Resilience of the VO membership vetting process

AKA seeing social accounts handled in an satisfying way

Sven Gabriel, on behalf of Baptiste Grenier

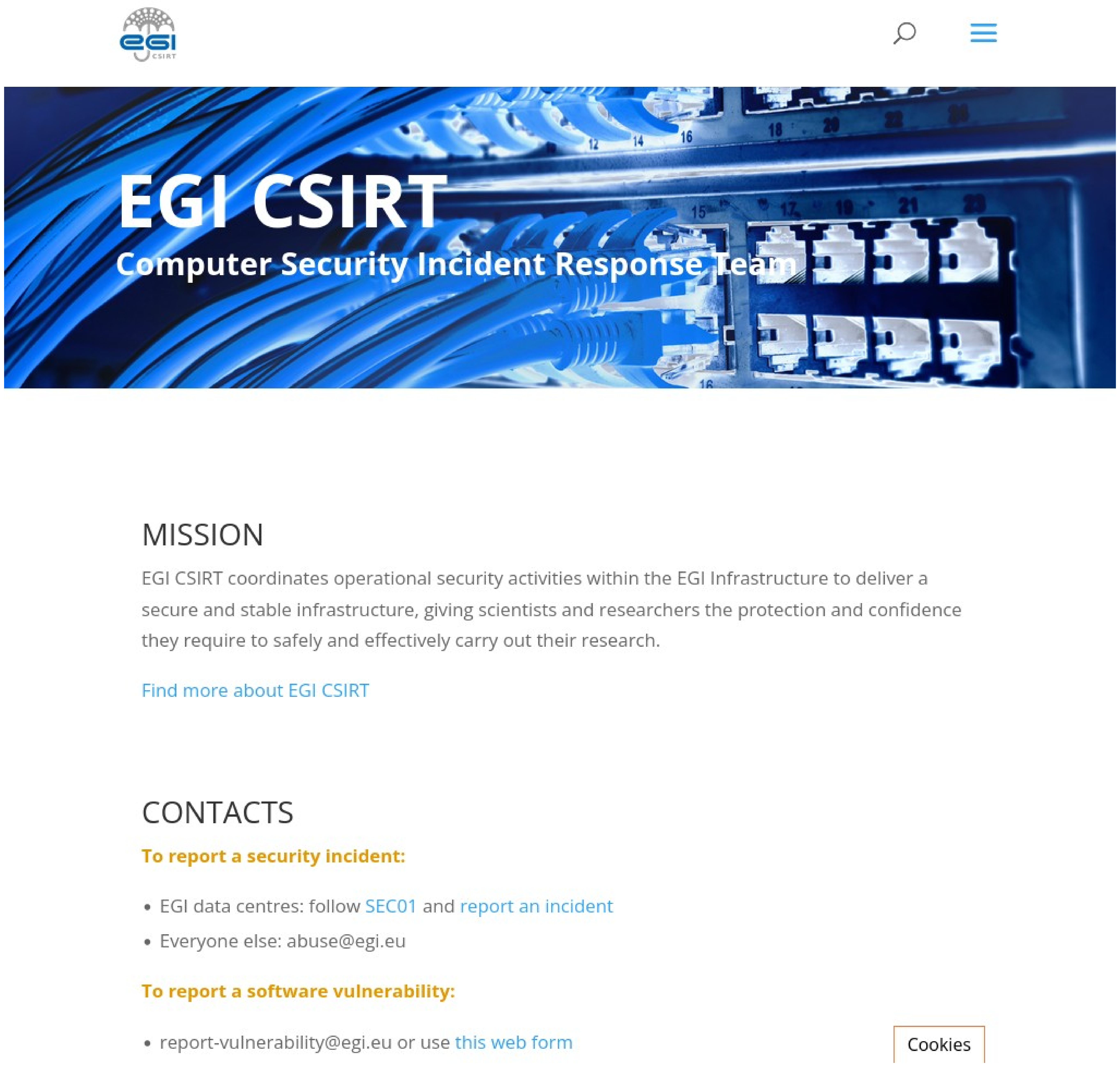
SDIS Officer, IRTF member

TLP:CLEAR Public

2023/03/16

Report on EGI CSIRT activities

https://csirt.egi.eu/



EGI CSIRT

Computer Security Incident Response Team

MISSION

EGI CSIRT coordinates operational security activities within the EGI Infrastructure to deliver a secure and stable infrastructure, giving scientists and researchers the protection and confidence they require to safely and effectively carry out their research.

Find more about EGI CSIRT

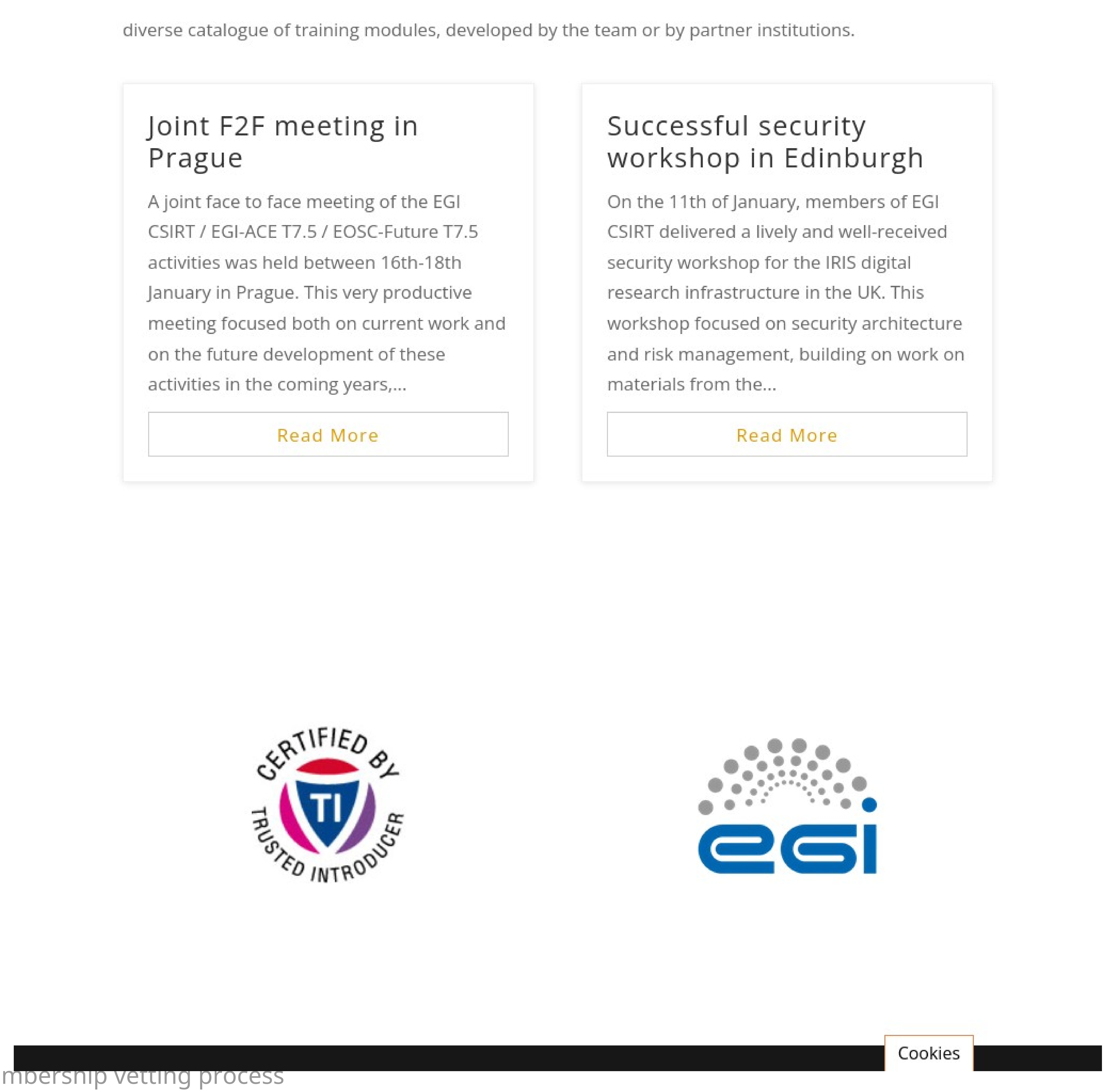
CONTACTS

To report a security incident:

- EGI data centres: follow SEC01 and report an incident
- Everyone else: abuse@egi.eu

To report a software vulnerability:

- report-vulnerability@egi.eu or use this web form



diverse catalogue of training modules, developed by the team or by partner institutions.

Joint F2F meeting in Prague

A joint face to face meeting of the EGI CSIRT / EGI-ACE T7.5 / EOSC-Future T7.5 activities was held between 16th-18th January in Prague. This very productive meeting focused both on current work and on the future development of these activities in the coming years,...

Read More

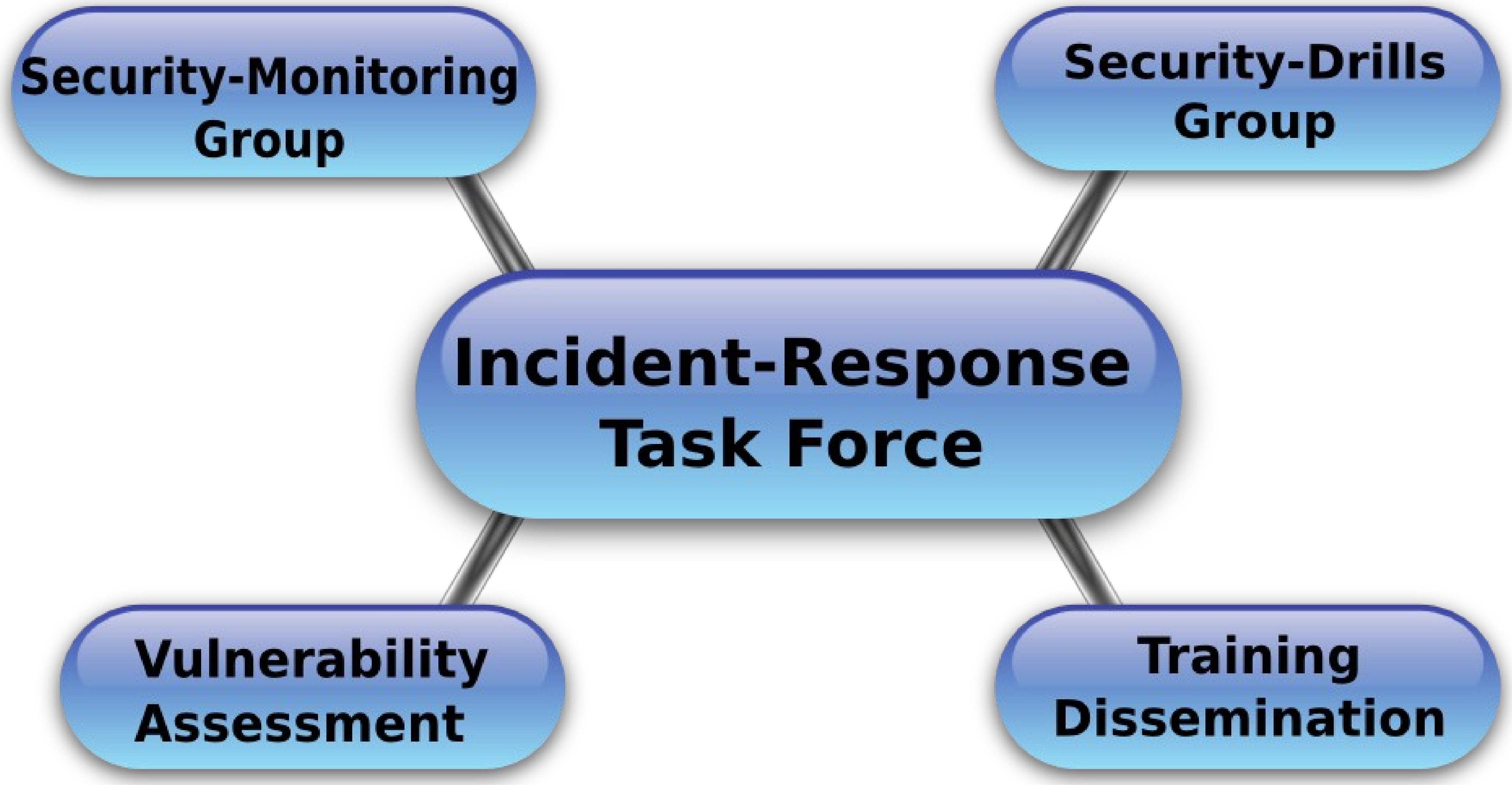
Successful security workshop in Edinburgh

On the 11th of January, members of EGI CSIRT delivered a lively and well-received security workshop for the IRIS digital research infrastructure in the UK. This workshop focused on security architecture and risk management, building on work on materials from the...

Read More

EGI-CSIRT

Members: NGI-Security-Officers



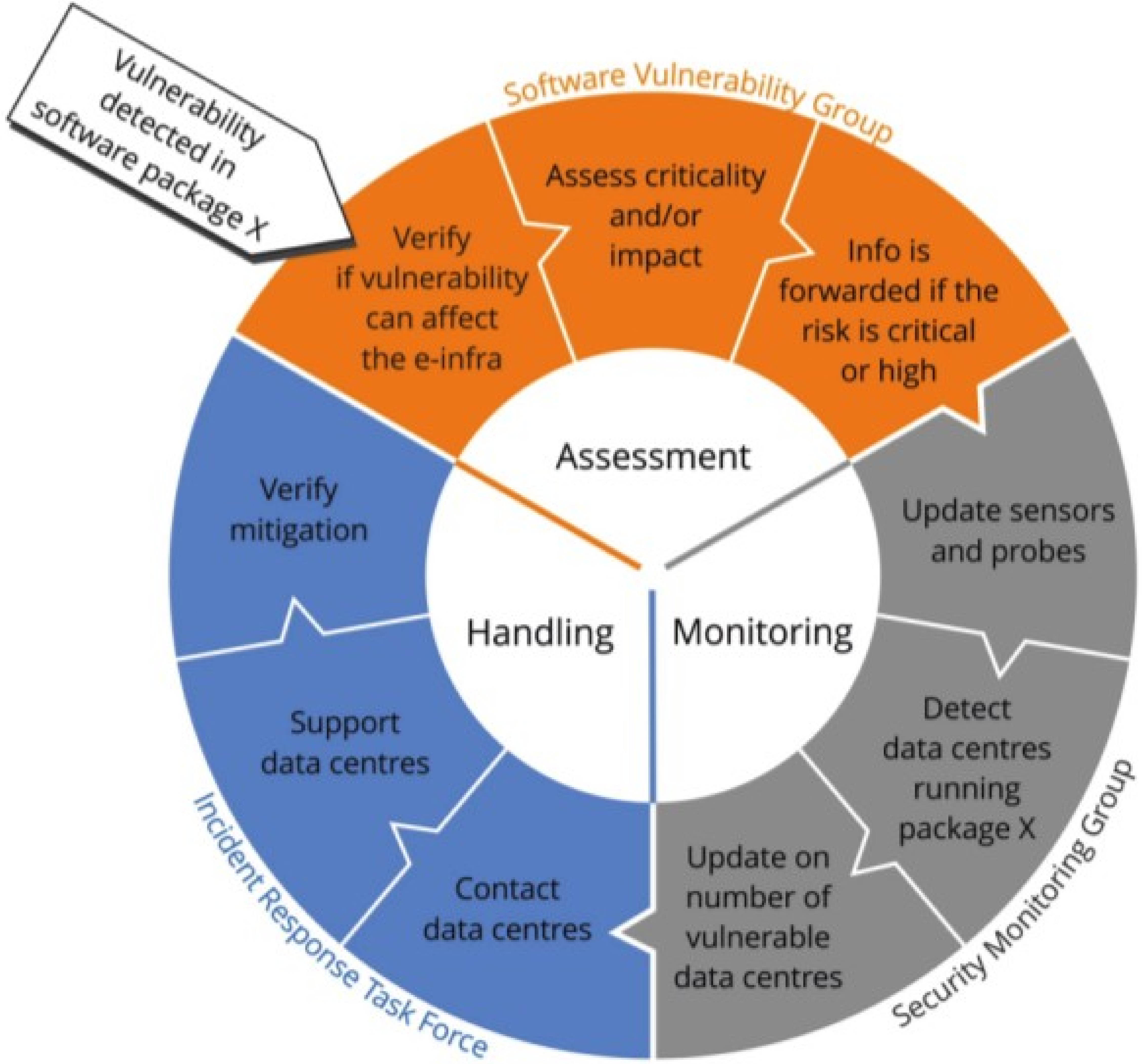
Security-Monitoring Group

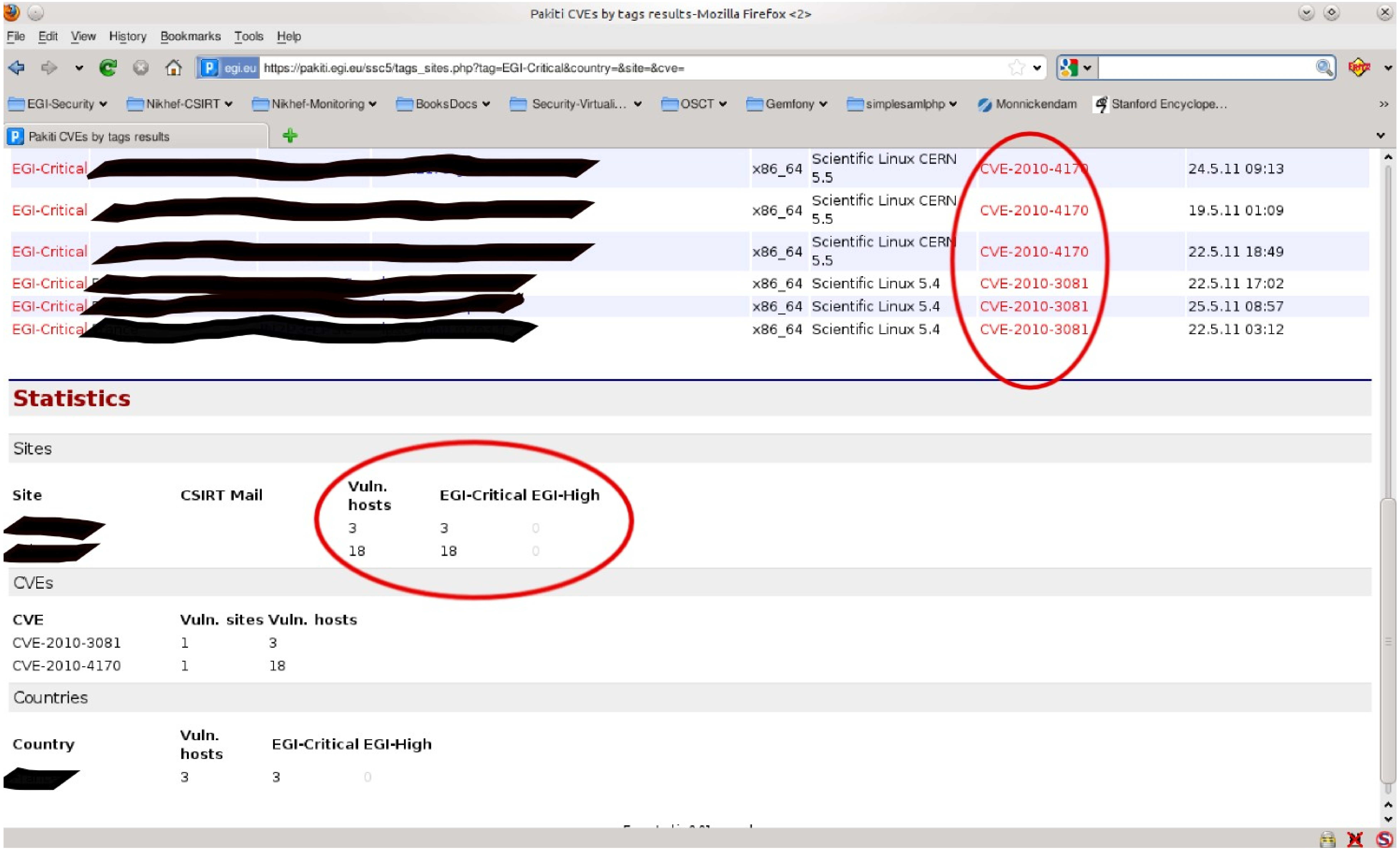
Security-Drills Group

Incident-Response Task Force

Vulnerability Assessment

Training Dissemination


Vulnerability detected in software package X
Software Vulnerability Group
Verify if vulnerability can affect the e-infra
Assess criticality and/or impact
Info is forwarded if the risk is critical or high
Assessment
Update sensors and probes
Detect data centres running package X
Update on number of vulnerable data centres
Security Monitoring Group
Monitoring
Handling
Contact data centres
Support data centres
Verify mitigation
Incident Response Task Force



