



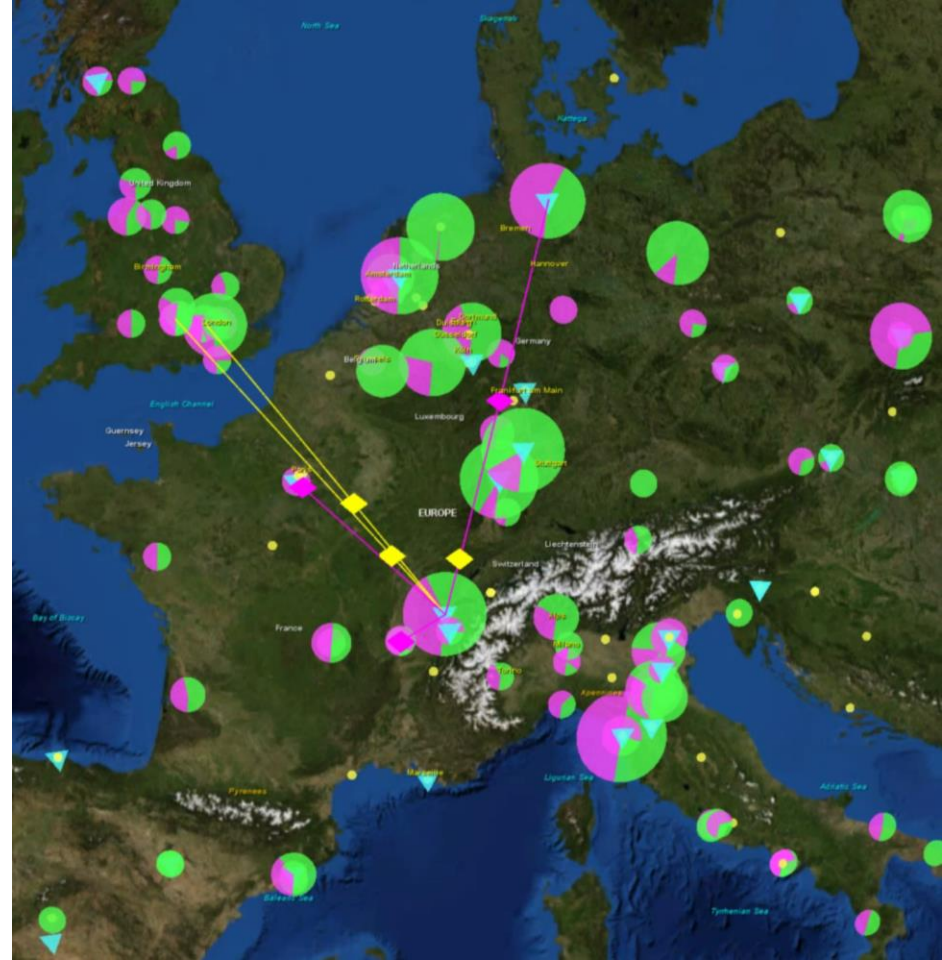
TRUST, SECURITY, AND OPERATIONS  
IN ICT INFRASTRUCTURES FOR RESEARCH  
AT THE NIKHEF PHYSICS DATA PROCESSING GROUP

# INFRASTRUCTURE FOR COLLABORATION

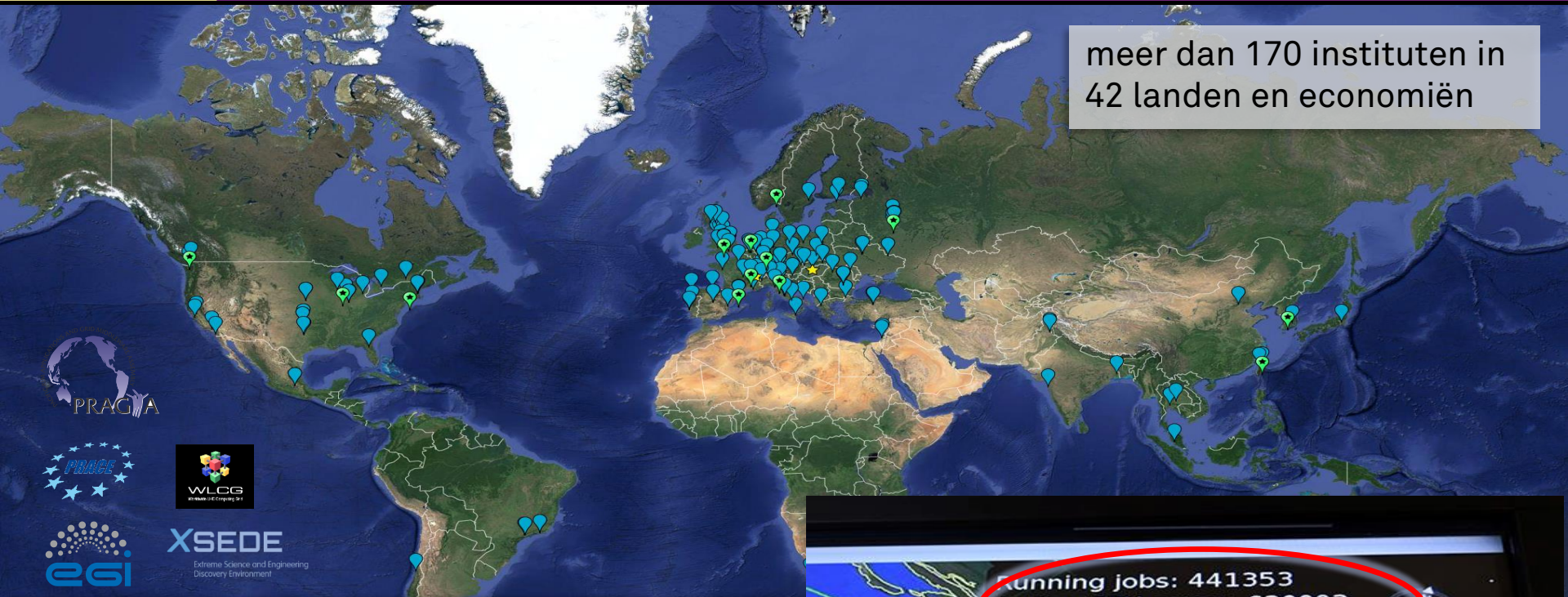
David Groep  
January 2019

# SECURITY: INFRASTRUCTURE FOR COLLABORATION

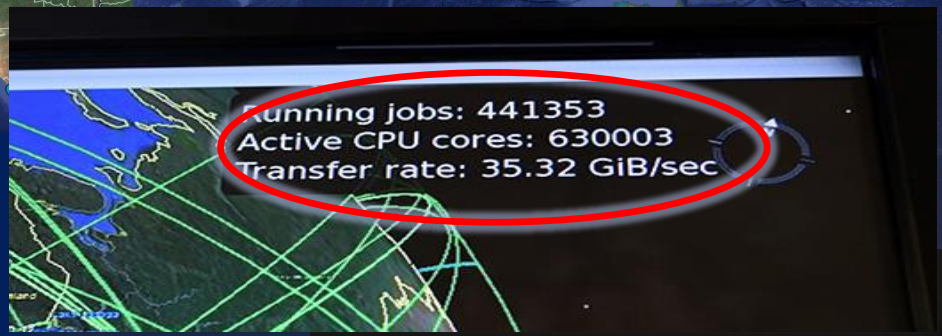
- global **policy** and best practice harmonization
- access control **middleware** for multi-domain services
- **operational security**: response and forensics
- **training** and communications



