**Identity and Access Management Implementation at PolyU**

1. **How has PolyU been providing IAM functionalities to the users and applications?**

   Most of the basic functionalities of a modern IAM Framework are not new to enterprises. However, they have been used to be provided by decentralized silo systems, rather than by a modern tightly-integrated infrastructure.

   Over the past decade, PolyU has gradually implemented some IAM functionalities for users and central applications of PolyU with its home-grown Account Management System (AMS) and the University Portal (myPolyU).

2. **How did PolyU come up with the idea of implementing IAM?**

   The completion of the implementation of AMS in 2003 has brought the following benefits to PolyU:

   - Complete NetID lifecycle management;
   - Enhanced security with audit trail on all NetID & account transactions;
   - Flexibility in enforcing service entitlement policies for different groups of users;
   - Savings in manpower for handling account related queries and requests, brought by self-service facilities (e.g. 1000+ ‘Forgotten NetPassword’ operations in September 2006 alone means a saving of 250 man-hours in helpdesk effort plus user travelling time);
   - Faster response and direct control of functional accounts with delegation of administration to CLOs of departments;
   - Improvement in user satisfaction by
     - Fast account updating (account creation within 15 minutes),
     - Enhancement of user communication with the use of emails for notification and confirmation of NetID related events;

   AMS has served its original design objectives well. However, PolyU has been facing the following challenges since 2003 onwards:

   - PolyU’s organizational structure and the user /group provisioning policies have undergone several major changes and they have become so complex that could not be efficiently and effectively handled in AMS.
   - Departments have been requesting for secure central authentication service on their self-developed applications for the wider University communities so that the internal development efforts could be reduced by decoupling authentication and user management modules to central IAM components. They can then focus on the business logic,
   - The requirements for addressing information security issues have gradually increased that could not be fully addressed in AMS.

   In the mean time, IAM industry standards (e.g. Liberty Alliance standards) have become mature. Furthermore, standard-compliant IAM products with strong workflow engine and
rich functionalities have emerged. ITS engaged an external consultant to conduct a comprehensive IAM consultancy study for PolyU in 2005.

3. What is the scope and objectives of the IAM consultancy study?

In 2005, PolyU engaged an external consultant to conduct a comprehensive IAM consultancy study for the University in 2005.

The objectives of the IAM Consultancy study were:

- To review existing PolyU IAM practices.
- To identify PolyU IAM requirements.
- To recommend future IAM Framework & Infrastructure (F & I) for PolyU in accordance with the identified requirements.
- To recommend implementation roadmap for the proposed IAM F&I.
- To describe benefits and costs analysis of the proposed IAM F&I.
- To identify training requirements for PolyU staff.
- To provide integration approaches for existing and new PolyU applications and systems.

The objectives of the new IAM F&I were:

- To extend or replace the current IAM F&I of PolyU managing all existing identities with different SLAs and extend to cover upcoming identities in an effective manner to support other departments, more services and users.
- To provide IAM functions available in the new IAM F&I for new developed systems / applications so that significant development and support costs in user authentication and authorization can be reduced.
- To provide means to let existing systems / applications externalize their IAM functions to the new IAM F&I in phases with minimum interruption to existing environment.

The final consultancy report was accepted in Dec 2005.

4. What is the Reference Architecture for PolyU’s IAM Framework & Infrastructure?
The above diagram illustrates the Reference Architecture for PolyU’s IAM F & I which was recommended by the consultant in the IAM Consultancy Report in 2005. The diagram illustrates the relationship of the functional components of the IAM Infrastructure. It can be visualized from left to right representing users coming into the system and attempting to access resources and applications. The middle portion of the diagram shows the relationship in among components in the four major IAM areas including Authentication, Authorization, User Management, and Central User Repository. The areas are shaded in ‘red’, ‘yellow’, ‘green’ and ‘blue’ colors respectively.

Note that some components in one area may be closely coupled with components in the other areas. For example, Role Management is in the User Management area but it is also being considered as a critical component enabling the Authorization service. The ‘IAM Components’ diagram below subdivides each IAM area into individual components.
5. What is the implementation plan of PolyU’s IAM Framework & Infrastructure?

Based on the recommendations in the IAM consultancy report, PolyU raised a tender on the implementation of PolyU’s IAM F & I in late 2007. The project has started in early 2008. The implementation is divided into five phases.

Phase 1 of the project covers the implementation of PolyU’s IAM Infrastructure (with the code name of ‘PUsecure’) and its Single Sign-On (PUsecure-SSO) service to two pilot systems: Intranet Web Server (www2) and University Portal (myPolyU). It is targeted to be completed by end of July 2010.

As of July 2010, we are reviewing the business requirements so that we can revise the implementation plan of subsequent phases to address them accordingly. We will update the progress of the project in future issues of Get Connected.