Ubuntunet Identity Federation Training

Identity Federation: How to support your community

www.geant.org

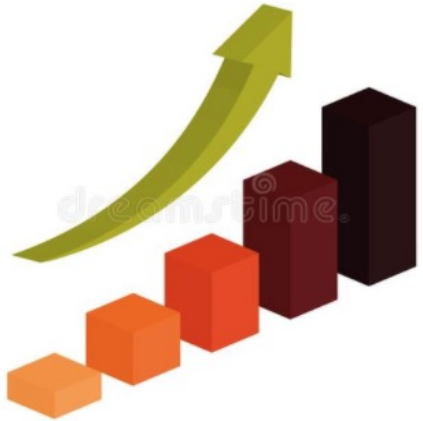
Content

- Getting to know your community
- Building trust
- Onboarding to federated Identity Management
  - Supporting IdPs
  - Supporting SPs
  - Central Discovery Service
- You are not alone

Getting to know your community

- It is fundamental **to get to know your user community**
  - **End Users are the ultimate reason for providing services** and implementing Identity Federations and related tools
  - User are usually initially shy or unaware of what their potential benefit is in endorsing federated identity
- Key element to involve users is to bootstrap a **virtuous user engagement cycle:**
  - Users successfully access federated services
  - They benefit from Web SSO and services published in eduGAIN and engage in global Research collaborations
  - Research grows and involves more disciplines, more end users, more data, more online services
  - Being able to get to services and data becomes a wheel which further push for the onboarding of Service Providers and the establishment of institutional Identity Providers

The Virtuous Engagement Cycle



User successfully access federated services

Users experience benefits of WebSSO and engage in new research collaborations

Demand from new users grows to access federated services, data, resources

Awareness and stakeholders management commitments grow

New SPs and IdPs are spawned, more corresponding users are reached

Getting to know your community

- Involve your member institutions in:
  - **Tutorial events**
  - **Dissemination events** on Identity Federations and eduGAIN
  - **Informative workshops** on specific topics (e.g.: GEANT services)
  - **User engagement events** where researchers are invited to attend and present their work, needs, research workflows, data, computing and services requirements

- Use **surveys** to ask your member institutions about their internal departments, ongoing collaborations, desirable services, current needs, most critical issues impacting research

- Act as a **liaison engine** among member institutions to connect researchers, users' groups, Research Communities among themselves and to put them in touch with foreign, external communities

- Consolidate and **distribute the know-how** on Identity Federations, best practices, security, incident response, recommended procedures

Key aspect in the process of spawning an Identity Federation and a community around it is …..

picture from am-online.com

Building Trust

- Gaining and keeping the trust of your member institutions and user communities is a **daily demanding process, easily and quickly harmed by security incidents and breaches**.
- Violation of privacy matters, lack of due user consent requests, excessive and intrusive management policies can all harm your users' trust.
- **Federation Operators need to**
  - cope with the will and inclination of **single institutions about attribute release**
  - **encourage conscious and informed release of all fundamental, non optional attributes by IdP towards services**
  - make sure SPs apply policy for users to ensure they are always informed about the usage of their personal data and express consensus about them (SPs process personal data according to the relevant data protection laws)
  - **push for adoption/support to Entity Categories and SIRTFI** security incident framework in particular related to MD health and compliance (e.g. security contacts, logos..)
  - proactively inform the community of mandatory security patches/vulnerabilities
  - coordinate with eduGAIN support about all security incident related matters and adoption of new baseline expectations if/when needed
  - disseminate and evangelize about the protocols, best practices, tools to ensure knowledge is a spread and shared resource in the community

Building trust.. in practice

- Create open wikis and eLearning resources on:
  - SAML and OIDC/OAuth2 protocols
  - Best Practices and Guidelines on T&I
    (see for example https://aarc-project.eu/guidelines/)
  - Security related policies and guidelines
  - Monitoring and Incident Reporting
  - Further available online guides / best practices / educational resources
- Promote the adoption of Entity Categories: CoCo, SIRTFI and R&S
- Promote the adoption of security best practices
- Inform about relevant data protection laws. (e.g.: GDPR) and push for adoption of SIRTFI
- Be proactive towards your community about security measures
  - Echo toward the community about newly coming mandatory security patches related to popular applications or operating systems
  - Train IdP and SP admins about best practices on security
  - Inform all the relevant bodies and individuals in case of incident

Ensure Users and Institutions acting responsibly

- Users are often **not fully aware of the global scope** of the security implications **of their behaviors** - which can affect the whole community
  - Since an identity is globally spendable, misbehavior or breaches can impact everyone at the global scale
    - E.g.: not sharing your password with anyone else is not *“my own business”*
- Individual institutions should also endorse this **community perspective**
  - Again, since an identity is globally spendable, misbehavior or breaches can impact everyone at the global scale
    - E.g.: setting up a firewall to protect your LDAP server is no longer *“my own business”*

