AARC Authentication and Authorisation for Research and Collaboration

Sirtfi Update

Hannah Short
AARC
CERN-IT

REFEDS Meeting
12th June 2016

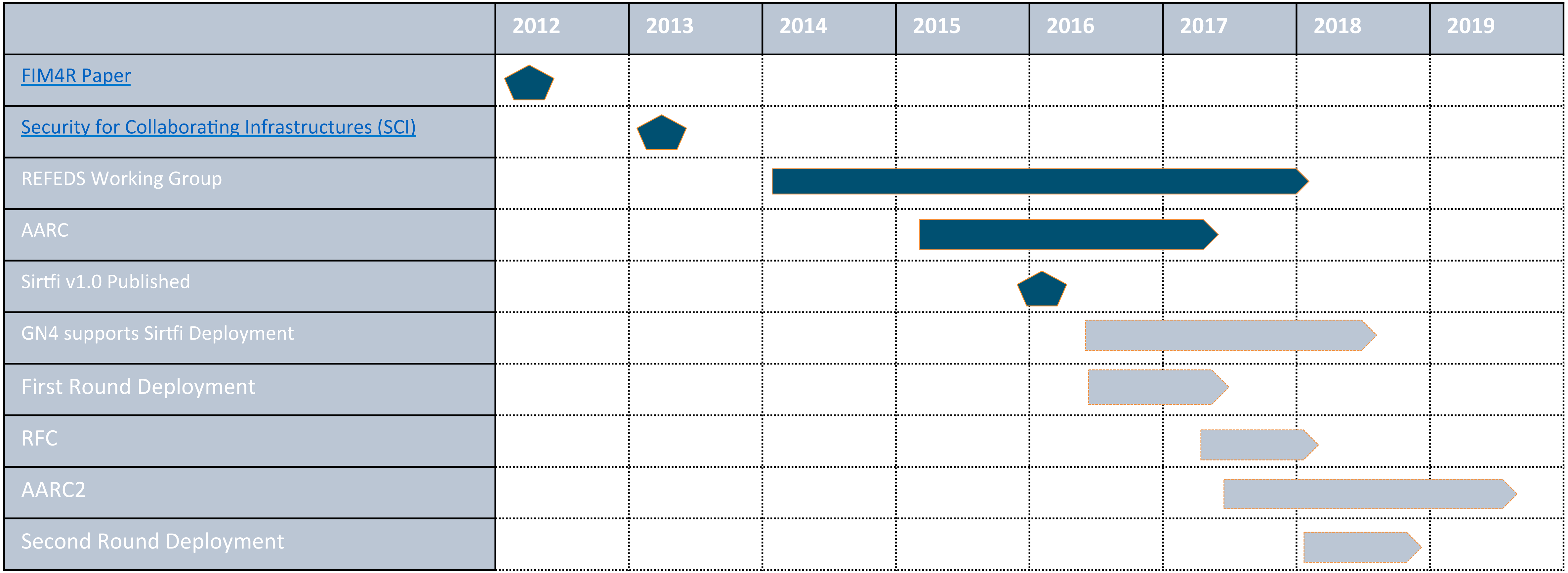
Agenda

What have we done since the last meeting?

Future plans

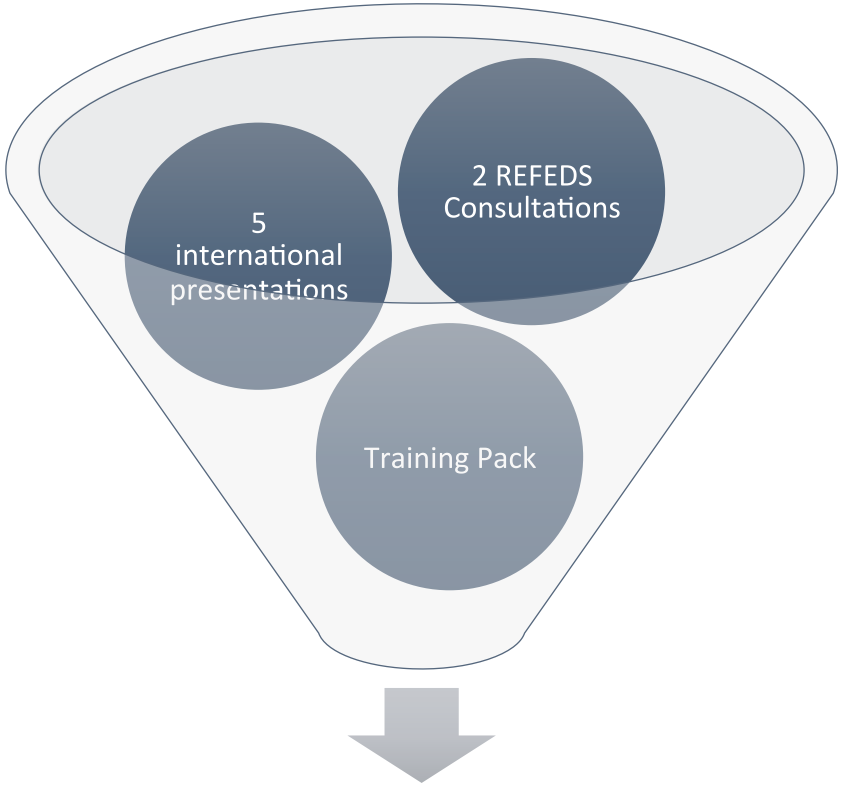
What do you want to do?

