Nikhef

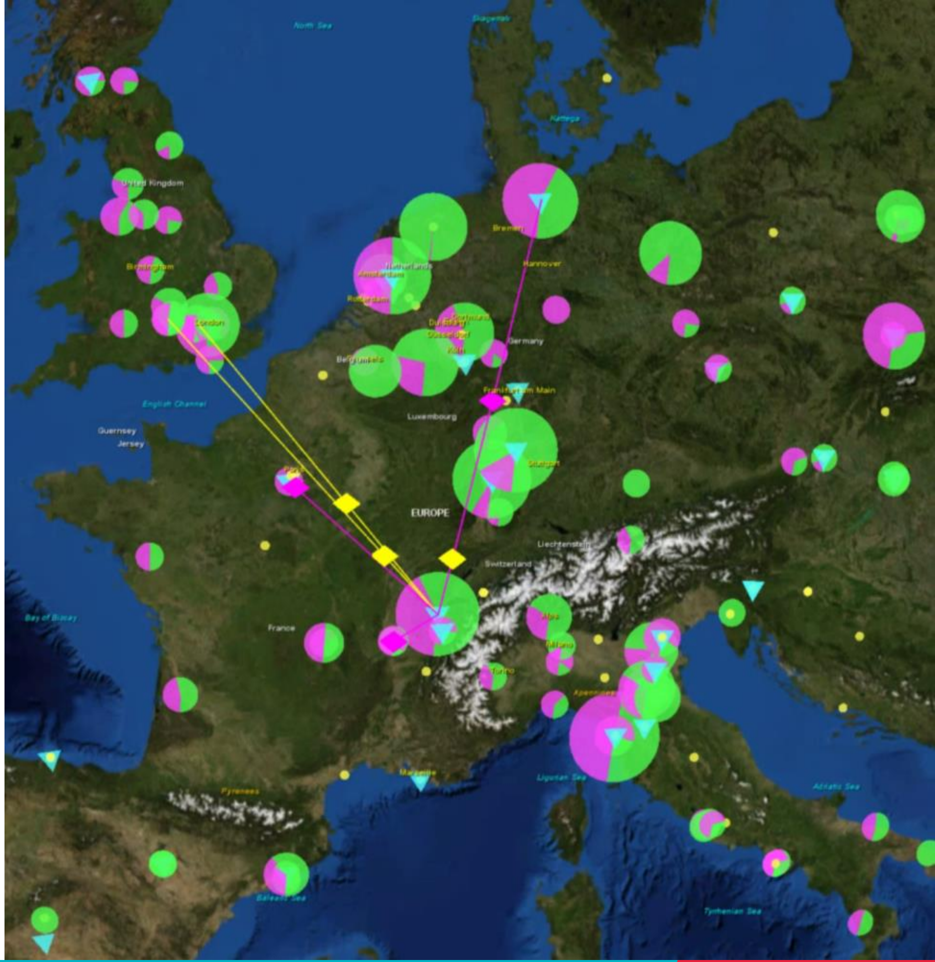
TRUST, SECURITY, AND OPERATIONS
IN ICT INFRASTRUCTURES FOR RESEARCH
AT THE NIKHEF PHYSICS DATA PROCESSING GROUP

INFRASTRUCTURE FOR COLLABORATION

David Groep
January 2019
KPN subset

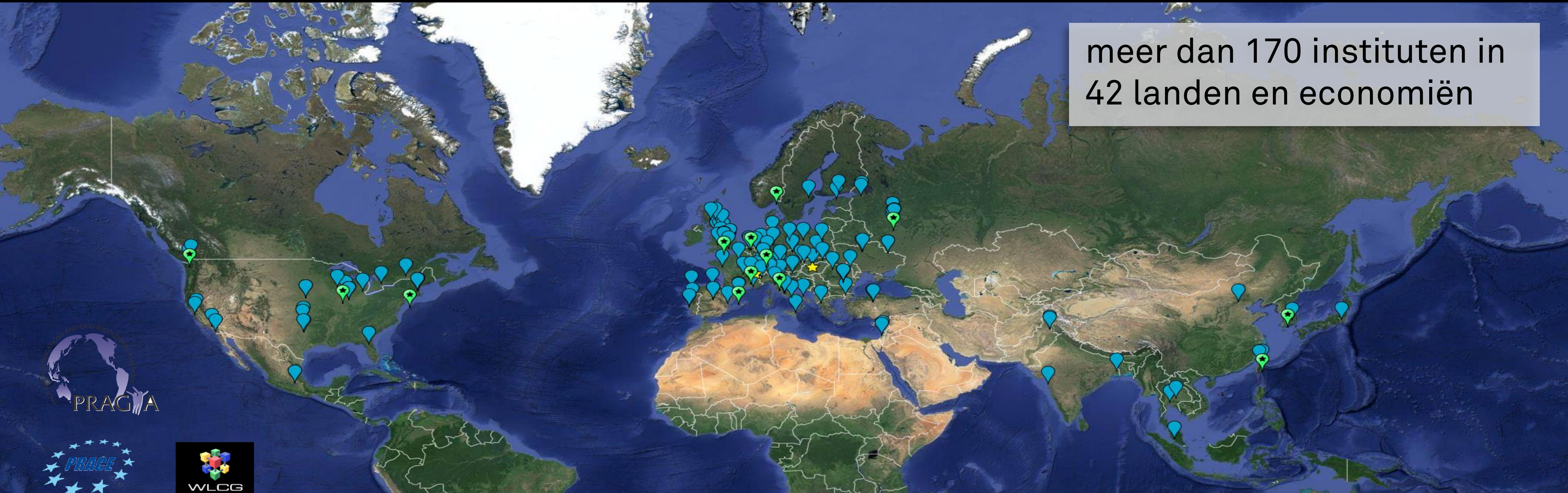
SECURITY: INFRASTRUCTURE FOR COLLABORATION

- global **policy** and best practice harmonization
- access control **middleware** for multi-domain services
- **operational security**: response and forensics
- **training** and communications



Nikhef

LCG – a global collaboration



meer dan 170 instituten in 42 landen en economiën

PRAGMA

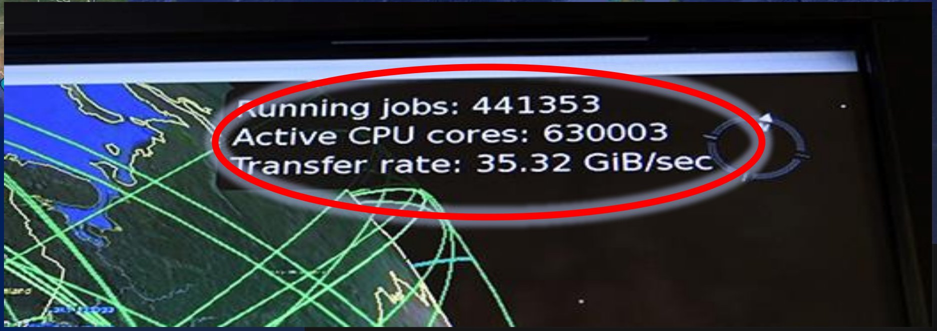
PRACE

WLCG
Worldwide LHC Computing Grid

egi

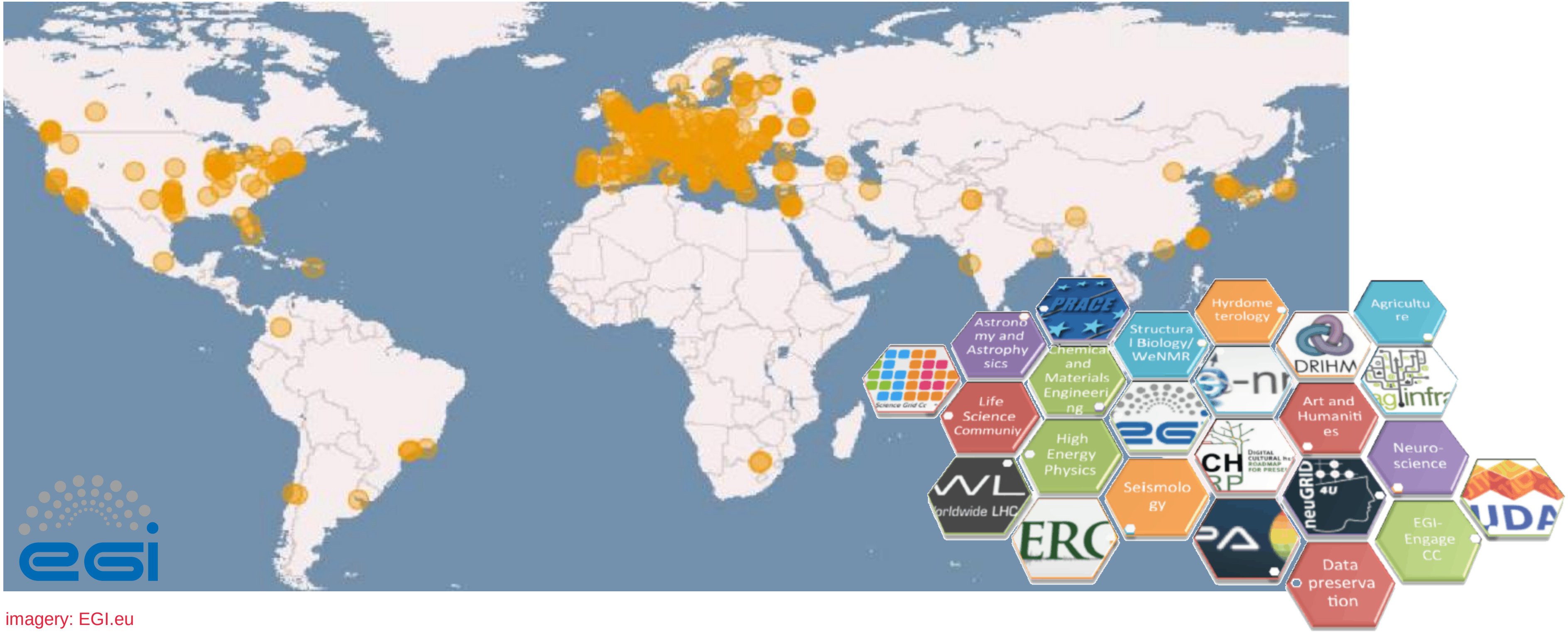
XSEDE
Extreme Science and Engineering Discovery Environment

