AARC Authentication and Authorisation for Research and Collaboration

Testing Incident Response Channels and Communications End Points

whilst not overloading the target audience

David Groep

AARC Policy and Best Practice Activity Coordinator

Nikhef

WISE Community meeting, Abingdon

February 27, 2018

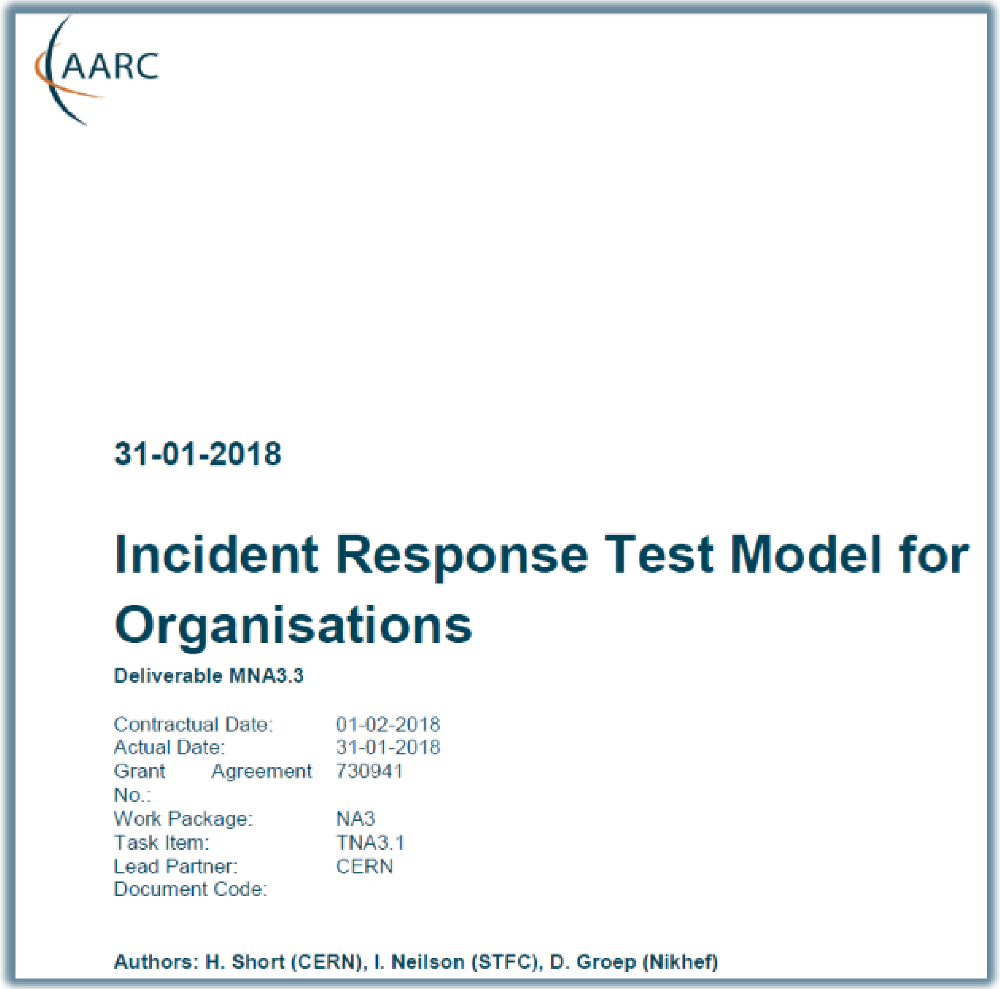
Distributed Incident Response and Readiness Challenges

Sirtfi version 1 is gaining traction

- provides - self-asserted - security contacts
- point-to-point communications
- interaction not usually visible at the 'global' level

we need to now go 'beyond *Sirtfi*'

- incidents are not usually bi-lateral
- may spread through federated identity systems
- and outside to relying parties or entire Infrastructure



31-01-2018

Incident Response Test Model for Organisations

Deliverable MNA3.3

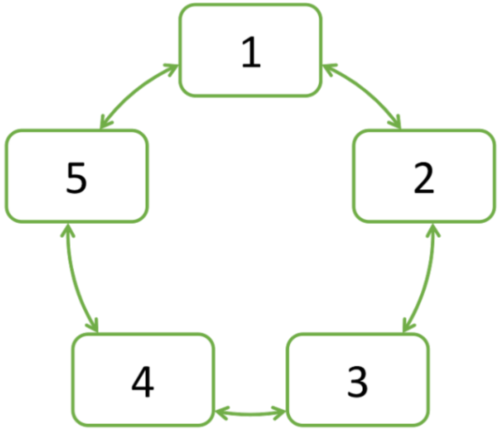
Contractual Date:	01-02-2018
Actual Date:	31-01-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	TNA3.1
Lead Partner:	CERN
Document Code:	

