AARC Authentication and Authorisation for Research and Collaboration

Trust by Demonstration … without overdoing it

Security Coordination Communications Challenges – all in it together

David Groep

AARC Community, policy and best practice area

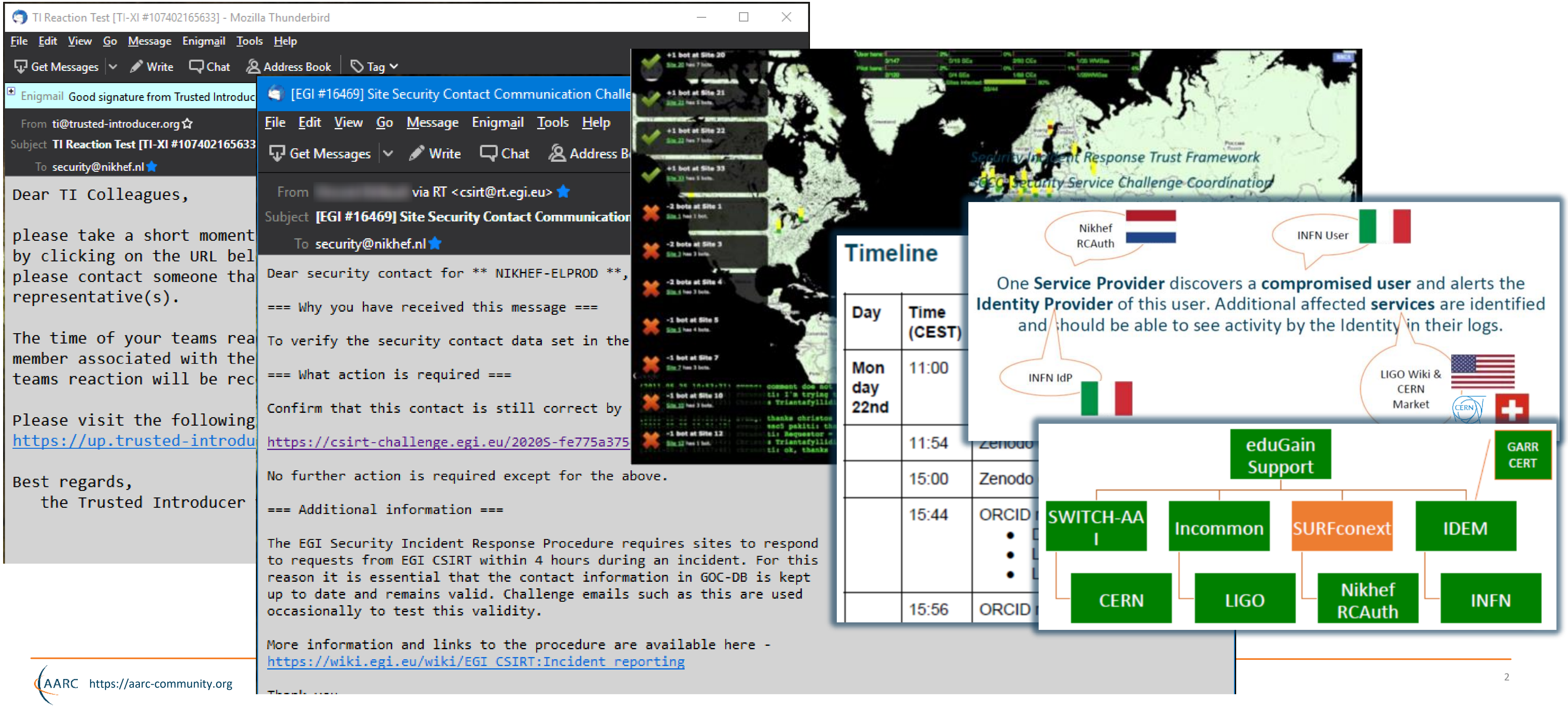
Nikhef PDP programme

Nikhef

WISE Community meeting

April 2020

Many communities test, test, and test again



TI Reaction Test [TI-XI #107402165633] - Mozilla Thunderbird
File Edit View Go Message Enigmail Tools Help
Get Messages
Write
Chat
Address Book
Tag