- ❑ CPU: ~ 350,000 modern rekenkernen
- ❑ Disk 310 PB
- ❑ Tape 390 PB



Running jobs: 441353
Active CPU cores: 630003
Transfer rate: 35.32 GiB/sec

E-INFRASTRUCTURES: EGI, EUDAT, GEANT, PRACE, …

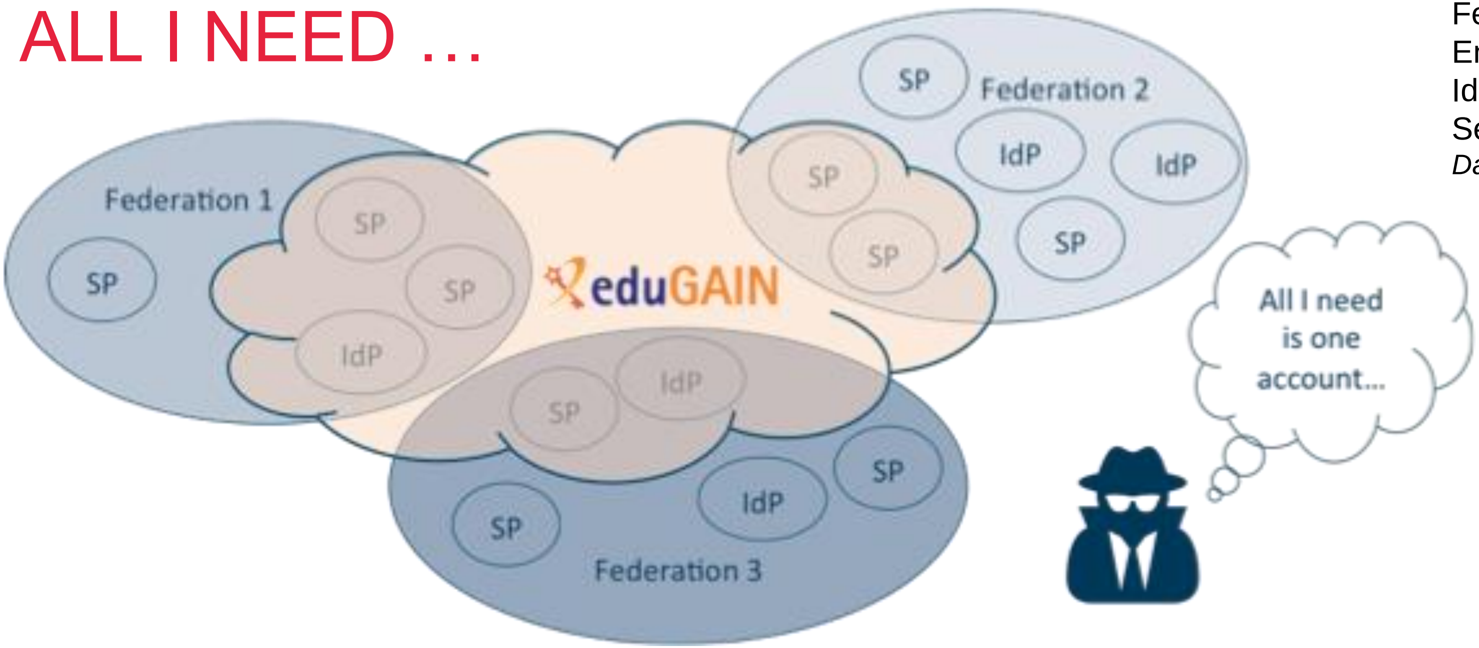


imagery: EGI.eu

ALL I NEED …

eduGAIN statistics	
Federations	59
Entities	5284
Identity providers	2965
Service providers	2319

Data: edugain.org, January 2019



A loose federation, but with some big advantages

- we see *more than just the network*
  incidents spread through the communities whose structure we already know
- recognized need and willingness to *collaborate and share data*

Imagery by GEANT and Hannah Short, CERN

TRUST AND GLOBAL POLICY

E-INFRASTRUCTURES:
MAKING EUROPE THE BEST PLACE
FOR RESEARCH AND INNOVATION
SECURITY FOR COLLABORATING INFRASTRUCTURES
security

A single policy cannot apply

- different risk scenarios for participants,
- different risk appreciation,
- distinct legal contexts, …

But one can 'map' policies and align policy structures

> *"enable interoperation of collaborating Infrastructures in managing cross-infrastructure operational security risks."*

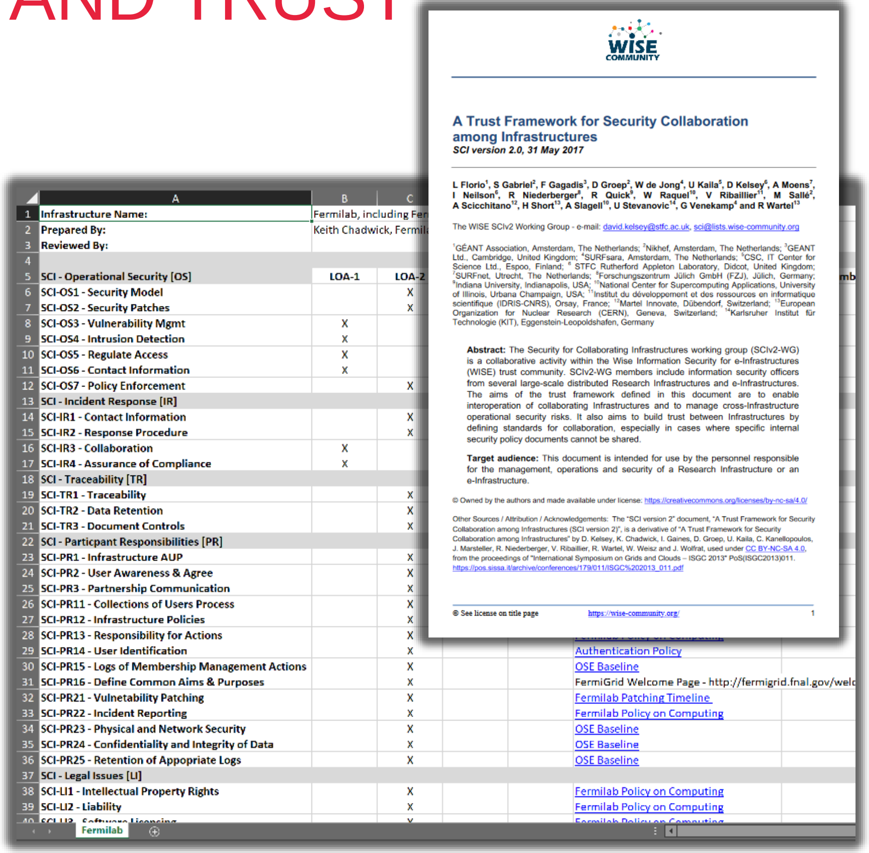
which is the role of **SCI**: Security for Collaboration among Infrastructures

SCI V2 – PEER ASSESSMENT AND TRUST

Interoperation areas

- Operational Security
- Incident Response
- Traceability
- Participant Responsibilities
- Individual users
- Collections of users (communities)
- Service providers
- Data Protection

Alongside: assessment maturity model using **peer-reviewed self-assessment**



A Trust Framework for Security Collaboration among Infrastructures
SCI version 2.0, 31 May 2017

L Florio[1], S Gabriel[2], F Gagadis[3], D Groep[2], W de Jong[4], U Kaila[5], D Kelsey[6], A Moens[7], I Neilson[6], R Niederberger[8], R Quick[9], W Raquel[10], V Ribaillier[11], M Sallé[2], A Scicchitano[12], H Short[13], A Slagell[10], U Stevanovic[14], G Venekamp[4] and R Wartel[13]

The WISE SCIv2 Working Group - e-mail: david.kelsey@stfc.ac.uk, sci@lists.wise-community.org

[1]GÉANT Association, Amsterdam, The Netherlands; [2]Nikhef, Amsterdam, The Netherlands; [3]GEANT Ltd., Cambridge, United Kingdom; [4]SURFsara, Amsterdam, The Netherlands; [5]CSC, IT Center for Science Ltd., Espoo, Finland; [6] STFC Rutherford Appleton Laboratory, Didcot, United Kingdom; [7]SURFnet, Utrecht, The Netherlands; [8]Forschungszentrum Jülich GmbH (FZJ), Jülich, Germany; [9]Indiana University, Indianapolis, USA; [10]National Center for Supercomputing Applications, University of Illinois, Urbana Champaign, USA; [11]Institut du développement et des ressources en informatique scientifique (IDRIS-CNRS), Orsay, France; [12]Martel Innovate, Dübendorf, Switzerland; [13]European Organization for Nuclear Research (CERN), Geneva, Switzerland; [14]Karlsruher Institut für Technologie (KIT), Eggenstein-Leopoldshafen, Germany

Abstract: The Security for Collaborating Infrastructures working group (SCIv2-WG) is a collaborative activity within the Wise Information Security for e-Infrastructures (WISE) trust community. SCIv2-WG members include information security officers from several large-scale distributed Research Infrastructures and e-Infrastructures. The aims of the trust framework defined in this document are to enable interoperation of collaborating Infrastructures and to manage cross-Infrastructure operational security risks. It also aims to build trust between Infrastructures by defining standards for collaboration, especially in cases where specific internal security policy documents cannot be shared.

Target audience: This document is intended for use by the personnel responsible for the management, operations and security of a Research Infrastructure or an e-Infrastructure.

© Owned by the authors and made available under license: https://creativecommons.org/licenses/by-nc-sa/4.0/

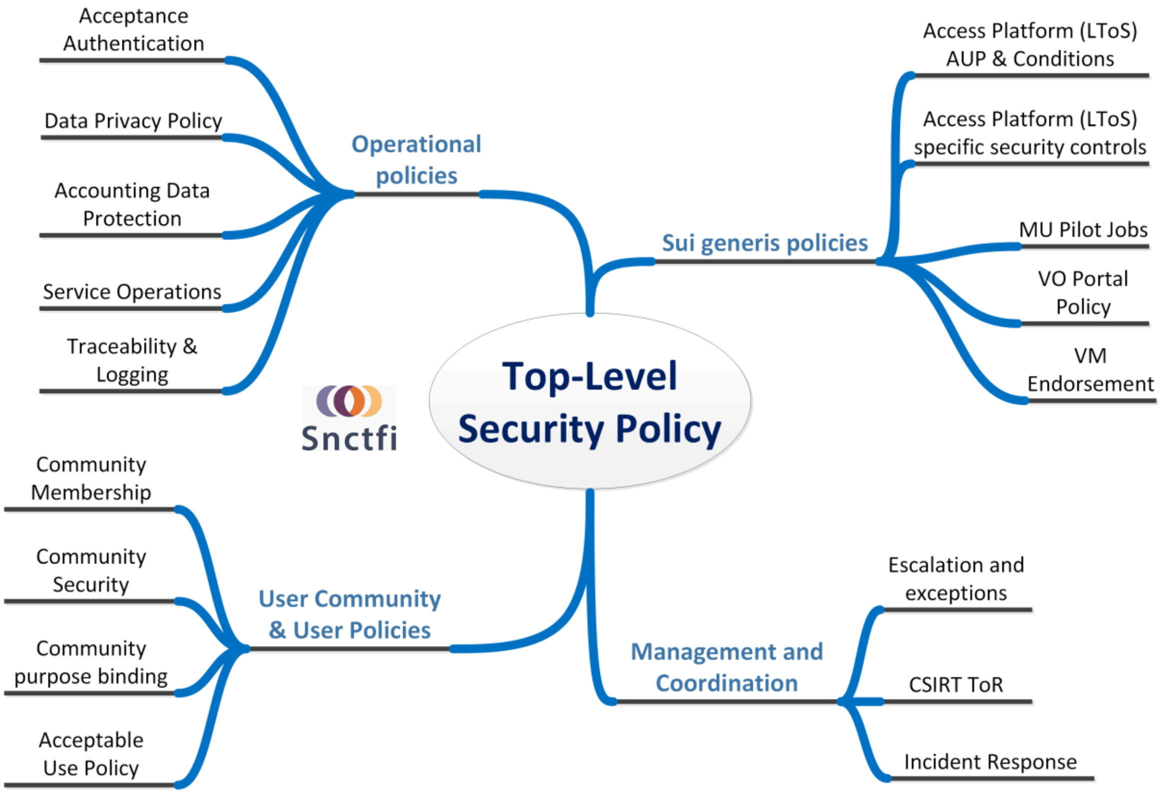
Other Sources / Attribution / Acknowledgements: The "SCI version 2" document, "A Trust Framework for Security Collaboration among Infrastructures (SCI version 2)", is a derivative of "A Trust Framework for Security Collaboration among Infrastructures" by D. Kelsey, K. Chadwick, I. Gaines, D. Groep, U. Kaila, C. Kanellopoulos, J. Marsteller, R. Niederberger, V. Ribaillier, R. Wartel, W. Weisz and J. Wolfrat, used under CC BY-NC-SA 4.0, from the proceedings of "International Symposium on Grids and Clouds – ISGC 2013" PoS(ISGC2013)011. https://pos.sissa.it/archive/conferences/179/011/ISGC%202013_011.pdf

