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

HONG KONG ACCESS FEDERATION

Hong Kong Access Federation (HKAF)

Identity Provider Management Standard

Version 1.0

1. Document Control

1. Document Status

Document Name	HKAF Identity Provider Management Standard
Document Code	HKAF-P-IDPMS
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Superseded Version	N/A

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

The HKAF Federation Policy requires that, when acting as a Home Organization, Federation Member MUST ensure that the deployment of each of its Identity Providers complies with all the rules defined in this HKAF Identity Provider Management Standard.

4. Rules for Identity Provider

a. The Home Organization MUST collect or generate in its Identity Provider the Core Attributes as defined by the Federation.

b. The Home Organization MAY ONLY release Attributes from its Identity Provider to a Service Provider, or another Identity Provider, with the permission of the End User.

c. The Home Organization MUST ensure that accurate information is provided about End Users in its Identity Provider. In particular:

- Credentials of End Users who are no longer permitted by the Home Organization to access the Federation MUST be revoked promptly, or at least no Attributes must be asserted for such End Users from its Identity Provider to other Service Providers;
- Where unique persistent Attributes are associated with an End User, the Home Organization MUST ensure that these Attribute values are not re-issued to another End User for at least 24 months after the last possible use by the previous End User; and
- Where an End User's status, or any other information described by Attributes, changes, the relevant Attributes MUST be also changed as soon as possible.

d. The Home Organization MUST use reasonable endeavors to provide those End Users in respect of to whom it provides the Attributes, with appropriate information on how to use their credentials safely and securely.

e. The Home Organization MUST ensure that sufficient logging information in its Identity Provider is retained for the period specified by the Federation (6 months) to be able to associate a particular End User with a given session that it has authenticated.

f. The Home Organization MUST make anonymized usage and log information of its Identity Provider available to the Federation Operator for the purposes of assisting the troubleshooting of access issues and developing aggregated /anonymized usage statistics.

g. The End User will be responsible for their acts or omissions, including abiding by any licenses or other agreements, and complying with the policies set by the Home Organization and /or the Service Provider Organization. If an End User is subject to conflicting policies, then the more restrictive policy will apply.

5. Amendment

The HKAF Federation Operator has the right to amend the HKAF Identity Provider Management Standard 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 Identity Provider Management Standard available on the HKAF website at https://www.hkaf.edu.hk/idp-management-standard. The HKAF Federation Operator will also communicate changes to the HKAF Identity Provider Management Standard to all HKAF Federation Members with reasonable advance notice.