Enigmail Good signature from Trusted Introduc

From ti@trusted-introducer.org

Subject TI Reaction Test [TI-XI #107402165633

To security@nikhef.nl

```
Dear TI Colleagues,

please take a short moment
by clicking on the URL bel
please contact someone tha
representative(s).

The time of your teams rea
member associated with the
teams reaction will be rec

Please visit the following
https://up.trusted-introdu

Best regards,
   the Trusted Introducer
```

[EGI #16469] Site Security Contact Communication Challe
File Edit View Go Message Enigmail Tools Help
Get Messages
Write
Chat
Address B

From [redacted] via RT <csirt@rt.egi.eu>

Subject [EGI #16469] Site Security Contact Communication

To security@nikhef.nl

```
Dear security contact for ** NIKHEF-ELPROD **,

=== Why you have received this message ===

To verify the security contact data set in the

=== What action is required ===

Confirm that this contact is still correct by

https://csirt-challenge.egi.eu/2020S-fe775a375

No further action is required except for the above.

=== Additional information ===

The EGI Security Incident Response Procedure requires sites to respond
to requests from EGI CSIRT within 4 hours during an incident. For this
reason it is essential that the contact information in GOC-DB is kept
up to date and remains valid. Challenge emails such as this are used
occasionally to test this validity.

More information and links to the procedure are available here -
https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting

Thank you
```

```
+1 bot at Site 20
Site 20 has 7 bots.
+1 bot at Site 21
Site 21 has 5 bots.
+1 bot at Site 22
Site 22 has 7 bots.
+1 bot at Site 33
Site 33 has 5 bots.
-2 bots at Site 1
Site 1 has 1 bot.
-2 bots at Site 3
Site 3 has 3 bots.
-2 bots at Site 4
Site 4 has 3 bots.
-1 bot at Site 5
Site 5 has 4 bots.
-1 bot at Site 7
Site 7 has 3 bots.
-1 bot at Site 10
Site 10 has 3 bots.
-1 bot at Site 12
Site 12 has 1 bot.
comment doe not
ti: I'm trying
s Triantafyllidi
thanks christos
sec5 pakiti: th
ti: Requestor -
s Triantafyllidi
ti: ok, thanks
```

Security Incident Response Trust Framework

SCCC Security Service Challenge Coordination

Timeline

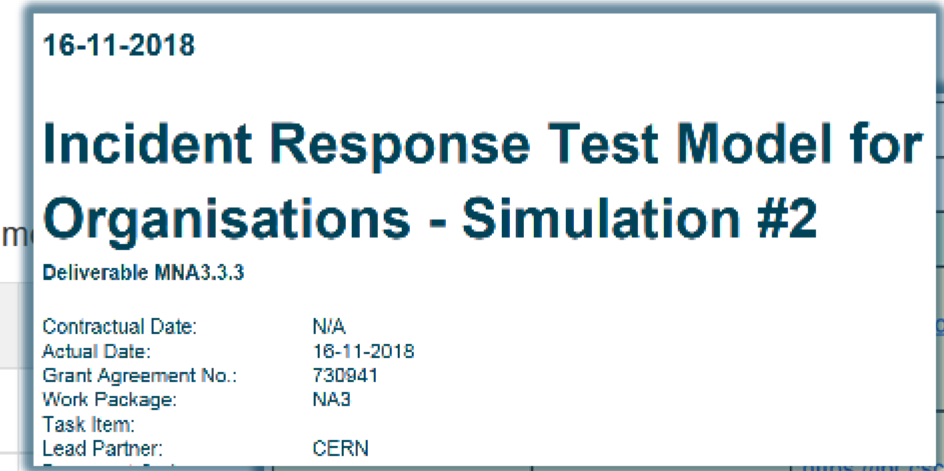
Day	Time (CEST)	
Monday 22nd	11:00	
	11:54	Zenodo
	15:00	Zenodo
	15:44	ORCID • • •
	15:56	ORCID

One **Service Provider** discovers a **compromised user** and alerts the **Identity Provider** of this user. Additional affected **services** are identified and should be able to see activity by the Identity in their logs.