© See license on title page https://wise-community.org/ 1

	A	B	C				
1	Infrastructure Name:	Fermilab, including Fer					
2	Prepared By:	Keith Chadwick, Fermila					
3	Reviewed By:						
4							
5	SCI - Operational Security [OS]	LOA-1	LOA-2				mb
6	SCI-OS1 - Security Model		X				
7	SCI-OS2 - Security Patches		X				
8	SCI-OS3 - Vulnerability Mgmt	X					
9	SCI-OS4 - Intrusion Detection	X					
10	SCI-OS5 - Regulate Access	X					
11	SCI-OS6 - Contact Information	X					
12	SCI-OS7 - Policy Enforcement		X				
13	SCI - Incident Response [IR]						
14	SCI-IR1 - Contact Information		X				
15	SCI-IR2 - Response Procedure		X				
16	SCI-IR3 - Collaboration	X					
17	SCI-IR4 - Assurance of Compliance	X					
18	SCI - Traceability [TR]						
19	SCI-TR1 - Traceability		X				
20	SCI-TR2 - Data Retention		X				
21	SCI-TR3 - Document Controls		X				
22	SCI - Particpant Responsibilities [PR]						
23	SCI-PR1 - Infrastructure AUP		X				
24	SCI-PR2 - User Awareness & Agree		X				
25	SCI-PR3 - Partnership Communication		X				
26	SCI-PR11 - Collections of Users Process		X				
27	SCI-PR12 - Infrastructure Policies		X				
28	SCI-PR13 - Responsibility for Actions		X			Fermilab Policy on Computing	
29	SCI-PR14 - User Identification		X			Authentication Policy	
30	SCI-PR15 - Logs of Membership Management Actions		X			OSE Baseline	
31	SCI-PR16 - Define Common Aims & Purposes		X			FermiGrid Welcome Page - http://fermigrid.fnal.gov/welc	
32	SCI-PR21 - Vulnetability Patching		X			Fermilab Patching Timeline	
33	SCI-PR22 - Incident Reporting		X			Fermilab Policy on Computing	
34	SCI-PR23 - Physical and Network Security		X			OSE Baseline	
35	SCI-PR24 - Confidentiality and Integrity of Data		X			OSE Baseline	
36	SCI-PR25 - Retention of Appopriate Logs		X			OSE Baseline	
37	SCI - Legal Issues [LI]						
38	SCI-LI1 - Intellectual Property Rights		X			Fermilab Policy on Computing	
39	SCI-LI2 - Liability		X			Fermilab Policy on Computing	
40	SCI-LI3 - Software Licensing		X			Fermilab Policy on Computing	

Fermilab

A POLICY STRUCTURE FOR EGI AND WLCG



Top-Level Security Policy

Operational policies

Acceptance Authentication

Data Privacy Policy

Accounting Data Protection

Service Operations

Traceability & Logging

Sui generis policies

Access Platform (LToS) AUP & Conditions

Access Platform (LToS) specific security controls

MU Pilot Jobs

VO Portal Policy

VM Endorsement

User Community & User Policies

Community Membership

Community Security

Community purpose binding

Acceptable Use Policy

Management and Coordination

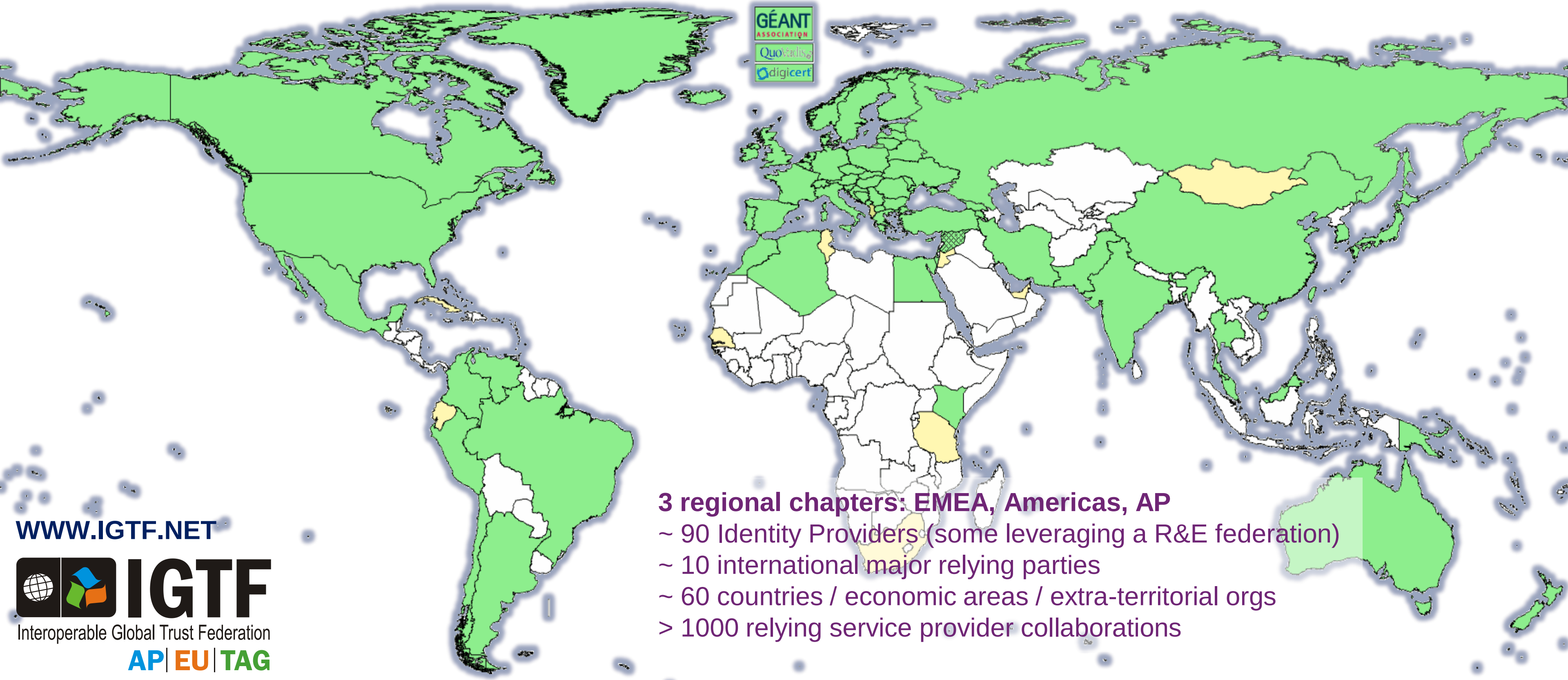
Escalation and exceptions

CSIRT ToR

Incident Response

Snctfi

INTEROPERABLE GLOBAL TRUST FEDERATION IGTF



3 regional chapters: EMEA, Americas, AP

~ 90 Identity Providers (some leveraging a R&E federation)

~ 10 international major relying parties

~ 60 countries / economic areas / extra-territorial orgs

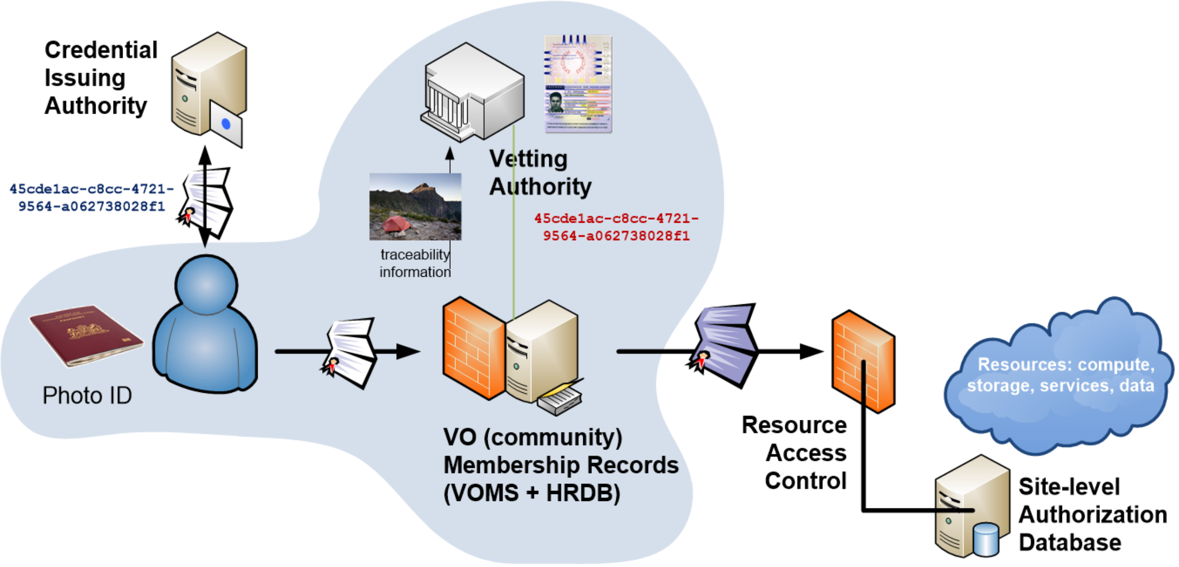
> 1000 relying service provider collaborations

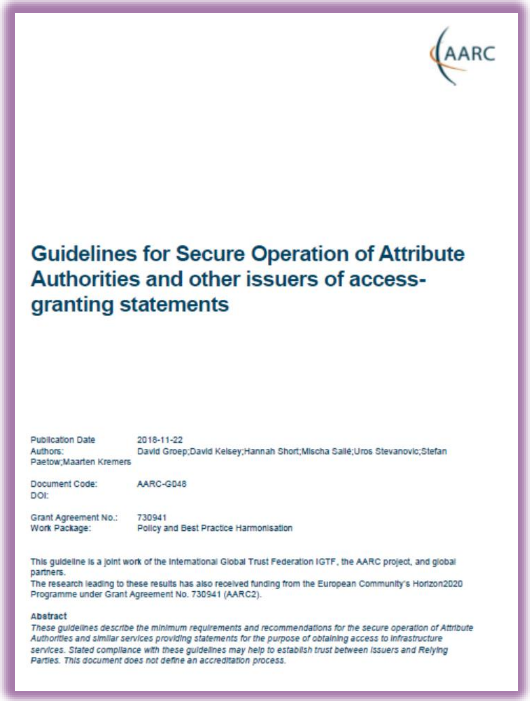
WWW.IGTF.NET

IGTF
Interoperable Global Trust Federation
AP | EU | TAG

BEYOND *AUTHN*: COLLABORATIVE ASSURANCE

Assurance elements may come from distinct sources


Credential Issuing Authority
45cde1ac-c8cc-4721-9564-a062738028f1
Vetting Authority
traceability information
45cde1ac-c8cc-4721-9564-a062738028f1
Photo ID
VO (community) Membership Records (VOMS + HRDB)
Resource Access Control
Resources: compute, storage, services, data
Site-level Authorization Database



AARC

Guidelines for Secure Operation of Attribute Authorities and other issuers of access-granting statements

Publication Date 2018-11-22
Authors: David Groep;David Kelsey;Hannah Short;Mischa Sallé;Uros Stevanovic;Stefan Paetow;Maarten Kremers

Document Code: AARC-G048
DOI:

Grant Agreement No.: 730941
Work Package: Policy and Best Practice Harmonisation

This guideline is a joint work of the International Global Trust Federation IGTF, the AARC project, and global partners.
The research leading to these results has also received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
These guidelines describe the minimum requirements and recommendations for the secure operation of Attribute Authorities and similar services providing statements for the purpose of obtaining access to infrastructure services. Stated compliance with these guidelines may help to establish trust between Issuers and Relying Parties. This document does not define an accreditation process.

