JUCC Joint Universities Computer Centre Ltd.
大學聯合電腦中心

HONG KONG ACCESS FEDERATION

Hong Kong Access Federation (HKAF)

Level-1 Identity Assurance Profile

Version 1.1

1. Document Control

1.1 Document Status

Document Name	HKAF Level-1 Identity Assurance Profile
Document Code	HKAF-P-IDAL1P
Author	HKAF Operator Team
Version Number	1.1
Document Status	~~Draft for Internal Review~~ / ~~Release for Consultation~~ / Approved
Date Approved	05-Jan-2018
Date of Next Review	01-Jul-2021
Superseded Version	N/A

1.2 Document History

Version Number	Revision Date	Summary of Changes	Authored By	Approved By
1.0	06-Oct-2017	Official release	HKAF Operator Team	JUCC Steering Committee
1.1	18-Dec-2017	• Updating the scope in p.4 to specify the user identities required to be covered under the compliance with this level of identity assurance	HKAF Operator Team	JUCC Steering Committee

2. Terminology and Typographical Conventions

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.

Text in *Italics* is non-normative. All other text is normative unless otherwise stated. All normative parts of the profile are governed by the Hong Kong Access Federation Steering Committee.

The non-normative (guidance) is maintained by the HKAF Operator Team. HKAF has multiple identity assurance levels. All identity assurance profiles share the same numbering scheme.

2.1. Definition of terminology

Home Organization: The HKAF Member Organization with which a Subject is affiliated, operating the Identity Provider by itself or through a third party.

Member Organization: Used in this document as a synonym for Home Organization.

Subject: any natural person affiliated with a Home Organization, e.g. as a teacher, researcher, staff or student.

Identity Provider (IdP): The system component that issues Attribute assertions on behalf of Subjects who use them to access the services of Relying Party.

Relying Party (RP): A Service that relies upon a Subject’s credentials, typically to process a transaction or grant access to information or a system. Also called a Service Provider (SP).

Shared Secret: A piece of information that is shared exclusively between the parties involved in a secure communication. The shared secret can be a password, a passphrase, a big number or an array of randomly chosen bytes.

Credential: A piece of information which the Subject use to authenticate with (aka. login). The credential can be for example a password, a passphrase, a one-time password device or a certificate.

CAPTCHA: A challenge-response test used as an attempt to ensure that the response is generated by a human being, e.g. a picture with characters that a Subject must retype in a text field.

3. Purpose, Scope and Summary

This document defines the lowest common level of identity assurance which each Member Organization of the Hong Kong Access Federation (HKAF) who acts as a Home Organization MUST attain for its end user identities with the affiliation of ‘staff’ or ‘student’, or both. Please note that some Relying Parties may have this as a requirement for their services.

This identity assurance profile does not represent Assurance Level 1 (AL1) in the sense of Kantara Initiative Identity Assurance Framework: Service Assessment Criteria (Kantara IAF-1400-SAC).

This identity assurance profile does not represent Level of Assurance 1 (LoA1) in the sense of NIST Electronic Authentication Guideline (NIST SP 800-63).

A claim at this level of identity assurance implies roughly the following:

- The subject is probably affiliated with the HKAF Member.
- The subject is very likely a human and not a robot or piece of software.
- The subject is most likely identified by a unique permanent user identifier.
- Attributes /information released may be self-asserted.

Relying parties in HKAF may require elevated levels of identity assurance.

4. Compliance and Audit

4.1 Evidence of compliance with this profile MUST be part of the Identity Management Practice Statement, maintained as a part of the HKAF membership process. The Identity Management Practice Statement MUST describe how the organization fulfils the normative parts of this document.

4.2 The organization declares compliance with this assurance profile via a self-audit. This declaration is submitted to the HKAF Operator Team together with the IMPS.

The Member MUST annually confirm that their IMPS is still valid.

When there are changes in the identity management process or technology, a new self-audit with the updated IMPS MUST be submitted.

Guidance: *HKAF Operator Team supplies both an IMPS form and a compliance evaluation form. All parts of the template must be reflected in the Member's submitted IMPS. The organization declares their compliance with this assurance profile via the compliance evaluation form.*

4.3 The HKAF Steering Committee MAY impose an external audit performed by HKAF Operator Team in special cases.

Guidance: *This type of audit is normally conducted after a security incident.*

5. Organizational Requirements

The purpose of this section is to define conditions and guidance regarding the responsibilities of participating organizations.

