

## Hong Kong Access Federation (HKAF) Identity Management Practice Statement (IMPS)

This document (IMPS) facilitates an organization to provide relevant information to describe how it fulfils the normative parts of the HKAF Level-1 Identity Assurance Profile.

The organization **MUST** also declare its compliance via a self-audit on the 'HKAF Identity Assurance Compliance Evaluation Form', to be submitted with this document to the HKAF Operator Team.

The document must be signed by a person who is officially nominated by the organization as the 'Service Manager' of the 'HKAF Federated Authentication Service' for the organization.

<b>Official Organization Name in English</b>
<b>Official Address</b>

Signature: I hereby certify that, on behalf of the organization I represent, the information provided in this document is correct.

<b>Signature</b>	<b>Date</b>
<b>Full name (in block letters)</b>	<b>Title</b>

Note:

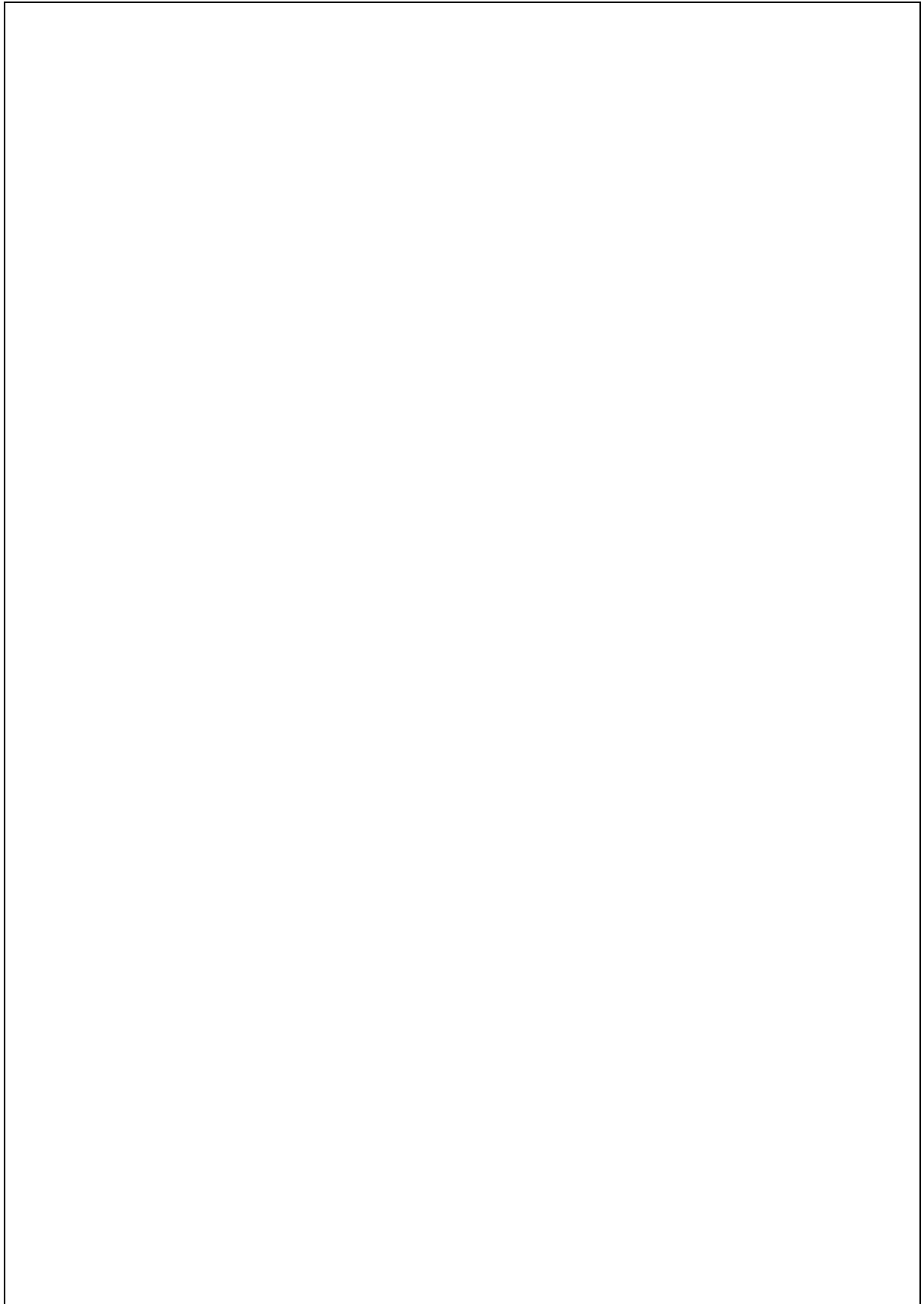
1. For the sake of clarity, the numbering scheme used for the requirements in this IMPS is kept consistent with the HKAF Level-1 Identity Assurance Profile and the HKAF Identity Assurance Compliance Evaluation Form.
2. Please declare the compliance of each requirement in the corresponding text box in the 'HKAF Identity Assurance Compliance Evaluation Form'.
3. Please refer to the 'HKAF Identity Assurance Compliance Declaration Guidance' document for support in providing the supporting information in the corresponding text box for the requirements in this IMPS.

