SEE Identity Federation Training

eduGAIN Policies and Membership
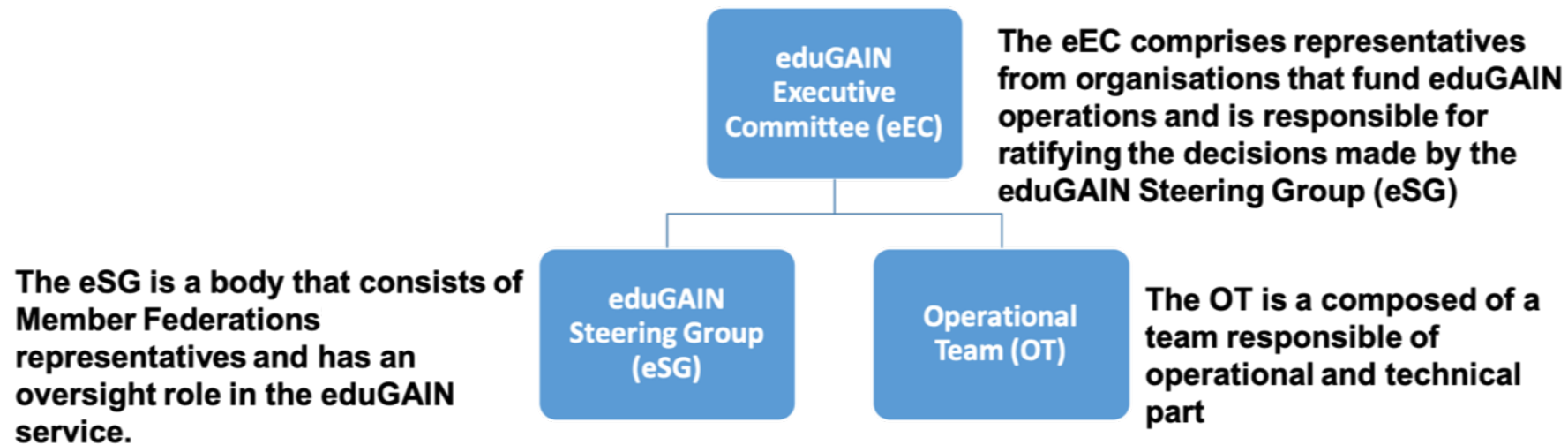
April 20, 2021

Slides v1.0

www.geant.org

eduGAIN Constitution

- The eduGAIN service enables National Federations to interfederate. The Member Federations primarily serve the authentication and authorization interests of research and education sectors.

- An Entity (SP/IdP) is always registered by a Participant Federation which uses an appropriate mechanism to exchange its metadata stream of Entities via eduGAIN as described in the Technology Profiles. **It means that an Entity can't joint eduGAIN directly without being registered by a federation.**

https://technical.edugain.org/doc/eduGAIN-Constitution-v3ter-web.pdf

Governance and Governing Bodies

eduGAIN Executive Committee (eEC)

The eEC comprises representatives from organisations that fund eduGAIN operations and is responsible for ratifying the decisions made by the eduGAIN Steering Group (eSG)

The eSG is a body that consists of Member Federations representatives and has an oversight role in the eduGAIN service.

eduGAIN Steering Group (eSG)

Operational Team (OT)

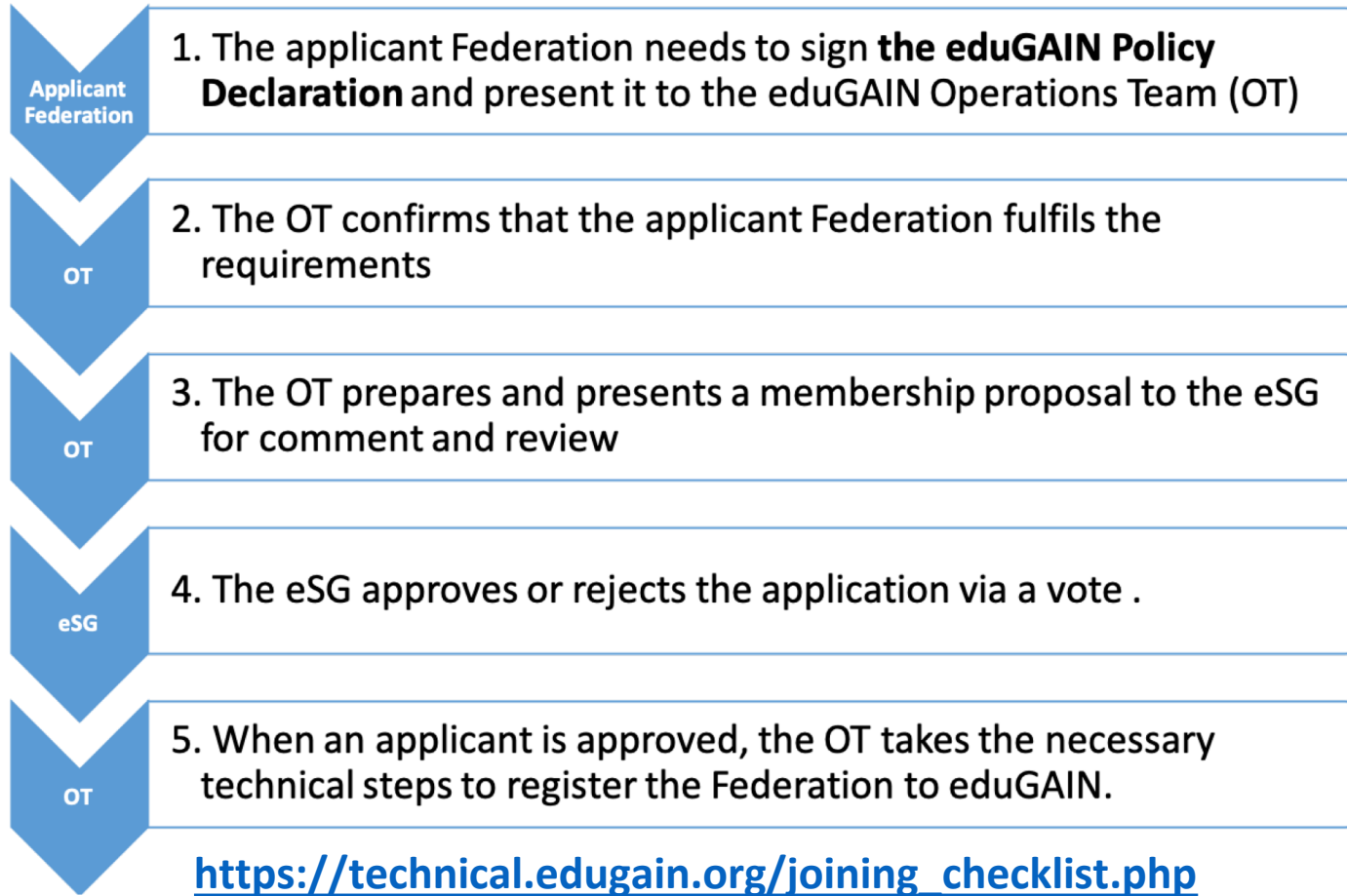The OT is a composed of a team responsible of operational and technical part