meer dan 170 instituten in  
42 landen en economiën

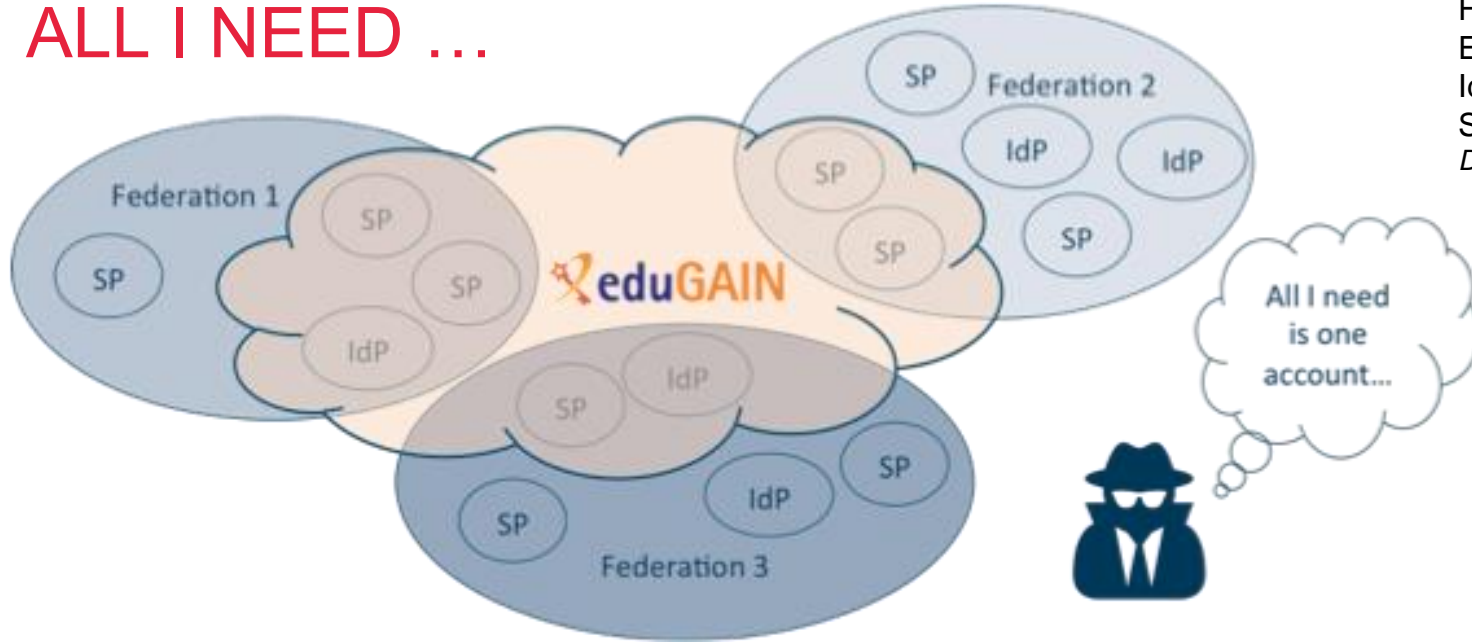


- CPU: ~ 350,000 modern rekenkernen
- Disk 310 PB
- Tape 390 PB





# ALL I NEED ...



## eduGAIN statistics

Federations	59
Entities	5284
Identity providers	2965
Service providers	2319

Data: [edugain.org](http://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

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

**WISE COMMUNITY**

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

L Florio<sup>1</sup>, S Gabriel<sup>2</sup>, F Gagadi<sup>3</sup>, D Groep<sup>4</sup>, W de Jong<sup>5</sup>, U Kalla<sup>6</sup>, D Kelsey<sup>7</sup>, A Moens<sup>8</sup>, I Neilson<sup>9</sup>, R Niederberger<sup>10</sup>, R Quick<sup>11</sup>, W Raquel<sup>12</sup>, V Ribaillier<sup>13</sup>, M Salle<sup>14</sup>, A Scicchitano<sup>15</sup>, H Short<sup>16</sup>, A Stajgel<sup>17</sup>, U Stevanovic<sup>18</sup>, G Venekamp<sup>19</sup> and R Warte<sup>20</sup>

The WISE SCIv2 Working Group - e-mail: [david.kelsey@efc.ac.uk](mailto:david.kelsey@efc.ac.uk), [sci@lists.wise-community.org](mailto:sci@lists.wise-community.org)

**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.

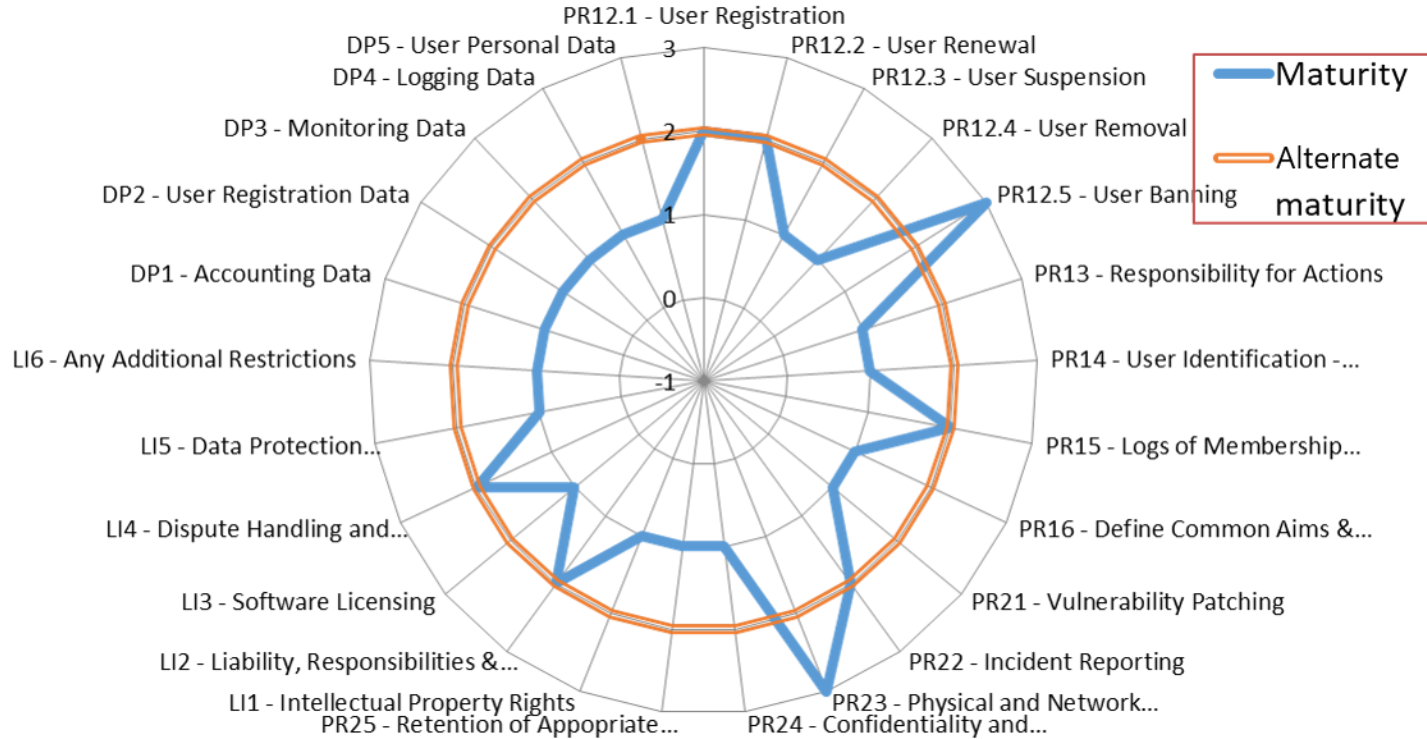
© Owned by the authors and made available under license: <https://creativecommons.org/licenses/by-nc-sa/4.0/>

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, L. Garret, D. Groep, U. Kalla, C. Karielopoulos, J. Mandel, R. Niederberger, V. Raquel, R. Warte, W. Weisz and J. Wolff, used under CC BY-NC-SA 4.0 from the proceedings of "International Symposium on Grids and Clouds - ISGC 2017" PublISGC2017011. [https://doi.org/10.1007/978-3-319-52073-1\\_141](https://doi.org/10.1007/978-3-319-52073-1_141)

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

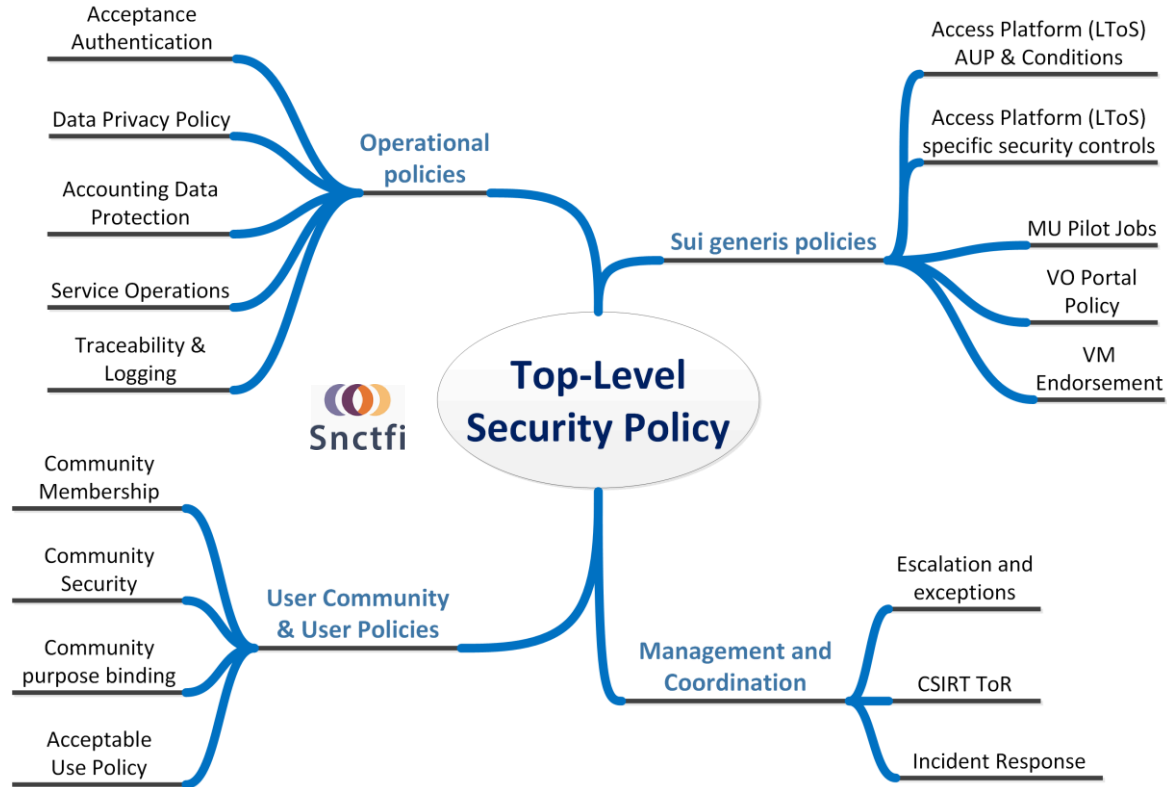
	A	B	C
1 Infrastructure Name:	Fermilab, including Fermi		
2 Prepared By:	Keith Chadwick, Fermi		
3 Reviewed By:			
4			
5 SCI - Operational Security [OS]	LOA-1	LOA-2	
6 SCI-OS1 - Security Model			X
7 SCI-OS2 - Security Patches			X
8 SCI-OS3 - Vulnerability Mgmt	X		X
9 SCI-OS4 - Intrusion Detection			X
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 - Participant 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
29 SCI-PR14 - User Identification			X
30 SCI-PR15 - Logs of Membership Management Actions			X
31 SCI-PR16 - Define Common Aims & Purposes			X
32 SCI-PR21 - Vulnerability Patching			X
33 SCI-PR22 - Incident Reporting			X
34 SCI-PR23 - Physical and Network Security			X
35 SCI-PR24 - Confidentiality and Integrity of Data			X
36 SCI-PR25 - Retention of Appropriate Logs			X
37 SCI - Legal Issues [LI]			
38 SCI-LI1 - Intellectual Property Rights			X
39 SCI-LI2 - Liability			X
40 SCI-LI3 - Confidentiality			X
41			

# EXAMPLE SCI ASSESSMENT





# A POLICY STRUCTURE FOR EGI AND WLCG





# Scaling Acceptable Use Policy and data release

impractical to present user 'click-through' screens on each individual service

Community specific terms & conditions

Community specific terms & conditions

Community conditions

RI Cluster-specific terms & conditions

## Common baseline AUP

### for e-Infrastructures and Research Communities

(current draft Baseline AUP –

leveraging comparison study and joint e-Infrastructure work)

AARC-I044

Implementers Guide to the WISE Baseline Acceptable Use Policy



### 3. The WISE Baseline AUP

The WISE Baseline AUP<sup>1</sup> in its preamble and final clauses, it given below. The blue text elements should be substituted on-line, whereas the green elements are optional and need to be filled on only when needed, e.g. based on the guidance in this document.

