

Deployment & Usage of eduGAIN

Anass CHABLI : Head of Security of Services Department (RENATER)

WACREN NREN CEOs Academy - eduGAIN in practice

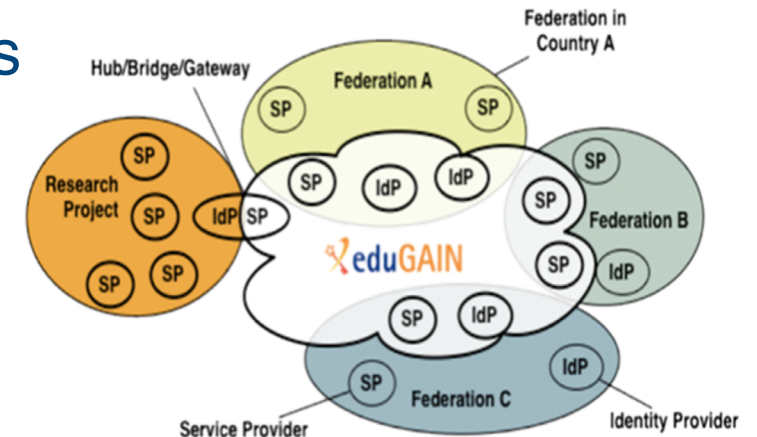
08/12/2021

Deployment of eduGAIN

- How to deploy eduGAIN ?
- What is identity Federation ?
- Why would you need an Identity Federation ?
- Role of NRENs
- What is needed to build an Identity Federation & join eduGAIN?

How to deploy eduGAIN ?

- The right question would be : How to join eduGAIN ?
 - eduGAIN is a inter-federation service connects Identity Federations around the world
- To join eduGAIN you need to :
 - Primarily serve the interests of the education and research sector
 - Have an identity Federation
 - Meet the requirement of the eduGAIN Constitution (detailed later)



How to build an Identity Federation ?

- 1. What is Identity Federation ?**
- 2. Why would you need an Identity Federation ?**
- 3. What is needed to build an Identity Federation & join eduGAIN?**

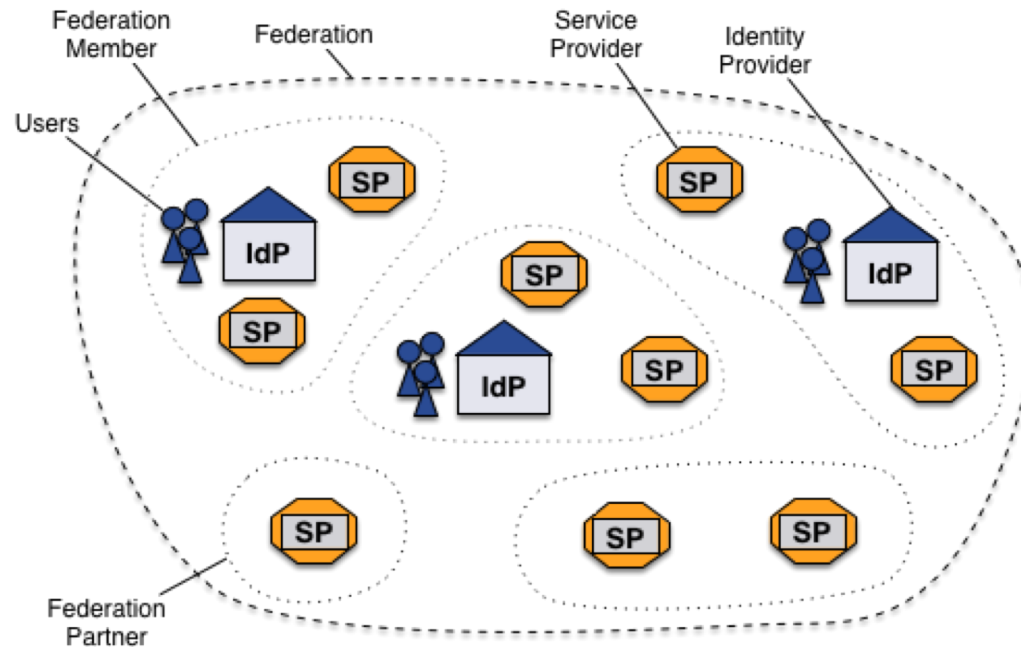
Deployment of eduGAIN

- How to deploy eduGAIN ?
- What is identity Federation ?
- Why would you need an Identity Federation ?
- Role of NRENs
- What is needed to build an Identity Federation & join eduGAIN?