Support institutions for IdP deployment

- Many different ways:
  - **Host an instance on the cloud** at the NRENs/Federation premises
    - Include the IdM component, or
    - Leave the IdM component at the Institution's premises
  - **Provide pre-installed/pre-configured**
    - Virtual Machines Images for virtualization platforms (eg: VMware, KVM, Xen, Hyper V..) or private cloud (eg.Openstack Glance)
    - Docker Images
    - Docker Swarm deployment playbooks
  - **Deploy IdP on Public Cloud Providers or an Hybrid Cloud** platform
    - by implementing VPN tunnelling from the running IdP instance to the Institution Identity Management component (e.g. LDAP, AD..)
  - **Provide deployment IdP guides and scripts** and support around their usage
  - Point users willing to test/learn to available test instances
  - Spawn an **IdP of Last Resort** for testing and piloting purposes for newcomers

Support the Community with deploying SP

- Enable federated access to services **implies no single "magic" recipe**
  - being normally dependent on the specific service implementation

- Wise options for a newly formed federations are
  - **Gather resources on public wiki on guides / HowTos** on how to federate popular services
    - Wikis
    - Moodle
    - eLearning tools
  - In many cases this implies **using plugins** and configure them to work with SAML AAI

Provide a test infrastructure to your user community

- An open laboratory for community members for the deployment of Identity Providers, Attribute Authorities, Service Providers is a key enabler tool to spread know how and skills on Federated Identity Management

- Asking member institutions to both provide resources and manpower and commit to the actual utilization of an open FIM laboratory is an option to take into account

Implement a test federation

- A fundamental feature to be provided to test SPs and IdPs before integration into the national production federation is the **TEST FEDERATION**
- Keep the Entities sets completely disjoint and separated (production and test federation) for safety reasons
- First grant access for resources to the TEST federation
- Perform all fundamental tests
  - functionality
  - security
  - metadata health
  - monitoring
  - user access
- Migrate resources to the production federation only after successful outcome of all above mentioned tests

Providing a Federation Central Discovery Service

- A Federation Central Discovery Service can be provided to the members of your community to
  - support IdP-SP functional integration in the federation
  - relieve Service Providers from the burden of having to implement their own Discovery of IdPs
  - ensure the DS meets the required standards of usability and security
  - centrally integrate with eduGAIN Identity providers
- SP-specific customizations won't be available on the centrally shared DS
- Embedded Discovery Service is an option to
  - Ensure easy javascript based implementation of DS running at the SP side
  - Fully Customizable (look and feel, IdP filtering…)
  - Sharing therefore same look and feel of the SP environment
  - Makes use of the centrally running Discovery Service instance

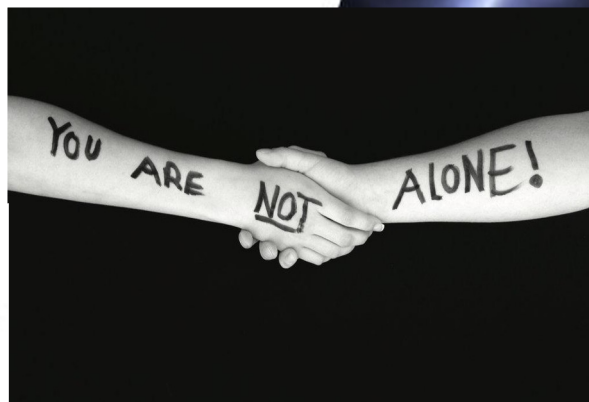
You are not alone

- The NREN and Identity Federations community **is very active in openly involving participation** to governing bodies, reference fora, public discussion lists and portals

- Some specific projects, like the AARC project (2015-2018) have devoted substantial effort in defining reference architecture, writing guidelines on how to support User Communities in adopting Federated AAI - contributing to standards, recommendations, best practices, guidelines https://aarc-project.eu

- Other relevant fora to discuss are the edugain-discuss maling list and the edugain-steering-group list

- The reference body to participate to the ongoing discussions on Federations and related matters is **REFEDS**, https://refeds.org/ the international coordination body to discuss, propose new items for a working group, refer to for initial orientation around Identity federations worldwise



REFEDS: example of activities and tools

- REFEDS keeps an up to date inventory of reference data on all existing Identity Federations: https://refeds.org/federations
- Coordinates and implements an yearly workplan on specific topics
- Manages the Metadata Explorer Tool https://met.refeds.org/
- Coordinates the activities of Working Groups, on
  - FOG - Federation Operators Group (closed, limited to Fed Ops)
  - SIRTFI -Security Incident Response Trust Framework for Federated Identity (open)
  - Entity Category Development (open)
  - Assurance Working Group (open)
  - Federation 2.0
  - SPOG - SP Operator Group (closed)
  - Baseline Expectations Working Group (open)
  - Best Practice around Error Handling (open)

GÉANT
Networks • Services • People

Thank you

Any questions?

www.geant.org

The research leading to these results has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 856726 (GN4-3).