#### Acceptable Use Policy and Conditions of Use

This Acceptable Use Policy and Conditions of Use ("AUP") defines the rules and conditions that govern your access to and use (including transmission, processing, and storage of data) of the resources and services ("Services") as granted by (community, agency, or infrastructure name) for the purpose of (describe the stated goals and policies governing the intended use).

<To further define and limit what constitutes acceptable use, the community, agency, or infrastructure may optionally add additional information, rules or conditions, or references thereto, here or at the placeholder below. These additions must not conflict with the clauses 1-10 below, whose wording and numbering must not be changed->

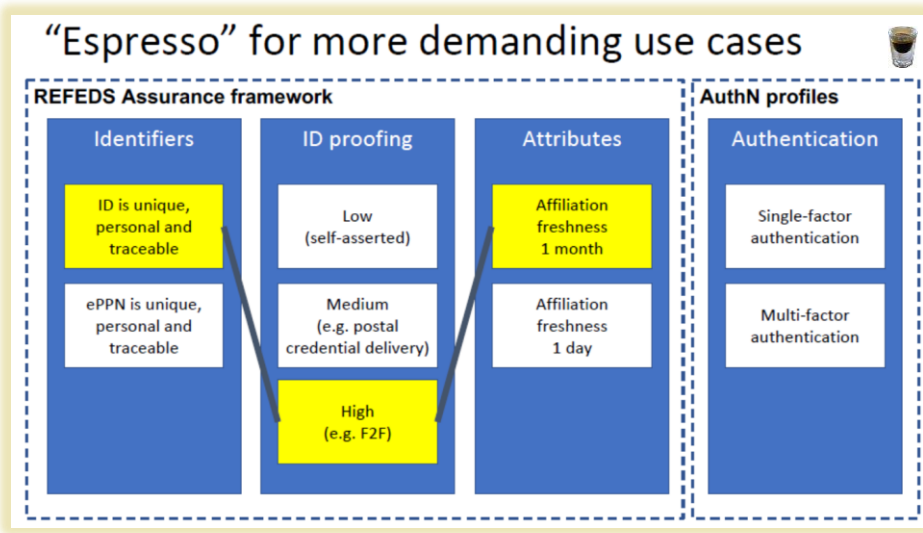
1. You shall only use the Services in a manner consistent with the policies and for the purposes described above, show consideration towards other users, and collaborate in the resolution of issues arising from your use of the Services.
2. You shall only use the Services for lawful purposes and not breach, attempt to breach, nor circumvent administrative or security controls.
3. You shall respect intellectual property and confidentiality agreements.

AARC-I044 Implementers Guide

# GLOBAL USERS? – GLOBAL TRUST!

Electronic identity assurance remains a scalability challenge ... globally

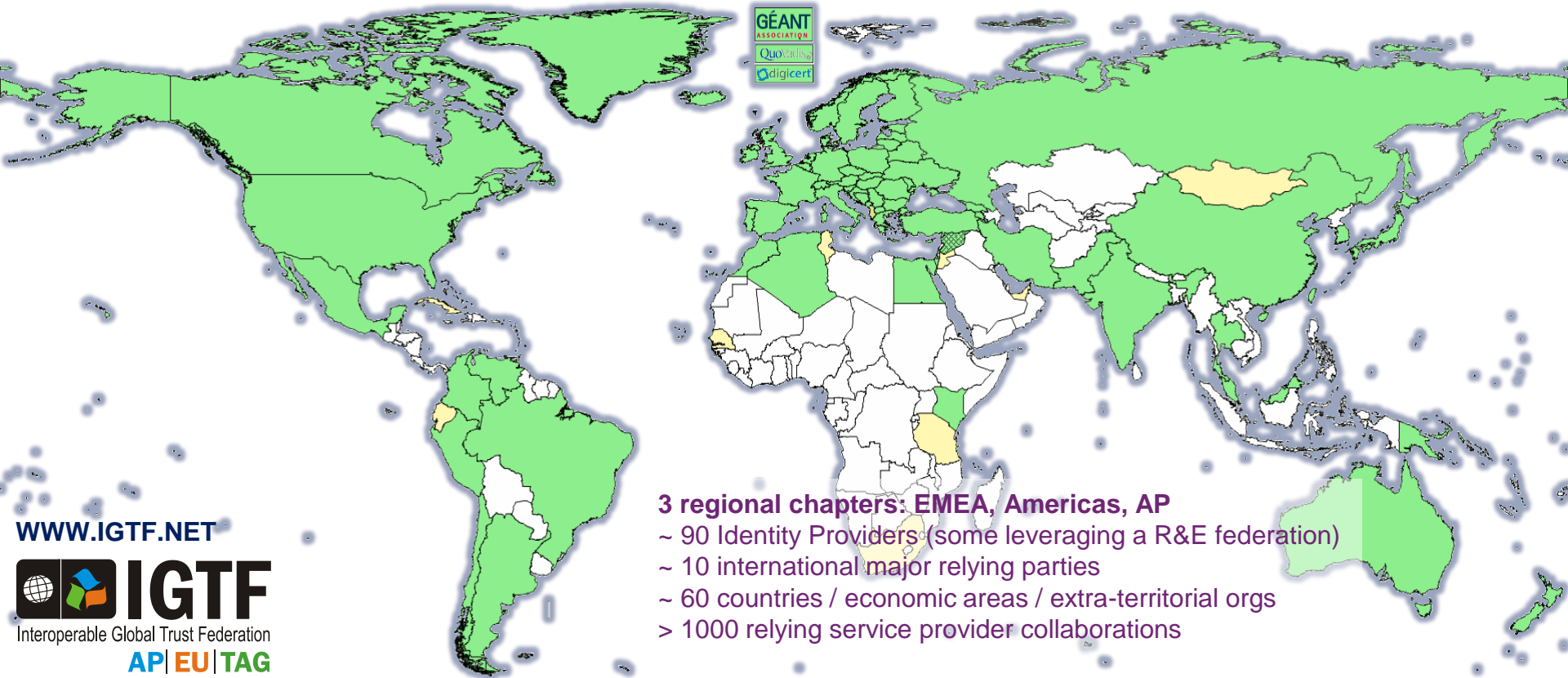
- many frameworks: Kantara, NIST, REFEDS, IGTF, eIDAS, TDIF, ...
- many components: uniqueness, ID proofing, ‘freshness’, authenticator



Infrastructures for Research:  
feasible assurance matching  
risk profile of service classes

- ‘Cappucino’, ‘Birch’, ‘Dogwood’, ...  
intentionally opaque naming  
and no ‘levels’

# INTEROPERABLE GLOBAL TRUST FEDERATION IGTF



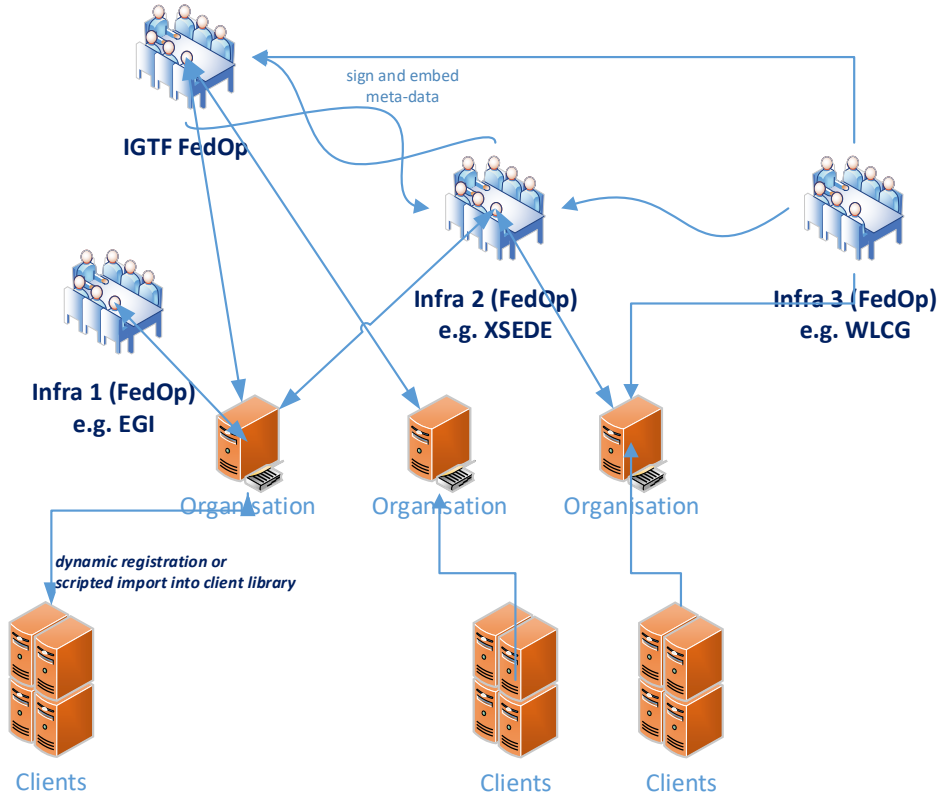
### 3 regional chapters: EMEA, Americas, AP

- ~ 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

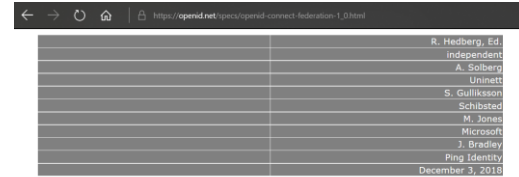
[WWW.IGTF.NET](http://WWW.IGTF.NET)



# OIDC FED – TRUST IS TECHNOLOGY AGNOSTIC



## OpenID Connect Federation: multilateral trust beyond GAFA



### OpenID Connect Federation 1.0 - draft 06 openid-connect-federation-1\_0

#### Abstract

The OpenID Connect standard specifies how a Relying Party (RP) can discover metadata about an OpenID Provider (OP), and then register to obtain relying party credentials. The discovery and registration process does not involve any mechanisms of dynamically establishing trust in the exchanged information, but instead rely on-out-of-band trust establishment.

