



Authentication and Authorisation for Research and Collaboration

## Incident Response

Sirtfi present, future and pilots

**Hannah Short**

NA3.2 Task Lead

CERN-IT



AARC Meeting, Utrecht

24<sup>th</sup> May 2016

## Agenda

---

### What have we done this year?

- Training
- Events

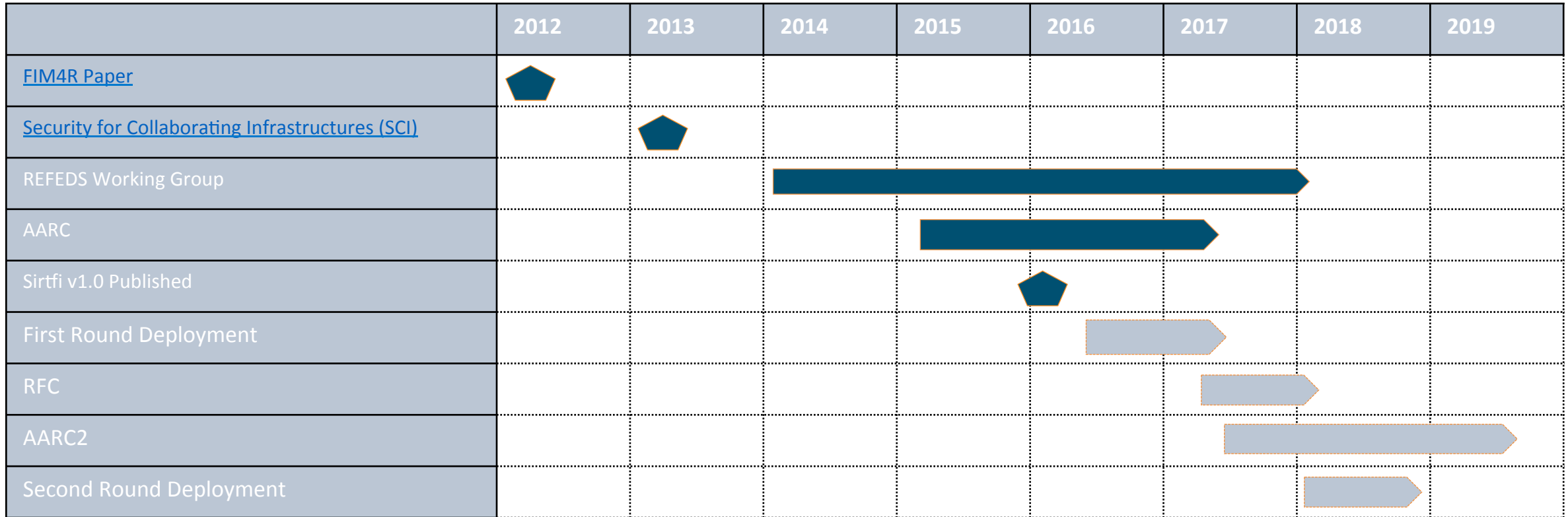
### What will we do next year?