One test amongst many – *but the first in the Sirtfi (eduGAIN) community*

In AARC2 we will further the work undertaken in AARC and provide a fram

Month	What	
9	Incident Response Test Model for Organizations **MNA3.3**	
10	Incident Simulation #1 Report	https://aarc-pr
19	Incident Simulation #2 Report	https://aarc-p
?	Guideline on Incident Response for Federation Participants	Draft at https:
22	Report on Security Incident Response **DNA3.2**	Draft at https:

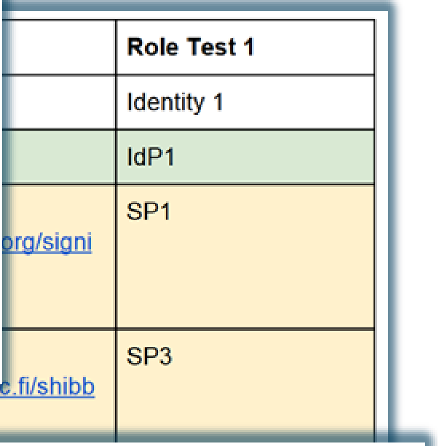


16-11-2018

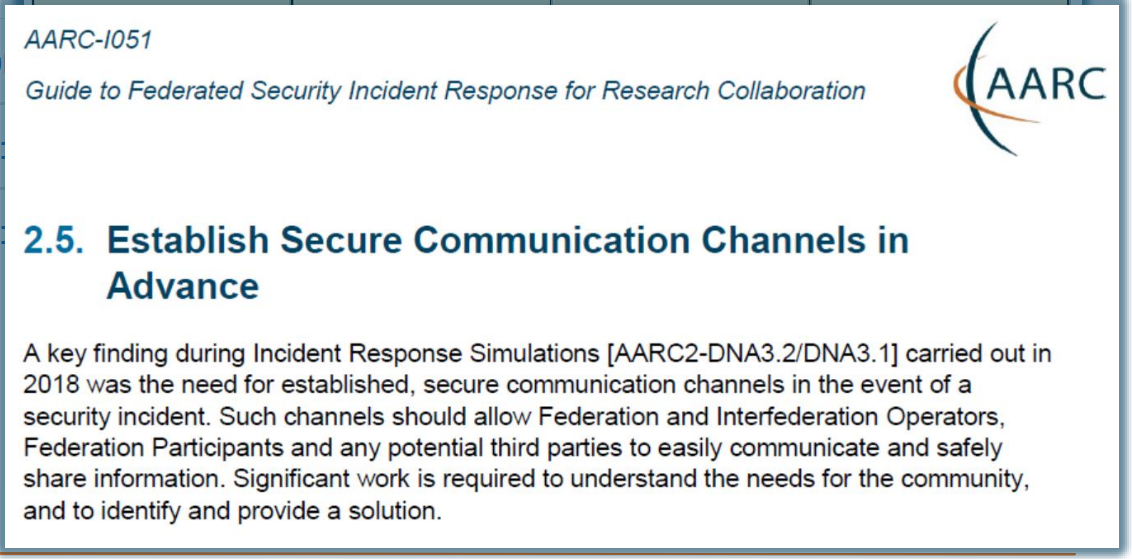
Incident Response Test Model for Organisations - Simulation #2

Deliverable MNA3.3.3

Contractual Date:	N/A
Actual Date:	16-11-2018
Grant Agreement No.:	730941
Work Package:	NA3
Task Item:	
Lead Partner:	CERN



	Role Test 1
	Identity 1
	IdP1
org/signi	SP1
https://ibr.csc.fi/shibboleth	SP3



AARC-I051

Guide to Federated Security Incident Response for Research Collaboration

2.5. Establish Secure Communication Channels in Advance

A key finding during Incident Response Simulations [AARC2-DNA3.2/DNA3.1] carried out in 2018 was the need for established, secure communication channels in the event of a security incident. Such channels should allow Federation and Interfederation Operators, Federation Participants and any potential third parties to easily communicate and safely share information. Significant work is required to understand the needs for the community, and to identify and provide a solution.

https://wiki.geant.org/display/AARC/AARC2+NA3+Task+1+-++Overview
https://aarc-project.eu/guidelines/aarc-i051/

Who runs the test?

