Inter federation incident response (IR) in eduGAIN

eduGAIN security Table Top Exercise (TTX)

S. Gabriel[1] D. Groep[1] T. Dussa[2] D. Kouřil[3,4]
D.Kelsey[5] M. Kremers[6] D. Vaghetti[7]

[1]Nikhef [2]DFN-CERT [3]CESNET [4]Masaryk University
[5]STFC/RAL [6]SURF [7]GARR

ISGC 2025 Security Day, Taipei

Motivation/Goal

The goal of the exercise:

Raising awareness of the complexity of IR in large/federated environment

Motivation for the TTX

Test IR procedures and policies in eduGAIN and promote/explain the role/utility of eduGAIN CSIRT

Questions to answer

Identify the organisational obstacles in IR, are the available policies complete enough?

Role-play

Why a role-play:

- Handling a simulated real-life incident affecting a complex environment, to get a better understanding of the risks.
- "Cheap" way to test available policies and procedures, are they sufficient, do they "work"?

Enabled learning objectives

- IdP/SP logfile analysis (check for/find a reported Id).
- know SIRTFI v2, and understand to apply it.
- Know how eduGAIN is organised, role of Federations, eduGAIN and eduGAIN CSIRT.
- Name the risks of federated Identity Management.

Agenda

- Intro to eduGAIN (D. Vaghetti)
- SIRTFI v1,2 (D. Kelsey)
- eduGAIN CSIRT (S. Gabriel)
- eduGAIN TTX (S. Gabriel, D. Kouřil, D. Groep, M. Kremers, D. Kelsey, D. Vaghetti)

Intro to eduGAIN (D. Vaghetti)

SIRTFI v1,2 (D. Kelsey)

eduGAIN CSIRT (S. Gabriel)

Approach: security in eduGAIN

- Organization
  - What is the organizational structure (see previous talks), Governance, Responsibility Accountability.
  - What are the existing policies, agreements etc.
- Options
  - Set up trust network. Trust is in individuals.
  - Formally set up a security team (▸ RFC 2350, ▸ TOR, mandate, services, ...etc.). Trust is in Organizations/Processes.

Organizational, Governance, Policies

eduGAIN Policy Framework Constitution:

- 2 Governance and Governing Bodies
- 2.1 eduGAIN Executive Committee (eEC), *Decisions about possible changes to the constitution are taken here*
- 2.2 eduGAIN Steering ~~Group (eSG)~~ Committee *Reviewing and approving the membership of new Federations, Approving the disqualification or temporary suspension for Member Federations as described in section 3.6*
- 2.3 Operational Team (OT)

Constituency

eduGAIN Policy Framework ▸ Constitution

1.2 Goal

The goal of eduGAIN is to support Identity Federations primarily engaged in research and education by providing a service which enables them to inter-federate.

eduGAIN entities: 9500+ (IdPs 5700+, SPs 3700) organised in 78 participants (Federations).

Primary Asset: Function which enables federations to inter-federate.

Role, Functions of the Security Team

- Role: Advisory only.
- Coordination function: *The eduGAIN-CSIRT provides computer security incident response coordination for eduGAIN.*
- It serves as the primary contact point for all security related issues affecting eduGAIN and more specifically for all the security issues affecting multiple entities from different Federations.

IT Security Incident Response (IR) and Root Cause Analysis (RCA)

- One of the goals of IR is to understand why an IT Security Incident has happened, identify which Security Measures could prevent this incident from happening again.
- The RCA concept is rather old and known for example in addressing aviationdisasters. IT development (here in particular sophisticated adversaried) is much more dynamic then engineering and faces challenges.
- It's beyond identifying a compromised account, or a malware, question is rather why an account could be comprimesed, or why a particular malware succeded to infiltrate the systems.
- A way to get to the Rot Cause is the "5 Whys" iterative method[1], Example

[1] Other Methods would be Fishbone (Ishikawa) or an Analysis Tree Diagram, many of these were developed by doing RCA in aviation.

The "5 Whys" iterative method

- Why could the malware planted → using legit account

The "5 Whys" iterative method

- Why could the malware planted $\rightarrow$ using legit account
- Why could this account be used by an attacker $\rightarrow$ password bruteforced, ... done?

The "5 Whys" iterative method

- Why could the malware planted $\rightarrow$ using legit account
- Why could this account be used by an attacker $\rightarrow$ password bruteforced, ... done?
- No, why could the password be bruteforced? $\rightarrow$ little complexity.

The "5 Whys" iterative method

- Why could the malware planted → using legit account
- Why could this account be used by an attacker → password bruteforced, ... done?
- No, why could the password be bruteforced? → little complexity.
- Why can weak password be used? → No policy, no policy enforcement

The "5 Whys" iterative method

- Why could the malware planted → using legit account
- Why could this account be used by an attacker → password bruteforced, ... done?
- No, why could the password be bruteforced? → little complexity.
- Why can weak password be used? → No policy, no policy enforcement
- Why is ther no password policy,→ Organisational security problem

Goal of RCA

Organize potential causes into key categories[2]:

- People: Training gaps, security awareness
- Process: Access management, change control
- Technology: System vulnerabilities, patch management
- Environment: Network architecture, security controls
- Management: Policy enforcement, resource allocation

[2] https://en.wikipedia.org/wiki/Root_cause_analysis

Some Remarks on Communication

How to Communicate Securely

- We don't mean encryption here!
- Rather, how to contain the *dissemination* of information by legitimate recipients.
- In other words: How to make sure that if you tell somebody a secret, that somebody does not blabber that secret to the rest of the world.
- Obviously an organizational measure, so all we can do is specify rules and then trust that everybody sticks to these rules.
- It should also be obvious that if somebody does not stick to these rules, they will not be trusted any longer.
- The set of generally-accepted rules are called the "Traffic Light Protocol" (TLP, see `https://www.first.org/tlp`).

TLP Principles

- Information is classified by the *sender* into one of these four categories: `TLP:CLEAR`, `TLP:GREEN`, `TLP:AMBER`, `TLP:RED`.
- The *recipient* is expected to treat the thusly-classified information in accordance with the TLP rules as laid out below.
- Information must be marked clearly with a TLP classification; it is generally a good idea to define a *default* classification in case there is no explicit marking. `TLP:AMBER` is usually a good starting point.
- The classification of a given bit of information may change over time (the classification is usually relaxed).

The TLP Classifications

- `TLP:CLEAR` (formerly `TLP:WHITE`): Information that can be shared freely with anybody—for instance, may be published on a public web page or released to the press.
- `TLP:GREEN`: Information that can be shared within the community—for instance, within the high-energy physics community—, but *not* released to the general public.
- `TLP:AMBER`: Information that may be shared *within the recipient's organisation and its clients*—for instance, within a university if the recipient is a member of a university, or a company *and its customers* if the recipient works for a company. If unsure, *ask the sender*. Additionally, `TLP:AMBER` may be restricted arbitrarily by the sender. For instance, `TLP:AMBER - FOR EDUGAIN ONLY` might be used so signal that information can only be shared with eduGAIN parties.

The TLP Classifications – cont'd

- `TLP:AMBER+STRICT`: This is a special, pre-defined restriction for `TLP:AMBER` that signals that information may be shared only within the recipient's organisation, but *not* with any customers.
- `TLP:RED`: This is the strictest classification and signals that information may *not be shared with anybody else whatsoever*. This means that whoever is told something under `TLP:RED` *cannot* tell *anybody* else this information.
  Note that this restriction in particular means that `TLP:RED` information cannot be shared through chat channels if a new member to the chat channel can read the channel history. If new members can read the history, then it is not clear who the ultimate recipients of a message will be because new members could be added at any time and thus gain access to earlier messages. Therefore, `TLP:RED` conditions cannot be guaranteed.

You will be expected to classify all your communications in this exercise, so contemplate what classification would be the right level of protection for your information and mark it accordingly!

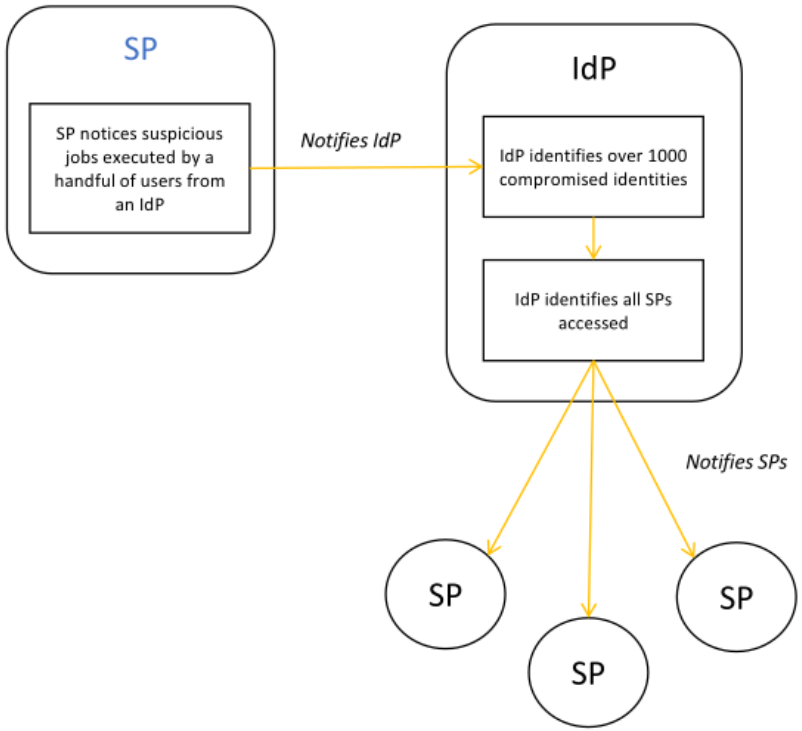
Background, Current situation

eduGAIN CSIRT, provided Services

- eduGAIN CSIRT listed (Feb. 2024) team in TF-CSIRTs
  ▸ TI-Directory
- Support in Development of an ▸ Incident Response Procedure
- IR procedure describes Roles and Responsibilities of *Federation Operators, IdPs, SPs*
- Technical IR support for IdP, SP operators with a focus on federation software. (Find relevant info in logs, act on identities, key-roleover etc)
- Support in Incident Triaging, Incident Coordination, Incident Resolution.

