ISGC 2024 Security Day

eduGAIN security Table Top Exercise (TTX)

Sven Gabriel

Nikhef/EGI CSIRT

March 25 2024

Agenda

- Intro to eduGAIN (M. Kremers)
- SIRTFI v1,2 (D. Kelsey)
- eduGAIN CSIRT (Sven Gabriel)
- Incident Response in eduGAIN (S. Gabriel)
- eduGAIN TTX (S. Gabriel, D. Groep, M, Kremers, D. Kelsey)
- lunchbreak
- Capture The Flag (CTF) in SSC 23.03 (S.Gabriel)
- Forensics 101 in context of the CTF (D. Groep)
- CTF, solve the riddles :-)

Intro to eduGAIN (M. Kremers)

SIRTFI v1,2 (D. Kelsey)

Incident Response in eduGAIN (S. Gabriel)

eduGAIN security: Task/Problem

Task: Build a security team for eduGAIN (Parts of this was presented 2020 at a Gèant meeting in Ljubljana)

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 (▸ CRFC 2350, ▸ TOR, mandate, services, ...etc.). Trust is in Organzations/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: 5801 (IdPs 3174, SPs 2625 + 4 Standalone AAS) organised in 68 participants (Federations).

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

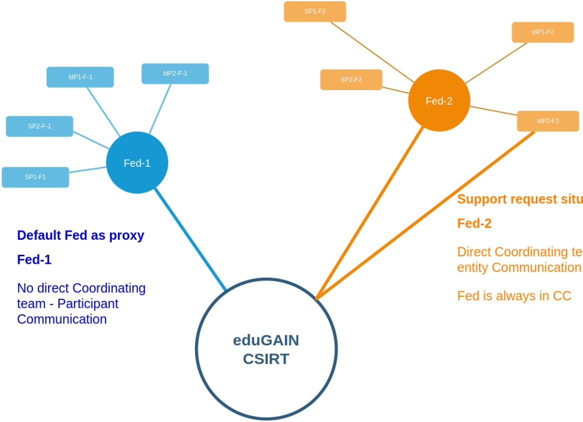
Role, Functions of the Security Team

- 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.

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 function depends on operational Communications Infra



Default Fed as proxy

Fed-1

No direct Coordinating team - Participant Communication

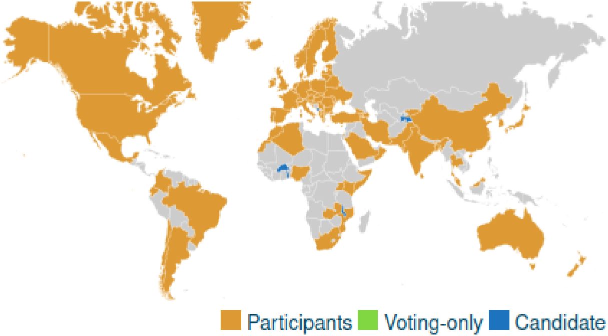
Support request situation

Fed-2

Direct Coordinating team - end entity Communication

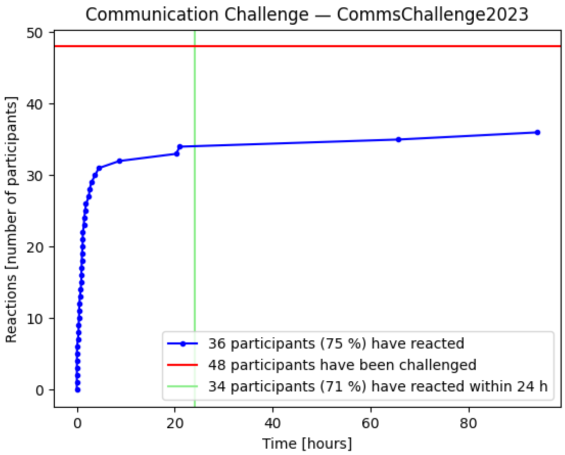
Fed is always in CC

Testing the Communications Infra



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

Testing the Communications Infra



Key elements from IR Handbook, relevant for the TTX

- Roles and responsibilities for IdP, SP operators. Federation Operators and eduGAIN CIRT.
- Description of the communication flow.
- For each role an Incident Response checklist is provided.
- For the rest, ...just read it, Its just 7 pages :-)