Authors: H. Short (CERN), I. Neilson (STFC), D. Groep (Nikhef)

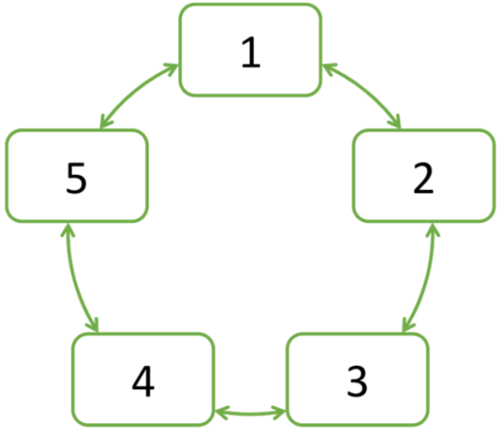
Beyond Sirtfi: streamlining the response process

trust relationships: allow information to flow rapidly to all that need to know

Infrastructure sharing model: PRACE, XSEDE, …

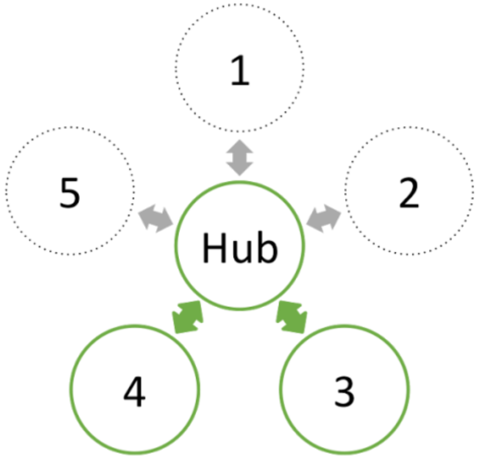


During Incident Response
Information shared between all participants

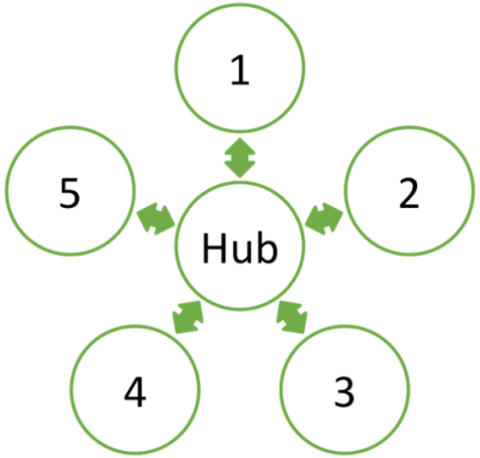


Post-Incident-Report Sharing
Information shared between all participants

Infrastructure sharing model: EGI, WLCG, …



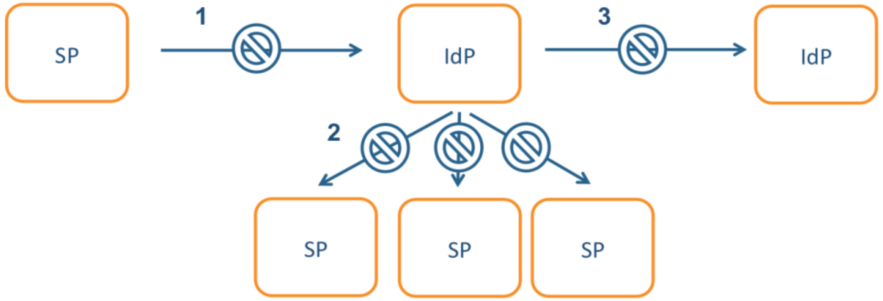
During Incident Response
Information shared between affected participants



Post-Incident-Report Sharing
Information shared between all participants

graphics: Hannah Short, AARC ‘DNA3.1’ incident response models

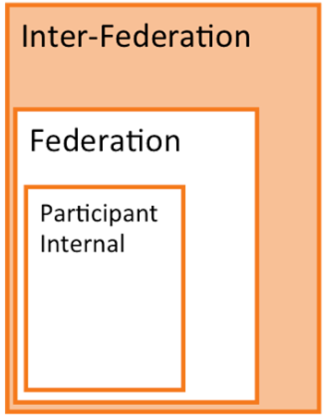
Incident response process evolution in federations