The first tests with these participants were run ‘by AARC’

Logical candidates that could all run the test

… and have an interest in knowing the result to establish trust

- eduGAIN
- GEANT.org
- but also any EOSC-HUB and e-Infrastructure CSIRT teams
- the IGTF (as it leverages federated id)
- each of the e-Infrastructures XSEDE, EGI, EUDAT, PRACE, OSG, HPCI, …
- every research infra with an interest: WLCG, LSAAI, BBMRI, ELIXIR, …

And any institution (or person) with access to https://mds.edugain.org/ can run them, of course

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

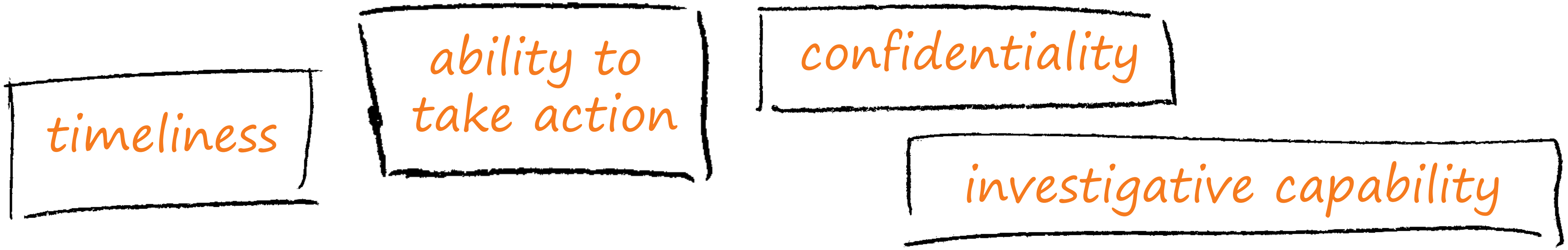
IGTF RAT Communications Challenges

- 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

Challenge elements – what is valued or expected might differ …

A single test and challenge can answer one **or more** of these questions



