kenet
Kenya Education Network

Future of Identity and Trust in Education

Anthony K. Kimani – Systems Administrator, KENET

Transforming Learning, Research and Working Environments using ICT

The Identity Management Landscape

Existing Fragmented Systems:

- No Central Identity infrastructure
- Dispersed user data across multiple systems

Resulting Operational Challenges:

- Security vulnerabilities from inconsistent practices across departments
- User experience friction – multiple logins for different systems
- High administrative overhead – manual account management
- Difficulty maintaining standards across the institution

Emerging Trends Shaping Education Identity

Global Trends Influencing Kenyan Institutions:

- **Biometric authentication** becoming mainstream in security
- **Decentralized identity** leveraging blockchain technology
- **Zero-trust architecture** replacing traditional perimeter security
- **Federated identity** enabling cross-institutional collaboration

These trends collectively address current challenges while preparing institutions for future demands.

Emerging Trends Shaping Education Identity

Key Drivers of Change:

- **Rising cybersecurity threats** - Education sector attacks increased in the recent years
- **Remote learning expansion** requiring cloud-based access solutions
- **Growing privacy concerns**
- **Digital transformation acceleration** across educational ecosystems

Multi-Factor, Biometric & Passwordless Authentication

Move beyond passwords – adoption of MFA, passkeys, and FIDO2 standards for strong, phishing-resistant authentication.

Passwordless logins: Use biometrics (fingerprint, face, voice), device-bound passkeys, or security keys (e.g., FIDO2) for seamless access.

Biometrics increasingly adopted for authentication, attendance, and access control.

Multi-Factor, Biometric & Passwordless Authentication

MFA methods:

- OTP (SMS/app), push notifications, biometric second-factor, hardware tokens.
- Adaptive/risk-based MFA—require additional proof for higher risk logins or unrecognized devices.

Benefits: Contactless convenience, robust security, reduced truancy(improve attendance), streamlined reporting, inclusion for remote/disabled learners

Decentralized Identity (DID) and Verifiable Credentials (VCs)

What is Decentralized Identity?

A framework that gives individuals true control over their digital identities without relying on central authorities.

Self-Sovereign Identity (SSI) “shifts control from institutions to individuals” using decentralized identifiers (DIDs).

Decentralized Identity (DID) and Verifiable Credentials (VCs)

Core Components:

- **Decentralized Identifiers (DIDs)** – User-controlled unique identifiers. ***Who you are***

- **Verifiable Credentials (VCs)** – Tamper-proof digital credentials/documents that makes a cryptographically verifiable claim about the DID subject. ***What you know or own***

- **Digital Wallets** – Secure storage on user devices

- **Blockchain/Distributed Ledger** – Tamper-resistant, Permanent; no shingle point of failure

Decentralized Identity (DID) and Verifiable Credentials (VCs)

How It Operates and Principal roles:

1. **Issuer:** Entity, such as a university, that creates and issues the credentials
2. **Holders:** The individual who stores the VC securely in their digital identity wallet.
3. **Verifiers:** Entities, such as an employer or another academic institution, who check the validity of the VC when presented.

Decentralized Identity (DID) and Verifiable Credentials (VCs)

Practical Education Applications:

- **Digital degrees and certificates** – Instantly verifiable by employers
- **Lifelong learning records** – Portable across institutions
- **Secure students transfers** – Between educational institutions
- **Research collaboration access** – Temporary, recoverable credentials

Cloud-Based Identity and Access Management (IAM) for Remote Learning

Cloud Identity and Access Management (IDaaS) – Institutions centralize account management and SSO in scalable cloud services.

User Identity Database hosted on the cloud (e.g. in Google Workspace, Azure AD, AWS IAM, or open-source solutions Keycloak, Gluu)

Cloud IAM (IDaaS) grows rapidly across Kenyan Educational and Research institutions, driven by increased remote learning and collaborative research demands.