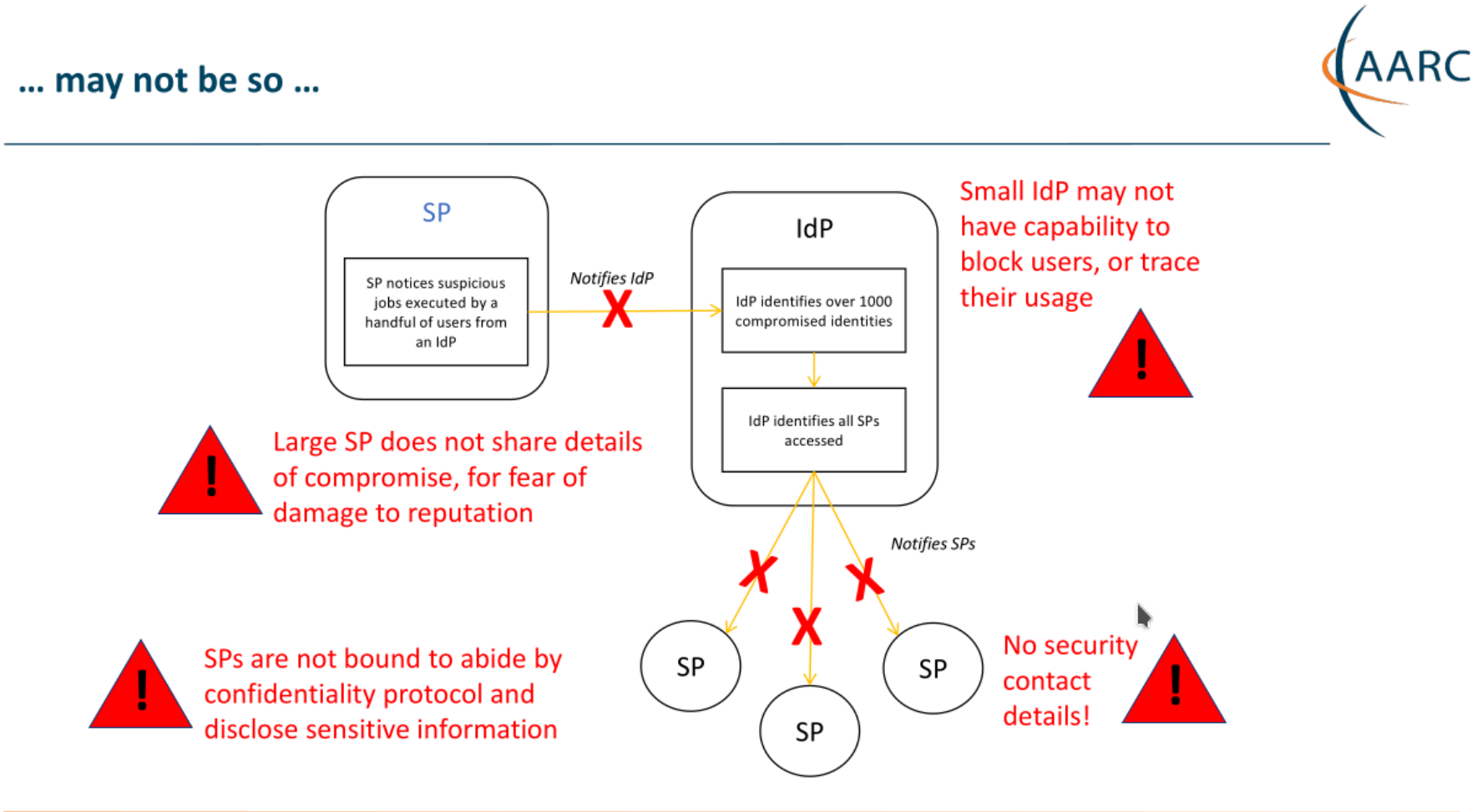
Coordination, who should talk to who?

But what appears trivial



graphics source: Hannah Short, CERN

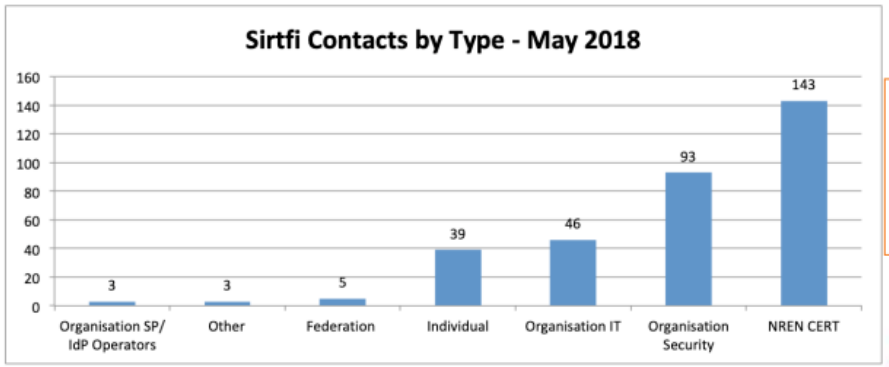
Coordination, who should talk to who?



Coordination, who should talk to who?... SIRTFI

Sirtfi is there today – 561 parties joined, in 28 federations

SIRTFI
Security Incident Response Trust Framework for Federated Identity



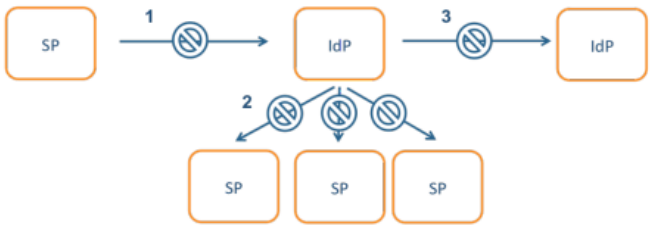
Incident Response

- Assure confidentiality of information exchanged
- Identify trusted contacts
- Guarantee a response during collaboration

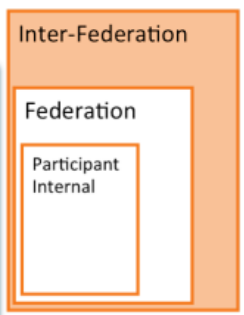
graphics source: AARC2 DNA3.2 Report on Incident Response in FIM; data: technical.edugain.org

Coordination, who should talk to who?... SIRTFI

Incident response process evolution in federations

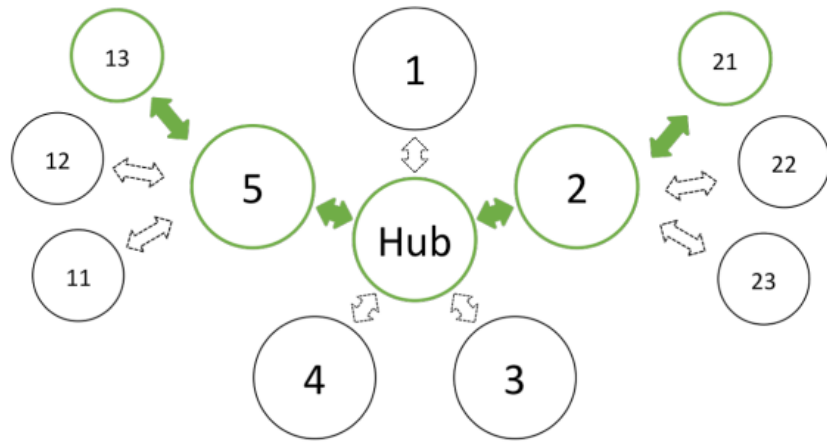


Incident Response Communication, communication blocks



Proposed solutions

- Stronger role for federation operators, as they are known to both SPs and IdPs
- Add hub capability centrally (@ eduGAIN)

