The University of Hong Kong
Information Technology Services

Terms and Conditions Governing the Use of HKU Authentication Service

Introduction

The HKU Authentication Service is to support Single Sign On (SSO) authentication of departmental web-based applications and mobile applications using HKU Portal UID/PIN. It supports three authentication protocols, namely the **OpenID Connect, Security Assertion Markup Language (SAML) version 2.0 Authentication Service** and **Central Authentication System (CAS)**. All these protocols provide the options to authenticate login by the types of HKU Portal account holders (i.e. HKU staff, students, departmental account holders and retirees).

OpenID Connect

OpenID Connect is an interoperable authentication protocol based on the OAuth 2.0 specifications. It uses REST/JSON message flows to simplify the authentication process compared to CAS and SAML. OpenID Connect can support SSO on both web applications and mobile applications.

SAML Authentication Service

SAML 2.0 is an open standard for exchanging authentication data between an identity provider (IdP) and a service provider (SP). SAML is an XML-based markup language for security assertions to facilitate SSO among different SPs. If a web application supports the SAML 2.0 protocol, departments should use this protocol to authenticate their applications.

CAS

Central Authentication Service (CAS) is an open source software product developed by the Yale University and it provides authentication service for facilitating SSO among different web applications. ITS customized the CAS which fits for use in the HKU environment. It supports the CAS protocol v2.0 and provides Client APIs for various types of programming platforms in developing web applications using the authentication service. The supported types of programming platforms include the following:

- JAVA
- ASP.NET (C#)
- PHP

Terms and Conditions

Departments applying for the use of HKU Authentication Service for applications developed by departments must abide by the following terms and conditions:

1. The use of HKU Authentication Service must comply with the University's Statement of Ethics on Computer Use (at http://www.its.hku.hk/policies/ethics.htm).

2. The use of HKU Authentication Service is only for discharging the instructional and administrative functions of the University. Departments shall keep the data obtained from HKU Authentication Service in good protection and destroy any related data if the purposes of use have been fulfilled. All the data obtained through HKU Authentication Service should not be passed to third parties without the approval of the Information Technology Services.

3. Departments have to make sure that all data, including personal information processed through HKU Authentication Service and their applications, will be protected and treated strictly confidential.

4. Departments are responsible for protecting the integrity of HKU Authentication Service and their applications during the use of HKU Authentication Service to make sure that no personal information will be disclosed, intentionally or unintentionally, to any unauthorized party(s) or person(s).

5. Departments will bear all responsibilities as a result of the unauthorized disclosure, either intentionally or unintentionally, of personal information which is caused, directly or indirectly, by their applications.

6. Departments will be responsible for damage of any kind to the University's information assets incurred as a result of the failure of their applications.

7. Departments have to make sure that their applications will not interfere, disrupt or impair the performance, reliability and efficiency of the University's servers and network traffic.

8. Departments must enable HTTPS access to ensure the data security when transferring user information from HKU Authentication Service Server to the application servers.

9. The Information Technology Services reserves the right to perform system checking at appropriate time and terminate the provision of HKU Authentication Service on applications should there be reports of hacking activities.

10. Departments engaging a third party to develop and/or maintain the applications are required to ask the third party to sign an agreement stipulating the terms and conditions of

system development to protect the University's interest. The agreement can be found at https://intraweb.hku.hk/local/its/agreement-sign-by-contractor.pdf.

Jan 2020