What is Identity Federation ?

A group of organizations running IdPs and SPs that agree on a common set of rules and standards

The grouping can be on a regional level or on a smaller scale (e.g. large campus)



IdPs and SPs are not linked directly but they **know** each others thanks to Federations

An organization may belong to more than one federation at a time

Deployment of eduGAIN

- How to deploy eduGAIN ?
- What is identity Federation ?
- Why would you need an Identity Federation ?
- Role of NRENs
- What is needed to build an Identity Federation & join eduGAIN?

Why would you need an Identity Federation ?

The first principle within federated identity management (FIM) is the active protection of user information



Protect the user's credentials - *only the IdP ever handles the credential*



Protect the user's identity information, including identifier - *customized set of information released to each SP*

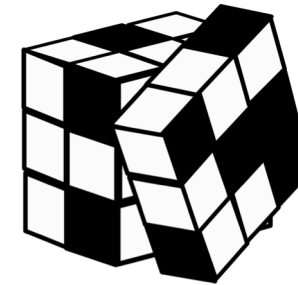


Different levels of identity management

- Local authentication



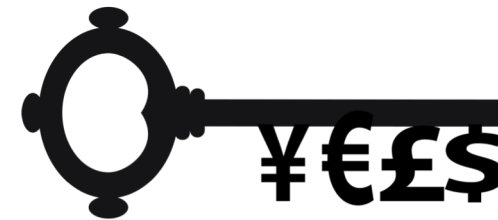
- Delegated authentication to N identity providers



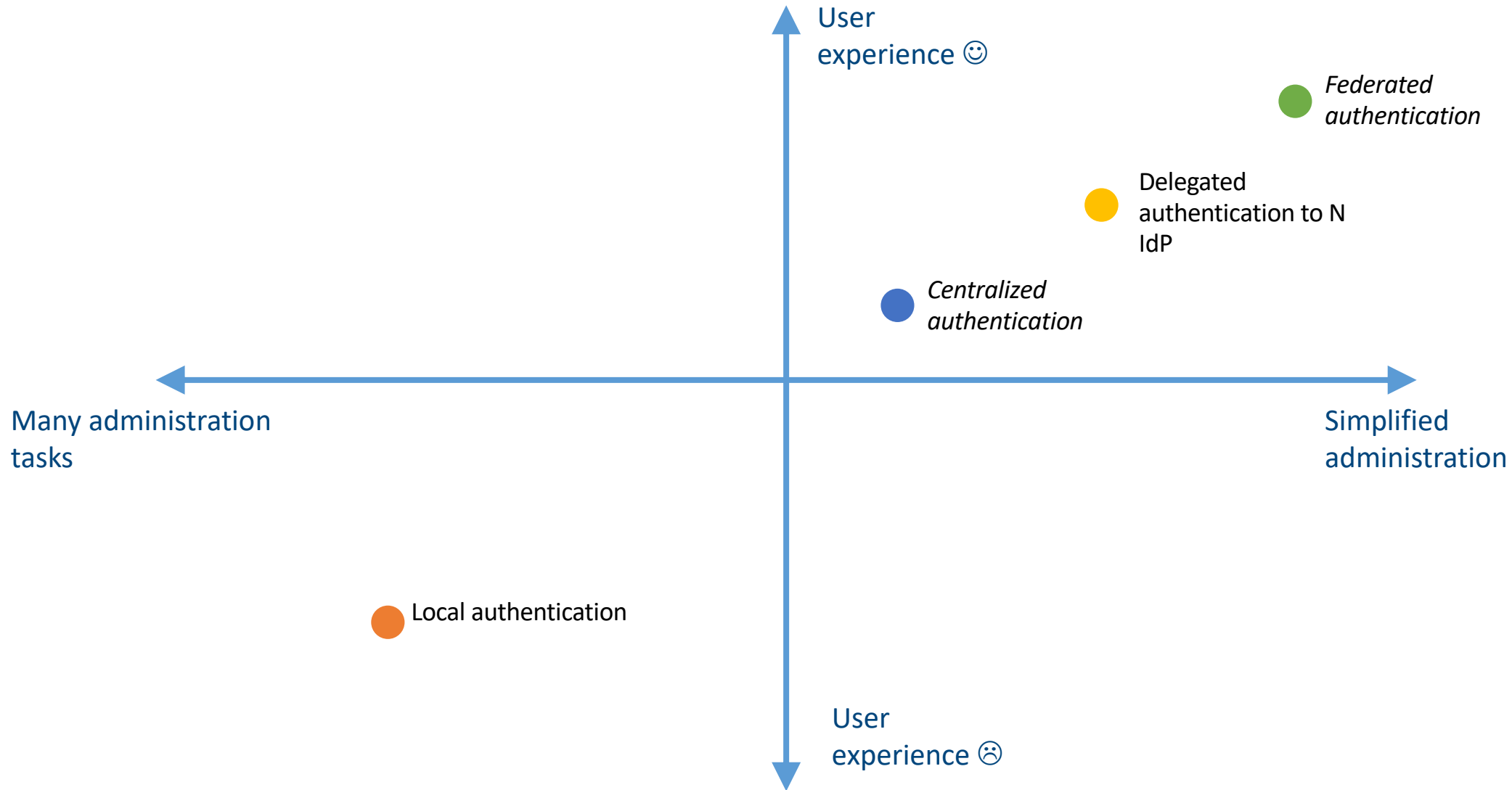
- Centralized or delegated authentication to 1 Identity Provider