In an identity federation context, this is not sufficient. The participants of the federation must be able to trust information provided about other participants in the federation. OpenID Connect Federations specifies how trust can be dynamically obtained from resolving trust from a common trusted third party.

While this specification is primarily targeting OpenID Connect, it is designed in order to allow for re-use by other protocols and in other use cases.

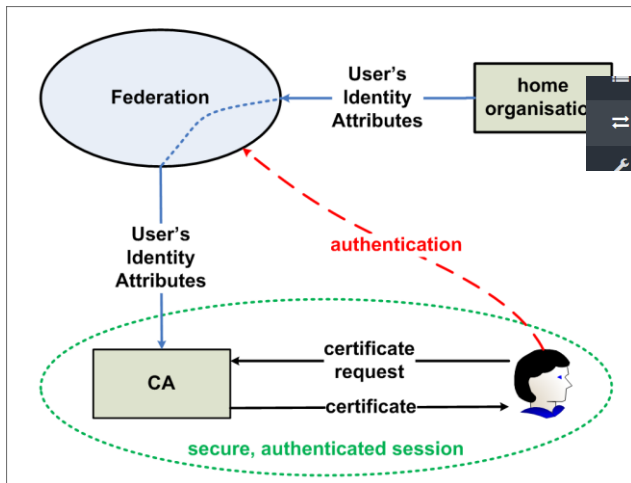
#### Table of Contents

1. Introduction
  - 1.1. Requirements Language
2. Entity Statement
  - 2.1. The trust anchor
3. Metadata
  - 3.1. OpenID Connect Relying Party Metadata

see: [openid.net](https://openid.net) → Specs & Dev info

# BRIDGES AND TOKEN TRANSLATION SERVICES

## GEANT Trusted Certificate Service



### Organization Mapping

Organization Mapping

+ New Mapping

Organization	At
Nikhef	nil
ECM Institute AMOLF	

### SURFconex - Profile Overview

My Profile My Apps Exit

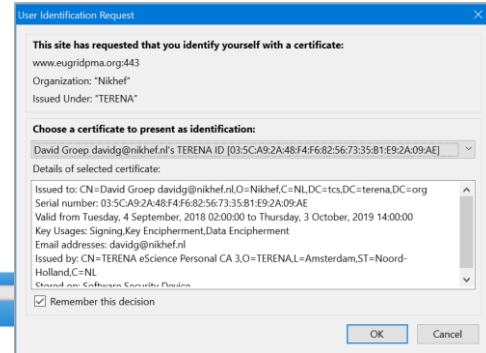
#### SURFconex Apps

You have given permission to share profile information with the following services:

Service/App	EULA	Support URL	Support email
CERTcentral   Digicert		<a href="#">Support pages</a>	

The following attributes are released to this Service Provider:

Attribute	Value
Surname	Groep
E-mailaddress	davidg@nikhef.nl
First name	David
Entitlement	<ul style="list-style-type: none"><li>urn:mace:terena.org:tcs:personal-admin</li><li>urn:mace:terena.org:tcs:personal-user</li></ul>
Institution user ID	davidg@nikhef.nl
Organization	nikhef.nl
Display Name	David Groep



DigiCert acts as a SAML Service provider to eduGAIN and eligible authenticated users can obtain their own certificate for access and delegation to services

