kenet
Kenya Education Network

Federated Identity and Trust

Anthony K. Kimani – Systems Administrator, KENET

Transforming Learning, Research and Working Environments using ICT

What is Federated Identity?

Digital identity linking across multiple independent systems

Single set of credentials to access resources across organizational boundaries

Trust-based framework where identity providers (IdPs) and service providers (SPs) establish secure relationships

Terminologies:

Identity Provider (IdP): Authenticates users and provides identity information

Service Provider (SP): Provides services and trusts the IdP

Federation: Group of organizations with established trust relationships

Trust Framework: Policies and standards governing the federation

The Core Components of Federation

Identity Provider (IdP):

- The system that authenticates the user.
- It retrieves the user’s information in form of attributes.
- It issues a digital token to confirm the user’s identity.

Service Provider (SP):

- The application or service that the user wants to access.
- It trusts the Identity Provider's token to grant access.

What is Trust in Federation?

Trust = Confidence that identity assertions are valid

Built on:

- Shared policies
- Technical standards (SAML, OIDC)
- Metadata exchange

The Core Components of Federation (Contd.)

Federation Operator (The "Trust Broker")

Central entity that manages the trust relationships between the IdPs and SPs.

- Provides the legal, technical, and governance framework.
- Publishes and maintains the **metadata** (like public keys and endpoints) for all members of the federation.
- It also ensures all members comply with the federation's rules and policies.

Authentication at Home IdP

IdP Authentication:

i. User is redirected to home organization’s login page

ii. Standard authentication methods (password, MFA, etc)

iii. IdP creates authentication assertion

Attribute Release & Trust Validation

Critical Trust Decisions:

i. IdP releases required attributes to SP

ii. SP validates signatures against federation metadata

iii. Attribute filtering based on federation policies

Access Granting at SP

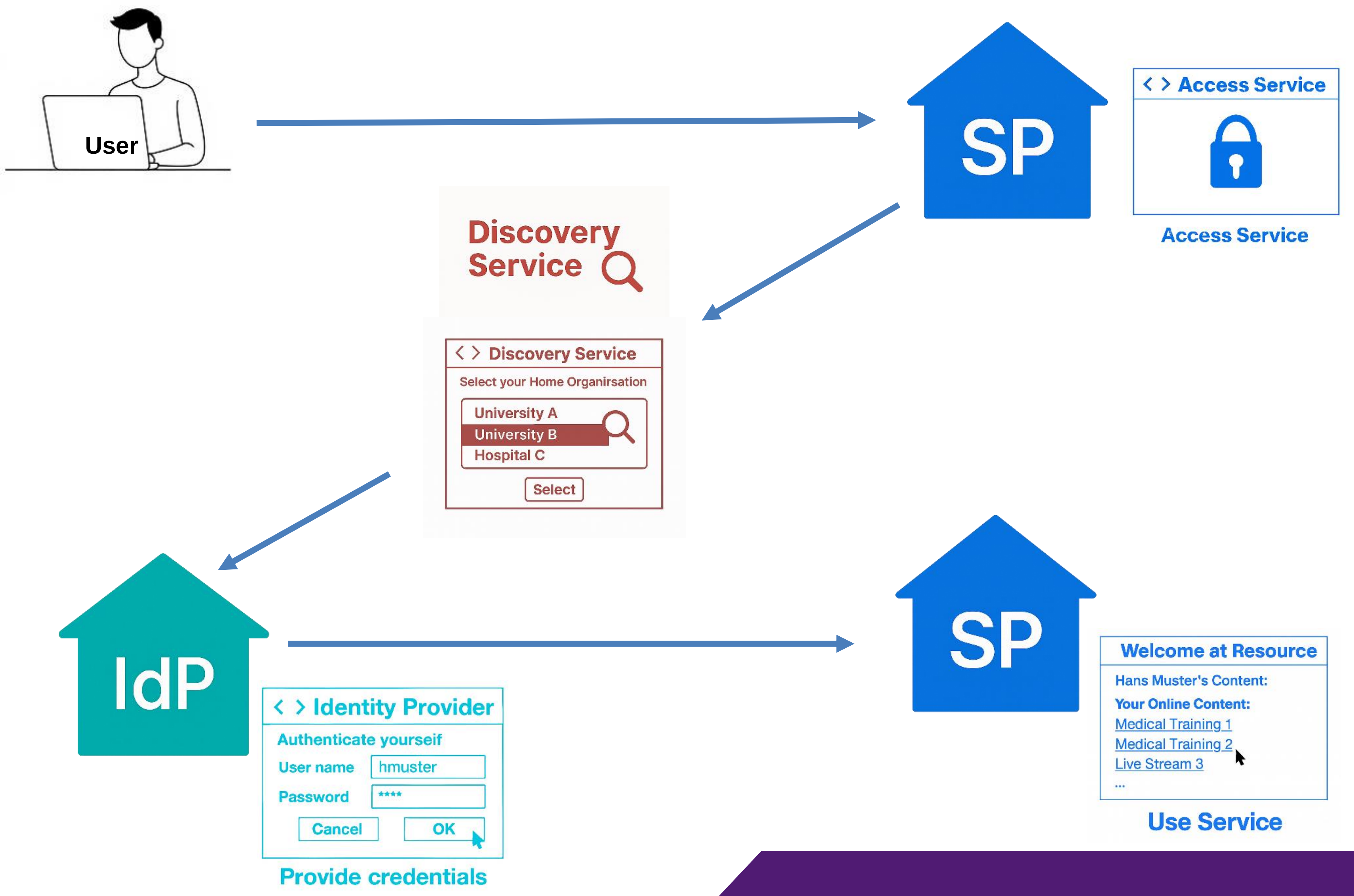
SP Final Authorization:

i. Maps received attributes to local roles/entitlements

ii. Applies access control policies

iii. Creates user session

Authentication Flow



< > Access Service

Access Service

< > Discovery Service

Select your Home Organirsation

University A
University B
Hospital C

Select

< > Identity Provider

Authenticate yourseif

User name: hmuster

Password: ****

Cancel OK

Provide credentials

Welcome at Resource

Hans Muster's Content:

Your Online Content:

Medical Training 1
Medical Training 2
Live Stream 3
...

Use Service

Key Software and Technologies

Identity Providers:

- Shibboleth IdP (most common in eduGAIN)
- SimpleSAMLphp
- ADFS (Microsoft)
- Keycloak

Service Providers:

- Shibboleth SP (Apache/Nginx modules)
- SimpleSAMLphp SP
- Commercial products

Federation Infrastructure:

- MDX (Metadata aggregators)
- COmanage (organization management)
- SATOSA (protocol translation)

Key Benefits for Education and Research:

- **Seamless Access to Global Resources**
  - **Access to Federation** (e.g., eduGAIN, InCommon)
  - **Reduced Friction**, Users avoid creating, managing, and remembering
  - **Access to High-Value Services** (e.g., High-Performance Computing (HPC) resources, e-portfolios, digital library collections)

- **Enhanced Security and Compliance**
  - **Centralized Credential Control**
  - **MFA Enforcement**
  - **Identity Assurance**
  - **Instant De-provisioning**

- **Reduced Administrative and Operational Cost**
  - **Zero Account Creation on External Systems**
  - **Simplified Auditing**, all authentications are logged centrally by the home IdP
  - **Standardized Interoperability**, integration with other academic services is fast, cheap and reliable

RAFIKI

Kenya Identity Federation for Research and Education Federation – RAFIKI

RAFIKI: Kenya's national identity federation.

Part of eduGAIN: An international **interfederation** service interconnecting research and education identity federations.

Enables Kenyan researchers, educators, and students to access global resources securely.

https://rafiki.ke

Interfederation is the process that allows a user from one identity federation to access a service registered in a different federation, enabling cross-border access to online resources.

