



OMREN Federation

Identity Federation Policy

Authors	Abdulmonem Alkharusi
Last Modified	2/9/2018
Version	1.2

Table of Contents

1	Definitions and Terminology
2	Introduction Technical implementation
3	Governance and Roles 3.1 Governance 3.2 Obligations and Rights of Federation Operator 3.3 Obligations and Rights of Federation Members
4	Eligibility
5	Procedures 5.1 How to Join 5.2 How to Withdraw
6	Legal conditions of use 6.1 Termination 6.2 Liability and indemnification 6.3 Jurisdiction and dispute resolution 6.4 Interfederation 6.5 Amendment

1 Definitions and Terminology

Attribute	A piece of information describing the End User, his/her properties or roles in an Organization.
Attribute Authority	An organization responsible for managing additional Attributes for an End User of a Home 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.
Digital Identity	A set of information that is attributable to an End User. It is issued and managed by a Home Organization and zero or more Attribute Authorities on the basis of the identification of the End User.
End User	Any natural person affiliated to a Home Organization, e.g. as an employee, researcher or student making use of the service of a Service Provider.
Technology Profile	A system consisted of hardware and software working to provide federation service like IDP or SP or AA or Registration or publish or all
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 a Home Organization and/or a Service Provider and/or an Attribute Authority.
Home Organization	The organization with which an 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.
Interfederation	Voluntary collaboration of two or more Identity Federations to enable End Users in one Identity Federation to access Service Providers in another Identity Federation.
Service Provider	An organization that is responsible for offering the End User the service he or she desires to use. Service Providers may rely on the authentication outcome and attributes that Home Organizations and Attribute Authorities assert for its End Users.
OMREN Federation	OMAN Research and Education Network Federation

2 Introduction

An Identity Federation (Federation) is an association of organizations that come together to exchange information, as appropriate, about their users and resources in order to enable collaborations and transactions.

The OMREN Federation is introduced to facilitate and simplify the introduction of shared services across the Federation. This is accomplished by using Federation Technologies to extend the scope of a digital identity issued by one Federation Member to be valid across the whole Federation. The Federation relies on Home Organizations and Attribute Authorities to correctly and accurately assert information about the identity of End Users to Service Providers, that may use that information to grant (or deny) access to the services and resources they offer to End Users.

The Federation Policy document defines the Federation by defining the Federation Members' obligations and rights to be able to use available Federation Technologies for electronic identification and for access to attribute and authorization information about End Users in the Federation.

Aggregate Signing Key:

OMREN federation metadata signing key is published on <https://fed.omren.om> in the form of an X.509 certificate referred to as OMREN federation metadata signing certificate. Its size is RSA(2048 bit) and its SHA256 signature is:
 27:1E:E1:CA:19:35:E2:EF:3E:E4:A4:84:A6:C2:39:C8:B6:CD:9D:3C:D7:AA:5B:8F:1A:C0:EC:72:F6:80:10:30

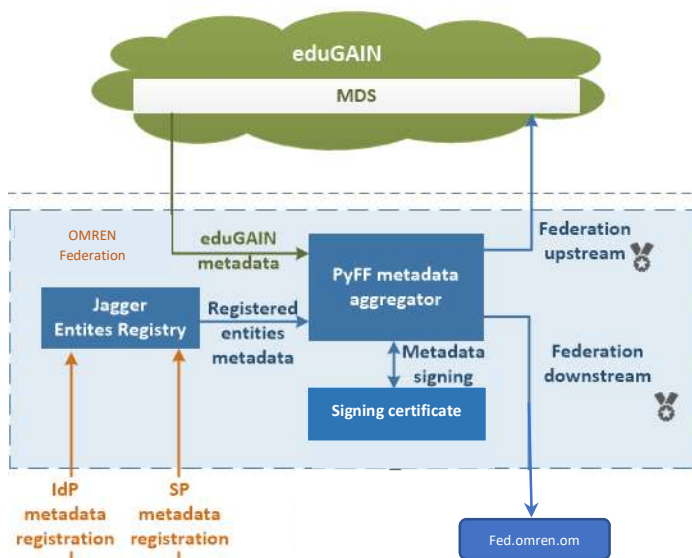
Metadata consumers MUST verify an aggregate's signature against this key and MUST reject an aggregate whose signature cannot be verified. This acts as a protection against attacks in which consumers are provided with fabricated metadata.