Community Attribute Authority needs
operational security equivalent to an authentication source

COMMUNITIES TAKING RESPONSIBILITY

Communities and infrastructures thus hold a lot of (personal) data:

- this is personal data *resulting from use of the infrastructure*
- each of the communities (or infrastructure 'on their behalf') has legitimate interest in processing that data:
  resource allocation, accounting, communicating with members, &c
- each entity in the e-Infrastructure (and EOSC-HUB) is its own controller

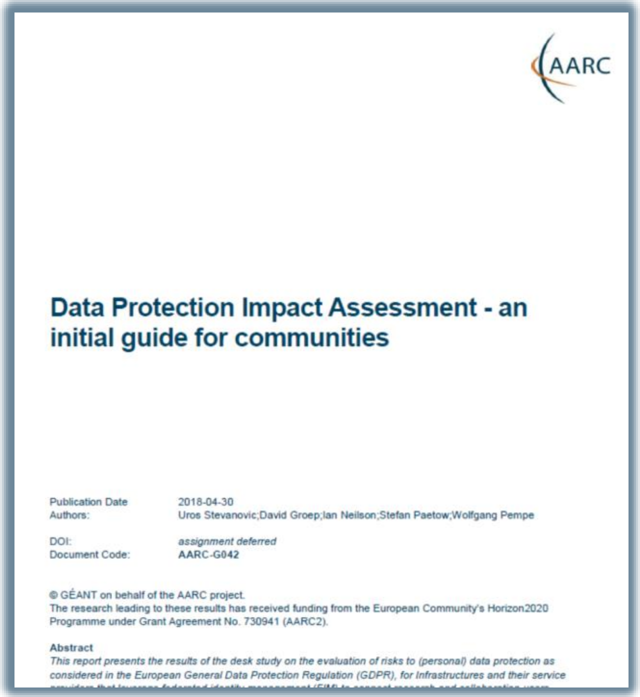
Adherence to common policy suite facilitates data sharing

- distributed incident response is explicitly allowed (and used) anyway
- facilitate global sharing through the Code of Conduct (art. 40)
- until EDBP is up to speed, we're essentially a 'BCR' like structure

DATA PROTECTION AND SHARING

Large discrepancy between practice, perception, and actual risk:

- communities themselves don’t see need to protect *infrastructure* AAI (accounting) data – tend to forego basic guidance
- misunderstanding issue, over-stating risk, falling victim to FUD law firms with “GDPR”
- even ‘simplified’ documents - like the GEANT Data Protection Code of Conduct – considered too complex to be understood



AARC

Data Protection Impact Assessment - an initial guide for communities

Publication Date 2018-04-30
Authors: Uros Stevanovic;David Groep;Ian Neilson;Stefan Paetow;Wolfgang Pempe

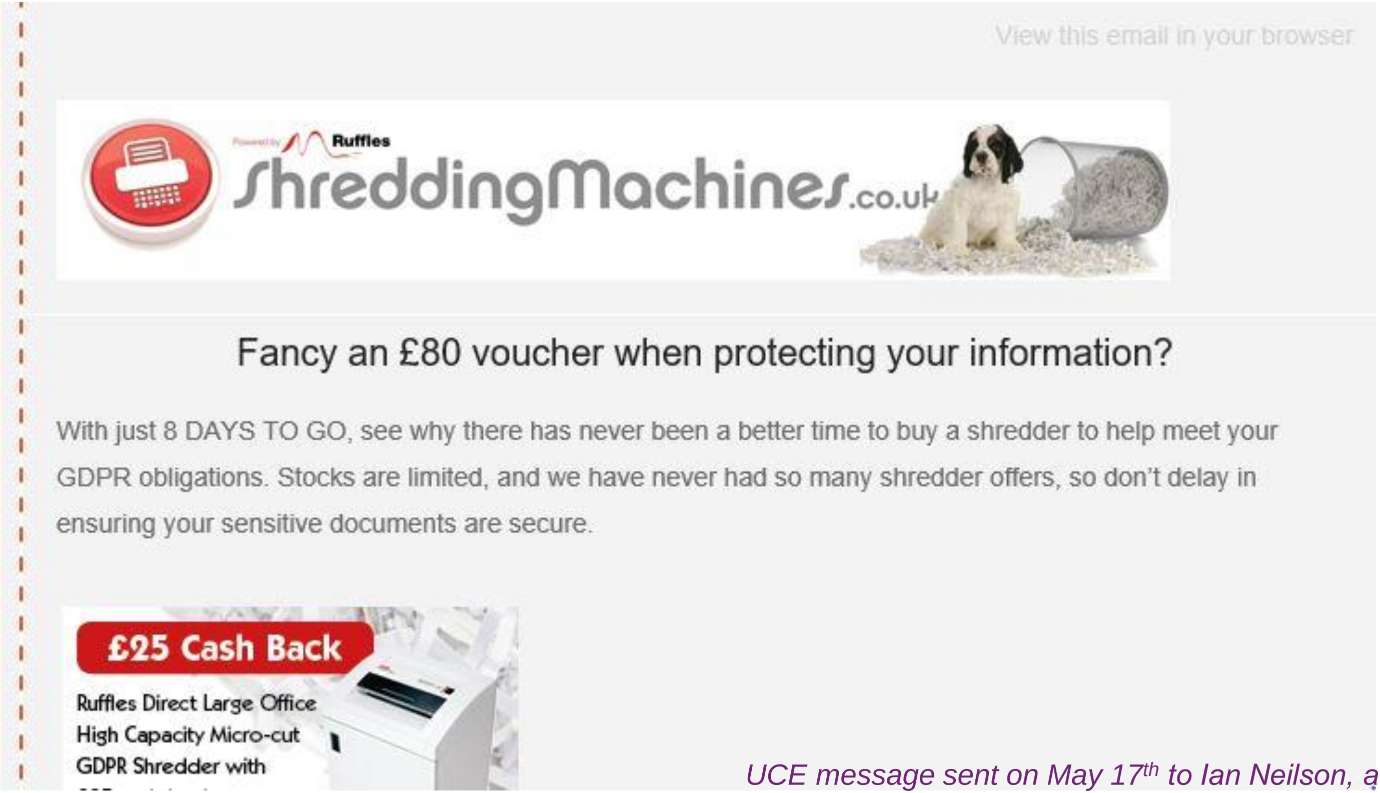
DOI: *assignment deferred*
Document Code: **AARC-G042**

© GÉANT on behalf of the AARC project.
The research leading to these results has received funding from the European Community's Horizon2020 Programme under Grant Agreement No. 730941 (AARC2).

Abstract
This report presents the results of the desk study on the evaluation of risks to (personal) data protection as considered in the European General Data Protection Regulation (GDPR), for Infrastructures and their service

https://aarc-project.eu/guidelines/aarc-g042/

THIS IS ONE SOLUTION …



View this email in your browser

Fancy an £80 voucher when protecting your information?

With just 8 DAYS TO GO, see why there has never been a better time to buy a shredder to help meet your GDPR obligations. Stocks are limited, and we have never had so many shredder offers, so don't delay in ensuring your sensitive documents are secure.

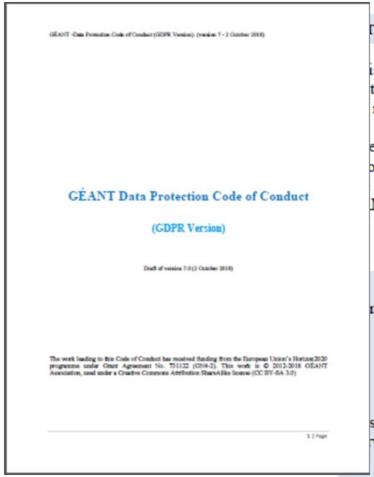
£25 Cash Back

Ruffles Direct Large Office
High Capacity Micro-cut
GDPR Shredder with

UCE message sent on May 17th to Ian Neilson, and millions more …

MODELS FOR DATA PROTECTION FOR FEDERATION

- BCR-like: put in place a set of policies that bind all participants (“SCI”)
- Code of Conduct



GÉANT -Data Protection Code of Conduct (GDPR Version). (version 7 - 2 October 2018)

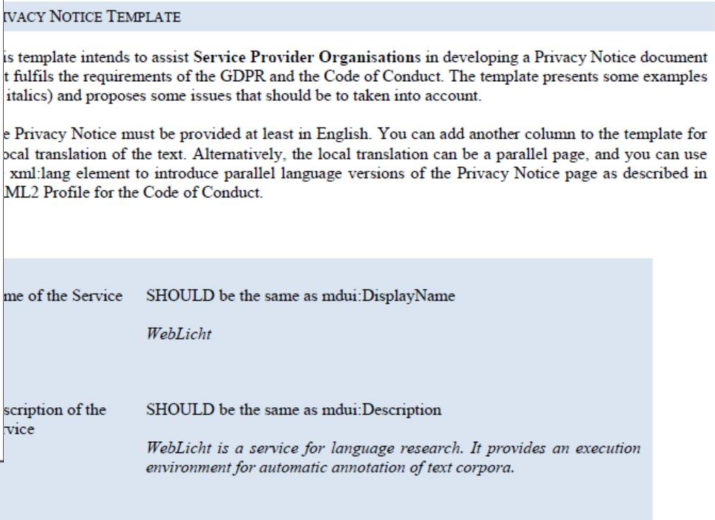
GÉANT Data Protection Code of Conduct

(GDPR Version)

Draft of version 7.0 (2 October 2018)

The work leading to this Code of Conduct has received funding from the European Union's Horizon2020 programme under Grant Agreement No. 731122 (GN4-2). This work is © 2012-2018 GÉANT Association, used under a Creative Commons Attribution ShareAlike license (CC BY-SA 3.0)