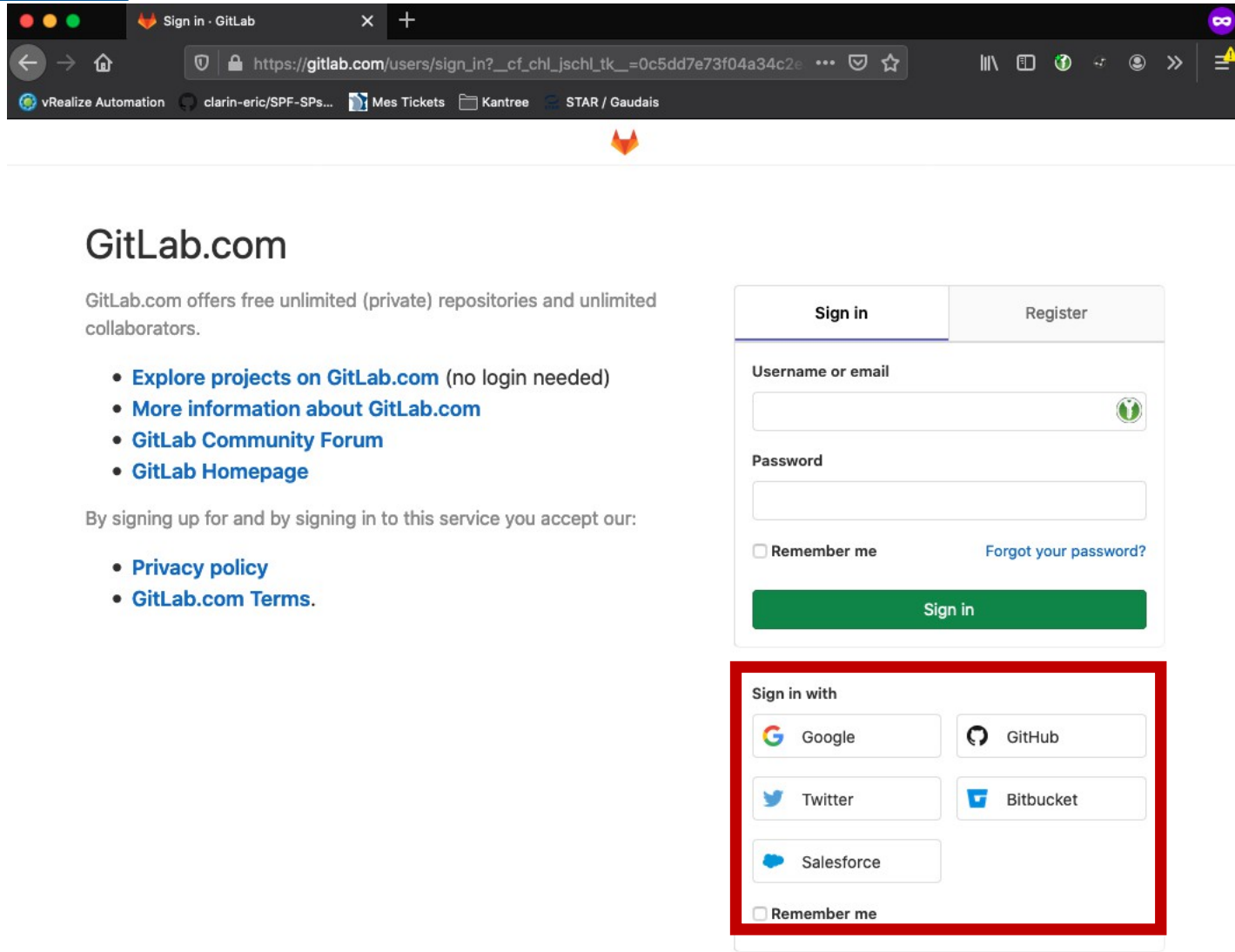
- Federated authentication



Comparison of the different levels



Example



Sign in - GitLab

https://gitlab.com/users/sign_in?__cf_chl_jschl_tk__=0c5dd7e73f04a34c2e...

vRealize Automation clarin-eric/SPF-SPs... Mes Tickets Kantree STAR / Gaudais

GitLab.com

GitLab.com offers free unlimited (private) repositories and unlimited collaborators.

- [Explore projects on GitLab.com](#) (no login needed)
- [More information about GitLab.com](#)
- [GitLab Community Forum](#)
- [GitLab Homepage](#)

By signing up for and by signing in to this service you accept our:

- [Privacy policy](#)
- [GitLab.com Terms.](#)

Sign in

Register

Username or email

Password

☐ Remember me

[Forgot your password?](#)

