

# Maeen Federation

## Technology Profile

<b>Authors</b>	Mohamad M. Al-Ghamdi, Naser Almesad
<b>Last Modified</b>	2019-03-18
<b>Version</b>	1.0

### License



This work is licensed under a [Creative Commons Attribution-ShareAlike 3.0 Unported License](https://creativecommons.org/licenses/by-sa/3.0/).

# Table of Contents

1. Terminology.....	3
2. Introduction.....	3
3. Requirements.....	3
4. Amendment.....	4
5. References.....	4

# 1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119, see <http://www.ietf.org/rfc/rfc2119.txt> .

## 2. Introduction

This document is a Maeen Federation Policy Technology Profile which describes how the Maeen Federation is made operational using the SAML V2.0 Web Browser SSO Profile [1].

The SAML V2.0 Web Browser SSO Profile defines a standard that enables Identity Providers and Service Providers to create and use web Single Sign on services using SAML.

## 3. Requirements

- All SAML metadata **MUST** fulfill the SAML V2.0 Metadata Interoperability Profile Version 1.0 or any later version [2].
- All identity providers **MUST** fulfill the Interoperable SAML 2.0 Profile (stable version) [3] and **MAY** optionally support the Shibboleth SAML 1.1 Profile [4] for interoperability with legacy systems.
- All service providers **SHOULD** fulfill the Interoperable SAML 2.0 Profile [3] or **MAY OPTIONAL** support the Shibboleth SAML 1.1 Profile [4]. Changing any such systems to conform with the Interoperable SAML 2.0 Profile as soon as possible is strongly **RECOMMENDED**.
- All SAML attributes **SHOULD** be represented using the `urn:oasis:names:tc:SAML:2.0:attrname-format:uri` Name Format
- All SAML attribute names **SHOULD** be represented using either the `urn:oid` or `http(s) URI` scheme namespaces. Usage of MACE-Dir [5] defined attributes **MUST** conform to the MACE-Dir SAML Attribute Profiles [6] (or any later version).
- All SAML Identity Providers **MUST** implement the Shibboleth Scope Metadata extension as defined in the Shibboleth Metadata Schema [7]. The Scope value **MUST** be a string equal to a DNS domain owned by the organization that is responsible for the Identity Provider.
- All SAML Service Providers **SHOULD** implement checks against the Shibboleth Scope Metadata extension when processing scoped attributes.

- All Service Providers and Identity Providers must not rely on any metadata without any limitation on validity. The metadata MUST not be refreshed less than daily.
- All Identity Providers MUST request user consent before delivering attributes.

## 4. Amendment

The Federation Operator Team has the right to amend this document from time to time

## 5. References

- [1] <http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>
- [2] <http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf>
- [3] <http://saml2int.org/>
- [4] <https://wiki.shibboleth.net/confluence/download/attachments/2162702/internet2-mace-shibboleth-arch-protocols-200509.pdf>
- [5] <http://middleware.internet2.edu/dir/>
- [6] <http://middleware.internet2.edu/dir/docs/internet2-mace-dir-saml-attributes-200804.pdf>
- [7] [https://svn.middleware.georgetown.edu/cpp-sp/branches/Rel\\_1\\_3/schemas/shibboleth-metadata-a-1.0.xsd](https://svn.middleware.georgetown.edu/cpp-sp/branches/Rel_1_3/schemas/shibboleth-metadata-a-1.0.xsd)