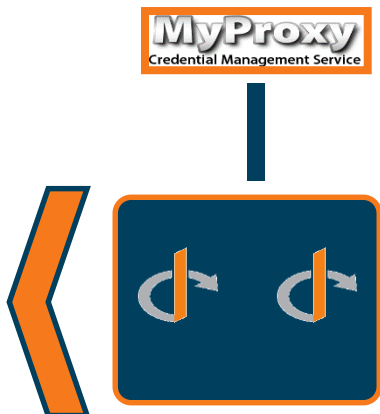
# RCAUTH.EU – BRIDGING TRUST TECHNOLOGY

USER LOGIN FLOW: ACCESS PORTAL → COMMUNITY INFRASTRUCTURE → RCAUTH SERVICE → FEDERATED AAI

CREDENTIAL FLOW: AUTHENTICATION FEDERATION, POLICY FILTER, OPENID CONNECT, GATEWAY CREDENTIAL PROVISIONING



SCIENCE GATEWAYS

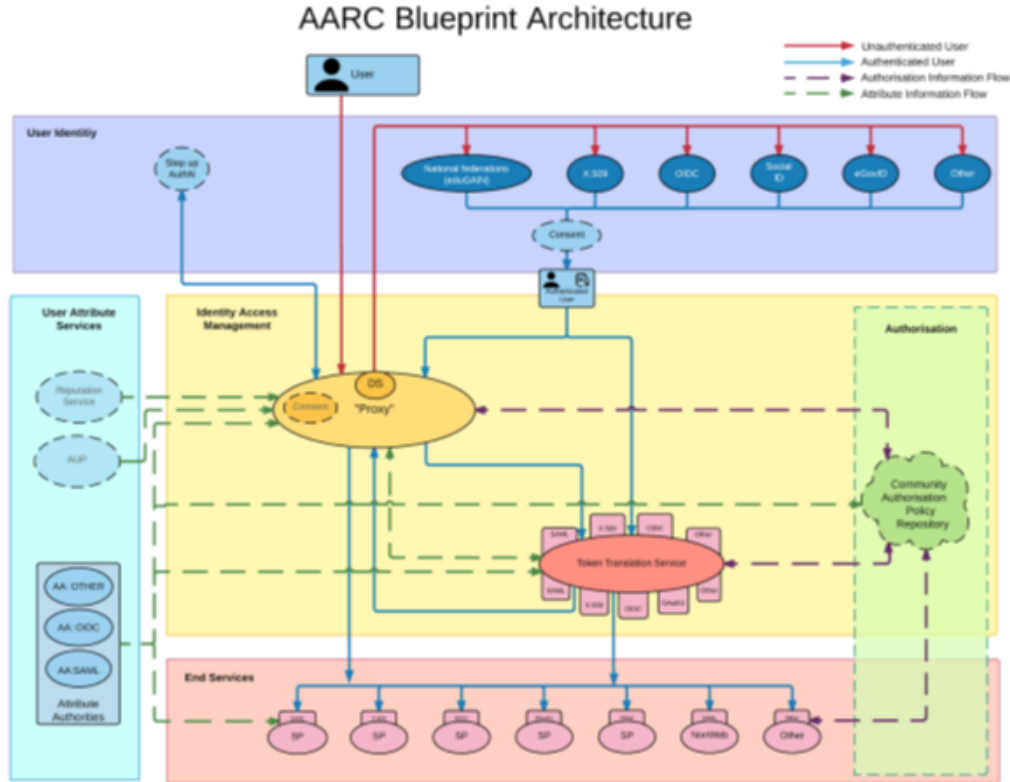


AARC MASTER PORTAL OR INFRASTRUCTURE SOLUTION





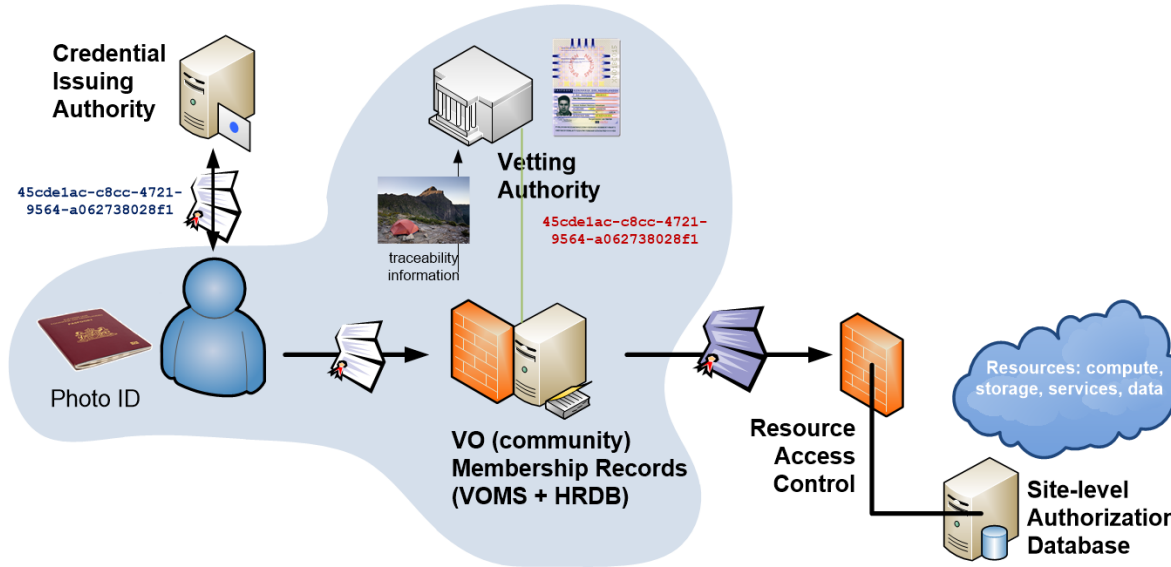
# AARC BPA – COHERENCY BY PROXYING



<https://aarc-project.eu/architecture/>

# BEYOND AUTHN: COLLABORATIVE ASSURANCE

Assurance elements may come from distinct sources



## 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 Galk, 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:

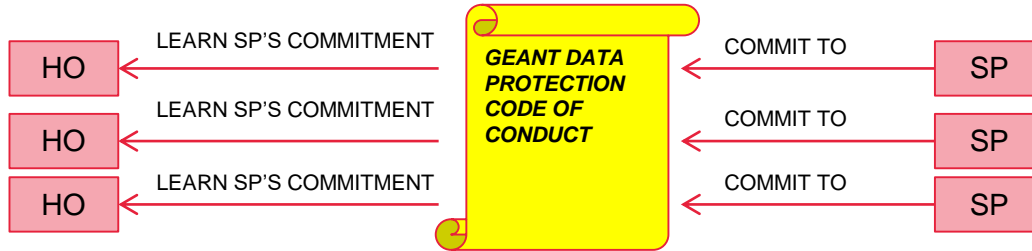
- each of the communities (or infrastructure 'on their behalf') has legitimate interest in processing that data:  
resource allocation, accounting, communicating with members, &c
- each entity in the e-Infrastructure (and EOSC-HUB) is its own controller

Adherence to common policy suite facilitates data sharing

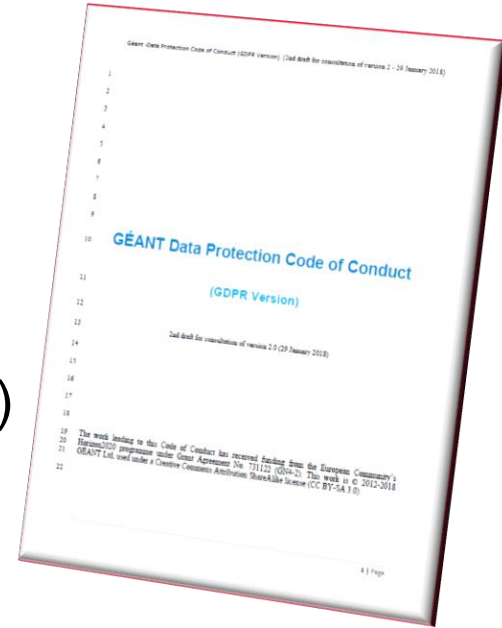
- distributed incident response is explicitly allowed (and used) anyway
- facilitate global sharing through the Code of Conduct (art. 40)
- until EDBP is up to speed, we're essentially a 'BCR' like structure

# GEANT DATA PROTECTION CODE OF CONDUCT V2

Works admirably for our distributed infrastructure



- 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)

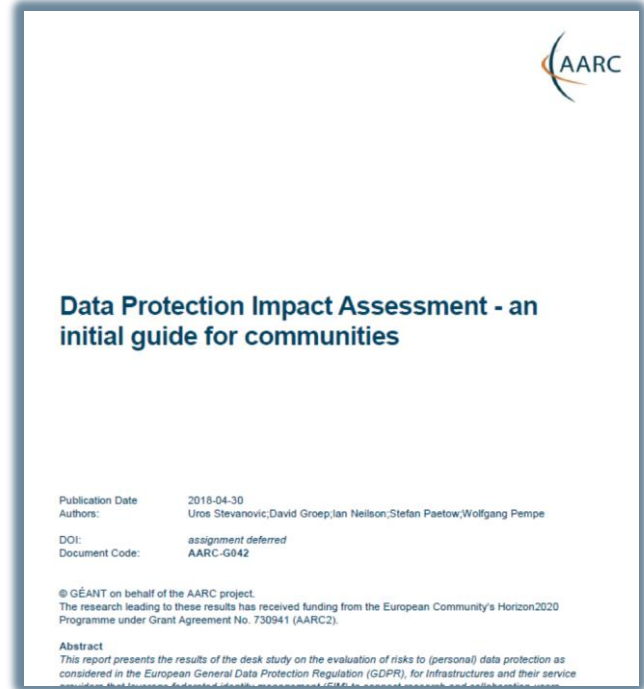


<https://wiki.refeds.org/display/CODE/Code+of+Conduct+ver+2.0+project>

# 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



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

# THIS IS ONE SOLUTION ...

View this email in your browser




**shreddingMachines.co.uk**

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**

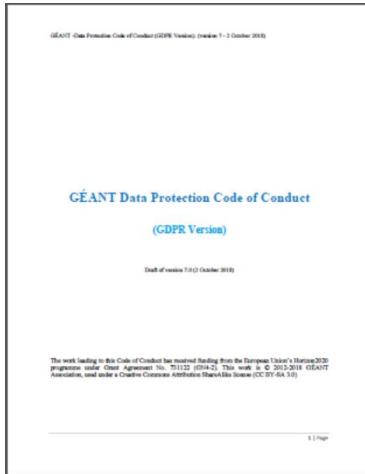
Ruffles Direct Large Office  
High Capacity Micro-cut  
GDPR Shredder with



*UCE message sent on May 17<sup>th</sup> 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



## PRIVACY NOTICE TEMPLATE

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

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

Name of the Service SHOULD be the same as `mdui:DisplayName`

*WebLicht*

Description of the Service 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 organisational 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 organisational 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 Sirtifi trust framework (ver 1.0) [SIRTIFI] 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 Sirtifi 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.

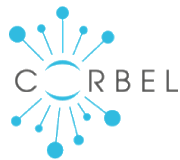
- [OS1] Security patches in operating system and application software are applied in a timely manner.
- [OS2] A process is used to manage vulnerabilities in software operated by the organization.
- [OS3] Mechanisms are deployed to detect possible intrusions and protect information systems.

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

# 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. Mikhaliava

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

Abstract	
Introduction	
Scope	2
Policy impact on infrastructure Operation	
Infrastructure Policies and Frameworks	2
Frameworks	
Sirtfi Trust Framework	3
Research and Scholarship Entity Category	3
GEANT Data Protection Code of Conduct	4
Policies	
Top Level	5
Infrastructure Policy	5
Data Protection	6
Privacy Statement	7
Risk Assessment	7
Membership Management	7
Community Membership Management Policy	8
Acceptable Use Policy	8
Acceptable Authentication Assurance	9
Operational Security	9
	10
	10
	10
	12



# POLICY DEVELOPMENT KIT TEMPLATES



## Policies

Top Level

Infrastructure Policy

Data Protection

Privacy Statement

Risk Assessment

Membership Management

Community Membership Management Policy

Acceptable Use Policy

Acceptable Authentication Assurance

Operational Security

Incident Response Procedure

## Policy Templates

Top Level Infrastructure Policy Template

Membership Management Policy Template

Acceptable Authentication Assurance Policy Template

Acceptable Use Policy Template

Privacy Policy Template

Risk Assessment

Incident Response Procedure

7

7

7

8

### Membership Management Policy Template

- Which information do you need to collect on your users? Name, contact information, nationality?
- How long is membership valid?
- How often do your users need to sign an AUP?

The following is based on the EGI Community Membership Management policy.

Taken from  
<https://docs.egi.eu/doc/diit#>

This policy

**INTRODU**

This policy  
Infrastruct

### Acceptable Authentication Assurance Policy Template

- Which identity providers are acceptable for your infrastructure? SAML Identity Federation IdPs? Social providers such as Google, Facebook etc?
- How much certainty does your community require of the identity? How will you validate this for each identity provider?
- How can you ensure that each user is covered by a security incident response capability at their home organisation?
- Do your

Taken from  
<https://docs.egi.eu/doc/diit#>

### Top Level Infrastructure Policy Template

- Who are the actors in your Infrastructure environment?
- How will you tie additional policies together for the infrastructure?
- Which bodies should approve policy wording?

The following template is based on work by EGI.eu, licensed under a Creative Commons Attribution 4.0 International License.  
<https://documents.egi.eu/public/RetrieveFile?docid=3015&version=3&filename=EGI-SPG-SecurityPolicy-V2.pdf>

#### INTRODUCTION AND DEFINITIONS

To fulfil its mission, it is necessary for the Infrastructure to protect its assets. This document presents the policy regulating those activities of participants related to the security of the

# IMPLEMENTING IT: RESOURCE & SERVICE ACCESS

Site Access Control

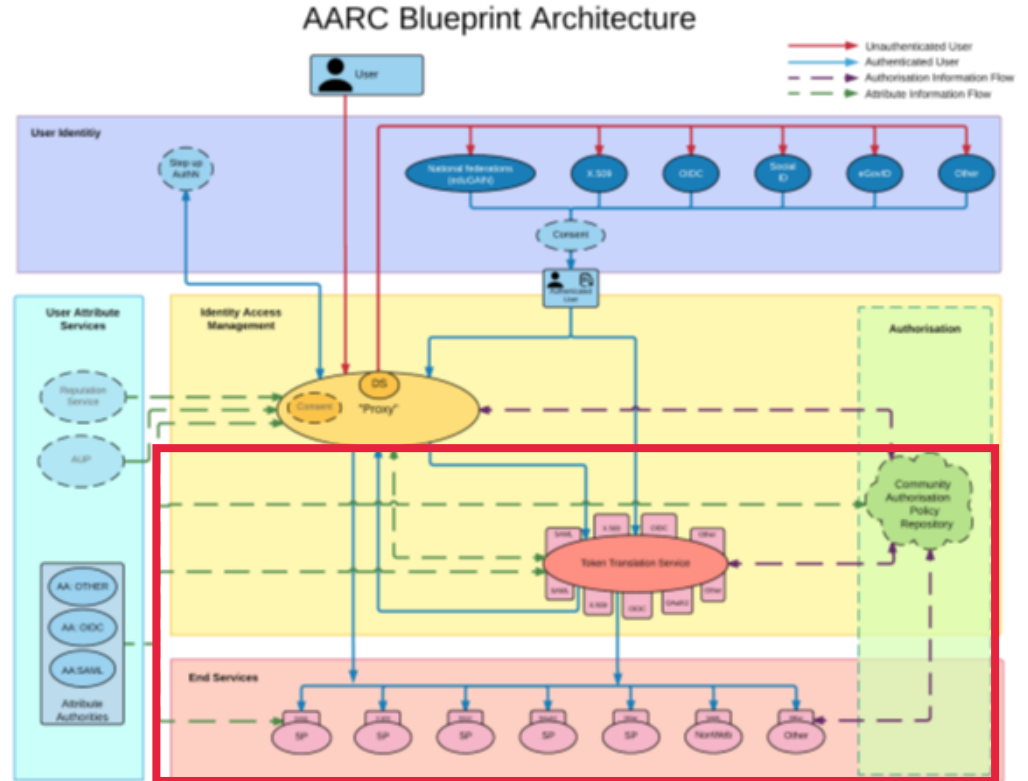
Delegation and support for secure brokering:

OAuth2 and RFC3820

Traceability and Isolation

SaToSa proxies for communities & COMange

Distributed policy and Argus



# PROXIES AND PROVISIONING

COManage and OpenStack and CTA and SCZ and ...

gLExec JIT provisioning from a pool with LCMAPS and the EES

embedding authZ decisions, local or global

Coordinated policy management with SAML-XACML

emergency suspension with Argus

towards operational security

# 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

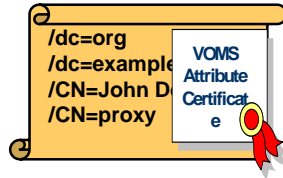
co-development with the AARC project

The image displays a collage of screenshots related to OpenStack and Nikhef COmanage. On the left, a screenshot of the OpenStack dashboard shows the 'Overview' page with a 'Limit Summary' section. This section contains five pie charts representing resource usage: Instances (Used 3 of 10), VCPUs (Used 3 of 25), RAM (Used 6GB of 10GB), Floating IPs (Used 1 of 50), and Security Groups (Used 1 of 10). Below this is a 'Usage Summary' section. On the right, a screenshot of the Nikhef COmanage login page is shown. It features the Nikhef logo and the text 'Nationaal Instituut voor subatomaire fysica'. The login form includes a 'Log in' button, a dropdown menu for 'Authenticate using' set to 'Security Assertion Markup Language', and a note: 'If you are not sure which authentication method to use, contact'. The user's email address 'davidg@nikhef.nl' is visible in the top right corner.

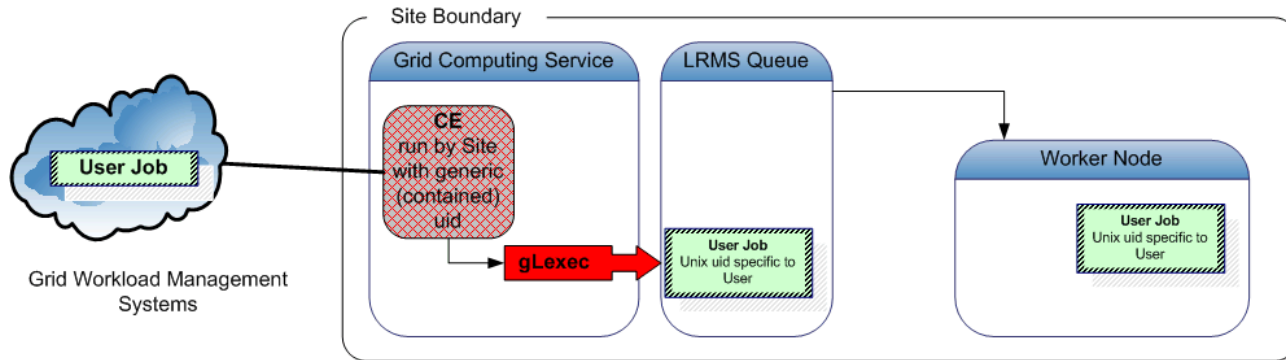
# USER CONTAINMENT AND ISOLATION

## Nikhef's Site Access Control suite for federated login to Unix systems

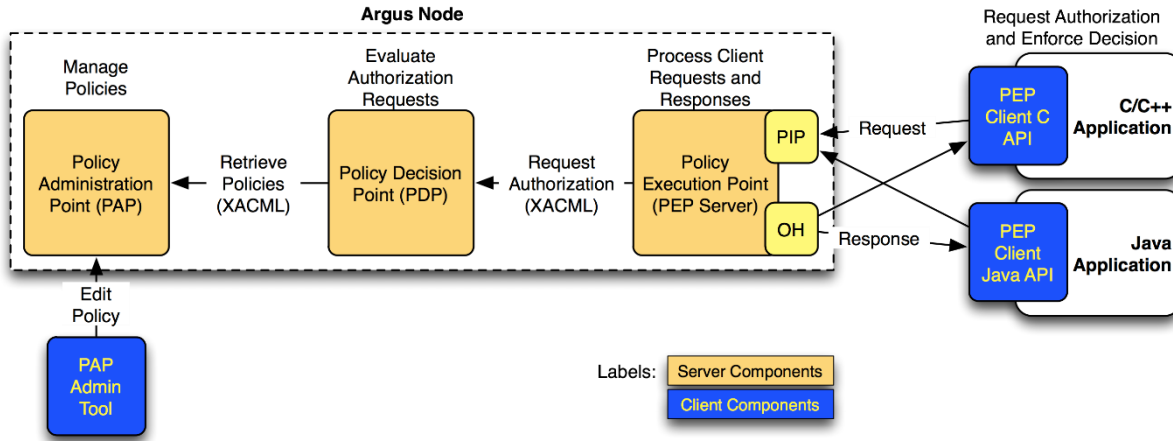
federated identity (with directory or principal name)  
+ **community membership**  
/dc=org/dc=example/CN=John Doe  
voms:/atlas.cern.ch/Group=adc/Role=lcgadmin



```
pvier001:x:43401:2029:PoolAccount VL-e P4 no.1:/home/pvier001:/bin/sh
```

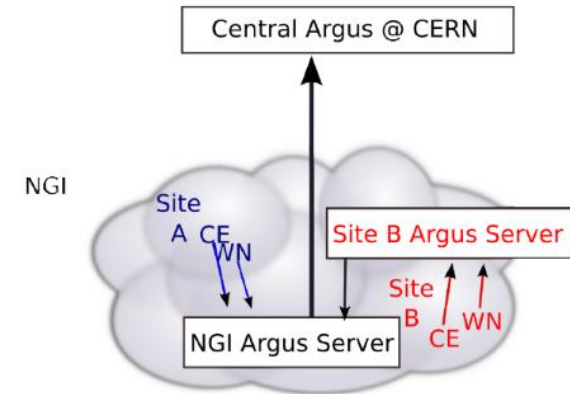


# FEDERATED AUTHORIZATION: LOCAL AND GLOBAL



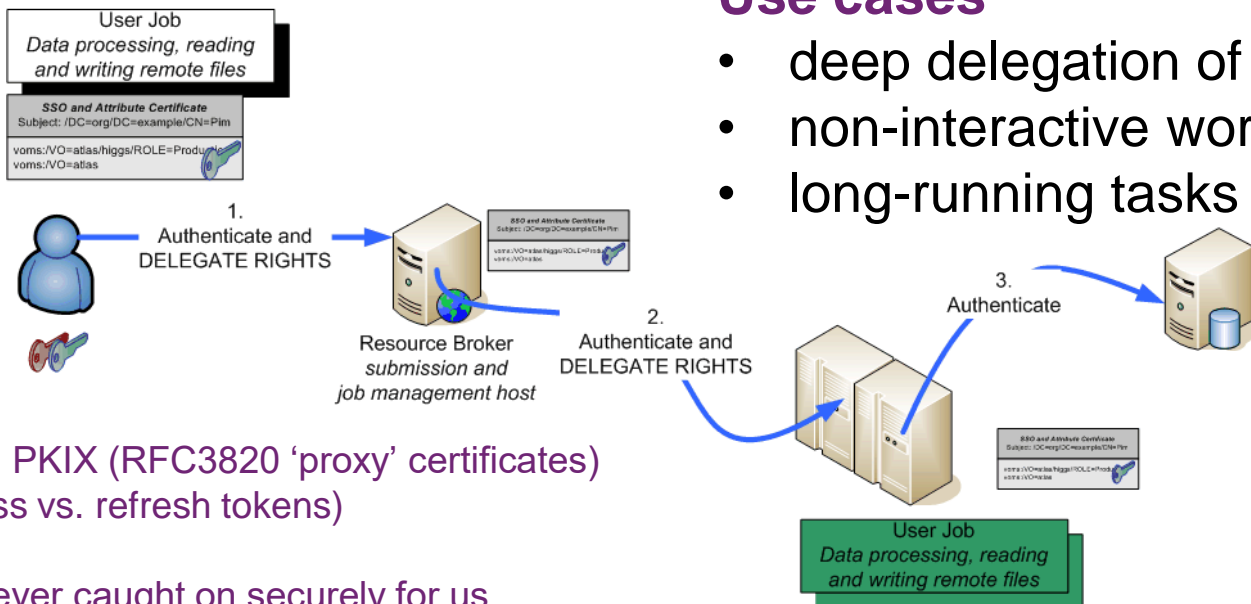
## Hierarchical distributed policy

- chaining
- Policy Administration Points
- service-local Policy Information Points and obligation handling  
(*"you shall be ua1242"*, *"you shall have role dept\_mgr"*)



