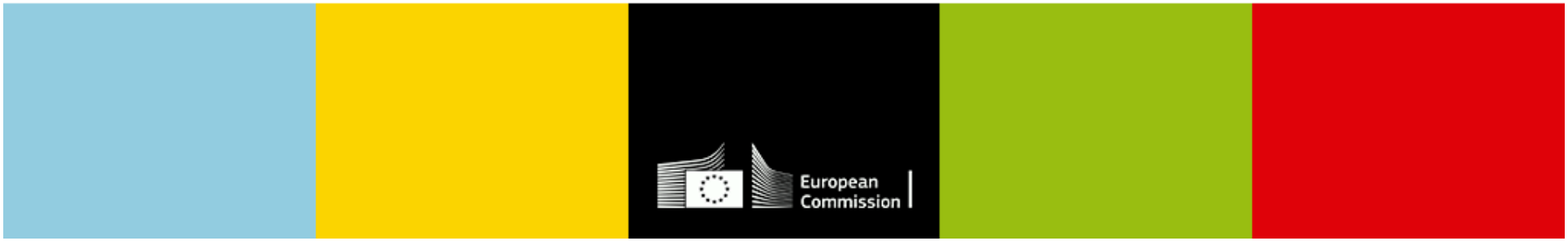
On line Training Material on AAI development

Identity Federation Governance and Best Practices

Ricardo Makino | RNP | 27-02-16 | WP2



Identity Federation Governance and Best Practices

Magic
Middleware for collaborative Applications and Global vIrtual Communities

- Given its complexity, breadth, implications and importance, the phrase “don’t attempt this at home” might well apply to federation identity management deployment.

- Although best practice federation identity management is a desirable goal, it is a status that can realistically be achieved only in stages.

Identity Federation Governance and Best Practices

Magic
Middleware for collaborative Applications and Global vIrtual Communities

- To ensure the Federation Identity Governance and Best Practices you should consider the following areas:
  - Data Protection
  - Discovery
  - Entity Eligibility
  - Operations Management
  - Identity Federation Policy
  - Identity Federation Procedures
  - Identifiers Used in Federations
  - Identity Federation Services Architecture
  - Identity Federation Audit

Data Protection

- Most of the countries have restrict laws related to release of personal data.
  - **European Union:** Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
  - **United States:** Health Insurance Portability and Accountability Act on the protection of individuals health information, Electronic Communications Privacy Act on the protection of individuals eletronic information and others.
  - **Switzerland:** The Swiss Federal Data Protection Act (DPA) applies to the processing of personal data by private persons and federal government agencies.

Data Protection

- An important issue for data protection in identity federations is the process of attribute release, some Service Providers require certain information about the user.

- Some need to know name, e-mail address, or a specific entitlement. Some merely want to know whether the user is faculty, staff, or student, and do not depend upon the particular identity of the user in question, only that institution is willing to vouch for them.

- So, some cares should be taken to avoid disclose of unnecessary information.

Data Protection

- **Only relevant attributes should be released to a SP**
  - When a new SP wants to register to the federation, the SP should provides a list of necessary attributes to the operator.
  - The attributes should be compatible with regional and national laws and regulations regarding privacy.
  - The parts should agree an appropriate balance between risk and value for all parties.

Data Protection

- **IdP asks user's consent for attribute release beforehand**
  - After IdP authenticates the user and before (s)he is redirected back to the SP the user should agree with the release of the attributes from your IdP to the SP.
- **To make the consent *informed*, the Privacy Policy of the SP should be provided to the end user**
  - The federation operator has a centralized repository that gathers links to the Privacy Policies of the SPs in the federation

Discovery

- Discovery services are the primary step to the end user access a federated service, so these should be well designed and implemented to improve the user experience in the federation identity.

- Some simple practices should be adopted to achive this goal, like:
  - Login location in the top right hand corner
  - Presente local login alongside other options
  - Show previously used logins
  - Etc.

- This simple practices will provide a better experience for the end user.

Discovery

- In other hand some practices should be avoided:
  - Login location in the top right hand corner
  - Abuse of technical words to explain functions or actions
  - Use of many drop down menus
  - Use of large drop down lists
  - Etc.

- REFEDS demonstrates the most effective way to present federated identity to users of your site, with best practice and examples of how to provide the best experience at https://discovery.refeds.org.

Discovery – REFEDS Guide for SPs

Discovery - Metadata for User Interfaces

- When reviewing or describing the MDUI requirements it is important to be clear about the importance of the recommendation:
  - A requirement may be mandatory. In this situation non conforming entities will not be inter-federable. Federations imposing such restrictions and federations not populating this field both need to be aware that this is a barrier to inter-federation.
  - A recommendation may be for aesthetic reasons. This is not a barrier to interoperability.
- Note that misuse of the elements specified for MDUI should be discouraged in guidance and disallowed by process.