Incident Response Communication, communication blocks

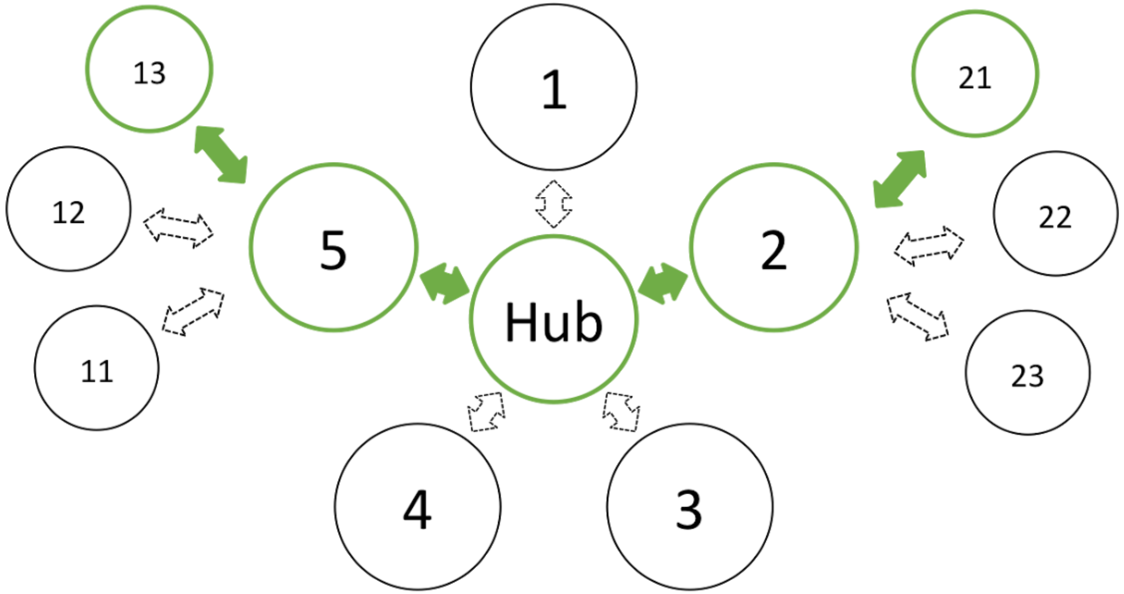
Challenges

- IdP appears ‘outside’ the service’s security mandate
- Lack of contact, or lack of trust, in IdP, which is an ‘unknown party’
- IdP fails to inform other affected SPs, for fear of leaking data or reputation
- No established channels of communication



Proposed solutions

- Stronger role for federation operators, as they are known to both SPs and IdPs
- Add hub capability centrally (@ eduGAIN)



Inter-Federation Incident Response Communication

graphics: Hannah Short, AARC ‘DNA3.1’ incident response models

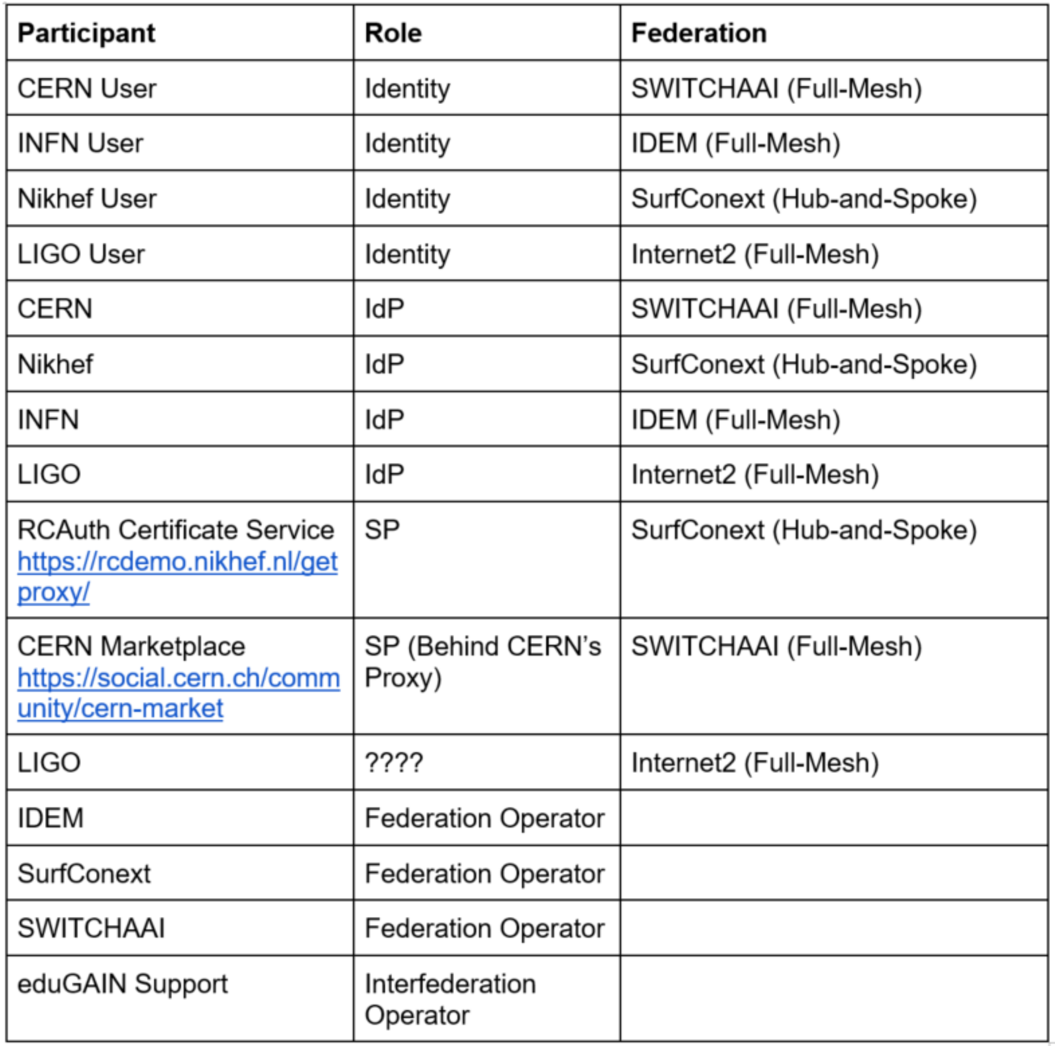
Would this model work? You have to test!