Sirtfi
A timeline



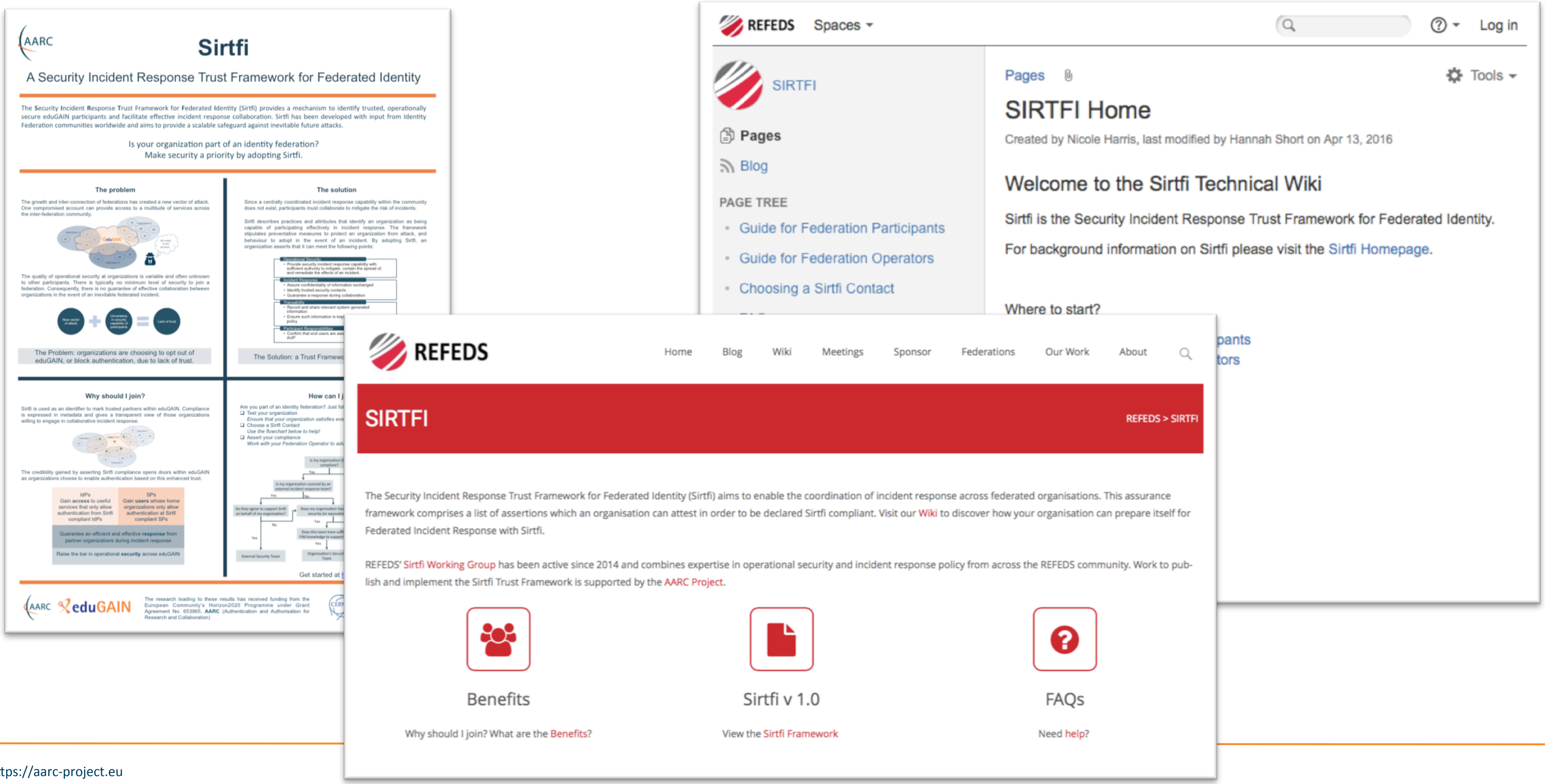
What have we done since the last meeting?