Pakiti CVEs by tags results-Mozilla Firefox <2>

https://pakiti.egi.eu/ssc5/tags_sites.php?tag=EGI-Critical&country=&site=&cve=

Pakiti CVEs by tags results

EGI-Critical	[redacted]	x86_64	Scientific Linux CERN 5.5	CVE-2010-4170	24.5.11 09:13
EGI-Critical	[redacted]	x86_64	Scientific Linux CERN 5.5	CVE-2010-4170	19.5.11 01:09
EGI-Critical	[redacted]	x86_64	Scientific Linux CERN 5.5	CVE-2010-4170	22.5.11 18:49
EGI-Critical	[redacted]	x86_64	Scientific Linux 5.4	CVE-2010-3081	22.5.11 17:02
EGI-Critical	[redacted]	x86_64	Scientific Linux 5.4	CVE-2010-3081	25.5.11 08:57
EGI-Critical	[redacted]	x86_64	Scientific Linux 5.4	CVE-2010-3081	22.5.11 03:12

Statistics

Sites

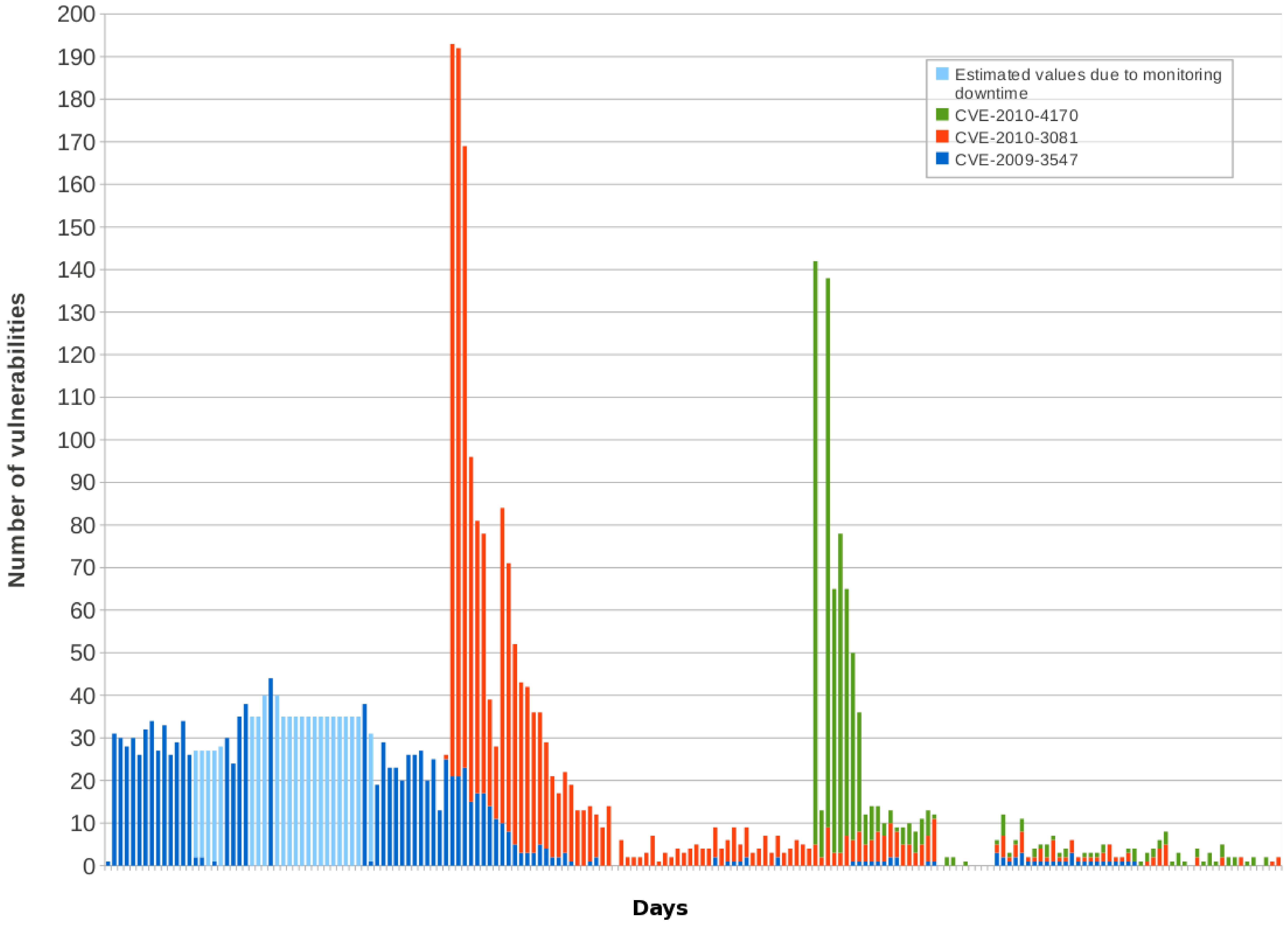
Site	CSIRT Mail	Vuln. hosts	EGI-Critical	EGI-High
[redacted]		3	3	0
[redacted]		18	18	0

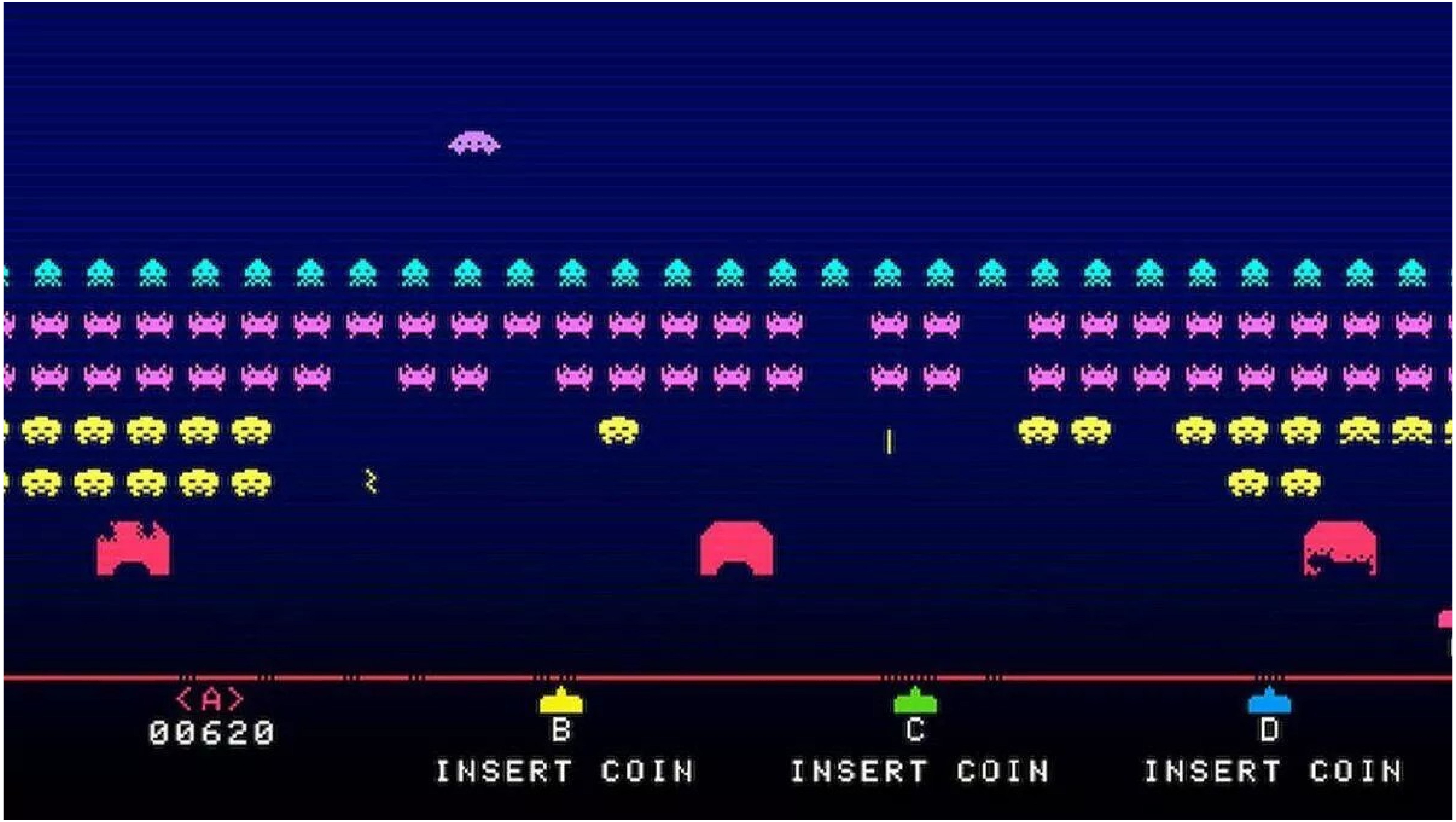
CVEs

CVE	Vuln. sites	Vuln. hosts
CVE-2010-3081	1	3
CVE-2010-4170	1	18

Countries

Country	Vuln. hosts	EGI-Critical	EGI-High
[redacted]	3	3	0


Estimated values due to monitoring downtime
CVE-2010-4170
CVE-2010-3081
CVE-2009-3547
Number of vulnerabilities
Days
200
190
180
170
160
150
140
130
120
110
100
90
80
70
60
50
40
30
20
10
0


<A>
00620
B
INSERT COIN
C
INSERT COIN
D
INSERT COIN

A bit of context

- Chit chats between some IRTF members leading to the idea of testing the vetting process of a cloud VO, using an identity from a social media platform
  - "What is needed to start a VM in fedcloud? A registered account in a VO?
  - "Maybe we should get some social media accounts and check if they get accepted there :-)"
  - "Sure, seem an interesting exercise, let's do it!"

Motivation

Open Science and Open Access do not mean there is no need to control who can use resources and services

- Many **security incidents** caused by the, **possibly on purpose**, **lack of authorisation and vetting** when granting access to resources and services. Social media IdPs, like Google, are providing unlimited accounts allowing to verify an email for free.

  - [EGI-20210318-001] **Proxying of nefarious content** via a misconfigured IaaS platform allowing anyone to create a local account and deploy services.
  - [EGI-20210430-01] **Crypto-mining** on a JupyterHub notebook, access granted without any vetting to every Check-in user.
  - [EGI-20220107-01] **Crypto-mining** on a JupyterHub notebook, access granted without any vetting to every Indigo IAM user. Also possible to access by creating a local account with just a mail verification.
  - [EGI-20220114-01] **Crypto-mining** on a JupyterHub notebook, access granted without any vetting to every Check-in user.

Ralphs
first in Southern California
Price Breaker
Extra Savings Every Day.
KOZY SHACK PUDDINGS
Lowe

#0: pretext impersonating a researcher in need of cloud resources

Welcome Dr Sobchack

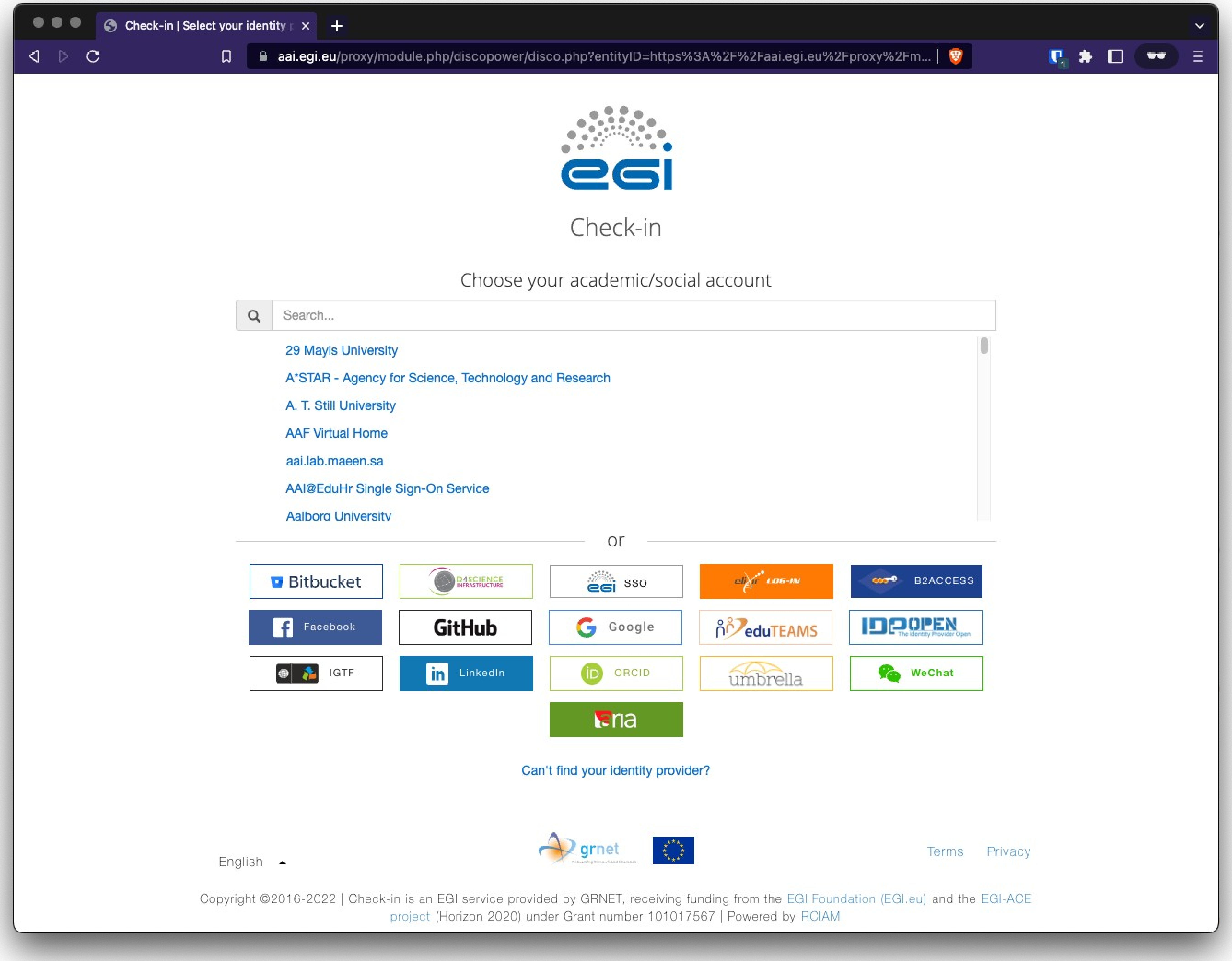
- Dr Walter Sobchack is a researcher, looking for cloud resources to do some analysis in the context of their research

  - **Identity card**
    - Name: Walter Sobchack
    - Title: Dr
    - Institute: Nizhny Novgorod State Academy of Medicine (Russia)
    - Email: dr.walter.sobchack@gmail.com
  - **Research papers - online proofs**
    - https://www.researchgate.net/scientific-contributions/DM-Sobchak-33763131
      - Content already available online, from a real researcher with a similar name
  - **Inspiration: Walter Sobchak character from "The Big Lebowski" movie**
    - https://coenbrothers.fandom.com/wiki/Walter_Sobchak

# 1: Getting a social media account integrated with Check-in

May options to choose from

- Google, GitHub, ORCID, LinkedIn…
- Decided to go with a **Google account** as it also provides a convenient way to have a **working email address**
  - **Easy to create and manage**
  - **One requirement:** having a phone number used at account creation



Check-in | Select your identity p

aai.egi.eu/proxy/module.php/discopower/disco.php?entityID=https%3A%2F%2Faai.egi.eu%2Fproxy%2Fm…

Check-in

Choose your academic/social account

Search...

29 Mayis University
A*STAR - Agency for Science, Technology and Research
A. T. Still University
AAF Virtual Home
aai.lab.maeen.sa
AAI@EduHr Single Sign-On Service
Aalborg University

or

Can't find your identity provider?

English

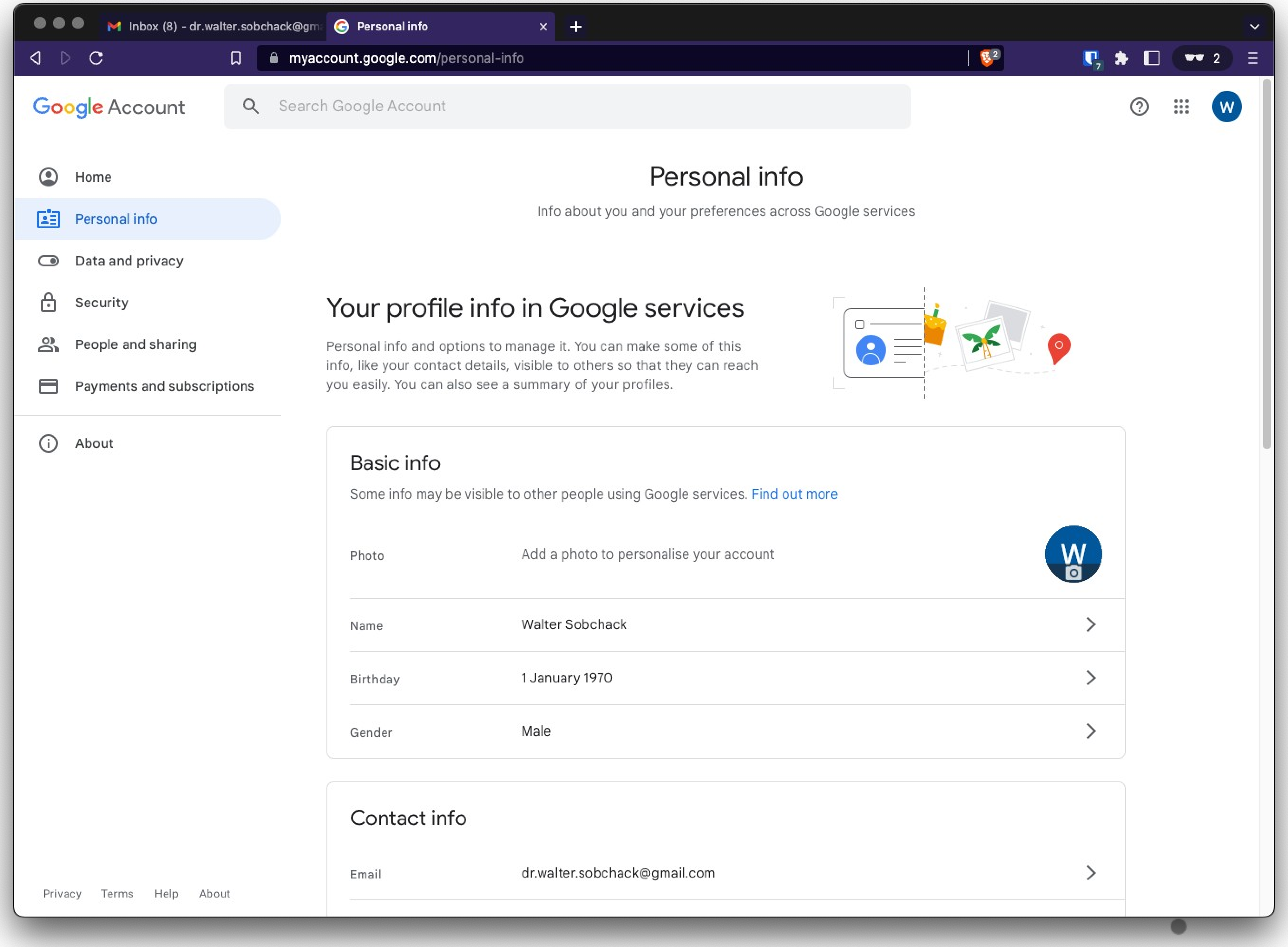
Terms Privacy

Copyright ©2016-2022 | Check-in is an EGI service provided by GRNET, receiving funding from the EGI Foundation (EGI.eu) and the EGI-ACE project (Horizon 2020) under Grant number 101017567 | Powered by RCIAM

# 1: Dr Walter Sobchack's Google account

An easy first step

- Welcome Dr Sobchack!
  - **Email:** dr.walter.sobchack@gmail.com



Personal info

Info about you and your preferences across Google services

Your profile info in Google services

Personal info and options to manage it. You can make some of this info, like your contact details, visible to others so that they can reach you easily. You can also see a summary of your profiles.

