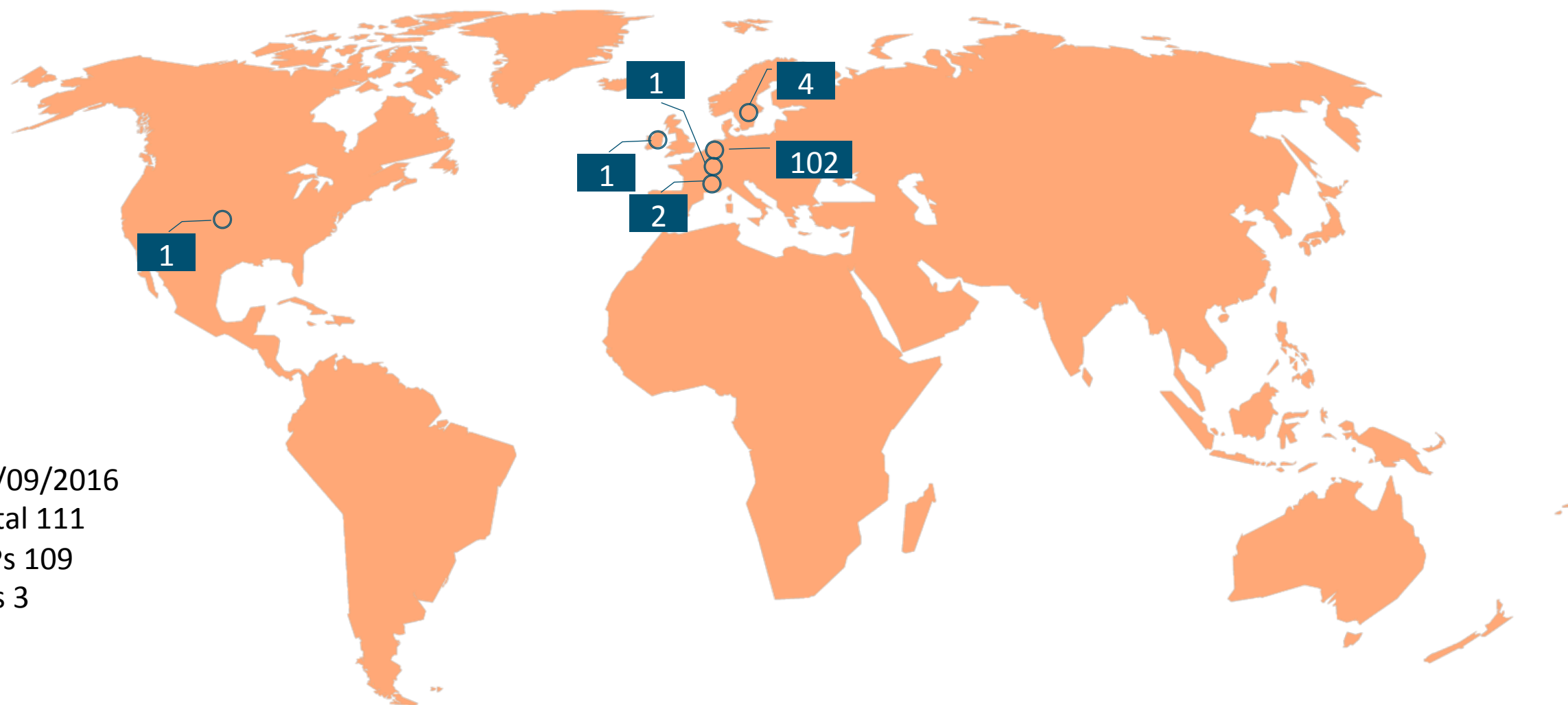
closes #269

06c0cd8



janul closed this in 06c0cd8 17 days ago

Current adoption



22/09/2016

Total 111

IdPs 109

SPs 3

RCauth.eu

- May 2016
- Accredited by IGTF with Sirtfi dependent policy

CiLogon Basic

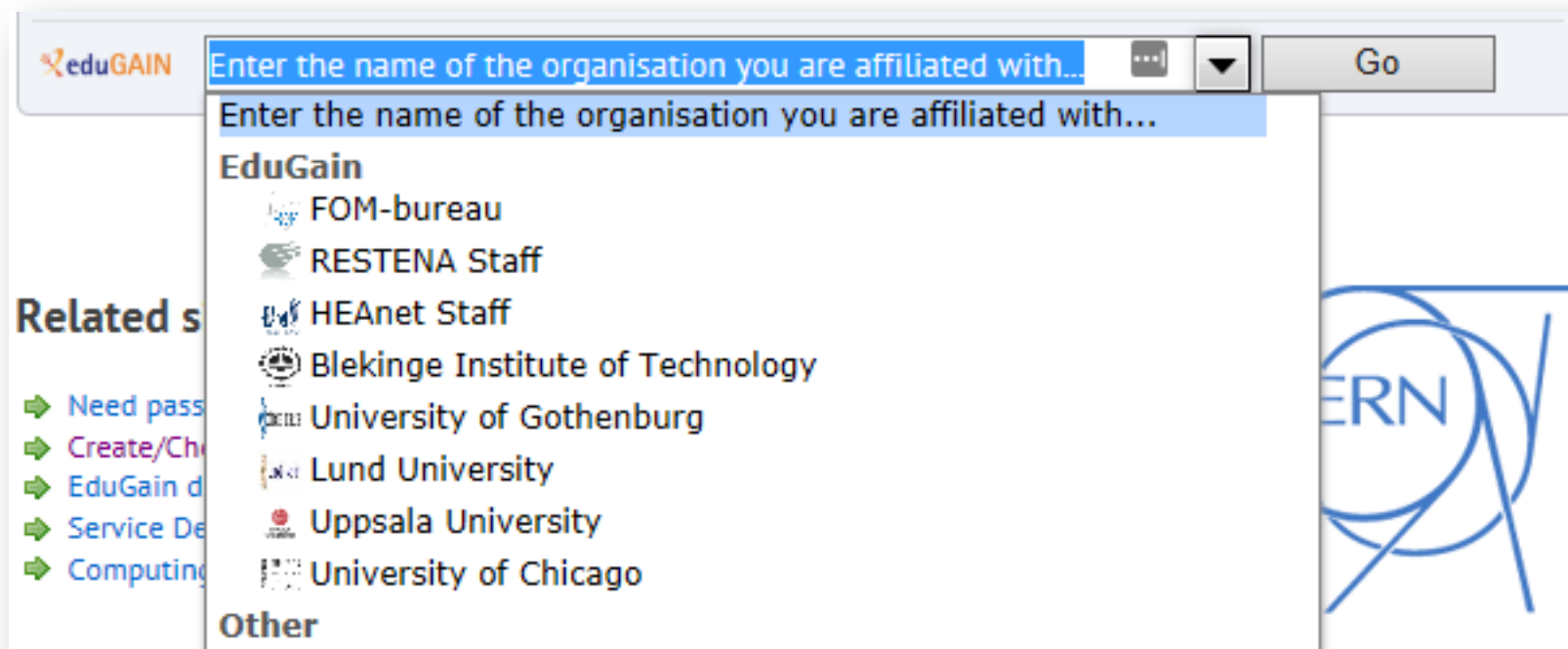
- July 2016
- Sirtfi compliance is sufficient to have access

CERN

- In Progress
- Restrict access based on Sirtfi
- MISP

Certificate uniqueness

- CERN's Sirtfi discovery service looks a little empty
- 102 of the 111 Sirtfi participants are using the same signing certificate...



The screenshot shows the eduGAIN search interface. At the top, there is a search bar with the text "Enter the name of the organisation you are affiliated with..." and a "Go" button. Below the search bar, a dropdown menu is open, displaying a list of affiliations. The list is divided into two sections: "EduGain" and "Other". The "EduGain" section includes the following affiliations: FOM-bureau, RESTENA Staff, HEAnet Staff, Blekinge Institute of Technology, University of Gothenburg, Lund University, Uppsala University, and University of Chicago. The "Other" section is currently empty. On the left side of the interface, there is a "Related s" section with links to "Need pass", "Create/Ch", "EduGain d", "Service De", and "Computing". On the right side, there is a large blue logo that partially shows the word "ERN".