Please send the completed IMPS together with the associated completed 'Identity Assurance Compliance Evaluation Form' to:

Joint Universities Computer Centre Ltd.  
 HKAF Operator Team  
 c/o Information Technology Services,  
 The University of Hong Kong,  
 Pokfulam Road,  
 Hong Kong.

# 1. Introduction

*[Short introductory text about the Member organization and its relationship to JUCC and HKAF]*

A large, empty rectangular box with a thin black border, occupying most of the page below the introductory text. It is intended for the user to provide the introductory text mentioned in the green italicized text above.

## 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.

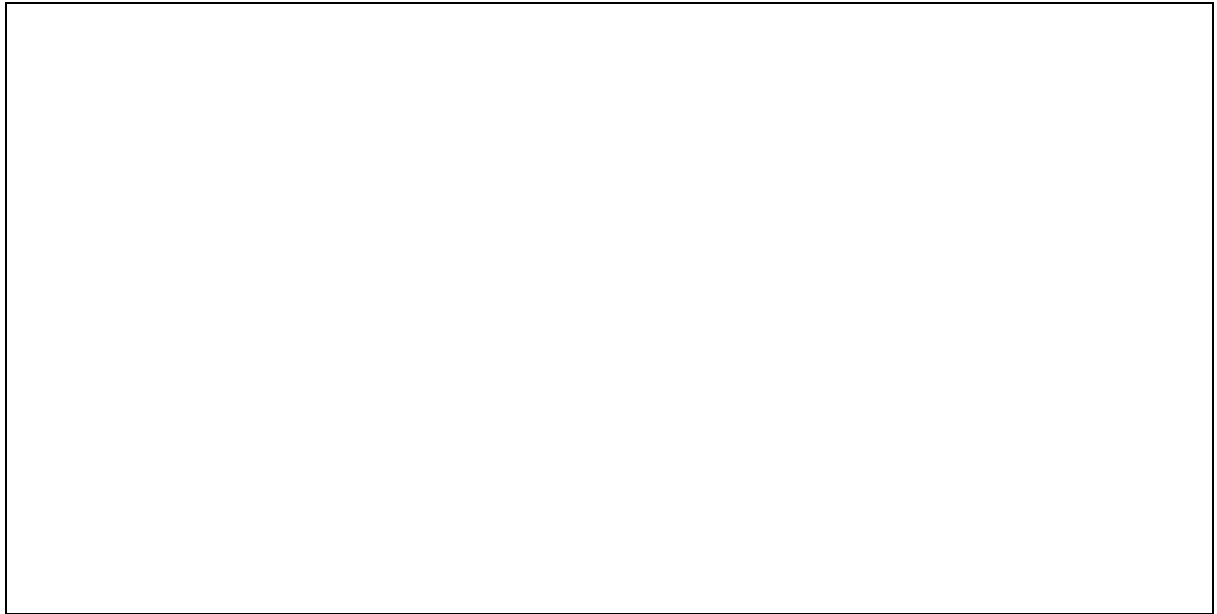
**5.1.3** The Member organization **MUST** have documented procedures for data retention and protection in order to ensure the safe management of Subject information.