Basic info

Some info may be visible to other people using Google services. Find out more

Photo: Add a photo to personalise your account

Name: Walter Sobchack

Birthday: 1 January 1970

Gender: Male

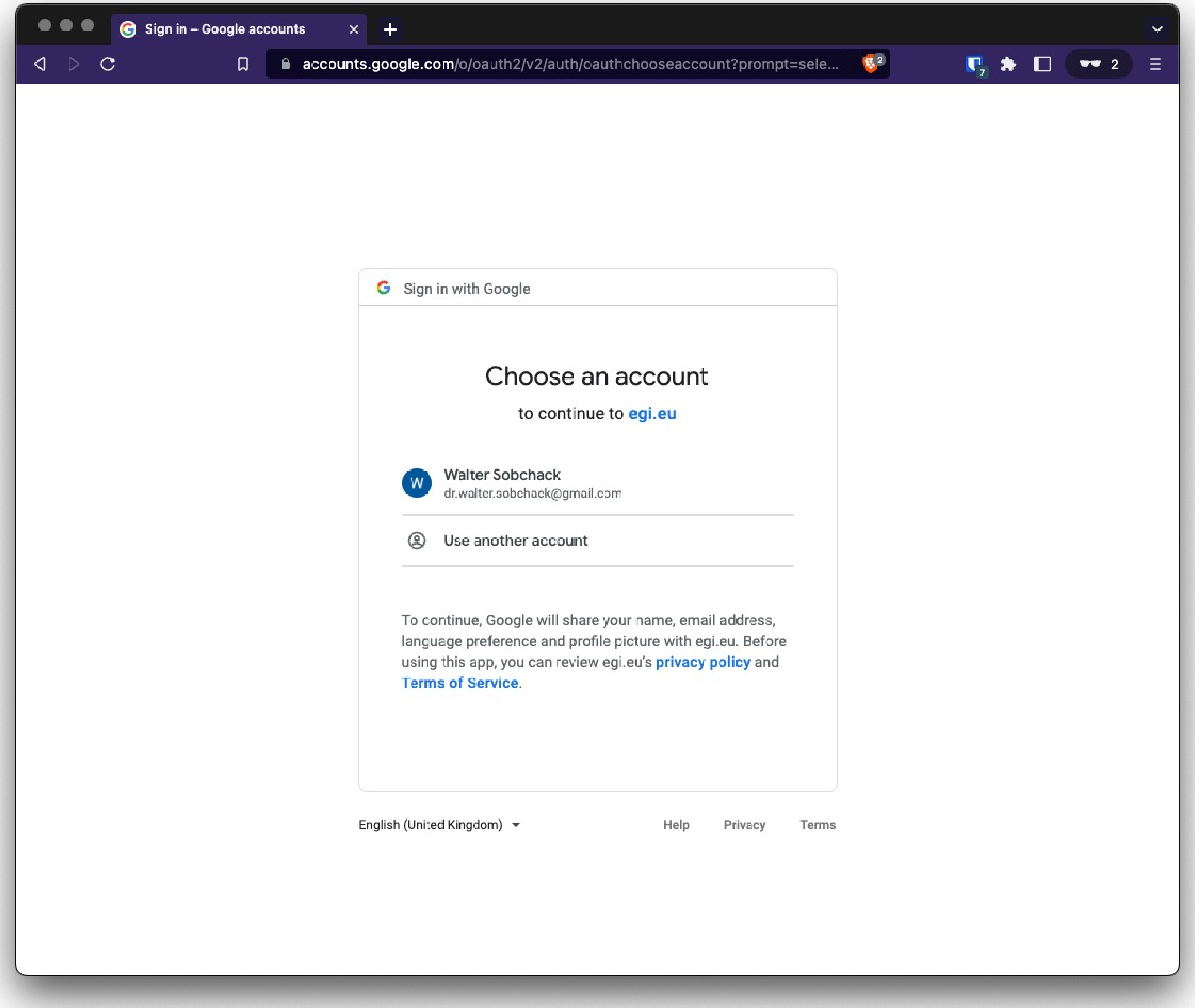
Contact info

Email: dr.walter.sobchack@gmail.com

#2 getting a Check-in account associated with the GMail account

Check-in account is one email verification away

- Registering and managing EGI Check-in account at https://aai.egi.eu/registry



Sign in – Google accounts

accounts.google.com/o/oauth2/v2/auth/oauthchooseaccount?prompt=sele...

Sign in with Google

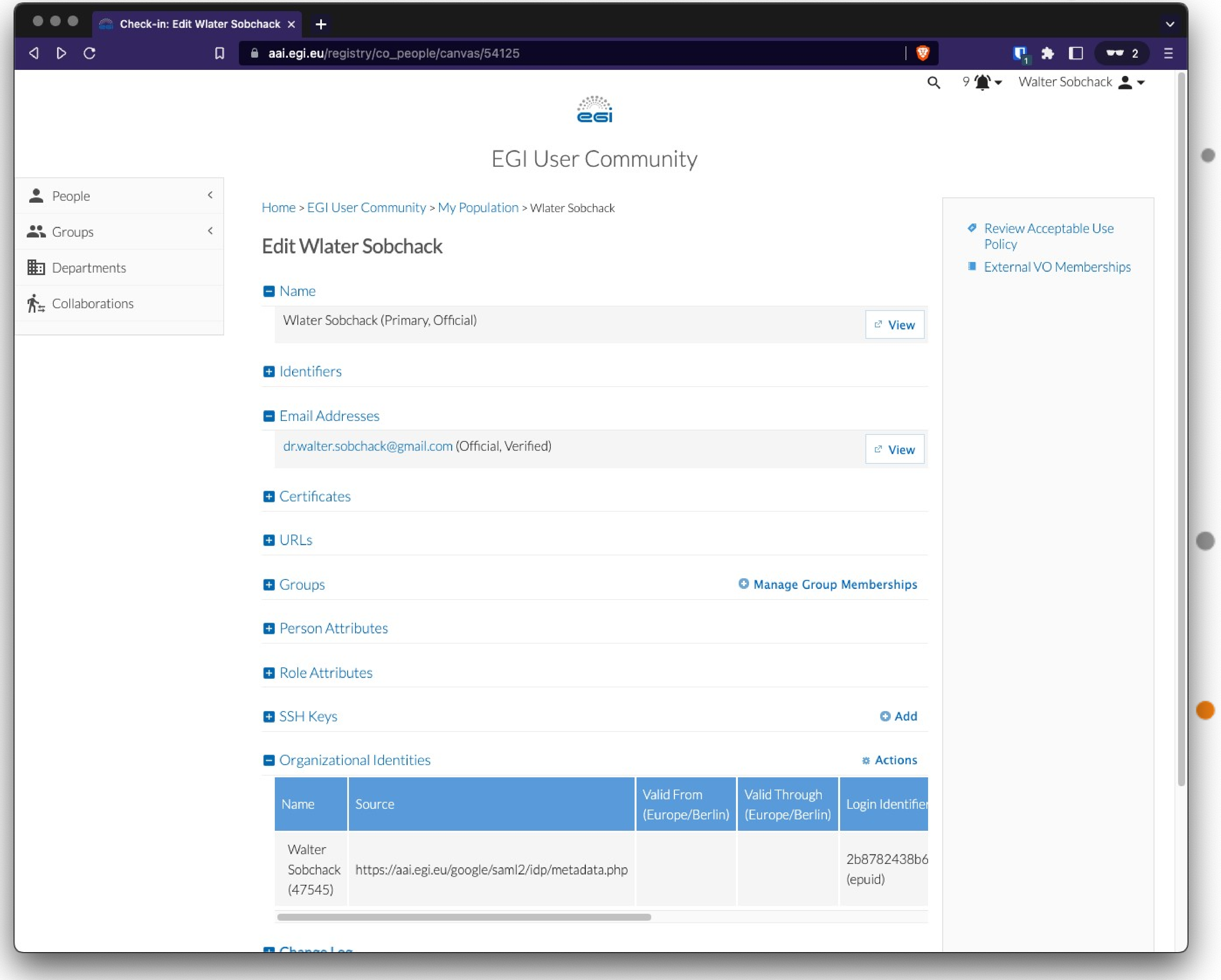
Choose an account

to continue to egi.eu

Walter Sobchack
dr.walter.sobchack@gmail.com

Use another account

To continue, Google will share your name, email address, language preference and profile picture with egi.eu. Before using this app, you can review egi.eu's privacy policy and Terms of Service.



Check-in: Edit Wlater Sobchack

aai.egi.eu/registry/co_people/canvas/54125

EGI User Community

Home > EGI User Community > My Population > Wlater Sobchack

Edit Wlater Sobchack

Name

Wlater Sobchack (Primary, Official) View

Identifiers

Email Addresses

dr.walter.sobchack@gmail.com (Official, Verified) View

Certificates

URLs

Groups — Manage Group Memberships

Person Attributes

Role Attributes

SSH Keys — Add

Organizational Identities — Actions

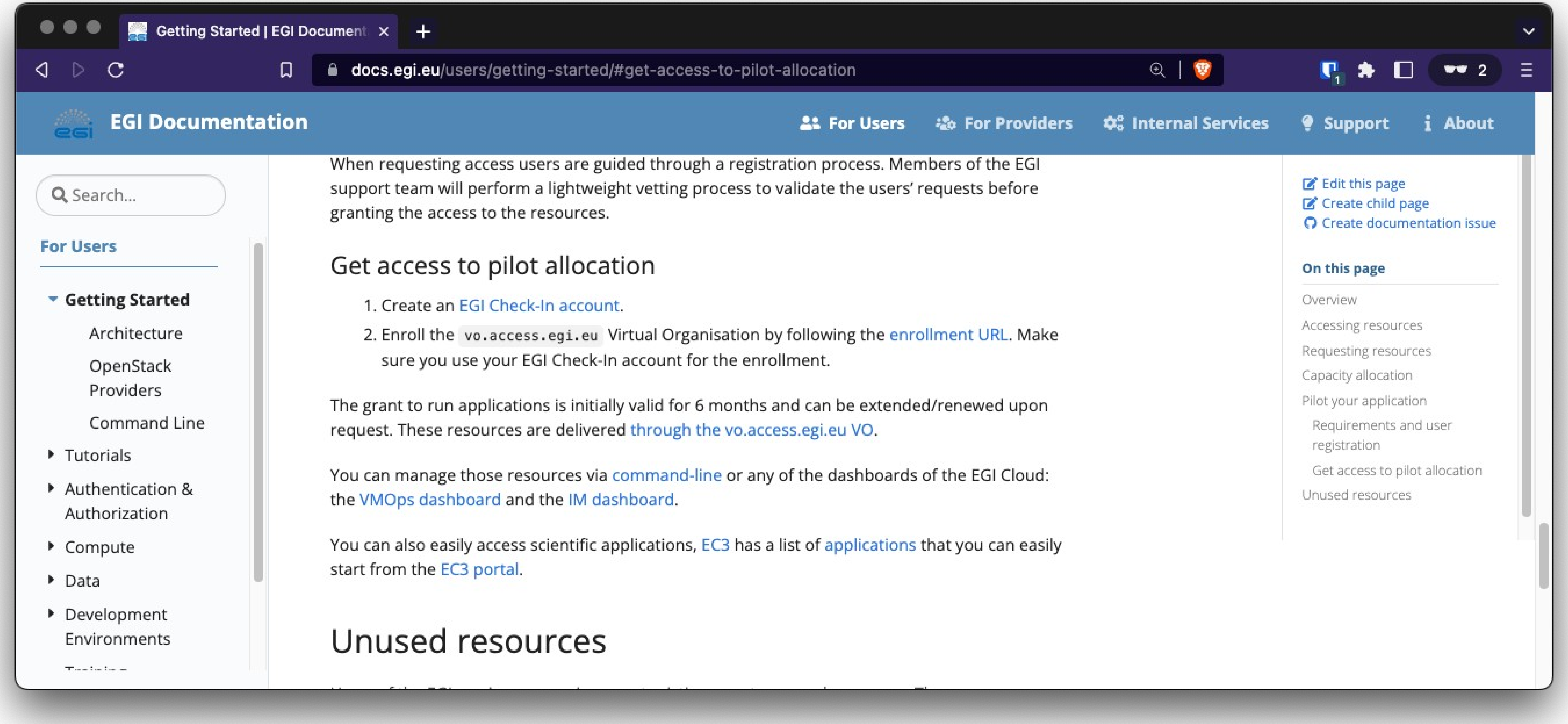
Name	Source	Valid From (Europe/Berlin)	Valid Through (Europe/Berlin)	Login Identifie
Walter Sobchack (47545)	https://aai.egi.eu/google/saml2/idp/metadata.php			2b8782438b6 (epuid)

Change Log

#3: enrolling to a VO for piloting activities

Looking for "easily" available resources

- See https://docs.egi.eu/users/getting-started/#get-access-to-pilot-allocation



When requesting access users are guided through a registration process. Members of the EGI support team will perform a lightweight vetting process to validate the users' requests before granting the access to the resources.

Get access to pilot allocation

1. Create an EGI Check-In account.
2. Enroll the `vo.access.egi.eu` Virtual Organisation by following the enrollment URL. Make sure you use your EGI Check-In account for the enrollment.

The grant to run applications is initially valid for 6 months and can be extended/renewed upon request. These resources are delivered through the vo.access.egi.eu VO.

You can manage those resources via command-line or any of the dashboards of the EGI Cloud: the VMOps dashboard and the IM dashboard.

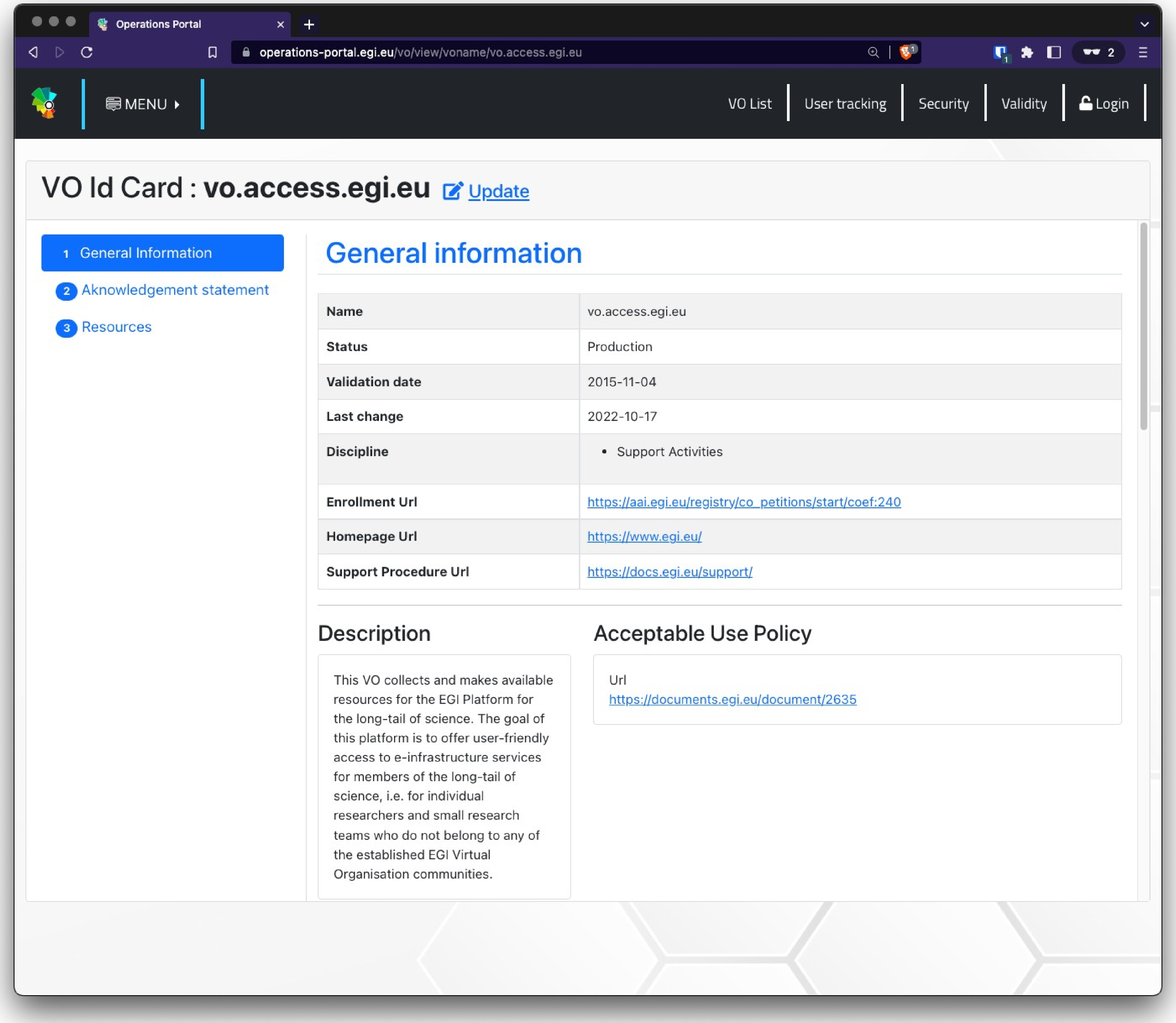
You can also easily access scientific applications, EC3 has a list of applications that you can easily start from the EC3 portal.

Unused resources

#3: enrolling to a VO for piloting activities

vo.access.egi.eu: a Check-in managed and cloud-enabled VO for piloting activities and the Long Tail of Science

- VO ID Card: https://operations-portal.egi.eu/vo/view/voname/vo.access.egi.eu
- VO managers from EGI Foundation
  - EGI Community Support Team (CST)
    - https://www.egi.eu/egi-foundation/team/#cst
  - EGI Technical Solutions Team (TST)
    - https://www.egi.eu/egi-foundation/team/#tst
  - Members on duty following a rota
  - Reviewing and vetting access requests
  - According to a clearly defined vetting procedure



VO Id Card : **vo.access.egi.eu** Update

General information

Name	vo.access.egi.eu
Status	Production
Validation date	2015-11-04
Last change	2022-10-17
Discipline	• Support Activities
Enrollment Url	https://aai.egi.eu/registry/co_petitions/start/coef:240
Homepage Url	https://www.egi.eu/
Support Procedure Url	https://docs.egi.eu/support/

Description

This VO collects and makes available resources for the EGI Platform for the long-tail of science. The goal of this platform is to offer user-friendly access to e-infrastructure services for members of the long-tail of science, i.e. for individual researchers and small research teams who do not belong to any of the established EGI Virtual Organisation communities.