- Big milestone was Sirtfi v1.0, which was published early 2016
- We have been presenting the framework
- We have created training material
- Now federations are interested in actually adopting Sirtfi!



Sirtfi is ready to go!

What have we done since the last meeting?
Training Material



Sirtfi

A Security Incident Response Trust Framework for Federated Identity

The Security Incident Response Trust Framework for Federated Identity (Sirtfi) provides a mechanism to identify trusted, operationally secure eduGAIN participants and facilitate effective incident response collaboration. Sirtfi has been developed with input from Identity Federation communities worldwide and aims to provide a scalable safeguard against inevitable future attacks.

Is your organization part of an identity federation?
Make security a priority by adopting Sirtfi.

The problem

The growth and inter-connection of federations has created a new vector of attack. One compromised account can provide access to a multitude of services across the inter-federation community.

The quality of operational security at organizations is variable and often unknown to other participants. There is typically no minimum level of security to join a federation. Consequently, there is no guarantee of effective collaboration between organizations in the event of an inevitable federated incident.

The Problem: organizations are choosing to opt out of eduGAIN, or block authentication, due to lack of trust.

The solution

Since a centrally coordinated incident response capability within the community does not exist, participants must collaborate to mitigate the risk of incidents.

Sirtfi describes practices and attributes that identify an organization as being capable of participating effectively in incident response. The framework stipulates preventative measures to protect an organization from attack, and behaviour to adopt in the event of an incident. By adopting Sirtfi, an organization asserts that it can meet the following points:

Operational Security
- Provide security incident response capability with sufficient authority to mitigate, contain the spread of, and remediate the effects of an incident.

Incident Response
- Assure confidentiality of information exchanged
- Identify trusted security contacts
- Guarantee a response during collaboration

Traceability
- Record and share relevant system generated information
- Ensure such information is kep
policy

Participant Responsibilities
- Confirm that end users are awa
AUP

The Solution: a Trust Framewo

Why should I join?

Sirtfi is used as an identifier to mark trusted partners within eduGAIN. Compliance is expressed in metadata and gives a transparent view of those organizations willing to engage in collaborative incident response.

The credibility gained by asserting Sirtfi compliance opens doors within eduGAIN as organizations choose to enable authentication based on this enhanced trust.

IdPs Gain **access** to useful services that only allow authentication from Sirtfi compliant IdPs	SPs Gain **users** whose home organizations only allow authentication at Sirtfi compliant SPs
Guarantee an efficient and effective **response** from partner organizations during incident response	
Raise the bar in operational **security** across eduGAIN	

How can I j

Are you part of an identity federation? Just fol
❑ Test your organization
Ensure that your organization satisfies eve
❑ Choose a Sirtfi Contact
Use the flowchart below to help!
❑ Assert your compliance
Work with your Federation Operator to add

Is my organisation S compliant?
Yes
Is my organisation covered by an external incident response team?
Yes
No
Do they agree to support Sirtfi on behalf of my organisation?
Does my organisation hav security (or equivalen
No
Yes
Yes
Does this team have suff FIM knowledge to support
Yes
External Security Team
Organisation's Securit Team

Get started at

The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 653965, **AARC** (Authentication and Authorisation for Research and Collaboration)

- Guide for Federation Participants
- Guide for Federation Operators
- Choosing a Sirtfi Contact

Pages

SIRTFI Home

Created by Nicole Harris, last modified by Hannah Short on Apr 13, 2016

Welcome to the Sirtfi Technical Wiki

Sirtfi is the Security Incident Response Trust Framework for Federated Identity.

For background information on Sirtfi please visit the Sirtfi Homepage.

Where to start?

pants
tors

SIRTFI

REFEDS > SIRTFI

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. Visit our Wiki to discover how your organisation can prepare itself for Federated Incident Response with Sirtfi.

REFEDS' Sirtfi Working Group has been active since 2014 and combines expertise in operational security and incident response policy from across the REFEDS community. Work to publish and implement the Sirtfi Trust Framework is supported by the AARC Project.

Benefits
Why should I join? What are the Benefits?

Sirtfi v 1.0
View the Sirtfi Framework

FAQs
Need help?

What have we done since the last meeting?

