Hong Kong Access Federation (HKAF)

SAML WebSSO Technology Profile

Version 1.0

1. Document Control

1.1 Document Status

Document Name	HKAF SAML WebSSO Technology Profile
Document Code	HKAF-P-SAMLSSOTP
Author	AFWG
Version Number	1.0
Document Status	~~Draft for Internal Review~~ / ~~Release for Consultation~~ / Approved
Date Approved	15-Jun-2017
Date of Next Review	01-Jul-2019
Superseded Version	N/A

1.2 Document History

Version Number	Revision Date	Summary of Changes	Authored By	Approved By
1.0	15-Jun-2017	Official release	AFWG	JUCC Steering Committee

2. Definitions and Terminology

Section 2 - ‘Definitions and Terminology’ of the latest HKAF Federation Policy published on the HKAF website at https://www.hkaf.edu.hk/federation-policy applies to this document.

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, see http://tools.ietf.org/html/rfc2119.

3. Introduction

This document is a HKAF Federation Technology Profile which describes how the Hong Kong Access Federation is realized 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 Relying Parties (Service Providers) to create and use Web Single Sign on services using SAML.

4. 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].
- All Service Providers SHOULD fulfill the Interoperable SAML 2.0 Profile [3].
- 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 [4] defined attributes MUST conform to the MACE-Dir SAML Attribute Profiles [5] (or any later version).
- All SAML Identity Providers MUST implement the Shibboleth Scope Metadata extension as defined in the Shibboleth Metadata Schema [6]. The Scope value MUST be a string equal to a DNS domain owned by the organization that is responsible for the Identity.
- All SAML Service Providers SHOULD implement checks against the Shibboleth Scope Metadata extension when processing scoped attributes.

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] http://middleware.internet2.edu/dir/

[5] http://macedir.org/docs/internet2-mace-dir-saml-attributes-200804a.pdf

[6] https://wiki.shibboleth.net/confluence/display/SC/ShibMetaExt+V1.0

6. Amendment

The HKAF Federation Operator has the right to amend the HKAF SAML WebSSO Technology Profile from time to time. Any such amendments need to be approved by the HKAF Steering Committee and will become binding upon the HKAF Federation Members at the time provided in the amendment.

The HKAF Federation Operator will make the latest version of the HKAF SAML WebSSO Technology Profile available on the HKAF website at https://www.hkaf.edu.hk/saml-technology-profile. The HKAF Federation Operator will also communicate changes to the HKAF SAML WebSSO Technology Profile to all HKAF Federation Members with reasonable advance notice.