**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.*

*[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind that the following points should be described:*

- *Organization's legal status reference (5.1.1).*
- *Applicable legislation (5.1.2).*

- *Procedures for destruction of storage media (5.1.3).]*



## 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 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.

*[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind the following points shall be described:*

- *The presence of terms and how they are presented to the users (5.2.1 – 5.2.4), examples of acceptable use policy are provided by HKAF Operator Team.*
- *The presence of Service definition and additional documentation (5.2.5), examples of service definition and privacy policy are provided by HKAF Operator Team.]*

## 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.

*[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind that the following points must be described:*

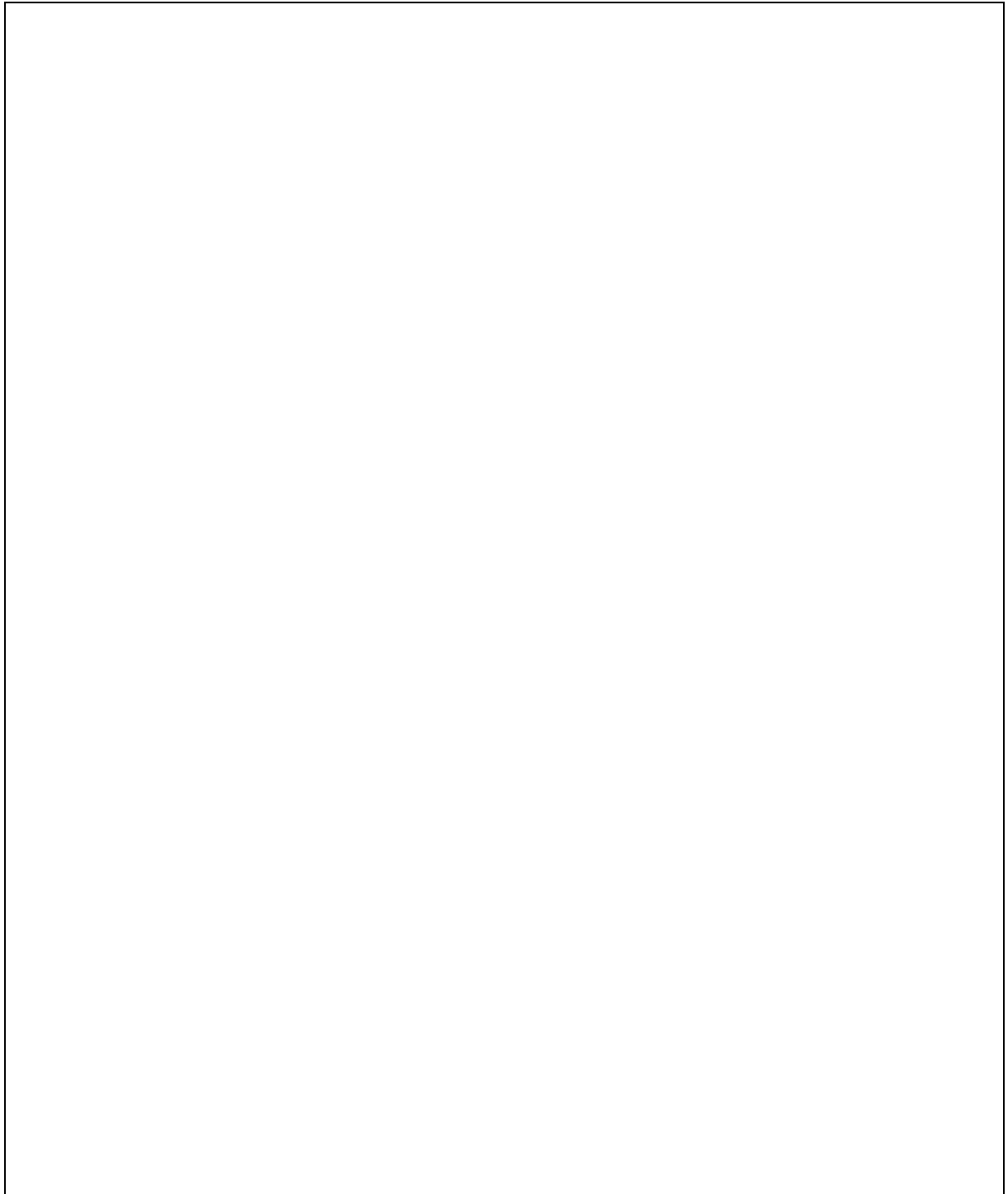
- *Technical implementation of IT security around Identity Manager (5.3.1-5.3.4).]*

## **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 guidance. 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.

[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind the following points shall be described:

- Password policy (6.1.1), example of password policy is provided by HKAF Operator Team.
- What are the technical protocols used (6.1.2).
- Procedures for protection against abuse (6.1.3-6.1.4).]