Events

- Webinars and in person presentations
- Security response workshop held at ISGC
- Discussions moving beyond FIM world, talking with SWITCH Security and TF-CSIRT

Event	Location	Date
EWTI (European Workshop on Trust and Identity	Vienna	01 Dec 2015
ISGC (International Symposium on Grids and Clouds)	Taiwan	15 Mar 2016
Kantara IAWG, Videoconference	US	07 Apr 2016
Internet2 Webinar	US	May 2016
Internet2 Global Summit	US	May 2016
TF-CSIRT	Riga	12 May 2016

What have we done since the last meeting?
Technical Specification

- REFEDS Consultation on managing metadata extensions completed in April
  https://wiki.refeds.org/display/CON/Consultation%3A+Managing+Metadata+Extensions
- Sirtfi is now on the official list of IANA Assurance Profiles
  https://www.iana.org/assignments/loa-profiles/loa-profiles.xhtml

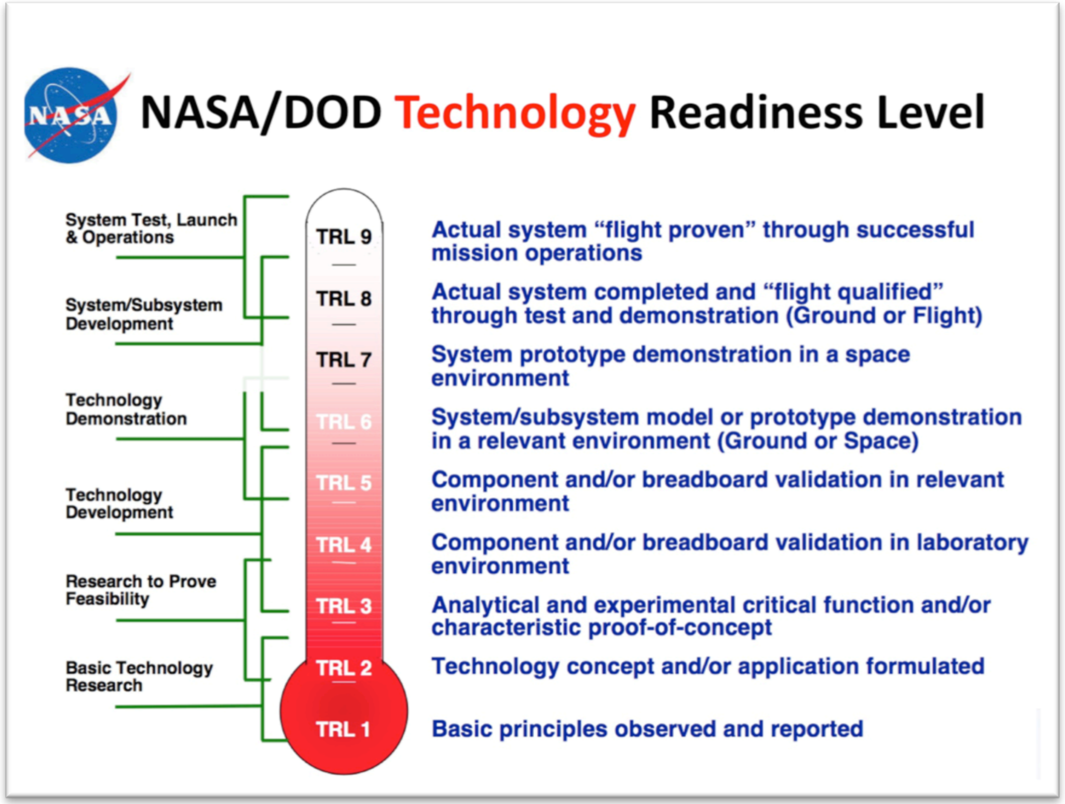
```
<EntityDescriptor ...>
  <Extensions>
     <attr:EntityAttributes>
          ...
          <saml:Attribute NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
                     Name="urn:oasis:names:tc:SAML:attribute:assurance-certification">
            <saml:AttributeValue>https://refeds.org/sirtfi
            </saml:AttributeValue>
          </saml:Attribute>
          ...
     </attr:EntityAttributes>
   </Extensions>
...
</EntityDescriptor>
```

```
<ContactPerson xmlns:remd="http://refeds.org/metadata"
           contactType="other"
           remd:contactType="http://refeds.org/metadata/contactType/security">
  <GivenName>Security Response Team</GivenName>
  <EmailAddress>security@xxxxxxxxxxxxxx</EmailAddress>
</ContactPerson>
```