This document, together with its appendices constitutes the Federation Policy.

DNS scope:

OMREN federation DNS scope is “.OM” domains all identity providers and attribute authorities need to need to use “.OM” domain. All service providers need to check for “.OM” users. In registration page, <https://fed.omren.om/rr3> the scope of every IDP is needed without “www” for example “unizwa.edu.om”

Technical implementation:



3 Governance and Roles

3.1 Governance

The governance of the Federation is delegated to The Research & Education Network (OMREN).

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

- Setting criteria for membership for the Federation.
- Evaluating and determining whether to grant or deny an application for membership in the Federation.
- Determining whether a Federation Member is entitled to act as Home Organization.
- Revoking the membership if a Federation Member is in a breach of the Policy.
- Plan future directions and enhancements for the Federation together with the Federation Operator who prepares the plans.
- Maintaining formal ties with relevant national and international organizations.
- Evaluate and determine whether to enter into an interfederation agreement.
- Approving changes to the Federation Policy prepared by the Federation Operator.
- Address financing of the Federation. Approves the fees to be paid by the Federation Members to cover the operational costs of the Federation, on proposal of Federation Operator.
- Deciding on any other matter referred to it by the Federation Operator.

3.2 Obligations and Rights of Federation Operator

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

- Secure and trustworthy operational management of the Federation and providing central services following the procedures and technical descriptions specified in this document and its appendices.
- Provides support services for Federation Members' appropriate contact persons to work out operational problems regarding the Federation services.
- Acts as centre of competence for Identity Federation: tests software, recommends and documents solutions, provides software deployment and configuration guides for selected software and operating systems for use within the Federation.
- Maintaining relationships with national and international stakeholders in the area of Identity Federations. This especially includes contacts regarding interfederation activities and work with other Identity Federations in the area of harmonization.
- Promoting the idea and concepts implemented in the Federation so prospective Federation Members learn about the possibilities of the Federation.

In addition to what is stated elsewhere in the Federation Policy, the Federation Operator reserves the right to:

- Temporarily suspend individual Technology Profiles for a Federation Member that is disrupting secure and trustworthy operation of the Federation.
- Publish a list of Federation Members along with information about which profiles each Federation Member fulfils or implements, for the purpose of promoting the Federation.
- Publish some of the data regarding the Federation Member using specific Technology Profile. Definition of which data may be published is provided in appropriate Technology Profiles.

3.3 Obligations and Rights of Federation Members

In addition to what is stated elsewhere in the Federation Policy all Federation Members:

- Shall appoint and name an administrative contact for interactions with the Federation Operator.
- Must cooperate with the Federation Operator and other Members in resolving incidents and should report incidents to the Federation Operator 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 of the Technology Profiles which it implements.
- Must ensure its IT systems that are used in implemented Technology Profiles are operated securely.
- If a Federation Member processes personal data, Federation Member will be subject to applicable cyber law applied in the Sultanate of Oman such as Royal Law Decree No. 69/2008 and Royal Law Decree No.12/2011 or its proceedings.

If a Federation Member is acting as a Home Organization, it:

- Is responsible for delivering and managing authentication credentials for its End Users and for authenticating them, as may be further specified in Level of Assurance Profiles.
- Should submit its Identity Management Practice Statement to the Federation Operator, who in turn makes 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. Specific requirements may be imposed by Level of Assurance Profiles.
- Ensures an End User is committed to the Home Organization's Acceptable Usage Policy.
- Operates a helpdesk for its End Users regarding Federation services related issues. Home Organizations are encouraged to maintain a helpdesk for user queries at least during normal office hours in the local time zone. Home Organizations must not redirect End User queries directly to the Federation Operator but must make every effort to ensure that only relevant problems and queries are sent to the Federation Operator by appropriate Home Organization contacts.

If a Federation Member is acting as a Home Organization or Attribute Authority, it:

- 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.

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.

4 Eligibility

The Federation sets out eligibility criteria that determines who is able to become a Federation Member and who is able to act as Home Organization. The criteria is fully described OMREN Website. Responsibility for setting membership criteria rests with OMREN and may be revised from time to time.

5 Procedures

5.1 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 writing by an official representative of the organization.