1 | Page

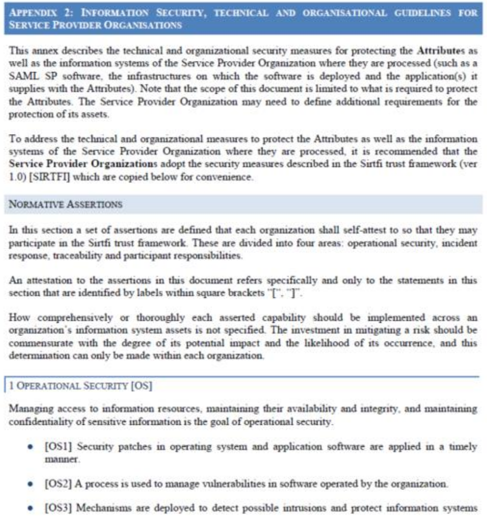


IVACY NOTICE TEMPLATE

is template intends to assist **Service Provider Organisations** in developing a Privacy Notice document t fulfils the requirements of the GDPR and the Code of Conduct. The template presents some examples italics) and proposes some issues that should be to taken into account.

e Privacy Notice must be provided at least in English. You can add another column to the template for ocal translation of the text. Alternatively, the local translation can be a parallel page, and you can use xml:lang element to introduce parallel language versions of the Privacy Notice page as described in ML2 Profile for the Code of Conduct.

me of the Service	SHOULD be the same as mdui:DisplayName *WebLicht*
scription of the vice	SHOULD be the same as mdui:Description *WebLicht is a service for language research. It provides an execution environment for automatic annotation of text corpora.*



APPENDIX 2: INFORMATION SECURITY, TECHNICAL AND ORGANISATIONAL GUIDELINES FOR SERVICE PROVIDER ORGANISATIONS

This annex describes the technical and organizational security measures for protecting the **Attributes** as well as the information systems of the Service Provider Organization where they are processed (such as a SAML SP software, the infrastructures on which the software is deployed and the application(s) it supplies with the Attributes). Note that the scope of this document is limited to what is required to protect the Attributes. The Service Provider Organization may need to define additional requirements for the protection of its assets.

To address the technical and organizational measures to protect the Attributes as well as the information systems of the Service Provider Organization where they are processed, it is recommended that the **Service Provider Organizations** adopt the security measures described in the Sirtfi trust framework (ver 1.0) [SIRTFI] which are copied below for convenience.

NORMATIVE ASSERTIONS

In this section a set of assertions are defined that each organization shall self-attest to so that they may participate in the Sirtfi trust framework. These are divided into four areas: operational security, incident response, traceability and participant responsibilities.

An attestation to the assertions in this document refers specifically and only to the statements in this section that are identified by labels within square brackets "[", "]".

How comprehensively or thoroughly each asserted capability should be implemented across an organization's information system assets is not specified. The investment in mitigating a risk should be commensurate with the degree of its potential impact and the likelihood of its occurrence, and this determination can only be made within each organization.

1 OPERATIONAL SECURITY [OS]

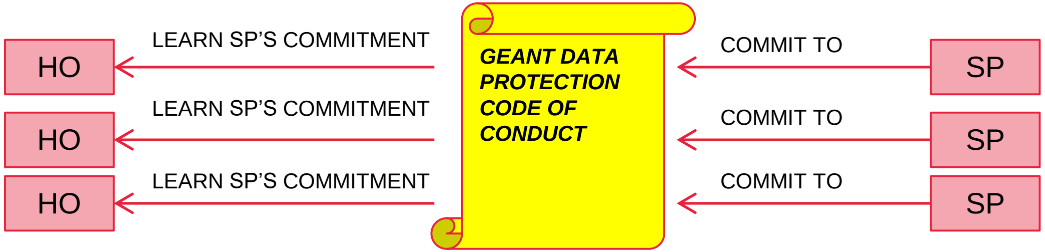
Managing access to information resources, maintaining their availability and integrity, and maintaining confidentiality of sensitive information is the goal of operational security.

- [OS1] Security patches in operating system and application software are applied in a timely manner.
- [OS2] A process is used to manage vulnerabilities in software operated by the organization.
- [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems

- ‘model clauses’ and contracts do not scale and thus don’t work

GEANT DATA PROTECTION CODE OF CONDUCT V2

Works admirably for our distributed infrastructure



Géant Data Protection Code of Conduct (GDPR Version) (2nd draft for consultation of version 2 - 29 January 2018)

GÉANT Data Protection Code of Conduct

(GDPR Version)

2nd draft for consultation of version 2.0 (29 January 2018)

The work leading to this Code of Conduct has received funding from the European Community's Horizon2020 programme under Grant Agreement No. 731122 (GN4-2). This work is © 2012-2018 GÉANT Ltd. used under a Creative Commons Attribution ShareAlike license (CC BY-SA 3.0)

1 | Page

- must be specific (can do that: it even includes Sirtfi!)
- applies for global transfers (great!)
- must be approved by a DPA (EDPB can't do it yet)
- needs a monitoring body (a challenge for us)

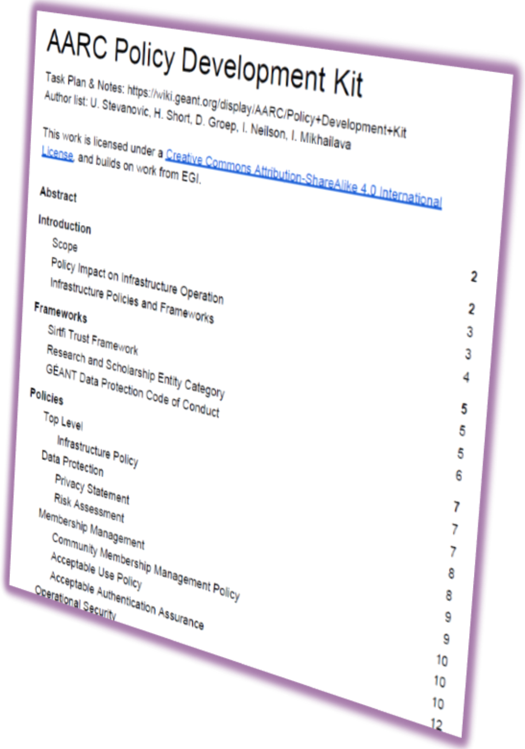
https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project

GEANT4-2 work by Mikael Linden, CSC and by Patrick van Eecke, UAntwerpen & DLA Piper

POLICY DEVELOPMENT KIT

Supporting our communities in joining the federation

- shows best examples from the e-Infrastructures
- comprehensive coverage
- enables *Sirtfi* and *Snctfi* compatibility
- includes a self-paced training module



AARC Policy Development Kit

Task Plan & Notes: https://wiki.geant.org/display/AARC/Policy+Development+Kit
Author list: U. Stevanovic, H. Short, D. Groep, I. Neilson, I. Mikhailava

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License, and builds on work from EGI.

IMPLEMENTING IT: RESOURCE & SERVICE ACCESS

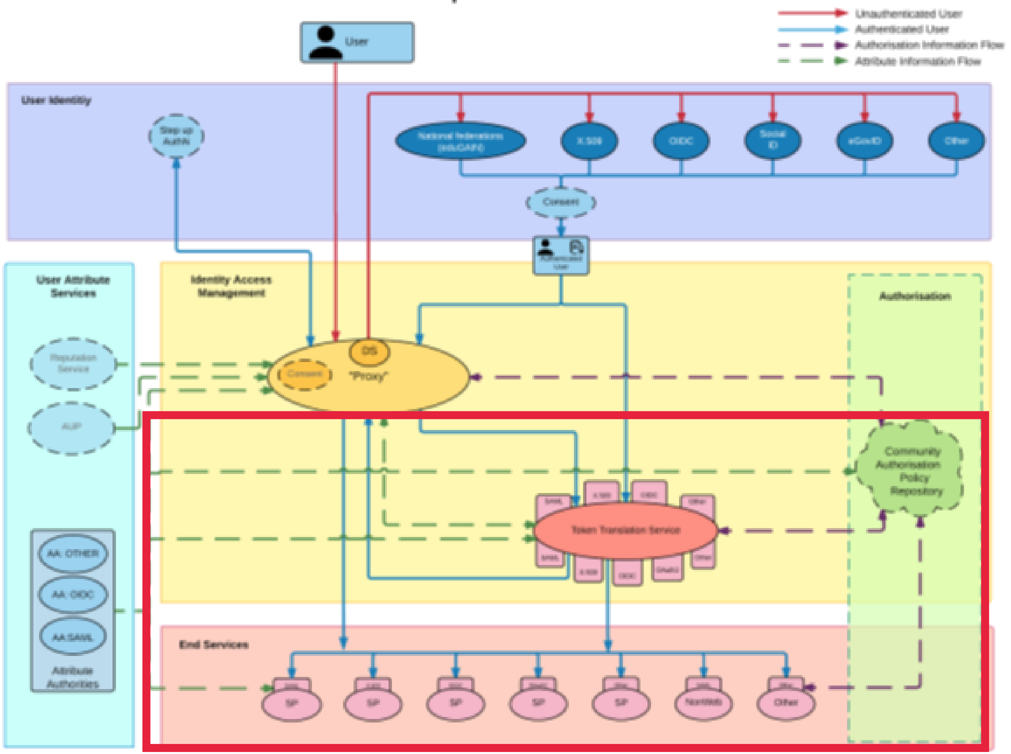
Site Access Control

Delegation and support for secure brokering: OAuth2 and RFC3820
Traceability and Isolation