Prerequisites to join eduGAIN as a Federation

- Participant Federations MUST:
  - **Primarily serve the interests of the education and research sector.**
  - Provide a point of contact for their Members for dealing with technical issues.
  - Provide processes for handling complaints and incidents involving their Members.
  - **Meet the requirements of the eduGAIN Policy Declaration.**
  - Have an agreement defining federation membership between the Federation and its members (typically known as a Federation Policy or Metadata registration practice statement).

  EduGAIN Policy Declaration: https://technical.edugain.org/doc/eduGAIN-Declaration-v2bis-web.pdf

4

How to join eduGAIN as Identity Federation

Applicant Federation
1. The applicant Federation needs to sign **the eduGAIN Policy Declaration** and present it to the eduGAIN Operations Team (OT)

OT
2. The OT confirms that the applicant Federation fulfils the requirements

OT
3. The OT prepares and presents a membership proposal to the eSG for comment and review

eSG
4. The eSG approves or rejects the application via a vote .

OT
5. When an applicant is approved, the OT takes the necessary technical steps to register the Federation to eduGAIN.

https://technical.edugain.org/joining_checklist.php

GÉANT

Joining steps: Non-technical

1. The first steps towards joining eduGAIN is to register the Federation's interest in joining by communicating this to the eduGAIN Operations Team. Send an email message to edugain@geant.org stating the interest to join eduGAIN and containing contact details (email address, full name) for eduGAIN related matters.

2. A person who is authorized to represent the federation should then sign the printed document and send it to the postal address of the eduGAIN Operations Team:

    eduGAIN c/o GÉANT
    Level 6
    Hoekenrode 3
    1012BR Amsterdam
    The Netherlands

    A scanned version of the signed declaration should be sent via signed email to the following address edugain@geant.org.

Joining steps: Technical

Being an eduGAIN Member federation on a technical level mostly means exchanging SAML2 metadata with eduGAIN.

There are basically two metadata files exchanged between a federation operator and eduGAIN:

1. **eduGAIN Upstream metadata:** The upstream metadata contains all entities (IdPs and SPs) of a member federation that should be included in eduGAIN metadata. The upstream metadata is provided by the federation operator for consumption by the eduGAIN Metadata Distribution Service (MDS).

2. **eduGAIN Downstream metadata:** The eduGAIN Downstream metadata contains all entities in eduGAIN. It is generated and published by the eduGAIN Metadata Distribution Service (MDS)

www.geant.org

Joining steps: Technical

Provide the necessary Federation information:

- The URL where the Federation publishes its metadata.
- The signing certificate with which Federation metadata is signed.
- The full names and email addresses of the delegate and the deputy delegate of the Federation.
- The URL pointing to the website (English version, if available) of the Federation.
- The URL pointing to the English version of Metadata Registration practice statement (MRPS) for the federation.
- The URL pointing to the English version of the Federation's policy.

Technical requirements to join eduGAIN as a Federation

1. **Be compliant with the eduGAIN SAML 2.0 Metadata Profile if it decides to exchange the metadata of Entities via eduGAIN**

2. **Before joining eduGAIN you might want to consider how the entities (Identity and Service Providers) in your federation can join eduGAIN.** There are basically two choices:
   - **Opt-In:** In this model each Service Provider (SP) and Identity Provider (IdP) of a federation has to do something to get included in eduGAIN.
   - **Opt-Out:** In this model Service Provider (SP) and Identity Provider (IdP) of a federation don't have to do anything specifically to be exposed to eduGAIN

For new Federations which do not have many IdPs and SPs, it's better to start with the Opt-In model.

If the number of IdPs and SPs increase considerably, a good choice is to use the opt-out model for IdPs and an opt-in model for SPs

Guide for Joining eduGAIN as a Federation :
https://wiki.geant.org/display/eduGAIN/Guide+for+Joining+eduGAIN+as+a+Federation

Thank you

Any questions?

www.geant.org