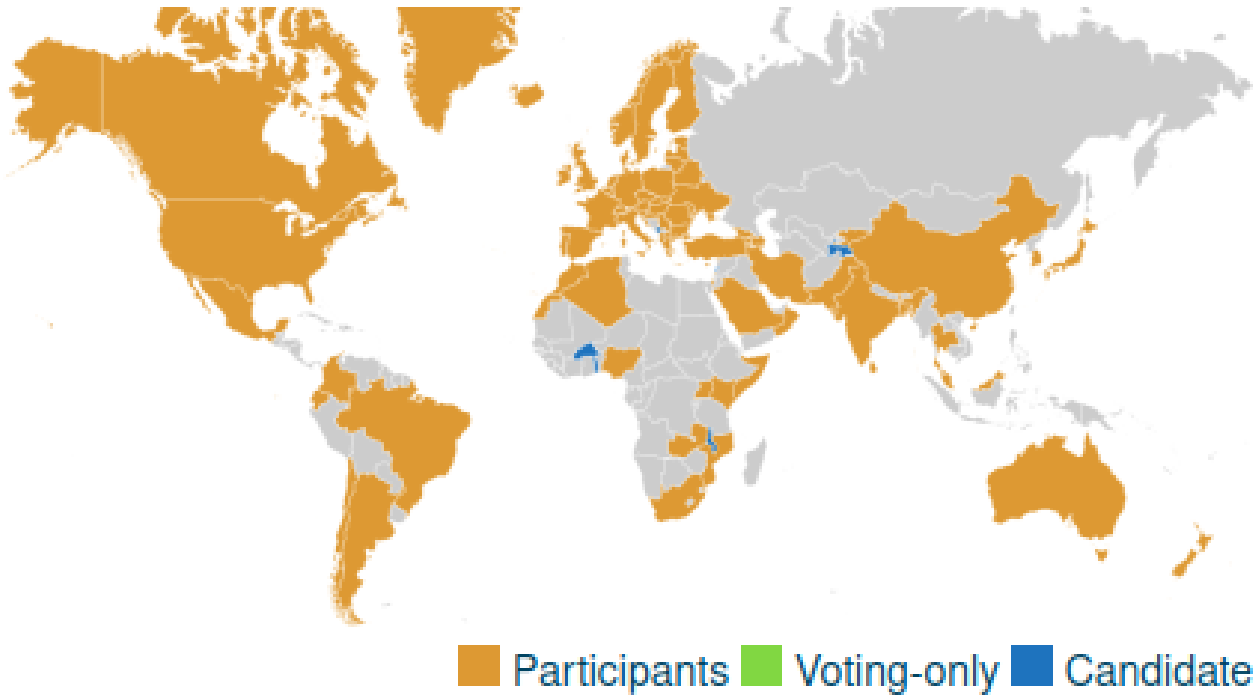


Inter-Federation Incident Response Communication

AARC https://aarc-project.eu

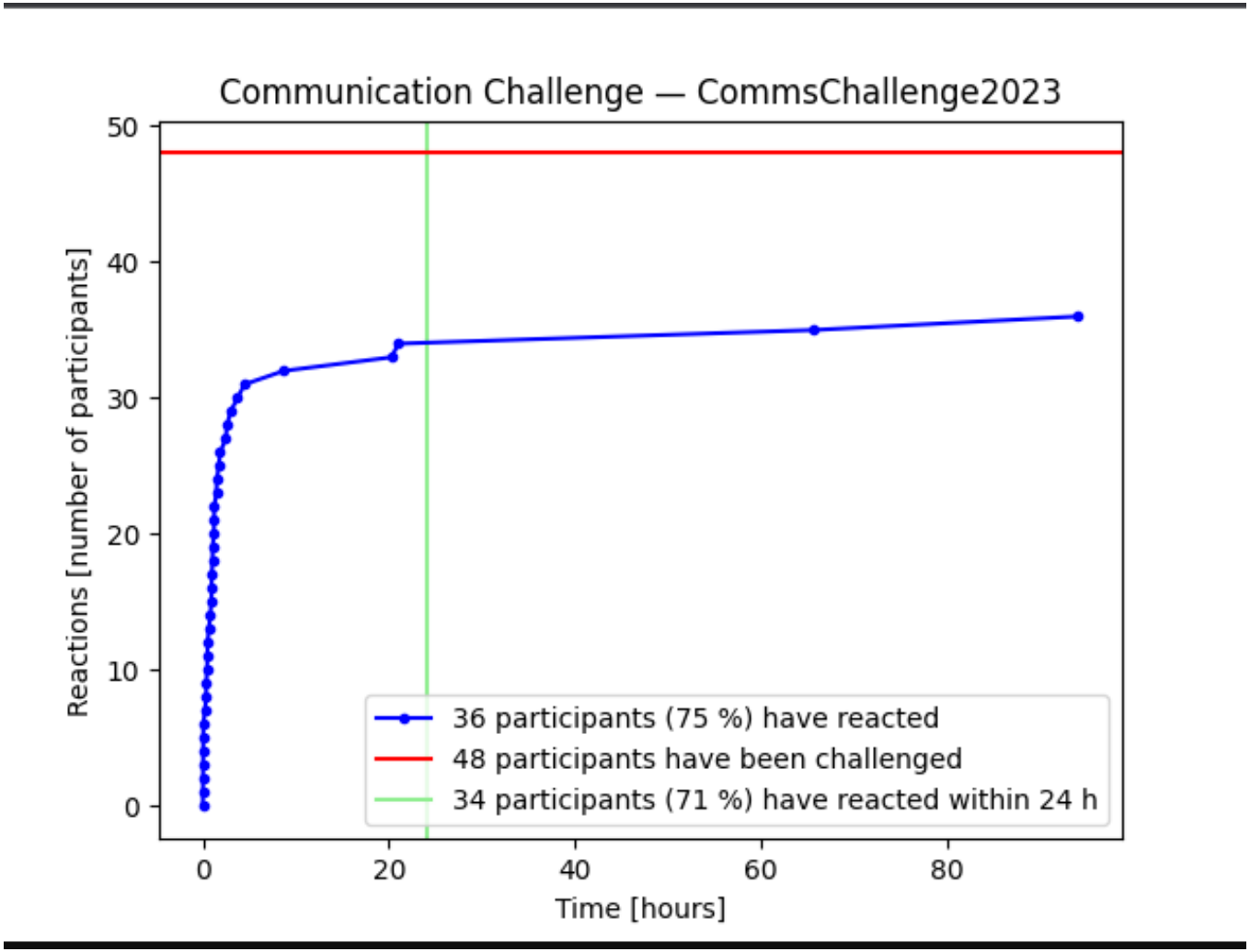
https://aarc-project.eu/guidelines/aarc-i051/

Testing the Communications Infra



79 participants, only sirtfi'd challenged (48), next slide

Testing the Communications Infra



The eduGAIN TTX, Background, Current situation.

Background, Current situation

This game mostly consists of elements of incident we handled, though not in the combination we show here.

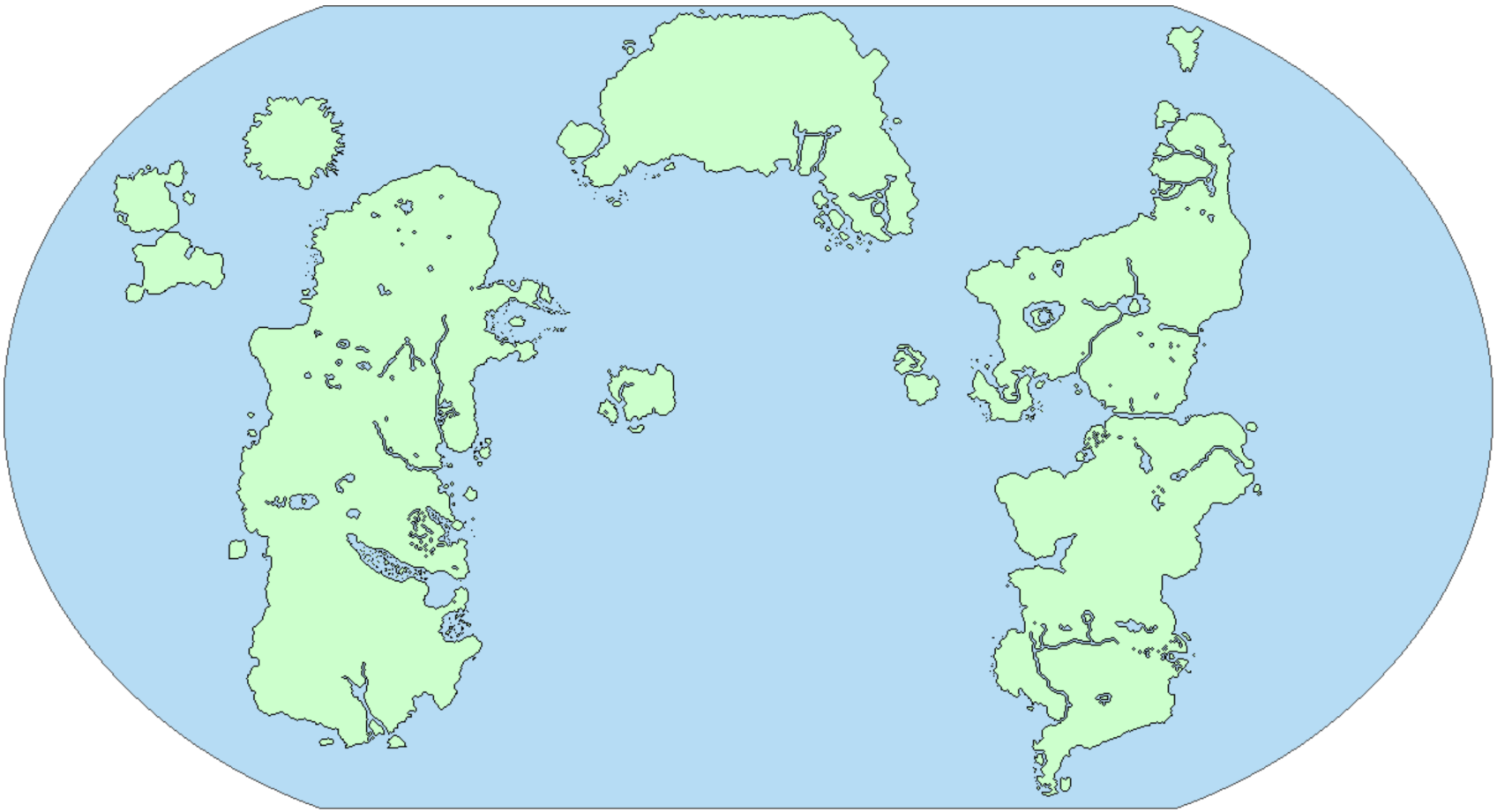
- We have a couple of IdP, SP and Federation Operators. All participants have carried out a self assessment and announce to be compliant with SIRTFI v2. (Hey its a perfect world, isn't it :-))
- Read, discuss your role description, get familiar with your IR tasks.
- if anything goes wrong, rest easy, finding the obstacles is one of the goals of the play.
- if anything is unclear, ask us.

