Pakistan Identity Federation

SAML Web Single Sign-On Technology Profile

Authors	Waqas Ahmed Khan
Last Modified	14-08-2018
Version	0.1

Acknowledgements

This document draws heavily from work carried out by SWAMID in the development of the [SWAMID SAML WebSSO Technology Profile].

License

Table of Contents

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 RFC 2119 [RFC2119].

2. Introduction

This document is a PKIFED Federation Policy Technology Profile which describes how the PKIFED Federation is realised using the [SAML V2.0 Web Browser SSO Profile].

The SAML V2.0 Web Browser SSO Profile defines a standard that enables Identity Providers and Relying Parties 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].
- All entities (service providers and identity providers) SHOULD fulfill either the [Interoperable SAML 2.0 Profile] or the [Shibboleth SAML 1.1 Profile].
- All SAML attributes SHOULD be represented using the urn:oasis:names:tc:SAML: 2.0:attrname-for mat:uri NameFormat
- All SAML attribute Names SHOULD be represented using either the urn:oid or urn: mace:dir:attribute-def namespace.
- All SAML Identity Providers SHOULD implement the Shibboleth Scope Extension. If the Shibboleth Scope Extension is implemented by an Identity Provider then it MUST be declared in the metadata as defined in the [Shibboleth Metadata Schema]. The Scope value MUST be a string equal to a domain owned by the organisation that owns the Identity Provider.
- All SAML Service Providers SHOULD implement checks against the Shibboleth Scope Extension when processing scoped attributes.

4. References

[SWAMID SAML WebSSO Technology Profile]	https://www.sunet.se/wp-content/uploads/2015/12/SWAMIDSAMLWebSSOTechnologyProfile-1.0.pdf
[Creative Commons CC BY-SA 3.0]	https://creativecommons.org/licenses/by-sa/3.0/deed.en
[RFC2119]	http://www.ietf.org/rfc/rfc2119.txt
[SAML V2.0 Web Browser SSO Profile]	http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
[SAML V2.0 Metadata Interoperability Profile Version 1.0]	http://docs.oasis-open.org/security/saml/Post2.0/sstc-metadata-iop.pdf
[Shibboleth SAML 1.1 Profile]	http://shibboleth.internet2.edu/docs/internet2-mace-shibboleth-arch-protocols-200509.pdf
[Shibboleth Metadata Schema]	https://svn.middleware.georgetown.edu/cpp-sp/branches/Rel_1_3/schemas/shibboleth-metadata-1.0.xsd
[PKIFED Federation Policy]	http://pkifed.pk/wp-content/uploads/2018/09/PKIFED-Identity-Federation-Policy-v0.1.pdf
[PKIFED Metadata Registration Practice Statement]	http://pkifed.pk/wp-content/uploads/2018/09/PKIFED-MRPS-v0.1.pdf