OMREN Federation evaluates each application for membership, including the optional Identity Management Practice Statement and it decides on whether to grant or deny the application.

If the application is denied, the Federation administrator communicates this decision and the reason for denying the application to the applying organization.

5.2 How to Withdraw

A Federation Member may cancel its membership in the Federation at any time by sending a request to the Federation Operator. The period between announcement and termination should be not less than 90 days. 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.

The Federation Operator may cancel its participation in the Federation by announcing the termination date to the Federation Members. The period between announcement and termination should be not less than 90 days. Until termination date, Federation Operator shall run the Federation on best effort basis. After the termination date, Federation Operator shall cancel the use of all Federations Technology Profiles for all Federation Members.

6 Legal conditions of use

6.1 Termination

A Federation Member who fails to comply with the Federation Policy may have its membership in the Federation revoked.

If the Federation Operator is aware of a breach of the Federation Policy by a Federation Member, the Federation Operator may issue a formal notification of concern. If the cause for the notification of concern is not rectified within the time specified by the Federation Operator, OMREN may issue a formal notification of impending revocation after which OMREN 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.

6.2 Liability and indemnification

The Federation Operator offers this service on an “as is” basis, that is, without liability for Federation Operator and OMREN for any faults and defects meaning amongst other that the Federation Member cannot demand that Federation Operator amend defects, refund payments or pay damages. Federation Operator will nevertheless strive to ensure that any faults and defects of significance are corrected within a reasonable period.

The Federation Operator and OMREN may not be held liable for any loss, damage or cost that arises as a result of the Federation Member connection to or use of Federation services, or other systems to which the Federation Member obtains access in accordance with the agreement. This limitation of liability does not however apply in the case of gross negligence or intent shown by Federation Operator personnel.

Neither the Federation Operator nor OMREN shall be liable for damage caused to the Federation Member or its End Users. The Federation Member shall not be liable for damage caused to the Federation Operator or the OMREN due to the use of the Federation services, service downtime or other issues relating to the use of the Federation services. For any other damage, the liability for damages in case of a breach is limited to the amount of money the Federation received that year from the member.

Unless agreed otherwise in writing between Federation Members, the Federation Member will have no liability to any other Federation Member solely by virtue of the Federation Member’s membership of the Federation. In particular, membership of the Federation alone does not create any enforceable rights or obligations directly between Federation Members. Federation Operator and the Federation Member shall refrain from claiming damages from other Federation Members

for damages caused by the use of the Federation services, service downtime or other issues relating to the use of Federation services. The Federation Member may, in its absolute discretion, agree variations with any other Federation Member to the exclusions of liability. Such variations will only apply between those Federation Members.

The Federation Member is required to ensure compliance with applicable laws. Neither the Federation Operator nor OMREN shall be liable for damages caused by failure to comply with any such laws on behalf of the Federation Member or its End Users relating to the use of the Federation services.

Neither party shall be liable for any consequential or indirect damage.

Neither the existence of interfederation agreements, nor the exchange of information enabled by it, shall create any new legal obligations or rights between Members or operators of any federation. Federation Operator and Federation Members remain bound only by their own respective laws and jurisdictions.

The Federation Member and Federation Operator shall refrain from claiming damages from entities in other federations involved in an interfederation agreement.

6.3 Jurisdiction and dispute resolution

Disputes concerning the Federation Policy shall be settled primarily through negotiation. If the issue cannot be resolved through negotiation, any disputes shall be submitted to an authorized court in Oman that will decide according to Omani law. If such negotiations do not succeed within four weeks of the date on which the claim for negotiations was made in writing by one party, each of the parties may bring the dispute before an authorized court in Oman that will decide according to Omani law. If any provision of the Federation Policy is held to be unenforceable by any court of competent jurisdiction, all other provisions will nevertheless continue in full force and effect.

6.4 Interfederation

In order to facilitate collaboration across national and organizational borders the Federation may participate in interfederation agreements. How the potential interfederation agreement is administratively and technologically reflected for certain technology is described in appropriate Technology Profiles.

The Member understands and acknowledges that via those interfederation arrangements the Member 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.

6.5 Amendment

The Federation Operator has the right to amend the Federation Policy from time to time. Any such changes need to be approved by the OMREN Board and shall be communicated to all Federation Members in written form at least 90 days before they are to take effect.