What would you do?

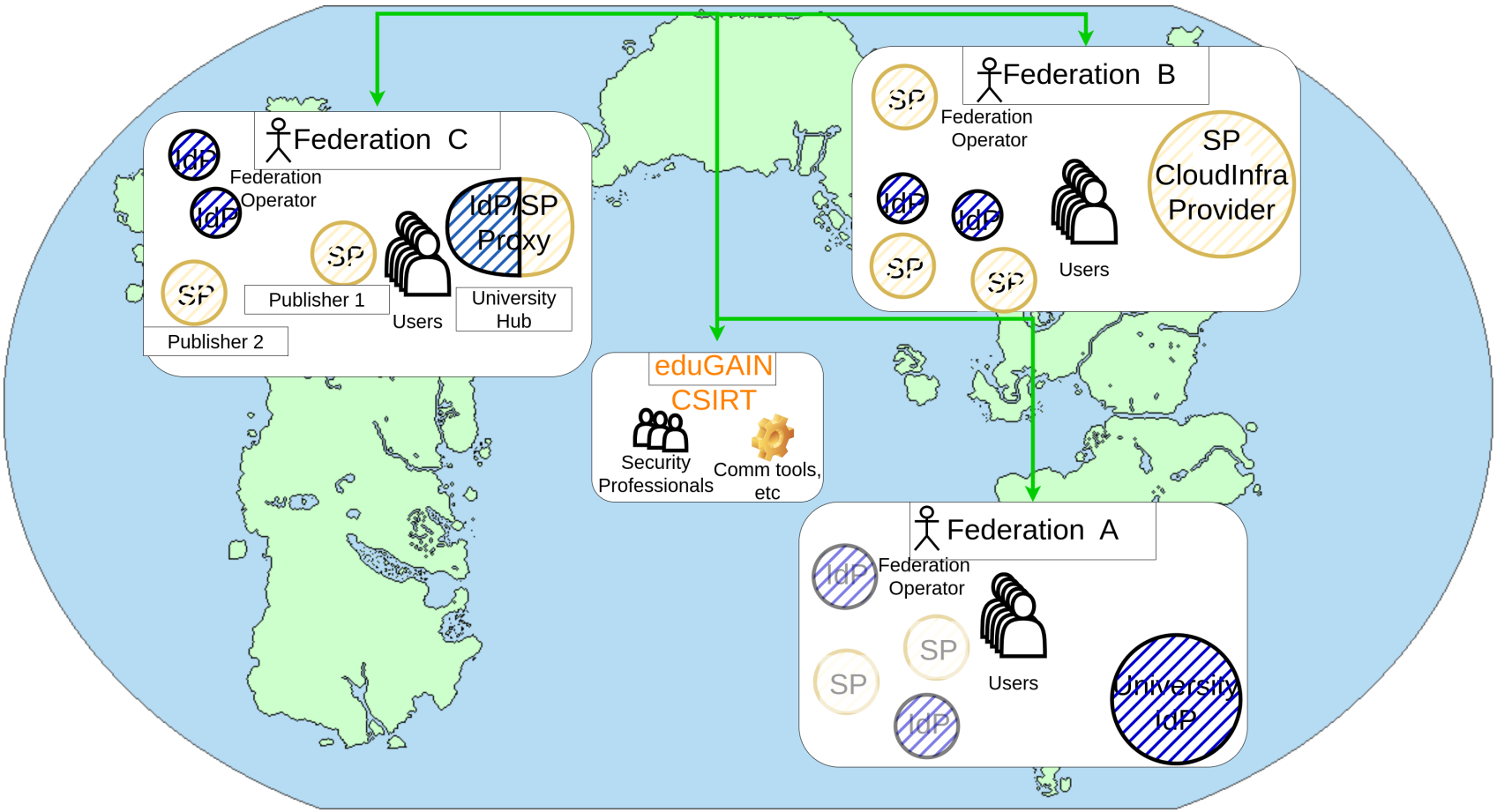
During the play you will have to make decisions and report them back to the other players, at each section you should think about what would you do.

When you need information, have instructions for another participants, just raise your hand, we will establish the communication.

The World



The World with Identity Federations



Description of the Services and the Role of the Service Operator

Roles

Roles, in order of appearance.

- Academic Hub (IdP/SP proxy)
- Federation of Academic Hub (Fed. C)
- IdP of university *uni.org*
- Federation of *uni.org* IdP (Fed. A) (needed)
- *User*
- Community cloud
- Federation of Community cloud (Fed. B)

Some roles have pretty little to do, can/will be covered by the trainers.

Roles

Roles explained.

- *Federation Operator*: admin of an Identity Federation to which belong IdPs and SPs (entities). Usually, IdPs represent Home Organizations of the Federation's country (Universities, Research Center, etc), while SPs are both services and resources provided by vendors, and home organizations themselves. The Federation Operator is responsible for entities registration and metadata management, eduGAIN membership and relations with other federation operators. With regards to security, the Federation Operator should publish a security contact that will act as reference for the eduGAIN CSIRT, other CERTs/CSIRTs and the eduGAIN Participants.

Roles, Federation and Federation Operator

Roles explained.
IdP Operator: admin an Identity Provider of an Home Organization. An IdP Operator has access to IdP logs with traces of users logins to SPs, and she/he's is expected to comply with SIRTFI requirements on IR, log tracking, etc. IdPs adhering to SIRTFI must publish a security contact that will handle IR and supports TLP.

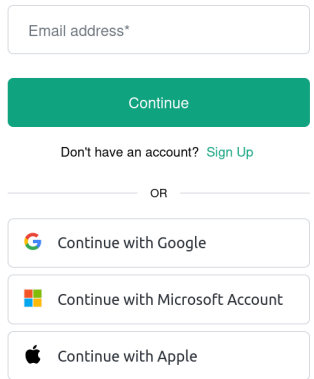
Roles, SP Operator

Roles explained. *SP Operator*: admin of a Service Provider of the resource. An SP operator has access to SP logs with traces of users' logging from the IdPs and she/he's expected to comply with SIRTFI on the service side. As for IdPs, SPs adhering to SIRTFI must publish a security contact that will handle IR and supports TLP.

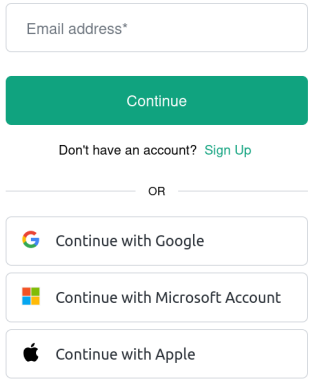
Roles, IdP/SP proxy operator

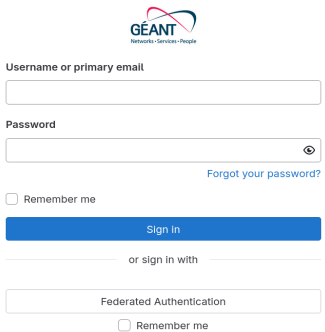
Roles explained. *IdP/SP proxy operator*: admin of an IdP/SP proxy, which means being responsible for managing both the IdP back end connecting internal services and the SP front end connected to the Federation. SIRTFI compliance is mostly on the front end (SP) side.