5.1 Enterprise and Service Maturity

This subsection defines the Member organization and the procedures that govern the operations of the Identity Provider connected to HKAF.

5.1.1 The Member organization MUST pass the eligibility tests for FULL membership of HKAF, as stated in the latest version of the HKAF Eligibility Policy, which is available on the HKAF website at https://www.hkaf.edu.hk/policy/eligibility-policy.

5.1.2 The Member organization MUST adhere to applicable legislation of Hong Kong. The Member organization SHOULD maintain a list of applicable legislation for the Identity Provider and underlying systems.

5.1.3 The Member organization MUST have documented procedures for data retention and protection in order to ensure the safe management of Subject information.

***Guidance**: The Member organization must have defined decommission procedures of the Identity Provider and underlying systems when they are replaced or decommissioned. Special considerations should be taken for decommissioned Components (e.g. hard drives, backup media and other storage media) that may contain sensitive or private Subject information, such as passwords, HKID Number etc. These must be safely and permanently disposed of.*

5.2 Notices and User Information

The Member organization provides an Acceptable Use Policy (AUP) and a Service Definition including a Privacy Policy (PP) for the End Users of the organization. These policies are needed to fulfil the HKAF Federation Policy and the applicable legislation of Hong Kong, including the Personal Data (Privacy) Ordinance (Cap. 486).

5.2.1 Each Member organization MUST publish the Acceptable Use Policy to all End Users including any and all additional terms and conditions.

5.2.2 All End Users MUST indicate acceptance of the Acceptable Use Policy before use of the Identity Provider.

***Guidance:** A suggested way to fulfil this requirement is to display and accept the Acceptable Use Policy at first login in the Identity Provider.*

5.2.3 All End Users MUST indicate renewed acceptance of the Acceptable Use Policy if the Acceptable Use Policy is modified.

***Guidance:** A suggested way to fulfil this requirement is to display and require acceptance of the Acceptable Use Policy from the End User after it has been modified.*

5.2.4 The Member organization MUST maintain a record of End User acceptance of the Acceptable Use Policy.

5.2.5 Each Member organization MUST publish the Identity Provider Service Definition. The Service Definition MUST at least include:

- a General Description of the service;
- a Privacy Policy with reference to applicable Hong Kong legislation;
- any Limitations of the Service Usage and
- Service desk, or equivalent, contact details.

Guidance: *HKAF's recommendation is to use HKAF's best practice policy template if none other exists.*

5.3 Secure Communications

This subsection defines how clear text passwords, private keys and shared secrets must be protected to obtain operational security.

5.3.1 Access to shared secrets MUST be subject to discretionary controls which permit access to those roles/applications needing such access.

Guidance: *There should be documented procedures for life cycle management of administrative accounts. Access should be limited to as few individuals as possible.*

5.3.2 Private keys and shared secrets MUST NOT be stored in plain text form unless given adequate physical or logical protection.

Guidance: *Password files and private keys on servers must not be openly accessible but should be subject to operating system access control/restrictions.*

5.3.3 All network communication between systems related to Identity or Credential management MUST be secure and encrypted, or be physically secured by other means.

Guidance: *Always use TLS or equivalent for establishing encrypted communications between endpoints and use client certificates or account authentication between services. For example, the communication between an Identity Provider and an LDAP server and the communication between a web application for account management and the identity management backend (e.g. Active Directory) must be encrypted.*

5.3.4 Service Provider and Identity Provider credentials (i.e. entity keys) MUST NOT use shorter comparable key strength (in the sense of NIST SP 800-57) than a 2048 bit RSA key.

5.3.5 Service Provider and Identity Provider credentials (entity keys) SHOULD NOT be used for more than 10 years and should be changed when doing a major software upgrade or a hardware replacement.

5.4 Security-relevant Event (Audit) Records

This section defines the need to keep an audit trail of relevant systems.