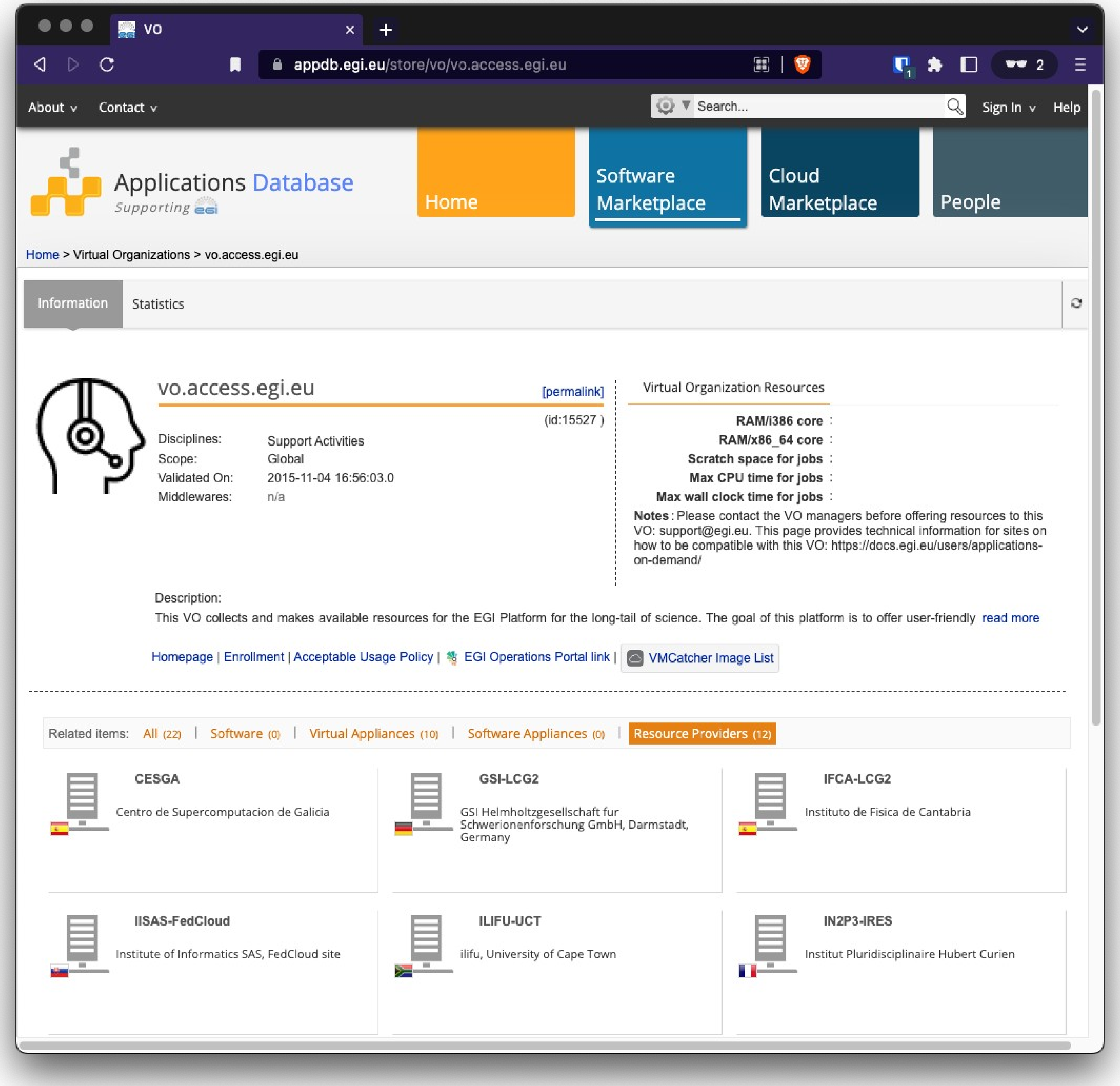
Acceptable Use Policy

Url
https://documents.egi.eu/document/2635

#3: enrolling to a VO for piloting activities

Investigating public information about the VO

- Cloud Compute EGI Service: https://docs.egi.eu/users/compute/cloud-compute/
  - ○ Supporting sites, images and flavours: https://appdb.egi.eu/store/vo/vo.access.egi.eu



Home > Virtual Organizations > vo.access.egi.eu

vo.access.egi.eu [permalink]
(id:15527)

Disciplines: Support Activities
Scope: Global
Validated On: 2015-11-04 16:56:03.0
Middlewares: n/a

Virtual Organization Resources

RAM/i386 core :
RAM/x86_64 core :
Scratch space for jobs :
Max CPU time for jobs :
Max wall clock time for jobs :

Notes : Please contact the VO managers before offering resources to this VO: support@egi.eu. This page provides technical information for sites on how to be compatible with this VO: https://docs.egi.eu/users/applications-on-demand/

Description:
This VO collects and makes available resources for the EGI Platform for the long-tail of science. The goal of this platform is to offer user-friendly read more

Homepage | Enrollment | Acceptable Usage Policy | EGI Operations Portal link | VMCatcher Image List

Related items: All (22) | Software (0) | Virtual Appliances (10) | Software Appliances (0) | Resource Providers (12)

CESGA
Centro de Supercomputacion de Galicia

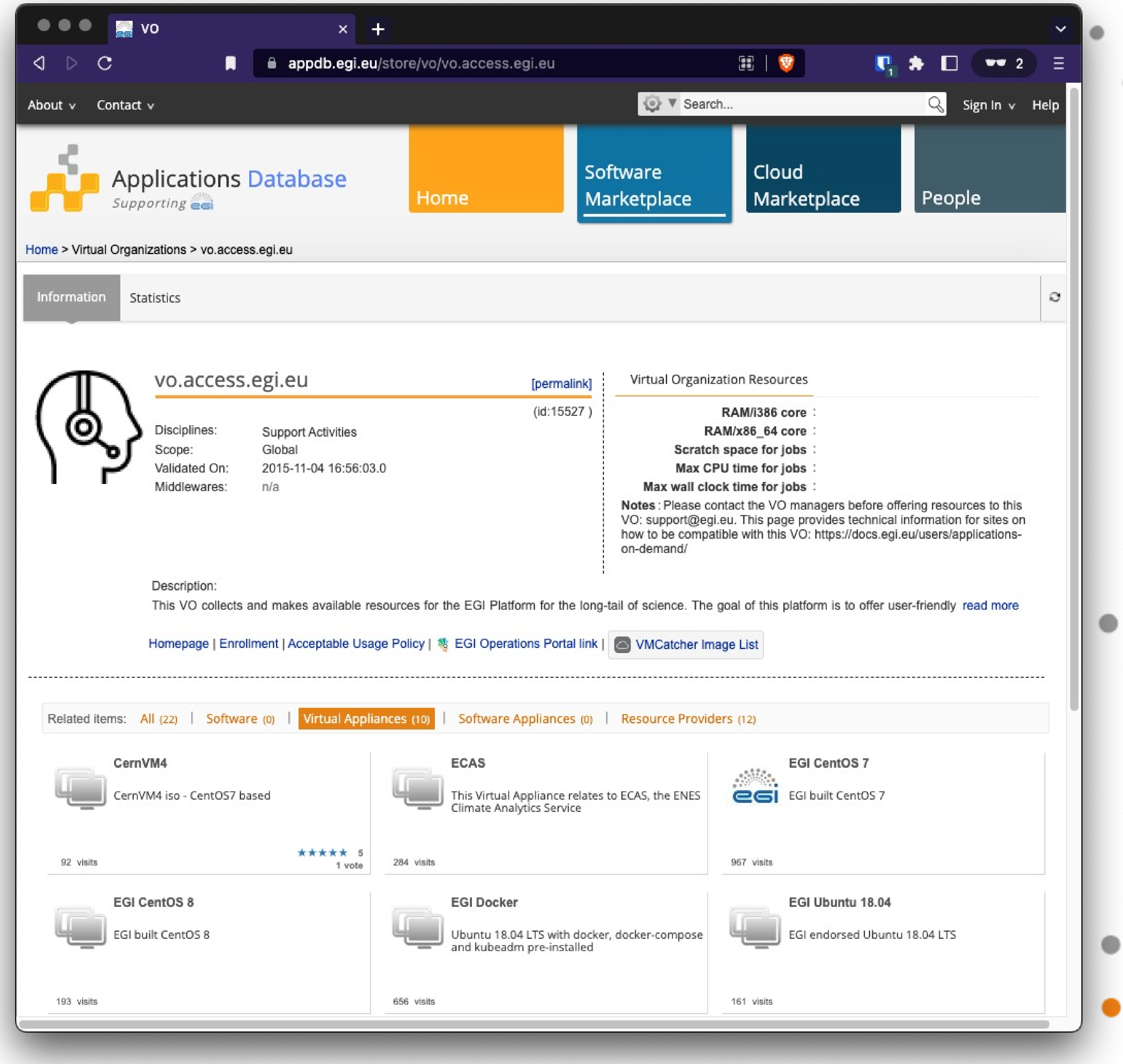
GSI-LCG2
GSI Helmholtzgesellschaft fur Schwerionenforschung GmbH, Darmstadt, Germany

IFCA-LCG2
Instituto de Fisica de Cantabria

IISAS-FedCloud
Institute of Informatics SAS, FedCloud site

ILIFU-UCT
ilifu, University of Cape Town

IN2P3-IRES
Institut Pluridisciplinaire Hubert Curien


VO
appdb.egi.eu/store/vo/vo.access.egi.eu
About Contact Search... Sign In Help
Applications Database Supporting
Home Software Marketplace Cloud Marketplace People
Home > Virtual Organizations > vo.access.egi.eu
Information Statistics
vo.access.egi.eu [permalink]
(id:15527)
Disciplines: Support Activities
Scope: Global
Validated On: 2015-11-04 16:56:03.0
Middlewares: n/a
Virtual Organization Resources
RAM/i386 core :
RAM/x86_64 core :
Scratch space for jobs :
Max CPU time for jobs :
Max wall clock time for jobs :
Notes : Please contact the VO managers before offering resources to this VO: support@egi.eu. This page provides technical information for sites on how to be compatible with this VO: https://docs.egi.eu/users/applications-on-demand/
Description:
This VO collects and makes available resources for the EGI Platform for the long-tail of science. The goal of this platform is to offer user-friendly read more
Homepage | Enrollment | Acceptable Usage Policy | EGI Operations Portal link | VMCatcher Image List

Related items: All (22) | Software (0) | Virtual Appliances (10) | Software Appliances (0) | Resource Providers (12)

CernVM4
CernVM4 iso - CentOS7 based
92 visits ★★★★★ 5
1 vote

ECAS
This Virtual Appliance relates to ECAS, the ENES Climate Analytics Service
284 visits

EGI CentOS 7
EGI built CentOS 7
967 visits

EGI CentOS 8
EGI built CentOS 8
193 visits

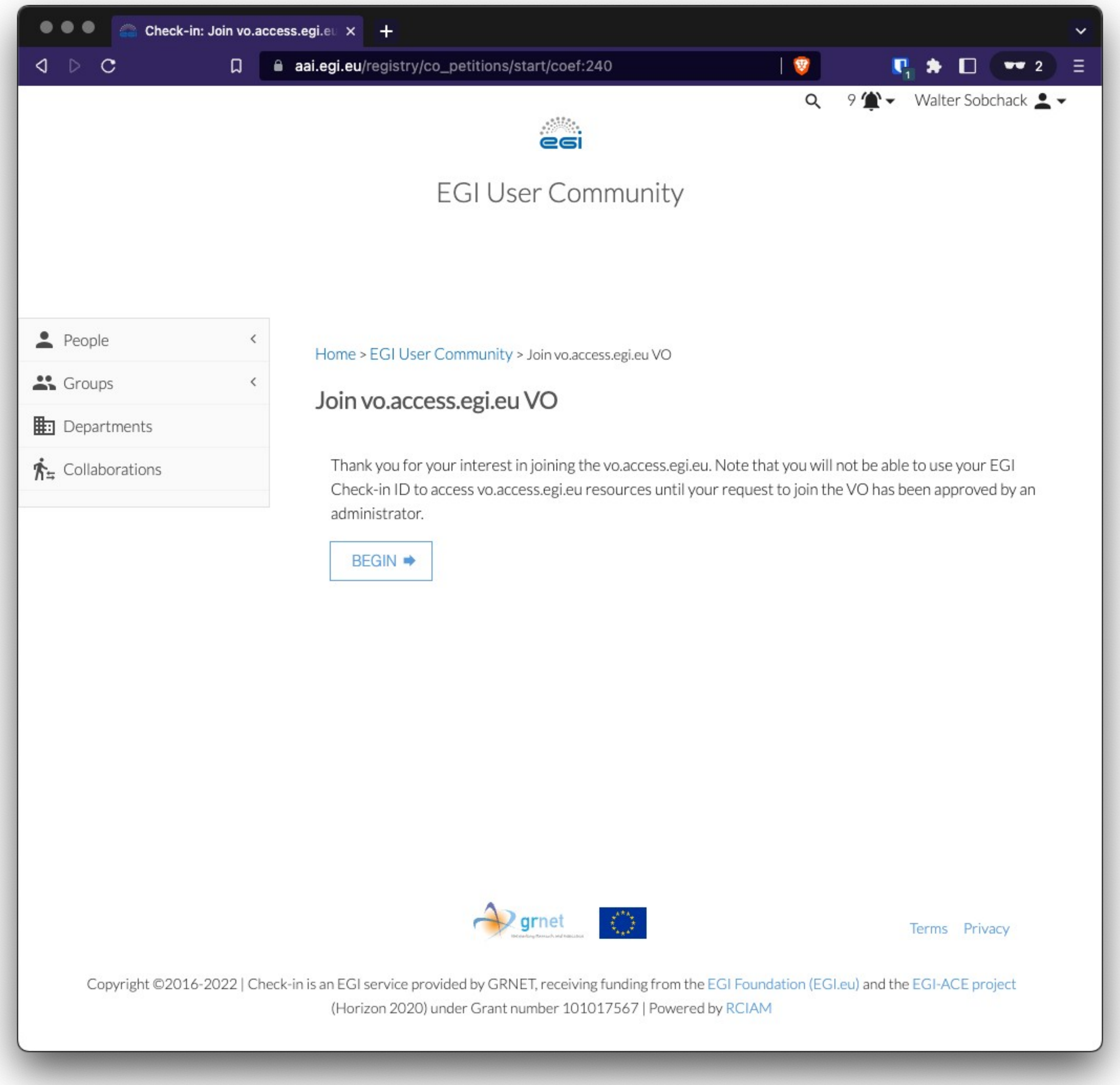
EGI Docker
Ubuntu 18.04 LTS with docker, docker-compose and kubeadm pre-installed
656 visits

EGI Ubuntu 18.04
EGI endorsed Ubuntu 18.04 LTS
161 visits

#3: enrolling to a VO for piloting activities

Using Check-in to enroll to the VO

- **Enrolling**: https://aai.egi.eu/registry/co_petitions/start/coef:240


Check-in: Join vo.access.egi.eu
aai.egi.eu/registry/co_petitions/start/coef:240
9
Walter Sobchack
People
Groups
Departments
Collaborations
BEGIN
grnet
Terms
Privacy

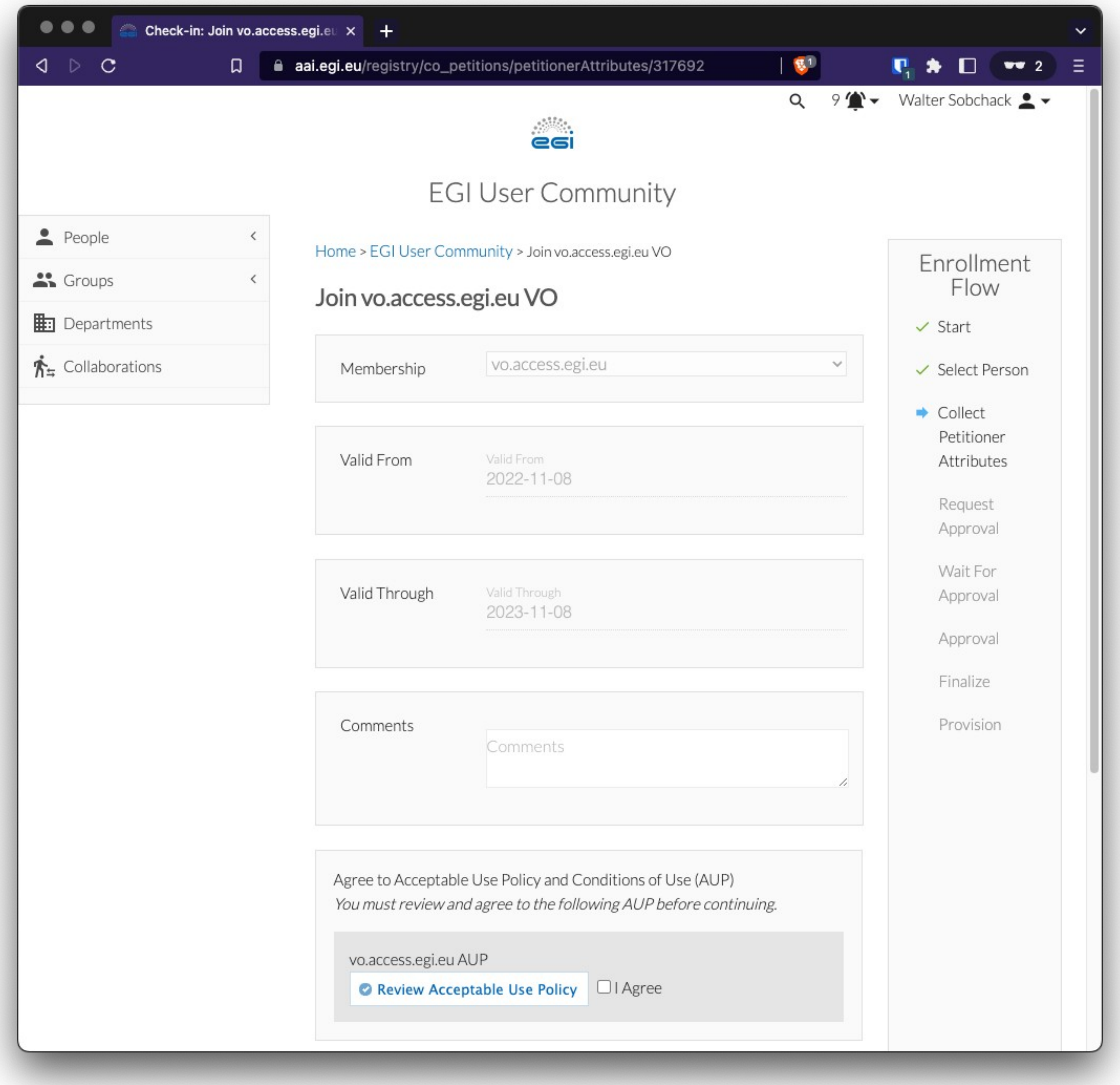
EGI User Community

Home > EGI User Community > Join vo.access.egi.eu VO

Join vo.access.egi.eu VO

Thank you for your interest in joining the vo.access.egi.eu. Note that you will not be able to use your EGI Check-in ID to access vo.access.egi.eu resources until your request to join the VO has been approved by an administrator.

Copyright ©2016-2022 | Check-in is an EGI service provided by GRNET, receiving funding from the EGI Foundation (EGI.eu) and the EGI-ACE project (Horizon 2020) under Grant number 101017567 | Powered by RCIAM


Check-in: Join vo.access.egi.eu
aai.egi.eu/registry/co_petitions/petitionerAttributes/317692
9
Walter Sobchack
People
Groups
Departments
Collaborations
Review Acceptable Use Policy

EGI User Community

Home > EGI User Community > Join vo.access.egi.eu VO

Join vo.access.egi.eu VO

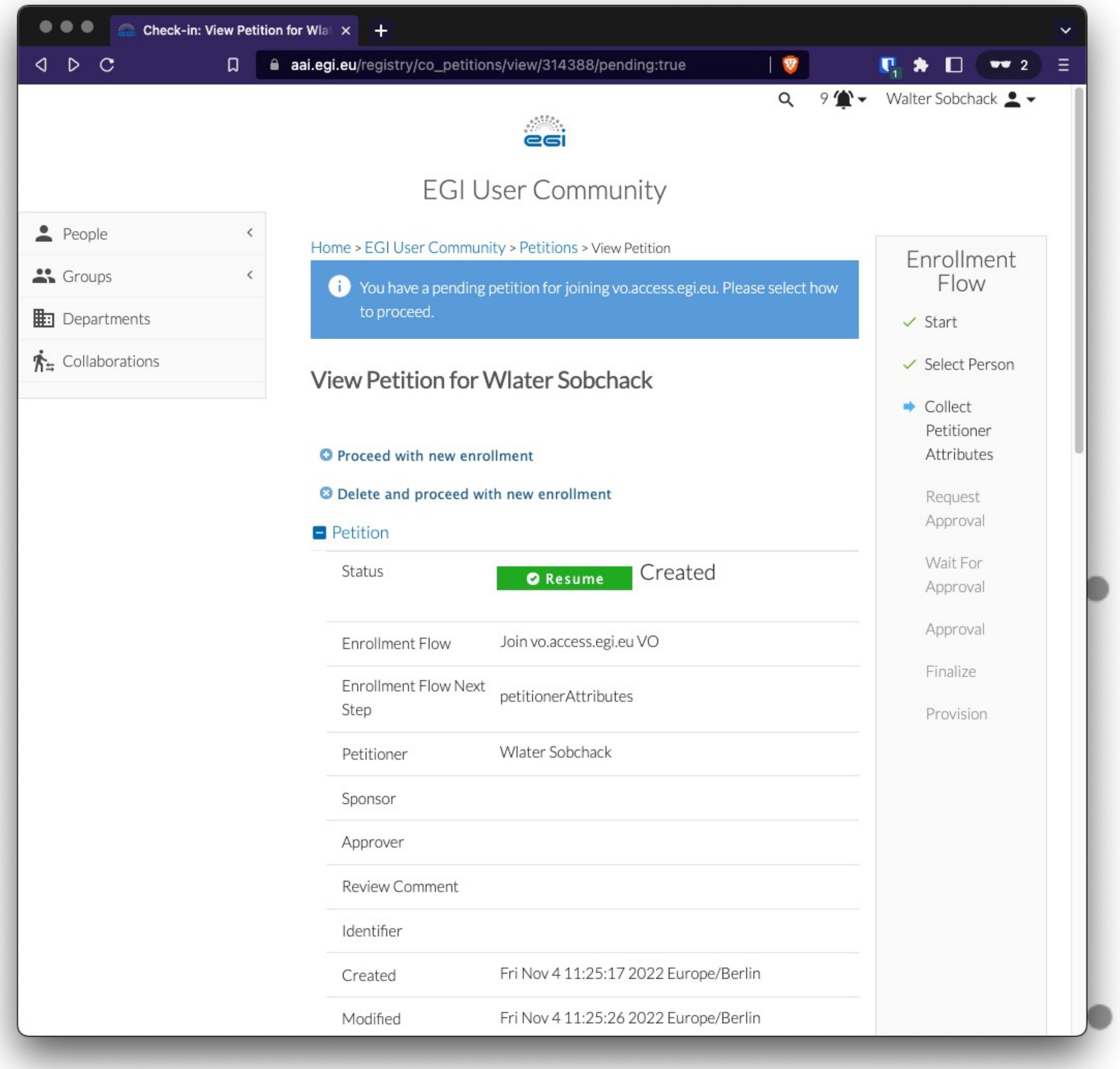
Membership	vo.access.egi.eu
Valid From	Valid From 2022-11-08
Valid Through	Valid Through 2023-11-08
Comments	Comments

Agree to Acceptable Use Policy and Conditions of Use (AUP)
You must review and agree to the following AUP before continuing.

vo.access.egi.eu AUP

□ I Agree

Enrollment Flow
- ✓ Start
- ✓ Select Person
- Collect Petitioner Attributes
- Request Approval
- Wait For Approval
- Approval
- Finalize
- Provision


Check-in: View Petition for Wlat
aai.egi.eu/registry/co_petitions/view/314388/pending:true
9
Walter Sobchack
People
Groups
Departments
Collaborations
Proceed with new enrollment
Delete and proceed with new enrollment
Resume

EGI User Community

Home > EGI User Community > Petitions > View Petition

You have a pending petition for joining vo.access.egi.eu. Please select how to proceed.