Authentication as a Service

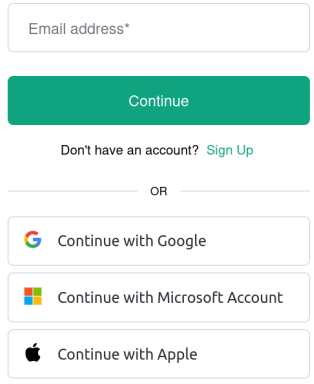


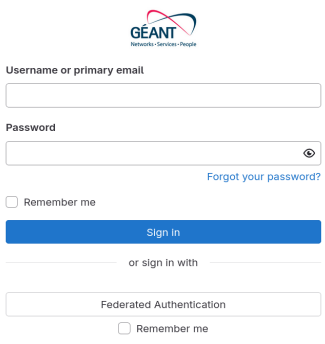
Authentication as a Service

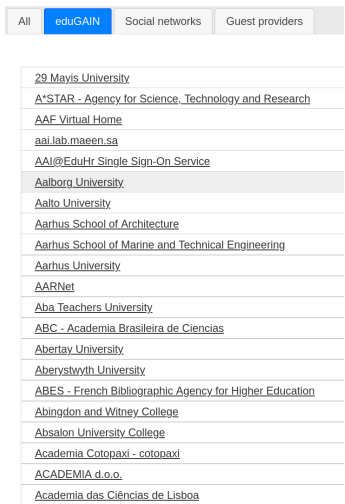




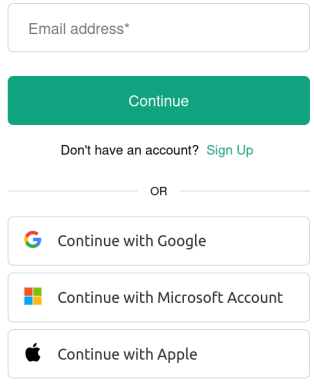
Authentication as a Service

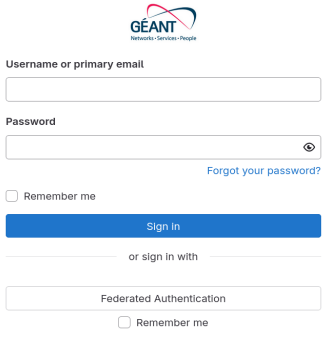


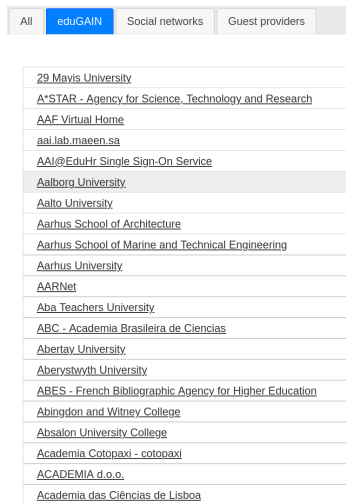


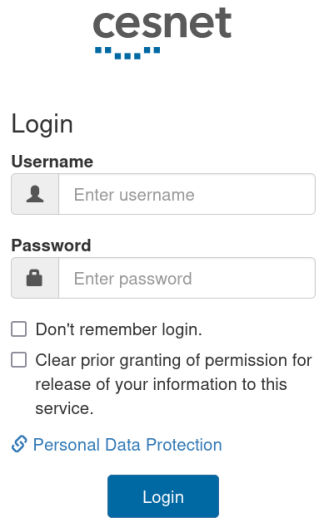


Authentication as a Service









Security tokens

- *Token* is a proof of authentication and/or authorization
- If token is compromised (leaked), the user can be impersonated or actions on their behalf can be taken by an adversary
- A number of token formats and types (HTTP Cookie, Kerberos tickets, X.509 certificates and private key combo)
- Protocols used for federated authentication/authZ use a number of tokens
  - SAML Assertions, OIDC ID tokens, OIDC Access token, OIDC Refresh tokens
  - different lifetimes (e.g., short-lived OIDC Access tokens vs. long-lived Refresh token)
  - Some tokens are only used in the protocol exchange (SAML assertions), some are designed to be maintained by the user's application (OIDC Refresh token)

eduGAIN TTX, outline of the TTX

- Intro to the TTX, get into groups, assign roles to groups.
- Background, Current Situation.
- Stage-1, Incident begins, report to IdP/SP Proxy
- Stage-2, Incident verified
- Stage-3, Incident spreads
- Stage-4, Investigation starts
- Stage-5, Incident handling
- Stage-6, Incident resolved, close out report

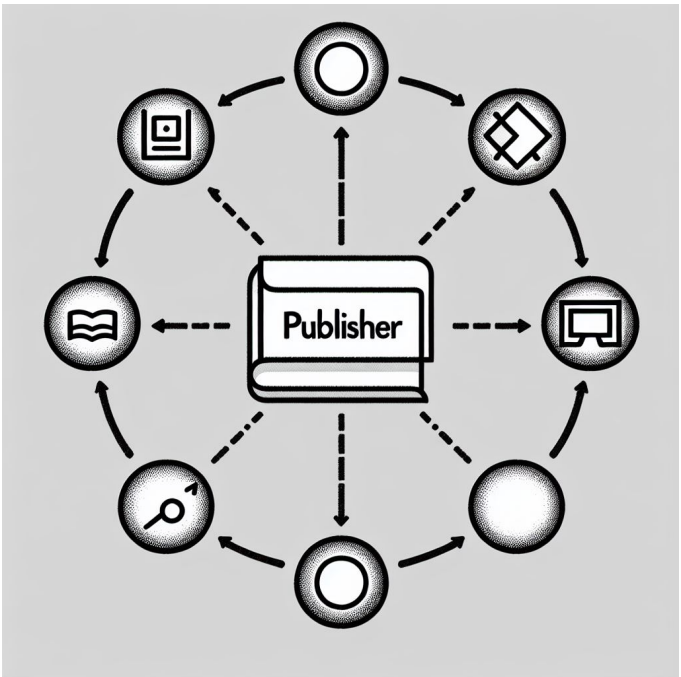
Supporting Materials

https://drive.google.com/drive/folders/18qA9Lzr9Rh_f_e39bK1DDD6fe4DWfXKc

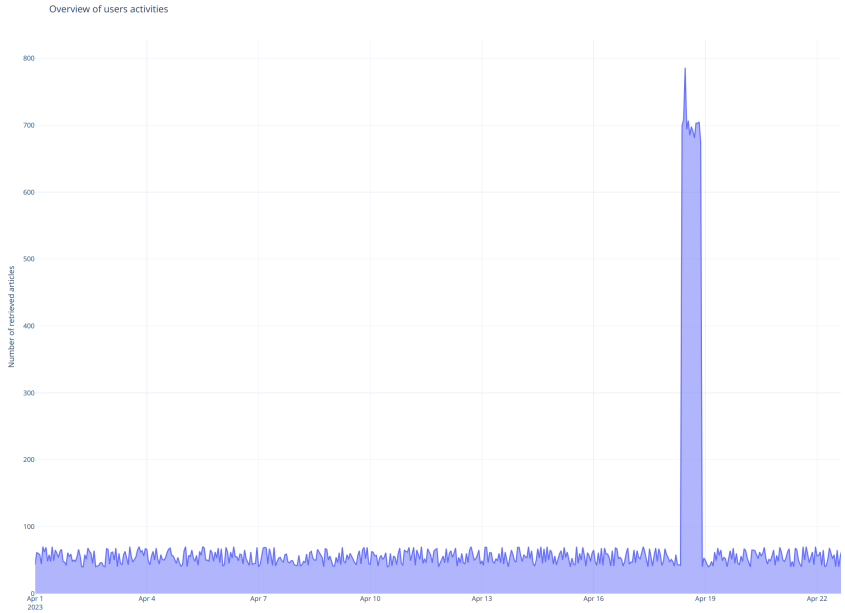
Stage-1, Incident begins, report to the Academic Hub (IdP/SP Proxy)

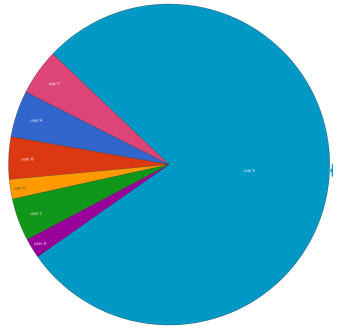
Publisher

- Publisher: This entity is responsible for publishing academic papers. They provide services such as peer review, editing, and distribution of research articles.
- Academic Hub: a consortium of universities that maintains a contract with the publisher.