Cloud-Based Identity and Access Management (IAM) for Remote Learning

Core features:

- Central user lifecycle management, SSO across apps, secure provisioning (add/remove users).
- Role-based access, granular permissions.
- Multi-factor and passwordless authentication.

Platforms: Open-source alternatives to AD (e.g., OpenLDAP, Univention, Gluu, FreeIPA), cloud-first directories (e.g., Google Identity, Azure AD, AWS IAM), specialized ERP-integrated products.

Cloud-Based Identity and Access Management (IAM) for Remote Learning

Hybrid IAM Architecture

Maintains a locally-hosted authoritative user database that synchronizes with cloud-based identity providers (Google Workspace, Azure AD, AWS IAM, or open-source)

Zero-Trust Architecture in Education

Built upon the principle of **Never Trust, Always Verify**

Assumes no user or device is trustworthy by default

Core principles:

- Verify explicitly: authenticate & authorize every request based on identity, device, context
- Use least privilege: grant minimal access necessary
- Assume breach: design for compromise, monitor continuously, segment

Zero-Trust Architecture in Education

Why it matters for educational institutions:

- Campus networks are dynamic, hybrid (on-campus, cloud, remote), BYOD heavy
- Research data, student records and cloud services require stronger identity and access controls

Zero-Trust Architecture in Education

Key architecture components for universities:

- Identity & device posture verification before granting access (e.g., integrate IAM with device management).
- Micro-segmentation of services: e.g., separate student portal, research systems, admin systems with fine-grained controls.
- Continuous monitoring, telemetry and adaptive policy enforcement (access changes based on context, risk).

Federated Identity & Trust Frameworks

Key Concept:

Federation connects universities and research institutions so that users can access services across organizations using their home credentials.

Uses standards like **SAML**, **OpenID Connect (OIDC)**, and **LDAP**.

Federated Identity & Trust Frameworks

Global Federation – eduGAIN:

- Connects national federations globally to form a **trust network** for research & education.
- Provides **single sign-on** for global research collaboration.

Kenya – RAFIKI Federation:

- Operated by **KENET**, connects local universities using **SAML.**

Federated Identity & Trust Frameworks

How It Works: The Technical Foundation (Recap)

Standard Protocols Enable Interoperability:

- **SAML / OIDC / LDAP:** Common languages for authentication.

The "Trust Fabric": All members agree to:

- **Common Security Policies (e.g., REFEDS BEs):** A baseline for security and privacy.
- **Metadata Exchanges:** A shared, secure list of trusted institutions and their services.

Key Benefit: Single Sign-On (SSO)

- Log in once with your home institution to access a world of resources.

kenet
Kenya Education Network

Federated Identity & Trust Frameworks

Trust Policies & Metadata:

- Common frameworks like **REFEDS Baseline Expectations (BEs)** define shared security standards.
- Federations exchange metadata to maintain trust and integrity.

Outcome:

- A **trusted digital campus** spanning institutions and countries.
- Access to global research resources (journals, HPC, online courses) using federated login.

AI and Adaptive IAM

Intelligent, Continuous Authentication

- Moves beyond one-time passwords. AI analyses behaviour (typing patterns, access habits) to create a continuous trust score, flagging anomalies in real-time.

Dynamic, Risk-Based Access Control

- Access decisions become context-aware. AI assesses the risk of each request—considering the user, device, and resource sensitivity—to apply the right level of security (e.g., seamless access vs. requiring MFA).

Predictive Threat Defence for Federations

- AI monitors the entire trust network to proactively detect coordinated attacks or compromised members, strengthening security for all participating institutions.

Automated Governance & Ethical Guardrails

- While AI automates user lifecycle management (onboarding/offboarding) and smart policy enforcement, it must be governed by ethical frameworks to prevent bias and ensure transparent, explainable decisions.

kenet
Kenya Education Network

Transforming education through ICT

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