SaToSa proxies for communities & COManage

Distributed policy and Argus

AARC Blueprint Architecture



PROVISIONING PROXY: SSH & OPENSTACK

Proxy Membership Management service

- pre-provisioning of account
- access rights linked to groups and roles

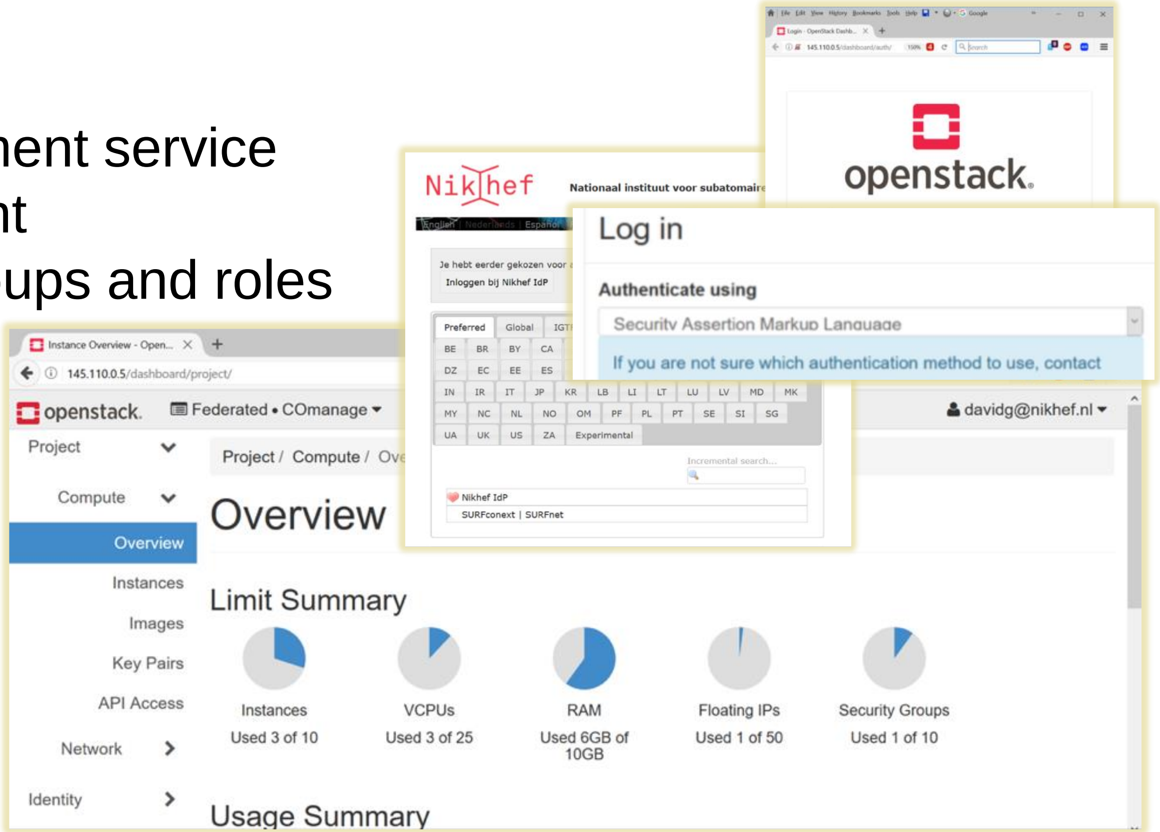
At Nikhef *COmanage*

- ssh via LDAP
- OpenStack
- …

and *VOMS*

- unix, batch, web portals

co-development with the AARC project



Login - OpenStack Dashb...

145.110.0.5/dashboard/auth/

Nationaal instituut voor subatomaire

Je hebt eerder gekozen voor

Inloggen bij Nikhef IdP

Incremental search...

Nikhef IdP

SURFconext | SURFnet

Log in

Authenticate using

Security Assertion Markup Language

If you are not sure which authentication method to use, contact

Instance Overview - Open...

145.110.0.5/dashboard/project/

Federated • COmanage

davidg@nikhef.nl

Project / Compute / Ove

Overview

Limit Summary

Instances: Used 3 of 10

VCPUs: Used 3 of 25

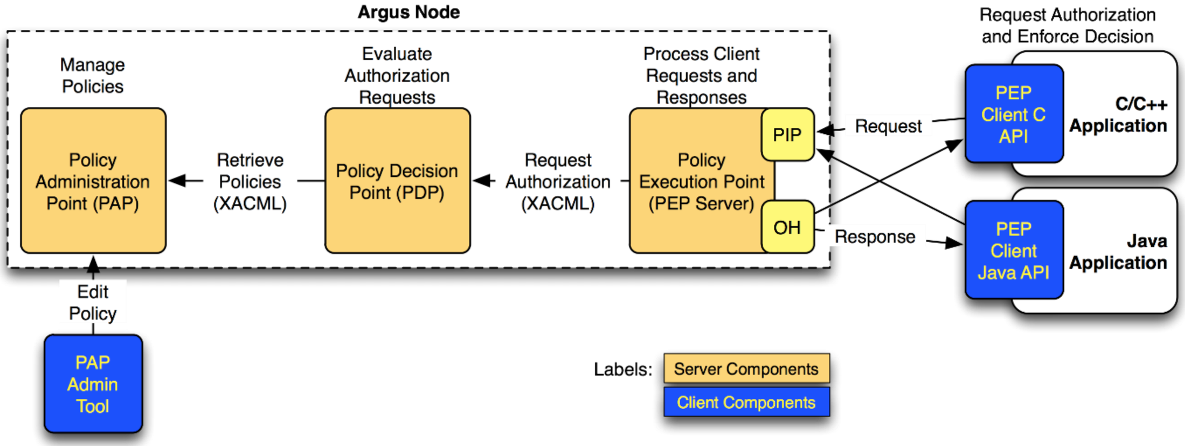
RAM: Used 6GB of 10GB

Floating IPs: Used 1 of 50

Security Groups: Used 1 of 10

Usage Summary

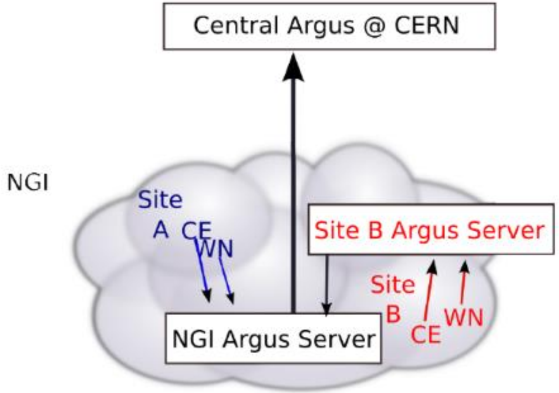
FEDERATED AUTHORISATION: LOCAL AND GLOBAL



Argus Node
Manage Policies
Policy Administration Point (PAP)
Retrieve Policies (XACML)
Evaluate Authorization Requests
Policy Decision Point (PDP)
Request Authorization (XACML)
Process Client Requests and Responses
Policy Execution Point (PEP Server)
PIP
OH
Request
Response
Request Authorization and Enforce Decision
PEP Client C API
C/C++ Application
PEP Client Java API
Java Application
Edit Policy
PAP Admin Tool
Labels:
Server Components
Client Components

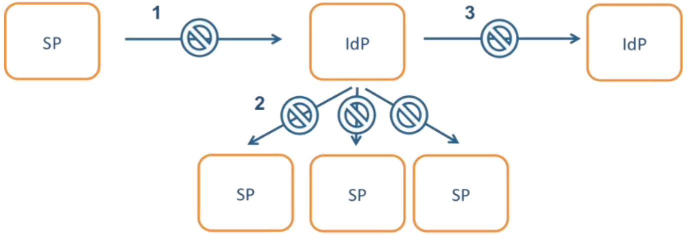
Hierarchical distributed policy

- chaining
  Policy Adminstration Points
- service-local
  Policy Information Points and obligation handling
  (“*you shall be ua1242*”,
  “*you shall have role dept_mngr*”)



https://github.com/argus-authz
https://argus-documentation.readthedocs.io/

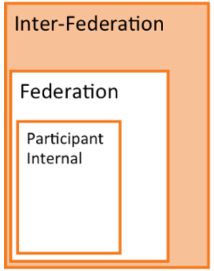
MANY PARTIES, SHARED SECURITY CHALLENGES

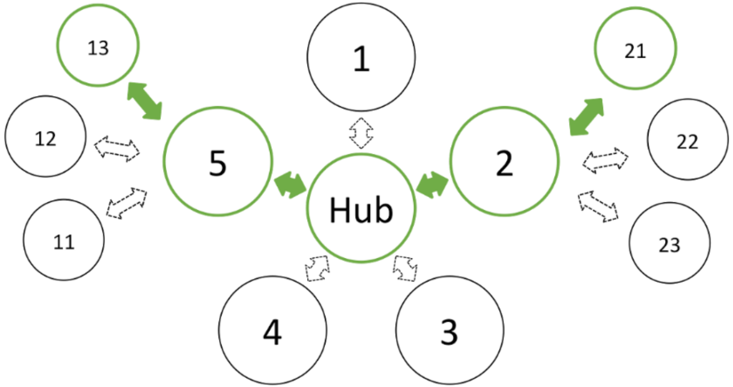


Incident Response Communication, communication blocks

Challenges

- IdP appears outside the service’s security mandate
- Lack of contact or lack of trust in the IdP which to the SP is an unknown party
- IdP **fails to inform other affected** SPs, for fear of leaking data, of reputation, or just lack of interest and knowledge
- No established channels of communication, esp. not to federations themselves!





Inter-Federation Incident Response Communication

EXERCISES – COMMUNICATIONS AND ACTIONS

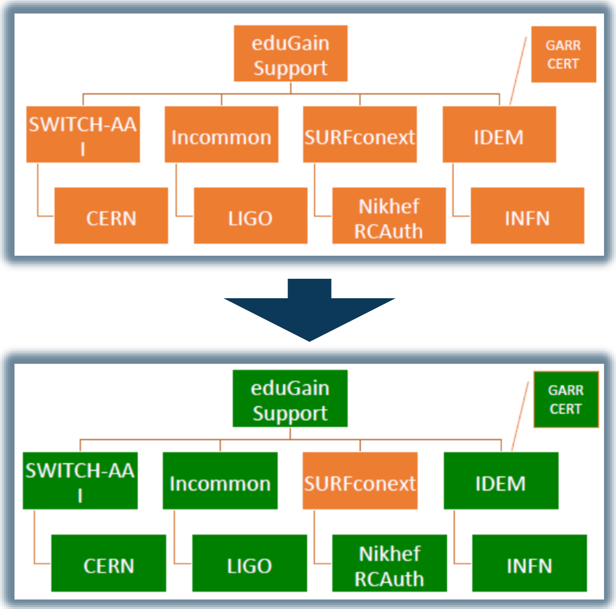
Nikhef
RCAuth
INFN User
INFN IdP
LIGO Wiki &
CERN
Market
CERN

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.