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

# SECURE NON-WEB REMAINS A CHALLENGE



## Use cases

- deep delegation of rights
- non-interactive workflows
- long-running tasks

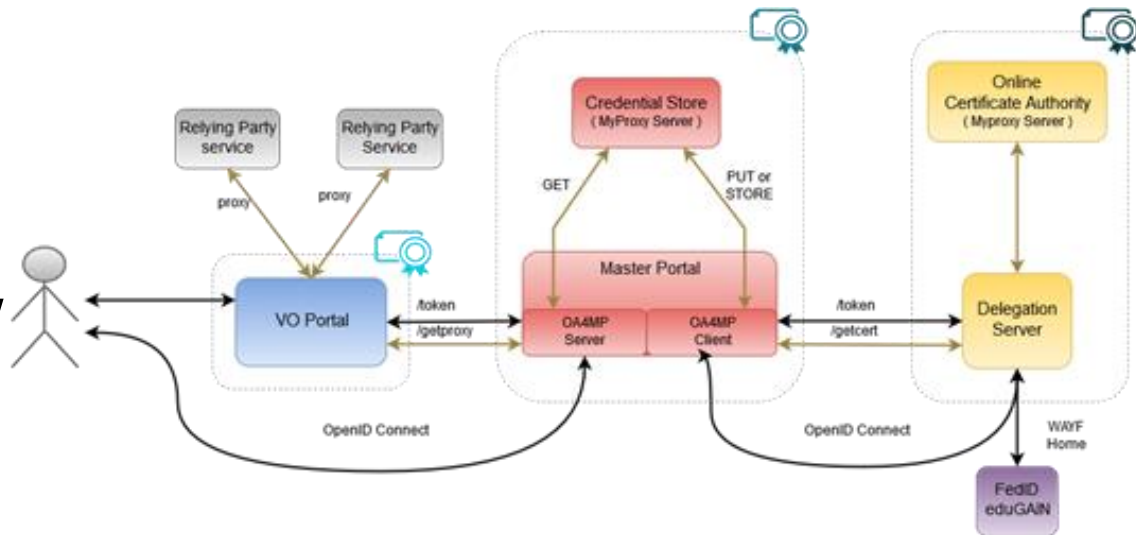
Solutions exist in PKIX (RFC3820 'proxy' certificates) in OAuth2 (access vs. refresh tokens) but

... SAML ECP never caught on securely for us  
... OAuth2 very new our federated use cases  
... and PKIX is not loved by end-users ☹

# SCIENCE GATEWAY AND THE MASTER PORTAL

## Credential management service

- registered portal can obtain user credentials via OAuth2 (refresh) flow
- act on behalf of user to execute workflows

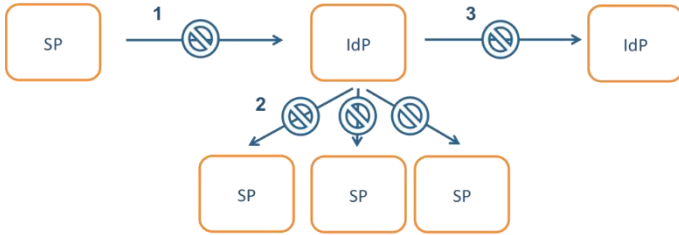


complements user-managed translation solutions

<https://rcauth.eu/>  
<https://github.com/rcauth-eu/aarc-master-portal>  
[https://wiki.nikhef.nl/grid/AARC\\_Pilot\\_-\\_RCAuth.eu](https://wiki.nikhef.nl/grid/AARC_Pilot_-_RCAuth.eu)



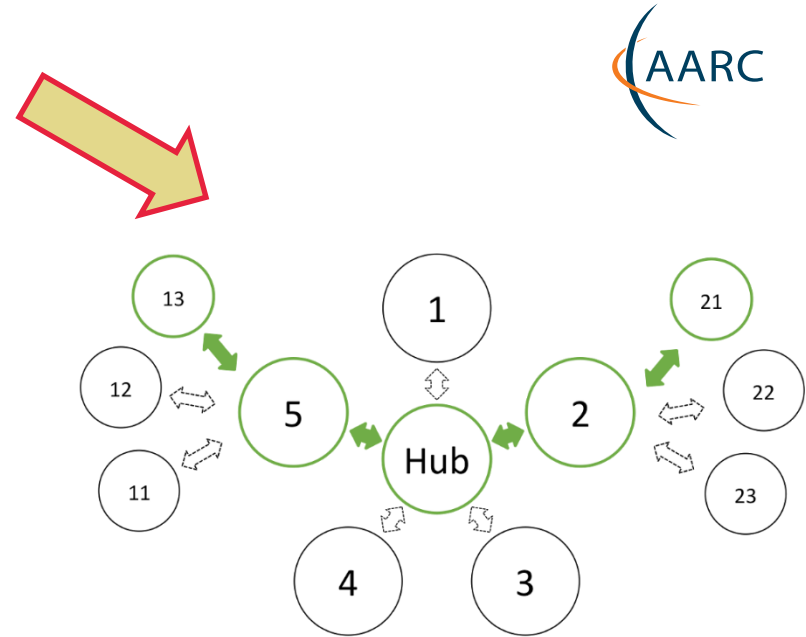
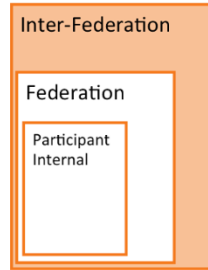
# MANY PARTIES, SHARED SECURITY CHALLENGES



*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!



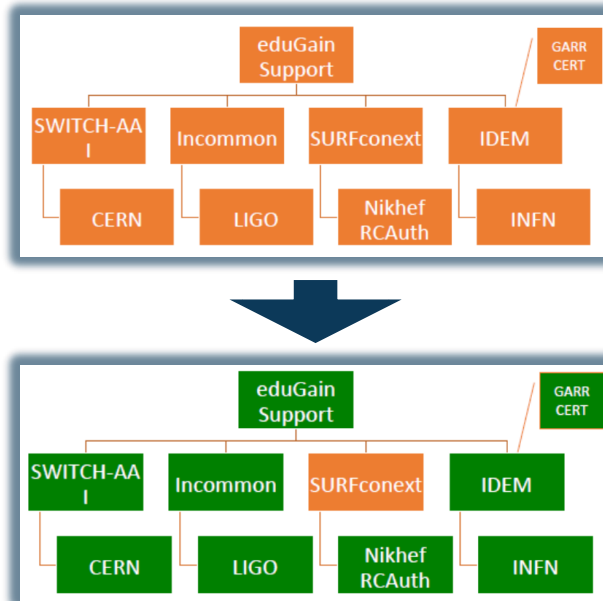
*Inter-Federation Incident Response Communication*



# EXERCISES – COMMUNICATIONS AND ACTIONS



## parties involved in response challenge



# 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, ...



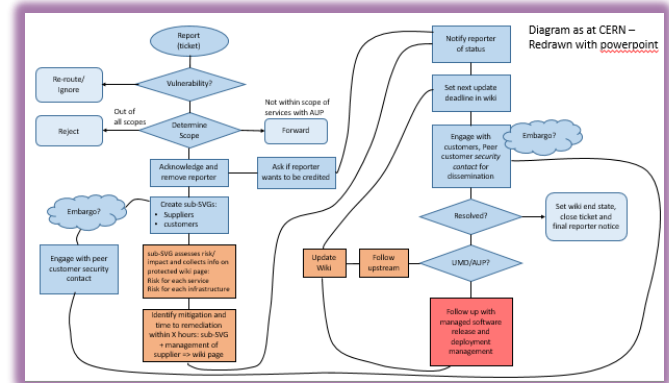
# VULNERABILITY ANALYSIS PLUS ADVISORIES

Most of the software we use originates outside, some comes from peers

- access control and containerization software has elevated privileges
- automated tools find only a fraction of the ‘real issues’

## Middleware Security Team

- code inspection and review
- impact assessment and risk
- advisory communications
- black-box and white-box pen-testing



# VULNERABILITY MITIGATION IN EGI AND WLCG

The screenshot shows the EGI Security Dashboard interface. At the top, it says "Security esiDashboard". Below that, there are navigation tabs: OVERVIEW >> MONITORING > HISTORY > DEBUG > COD. On the right, there are tabs for METRICS, REPORTS, EVENTS, and HELP OPERATIONS PORTAL TOOLS. A user greeting "We come Leif Nixon leini58@liu.se" is visible. On the left, there are icons for a globe, a document, a group of people, and a calendar. Below these icons is a list of regions with their respective counts:

Region	Count
NGI_IT	203
AsiaPacific	93
NGI_FRANCE	74
NGI_UK	50

The main content area shows a table for "monitoring > ngi ( 23 )". The table has columns for NGI, CRITICAL, ERROR, and OPENED GG. The rows are:

NGI	CRITICAL	ERROR	OPENED GG
AsiaPacific	28	65	
NGI_AECIS		1	
NGI_BG		1	
NGI_DE			

The screenshot shows an email notification from David Crooks via RT. The subject is "[EGI #15254] Critical vulnerability exposed at [redacted]; EGI-CVE-2017-5753/EGI-CVE-2017-5754". The email body contains the following information:

From: David Crooks via RT <vulnerability-handling@rt.egi.eu>  
Subject: [EGI #15254] Critical vulnerability exposed at [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-[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.

