ARNaai

Identity Federation Policy

Author : Aouaouche El-Maouhab
Version : 1.0
Created : 14 November 2015
Last modified : 30 November 2015
Based on : GrIDP Identity Federation Rules v. 2.2

https://www.aai.arn.dz

Table of Contents

1. Definitions and Terminology

Definitions and terminology used in this document:

Attribute	A piece of information describing a characteristic of an entity (in this context of the End User), his/her properties or roles in an Organization.
Authentication	Process of proving the identity of a previously registered End User.
Authorization	Process of granting or denying access rights to a service for an authenticated End User.
End User	Any natural person affiliated to an Identity Provider, e.g. as an employee, researcher or student.
Federation	Identity federation. An association of organizations that come together to exchange information as appropriate about their users and resources to enable collaborations and transactions.
Federation Operator	Organization providing Infrastructure for Authentication and Authorization to Federation Members.
Federation Member	An organization that has joined the Federation by agreeing to be bound by the Federation Policy in writing. Within the federation framework, a Federation Member can act as an Identity Provider and/or a Service Provider.
Identity Provider or IdP	A service managed by an entity with which the End User is affiliated. It is responsible for authenticating the End User and managing End Users' digital identity data.
Identity Management	Process of issuing and managing end users' digital identities.
Service Provider or SP or Resource	A service an entity is offering to the End User. Service Providers may rely on the authentication outcome and attributes that Identity Providers assert for its End Users.
Federation Metadata	SAML/XML file which contains information about Federation Members.
Discovery Service	Service used by Services Providers to manage a list of available Identity Providers of the Federation enabled to perform the authentication for the service.

2. Introduction :

The ARNaai Federation is introduced to facilitate and simplify the use of shared services between the ARNaai Participants.

With federation technologies, an End User from ARNaai Participant can use his Digital Identity to access services of Service Providers within the whole federation or based on inter-federation agreements even in other federations (see ARNaai Website).

ARN, the Algerian National Research and Education Network, as the Federation Operator coordinates and manages the necessary activities, which in the end enable the direct interoperation between End Users, the ARNaai Participants they belong to and ARNaai Federation Partners offering services. For ARN, the participation in the ARNaai Federation is a service among others services provided to ARN community.

Within the federation framework, a Federation Member can act as an Identity Provider and/or a Service Provider. Other organisations can become ARNaai Federation Partner and participate in the ARNaai Federation by signing the ARNaai Federation Member Request.

When requiring to join the Federation, Organizations accept the present Policy document.

3. Objectives

The Federation aims at carrying out the following activities:

- enable ARN end-users (i.e., researchers, professors, students etc.) to access online resources through simplified procedures, such as to facilitate the sharing of resources between Participant organizations;
- ensure that the end user's personal information is kept secure and confidential;
- eliminate or minimize the need for multiple credentials for a single end user to access online resources by different providers;
- reduce user management procedures on the Resource Providers' side;
- facilitate collaboration through a trust cycle;
- favor aggregation in accordance with a network-like model;
- promote its activities, knowledge and objectives through dissemination and communication actions, including its participation in national and international projects.

4 - Roles :

4.1 - Federation Operator :

ARNaai Federation is managed and operated by ARN, the Algerian National Research and Education Network.

4.2 - ARNaai Member :

All organisations participating in ARNaai can join as Members by signing the ARNaai Federation Member Request. They either belong to the ARN Community for Participants or they are Partners for others.

ARNaai Participant :

> ARNaai Participant is an organisation that belongs to the ARN Community and participates in the ARNaai Federation. ARNaai Participant that is entitled and wants to identify End Users MUST be an IdP Operator. ARNaai Participant that wants to offer a service MUST be an SP Operator.

ARNaai Federation Partner :

> ARNaai Federation Partner is an organisation that does not belong to the ARN Community but wants to contribute to the ARNaai Federation.

4.3 - IdP Operator

An IdP Operator identifies End Users and issues them Digital Identities. The IdP Operator MUST define an identification process for End Users.

To become an IdP Operator, a ARNaai Participant has either to belong to the ARN Community or needs to be entitled by ARN.

An IdP Operator MUST run an IdP. The IdP authenticates End Users based on a Digital Identity, issues them Assertions with which they can apply for access to services offered by SP Operators.

4.4 - SP Operator

A SP Operator relies on Assertions - issued by IdPs for authenticating users - and authorizes their access to the services operated. Any ARNaai Participant MAY be an SP Operator. An SP Operator MUST run an SP. The SP evaluates the Assertions it receives and interacts with the services it protects.

4.5 - End User

An End User identifies himself at the IdP Operator and receives a Digital Identity from the IdP Operator. The End User accesses services offered by SP Operators based on Federated Authentication.

An End User is typically a human person who belongs to an organisation, typically an employee or student, who uses Federated Authentication via its IdP Operator. However, an End User can also be a legal person, a virtual artefact (e.g. a computer process, an application).

5 – Governance

ARNaai Federation is managed by ARN, the Algerian National Research and Education Network. ARN is responsible for:

- Setting criteria for membership of the Federation;
- Evaluating and determining whether to grant or deny an application for membership in the Federation;
- Revoking the membership if a Federation Member is in a breach of the Federation Rules;
- Evaluating and determining future directions and enhancements for the Federation;
- Evaluating and determining the entering into inter-federation agreements according to the interest of Federation Members;
- Maintaining formal ties with relevant national and international organizations;
- Approving changes to the Federation.
- Deciding on any other matter referred to the Federation.