## 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.)

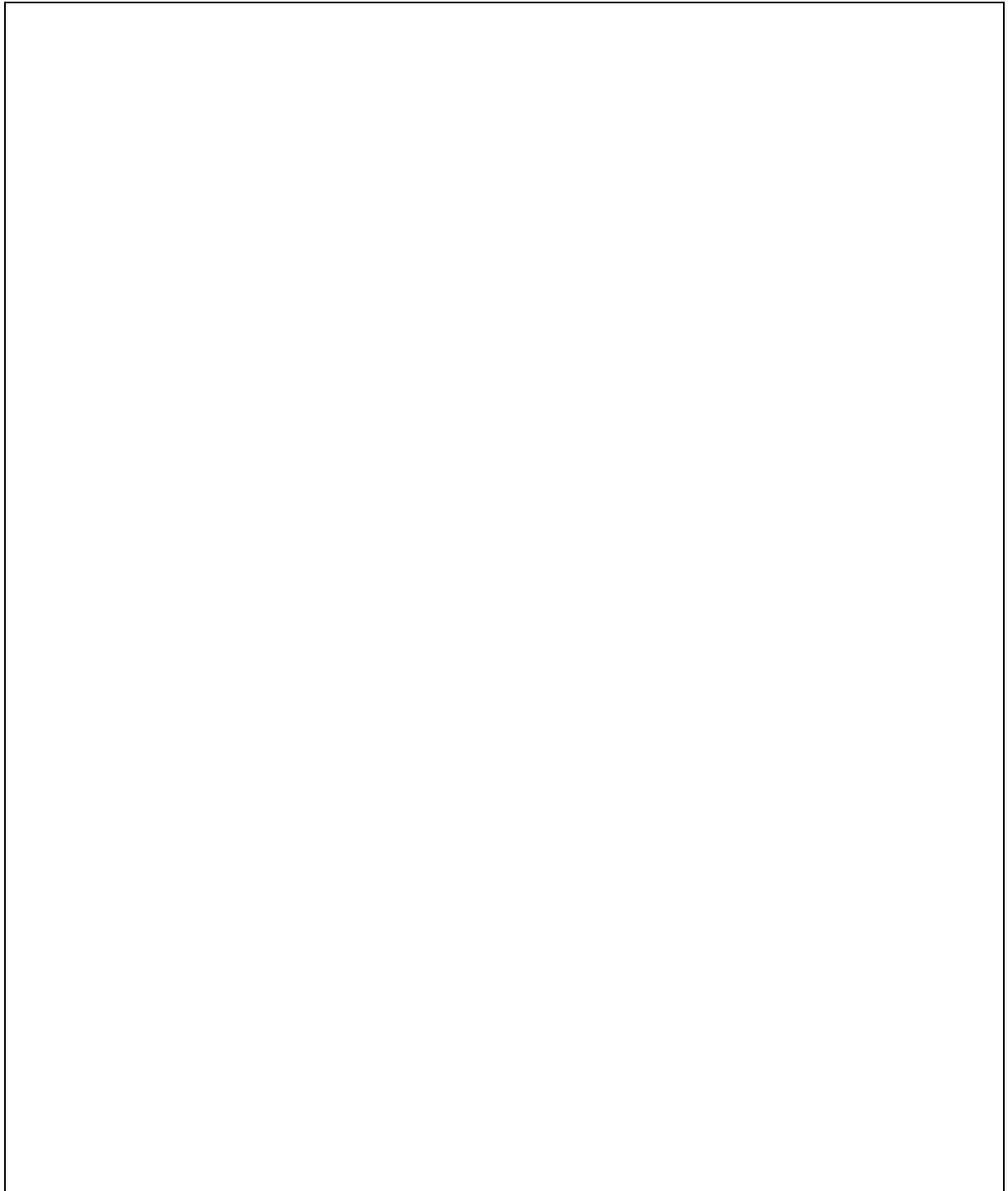
**6.2.7** The End User MUST be able to update stored self-asserted personal information.

**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.

[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind the following points shall be described:

- Identity Manager DNS domain (6.2.1).
- Management of user names /accounts (6.2.2-6.2.4).
- Identification methods (6.2.5).
- Change of the self declared information (6.2.7).
- Requirements for identity audit (6.2.8).]