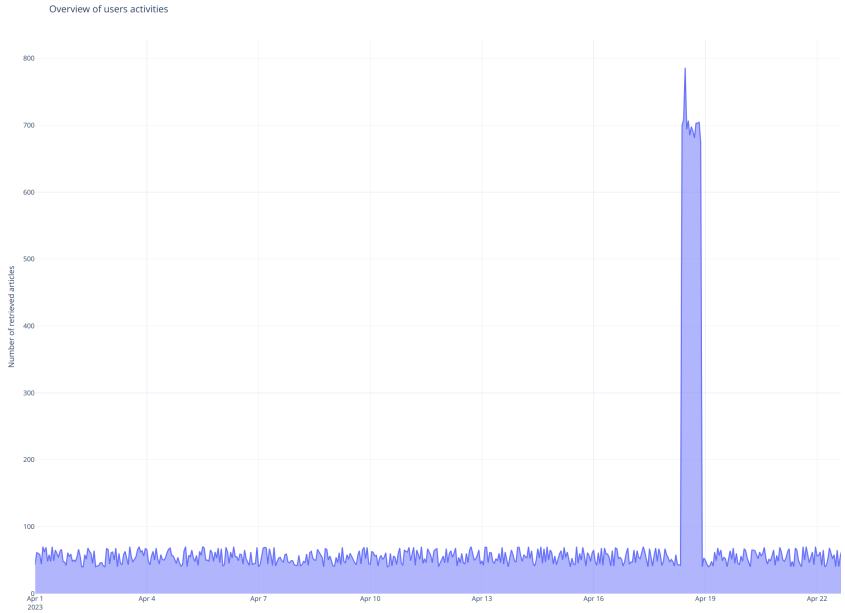


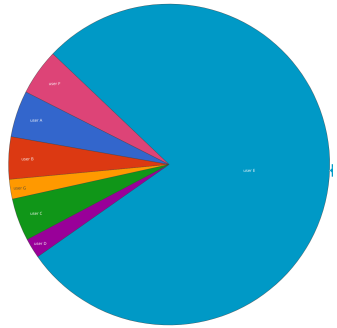
Usual business at a publisher





Usual business at a publisher





Complaints sent to the customer (the Academic Hub)

Subject: Notice of Excessive Content Downloads in Violation of AUP

Dear University Hub,

We are writing to inform you that our system has detected excessive content downloads from your organization's account, specifically from a user under the identifier **134273@uni-hub.org**, which exceeds the limitations set forth in our Acceptable Use Policy (AUP).

We understand that in some cases, such incidents may occur unintentionally. However, to ensure the continued quality of service and fairness for all users, we kindly request your cooperation in reviewing this matter and taking appropriate corrective actions.

We appreciate your prompt attention to this matter. If no corrective measures are taken, we may be required to take further action, which could include a temporary suspension of services, as per our policy.

Please don't hesitate to reach out if you need assistance or further information.

Thank you for your understanding and cooperation.

Kind regards,

John Smith

Stage-1, Incident begins, report reached operators @ Academic Hub

- Academic Hub operates an IdP/SP Proxy covering connected universities
- IdP/SP Proxy receives a request to verify legitimacy of a user, checks the logs.

Stage-1, Incident begins, report reached operators @ Academic Hub

- Academic Hub operates an IdP/SP Proxy covering connected universities
- IdP/SP Proxy receives a request to verify legitimacy of a user, checks the logs.
- the user identifier is `134273@uni-hub.org`, the access to the publisher SP is logged in logs of *University Hub* (logs-einfra.tx):

```
Apr 18 08:05:10 login3-d10 proxyaai/simplesamlphp[936]: 185.177.126.151 uni-hub NOTICE [ac2e8bef12] User ID: 134273, identifiers:
↪ [eduPersonUniqueId: 8ece13c45965afea5d48e203ac65d20f37bb0437d2bc38c3854290b714439382@uni.org, eduPersonPrincipalName:
↪ 19382@uni.org], service: https://brno-publishing.org/shibboleth/, external identity: 19382@uni.org from
↪ https://idp2.uni.org/idp/shibboleth
```

- Token life time issue.

Identifiers insight

- `eduPersonPrincipalName`: scoped identifier for a person.
  - SYNTAX: `user @ scope` where:
  - `user` is a name-based identifier (often the employee or student number).
  - `scope` is the administrative domain of the identity system.
- `eduPersonUniqueId`: unique, long-lived, non re-assignable, omnidirectional identifier.
  - SYNTAX: `uniqueID @ scope`
  - `uniqueID` is a string of 64 alphanumeric characters.
  - `scope` is the administrative domain of the identity system.

Stage-1, Incident verified

- The Academic Hub reaches out to university *uni.org* (the user's Identity provider), forwarding the publisher's complain is passed and the user's identifier (*19382@uni.org*)

Stage-1, Incident verified

- The Academic Hub reaches out to university *uni.org* (the user's Identity provider), forwarding the publisher's complain is passed and the user's identifier (*19382@uni.org*)
- The Uni Identity provider determines the recent activities to confirm or deny the report (*logs-uni.txt*)

Stage-1, Incident verified

- The Academic Hub reaches out to university *uni.org* (the user's Identity provider), forwarding the publisher's complain is passed and the user's identifier (*19382@uni.org*)
- The Uni Identity provider determines the recent activities to confirm or deny the report (*logs-uni.txt*)

```
4 2023-04-18T08:04:29.526861+02:00 id1.idm.uni.org 185.177.126.151 simplesamlphp NOTICE STAT [52c5045275] audit-login
  ↪ https://aai.uni-hub.eu/sp/shibboleth UNI_IdP 19382@uni.org
```

- IdP has a report of an Id potentially involved in activities violating AUP. What do they do?

```
4 2023-04-18T08:04:29.526861+02:00 id1.idm.uni.org 185.177.126.151 simplesamlphp NOTICE STAT [52c5045275] audit-login
  ↪ https://aai.uni-hub.eu/sp/shibboleth UNI_IdP 19382@uni.org
```

- IdP has a report of an Id potentially involved in activities violating AUP. What do they do?
  - IdP operator to contact user?

```
4 2023-04-18T08:04:29.526861+02:00 id1.idm.uni.org 185.177.126.151 simplesamlphp NOTICE STAT [52c5045275] audit-login
  ↪ https://aai.uni-hub.eu/sp/shibboleth UNI_IdP 19382@uni.org
```

- IdP has a report of an Id potentially involved in activities violating AUP. What do they do?
  - IdP operator to contact user?(y)
  - User (reliably) denies any relation to the activity in question

```
4 2023-04-18T08:04:29.526861+02:00 id1.idm.uni.org 185.177.126.151 simplesamlphp NOTICE STAT [52c5045275] audit-login
  ↪ https://aai.uni-hub.eu/sp/shibboleth UNI_IdP 19382@uni.org
```

- IdP has a report of an Id potentially involved in activities violating AUP. What do they do?
  - IdP operator to contact user?(y)
  - User (reliably) denies any relation to the activity in question
  - To who to report these findings?

```
4 2023-04-18T08:04:29.526861+02:00 id1.idm.uni.org 185.177.126.151 simplesamlphp NOTICE STAT [52c5045275] audit-login
  ↪ https://aai.uni-hub.eu/sp/shibboleth UNI_IdP 19382@uni.org
```

- IdP has a report of an Id potentially involved in activities violating AUP. What do they do?
  - IdP operator to contact user?(y)
  - User (reliably) denies any relation to the activity in question
  - To who to report these findings?
- report to Fed Operator

```
2023-04-18T08:04:29.526861+02:00 id1.idm.uni.org 185.177.126.151 simplesamlphp NOTICE STAT [52c5045275] audit-login
↪ https://aai.uni-hub.eu/sp/shibboleth UNI_IdP 19382@uni.org
```

- IdP has a report of an Id potentially involved in activities violating AUP. What do they do?
  - IdP operator to contact user?(y)
  - User (reliably) denies any relation to the activity in question
  - To who to report these findings?
- report to Fed Operator
- What would/should the Fed Operator do with this info?

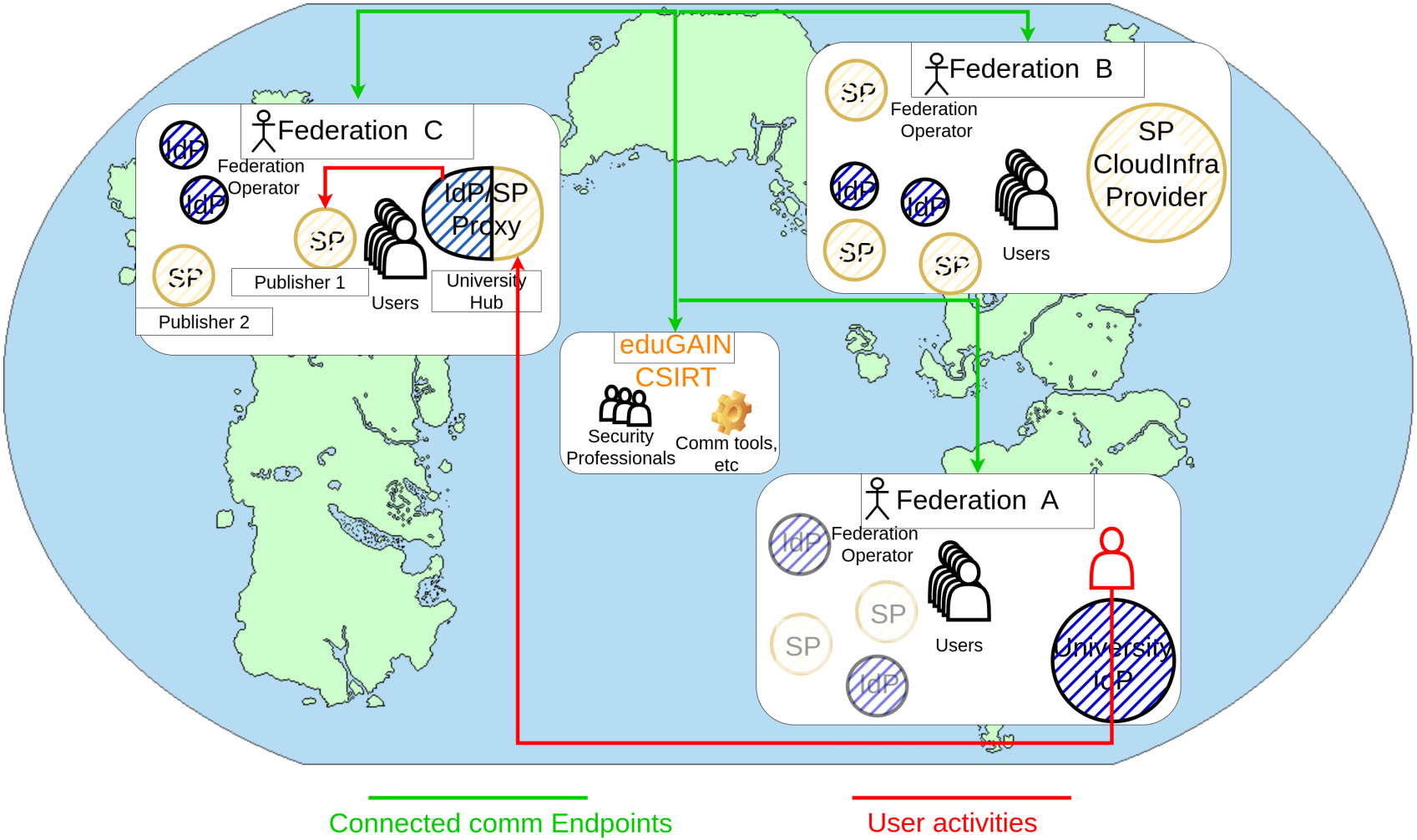
```
4 2023-04-18T08:04:29.526861+02:00 id1.idm.uni.org 185.177.126.151 simplesamlphp NOTICE STAT [52c5045275] audit-login
  ↪ https://aai.uni-hub.eu/sp/shibboleth UNI_IdP 19382@uni.org
```