5.4.1 The Member organization MUST maintain a log of all relevant security events concerning the operation of the Identity Provider and the underlying systems, together with an accurate record of the time at which the event occurred (timestamp), and retain such records with appropriate protection and controls to ensure successful retrieval, accounting for service definition, risk management requirements, applicable legislation, and organizational policy.

(Not applicable in HKAF Identity Assurance Level 1.)

6. Operational Requirements

The purpose of this section is to ensure safe and secure operations of the service.

6.1 Credential Operating Environment

The purpose of this subsection is to ensure adequate strength of End User credentials, such as passwords, and protection against common attack vectors.

6.1.1 Passwords MUST contain at least 10 bits of entropy as defined in NIST SP 800-63-2, Appendix A. If other authentication methods are used, they must be at least equivalent in strength.

Guidance: *HKAF's STRONG recommendation is to use complex passwords of at least 8 characters in length. This gives at least 24 bits of entropy. More details and a template password policy are provided in the compliance evaluation form associated with the IMPS template. Other authentication mechanism could be smartcards, hardware tokens that replaces passwords.*

6.1.2 All protocols used MUST be protected against message replay.

Guidance: *ALL HKAF technology profiles fulfil this requirement.*

6.1.3 End Users MUST be actively discouraged from sharing credentials with other End Users either by using technical controls or by requiring users to confirm policy forbidding sharing of credentials or acting in a way that makes stealing credentials easy.

6.1.4 The organization MUST take into account applicable system threats and apply appropriate controls to all relevant systems.

Guidance: *Example of system threats are:*

1. *the introduction of malicious code;*
2. *compromised authentication arising from insider action;*
3. *out-of-band attacks by other users and system operators;*
4. *spoofing of system elements /applications;*
5. *malfeasance on the part of Subscribers and Subjects.*

6.2 Credential Issuing

The purpose of this subsection is to ensure that the Identity Provider has control over the issuing process. All Service Providers have a need to uniquely identify the Identity Provider and the Identities provided by that Identity Provider.

6.2.1 Each End User assertion MUST include a unique representation of the administrative domain associated with the Identity Provider including a unique identifier of the Member organization.

Guidance*: Normally the administrative top level domain of the Member organization is used.*

6.2.2 Each Identity Provider instance MUST have a globally unique identifier.

Guidance*: ALL HKAF technology profiles fulfil this requirement.*

6.2.3 Each End User identity MUST be represented by an identifier ("username") which MUST be unique for the Identity Provider.

Guidance: *End User unique identifiers SHOULD not be re-assigned unless the unique identifier is known to be unused by all Service Providers.*

6.2.4 If an End User has more than one set of unique identifier within the Identity Provider (e.g. a student identifier and an employee identifier), the End User MUST be able to choose what set shall be used at login.

6.2.5 End User enrolment MUST be done using one of the following methods:

1. On-line using an e-mail with a one-time password /pin code in combination with an on-line CAPTCHA or equal;
2. On-line authenticating the End User at HKAF Identity Assurance Level 1 or higher level using an external Identity Provider;
3. In-person visit at a service desk, or equivalent;
4. Off-line using a postal mail with a one-time password /pin code; or
5. Other equivalent identity proofing method.

Guidance: *No identity verification is formally required for this Identity Assurance Level. However, HKAF strongly recommends that when in-person visit is used, a verification of valid and legal identity documents is performed and a record of this is maintained in the Identity Management System.*

6.2.6 The Member organization MUST maintain a record of all changes regarding Identity Assurance Level of Subjects.

(Not applicable in HKAF Identity Assurance Level 1.)

6.2.7 The End User MUST be able to update stored self-asserted personal information.

6.2.8 The Registration Authority performing the identity proofing needed to verify HKAF Identity Assurance Level 1 compliance MUST be authorized to perform identity proofing at HKAF Identity Assurance Level 1 (IDAL1) or higher. To be authorized to perform identity proofing at HKAF Identity Assurance Level 1, the Registration Authority itself MUST be using credentials at HKAF Identity Assurance Level 1 or higher.

Guidance*: Both systems and system administrators, personnel at helpdesks and other Registration Authorities must use at least IDAL1 credentials when working with other IDAL1 credentials.*

6.3 Credential Renewal and Re-issuing

Renewal of credentials occur when the End User changes its credential using normal password reset. Re-issuing occurs when credentials have been invalidated.