6 - Obligations and Rights of Federation Members :

All ARNaai Federation Members:

- Must appoint a technical and/or an administrative contact for interactions with ARN;
- Must cooperate with ARN and other Members in resolving incidents and should report incidents to ARN in cases where these incidents could negatively affect the security, trustworthiness or reputation of the Federation or any of its Members;
- Must comply with the obligations defined in the Technology Profiles, when specified;
- Must agree in facilitate the use of their names in the communicational channels disposed by ARN, for the purpose of promoting the Federation;
- In the same way, the member must commit to mention ARN as the Federation operator in their communicational media as appropriate.

6.1 - Obligations and Rights of Federation Operator

In addition to what is stated elsewhere in the Federation Policy, ARN is responsible for:

- Secure and trustworthy operational management of the Federation Metadata and Discovery Services.
- Publish the information about the Attributes needed by Services Providers

6.2 - Obligations and Rights of Identity Provider :

If a Federation Member is acting as an Identity Provider, it:

- Is responsible for managing authentication credentials for its End Users and for authenticating them;

- Should submit its Identity Management Practice Statement to ARN, who in turn make it available to other Federation Members upon their request. The Identity Management Practice Statement is a description of the Identity Management life-cycle including a description of how individual digital identities are enrolled, maintained and removed from the identity management system. The statement must contain descriptions of administrative processes, practices and significant technologies used in the identity management life-cycle, which must be able to support a secure and consistent identity management life-cycle;

• Operates a helpdesk for its End Users regarding Federation services related issues. Identity Providers are encouraged to maintain a helpdesk for user queries at least during normal officehours in the local time zone. Identity Provider Organizations must not redirect End User queries directly to ARN, but must make every effort to ensure that only relevant problems and queries are sent to ARN by appropriate Identity Provider contacts;

• Is responsible for assigning Attribute values to the End Users and managing the values in a way which ensures they are up-to-date;

• Is responsible to releasing the Attributes to Service Providers;

• Is responsible for keeping its metadata up-to-date;

• Must send a list of Services Providers which it is related to if there is an intention of cancelling its membership.

6.3 - Obligations and Rights of Service Provider :

If a Federation Member is acting as a Service Provider, it:

• Is responsible for making decision on which End Users can access the services they operate and which access rights are granted to an End User. It is Service Providers responsibility to implement those decisions;

• In addition to access grant, the Service provider can use the information retrieved from Identity Providers only for the following purposes:
  - o Customization (Interface);
  - o Audit;
  - o Usage reports;
  - o For any other purpose specifically agreed between the Identity Provider and the Service Provider.

• Is responsible for noticing ARN which Attributes are needed for access grant and the other purposes described before;

• Can make use of the ARNaai's Discovery Service;

• Is responsible for keeping its metadata up-to-date;

- Must send a list of Identity Providers which it is related to if there is an intention of cancelling its membership.

6.4 - Obligations and Rights of End User :

End Users MUST comply with the applicable rules of this Service Description and the rules by their ARNaai Member. They are in particular responsible and liable for the misuse of their Digital Identity towards the IdP Operator, the SP Operator and ARN. The End User is responsible and liable for any misuse of his username and password or other protection of his Digital Identity.

The End User has no liability claims or other claims against ARN if, owing to negligent keeping or management of the access to his Digital Identity or because of its disclosure to third parties, unauthorised actions are made and processed by ARN or a ARNaai Member.

7 - Eligibility :

All organisations participating in ARNaai can join as Members. They either belong to the ARN Community for Participants or they became Partners. In both cases they can join as members by signing the ARNaai Federation Member Request.

Identity Providers and/or Service Providers can apply for membership at any time by submitting a specific application form available on the ARNaai website. Their applications will be evaluated (either accepted or denied) within 15 days against the following criteria:

- completeness, consistency of the documentation;
- installed certificates;
- the accuracy of the Service registration in the Federation;
- the proper working of the Service;
- the consistency with the information provided through the request forms.

Upon acceptance, the Organisation receives exclusively to the provided email addresses the countersigned documents. If rejected, the Organisation is notified with the reason of the refusal.

8 – Procedures :

8.1 - How to join

In order to become a Federation Member, an organization applies for membership in the Federation by agreeing to be bound by the Federation Policy in written by an official representative of the organization. Each application for membership has to be sent to ARN who in turn decides on whether to grant or deny the application. If the application is denied, the decision and the reason for denying the application are communicated to the applying organization by ARN.

8.2- How to Withdraw :

A Federation Member may cancel its membership in the Federation at any time by sending a request to ARN. A cancellation of membership in the Federation implies the cancellation of the use of all federations Technology Profiles for the organization in reasonable time interval.

9 - Legal conditions of use :

9.1 – Termination

A Federation Member who fails to comply with the Federation Policy may have its membership revoked. If ARN is aware of a breach of the Federation Policy by a Federation Member, they may issue a formal notification of concern within 5 working days. If the cause for the notification of concern is not rectified within 60 days by the Federation Member, ARN can make a decision to revoke the membership. Revocation of a membership implies as soon as possible the revocation of the use of all Technology Profiles for the Federation Member.

9.2 – Inter-federation

In order to facilitate collaboration across national and organizational borders the Federation may participate in inter-federation agreements. The Members understand and acknowledge that via those inter-federation arrangements they may interact with organizations which are bound by and committed to foreign laws and federation policies. Those laws and policies may be different from the laws and policies in this Federation.

10 – Amendment :

ARN has the right to amend the Federation Policy from time to time. Any such changes need to be reviewed and shall be communicated to all Federation Members via email at least 30 days before they enter into force.