timeliness

ability to take action

confidentiality

investigative capability

- when data available: infrastructure can set its *own level* of expectancy and gives *deep trust*
- assessment supported with community controls (suspension) gives a *baseline compliance*

Communications challenges build ‘confidence’ and trust – an important social aspect!

- different tests bring complementary results: responsiveness vs. ability act , or do forensics
- unless you run the test yourself, you may not be growing more trust in the entities tested
- for a ‘warm and fuzzy feeling of trust’, share results: but this is sociologically still challenging …

Coordination and mutual reliance

Target audiences and capabilities mostly have a 'natural' primary home

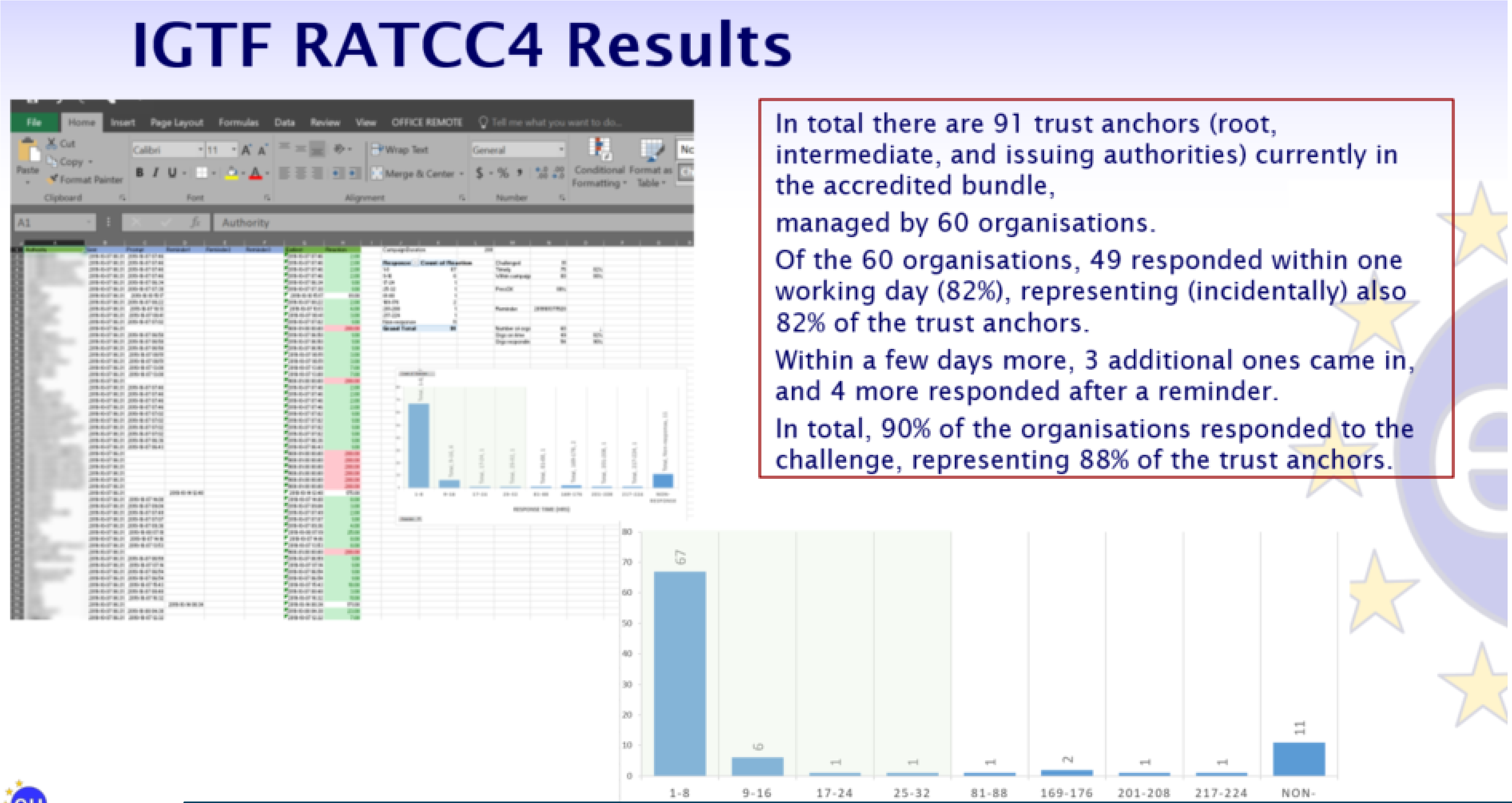
so that each 'target' does not get hit by many concurrent challenges