Future plans

Deployment – Support from GN4

- GN4 has recognised the value of Sirtfi and will be providing support to move Sirtfi to TRL "Late-stage-pilot", level 7
- Concrete aims
  1. Push for wide-scale adoption at both hub-and-spoke and full-mesh federations
  2. Push for adoption at key e/r-infrastructures
  3. Troubleshoot propagation problems (i.e. metadata filtering)
  4. Define and test KPIs
  5. Add Sirtfi to Highly Recommended eduGAIN practices

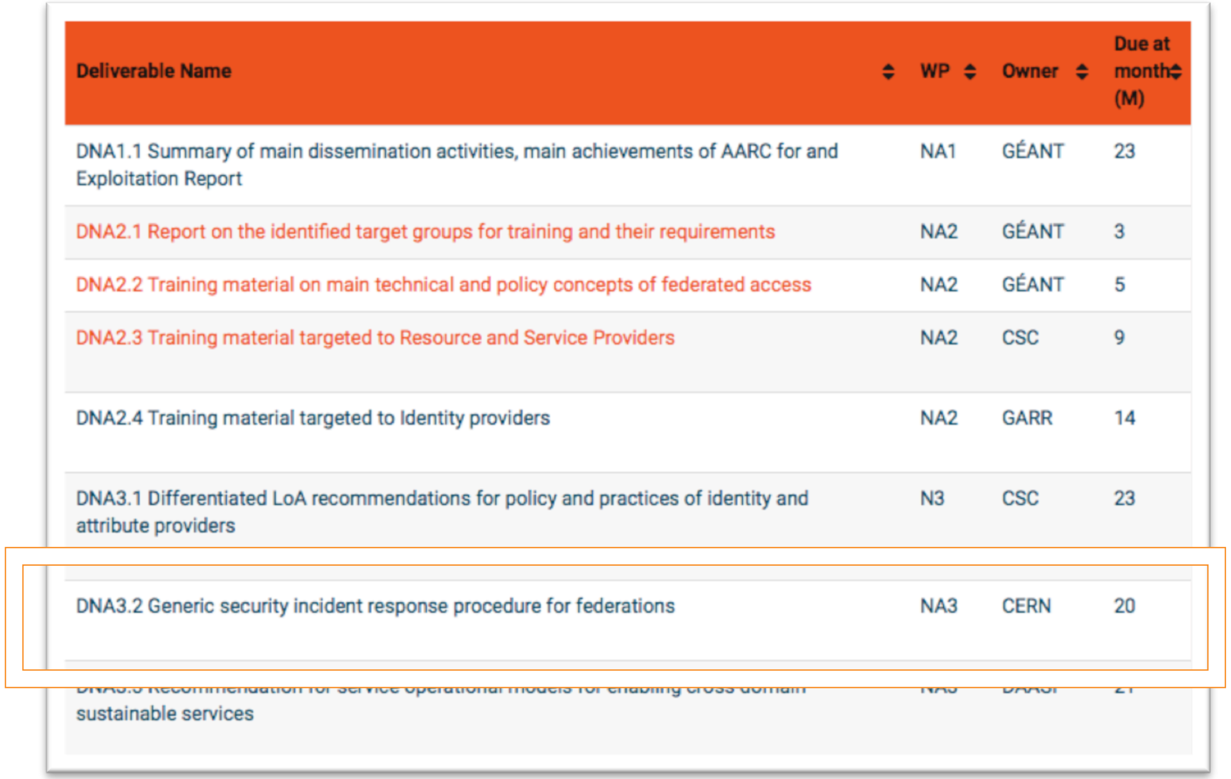

NASA
NASA/DOD Technology Readiness Level
System Test, Launch & Operations
System/Subsystem Development
Technology Demonstration
Technology Development
Research to Prove Feasibility
Basic Technology Research
TRL 9
TRL 8
TRL 7
TRL 6
TRL 5
TRL 4
TRL 3
TRL 2
TRL 1
Actual system "flight proven" through successful mission operations
Actual system completed and "flight qualified" through test and demonstration (Ground or Flight)
System prototype demonstration in a space environment
System/subsystem model or prototype demonstration in a relevant environment (Ground or Space)
Component and/or breadboard validation in relevant environment
Component and/or breadboard validation in laboratory environment
Analytical and experimental critical function and/or characteristic proof-of-concept
Technology concept and/or application formulated
Basic principles observed and reported

Future plans
AARC DNA3.2 Incident Response Procedure

- Sirtfi will form the basis for the “Generic Security Incident Response Procedure for Federations”

- Due January 2017

- Will need to expand on Sirtfi to include
  - Workflows for incident scenarios
  - Interaction with existing policies
  - …