Entity Eligibility

- The entity eligibility to join the federation as an Identity Provider or as a Service Provider should be well documented.
- This document should describe the eligibility requirements and restrictions that any Identity Provider and Service Provider have to follow.
- This will help to ensure the trust relationship in the Identity Federation.

Operations Management

Operations Management is the process of managing the day-to-day federation infrastructure including managing the provisioning, capacity, performance and availability of the computing, networking and application environment that support the Identity Federation.

Operations Management

- The first step is to define an organizational structure and a team considering the roles and responsibilities needed:
  - Steering Committee - Responsibility for management of the business and affairs of the federation.
  - Committees - The Steering Committee may designate subordinate or advisory committees to make decisions and/or provide advice on particular matters of importance to the federation.
  - Meetings - The Steering Committee meets no less frequently than once per year, advisory and other committees meet as needed.
  - Personnel – Guarantee personnel to provide legal, administrative, communications, operational, and other support to the OM.

Operations Management for SPs

- Determine which services you would like to offer to the federation
  - Determine audience and risk for each offered service and related requirements, to do this answer these questions:
    - How will you decide whether they are eligible or not to use the service?
    - What kind of assurance of the user's identity will you require from the accessing organizations?

Operations Management for SPs

- Develop policy governing the use of attributes received by SPs such as attribute retention, sharing, etc
  - Will you keep the identity attribute information that identity providers send to you and if so, for how long?
- Add service provider information to the federation metadata and configure service provider software to use federation metadata and credentials and refresh when required

Operations Management for SPs

- Ensure your policies are in compliance with the federation requirements
  - Check the Federation repository to ensure that your policies are in compliance with the current federation requirements.
- Identify what attributes you will require from identity providers for access to your service.
  - Determine which services are eligible to receive which attributes

Operations Management for SPs

- Ensure you have a defined problem resolution process for remote users
  - If a user has a problem accessing your service, where will they get help?
- Define problem escalation and support procedure for IdP users of your service
  - If you have a break in service, how will you let your partners know?
  - If you find one or more users abusing your service, how will you contact their home organization?

Operations Management for IdPs

- Ensure basic identity management policies are in place, including data stewardship and acceptable use policies
  - Outside service providers to whom you provide identity information may have questions about your institution's acceptable user and data stewardship policies and how these compare with their requirements.
  - If you plan to provide federated services to your community, these questions are especially important as they will let others from outside your network understand policies that relate to their use of your organization resources.

Operations Management for IdPs

- Define policies on log retention for identity management and provision
  - Regarding to account creation and termination and identity management, service providers may request information related to your logs.
  - Your organization may need to develop policies related to the retention of logs and their use.

Operations Management for IdPs

- Provision/de-provision accounts for your users (faculty, staff, and students) based on published policies
  - Before you provide identity to outside providers, your organization needs to ensure compliance with its published policies.
  - For example, have accounts been terminated which are supposed to have been terminated?
  - Since federated identity is heavily reliant on shared policy statements, it is crucial to ensure that your organization is acting in the expected manner.

Operations Management for IdPs

- Create problem resolution process for when users forget or lose passwords
  - As with the authentication problems, your organization likely has such processes, and these should be checked against any policies set previously.
  - Pay special attention to users who may need password reset performed when they are in a remote location.

Operations Management for IdPs

- Create Help Desk support procedures for authentication problems and password changes
  - Your organization probably already has such procedures, but it is best to check these again against the policies in the above steps.
  - Again, special attention is needed for the remote user scenario.
- Let users know best practices regarding the use and confidentiality of passwords, and the need to replace them periodically.

Operations Management for IdPs

- Consider setting up tiers or groups of attribute release policies for different categories of service providers
  - Identifying groups of service providers (library content providers, for instance) and related attribute release constraints can help streamline the governance process for approval.

Operations Management for Both

- Create a process to address reports of abuse
  - Incident response becomes somewhat more challenging in the federated scenario, because two organizations have to cooperate to collect the necessary forensic information.
  - It is important that these procedures be in place before an incident occurs.
- Ensure the high availability of the Identity Provider or Service Provider
  - High availability, both from the point of view of the Service Provider and the Identity Provider, will give a better experience for the federation end user.

Operations Management for Both

- Establish a secure communications channel between the federation operators
  - Establishment of a secure communication channel between operations team is a requirement to guarantee the source and integrity of the information.
  - All messages must be signed with a personal certificate and sent by official channels, like institutional e-mail or tickets systems.

Operations Management for Both

- Keep the server's clock synchronized with an NTP server
  - The clock synchronization for all components in the federation is important to guarantee that the authentication process will work as expected.
- Maintain backup routines for all settings
  - Backup routines will ensure that the federation will be recovered in a easy way in case of a disaster in any point of the federation.