- 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?

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

- unless you test yourself, or get insight in the results of a challenge, trust may now grow enough
- so to get that 'warm and fuzzy feeling of trust', results could be shared
- *and that sharing needs to be confidential as well, and granularity tunes to audience*

IGFT RATCC4



IGTF RATCC4 Results

In total there are 91 trust anchors (root, intermediate, and issuing authorities) currently in the accredited bundle,

managed by 60 organisations.

Of the 60 organisations, 49 responded within one working day (82%), representing (incidentally) also 82% of the trust anchors.

Within a few days more, 3 additional ones came in, and 4 more responded after a reminder.

In total, 90% of the organisations responded to the challenge, representing 88% of the trust anchors.

PS: of the non-response organisations,
4 had their public contact meta-data fixed, and 2 were withdrawn from the distribution

The SCCC Working Group – a joint effort of many

Coordination of ‘CCs recipient groups’ among participating infrastructures

- ensure targets are not overloaded by coinciding or overlapping challenges, for example by designating lead agency

Transitivity of trust based on challenge frequency and results

- for example by specifying the level of disclosure detail for CCs
- as extension: could CCs be requested e.g. in response to changed risk assessments between infrastructures?

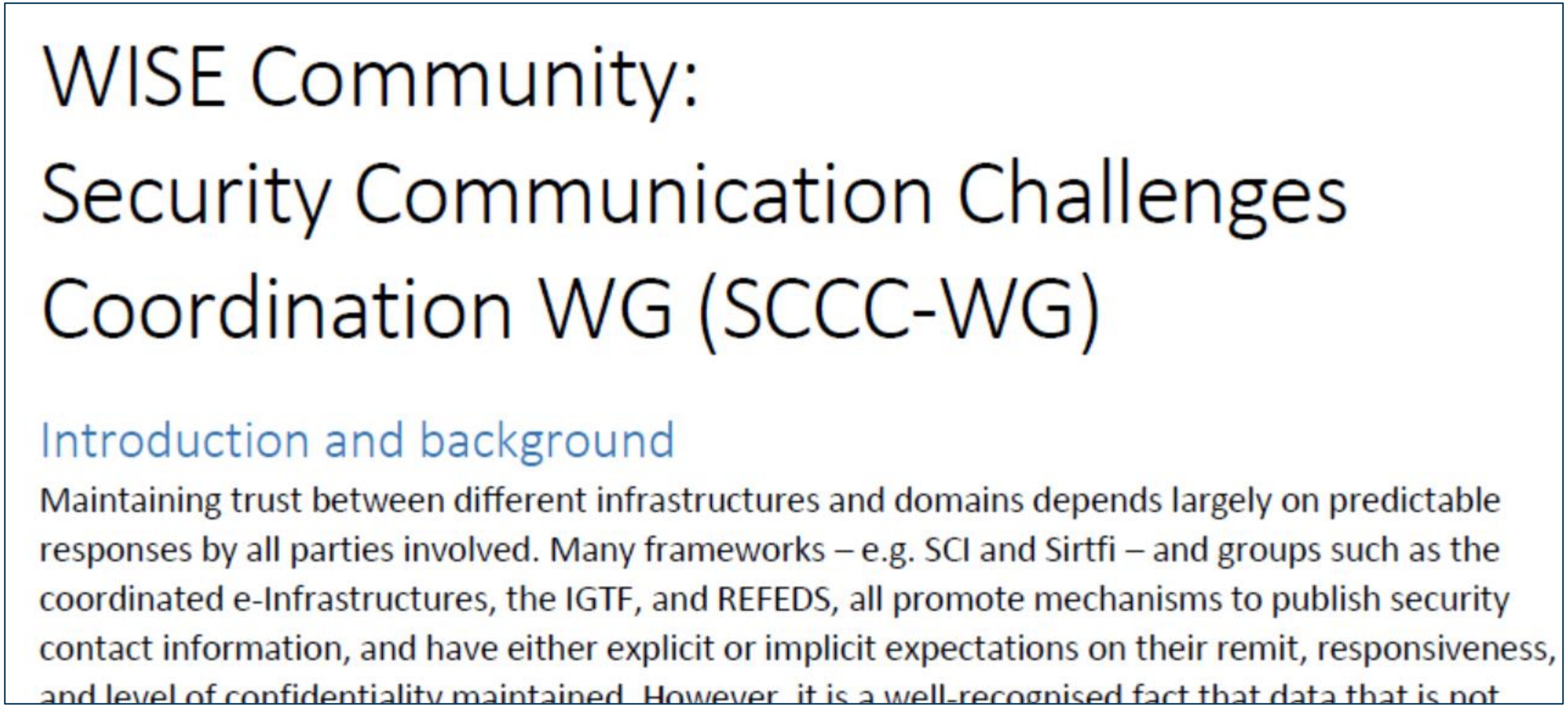
Definition of CC models and classification

- ‘depth’ of the CC testing is a balance between the level of trust gained
  (more profound testing and good results gives more trust)
  and expediency
  (asking mail or click response consumes less resources than requesting forensics of simulated incident)

Frequency of CCs

- simple communications challenges are often performed one or several times per year
- complex challenges are less frequent (e.g. ‘black-box traceability’ trials in EGI take place once every 1-2 years)
- following a CC model classification, propose an appropriate frequency for each class

Continued engagement and coordination: WISE SCCC JOINT WG



WISE Community:
Security Communication Challenges Coordination WG (SCCC-WG)

Introduction and background

Maintaining trust between different infrastructures and domains depends largely on predictable responses by all parties involved. Many frameworks – e.g. SCI and Sirtfi – and groups such as the coordinated e-Infrastructures, the IGTF, and REFEDS, all promote mechanisms to publish security contact information, and have either explicit or implicit expectations on their remit, responsiveness, and level of confidentiality maintained. However, it is a well-recognised fact that data that is not