- Deployment
- DNA3.2
- Events

### Some blue sky thinking...

# Sirtfi

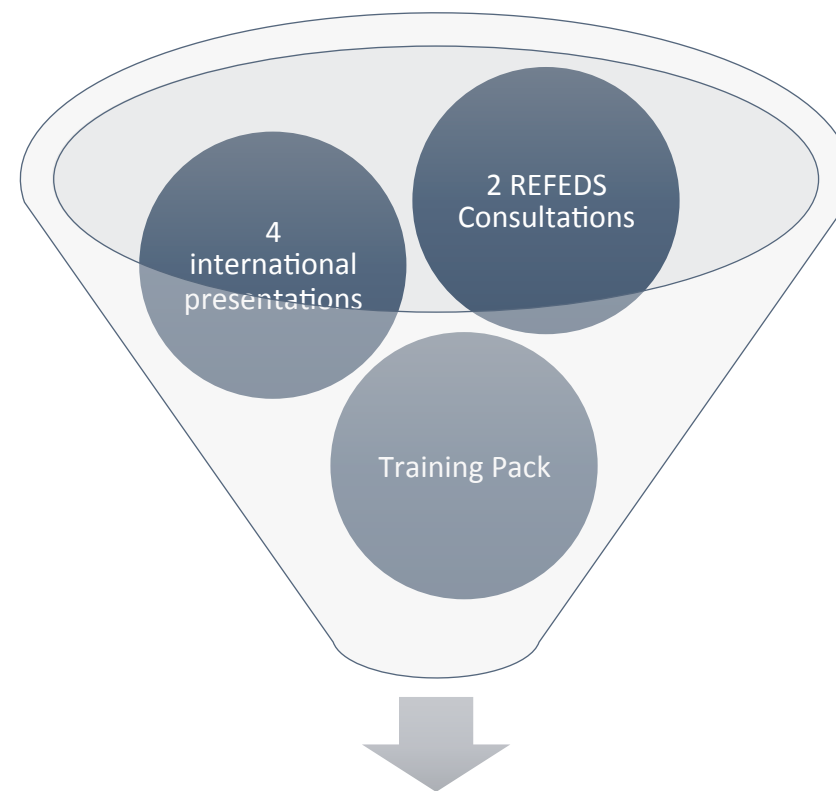
## A timeline



## What have we done this year?

---

- It's been quite a busy year...
- AARC took on the Sirtfi work from the REFEDS WG
- Big milestone was Sirtfi v1.0, which was published early 2016!
- We have been presenting the framework
- We have created training material
- Now we are ready to deploy



**Sirtfi is ready to go!**

# What have we done this year?

## Training Material



### Public Facing Site

- Sirtfi Brochure
- The framework: Sirtfi v1.0
- General FAQs

### Technical Wiki

- Federation Participants Guide
  - Recipe for adoption
- Federation Operators Guide
  - Whitelisting metadata extensions
  - Metadata aggregates
  - Coordinating adoption
- Choosing a Sirtfi Contact
- Technical FAQs

### Additional Background Material

- Blog post
- ISGC Proceedings paper (TBC) – *thank you so much for the feedback and input I received!*
- Poster
- Logo

If you notice gaps or improvements – please speak up!

# What have we done this year?

## Training Material

The screenshot shows the title page of the Sirtfi document, "A Security Incident Response Trust Framework for Federated Identity". It includes the AARC logo, a summary paragraph, a central question "Is your organization part of an identity federation?", and a diagram comparing "The problem" (lack of trust) with "The solution" (a trust framework). It also lists "Why should I join?" and "How can I join?".

The screenshot shows the "Sirtfi Home" page on the REFEDS Spaces platform. It features the Sirtfi logo, navigation links for Pages, Blog, and a Page Tree with items like "Guide for Federation Participants" and "Choosing a Sirtfi Contact". A welcome message states: "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."

The screenshot shows the Sirtfi Wiki page on REFEDS. It has a red header with the Sirtfi logo and navigation links. The main content includes a description of Sirtfi's purpose, a list of assertions for compliance, and information about the REFEDS Sirtfi Working Group. At the bottom, there are three red icons with labels: "Benefits" (Why should I join? What are the Benefits?), "Sirtfi v 1.0" (View the Sirtfi Framework), and "FAQs" (Need help?).