View Petition for Wlater Sobchack

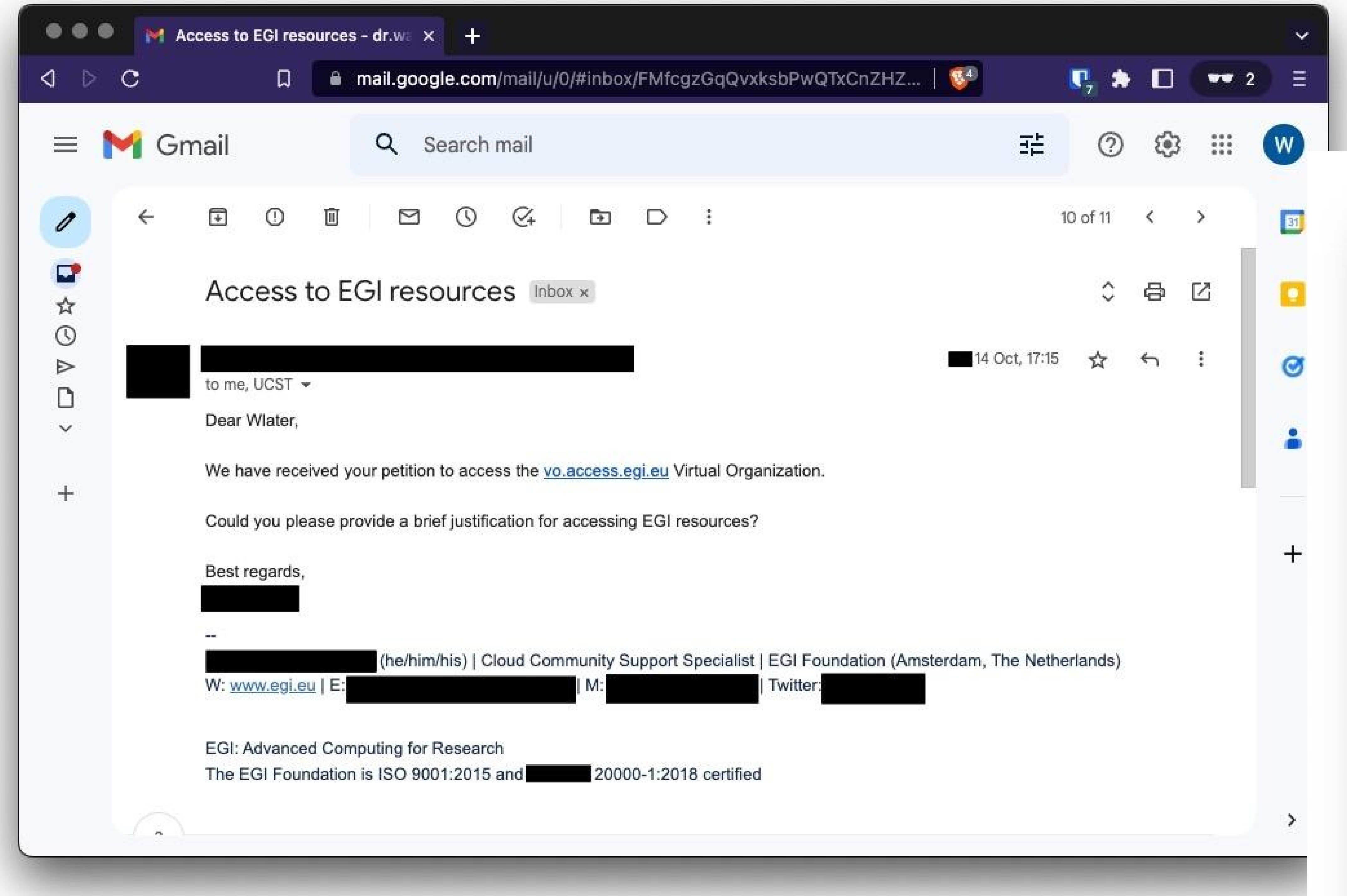
Petition

Status	Created
Enrollment Flow	Join vo.access.egi.eu VO
Enrollment Flow Next Step	petitionerAttributes
Petitioner	Wlater Sobchack
Sponsor	
Approver	
Review Comment	
Identifier	
Created	Fri Nov 4 11:25:17 2022 Europe/Berlin
Modified	Fri Nov 4 11:25:26 2022 Europe/Berlin

Enrollment Flow
- ✓ Start
- ✓ Select Person
- Collect Petitioner Attributes
- Request Approval
- Wait For Approval
- Approval
- Finalize
- Provision

#4: Going through the vetting process

Welcome message and discussing the justification for requesting resources


Access to EGI resources - dr.w
mail.google.com/mail/u/0/#inbox/FMfcgzGqQvxksbPwQTxCnZHZ...
Gmail
Search mail
10 of 11
Inbox ×

Access to EGI resources

[redacted]

[redacted] 14 Oct, 17:15

to me, UCST

Dear Wlater,

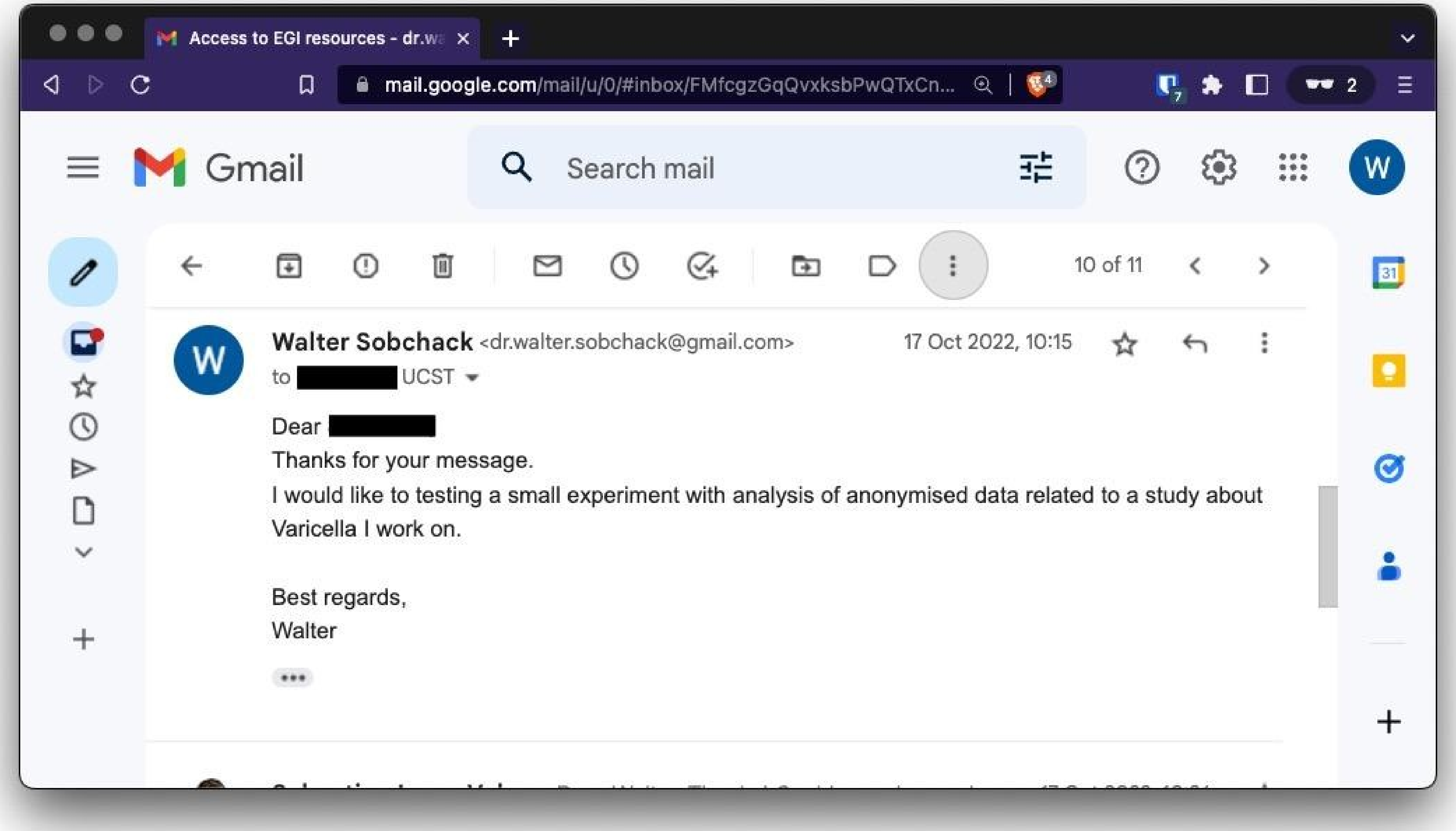
We have received your petition to access the vo.access.egi.eu Virtual Organization.

Could you please provide a brief justification for accessing EGI resources?

Best regards,
[redacted]

--
[redacted] (he/him/his) | Cloud Community Support Specialist | EGI Foundation (Amsterdam, The Netherlands)
W: www.egi.eu | E: [redacted] | M: [redacted] | Twitter: [redacted]

EGI: Advanced Computing for Research
The EGI Foundation is ISO 9001:2015 and [redacted] 20000-1:2018 certified


Access to EGI resources - dr.w
mail.google.com/mail/u/0/#inbox/FMfcgzGqQvxksbPwQTxCn...
Gmail
Search mail
10 of 11

Walter Sobchack <dr.walter.sobchack@gmail.com> 17 Oct 2022, 10:15

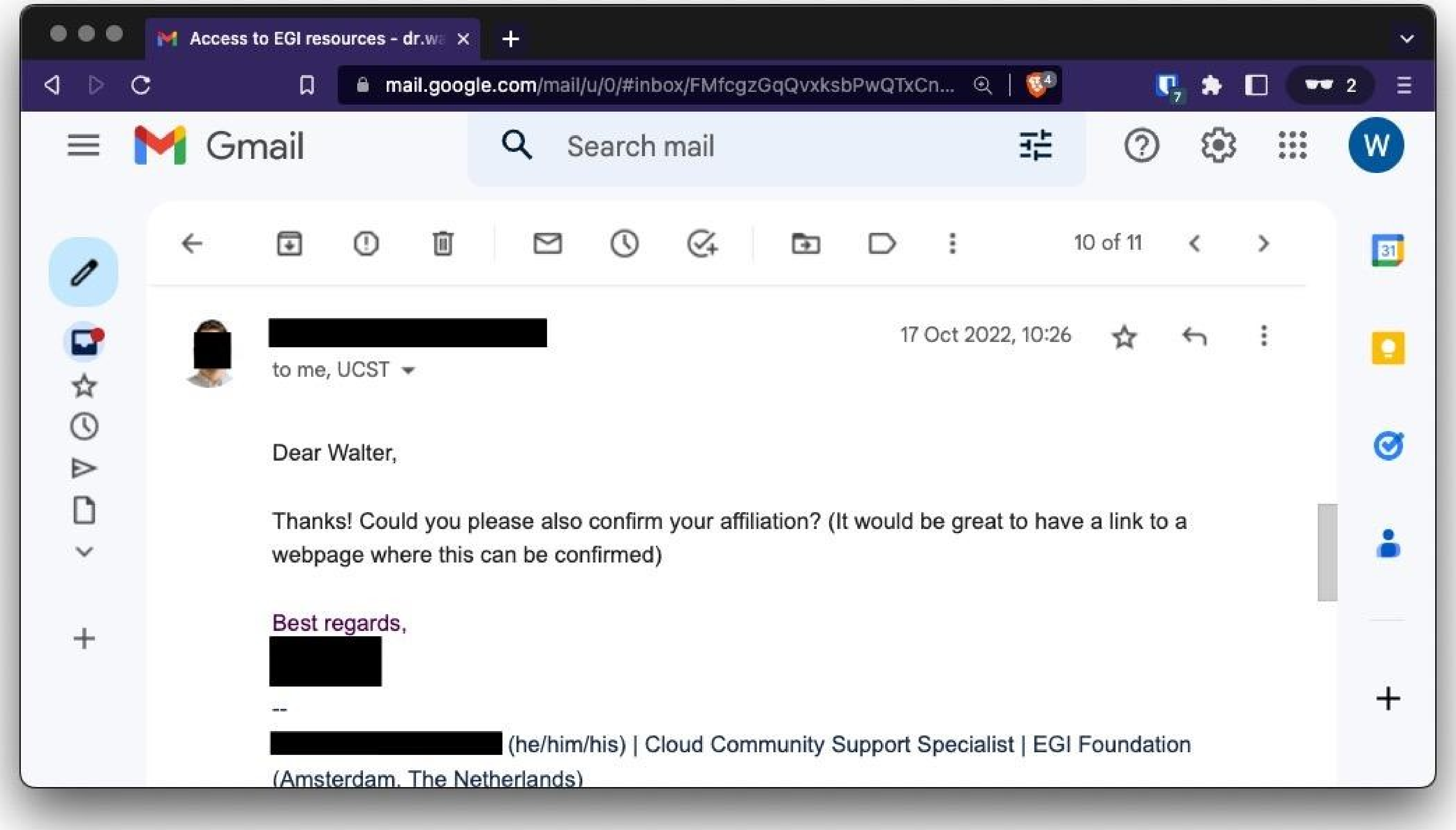
to [redacted] UCST

Dear [redacted]
Thanks for your message.
I would like to testing a small experiment with analysis of anonymised data related to a study about Varicella I work on.

Best regards,
Walter

#4: Going through the vetting process

Checking the Affiliation. Pointing to Dr Sobchak's research on ResearchGate...


Access to EGI resources - dr.w
mail.google.com/mail/u/0/#inbox/FMfcgzGqQvxksbPwQTxCn...
Gmail
Search mail
10 of 11

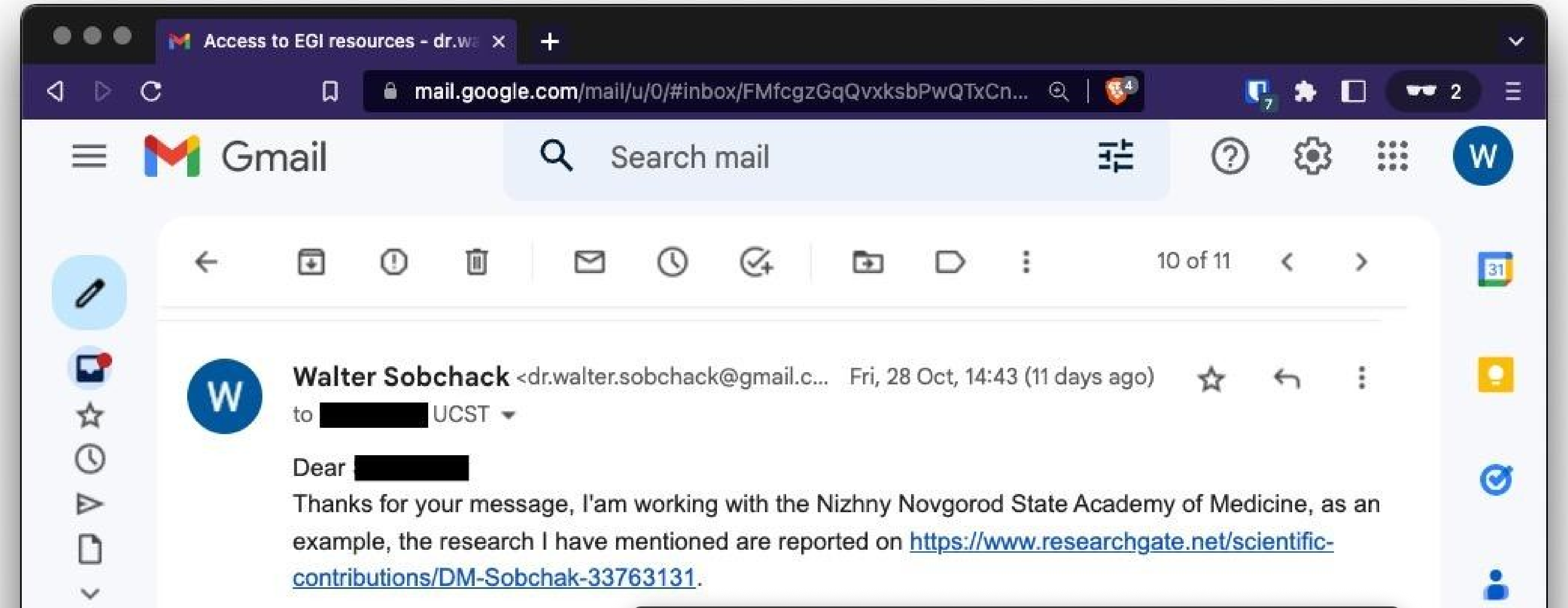
[redacted]
to me, UCST
17 Oct 2022, 10:26

Dear Walter,

Thanks! Could you please also confirm your affiliation? (It would be great to have a link to a webpage where this can be confirmed)

Best regards,
[redacted]
--
[redacted] (he/him/his) | Cloud Community Support Specialist | EGI Foundation
(Amsterdam, The Netherlands)

[DM Sobchak's research while affiliated with Nizhny Novgorod State Academy of M edicine and other places]

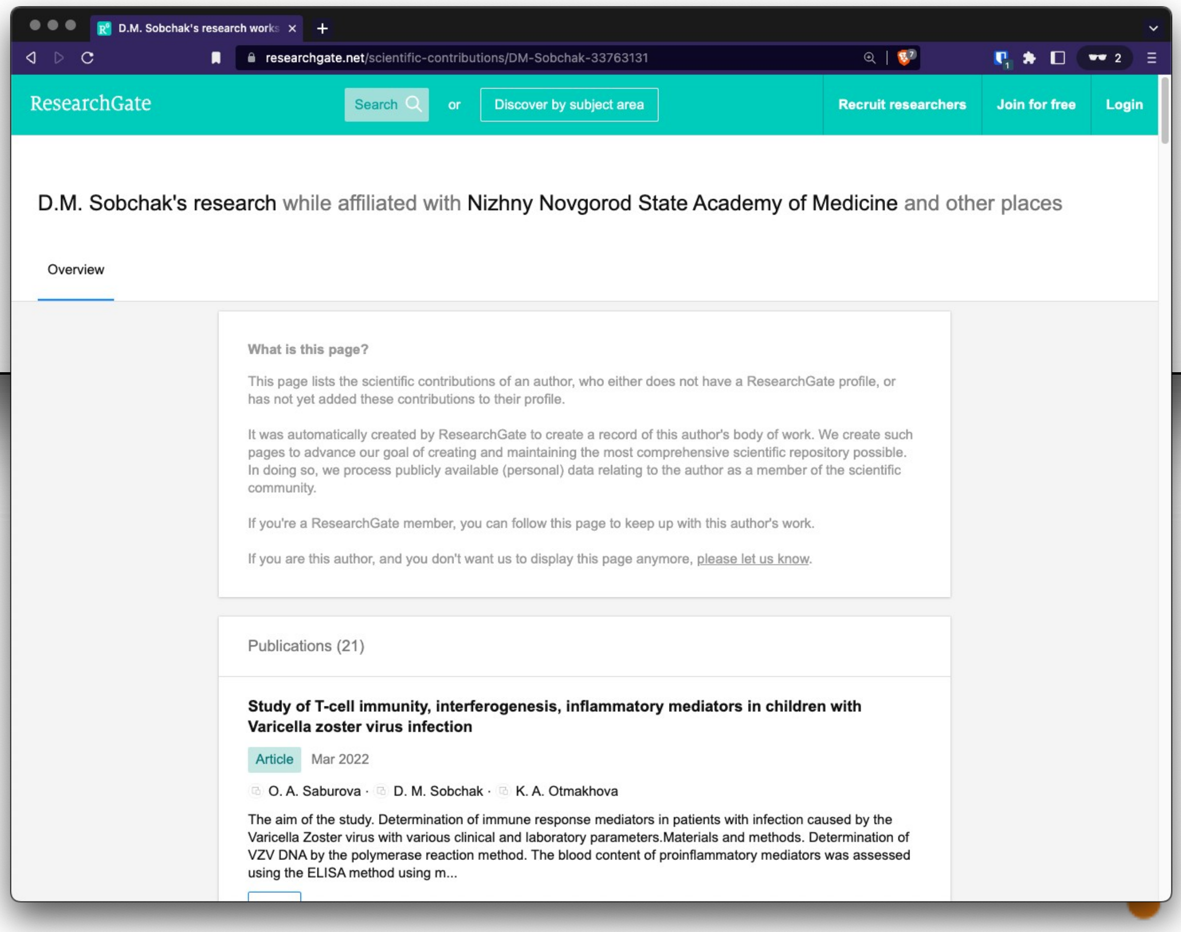

Access to EGI resources - dr.w
mail.google.com/mail/u/0/#inbox/FMfcgzGqQvxksbPwQTxCn...
Gmail
Search mail
10 of 11

Walter Sobchack <dr.walter.sobchack@gmail.c... Fri, 28 Oct, 14:43 (11 days ago)
to [redacted] UCST

Dear [redacted]
Thanks for your message, I'am working with the Nizhny Novgorod State Academy of Medicine, as an example, the research I have mentioned are reported on https://www.researchgate.net/scientific-contributions/DM-Sobchak-33763131.