Deliverable Name	WP	Owner	Due at month (M)
DNA1.1 Summary of main dissemination activities, main achievements of AARC for and Exploitation Report	NA1	GÉANT	23
DNA2.1 Report on the identified target groups for training and their requirements	NA2	GÉANT	3
DNA2.2 Training material on main technical and policy concepts of federated access	NA2	GÉANT	5
DNA2.3 Training material targeted to Resource and Service Providers	NA2	CSC	9
DNA2.4 Training material targeted to Identity providers	NA2	GARR	14
DNA3.1 Differentiated LoA recommendations for policy and practices of identity and attribute providers	N3	CSC	23
DNA3.2 Generic security incident response procedure for federations	NA3	CERN	20
DNA3.3 Recommendation for service operational models for enabling cross domain sustainable services	NA3	DAASI	21

Future plans
SCIV2

- WISE Working group SCIV2 https://wiki.geant.org/display/WISE/SCIV2-WG
- SCI document needs some care and attention…
- Incident Response may have an update

- **Come to the WISE BoF this Wednesday! https://tnc16.geant.org/core/event/21**

Future plans
Events

- Moving away from theory and towards proof-of-concept presentations
- The security workshop at ISGC proved an interesting exercise and it would be worth repeating ☺
- Much of this outreach work will be moved to GN4

Event	Location	Date
TNC-16	Prague	June 2016
CIC (15 US Universities)	Michigan	July 2016
TechEx16	Miami	September 2016
TF-CSIRT	Zurich	October 2016
GN4	?	December 2016
EWTI	?	December 2016

Future plans
Country Updates – NL

- **Live for IdPs!**
- Using SURFcert as Security Contact Proxy
- SPs on TODO list

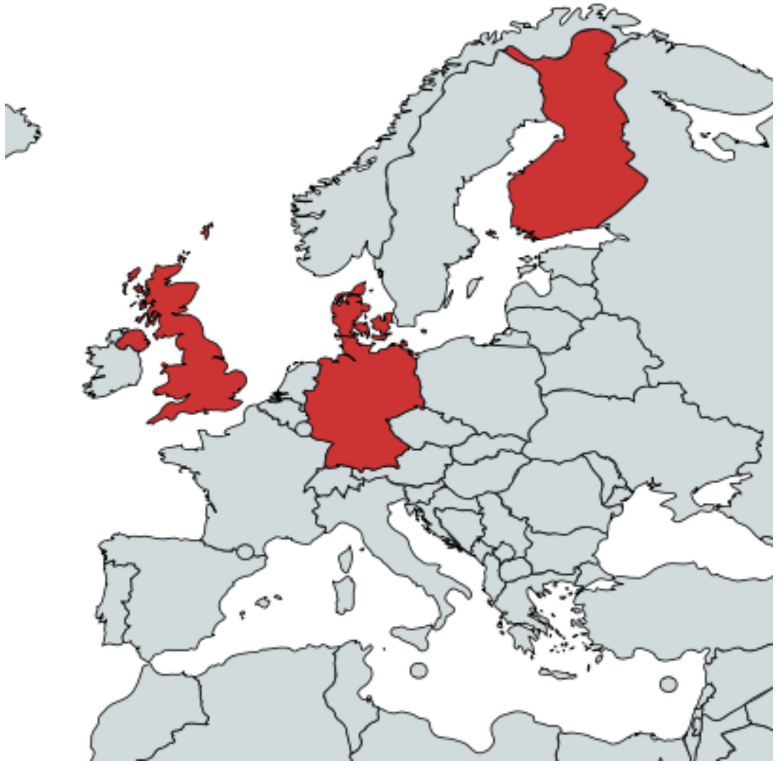
Future plans
Country Updates – U.S.

- Technical work needed
  - Changing from incommon to refeds namespace
  - Would want formal definition of framework, akin to Entity Category Definition
- Outreach work needed
- May leverage REN-ISAC's ~10,000 Security Contacts to get started

Future plans
Country Updates – CH

- Aims to support Sirtfi by Autumn
- Strong support from SWITCH Security Team

Future plans
Deployment - Pilots



Interest from Denmark, Finland, Germany and UK.

Want to be on this map? Come and find me over coffee ☺

Sirtfi is also being incorporated as a requirement for other services, e.g. CERN Services & CiLogon Pilot. To help this, AARC will work on a Pilot for a Sirtfi Discovery Service.