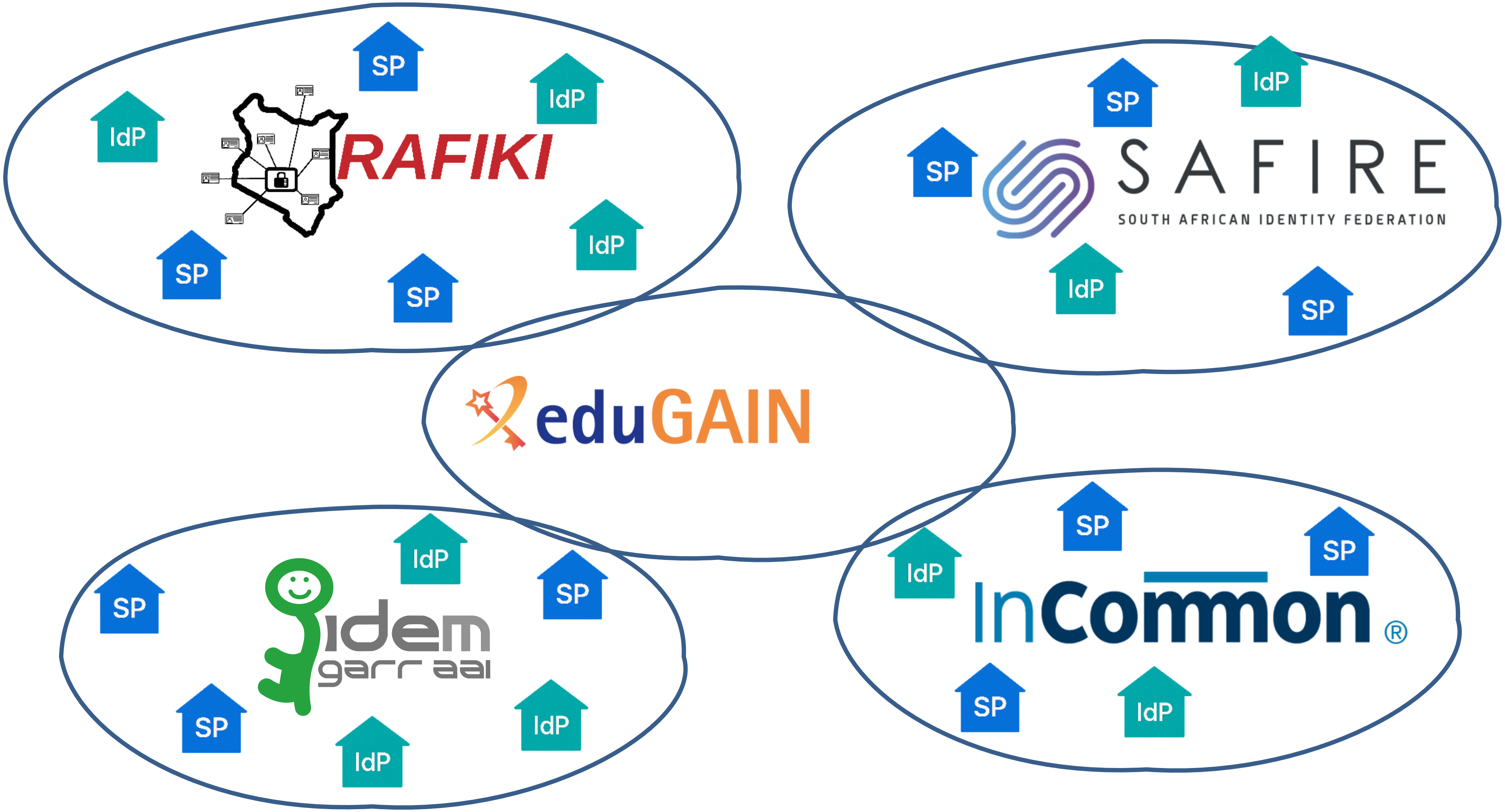
eduGAIN

It is an international **interfederation** service interconnecting **research** and **education** identity **federations**.

eduGAIN solves the **"trust problem"** between national federations

Extends the reach of a single login across international borders.

https://edugain.org


SP
IdP
IdP
RAFIKI
IdP
SP
SP
SP
IdP
SP
SP
SAFIRE
SOUTH AFRICAN IDENTITY FEDERATION
IdP
SP
eduGAIN
IdP
SP
SP
idem
garr aai
SP
IdP
IdP
SP
SP
IdP
InCommon®
SP
IdP

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