Thanks for your support!

Best regards,
Walter


D.M. Sobchak's research works
researchgate.net/scientific-contributions/DM-Sobchak-33763131
ResearchGate
Search
or
Discover by subject area
Recruit researchers
Join for free
Login
Overview

D.M. Sobchak's research while affiliated with Nizhny Novgorod State Academy of Medicine and other places

What is this page?

This page lists the scientific contributions of an author, who either does not have a ResearchGate profile, or has not yet added these contributions to their profile.

It was automatically created by ResearchGate to create a record of this author's body of work. We create such pages to advance our goal of creating and maintaining the most comprehensive scientific repository possible. In doing so, we process publicly available (personal) data relating to the author as a member of the scientific community.

If you're a ResearchGate member, you can follow this page to keep up with this author's work.

If you are this author, and you don't want us to display this page anymore, please let us know.

Publications (21)

Study of T-cell immunity, interferogenesis, inflammatory mediators in children with Varicella zoster virus infection

Article Mar 2022

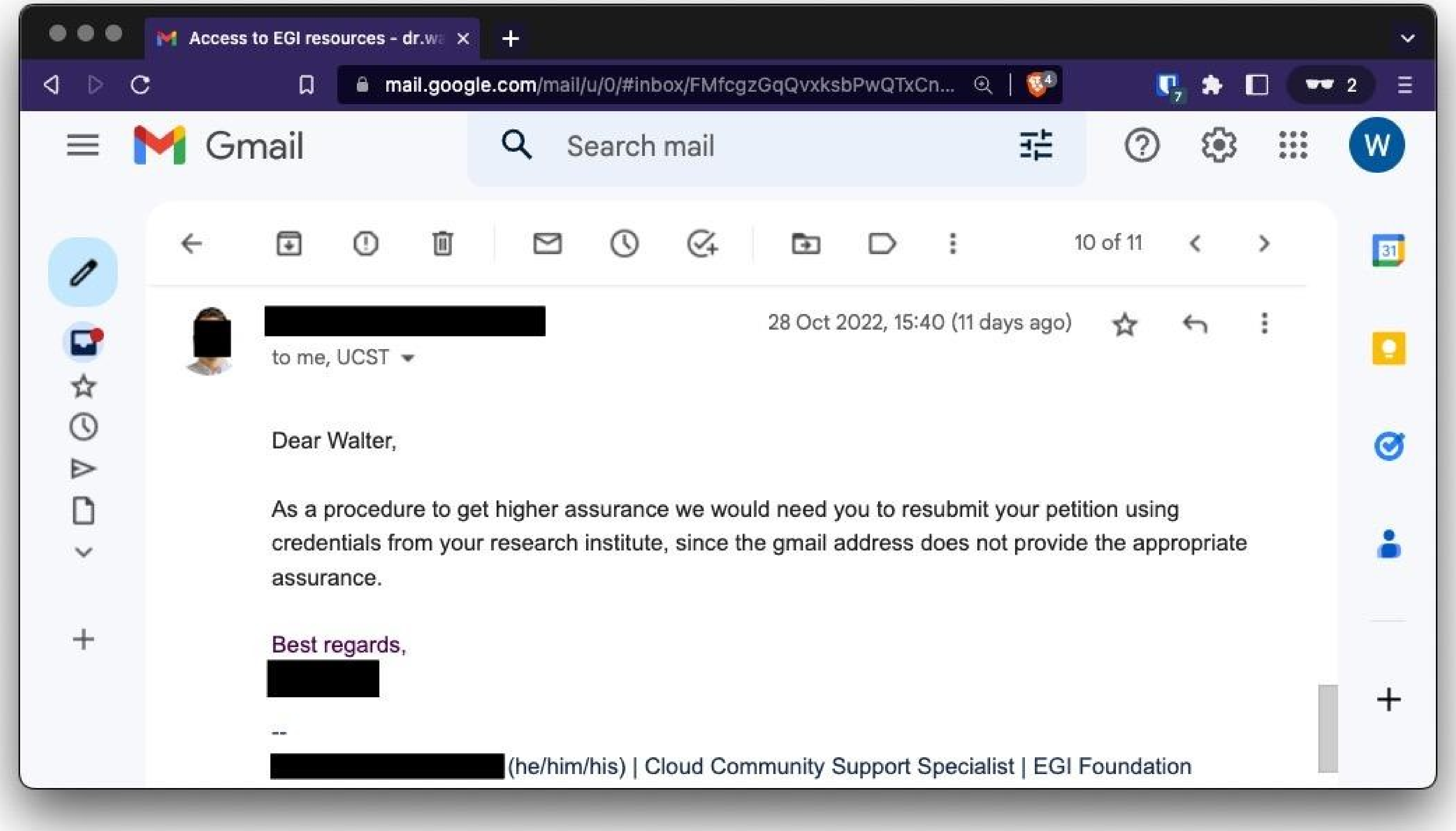
O. A. Saburova · D. M. Sobchak · K. A. Otmakhova

The aim of the study. Determination of immune response mediators in patients with infection caused by the Varicella Zoster virus with various clinical and laboratory parameters.Materials and methods. Determination of VZV DNA by the polymerase reaction method. The blood content of proinflammatory mediators was assessed using the ELISA method using m...

#4: Going through the vetting process

Not enough trust, please use a higher assurance level Identity Provider

- Well done guys, better not let me in!


Access to EGI resources - dr.w
mail.google.com/mail/u/0/#inbox/FMfcgzGqQvxksbPwQTxCn...
Gmail
Search mail
10 of 11
W

[redacted]

to me, UCST

28 Oct 2022, 15:40 (11 days ago)

Dear Walter,

As a procedure to get higher assurance we would need you to resubmit your petition using credentials from your research institute, since the gmail address does not provide the appropriate assurance.

Best regards,

[redacted]

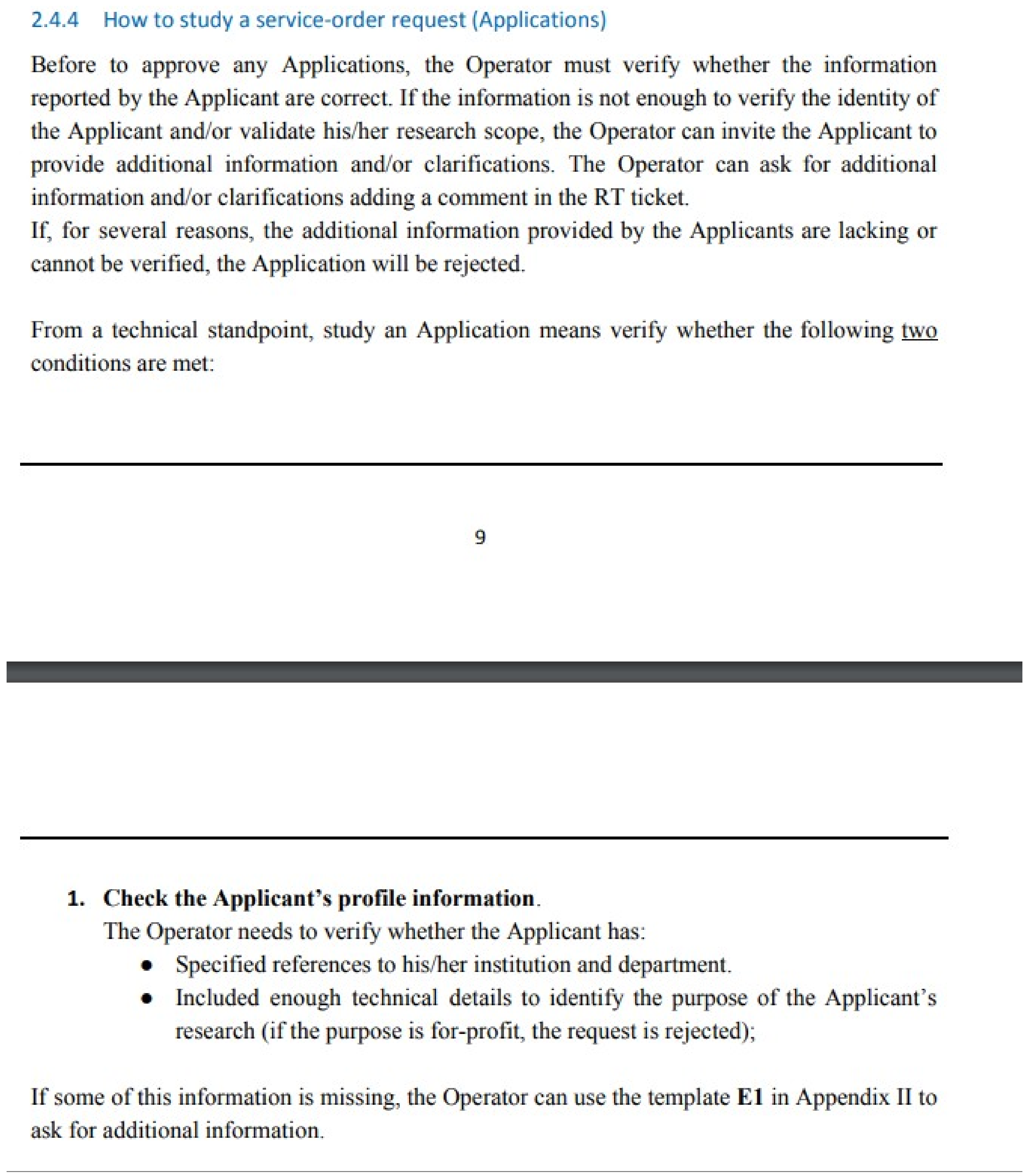
--

[redacted] (he/him/his) | Cloud Community Support Specialist | EGI Foundation

#4: A few details about the legacy EGI AoDS vetting process

Vetting process for the legacy Applications on Demand Service (AoDS)

- **EGI Applications on Demand - Documentation for operator**
  - https://documents.egi.eu/document/3127



2.4.4 How to study a service-order request (Applications)

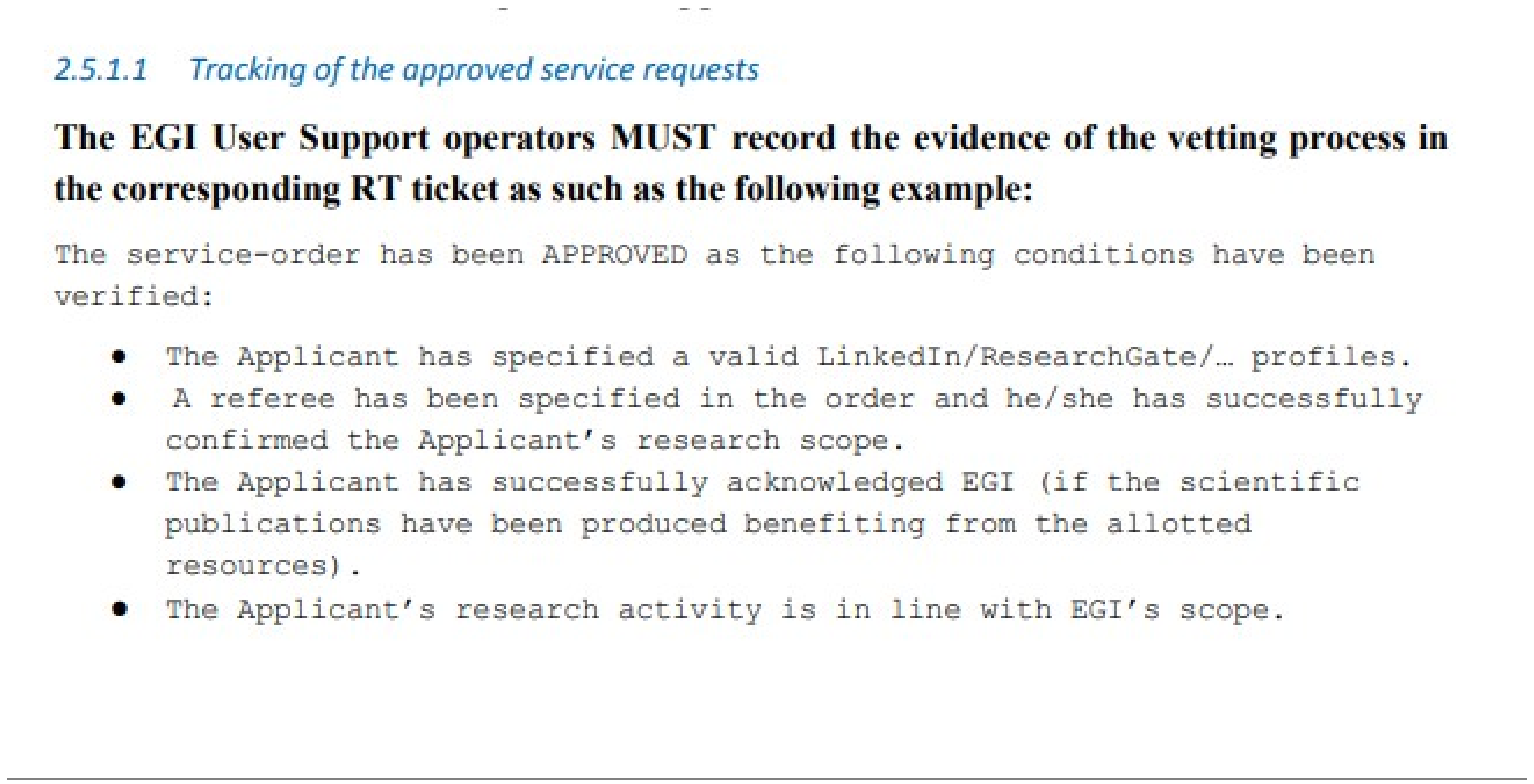
Before to approve any Applications, the Operator must verify whether the information reported by the Applicant are correct. If the information is not enough to verify the identity of the Applicant and/or validate his/her research scope, the Operator can invite the Applicant to provide additional information and/or clarifications. The Operator can ask for additional information and/or clarifications adding a comment in the RT ticket.
If, for several reasons, the additional information provided by the Applicants are lacking or cannot be verified, the Application will be rejected.

From a technical standpoint, study an Application means verify whether the following two conditions are met:

9

1. **Check the Applicant's profile information**.
   The Operator needs to verify whether the Applicant has:
   - Specified references to his/her institution and department.
   - Included enough technical details to identify the purpose of the Applicant's research (if the purpose is for-profit, the request is rejected);

If some of this information is missing, the Operator can use the template **E1** in Appendix II to ask for additional information.



2.5.1.1 Tracking of the approved service requests

The EGI User Support operators MUST record the evidence of the vetting process in the corresponding RT ticket as such as the following example:

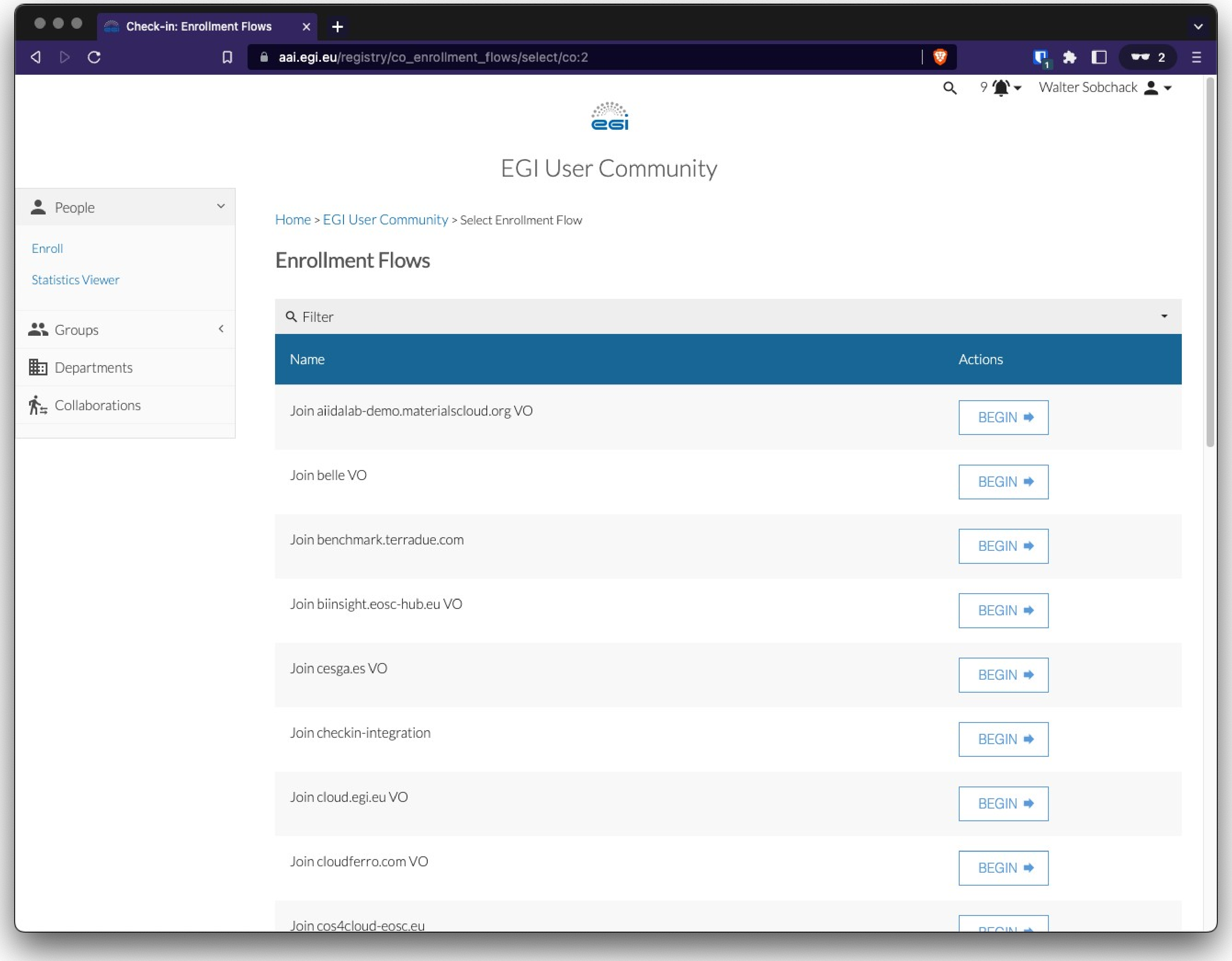
```
The service-order has been APPROVED as the following conditions have been
verified:

  •  The Applicant has specified a valid LinkedIn/ResearchGate/… profiles.
  •   A referee has been specified in the order and he/she has successfully
     confirmed the Applicant's research scope.
  •  The Applicant has successfully acknowledged EGI (if the scientific
     publications have been produced benefiting from the allotted
     resources).
  •  The Applicant's research activity is in line with EGI's scope.
```

#5: Are we done?