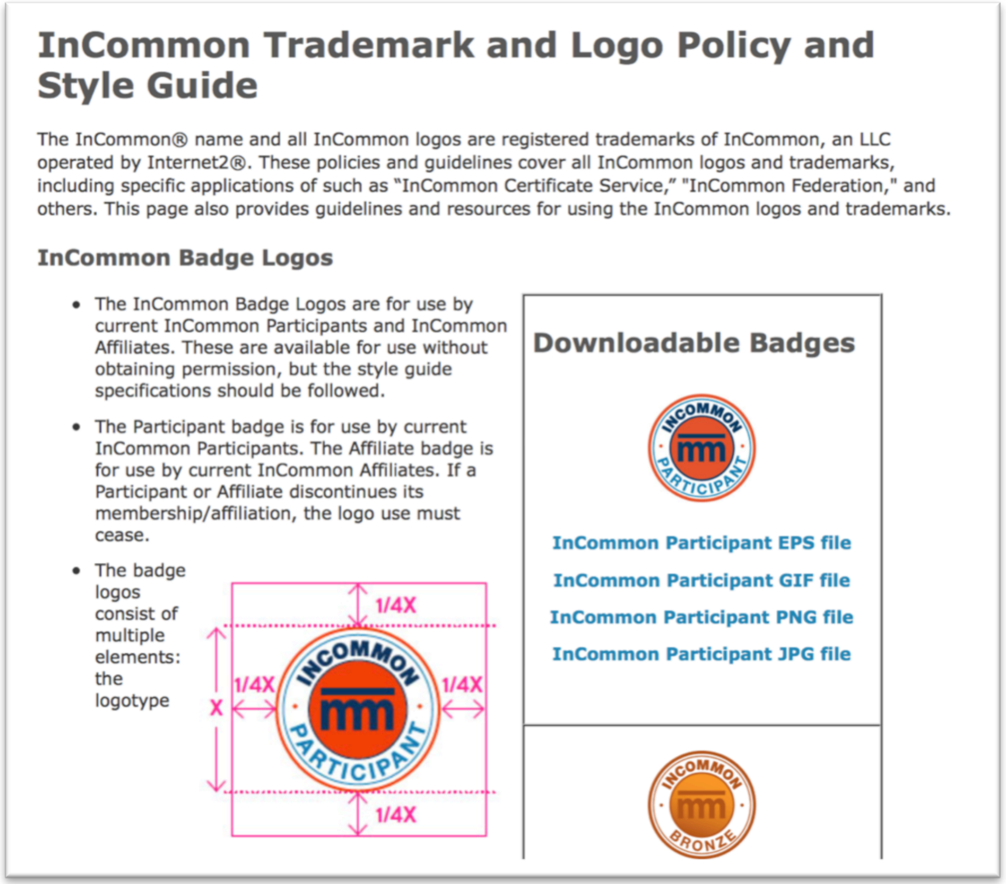
Number of Sirtfi Compliant Entities…

87!

What do you want to do?
How can we show which entities are Sirtfi compliant?

- In the spirit of borrowing InCommon's good ideas…
- There have been several discussions about having a Sirtfi logo
- There is budget in AARC to get this done
- A visual indication of trust would act as a mark of confidence and hopefully encourage other organisations to take a look

What do you think?



InCommon Trademark and Logo Policy and Style Guide

The InCommon® name and all InCommon logos are registered trademarks of InCommon, an LLC operated by Internet2®. These policies and guidelines cover all InCommon logos and trademarks, including specific applications of such as "InCommon Certificate Service," "InCommon Federation," and others. This page also provides guidelines and resources for using the InCommon logos and trademarks.

InCommon Badge Logos

- The InCommon Badge Logos are for use by current InCommon Participants and InCommon Affiliates. These are available for use without obtaining permission, but the style guide specifications should be followed.
- The Participant badge is for use by current InCommon Participants. The Affiliate badge is for use by current InCommon Affiliates. If a Participant or Affiliate discontinues its membership/affiliation, the logo use must cease.
- The badge logos consist of multiple elements: the logotype