# What have we done this year?

## Events

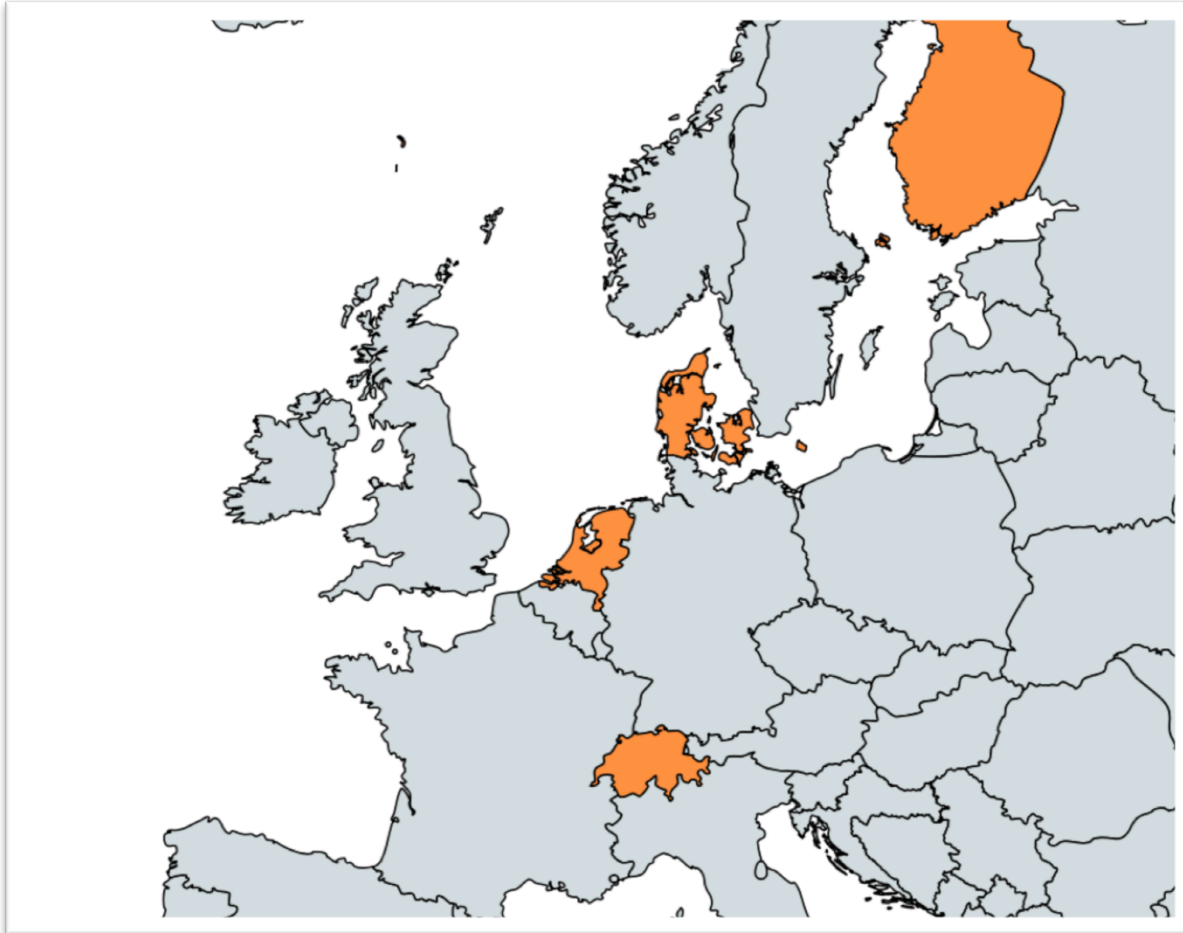
---

- Interest from international audiences
- Requested to present to the Kantara Identity Assurance Working Group
- 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
TF-CSIRT	Riga	12 May 2016

# What will we do next year?

## Deployment - Pilots



Our pilot federations:

- **CSC**
- **SURFconext** – bulk adoption by IdPs!
- **SWITCH** – “By fall 2016 we want to have all IdP/ SP SIRTfI compliant”
- **WAYF**

