JOINT UNIVERSITIES COMPUTER CENTRE LTD.
大學聯合電腦中心

HONG KONG ACCESS FEDERATION

Hong Kong Access Federation (HKAF)

Attribute Profile

Version 1.2

1. Document Control

1.1 Document Status

Document Name	HKAF Attribute Profile
Document Code	HKAF-P-AP
Author	HKAF Operator Team
Version Number	1.2
Document Status	~~Draft for Internal Review~~ / ~~Release for Consultation~~ / Approved
Date Approved	06-Jul-2018
Date of Next Review	01-Jul-2019
Superseded Version	1.1

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
1.1	20-Oct-2017	• Addition of [SAML Core] as a source of attributes in p.5 • Addition of “SAML2 Persistent NameID (eduPersonTargetedID)” as a Core Attribute in p.6 & 7	HKAF Operator Team	JUCC Steering Committee
1.2	06-Jul-2018	• Addition of “eduPersonEntitlement” as a Recommended Attribute in p.7	HKAF Operator Team	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 Attribute Profile is the required profile for End Users' attributes exchanged throughout the HKAF service. It covers the scenario under the SAML WebSSO Technology Profile. The profile may be amended later by adding scenarios with different requirements.

This profile summarizes the details about the attributes of End Users, their handling and exchange in the Federation.

4. Attribute Standard

HKAF supports attributes defined in various sources. These include:

a. [eduPerson]
   - eduPerson object class specification (201602)
   - http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html

b. [person]
   - LDAP Schema for User Applications (RFC4519)
   - https://tools.ietf.org/html/rfc4519

c. [inetOrgPerson]
   - inetOrgPerson LDAP Object Class Definition (RFC2798)
   - https://www.ietf.org/rfc/rfc2798

d. [SCHAC]
   - SCHema for ACademia (v:1.5.0)
   - https://wiki.refeds.org/download/attachments/1606048/SCHAC%2B1.5.0.pdf?version=3&modificationDate=1429195142624&api=v2

e. [SAML Core]
   - Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0. OASIS Standard, 15 March 2005
   - https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

The syntax for expressing all HKAF attributes SHALL follow the MACE-Dir SAML Attribute Profiles [MACEDir] (http://macedir.org/docs/internet2-mace-dir-saml-attributes-200804a.pdf).

5. Attributes for SAML Web Single Sign-On

The HKAF Federation Policy requires that, when acting as a Service Provider Organization, Federation Member MUST ensure that the deployment of each of its Service Providers follows all the attribute processing principles defined in the HKAF Data Protection Profile for providing access to the protected resources or services.

The technical representation of an attribute during the transfer in the Federation is presented in the HKAF SAML WebSSO Technology Profile.

5.1 Core Attributes

A Core Attribute means that it is available, in general, for most End Users. However, it can be left empty for those End Users who do not qualify for any of the values in the vocabulary.

The HKAF Federation Policy requires that Federation Member MUST collect or generate the Core Attributes regarding their qualified End Users for their Identity Providers.

The set of Core Attributes supported in the Federation are summarized in the table below.

Attribute	Defining Schema	Meaning	Example Value
eduPersonAffiliation	[eduPerson]	Specifies the person's relationship(s) to the institution in broad categories such as student, faculty, staff, alum, etc. (See Controlled Vocabularies)	Staff
eduPersonScopedAffiliation	[eduPerson]	Specifies the person's affiliation within a particular security domain in broad categories such as student, faculty, staff, alum, etc.	staff@polyu.edu.hk
eduPersonAssurance	[eduPerson]	Set of URIs that assert compliance with specific standards for identity assurance for the person	urn:mace:aaf.edu.au:iap:id:1 urn:mace:aaf.edu.au:iap:authn:1
eduPersonPrincipalName	[eduPerson]	The "NetID" of the person for the purposes of inter-institutional authentication.	pchan@polyu.edu.hk
SAML2 Persistent NameID (eduPersonTargetedID)	[SAMLCore, eduPerson]	A persistent, non-reassigned, privacy-preserving identifier for a principal shared between a pair of coordinating entities.	7eak0QQIEhygtPXtpgmu5l5hRnY
cn (commonName)	[person]	An individual's common name, typically their full name. This attribute should not be used in transactions where it is desirable to maintain user anonymity.	Peter Chi Fung Chan
displayName	[inetOrgPerson]	Preferred name of a person to be used when displaying entries. This attribute should not be used in transactions where it is desirable to maintain user anonymity.	CHAN, Peter
mail	[inetOrgPerson]	Preferred address for the "to:" field of e-mail to be sent to this person.	peter.chan@polyu.edu.hk

Table 1: HKAF Core Attributes

The set of Core Attributes may evolve over time in response to the needs of the Federation Members.

5.2 Recommended Attributes

It is RECOMMENDED that Federation Members support in their Identity Providers the Recommended Attributes summarized in the following table. They can assist in interacting with some federation services.

Attribute name	Defining Schema	Meaning	Example
givenName	[eduPerson]	Contains name strings that are the part of a person's name that is not their surname	Peter
schacHomeOrganization	[SCHAC]	Specifies a person´s home organization using the domain name of the organization	polyu.edu.hk
sn (surname)	[eduPerson]	Surname or family name	CHAN
eduPersonEntitlement	[eduPerson]	URI (either URN or URL) that indicates a set of rights to specific resources	http://xstor.com/contracts/HEd123

Table 2: HKAF Recommended Attributes

The list of Recommended Attributes may evolve over time in response to the needs of the Federation Members.

5.3 Controlled Vocabularies

5.3.1 eduPersonAffiliation and eduPersonScopedAffiliation

eduPersonAffiliation and derivatives have a controlled vocabulary, as defined in [eduPerson]. HKAF Federation Members SHOULD limit their Identity Providers to use the following attribute values:

- member
- staff
- student
- alum
- affiliate
- library-walk-in
- employee

5.4 Unique Identifiers

5.4.1 SAML2 Persistent NameID (eduPersonTargetedID)

HKAF Federation Members MUST use SAML2 Persistent Identifier as the unique opaque identifier in their Identity Providers for their End Users. To ensure proper functioning of (possible) consent modules for attribute release, SAML2 Persistent Identifier MUST be placed both in the subject /nameID element and the attribute statement of a SAML assertion. The attribute name used in the attribute statement MUST be eduPersonTargetedID as defined in Section 3.3.1.1 under Section 3 “MACE-Dir Attribute Profile for SAML 2.0” of the “MACE-Dir SAML Attribute Profiles” [MACEDir], which is available at http://macedir.org/docs/internet2-mace-dir-saml-attributes-200804a.pdf.

5.4.2 eduPersonPrincipalName (ePPN)

ePPN MAY be used as a unique identifier, but Federation Members who decide to use it must recognize that ePPN may not be privacy preserving.

5.5 Scoped Attributes

If a Federation Member makes use of a scoped attribute (such as eduPersonScopedAffiliation or eduPersonPrincipalName) in its Service Provider, it is encouraged to use available mechanisms to ensure the “scope” value of the attribute asserted by an Identity Provider matches one permitted to the associated Home Organization.

6. Amendment

The Federation Operator has the right to amend the Attribute Profile from time to time. Any such amendments need to be approved by the HKAF Steering Committee and shall be communicated to all Federation Members with reasonable advance notice.

The amended Attribute Profile will become binding upon the Federation Members at the time provided in the amendment. All Federation Members MUST support the latest set of Core Attributes in their Identity Providers within the timeframe specified by the Federation Operator. The latest version of the Attribute Profile is made available on the HKAF website at https://www.hkaf.edu.hk/attribute-profile.