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 (hereafter "applications") using HKU Portal UID/PIN. It supports two authentication protocols, namely the HKU Central Authentication System (HKUCAS) and the Security Assertion Markup Language (SAML) version 2.0. Both protocols can authenticate HKU staff, student, departmental and retiree accounts with valid HKU Portal UID/PIN.

Modern applications have been using SAML version 2.0. For departmental applications supporting SAML version 2.0, departments should use this protocol to authenticate their applications.

HKU Central Authentication System using HKUCAS API

Central Authentication Service (CAS) is an open source Single Sign On System created in the early 2000s at the Yale University. HKUCAS is customized based on CAS for the HKU environment. It supports the CAS protocol v2.0 and provides Client APIs for various types of programming platforms including:

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

SAML 2.0 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 Single Sign On among different SPs. SAML 2.0 is more preferable than HKUCAS.

Terms and conditions

Departments applying for the use of the HKU Authentication Service for their applications 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 any 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. 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.

9. 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.

June 2018