 

**Hong Kong Access Federation (HKAF)**

**Level-1 Identity Assurance Compliance Evaluation Form**

This form facilitates an organization to declare its compliance with the requirements in the HKAF Level-1 Identity Assurance Profile, via a self-audit.

The organization MUST also provide relevant information in its Identity Management Practice Statement (IMPS) to describe how it fulfils the normative parts of the HKAF Level-1 Identity Assurance Profle, to be submitted together with this form to the HKAF Operator Team.

The completed form must be signed by a person who is officially nominated by the organization as the ‘Management Contact’ of the ‘HKAF Federated Authentication Service’ for the organization.

|  |
| --- |
| **Official Organization Name in English** |
| **Official Address** |

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

|  |  |
| --- | --- |
| **Signature** | **Date** |
| **Full name (in block letters)** | **Title** |

Note:

# For the sake of clarity, the numbering scheme used for the requirements in this form is kept consistent with IMPS and the HKAF Level-1 Identity Assurance Profile.

# Please declare the compliance of each requirement in the corresponding text box in this form.

# Please refer to the ‘HKAF Level-1 Identity Assurance Compliance Declaration Guide’ for guidance in providing the supporting information in the corresponding text box for the requirements in the IMPS.

# Please send the completed ‘HKAF Level-1 Identity Assurance Compliance Evaluation Form' together with the associated ‘Identity Management Practice Statement’ (IMPS) to:

Joint Universities Computer Centre Ltd.

HKAF Operator Team

c/o Information Technology Services,

The University of Hong Kong,

Pokfulam Road,

Hong Kong.

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement Reference** | **Requirement** | **Comply?** **(Yes /No /NA)** | **Remarks** |
| **5. Organizational Requirements** |  |  |
| **5.1 Enterprise and Service Maturity** |  |  |
| 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. |  |  |
| 5.1.2 | The Member organization MUST adhere to applicable legislation of Hong Kong and 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. |  |  |
| **5.2 Notices and User Information**  |  |  |
| 5.2.1 | The 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. |  |  |
| 5.2.3 | All End Users MUST indicate renewed acceptance of the Acceptable Use Policy if the Acceptable Use Policy is 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. |  |  |
| **5.3 Secure Communications**  |  |  |
| 5.3.1 | Access to shared secrets MUST be subject to discretionary controls which permit access to those roles/applications needing such access. |  |  |
| 5.3.2 | Private keys and shared secrets MUST NOT be stored in plain text form unless given adequate physical or logical protection.  |  |  |
| 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. |  |  |
| 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** |  |  |
| 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.) |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Requirement Reference** | **Requirement** | **Comply?** **(Yes /No /NA)** | **Remarks** |
| **6. Operational Requirements** |  |  |
| **6.1 Credential Operating Environment** |  |  |
| 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. |  |  |
| 6.1.2 | All protocols used MUST be protected against message replay. |  |  |
| 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. |  |  |
| **6.2 Credential Issuing** |  |  |
| 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. |  |  |
| 6.2.2 | Each Identity Provider instance MUST have a globally unique identifier.  |  |  |
| 6.2.3 | Each End User identity MUST be represented by an identifier ("username") which MUST be unique for the Identity Provider. |  |  |
| 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.
 |  |  |
| 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. |  |  |
| **6.3 Credential Renewal and Re-issuing** |  |  |
| 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). |  |  |
| 6.3.2 | End Users MUST demonstrate possession of current credentials before allowing the credential to be renewed. |  |  |
| 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
 |  |  |
| **6.4 Credential Revocation** |  |  |
| 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** |  |  |
| 6.5.1 | The Member organization MUST maintain a record of all credentials issued. |  |  |
| 6.5.2 | The Member organization’s Identity Management System MUST have a minimum availability of 95%. |  |  |
| **6.6 Credential Validation/Authentication**  |  |  |
| 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:
8. be signed when provided directly to the Service Provider, or;
9. have a minimum of 64 bits of entropy when provision is indirect (i.e. through the credential user).
 |  |  |
| 6.6.2 | The Identity Provider MUST not authenticate credentials that have been revoked.  |  |  |
| 6.6.3 | The Identity Provider MUST use an authentication protocol that requires the claimant to prove possession and control of the authentication token.  |  |  |
| 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. |  |  |
| 6.6.5 | The Member organization MUST effect in the Identity Provider any change in identity status within 24 hours. |  |  |