Incident Response Test Model for Organisations

simulated incident to evaluate the model

- Many participants
- Participants from multiple (existing) infrastructures
- Leverages (and overlaps with) existing groups

Test with these participants was run by Hannah as 'AARC' – *phase 1 ran last week*



Participant	Role	Federation
CERN User	Identity	SWITCHAAI (Full-Mesh)
INFN User	Identity	IDEM (Full-Mesh)
Nikhef User	Identity	SurfConext (Hub-and-Spoke)
LIGO User	Identity	Internet2 (Full-Mesh)
CERN	IdP	SWITCHAAI (Full-Mesh)
Nikhef	IdP	SurfConext (Hub-and-Spoke)
INFN	IdP	IDEM (Full-Mesh)
LIGO	IdP	Internet2 (Full-Mesh)
RCAuth Certificate Service https://rcdemo.nikhef.nl/getproxy/	SP	SurfConext (Hub-and-Spoke)
CERN Marketplace https://social.cern.ch/community/cern-market	SP (Behind CERN's Proxy)	SWITCHAAI (Full-Mesh)
LIGO	????	Internet2 (Full-Mesh)
IDEM	Federation Operator	
SurfConext	Federation Operator	
SWITCHAAI	Federation Operator	
eduGAIN Support	Interfederation Operator	

Who runs the test?

- Test with these participants was run ‘by AARC’

Logical candidates that could all run the test … and ‘legitimately’ claim an interest

- eduGAIN
- GEANT.org
- EOSC-HUB ops, or EGI CSIRT
- IGTF
- each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, OSG, HPCI, …
- every research infra with an interest: WLCG, LSAAI, BBMRI, ELIXIR, …
- any institution (or person) with access to https://mds.edugain.org/

so in a short while, all the email in the world will be on Sirtfi Incident Response tests??

Frequency of challenges and tests - examples

Trusted Introducer and TF-CSIRT

- 2-3 Reaction Tests per year
- supported by web click infrastructure, but requires (team) authentication

SURFcert challenges

- annual response challenges, just reply to email to a (traceable) ticket

IGTF RAT Communications Challenges

- every 1-2 years
- in parallel with continuous operational monitoring

yet we already listed 14 entities that have a real interest in running tests, 5000+ entities can claim the same

How to coordinate – discussion items!

Designate a lead 'management' organization for each element?

so that each 'target' does not get hit by many competing and concurrent challenges?

- e.g. eduGAIN to run communications challenges against Sirtfi email addresses
- the e-Infrastructures to test responsiveness of SPs and RPs
  with each RP/SP/Site having a primary e-Infra as its home?
  or can we jointly (EOSC-HUB) run these challenges per continent?
- coordination must be global

Communications challenges also build 'confidence' and trust – an important social aspect

- unless you run the test yourself, or get full insight in the results of a challenge,
  you may not be growing more trust in the entities tested
- so to get that 'warm and fuzzy feeling of trust',
  results (responsiveness measurement data) should be shared
  but that sharing needs to be confidential as well – limit to WISE SCI checked infrastructures?

Thank you

Any Questions?

davidg@Nikhef.nl

AARC

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. 730941 (AARC2).