- IdP has a report of an Id potentially involved in activities violating AUP. What do they do?
  - IdP operator to contact user?(y)
  - User (reliably) denies any relation to the activity in question
  - To who to report these findings?
- report to Fed Operator
- What would/should the Fed Operator do with this info?
  - report it to eduGAIN CSIRT? Is it already an (potential) inter-federation incident?

```
4 2023-04-18T08:04:29.526861+02:00 id1.idm.uni.org 185.177.126.151 simplesamlphp NOTICE STAT [52c5045275] audit-login
  ↪ https://aai.uni-hub.eu/sp/shibboleth UNI_IdP 19382@uni.org
```

- IdP has a report of an Id potentially involved in activities violating AUP. What do they do?
  - IdP operator to contact user?(y)
  - User (reliably) denies any relation to the activity in question
  - To who to report these findings?
- report to Fed Operator
- What would/should the Fed Operator do with this info?
  - report it to eduGAIN CSIRT? Is it already an (potential) inter-federation incident?
  - Case has the potential to affect other federations, eduGAIN CSIRT gets informed.

End of Stage-1



Findings: User account likely breached, Identifier of the user changes with every IdP/SP Proxy involved.

Stage-2, Incident spreads

Stage-2, Incident spreads

- eduGAIN CSIRT aggregates current findings and reports on the compromised identity
  - Two identifiers so far: *19382@uni.org* and *134273@uni-hub.org*
- Compromised identity is shared with the federation operators
- What does the IdP hosting the compromised identity do?

Stage-2, Incident spreads

- eduGAIN CSIRT aggregates current findings and reports on the compromised identity
  - Two identifiers so far: *19382@uni.org* and *134273@uni-hub.org*
- Compromised identity is shared with the federation operators
- What does the IdP hosting the compromised identity do?
- Suspend Identity.

Stage-2, Incident spreads

- eduGAIN CSIRT aggregates current findings and reports on the compromised identity
  - Two identifiers so far: *19382@uni.org* and *134273@uni-hub.org*
- Compromised identity is shared with the federation operators
- What does the IdP hosting the compromised identity do?
- Suspend Identity.
- Fed Ops share IoC (compromised Identity) with end entities/Federation Participants (IdPs, SPs)

Stage-2, Incident spreads

- eduGAIN CSIRT aggregates current findings and reports on the compromised identity
  - Two identifiers so far: *19382@uni.org* and *134273@uni-hub.org*
- Compromised identity is shared with the federation operators
- What does the IdP hosting the compromised identity do?
- Suspend Identity.
- Fed Ops share IoC (compromised Identity) with end entities/Federation Participants (IdPs, SPs)
- SPs need to check their logs for IoCs

Stage-2, Incident spreads

- A community cloud provider finds another activity of the user in question (in `logs-community.txt`).

Stage-2, Incident spreads

- A community cloud provider finds another activity of the user in question (in `logs-community.txt`).

```
2023-04-19T16:30:30.751015+02:00 idp3.community.edu 212.8.243.71 simplesamlphp INFO [7769d2ae22] Authentication source
↪ 'https://aai.uni-hub.eu/sp/shibboleth': User 134273 logged in to service OpenStack@community.edu; UA Mozilla/5.0 (Android 13;
↪ Mobile; rv:109.0) Gecko/111.0 Firefox/111.0
```

Note: the access could also be identified by uni-hub (from the IdP log)

- The compromised identity was used to obtain an account in the Community cloud facility
- What the Community cloud service needs to do?

Stage-2, Incident spreads

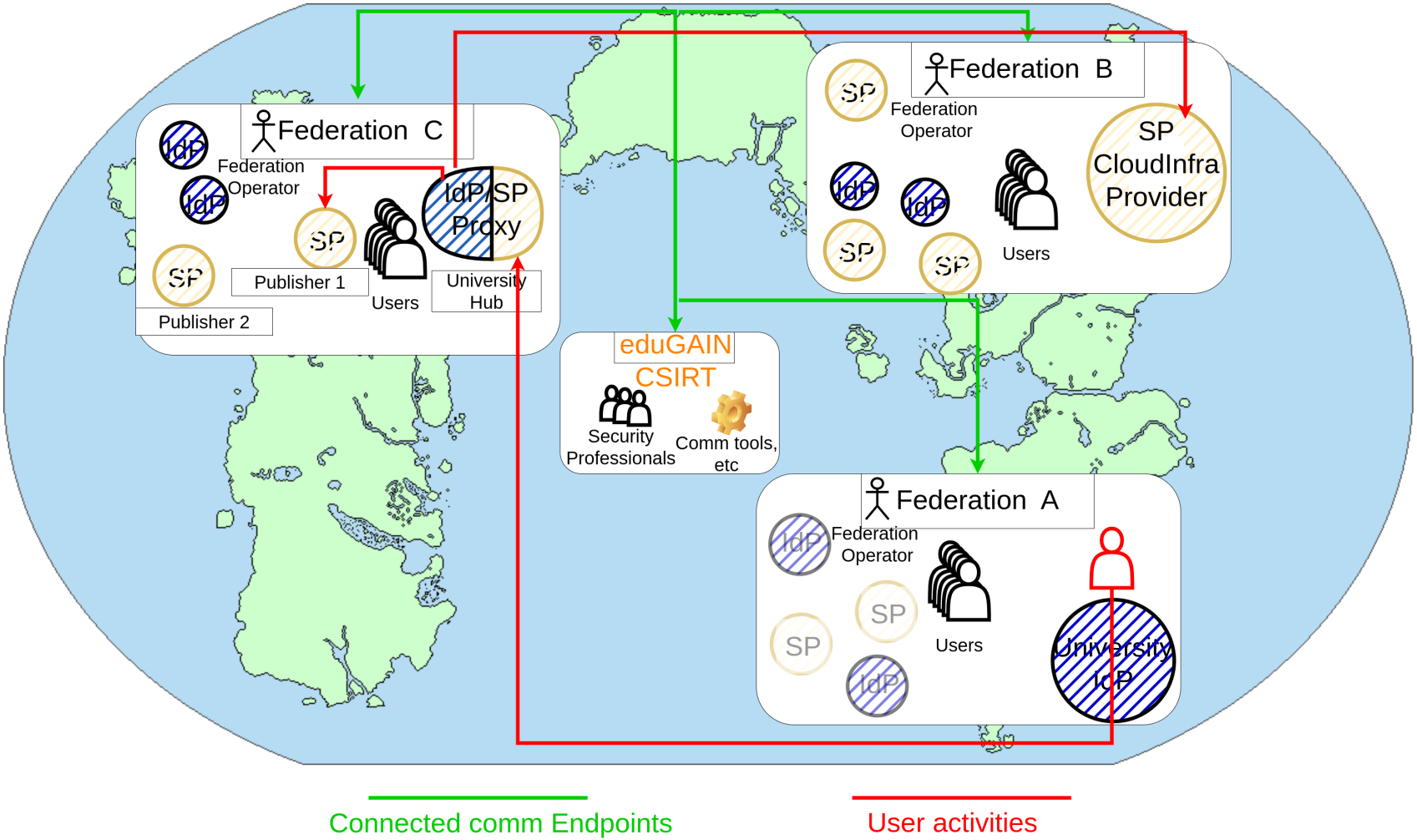
- A community cloud provider finds another activity of the user in question (in `logs-community.txt`).

```
2023-04-19T16:30:30.751015+02:00 idp3.community.edu 212.8.243.71 simplesamlphp INFO [7769d2ae22] Authentication source
↪ 'https://aai.uni-hub.eu/sp/shibboleth': User 134273 logged in to service OpenStack@community.edu; UA Mozilla/5.0 (Android 13;
↪ Mobile; rv:109.0) Gecko/111.0 Firefox/111.0
```

Note: the access could also be identified by uni-hub (from the IdP log)

- The compromised identity was used to obtain an account in the Community cloud facility
- What the Community cloud service needs to do?
- Cloud checks network connections to VM and other activities. The machine is:
  - deleted
  - stopped

End of Stage-2



Findings: User account likely breached, Identifier of the user changes with every IdP/SP Proxy involved.