Going through the list of available VO in Check-in, opened to self-enrollment

- Currently 118 available VO available for self enrollment



Check-in: Enrollment Flows

aai.egi.eu/registry/co_enrollment_flows/select/co:2

Walter Sobchack

EGI User Community

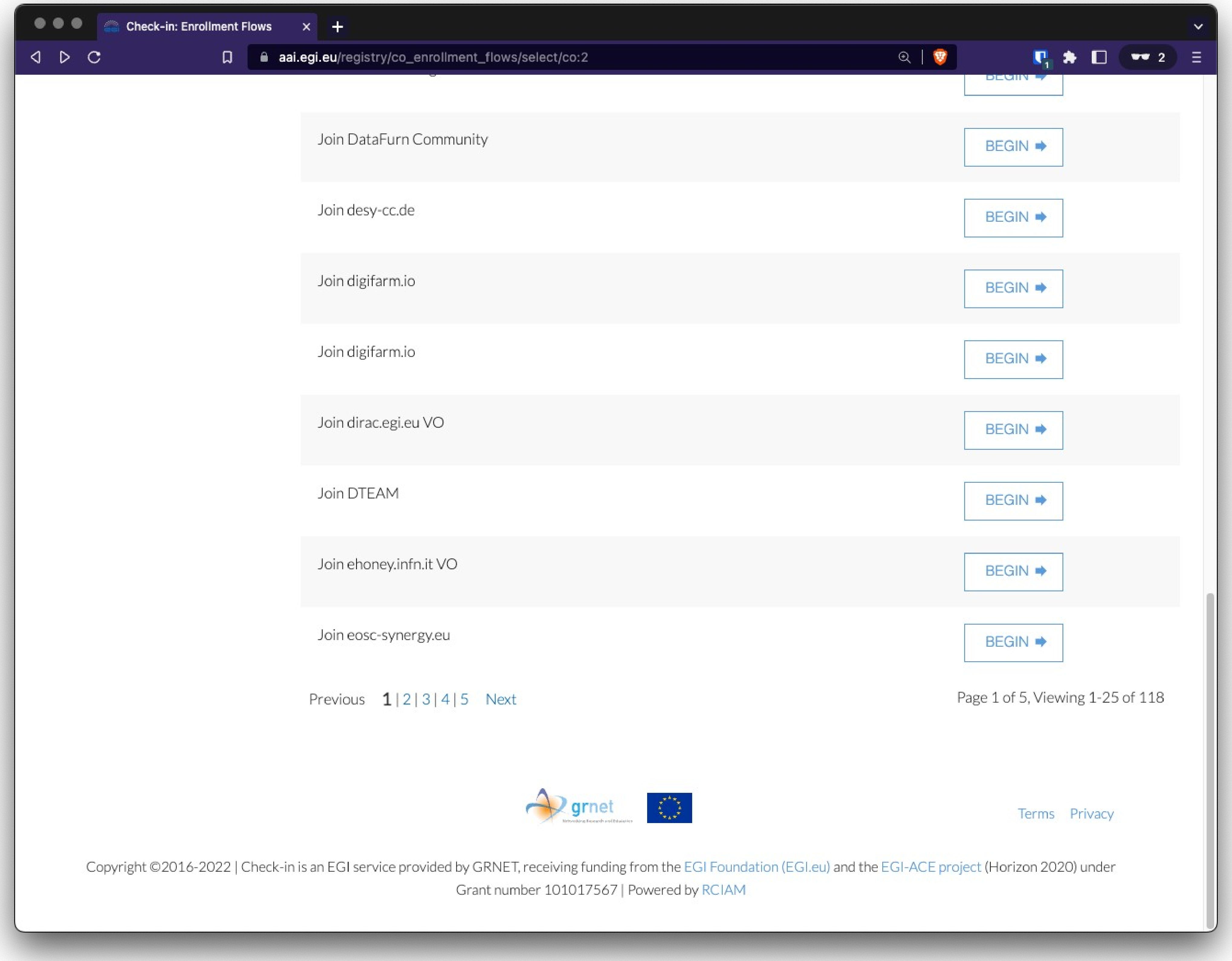
People
Enroll
Statistics Viewer
Groups
Departments
Collaborations

Home > EGI User Community > Select Enrollment Flow

Enrollment Flows

Filter

Name	Actions
Join aiidalab-demo.materialscloud.org VO	BEGIN
Join belle VO	BEGIN
Join benchmark.terradue.com	BEGIN
Join biinsight.eosc-hub.eu VO	BEGIN
Join cesga.es VO	BEGIN
Join checkin-integration	BEGIN
Join cloud.egi.eu VO	BEGIN
Join cloudferro.com VO	BEGIN
Join cos4cloud-eosc.eu	



Check-in: Enrollment Flows

aai.egi.eu/registry/co_enrollment_flows/select/co:2

Join DataFurn Community	BEGIN
Join desy-cc.de	BEGIN
Join digifarm.io	BEGIN
Join digifarm.io	BEGIN
Join dirac.egi.eu VO	BEGIN
Join DTEAM	BEGIN
Join ehoney.infn.it VO	BEGIN
Join eosc-synergy.eu	BEGIN

Previous 1 | 2 | 3 | 4 | 5 Next

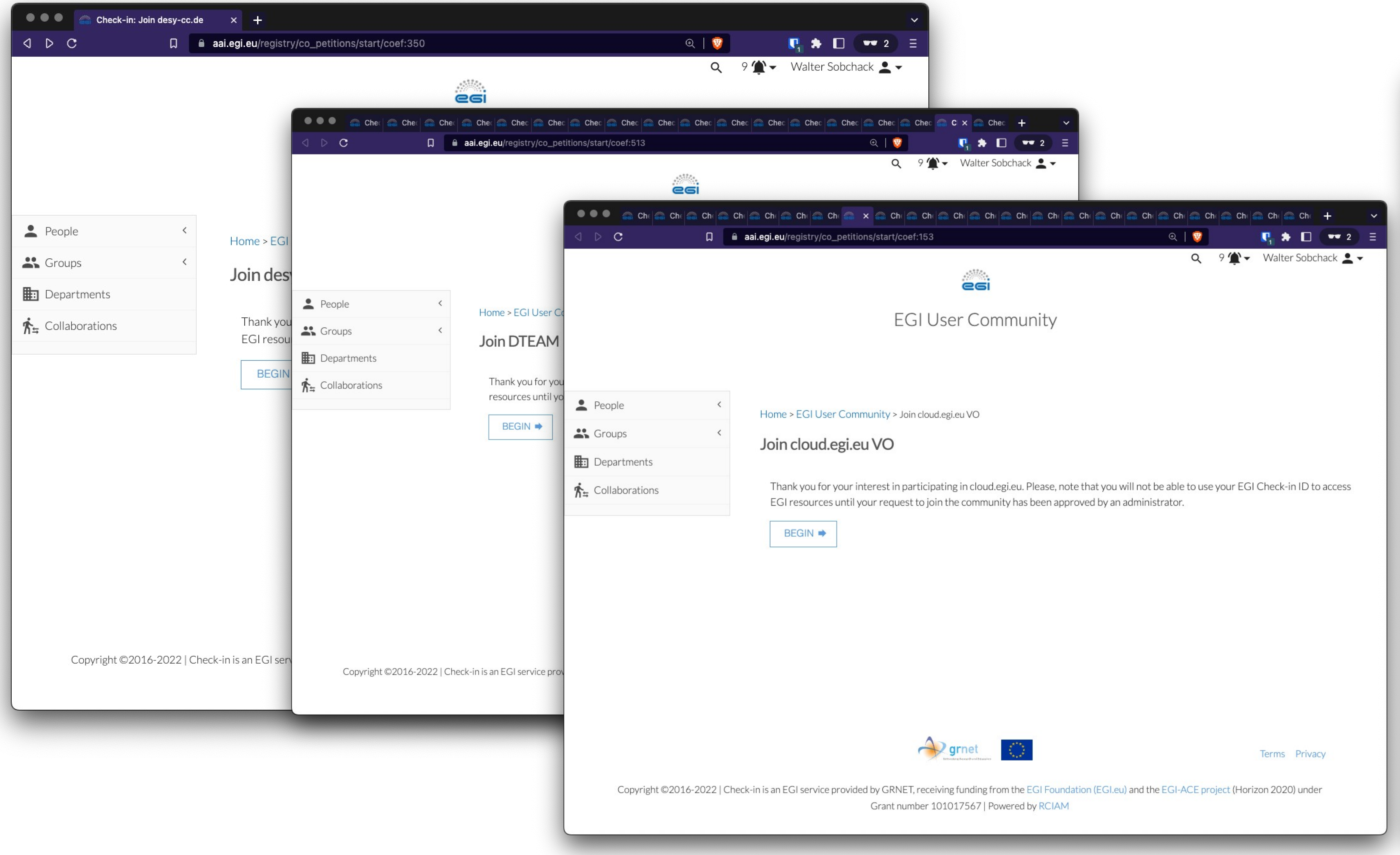
Page 1 of 5, Viewing 1-25 of 118

Terms Privacy

Copyright ©2016-2022 | Check-in is an EGI service provided by GRNET, receiving funding from the EGI Foundation (EGI.eu) and the EGI-ACE project (Horizon 2020) under Grant number 101017567 | Powered by RCIAM

#6: Knocking at heaven's door

Trying to enrolling to the first 25 VOs, requesting or not to write a comment to justify request



Check-in: Join desy-cc.de
aai.egi.eu/registry/co_petitions/start/coef:350
aai.egi.eu/registry/co_petitions/start/coef:513
aai.egi.eu/registry/co_petitions/start/coef:153
Walter Sobchack
People
Groups
Departments
Collaborations
Terms
Privacy

Home > EGI User Community > Join cloud.egi.eu VO

EGI User Community

Join cloud.egi.eu VO

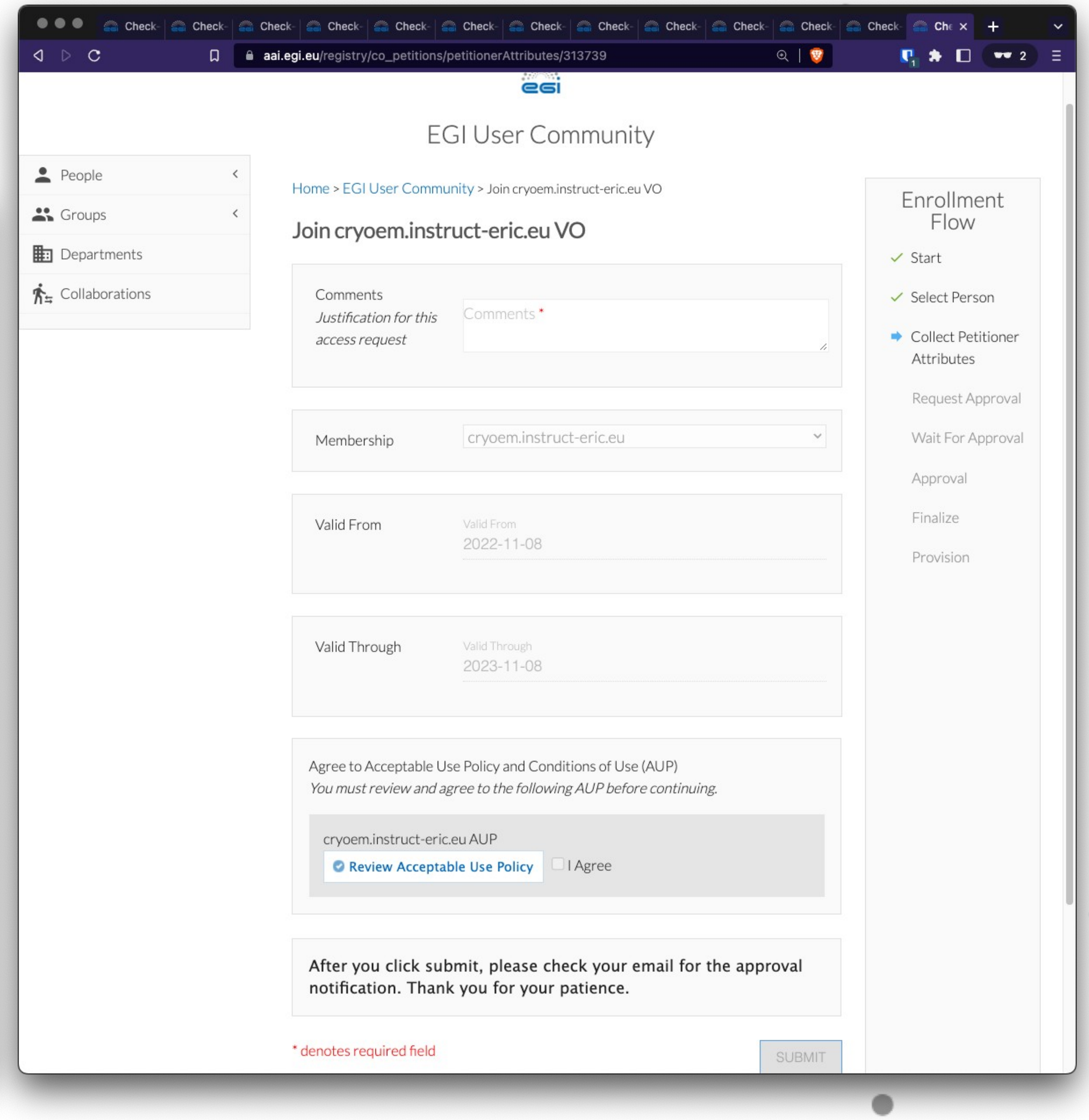
Thank you for your interest in participating in cloud.egi.eu. Please, note that you will not be able to use your EGI Check-in ID to access EGI resources until your request to join the community has been approved by an administrator.

BEGIN

Join DTEAM

Join des

Copyright ©2016-2022 | Check-in is an EGI service provided by GRNET, receiving funding from the EGI Foundation (EGI.eu) and the EGI-ACE project (Horizon 2020) under Grant number 101017567 | Powered by RCIAM



aai.egi.eu/registry/co_petitions/petitionerAttributes/313739
People
Groups
Departments
Collaborations

EGI User Community

Home > EGI User Community > Join cryoem.instruct-eric.eu VO

Join cryoem.instruct-eric.eu VO

Comments
Justification for this access request
Comments *

Membership: cryoem.instruct-eric.eu

Valid From: 2022-11-08

Valid Through: 2023-11-08

Agree to Acceptable Use Policy and Conditions of Use (AUP)
You must review and agree to the following AUP before continuing.

cryoem.instruct-eric.eu AUP
Review Acceptable Use Policy □ I Agree

After you click submit, please check your email for the approval notification. Thank you for your patience.

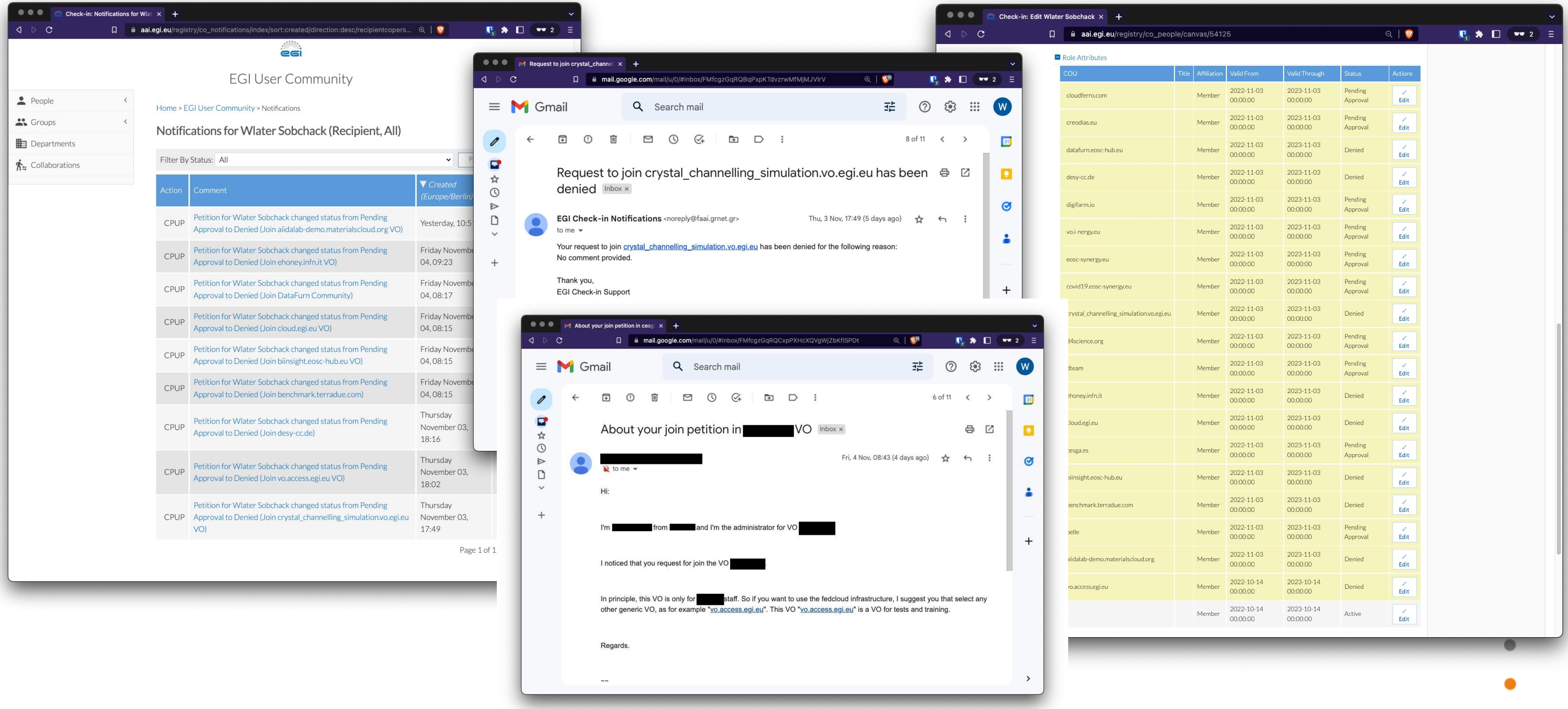
* denotes required field

SUBMIT

Enrollment Flow
- ✓ Start
- ✓ Select Person
- Collect Petitioner Attributes
- Request Approval
- Wait For Approval
- Approval
- Finalize
- Provision

#6: Doors staying closed

No VO managers granted access to Walter…



Check-in: Notifications for Wlat

aai.egi.eu/registry/co_notifications/index/sort:created/direction:desc/recipientcopers...

EGI User Community

- People
- Groups
- Departments
- Collaborations

Home > EGI User Community > Notifications

Notifications for Wlater Sobchack (Recipient, All)

Filter By Status: All

Action	Comment	▼ Created (Europe/Berlin)
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join aiidalab-demo.materialscloud.org VO)	Yesterday, 10:5
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join ehoney.infn.it VO)	Friday Novemb 04, 09:23
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join DataFurn Community)	Friday Novemb 04, 08:17
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join cloud.egi.eu VO)	Friday Novemb 04, 08:15
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join biinsight.eosc-hub.eu VO)	Friday Novemb 04, 08:15
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join benchmark.terradue.com)	Friday Novemb 04, 08:15
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join desy-cc.de)	Thursday November 03, 18:16
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join vo.access.egi.eu VO)	Thursday November 03, 18:02
CPUP	Petition for Wlater Sobchack changed status from Pending Approval to Denied (Join crystal_channelling_simulation.vo.egi.eu VO)	Thursday November 03, 17:49

Page 1 of 1

Request to join crystal_channe

mail.google.com/mail/u/0/#inbox/FMfcgzGqRQBqPxpKTdvzrwMfMjMJVlrV

Search mail

8 of 11

Request to join crystal_channelling_simulation.vo.egi.eu has been denied Inbox ×

EGI Check-in Notifications <noreply@faai.grnet.gr> — Thu, 3 Nov, 17:49 (5 days ago)

to me

Your request to join crystal_channelling_simulation.vo.egi.eu has been denied for the following reason:
No comment provided.

