



Authentication and Authorisation for Research and Collaboration

## Get in touch – and be sure to get an answer?

Security Communications Challenge Coordination – all in it together

**David Groep**

AARC Community, policy and best practice area

*Nikhef PDP programme*

Nikhef

WISE Community meeting

May 2021

# 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 Introducer

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 below please contact someone that is representative(s).

The time of your teams reaction member associated with the teams reaction will be recorded.

Please visit the following <https://up.trusted-introducer.org/>

Best regards,  
the Trusted Introducer

---

[EGI #16469] Site Security Contact Communication Challenge

File Edit View Go Message Enigmail Tools Help

Get Messages Write Chat Address Book Tag

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

Subject [EGI #16469] Site Security Contact Communication Challenge

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 GOC-DB.  
 === What action is required ===  
 Confirm that this contact is still correct by visiting the following URL:  
<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.

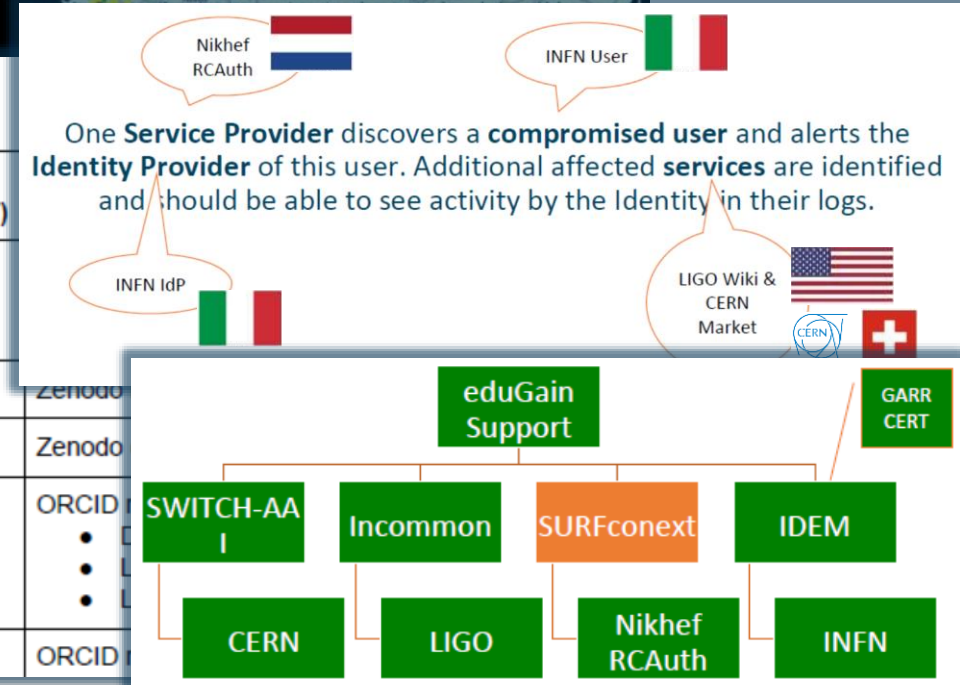
More information and links to the procedure are available here - [https://wiki.egi.eu/wiki/EGI\\_CSIRT:Incident\\_reporting](https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting)

Thank you



## Timeline

Day	Time (CEST)	Event
Monday	11:00	
	11:54	Zenodo
	15:00	Zenodo
	15:44	ORCID
	15:56	ORCID



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

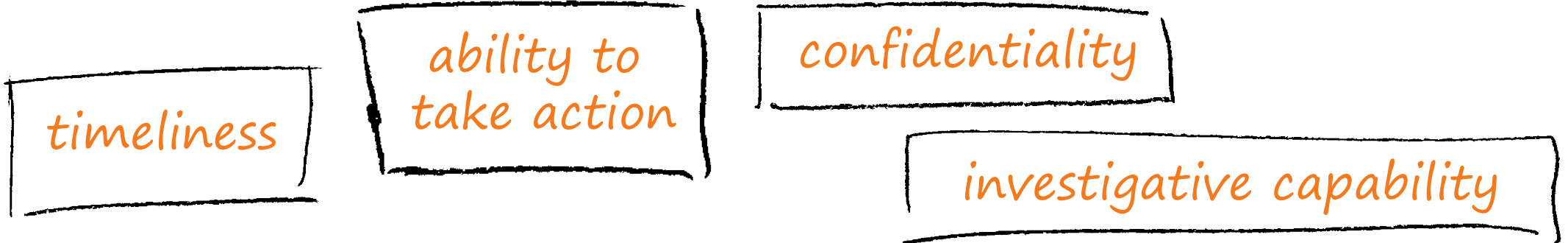
## Introduction and background

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

Joint WG with  
WISE  
SIG-ISM  
REFEDS  
IGTF

## Challenge elements – what is valued or expected might differ ...

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



- 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, ability act, do forensics, ...

# WISE SCCC-WG – participate!

WISE Community:

Security Comm

Coordination V

Introduction and backgr

Maintaining trust between differ  
responses by all parties involved. N  
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 agains

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

## Communications Challenge planning

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

Body	Last challenge	Campaign name	Next challenge	Campaign
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  
bounced to testing if the communication contacted people, custom messages, forwarding analysis and response effectiveness with I.E. The success level

### 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	<i>Preliminary result: 82% prompt (1 working day) response, follow-up ongoing</i>

WISE, SIGISM, REFEDS, TI joint working group  
*see wise-community.org wiki and join!*

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

# Thank you Any Questions?

davidg@nikhef.nl



<https://aarc-community.org>



© members of the AARC Community.

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 (GN4-3).

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