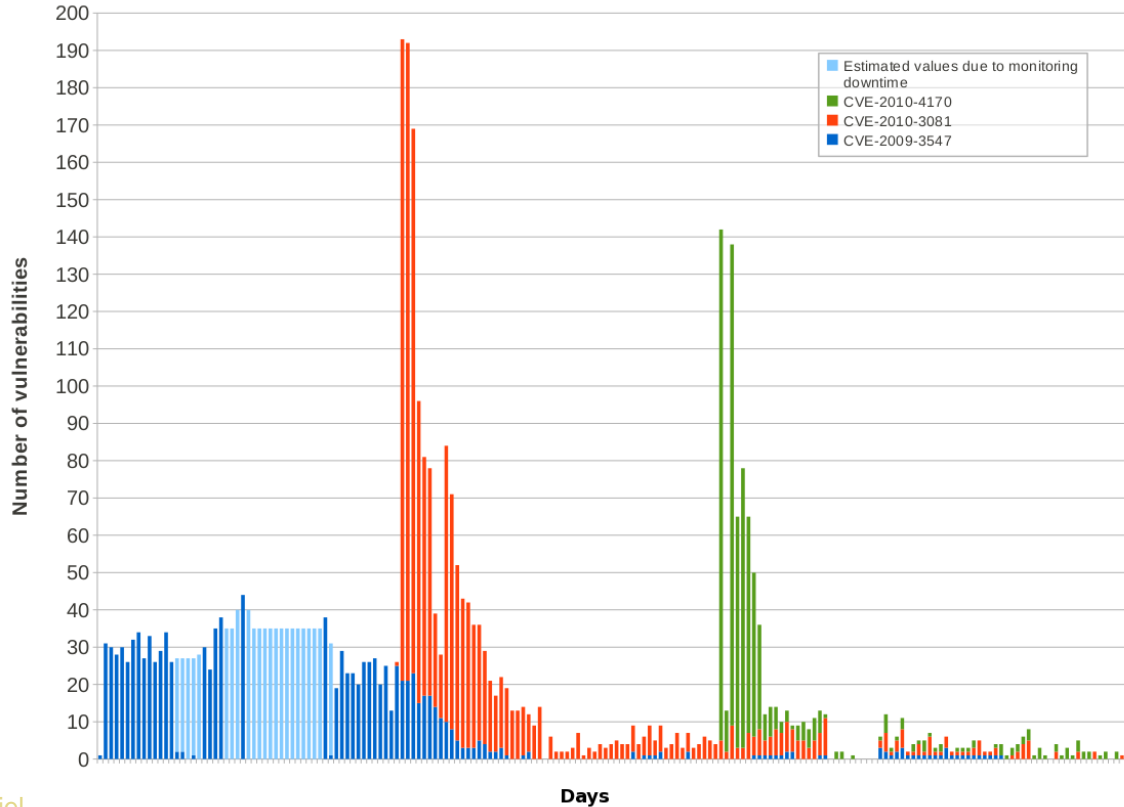
=== What you are being asked to do now ===

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

# PROACTIVE MONITORING – PAKITI AND EGI CSIRT



Data: EGI-CSIRT/Sven Gabriel

# 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.*



# TRAINING IN A DISTRIBUTED FEDERATION

Developed a framework to automate distribution of 'fake incidents' across infrastructure and monitor response

- automated service access and 'job submission'
- challenging test mimicking real malware (including process hiding, use of encryption and TOR, P2P C2 control, and torrent payload transfer) *but of course not weaponized ...*
- monitoring of intervention and suspension of suspect credentials
- report-out and information sharing part of the challenge



# FEEDBACK TO SERVICE PROVIDERS

## Communication:

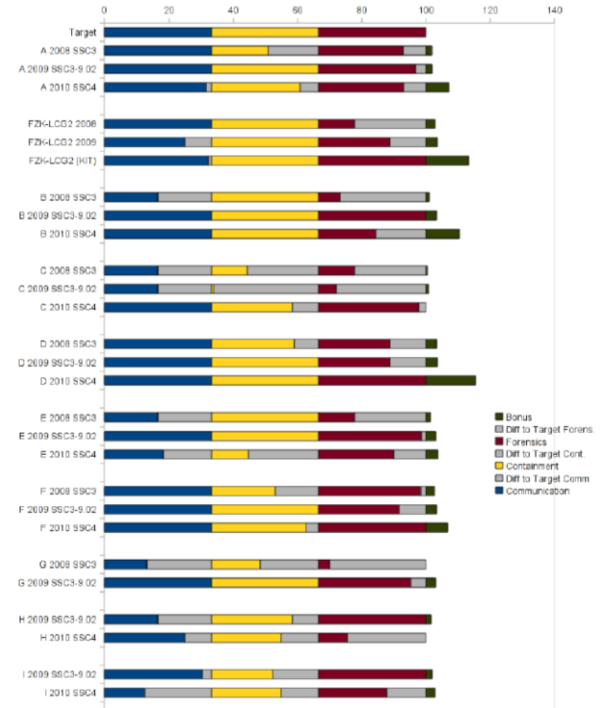
- Endpoints valid?
- Form/Content OK ?

## Containment

- Ban "malicious" users
- Find/Stop malicious processes
- Find submission IP

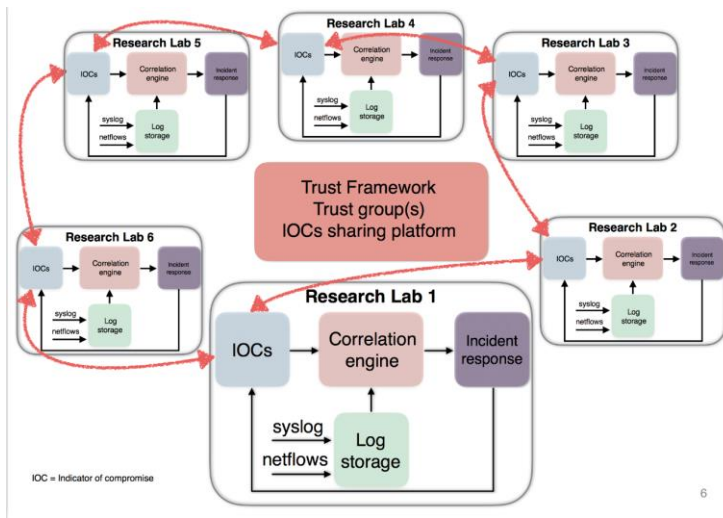
## Forensics

- Basic Forensics on binary
- Network traffic



# 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



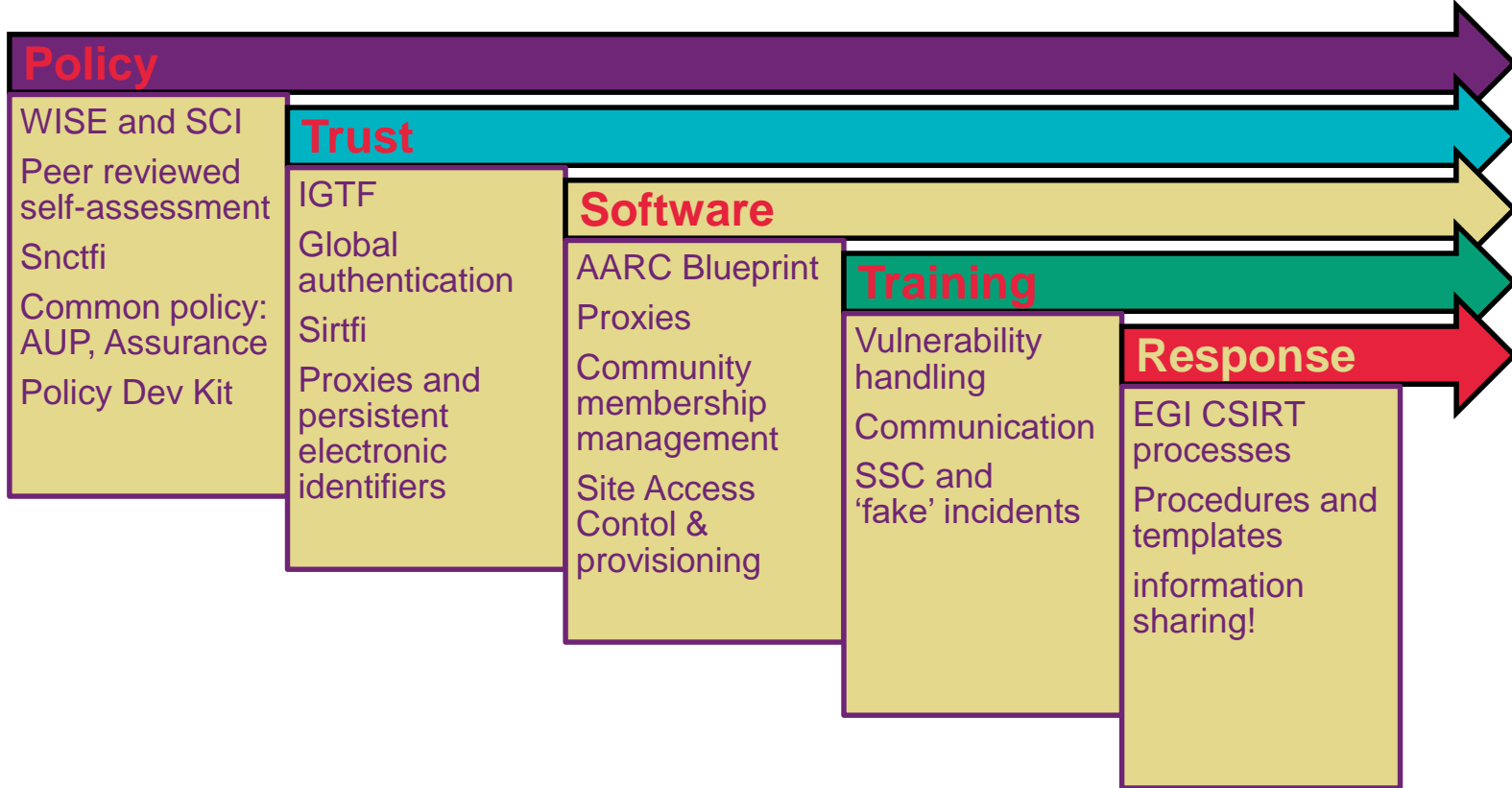
Legitimate interest 6.1(f) as usual basis appropriate safeguards within EEA in place

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



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



Nikhef

David Groep

davidg@nikhef.nl

<https://www.nikhef.nl/~davidg/presentations/>

 <https://orcid.org/0000-0003-1026-6606>