Joint Universities Computer Centre Limited

Identity and Access Management Task Force (IAM-TF)

A. Terms of Reference

1. Fostering periodic sharing and discussion in the application of IAM technologies and practices;
2. Facilitating collaboration in the discussion, evaluation and pilot deployment of innovative technologies to support core businesses of common interest which are related to user experience improvement;
3. Providing advices to the HKAF Operator Team on proposal of long-term strategy and development, administrative and technical optimization;
4. Providing advices to the HKAF Operator Team on proposal of changes to the HKAF policy framework;
5. Establishment of relationship and collaboration with international IAM organizations;
6. Preparation of IAM-TF annual project and budget plan.

B. Membership

1. Each JUCC Member Institution appoints a person as its Official Representative in the IAM-TF and an additional person as its Alternate Representative in the IAM-TF;
2. Only the Official Representatives of JUCC Full Member Institutions are entitled to vote at IAM-TF meetings;
3. The Convenor of the JUCC IAM-TF is appointed by the JUCC Steering Committee;
4. Members of the IAM-TF would take turns to serve as secretary in the meetings;
5. HKAF Operator Team members are *ex-officio* IAM-TF members.

C. Roles and Responsibilities of Representatives

1. Updating /consulting /reporting to relevant stakeholders in their home institutions (including their official representatives in JUCC-SC) on matters related to IAM-TF activities and representing their home institutions in the voting in IAM-TF meetings;
2. Contributing in HKAF projects led by Project Leads of the HKAF Operator Team for the collective benefits of all member institutions;
3. Providing advices to the HKAF Operator Team on proposal of long-term strategy and development, administrative and technical optimization;
4. Providing advices to the HKAF Operator Team on proposal of changes to the HKAF policy framework;
5. Contributing to propose and lead the sharing and discussion on different topics of interest;
6. Participating in the sharing and discussion on different topics of interest;

7. Collaborating with other members in the discussion, evaluation and pilot deployment of innovative technologies to support core businesses of common interest which are related to user experience improvement.

D. Frequency of Meetings

On need basis

E. Reporting to Steering Committee

On need basis, not less than once per year

F. Current Projects

1. CyrptoBLK was awarded by JUCC as the contractor to implement Academic Certificate Verification Platform, CryptoBLK is currently working with HKAF member to join HKAF as Service Provider (SP).
2. Vocational Training Council (VTC) and Tung Wah College are currently working in progress to join HKAF as Identity Provider (IDP).

The HKAF Technology Infrastructure Service & Operation and Development could be referred to in Appendix I.

G. Potential projects

1. HKAF-OT will focus on recruiting and helping more organizations to join HKAF.

Version: 19 February 2021

Appendix I: HKAF Technology Infrastructure Service & Operation and Development

1.1 HKAF Production Federation

The Authentication & Authorization Infrastructure (AAI) for the HKAF Production Federation was deployed by support staff of AAF (Australian Access Federation) in Jun 2016 under a professional service contract established via a tender exercise. Server hosting service was provided by CUHK.

The AAI has the following components:

1.1.1 HKAF Federation Registry

HKAF operates and maintains the Federation Registry for the administration of the Federation. IdPs and SPs are called entities in the context of the Federation Registry. IdP and SP administrators of HKAF federation members keep all relevant information about their respective entities up to date, including contact and support information, technical configuration details, attribute requirements, attribute release policies, intended audience, etc. This data is stored in a database. From this database, HKAF generates various types of other data used elsewhere, such as metadata files or attribute release configurations for IdPs. New SP entries and changes to existing SPs in the Federation Registry require approval before they become active and appear in the metadata. This is the responsibility of the Technical Contact of the HKAF member organization accountable for the SP. After a check for correctness and compliance, they approve the new entry or change.

1.1.2 HKAF Metadata Service

HKAF operates and maintains the Metadata Service, which digitally signs and publishes the properties of HKAF Members and eduGAIN metadata.
The HKAF publishes three metadata documents:

- https://md.hkaf.edu.hk/hkaf-metadata.xml
  Containing all HKAF Member organizations.
- https://md.hkaf.edu.hk/edugain-metadata.xml
  Containing IdP and SP which have been approved for consumption by HKAF subscribers from the global eduGAIN metadata source (eduGAIN Downstream Metadata).
- https://md.hkaf.edu.hk/hkaf-edugain-metadata.xml
  Containing HKAF subscribed IdP and SP which have been approved for publishing to the global eduGAIN metadata source.

1.1.3 HKAF Central Discovery Service

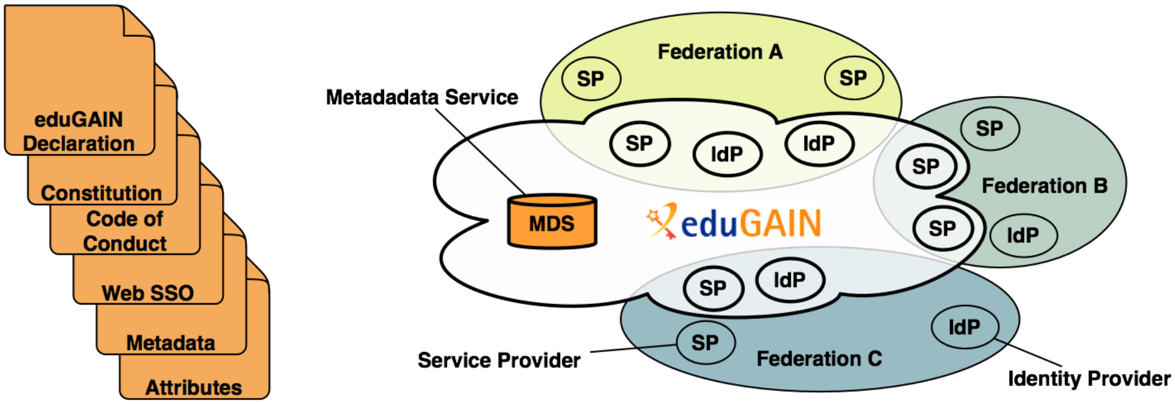
HKAF operates and maintains a Central Discovery Service, also known as a Where Are You From (WAYF) service.
SPs can either use this Central Discovery Service or configure a local Discovery Service. It lets the User choose his /her Home Organization from a list of organizations and then redirects the User to the Login Page of the Identity Provider of the selected organization for authentication. HKAF provides the SP administrators with the information they require.