6.3.1 All End Users MUST be allowed to change their credentials while applying best practice with regards to credentials management (e.g. password reset and quality policies).

Guidance*: For example, use of Active Directory password policy fulfils this requirement.*

6.3.2 End Users MUST demonstrate possession of current credentials before allowing the credential to be renewed.

Guidance*: Ask and verify the user's current password before allowing it to be changed. Remember to* *disable SSO for the changing password application.*

6.3.3 Credential Re-issuing MUST be done using one of the following methods

1. Any of the methods in 6.2.5
2. A channel that MUST be verified in advance using HKAF Identity Assurance Level 1 (IDAL1) credentials by the End User
3. A pre-linked account from another external Identity Provider compliant with IDAL1 or higher

***Guidance item 1**: A channel can for example be an activation link by email or a PIN code by SMS.*

***Guidance item 2**: Account linking can be used during password reset of End Users using a pre-linked account at an external Identity Provider compliant with IDAL1 or higher. However, the two Identity Providers MUST use different unique identifiers.*

6.4 Credential Revocation

The purpose of this subsection is to ensure that credentials can be revoked.

6.4.1 The Member organization MUST be able to revoke an End User's credentials.

6.4.2 For Credential Re-issuing after Revocation, the Member organization MUST use one of the methods in 6.2.5.

6.5 Credential Status Management

The purpose of this subsection is to ensure that credentials are stored properly and that Identity Management systems have a high degree of availability.

6.5.1 The Member organization MUST maintain a record of all credentials issued.

***Guidance:** All changes, such as password changes and/or new/closed credentials shall be stored in accordance with the applicable legislation of Hong Kong.*

6.5.2 The Member organization’s Identity Management System MUST have a minimum availability of 95%.

***Guidance:** This requirement is to give Service Providers a minimum level of expected uptime from the Identity Provider which the Service Provider can perform an authentication request. The figure is on annual basis.*

6.6 Credential Validation /Authentication

The purpose of this subsection is to ensure that the implemented Validation /Authentication processes meet proper technical standards.

6.6.1 The Identity Provider MUST provide validation of credentials to a Service Provider using a protocol that:

1. requires authentication of the specified service or of the validation source;
2. ensures the integrity of the authentication assertion;
3. protects assertions against manufacture, modification and substitution, and secondary authenticators from manufacture;

   and which, specifically:

4. creates assertions which are specific to a single transaction;
5. where assertion references are used, generates a new reference whenever a new assertion is created;
6. when an assertion is provided indirectly, either signs the assertion or sends it via a protected channel, using a strong binding mechanism between the secondary authenticator and the referenced assertion;
7. requires the secondary authenticator to:
    1. be signed when provided directly to the Service Provider, or;
    2. have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).

***Guidance**: ALL HKAF technology profiles fulfil this requirement when implemented as recommended by the HKAF Operator Team.*

6.6.2 The Identity Provider MUST not authenticate credentials that have been revoked.

***Guidance**: Only active accounts shall be authenticated, i.e. don't authenticate revoked or closed accounts.*

6.6.3 The Identity Provider MUST use an authentication protocol that requires the claimant to prove possession and control of the authentication token.

***Guidance**: Any authentication protocols used when authenticating Subjects MUST require a proof-of-possession step for Subject credentials. For regular passwords this involves validating that the user knows his /her password.*

6.6.4 The Identity Provider MUST generate assertions so as to indicate and effect the expiration of the Single Sign-On sessions within one hour after their creation, where the Identity Provider does not share an Internet Domain with the Service Provider.

***Guidance**: This means that Single Sign-On sessions can only be valid for a maximum of one hour.*

6.6.5 The Member organization MUST effect in the Identity Provider any change in identity status within 24 hours.

7. Technical Representation

For all technology profiles, compliance with this identity assurance profile is equivalent with the existence of a valid Identity Provider issuing valid identity claims, specifically:

Technology Profile	**Representation of https://www.hkaf.edu.hk/idal1-profile**	**Representation of the administrative domain**
SAML WebSSO	The existence of a SAML IdP in published SAML metadata	Shibboleth scope