## 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.

*[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind that the following points must be described:*

- *User's optional password change (6.3.1-6.3.2).*
- *Resetting the user's password (6.3.3).]*

## 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.

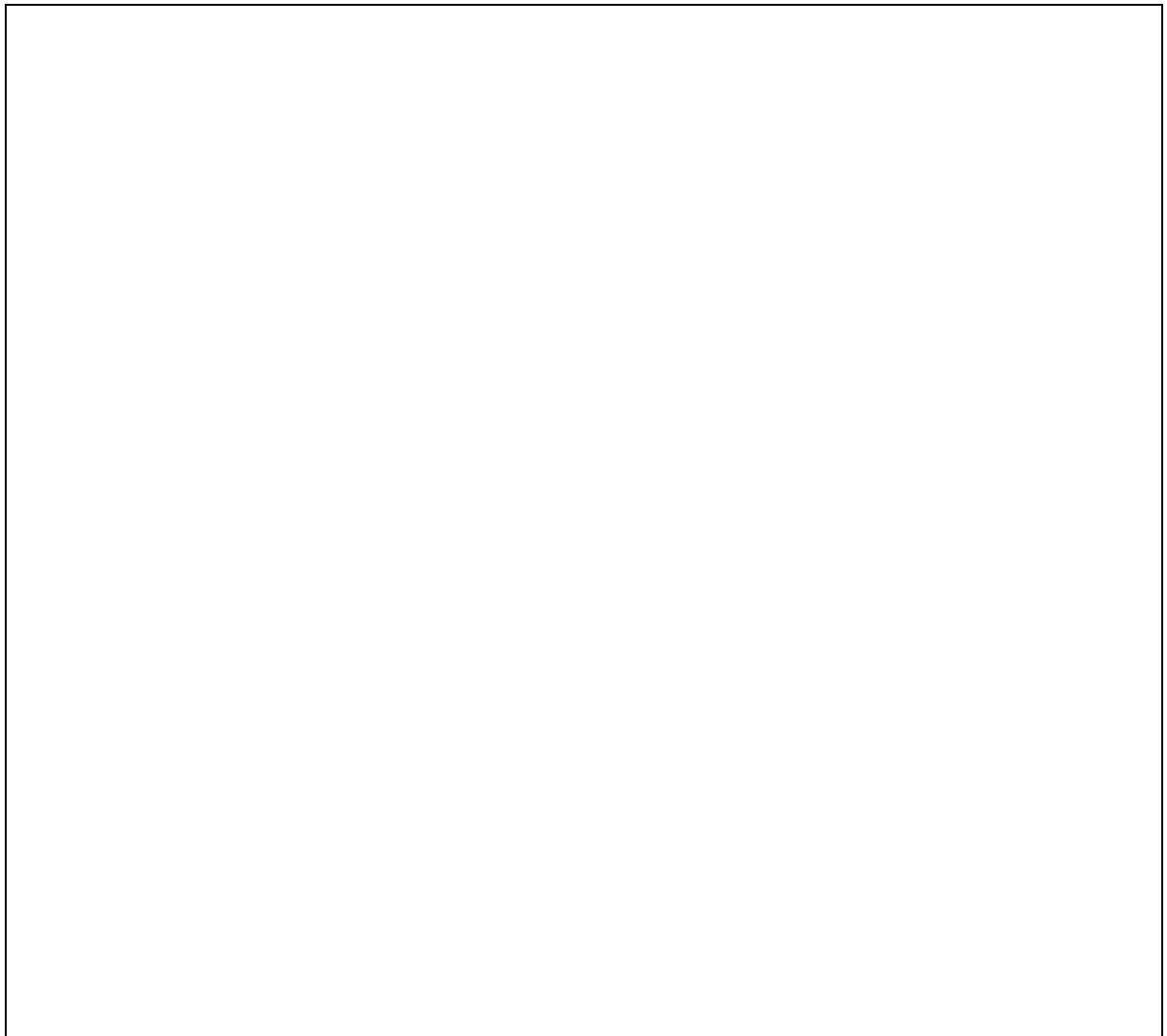
**6.4.2** For Credential Re-issuing after Revocation, the Member organization MUST use one of the methods in

#### 6.2.5.

*[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind the following points shall be described*

- *freezing of login (6.4.1).*
- *Reactivation of log-in (6.4.2).*

*Freezing and reactivation of sign-on means that it should be possible to block the use of a user account and the user must change their sign-in secret, for example. password before the user can use the user account again. A good example of when this needs to be used is when a user lost his password through fishing.]*



## 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.*

*[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind that the following points must be described:*

- *History of issued identities (6.5.1).*
- *The availability of identity service (6.5.2).]*

## **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.

*[Please describe below in the text how the Member organization is in compliance with the section. Keep in mind the following points shall be described:*

- Configurations and protocols not covered by HKAF's recommended best practice (6.6.1-6.6.4).*
- If this type is using explicitly HKAF's recommendations!]*