Sirtfi Update

Authentication and Authorisation for Research and Collaboration

Hannah Short, CERN
AARC NA3
CERN, Computer Security

REFEDS, Miami
25 September 2016
Overview

Adoption Status

Recent Progress

Hurdles

Next Steps
## A timeline

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>FiM4R Paper</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security for Collaborating Infrastructures (SCI)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>REFEDS Working Group</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AARC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sirtfi v1.0 Published</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GN4 supports Sirtfi Deployment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>First Round Deployment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>RFC</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AARC2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Second Round Deployment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What is Sirtfi Deployment?

- Software enhancements
- Attribute adoption
- Attribute based AuthZ
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

---

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](https://wiki.refeds.org/display/SIRTFI/Guide+for+Federation+Participants)
Current adoption

22/09/2016
Total 111
IdPs 109
SPs 3
### Attribute based AuthZ

<table>
<thead>
<tr>
<th>RCauth.eu</th>
<th>CiLogon Basic</th>
<th>CERN</th>
</tr>
</thead>
<tbody>
<tr>
<td>• May 2016</td>
<td>• July 2016</td>
<td>• In Progress</td>
</tr>
<tr>
<td>• Accredited by IGTF with Sirtfi dependent policy</td>
<td>• Sirtfi compliance is sufficient to have access</td>
<td>• Restrict access based on Sirtfi</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• MISP</td>
</tr>
</tbody>
</table>
Certificate uniqueness

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

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?

Source: 2015. REUTERS/Damir Sagolj
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?

(See Nick R’s thread to the REFEDS list, “[refeds] Whither Entity Attributes?”, for InCommon’s perspective)
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](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/1I3IhatjdP5sa6Sfji8SIT6yXo4Cl1tf2kNOaccD9QCU/edit?usp=sharing](https://docs.google.com/document/d/1I3IhatjdP5sa6Sfji8SIT6yXo4Cl1tf2kNOaccD9QCU/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!

https://wiki.refeds.org/display/CON/Sirtfi+Consultation%A+Sirtfi+Identity+Assurance+Certification+Description
Thank you

Any Questions?

hannah.short@cern.ch