SIRTFI

Security Incident Response Trust Framework for Federated Identity

parties involved in response challenge



eduGain Support

GARR CERT

SWITCH-AAI

Incommon

SURFconext

IDEM

CERN

LIGO

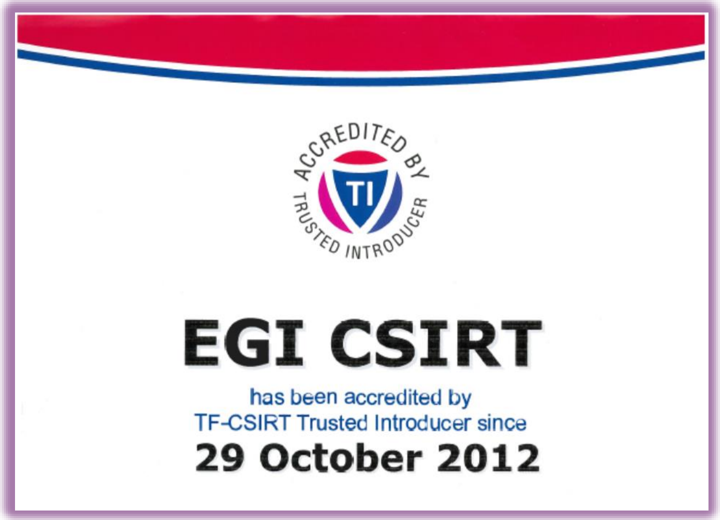
Nikhef RCAuth

INFN

EGI CSIRT CAPABILITIES – NIKHEF OPSEC TEAM

Nikhef provides the Security Officer for EGI

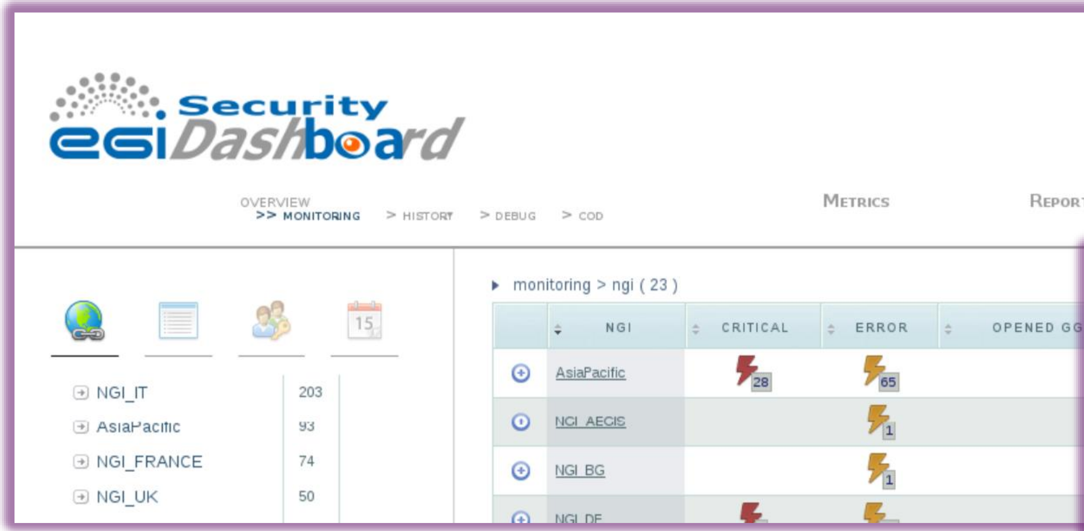
- vulnerability mitigation monitoring
- training and communications
- traceability exercises
  (“*Security Service Challenges*”)
- incident handling
- emergency suspensions of service providers
- liaison with industry trust groups:
  TF-CSIRT/TI, FIRST, OPS-T, …


ACCREDITED BY
TI
TRUSTED INTRODUCER

EGI CSIRT

has been accredited by
TF-CSIRT Trusted Introducer since
29 October 2012

VULNERABILITY MITIGATION IN EGI AND WLCG

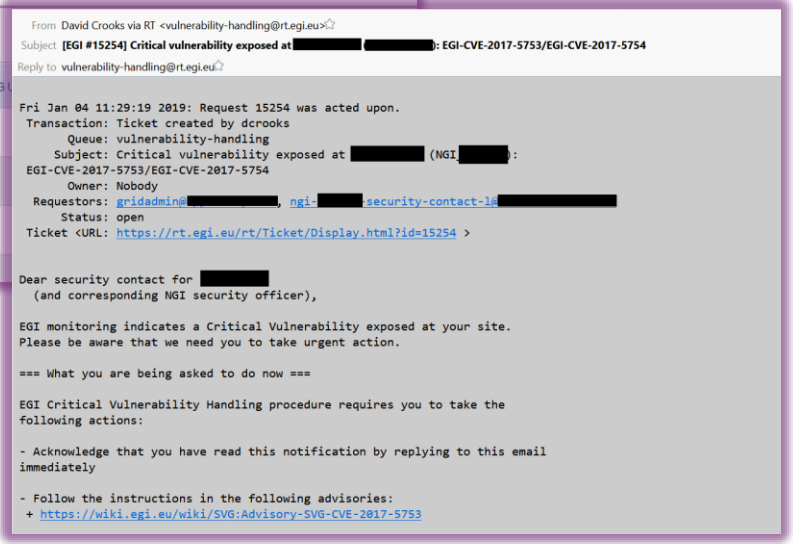


We come **Leif Nixon leini58@liu.se**

NGI_IT	203
AsiaPacific	93
NGI_FRANCE	74
NGI_UK	50

monitoring > ngi (23)

	NGI	CRITICAL	ERROR	OPENED GGU
⊕	AsiaPacific	28	65	
⊕	NGI_AEGIS		1	
⊕	NGI_BG		1	
⊕	NGI_DE			



From David Crooks via RT <vulnerability-handling@rt.egi.eu>

Subject **[EGI #15254] Critical vulnerability exposed at [redacted] ([redacted]): EGI-CVE-2017-5753/EGI-CVE-2017-5754**

Reply to vulnerability-handling@rt.egi.eu

```
Fri Jan 04 11:29:19 2019: Request 15254 was acted upon.
 Transaction: Ticket created by dcrooks
       Queue: vulnerability-handling
     Subject: Critical vulnerability exposed at [redacted] (NGI_[redacted]):
 EGI-CVE-2017-5753/EGI-CVE-2017-5754
       Owner: Nobody
  Requestors: gridadmin@[redacted], ngi-[redacted]-security-contact-l@[redacted]
      Status: open
 Ticket <URL: https://rt.egi.eu/rt/Ticket/Display.html?id=15254 >


Dear security contact for [redacted]
  (and corresponding NGI security officer),

EGI monitoring indicates a Critical Vulnerability exposed at your site.
Please be aware that we need you to take urgent action.

=== What you are being asked to do now ===

EGI Critical Vulnerability Handling procedure requires you to take the
following actions:

- Acknowledge that you have read this notification by replying to this email
immediately

- Follow the instructions in the following advisories:
 + https://wiki.egi.eu/wiki/SVG:Advisory-SVG-CVE-2017-5753
```

- for consistent security in federation:
  policy allows continuous vulnerability monitoring
- monitoring data itself protected:
  access for service provider and CSIRT

Data: EGI-CSIRT

EGI CSIRT – INCIDENT RESPONSE

Typical incidents in the federated e-Infrastructure are the usual

- phished accounts
- jumping via compromised accounts and *ssh* keys
- weak credentials (even for service administrators ☹)
- **new**: insecure virtual appliances and bad orchestration scripts

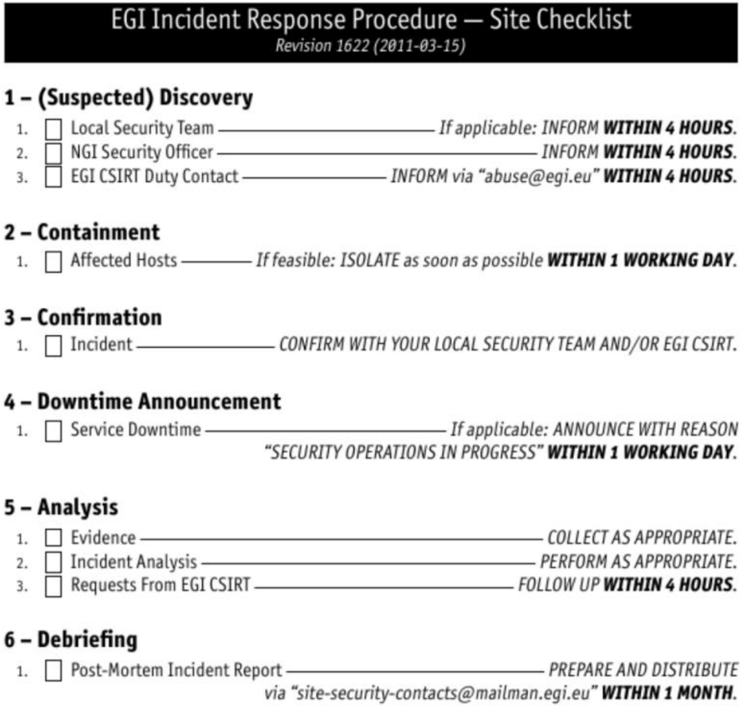
Miscreant activities

- mostly: cryptocurrency mining
  which we also see from legit users lacking a moral compass…
- a bit of spamming and DDoSing

SERVICE PROVIDER RESPONSE CHECKLIST

EGI CSIRT acts as expert-centre for service providers that lack local security expertise:

- standard processes & procedures
- communications templates
- advanced forensics



EGI Incident Response Procedure – Site Checklist

Revision 1622 (2011-03-15)

1 – (Suspected) Discovery

1. □ Local Security Team — *If applicable: INFORM **WITHIN 4 HOURS**.*
2. □ NGI Security Officer — *INFORM **WITHIN 4 HOURS**.*
3. □ EGI CSIRT Duty Contact — *INFORM via "abuse@egi.eu" **WITHIN 4 HOURS**.*

2 – Containment

1. □ Affected Hosts — *If feasible: ISOLATE as soon as possible **WITHIN 1 WORKING DAY**.*

3 – Confirmation

1. □ Incident — *CONFIRM WITH YOUR LOCAL SECURITY TEAM AND/OR EGI CSIRT.*

4 – Downtime Announcement

1. □ Service Downtime — *If applicable: ANNOUNCE WITH REASON "SECURITY OPERATIONS IN PROGRESS" **WITHIN 1 WORKING DAY**.*

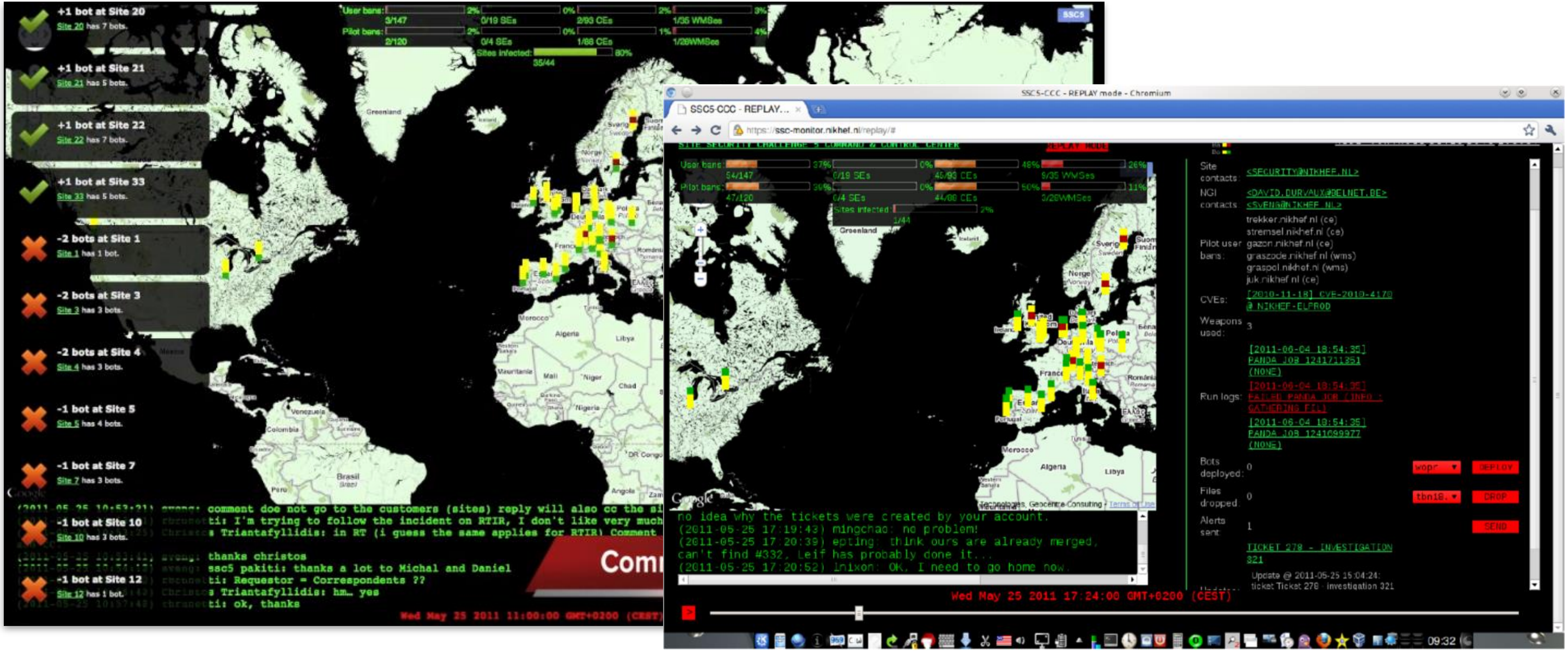
5 – Analysis

1. □ Evidence — *COLLECT AS APPROPRIATE.*
2. □ Incident Analysis — *PERFORM AS APPROPRIATE.*
3. □ Requests From EGI CSIRT — *FOLLOW UP **WITHIN 4 HOURS**.*