Thank you,
EGI Check-in Support

About your join petition in cesg

mail.google.com/mail/u/0/#inbox/FMfcgzGqRQCxpPXHcXQVgWjZbKfISPDt

Search mail

6 of 11

About your join petition in [redacted] VO Inbox ×

[redacted] — Fri, 4 Nov, 08:43 (4 days ago)

to me

Hi:

I'm [redacted] from [redacted] and I'm the administrator for VO [redacted]

I noticed that you request for join the VO [redacted].

In principle, this VO is only for [redacted] staff. So if you want to use the fedcloud infrastructure, I suggest you that select any other generic VO, as for example "vo.access.egi.eu". This VO "vo.access.egi.eu" is a VO for tests and training.

Regards.

--

Check-in: Edit Wlater Sobchack

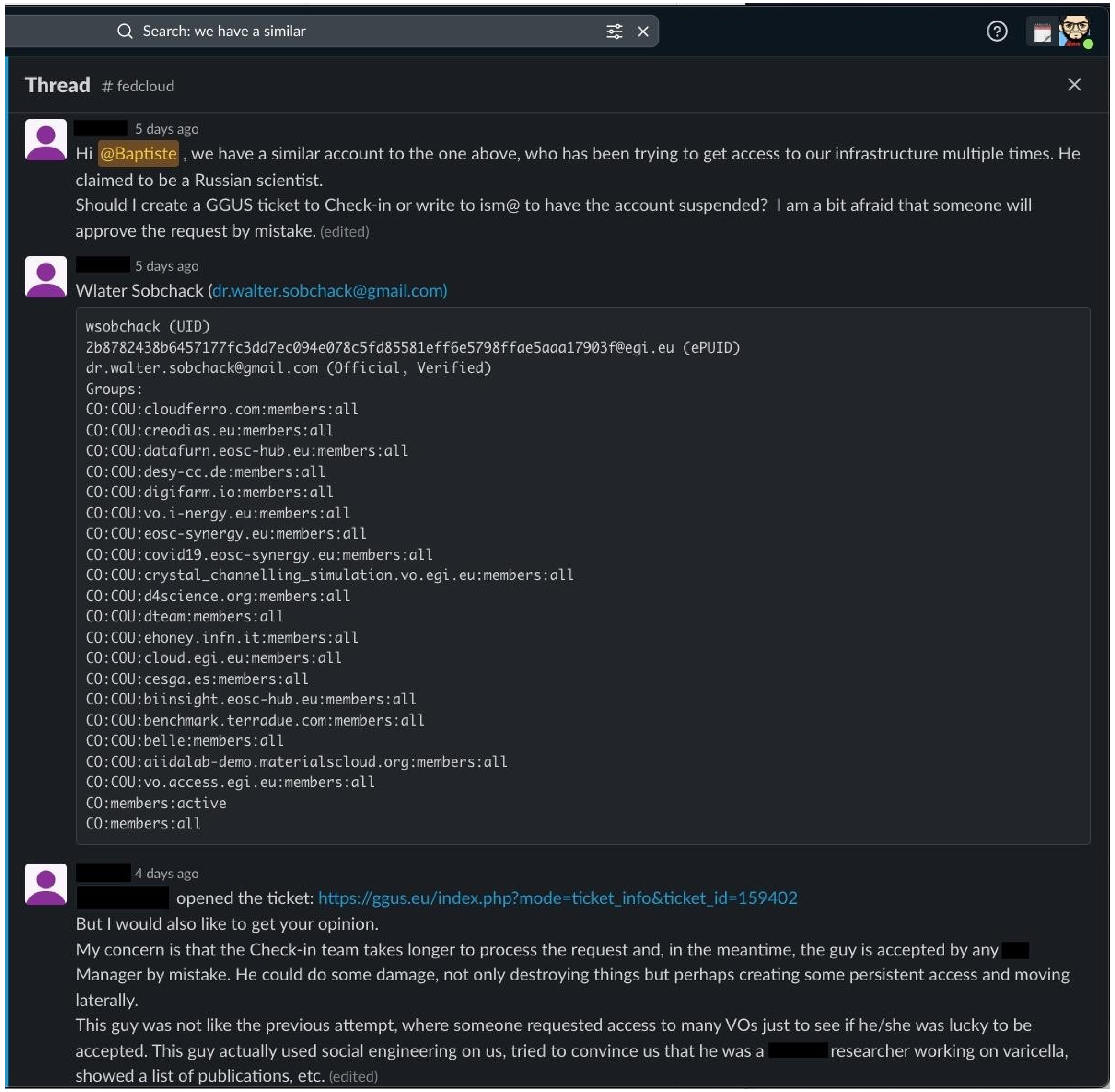
aai.egi.eu/registry/co_people/canvas/54125

Role Attributes

COU	Title	Affiliation	Valid From	Valid Through	Status	Actions
cloudferro.com		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
creodias.eu		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
datafurn.eosc-hub.eu		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Denied	Edit
desy-cc.de		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Denied	Edit
digifarm.io		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
vo.i-nergy.eu		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
eosc-synergy.eu		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
covid19.eosc-synergy.eu		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
rystal_channelling_simulation.vo.egi.eu		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Denied	Edit
d4science.org		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
dteam		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
honey.infn.it		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Denied	Edit
loud.egi.eu		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Denied	Edit
esga.es		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
iinsight.eosc-hub.eu		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Denied	Edit
enchmark.terradue.com		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Denied	Edit
elle		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Pending Approval	Edit
iidalab-demo.materialscloud.org		Member	2022-11-03 00:00:00	2023-11-03 00:00:00	Denied	Edit
o.access.egi.eu		Member	2022-10-14 00:00:00	2023-10-14 00:00:00	Denied	Edit
		Member	2022-10-14 00:00:00	2023-10-14 00:00:00	Active	Edit

#7: Triggering alerts in EGI Foundation

EGI Foundation Central VO management team getting suspicious



Thread # fedcloud

[redacted] 5 days ago

Hi @Baptiste , we have a similar account to the one above, who has been trying to get access to our infrastructure multiple times. He claimed to be a Russian scientist.

Should I create a GGUS ticket to Check-in or write to ism@ to have the account suspended? I am a bit afraid that someone will approve the request by mistake. (edited)

[redacted] 5 days ago

Wlater Sobchack (dr.walter.sobchack@gmail.com)

```
wsobchack (UID)
2b8782438b6457177fc3dd7ec094e078c5fd85581eff6e5798ffae5aaa17903f@egi.eu (ePUID)
dr.walter.sobchack@gmail.com (Official, Verified)
Groups:
CO:COU:cloudferro.com:members:all
CO:COU:creodias.eu:members:all
CO:COU:datafurn.eosc-hub.eu:members:all
CO:COU:desy-cc.de:members:all
CO:COU:digifarm.io:members:all
CO:COU:vo.i-nergy.eu:members:all
CO:COU:eosc-synergy.eu:members:all
CO:COU:covid19.eosc-synergy.eu:members:all
CO:COU:crystal_channelling_simulation.vo.egi.eu:members:all
CO:COU:d4science.org:members:all
CO:COU:dteam:members:all
CO:COU:ehoney.infn.it:members:all
CO:COU:cloud.egi.eu:members:all
CO:COU:cesga.es:members:all
CO:COU:biinsight.eosc-hub.eu:members:all
CO:COU:benchmark.terradue.com:members:all
CO:COU:belle:members:all
CO:COU:aiidalab-demo.materialscloud.org:members:all
CO:COU:vo.access.egi.eu:members:all
CO:members:active
CO:members:all
```

[redacted] 4 days ago

[redacted] opened the ticket: https://ggus.eu/index.php?mode=ticket_info&ticket_id=159402

But I would also like to get your opinion.

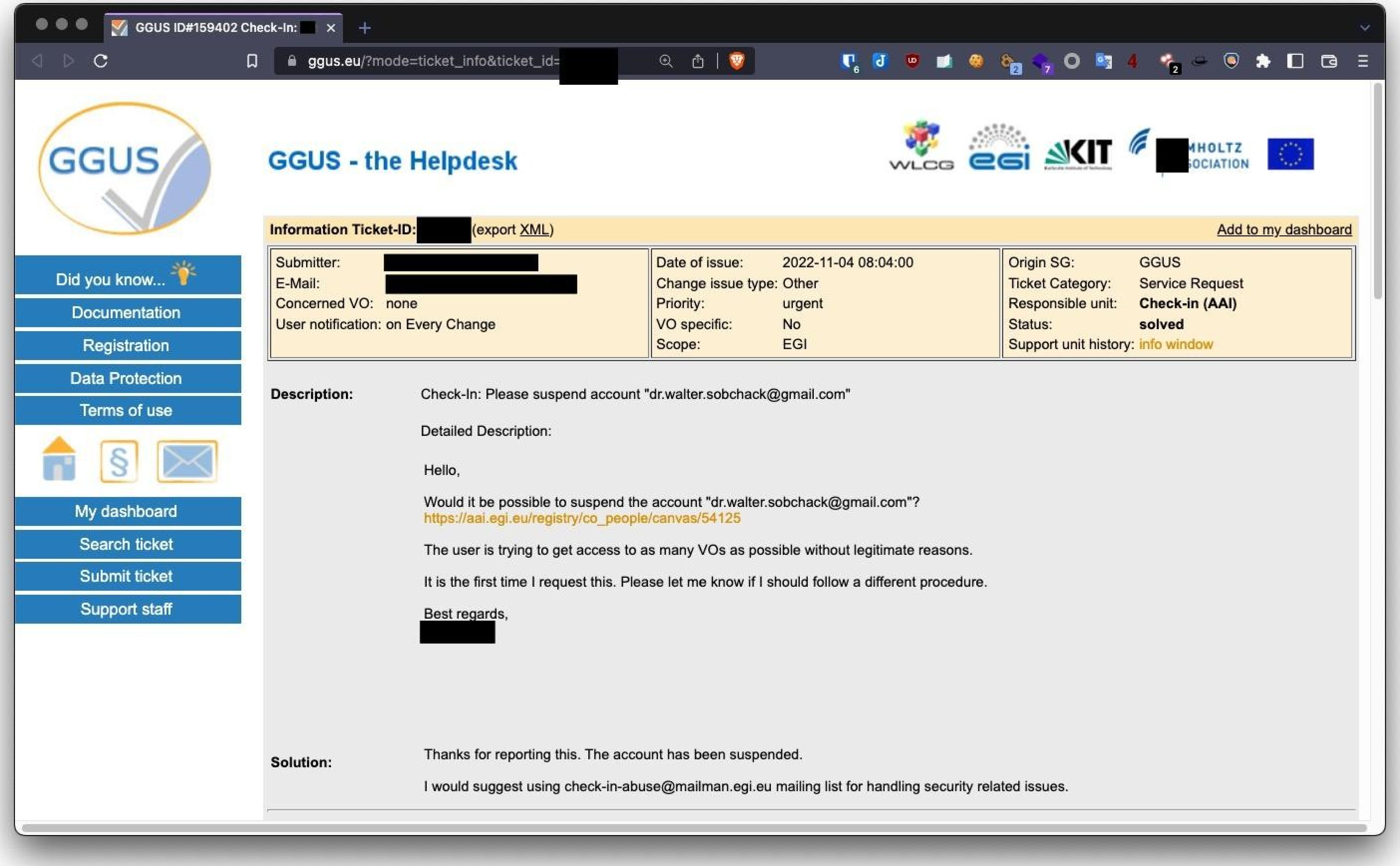
My concern is that the Check-in team takes longer to process the request and, in the meantime, the guy is accepted by any [redacted] Manager by mistake. He could do some damage, not only destroying things but perhaps creating some persistent access and moving laterally.

This guy was not like the previous attempt, where someone requested access to many VOs just to see if he/she was lucky to be accepted. This guy actually used social engineering on us, tried to convince us that he was a [redacted] researcher working on varicella, showed a list of publications, etc. (edited)

- In fact many VOs are managed by the EGI Foundation team
  - ○ They got multiple access requests from the same user
  - ○ => reported to the EGI Foundation Information Security Manager, asking for support

#7: Requesting the account suspension

EGI Foundation Central VO management team taking actions



GGUS - the Helpdesk

Information Ticket-ID: [redacted] (export XML)   Add to my dashboard

Submitter: [redacted]
E-Mail: [redacted]
Concerned VO: none
User notification: on Every Change

Date of issue: 2022-11-04 08:04:00
Change issue type: Other
Priority: urgent
VO specific: No
Scope: EGI

Origin SG: GGUS
Ticket Category: Service Request
Responsible unit: **Check-in (AAI)**
Status: **solved**
Support unit history: info window

Description: Check-In: Please suspend account "dr.walter.sobchack@gmail.com"

Detailed Description:

Hello,

Would it be possible to suspend the account "dr.walter.sobchack@gmail.com"?
https://aai.egi.eu/registry/co_people/canvas/54125

The user is trying to get access to as many VOs as possible without legitimate reasons.

It is the first time I request this. Please let me know if I should follow a different procedure.

Best regards,
[redacted]

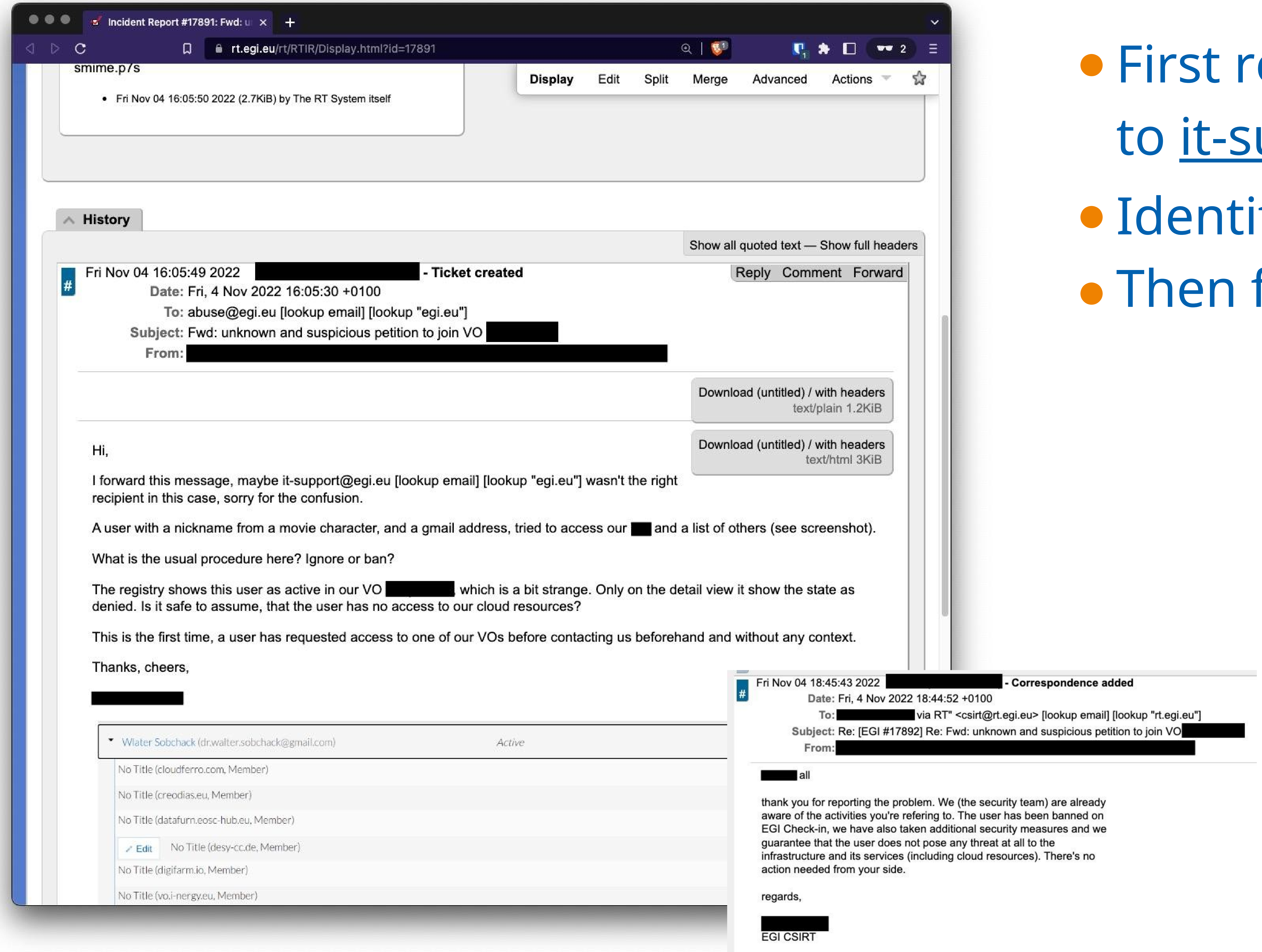
Solution: Thanks for reporting this. The account has been suspended.

I would suggest using check-in-abuse@mailman.egi.eu mailing list for handling security related issues.

- Requesting account suspension in GGUS

#7: A VO manager reporting to EGI CSIRT

EGI Foundation Central VO management team getting suspicious



Incident Report #17891: Fwd: u
rt.egi.eu/rt/RTIR/Display.html?id=17891
Display
Edit
Split
Merge
Advanced
Actions
History
Show all quoted text — Show full headers
Reply
Comment
Forward

smime.p7s

- Fri Nov 04 16:05:50 2022 (2.7KiB) by The RT System itself

Fri Nov 04 16:05:49 2022 [redacted] - **Ticket created**

Date: Fri, 4 Nov 2022 16:05:30 +0100
To: abuse@egi.eu [lookup email] [lookup "egi.eu"]
Subject: Fwd: unknown and suspicious petition to join VO [redacted]
From: [redacted]

Download (untitled) / with headers
text/plain 1.2KiB

Download (untitled) / with headers
text/html 3KiB

Hi,

I forward this message, maybe it-support@egi.eu [lookup email] [lookup "egi.eu"] wasn't the right recipient in this case, sorry for the confusion.

A user with a nickname from a movie character, and a gmail address, tried to access our [redacted] and a list of others (see screenshot).

What is the usual procedure here? Ignore or ban?

The registry shows this user as active in our VO [redacted] which is a bit strange. Only on the detail view it show the state as denied. Is it safe to assume, that the user has no access to our cloud resources?

This is the first time, a user has requested access to one of our VOs before contacting us beforehand and without any context.

Thanks, cheers,

[redacted]

Wlater Sobchack (dr.walter.sobchack@gmail.com) *Active*

No Title (cloudferro.com, Member)
No Title (creodias.eu, Member)
No Title (datafurn.eosc-hub.eu, Member)
Edit No Title (desy-cc.de, Member)
No Title (digifarm.io, Member)
No Title (vo.i-nergy.eu, Member)

Fri Nov 04 18:45:43 2022 [redacted] - **Correspondence added**

Date: Fri, 4 Nov 2022 18:44:52 +0100
To: [redacted] via RT" <csirt@rt.egi.eu> [lookup email] [lookup "rt.egi.eu"]
Subject: Re: [EGI #17892] Re: Fwd: unknown and suspicious petition to join VO [redacted]
From: [redacted]

[redacted] all

thank you for reporting the problem. We (the security team) are already aware of the activities you're refering to. The user has been banned on EGI Check-in, we have also taken additional security measures and we guarantee that the user does not pose any threat at all to the infrastructure and its services (including cloud resources). There's no action needed from your side.

regards,

[redacted]
EGI CSIRT

- First report about suspicious activity sent to it-support@egi.eu
- Identifying the pretext's context
- Then forwarding to abuse@egi.eu

Lessons from the exercise

It was both successful (from a defender side) and a failure (from an attacker side)

What went well

- Dr Sobchak **never got access to any resources**
- **Vetting** of vo.access.egi.eu was very **effective**
  - Professional tone in communication
  - Following a defined procedure, looking for:
    - Justifications for accessing the resources
    - Justifications on the identity, researcher status and institute
    - Asked for using a Identity Provider providing more assurance
- **Reporting** dubious activity to the **local security team**
- Taking **protective measures** (account suspension)
  - Check-in team was reactive, account got blocked
- A VO manager **reported** suspicious request **to EGI CSIRT**

What may be improved

- Account suspension request in GGUS should have been managed with the involvement of the local security team and possibly of the EGI CSIRT
- It's possible to easily discover many VO and try to enroll
  - Not all VO Managers may be as careful
- Due to a configuration error, for some time, the Check-in account was still usable

Ideas for the future

- Promoting/sharing VO vetting procedure
- Only exposing VO that needs to be exposed
- Running the tests on a more targeted way, like for the SSC

Contact us

baptiste.grenier@egi.eu

EGI CISRT: security-requests@egi.eu

Let's talk. Or
meet in person

Get in touch with us

www.egi.eu

This work is partially funded by the EU research and innovation programme