WISE

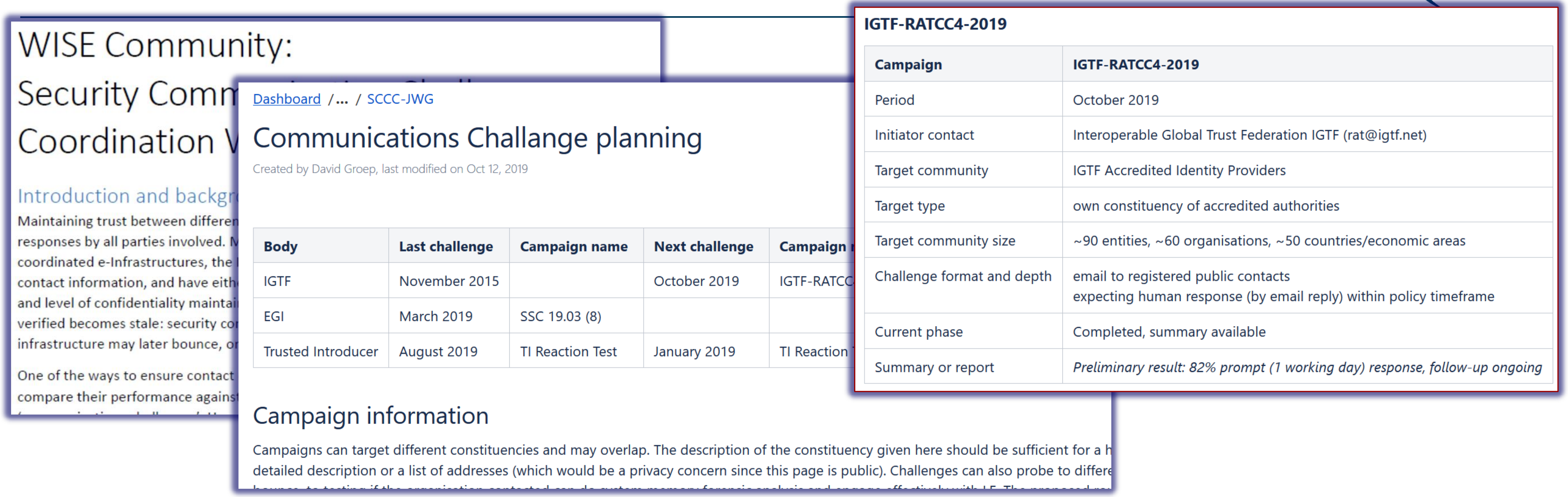
SIG-ISM

REFEDS

IGTF

https://wiki.geant.org/display/WISE/SCCC-JWG

WISE SCCC-WG – participate!



WISE Community:
Security Comm
Coordination W

Introduction and backgr

Maintaining trust between differen
responses by all parties involved. M
coordinated e-Infrastructures, the
contact information, and have eith
and level of confidentiality maintai
verified becomes stale: security co
infrastructure may later bounce, or

One of the ways to ensure contact
compare their performance against

[Dashboard](#) / ... / SCCC-JWG

Communications Challange planning

Created by David Groep, last modified on Oct 12, 2019

Body	Last challenge	Campaign name	Next challenge	Campaign n
IGTF	November 2015		October 2019	IGTF-RATCC
EGI	March 2019	SSC 19.03 (8)		
Trusted Introducer	August 2019	TI Reaction Test	January 2019	TI Reaction

Campaign information

Campaigns can target different constituencies and may overlap. The description of the constituency given here should be sufficient for a h
detailed description or a list of addresses (which would be a privacy concern since this page is public). Challenges can also probe to differe

IGTF-RATCC4-2019

Campaign	IGTF-RATCC4-2019
Period	October 2019
Initiator contact	Interoperable Global Trust Federation IGTF (rat@igtf.net)
Target community	IGTF Accredited Identity Providers
Target type	own constituency of accredited authorities
Target community size	~90 entities, ~60 organisations, ~50 countries/economic areas
Challenge format and depth	email to registered public contacts expecting human response (by email reply) within policy timeframe
Current phase	Completed, summary available
Summary or report	*Preliminary result: 82% prompt (1 working day) response, follow-up ongoing*

WISE, SIGISM, REFEDS, TI joint working group

see wise-community.org and join!

https://wiki.geant.org/display/WISE/SCCC-JWG

co-chairs: Hannah Short (CERN) and David Groep (Nikhef)

Making the SCCC JWG a useful place for all

- How to grow the community and leverage the trust built?
- Can we use joint machinery for running challenges?
  eduGAIN, EGI, TI, SURF all have tooling, and more is coming
- The Wiki page is a start – evolution and completeness requires *you*!

And beyond communications, there is more to be had:

1. **Crisis exercises – the true test of readiness, and a great way of being prepared!**
   look at the great things Charlie et al. are doing, like CLAW ☺

2. **eduGAIN communications and crises simulation – join in the discussion**
   see https://etherpad.servus.at/p/tiime19_edugain

Thank you

Any Questions?

davidg@nikhef.nl

AARC

https://aarc-community.org

The work leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme and other sources.

This work is part of a project that has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 731122 (GN4-2).

We thank the following sources: EC Horizon 2020 projects GN4-3, EOSChub, and AARC-2; and the Dutch National e-Infrastructure coordinated by SURF