Sign in

Sign in with

 Google

 GitHub

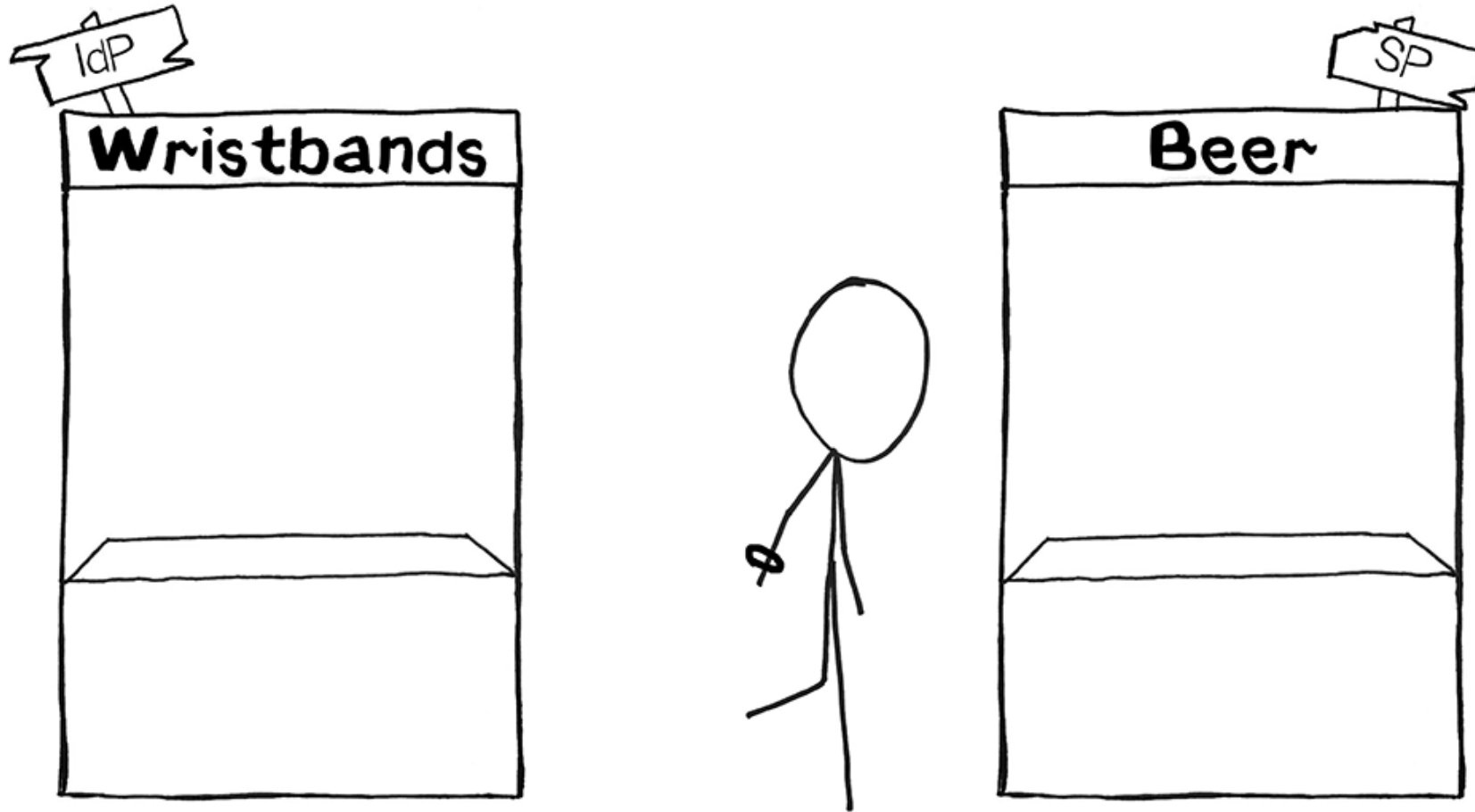
 Twitter

 Bitbucket

 Salesforce

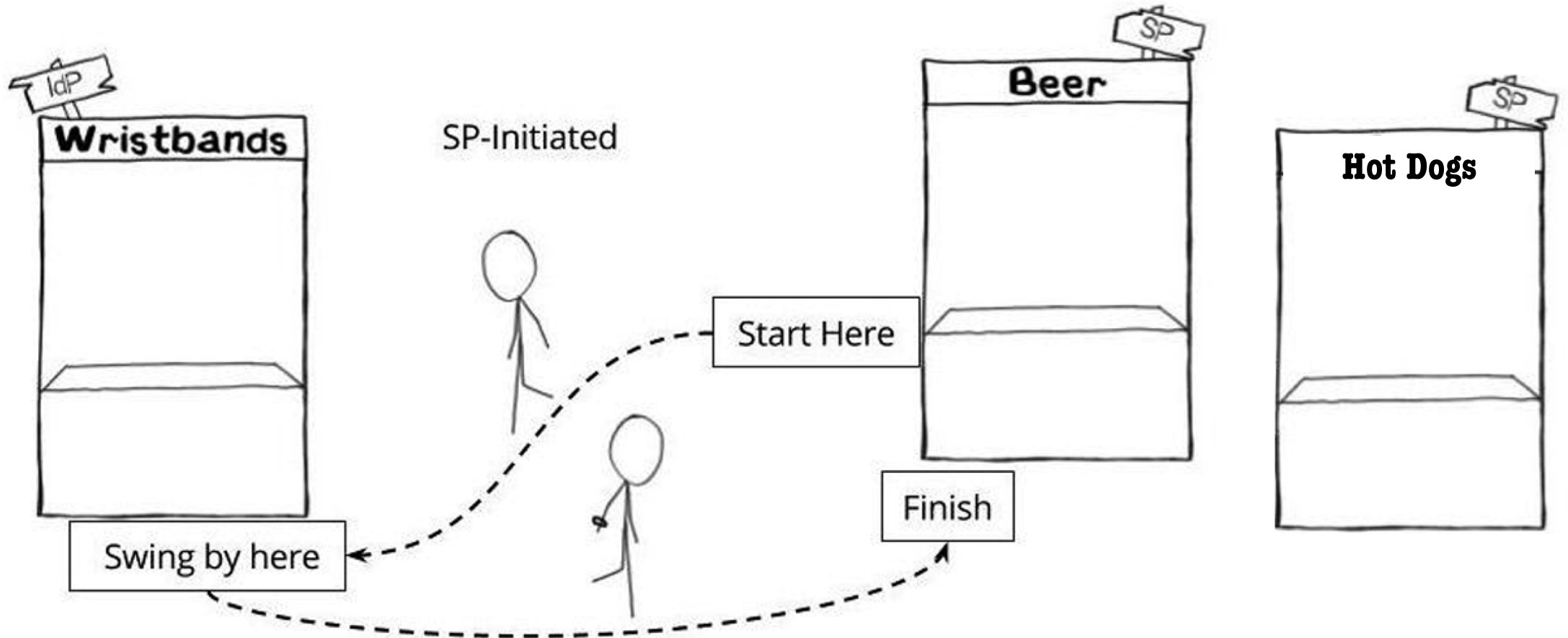
☐ Remember me

Example in real life



Crédit: <https://duo.com/blog/the-beer-drinkers-guide-to-saml>

Example in real life



Crédit: <https://duo.com/blog/the-beer-drinkers-guide-to-saml>

Benefits from Identity Federation

Reduces work

- Authentication-related calls to support team reduce scientifically (1 login/password for each user and for all services)

Provides current data

- Studies of applications that maintain user data show that the majority of data is out of date. Are you “protecting” your app with stale data?

Insulation from service compromises

- In FIM data is pushed to services as needed. If those services are compromised the attacker can't get everyone's data.

Minimize attack surface area

- Only the IdP needs to be able to contact user data stores. All effort can be focused on securing this one connection instead of one or more connections per service.

Deployment of eduGAIN

- How to deploy eduGAIN ?
- What is identity Federation ?
- Why would you need an Identity Federation ?
- **Role of NRENs**
- What is needed to build an Identity Federation & join eduGAIN?

Role of NRENs

At a minimum a federation maintains the list of which IdPs and SPs are in the federation

Most federations also

- Define agreements, rules, and policies
- Provide some user support (documentation, email list, etc.)
- Operate a central discovery service and test infrastructure

Some federations

- Provide self-service tools for managing IdP and SP data (Resource Registry)
- Provide application integration support
- Host or help with outsourced IdPs (IdP in the Cloud, hosted IdP)
- Provide tools for managing "guest" users
- Develop custom tools for the community



Role of NRENs (in eduGAIN)

Governance and Governing Bodies

- eduGAIN Executive Committee (eEC)
- eduGAIN Steering Group (eSG)
- Operational Team (OT)



Participant Federations MUST:

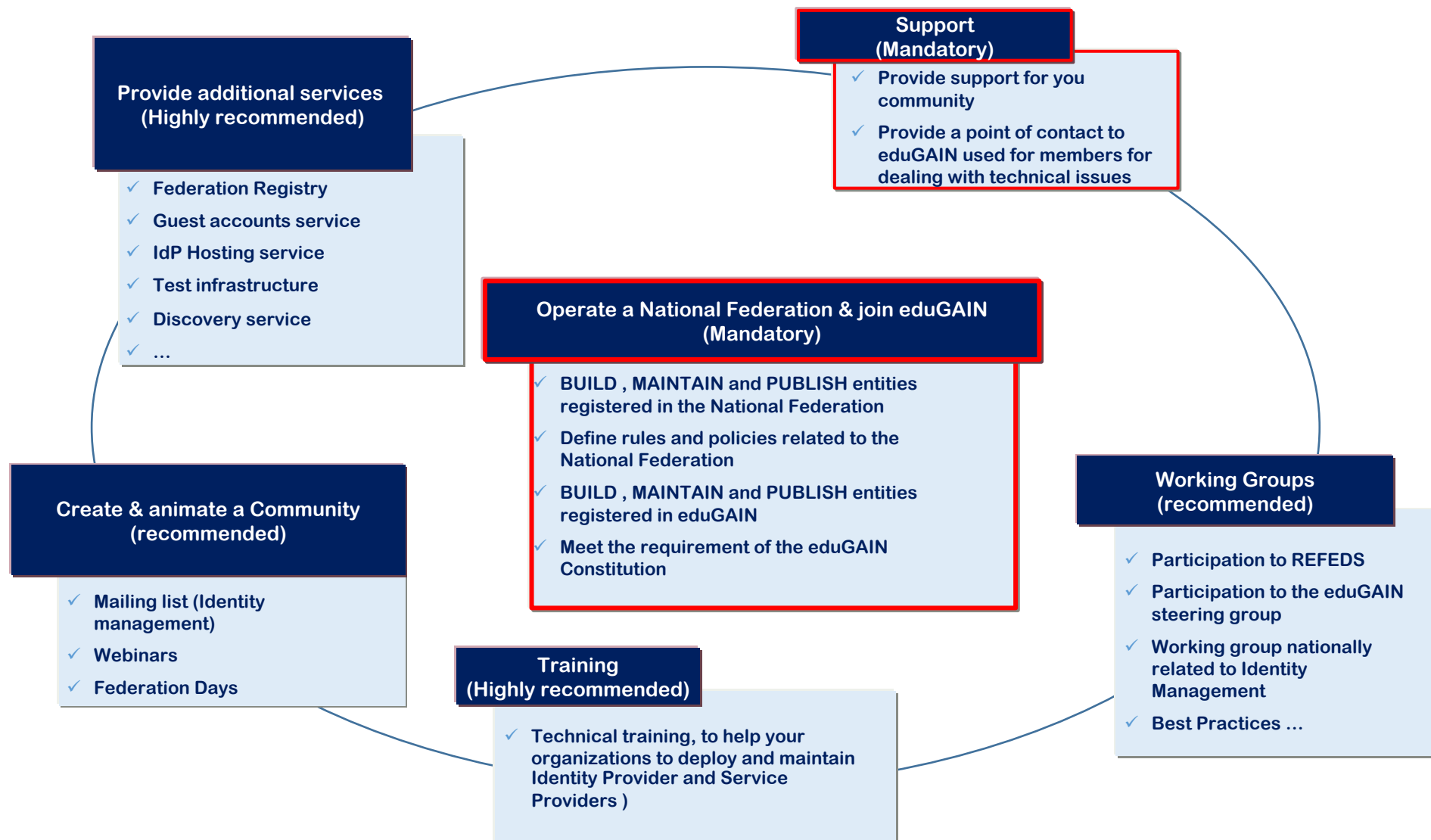
- Primarily serve the interests of the education and research sector.
- Provide a point of contact for their Members for dealing with technical issues.
- Provide processes for handling complaints and incidents involving their Members.
- Have a published Metadata registration practice statement.
- Follow the eduGAIN SAML 2.0 Metadata Profile



Deployment of eduGAIN

- How to deploy eduGAIN ?
- What is identity Federation ?
- Why would you need an Identity Federation ?
- Role of NRENs
- What is needed to build an Identity Federation & join eduGAIN ?

What is needed to build an Identity Federation & join eduGAIN?



Most important

TRAIN the TRAINERS





Thanks !

Time for questions

anass.chabli@renater.fr