Normative Document

- Syntax, semantics & responsibilities
- First version out for consultation

Logo

- Thanks for voting!
- AARC has some budget to get this registered as a trademark – in progress





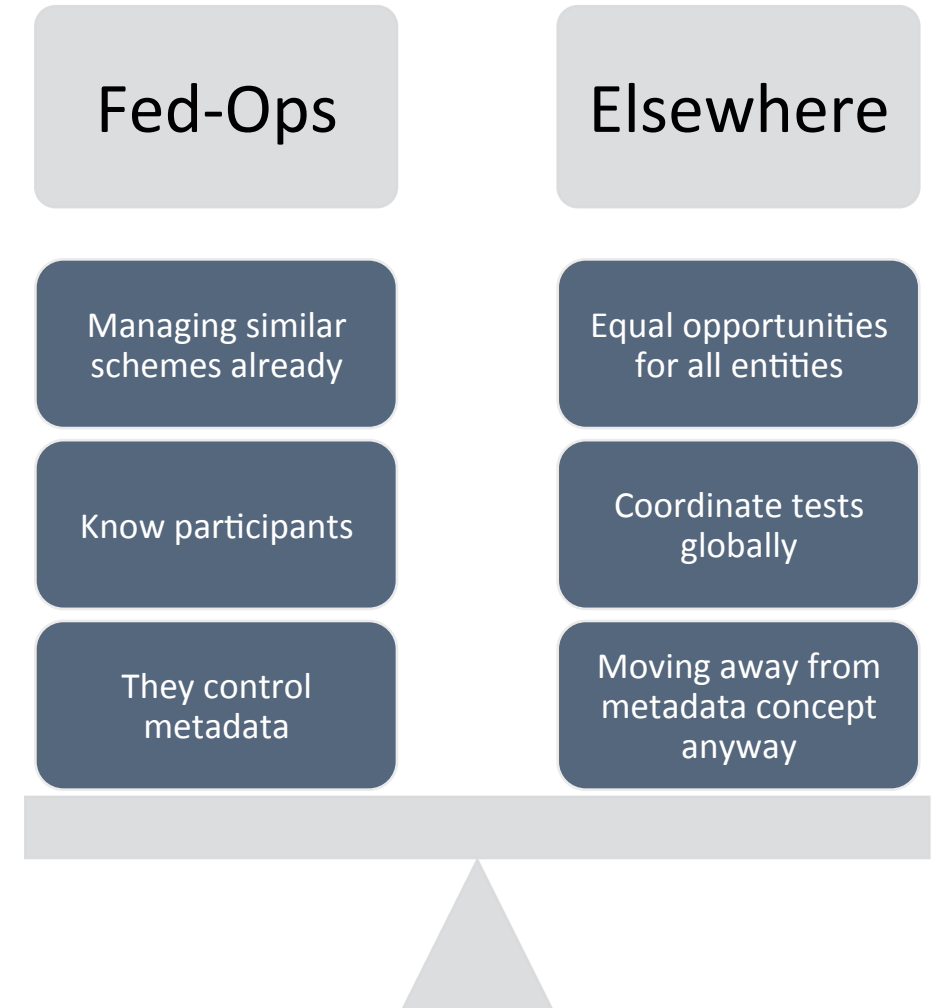
Hurdles? What hurdles?

Operational Support

Problem: Self Assertion is much easier than Self Discipline... what happens when someone breaks the trust?

We need some operational support

- Respond to complaints, remove attributes & block re-assertion
- Test contact responsiveness
- Make decisions, e.g. Use of obsolete software (**cough** Shibboleth IdP v2), does that count as Sirtfi violation?



How will it work in practice?

1. Something goes wrong
2. Panic, panic. Need to contact 200 SPs!
3. Look up entity #1 on <https://technical.edugain.org/entities> and find contact details
4. Repeat for 10 entities
5. Decide this is silly
6. Write a script
7. Debug script
8. ...

Wouldn't it be better if we could simplify this? Perhaps upload comma separated list of entity IDs and retrieve comma separated list of security contacts?