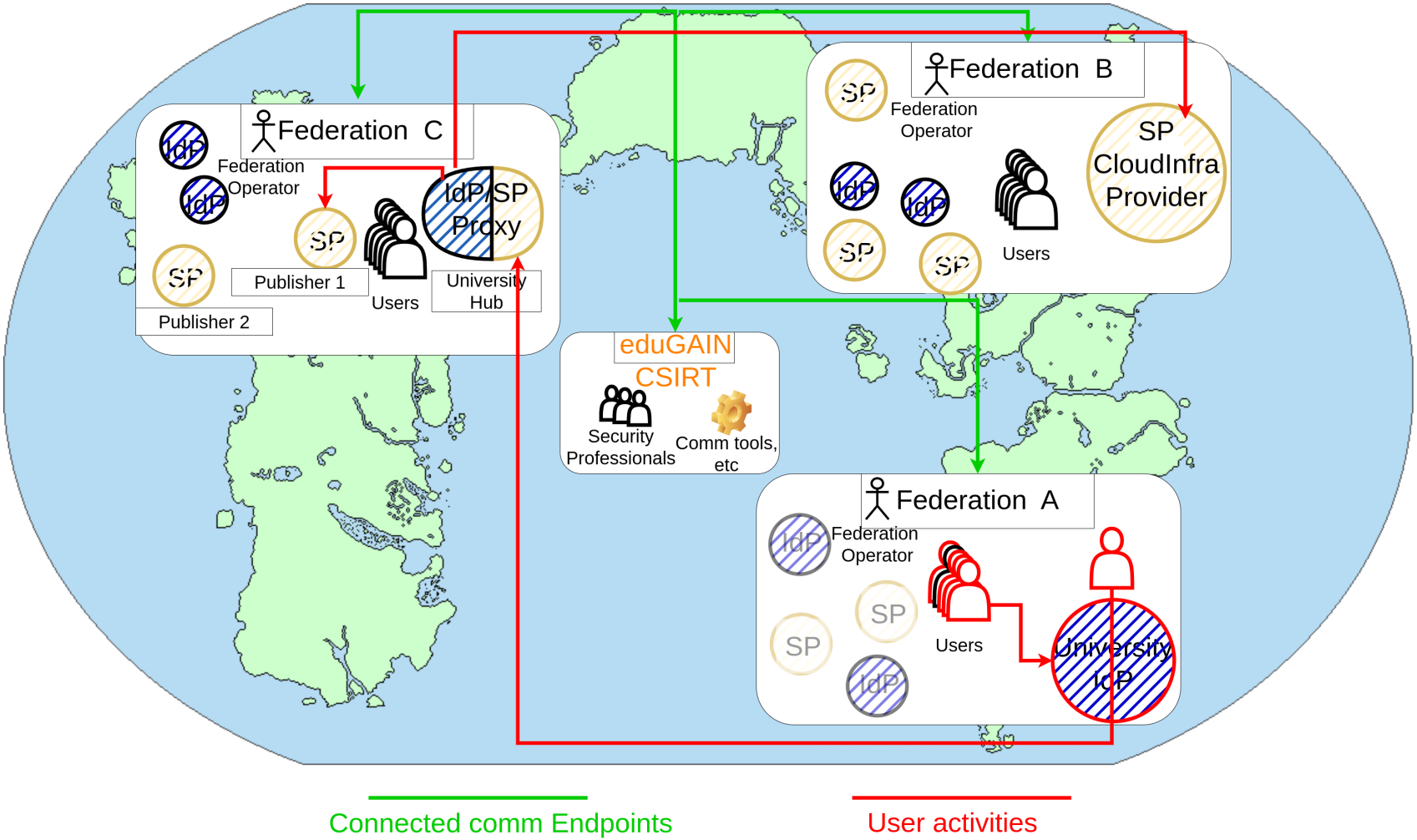
Stage-3, Investigation starts

Stage-3, eduGAIN CSIRT starts own investigation

(Spoiler, we never did this). Rumours has it that Identities/Accounts are traded on the darkweb `http://abacusmu34ooa6hoyg7xic5j2gztky3rplpsbvmqxk6ywnyqb433poyd.onion`.
Some of us tried to log in, but failed to pass the captcha challenge :-(so no fancy screen shots.
Findings:

- many Ids from IdP in question are on the marked, selling cheap.
- checking the software of the IdP in question show its heavily outdated.
- assumption IdP is compromised

End of Stage-3



Findings: User account likely breached, Identifier of the user changes with every IdP/SP Proxy involved.

Stage-4, Compromised IdP you say ...

If you need some advise on how this problem **can** be addressed **and** get some international attention, , ask Univ. Giessen:

Bei der Ausgabe der neuen Passwörter kommt es zum Teil zu langen Schlangen. FOTO: LKL © Lena Karber

`https://www.bbc.com/news/technology-50838673`

Stage-4, Situation

Situation:

- Compromised identity, how it got lost unclear.
- Moreover, indications that the IdP is controlled by someone else.
- Identity used at IdP/SP proxy to create an identity (token) which is used at SP-1 (publisher) and SP-2 (Community cloud)
- Compromised identity is suspended at IdP

Stage-4, Situation

Situation:

- Compromised identity, how it got lost unclear.
- Moreover, indications that the IdP is controlled by someone else.
- Identity used at IdP/SP proxy to create an identity (token) which is used at SP-1 (publisher) and SP-2 (Community cloud)
- Compromised identity is suspended at IdP
- What is the effect of suspending the compromised identity?

Stage-4, Situation

Situation:

- Compromised identity, how it got lost unclear.
- Moreover, indications that the IdP is controlled by someone else.
- Identity used at IdP/SP proxy to create an identity (token) which is used at SP-1 (publisher) and SP-2 (Community cloud)
- Compromised identity is suspended at IdP
- What is the effect of suspending the compromised identity?
- Started VMs will continue to run until the SP-2 manually suspends VMs

Stage-4, Situation

Situation:

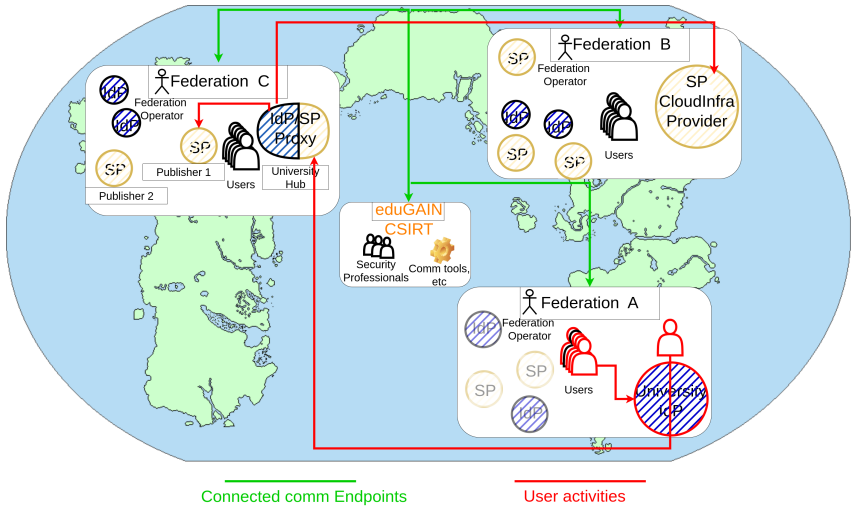
- Compromised identity, how it got lost unclear.
- Moreover, indications that the IdP is controlled by someone else.
- Identity used at IdP/SP proxy to create an identity (token) which is used at SP-1 (publisher) and SP-2 (Community cloud)
- Compromised identity is suspended at IdP
- What is the effect of suspending the compromised identity?
- Started VMs will continue to run until the SP-2 manually suspends VMs
- Created token will remain valid, no means to "revoke" it

Stage-5, Incident handling

Stage-5, Incident Handling

given the situation described in the previous section, groups try to find answers to the following question (10 min):

- What can/would the Federation Operator of the potentially compromised IdP do?
- if the Fed Operator suggests the IdP shuts down, IdP Operator explains his/her situation (see ../../supporting_material/compromised_idp_situation.txt)
- What would the IdP operator do (besides reading job adverts)?
- What can/would eduGAIN CSIRT do?
- What can/would SP operators do,



Stage-6, Incident resolved, close out report

Stage-6, Incident resolved, close out report (lessons learned)

All groups collectively provide input to the close out report:

- What happened?
- How was it addressed?
- Did the procedures work?
- What to change in the procedures/policies?