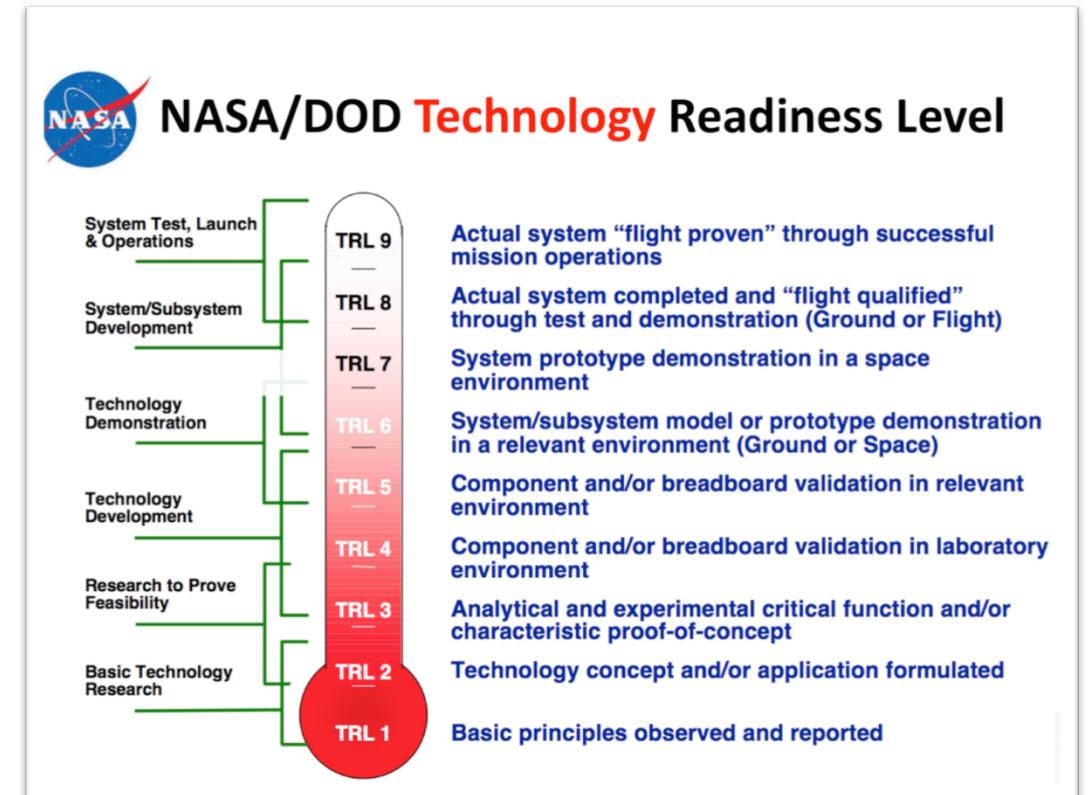
**Sirtfi is also being incorporated into other projects, e.g. CERN Cloud & CiLogon Pilot**



# What will we do next year?

## Deployment - Transition to GN4

- GN4 will take over to move Sirtfi to TRL “Late-stage-pilot”, level 7
- Federation Operator support work will shift to the GN4 project
- Federation Participant support will partially remain an AARC task
- 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



# What will we do next year?

## DNA3.2 Incident Response Procedure

- Sirtfi will form the basis for the “Generic Security Incident Response Procedure for Federations”
- Due in Month 20, i.e. January 2017
- Draft planned for Autumn
- Will need to expand on Sirtfi to include
  - Workflows for incident scenarios
  - Interaction with existing policies
  - ...
- *Watch this space for requests for input!*

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	CERN	21

# What will we do next year?


## 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
TechEx16	Miami	September 2016
TF-CSIRT	Zurich	October 2016
GN4	?	December 2016
EWTI	?	December 2016





What would help the  
community to adopt and  
benefit from Sirtfi?

## Blue sky thinking...

---

### Various tools could help support Sirtfi

- Sirtfi-filtered eduGAIN metadata, handled by Federation Operators
- A dashboard of Sirtfi contacts for quick lookup during an incident
- Self-Assessment tool to distribute Sirtfi Assessments and monitor adoption
- Testing framework to monitor response time in mock-incidents (or real!)

## Blue sky thinking...

---

### Various tools could help support Sirtfi

- Sirtfi-filtered eduGAIN metadata, handled by Federation Operators – *New AARC Pilot*
- A dashboard of Sirtfi contacts for quick lookup during an incident – *GN4*
- Self-Assessment tool to distribute Sirtfi Assessments and monitor adoption - ??
- Testing framework to monitor response time in mock-incidents (or real!) – *GN4*

# Thank you

## Any Questions?

[hannah.short@cern.ch](mailto: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).