Identity Federation Policies

- Defining a federation rules: how to adhere to, how to get out, obligations and rights of members and federation, etc.
- A formal document that defines the agreements between members of a federation and the federation itself them
- It should also guarantee that the use of services does not violate the rules defined by the NREN or even by the user's country

Identity Federation Policies

- It is unlikely that you will want to have just one single document to describe your federation to its members.

- Most federations will have some combination of the following:
  - A Federation Policy;
  - Technical Profile(s) for participants;
  - Technical Profile(s) for the operator;
  - Assurance Profiles;
  - A description of how to join;
  - A description of eligibility.

Identity Federation Policies

- It is recommended that you make your federation policy and indeed all of your core federation documents available in English as well as in appropriate local language(s).

- Many Service Providers will only be able to engage with documents in English, and a translation process will slow down membership uptake.

- Additionally, it facilitates to inter-federation process.

Identity Federation Policy Content

- **STUCTURE – General information about how the federation works** :
  - RFC2119*.
  - Definitions.
  - Background and Purpose.
  - Governance.
  - Eligibility.
  - How to Join.
  - How to Withdraw.

* RFC2119 is a specification used by the IETF to explain how key words such as 'MUST', 'REQUIRED' etc. should be interpreted.

Identity Federation Policy Content

- **TERMS OF USE – What everyone is allowed and not allowed to do:**
  - Terms of Use (IdP).
  - Terms of Use (SP).
  - Termination / Dispute Resolution.
  - Logging.
  - Data Protection.
  - Audit.
  - Use of Attributes.
  - Operator Rights / Role.
  - Interfederation / Publish rights.

Identity Federation Policy Content

- **LEGAL – All the legal stuff**
  - Liability.
  - Jurisdiction and Legal.
  - Fee schedule.
  - Copyright.

Identity Federation Policies Templates and Examples

- Templates for policies:
  - REFEDS
    - https://wiki.refeds.org/display/FBP/Identity+Federation+Policy+template

- How to
  - https://wiki.refeds.org/display/FBP/Federation+Policy+Mapping+Exercise

Identity Federation Procedures

- Procedures should be designed to manage the Identity Federation considering the following areas:
  - Membership application – Procedure describing the steps to become a member of the Identity Federation;
  - Membership cancellation – Procedure describing the steps to cancel an Identity Federation membership;
  - Membership revocation – Procedure describing the steps to revoke the membership of a member who fails to comply with the Identity Federation policy.

Identifiers Used in Federations

- The core identifier attributes should be documented by the federations for IdPs and SPs and should be accessible by operations and developers.

- Note, that this does not mean that IdPs and SPs within the federation do not make use of other optional identifiers.

Identity Federation Services Architecture

- Many organizations have embarked on identity management initiatives and projects without understanding the implications for their infrastructure and applications.

- Especially in NRENs, many solutions are developed in house or open source software is adopted to provide some services.

- To a successful Identity Federation deployment the architecture or development of these services should define how the identity infrastructure will integrate with each of the applications running in the NREN.

Identity Federation Services Architecture

- Federated services architecture generally conforms to multiple desired characteristics, including:
  - Service oriented
  - Standards based
  - Flexible and interoperable
  - Loosely coupled
  - Secure
  - Appropriately redundant
  - Scalable
  - Efficient

Identity Federation Audit

- An audit of the identity federation should be established to ensure that members are following the documented processes, policies and procedures, this activity should cover all components, such like:
  - Identity Providers;
  - Service Providers;
  - Discovery Services;
  - Etc.

Quiz Time

Magic
Middleware for collaborative Applications and Global vIrtual Communities

Quiz Time

1. **Which of the following is NOT an best practice?**
   a) Data Protection
   b) Identity Federation Policy
   c) Identity Federation Procedures
   d) MDS

2. **Which of the following statements are true in Federated Identity Best Practices?**
   a) Best practice federation identity management is a desirable goal
   b) Best practice federation identity management is not a desirable goal
   c) All attributes should be released to a SP
   d) Abuse of technical words to explain functions or actions in discovery services are recommended

Quiz Time

3. **In Identity Federation Policy Content which of the following are NOT a requirement?**
   a) Liability
   b) Jurisdiction and Legal
   c) Fee schedule
   d) Management Process

4. **Which of the following is NOT desired in a federated services architecture?**
   a) Service oriented architecture
   b) Component based architecture
   c) Loosely coupled
   d) Scalable

5. **Name one feature of good discovery practice.**

Sources

- Identity Management Planning: Best Practices, Insights and Recommendations - Novell technical white paper.
- REFEDS Federation Best Practice Wiki
- InCommon Federated Identity Management Checklist