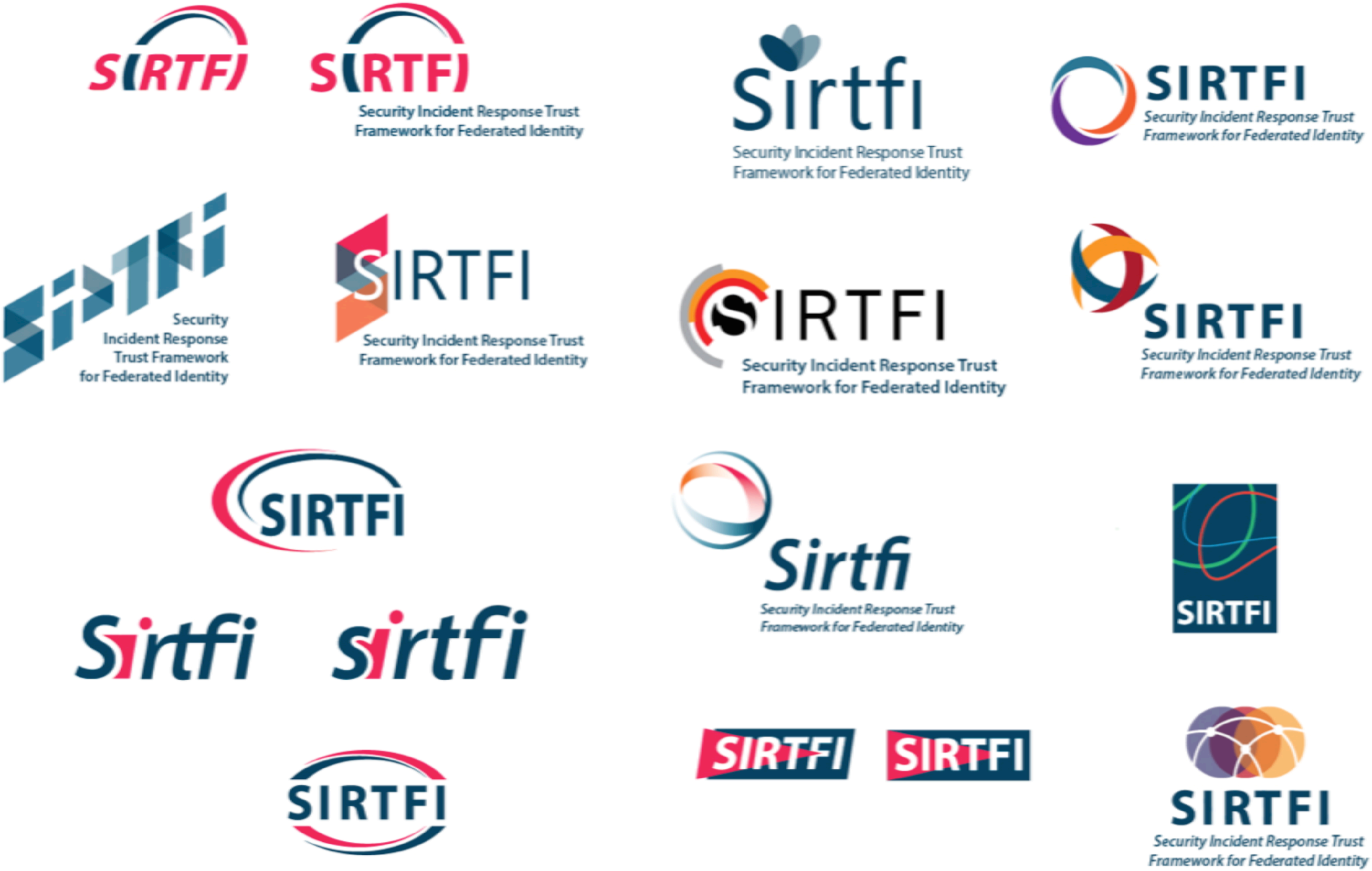
Downloadable Badges

InCommon Participant EPS file

InCommon Participant GIF file

InCommon Participant PNG file

InCommon Participant JPG file


SIRTFI
SIRTFI
Security Incident Response Trust
Framework for Federated Identity
Sirtfi
Security Incident Response Trust
Framework for Federated Identity
SIRTFI
Security Incident Response Trust
Framework for Federated Identity
SIRTFI
Security
Incident Response
Trust Framework
for Federated Identity
SIRTFI
Security Incident Response Trust
Framework for Federated Identity
SIRTFI
Security Incident Response Trust
Framework for Federated Identity
SIRTFI
Security Incident Response Trust
Framework for Federated Identity
SIRTFI
Sirtfi
Security Incident Response Trust
Framework for Federated Identity
SIRTFI
Sirtfi
sirtfi
SIRTFI
SIRTFI
SIRTFI
SIRTFI
Security Incident Response Trust
Framework for Federated Identity

What do you want to do?
Missing Material

Suggestions include:

- An official REFEDS doc akin to an entity category specification https://refeds.org/category/research-and-scholarship to define attestation duration, the relationship between organisations and IdPs/SPs
- Guidance on ensuring currency of contact details – should fed ops ping them regularly?

What do you think?

Thanks

- Sirtfi Working Group for their time, ideas and enthusiasm
- REFEDS Community for their support and input to Consultations
- Licia and AARC for the funding and focus
- Various individuals from AARC who have helped put the training material together

Thank you

Any Questions?

hannah.short@cern.ch

https://aarc-project.eu

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).