1.1.4 Interfederation Service - eduGAIN

Interfederation is the general term describing the interconnection of AAI (Authentication & Authorization Infrastructure) services across the boundaries of a federation.

The HKAF Operator Team, on behalf of JUCC, is responsible for maintaining relationship with national and international stakeholders in the area of Federated Authentication and Authorization, primarily in the R&E sector. This includes in particular relationship with interfederation activities. If it benefits the HKAF community, JUCC can enter into agreements with the stakeholders and exchange metadata; for example, with other federations and/or interfederation services. Through participation in interfederation, organizations can offer their services to end users of other federations and enable their own end users to access the services of other federations. Through participation in interfederation, organizations help reduce the number of local end user accounts.

JUCC submitted the eduGAIN Policy Framework Policy Declaration signed by the JUCC Director for HKAF to join eduGAIN in Jul 2017. HKAF was subsequently accepted by the eduGAIN Steering Group as the 54th Member of eduGAIN after a stringent review of the HKAF Policy & Identity Assurance Framework and Metadata Registration Practice Statement.



eduGAIN (education Global Authentication Infrastructure) is a global interfederation service that is developed and operated by the European GÉANT project. It is one of the first and currently the largest global interfederation service in operation. Its purpose is to provide a common set of technical standards, rules and policies that allow services and organizations from different countries to provide and use AAI-enabled services.

a. eduGAIN Upstream Metadata
   - All Identity Provider (IdP) entities registered in the HKAF Production Federation are included in the eduGAIN Upstream Metadata by default. The registering organization has to explicitly inform HKAF Operator Team to opt-out its IdP entity from the eduGAIN Upstream Metadata, if needed.
   - All Service Provider (SP) entities registered in the HKAF Production Federation are excluded from the eduGAIN Upstream Metadata by default. The registering organization has to explicitly inform HKAF Operator Team to opt-in its SP entity in the eduGAIN Upstream Metadata, if needed.

b. eduGAIN Downstream Metadata
   - All entities (Identity Provider, Service Provider and Attribute Authority) registered by other eduGAIN member federations in the eduGAIN Downstream Metadata are included in the eduGAIN metadata feed by default.
   - HKAF Operator Team will not filter any entity unless because of security consideration.

1.1.5 HKAF Attribute Validator

HKAF provides an SP known as the Attribute Validator that requests as many attributes as possible from the IdP, and displays them for the end user on a website.

- An IdP can use it to check whether its attributes are issued correctly.
- End users can see which attributes are issued by their IdP.
- If they suspect misconduct on the part of their SP, SP Administrators and advanced end users can check whether their IdP is working correctly with the Attribute Validator and thus narrow down the possible cause.

1.2 HKAF Test Federation

HKAF operates and maintains a Test Federation for the purpose of testing new components and configurations.

The AAI for the HKAF Test Federation was implemented by CUHK colleagues in Apr 2017 with the support of AAF. It contains the required components, which demonstrate the functionality of the HKAF Federation and the configuration options in details. Server hosting service was again provided by CUHK.

1.3 HKAF Website

The HKAF Website was designed and developed by PolyU under a web development contract. The website was launched in Jul 2017 with contents provided by different member institutions.

1.4 HKAF Business Operation

HKAF Business Operation is taken up by JUCC Office. The scope of works is as follows:

a. Membership Application & Registration
b. Policy & Identity Assurance Framework (with support of HKAF-OT)
c. Member Compliance Management (with support of HKAF-OT)
d. Communication & Promotion (including HKAF website)
e. Community Engagement & Outreach
f. International Ecosystem Relationship Management - eduGAIN, REFEDS, other federation operators (with support of HKAF-OT)

1.5 HKAF Service Operation

Operation of the HKAF Production Federation is supported by HKAF-OT, on voluntary basis. The scope of works is as follows:

a. Federation Registry
    - Creation /modification /removal of member organization (by JUCC Office)
    - Entity registration (IdP, SP)

b. Metadata Service
c. Central Discovery Service
d. Interfederation Service (eduGAIN)
e. Attribute Validator Service

The operation of the HKAF Test Federation is also supported by HKAF-OT.

With the coming adoption of Jisc’s Managed Federation Service for implementing the HKAF Technology Infrastructure, the effort of the HKAF-OT in the service operation of the technology infrastructure will decrease in the future.

1.6 HKAF Development

The international federation ecosystem is gradually evolving in various aspects: technology, policy & assurance, and service management. Development in different areas is essential for HKAF to transform and innovate in order to keep in line with the international trend and to remain relevant to the future needs of the Research and Education community of Hong Kong. These areas include the following:

a. Technology Infrastructure
b. Assurance & Compliance
c. OpenID Connect for Research & Education (OIDCre)
d. Federated Identity Management for Research (FIM4R)
e. Federated Identity Management for Library (FIM4L)
f. Service Management
g. Service Development

The requirements for the development will be managed under the IAM-TF. IAM-TF members discuss /initiate projects under different areas, and make proposals to JUCC-SC for approval.