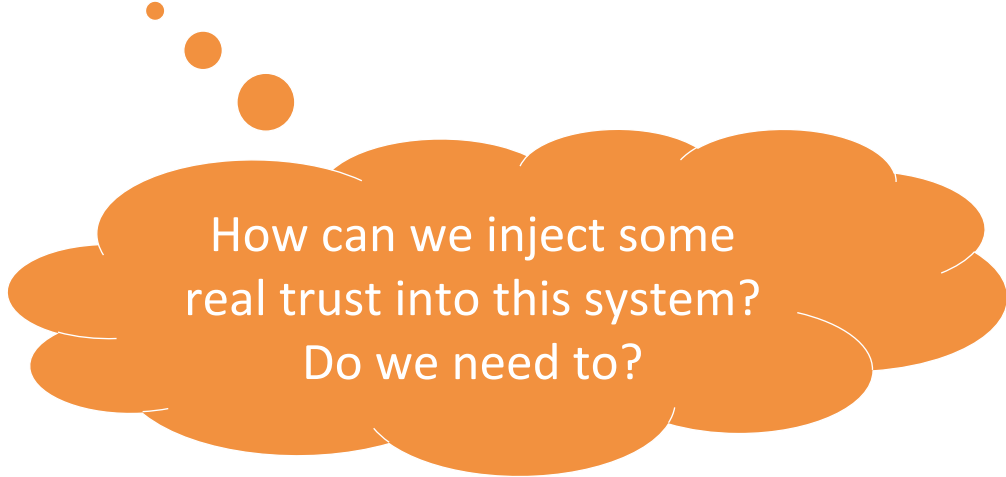
Is this real trust?

What Sirtfi does

- Provide contact details
- Guarantee that entities fulfill baseline operational security requirements
- Guarantee a response during incident response

What Sirtfi doesn't do

- Allow people to meet
- Convey operational security skill of contacts



How can we inject some
real trust into this system?
Do we need to?

Next Steps

- Normative Document – Feedback Please!!
 - <https://wiki.refeds.org/display/CON/Sirtfi+Consultation%3A+Sirtfi+Identity+Assurance+Certification+Description>
- AARC Deliverable – Generic Incident Response Procedure
 - Due December 2016
 - Comments welcome on the draft
 - <https://docs.google.com/document/d/1l3lhatjdP5sa6Sfji8SIT6yXo4CI1tf2kNOaccD9QCU/edit?usp=sharing>
- IGTF FIM Working Group
 - Specific requirement to raise security to same level as current grid infrastructures
 - Many willing volunteers!

Sirtfi Normative Description Consultation Closes October 28th!



REFEDS Spaces ▾

? ▾ Log in

Consultations

Pages

Blog

CHILD PAGES

Consultations Home

└ Sirtfi Consultation: Sirtfi Identity A...

Pages / Consultations Home

Tools ▾

Sirtfi Consultation: Sirtfi Identity Assurance Certification Description

Created by Nicole Harris, last modified by Hannah Short on Sep 16, 2016

Background

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) aims to enable the coordination of incident response across federated organisations. This assurance framework comprises a list of assertions which an organisation can attest in order to be declared Sirtfi compliant. Sirtfi has been developed by a [REFEDS Working Group](#), supported by AARC.

This consultation asks for comments and change proposals to the Sirtfi Identity Assurance Certification Description. This document defines the ways in which Federation Operators and Participants (such as Service Providers and Identity Providers) should implement Sirtfi as an entity attribute and the requirements placed on participants to support Sirtfi.

Overview

The consultation opens on Friday 16th September 2016 and closes on Friday 28th October 2016 at 5pm CEST.

Participants are invited to:

- Review and comment on the [Sirtfi Identity Assurance Certification Description](#) with the intention of approving the document as a normative REFEDS specification.

<https://wiki.refeds.org/display/CON/Sirtfi+Consultation%3A+Sirtfi+Identity+Assurance+Certification+Description>

Thank you

Any Questions?

hannah.short@cern.ch



<https://aarc-project.eu>



© GÉANT on behalf of the AARC project.
The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 653965 (AARC).