6 – Debriefing

1. □ Post-Mortem Incident Report — *PREPARE AND DISTRIBUTE via "site-security-contacts@mailman.egi.eu" **WITHIN 1 MONTH**.*

SSC MONITORING



+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.

```
User bans:  2%      0%        2%        3%
  3/147     0/19 SEs  2/93 CEs  1/35 WMSes
Pilot bans: 2%      0%        1%        4%
  2/120     0/4 SEs   1/88 CEs  1/28WMSes
Sites infected: 80%
  35/44
```

```
(2011-05-25 10:53:21) svengr: comment doe not go to the customers (sites) reply will also cc the si
                      ti: I'm trying to follow the incident on RTIR, I don't like very much
                      s Triantafyllidis: in RT (i guess the same applies for RTIR) Comment
(2011-05-25 10:53:41) svengr: thanks christos
(2011-05-25 10:54:12) svengr: ssc5 pakiti: thanks a lot to Michal and Daniel
                      ti: Requestor = Correspondents ??
                      s Triantafyllidis: hm… yes
(2011-05-25 10:57:42) ti: ok, thanks
Wed May 25 2011 11:00:00 GMT+0200 (CEST)
```

SSC5-CCC - REPLAY mode - Chromium

SSC5-CCC - REPLAY...

https://ssc-monitor.nikhef.nl/replay/#

SITE SECURITY CHALLENGE 5 COMMAND & CONTROL CENTER

REPLAY MODE

```
User bans:  37%     0%        48%        26%
  54/147    0/19 SEs  45/93 CEs  9/35 WMSes
Pilot bans: 39%     0%        50%        11%
  47/120    0/4 SEs   44/88 CEs  3/28WMSes
Sites infected: 2%
  1/44
```

```
no idea why the tickets were created by your account.
(2011-05-25 17:19:43) mingchao: no problem!
(2011-05-25 17:20:39) epting: think ours are already merged,
can't find #332, Leif has probably done it...
(2011-05-25 17:20:52) lnixon: OK, I need to go home now.
Wed May 25 2011 17:24:00 GMT+0200 (CEST)
```

Site contacts: <SECURITY@NIKHEF.NL>

NGI contacts: <DAVID.DURVAUX@BELNET.BE> <SVENG@NIKHEF.NL>

Pilot user bans: trekker.nikhef.nl (ce)
stremsel.nikhef.nl (ce)
gazon.nikhef.nl (ce)
graszode.nikhef.nl (wms)
graspol.nikhef.nl (wms)
juk.nikhef.nl (ce)

CVEs: [2010-11-18] CVE-2010-4170 @ NIKHEF-ELPROD

Weapons used: 3

Run logs: [2011-06-04 18:54:35] PANDA JOB 1241711351 (NONE)
[2011-06-04 18:54:35] FAILED PANDA JOB (INFO : GATHERING FIL)
[2011-06-04 18:54:35] PANDA JOB 1241699977 (NONE)

Bots deployed: 0 wopr ▾ DEPLOY

Files dropped: 0 tbn18. ▾ DROP

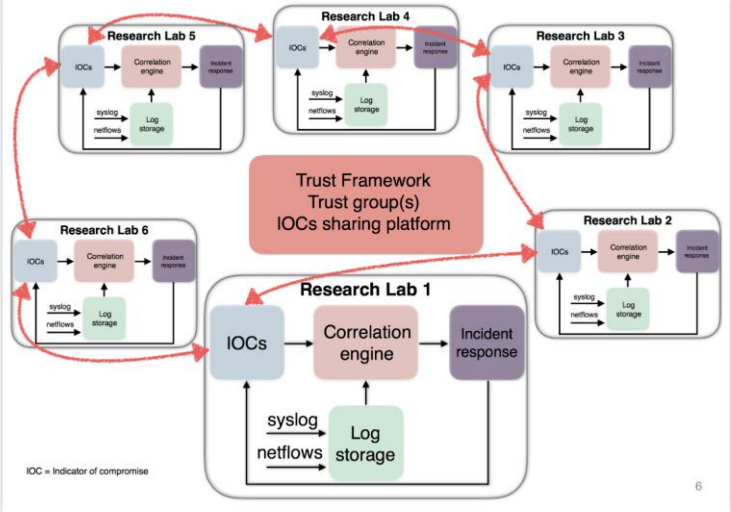
Alerts sent: 1 SEND

TICKET 278 - INVESTIGATION 321

Update @ 2011-05-25 15:04:24: ticket Ticket 278 - investigation 321

DATA SHARING IS ‘PART OF THE DEAL’

If good citizenship and preventing data leaks was no justification enough, GDPR recital 49 recognizes the CSIRT role explicitly



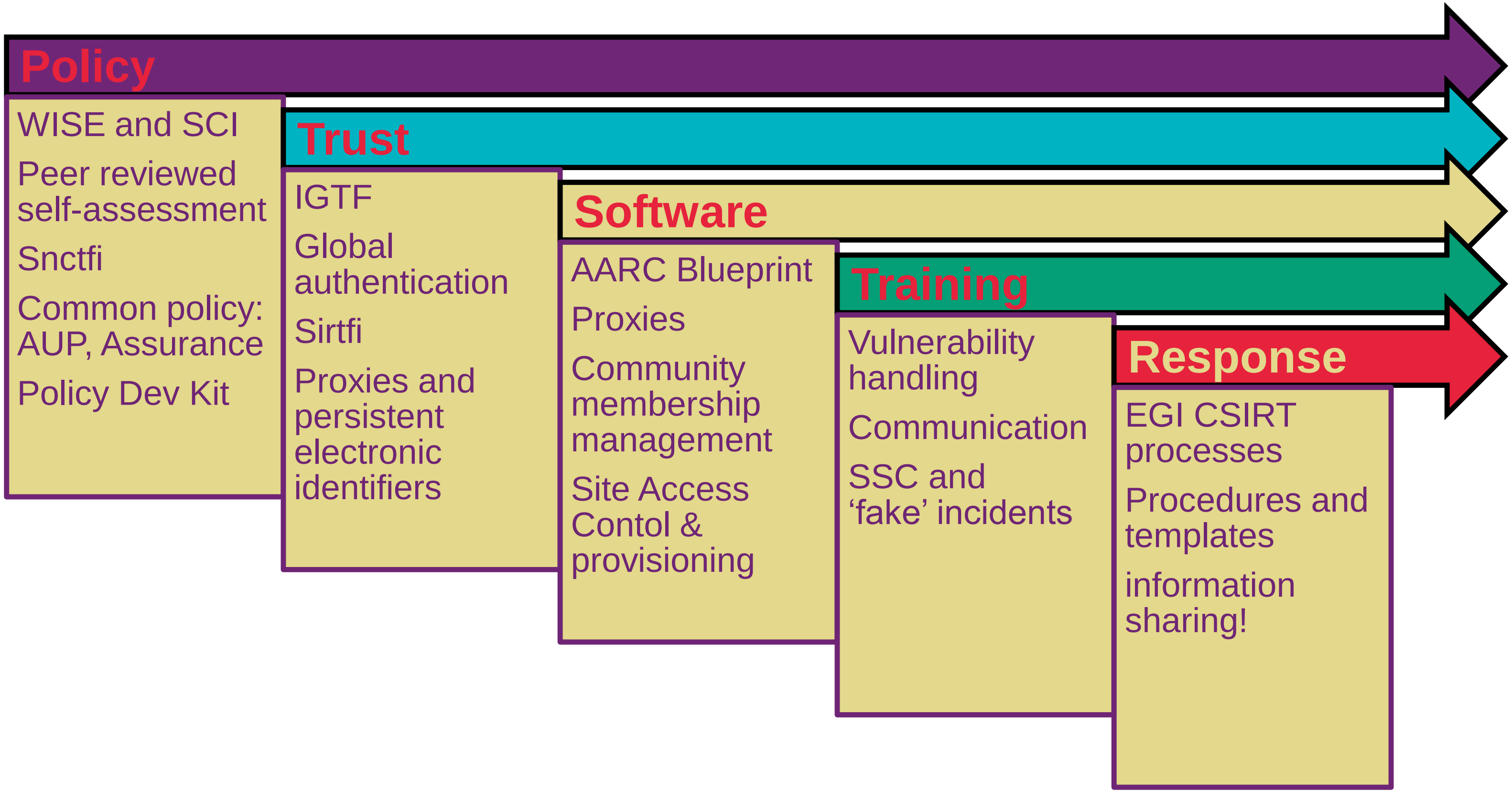
Legitimate interest 6.1(f) as usual basis
appropriate safeguards within EEA in place

For global sharing with trusted peers

- DP CoCo v2 (with Sirtfi embedded)
- an ‘SCI’ policy framework: very BCR-like
- NIS Directive (EU) 2016/1148 promotes it *despite some uncertainty under 49(1)§2’s need to inform the DPA post-hoc*
- SMEs not supposed to be burdened by BCR *EDBP Guidelines 2/2018 note 40:* suggests *compelling legitimate interest*

see e.g. Andrew Cormack in https://script-ed.org/article/incident-response-protecting-individual-rights-under-the-general-data-protection-regulation/

CLOSER TO A TRUSTED E-INFRASTRUCTURE



Policy

WISE and SCI

Peer reviewed self-assessment

Snctfi

Common policy: AUP, Assurance

Policy Dev Kit

Trust

IGTF

Global authentication

Sirtfi

Proxies and persistent electronic identifiers

Software

AARC Blueprint

Proxies

Community membership management

Site Access Contol & provisioning

Training

Vulnerability handling

Communication

SSC and ‘fake’ incidents

Response

EGI CSIRT processes

Procedures and templates

information sharing!

with special thanks to our (project) co-funders: **SURF** and the **European Commission** via H2020 for AARC/2, EOSC-HUB, GEANT4-3, ESCAPE, AENEAS, and their precursors DataGrid, EGEE, EMI, IGE, InSPIRE/ENGAGE; and our I4C peers: CERN, CESNET, EGI.eu , FZJ, GEANT, GRNET, KIT, RAL STFC, SURFsara, SURFnet

David Groep
davidg@nikhef.nl
https://www.nikhef.nl/~davidg/presentations/
https://orcid.org/0000-0003-1026-6606