Introduction to Identity Management in Educational Institutions

Anthony K. Kimani – Systems Administrator, KENET

What is Identity and Access Management?

IAM is the framework for managing digital identities (who users are) and controlling access (what they can do) across systems

Core Goal: Ensure the right people access the right resources, at the right time, for the right reasons - securely and efficiently

Why Identity and Access Management (IAM) in Educational Institutions

Security/Protect sensitive data: student records, staff info

Compliance: Meet data protection regulations

Efficiency: Streamline user lifecycle management

User Experience/Unified access: Single sign-on for multiple services (e.g Students Portal, ERP, Email, LMS, Eduroam))

Reduce IT support overhead

Core Components of an IAM System:

- **Central Directory/Identity Store**
  A single system (e.g., LDAP, AD) storing canonical user identities

- **Authentication Mechanisms**
  Passwords, multi-factor authentication (MFA), single sign-on (SSO)

- **Authorization/Access Control**
  Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC)

- **User Lifecycle/Provisioning**
  Onboarding, updating, offboarding users across systems

- **Audit/Logging/Accountability**
  Tracking who accessed what, when, for forensic, compliance, and security

Identity Lifecycle Management

- **Onboarding: Creating identities for new students/staff**

- **Management:** Updating information and managing roles (e.g., student → alumni).

- **Access Control:** Defining who can access which systems.

- **Offboarding:** Deactivating accounts after exit.

Authentication & Authorization Overview

- **Authentication:** Verifying who you are (passwords, MFA, biometrics).

- **Authorization:** Determining what you can do after login.

Example: A lecturer (**authenticated**) can grade exams (**authorized**) but not modify financial records.

Benefits of Centralized Identity Management

- Single identity for all institutional services (SSO).

- Reduced admin workload and faster onboarding.

- Improved user experience and fewer password resets.

- Enhanced security and compliance (account lifecycle visibility).

- Foundation for Federated Identity (RAFIKI, eduGAIN).

IAM Technologies in Practice

- **Directories:** LDAP, Active Directory, FreeIPA, OpenLDAP.

- **SSO Platforms:** Shibboleth, SimpleSAMLphp, Keycloak.

- **Provisioning:** SCIM, automated scripts, connectors to ERPs.

- **Authentication Enhancements:** MFA, Passwordless (FIDO2, WebAuthn).

IAM Governance and Policies

Define clear **ownership**: who manages identities (IT, HR, Registrar).

Establish **policies**: password strength, account expiry, approval workflows.

Define **roles and attributes**: student, lecturer, staff, alumni, guest.

Periodic **audits** and **reviews** to maintain data accuracy.

Thank You

www.kenet.or.ke

Jomo Kenyatta Memorial
Library, University of Nairobi
P. O Box 30244-00100, Nairobi.
0732 150 500 / 0703 044 500