kenet
Kenya Education Network

Identity and Access Management, and Trust Services

Transforming learning and working environments using ICT

Outline

- Identity and Access Management
  - What is IAM?
  - Components of IAM
  - Benefits of IAM

- KENET Trust and Federation Services
  - RAFIKI
  - Eduroam

Identity and Access Management

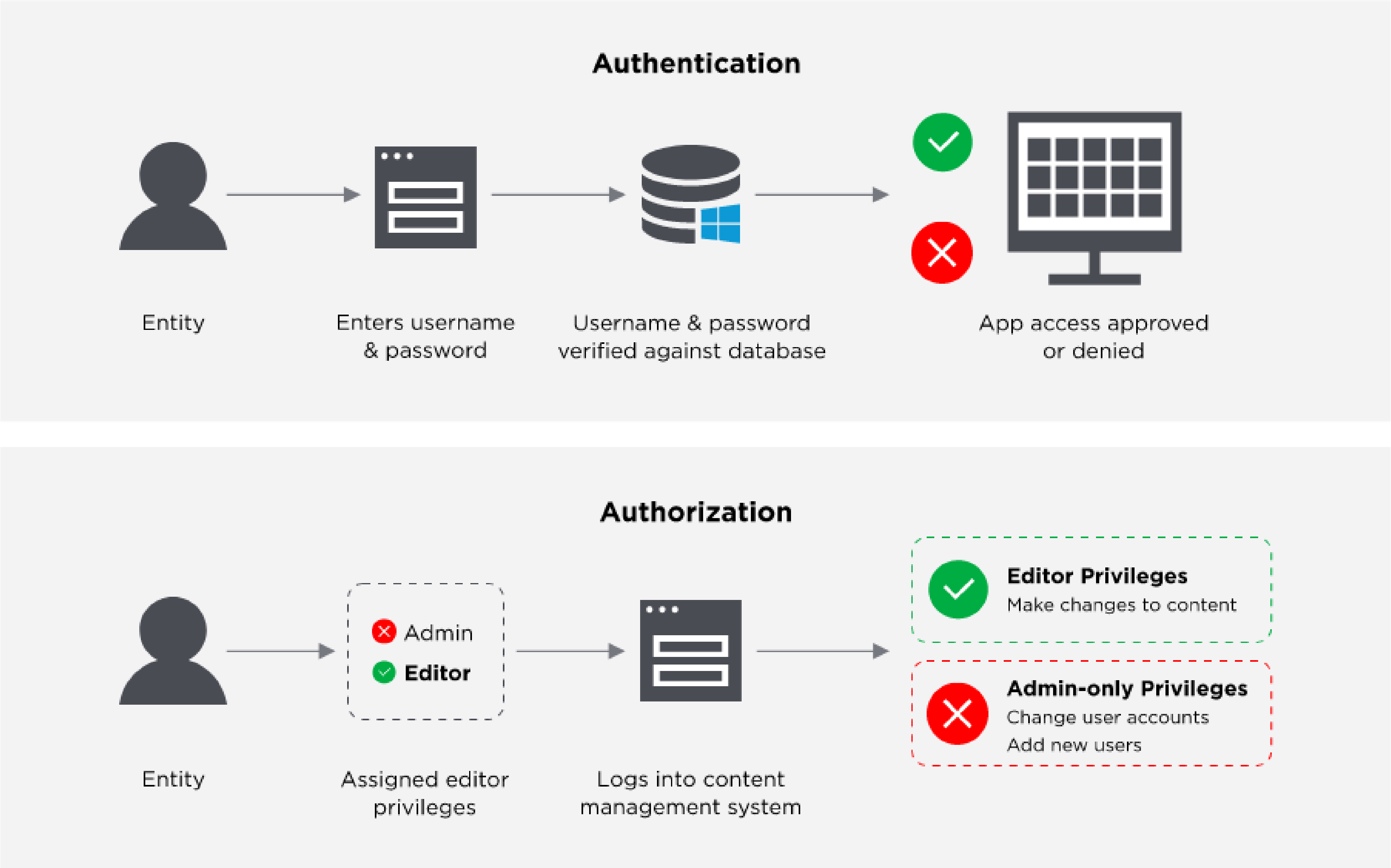
- IAM is a framework for managing user identities and access to resources
- Ensures that only authorized users can access specific resources based on their roles and permissions

Identity and Access Management

Components of IAM

- **Authentication:** Verifying a user’s identity
- **Authorization:** Granting access based on permissions
- **Access Control(User Management):** Enforcing access policies

IAM process…


Authentication
Entity
Enters username & password
Username & password verified against database
App access approved or denied
Authorization
Entity
✗ Admin
✓ Editor
Assigned editor privileges
Logs into content management system
Editor Privileges
Make changes to content
Admin-only Privileges
Change user accounts
Add new users

Identity and Access Management

Benefits of IAM

- **Improved Security:** IAM reduces the risk of unauthorized access by managing user identities and access controls
- **Reduce administrative burden:** IAM automates tasks like user provisioning and deprovisioning
- **Enhanced user experience:** IAM allows users to access multiple resources with a single sign-on, improving convenience
- **Increased compliance:** IAM helps organizations meet regulatory compliance requirements for data security

KENET Identity and Trust Services

- In today's digital world, organizations need to securely manage user identities and access to critical resources. Identity and Access Management (IAM) and Trust/Federation Services, two essential tools for achieving this goal

- IAM helps organizations establish who can access what, while Trust and Federation Services enable secure collaboration between organizations by allowing users to access resources from trusted partners using their existing credentials

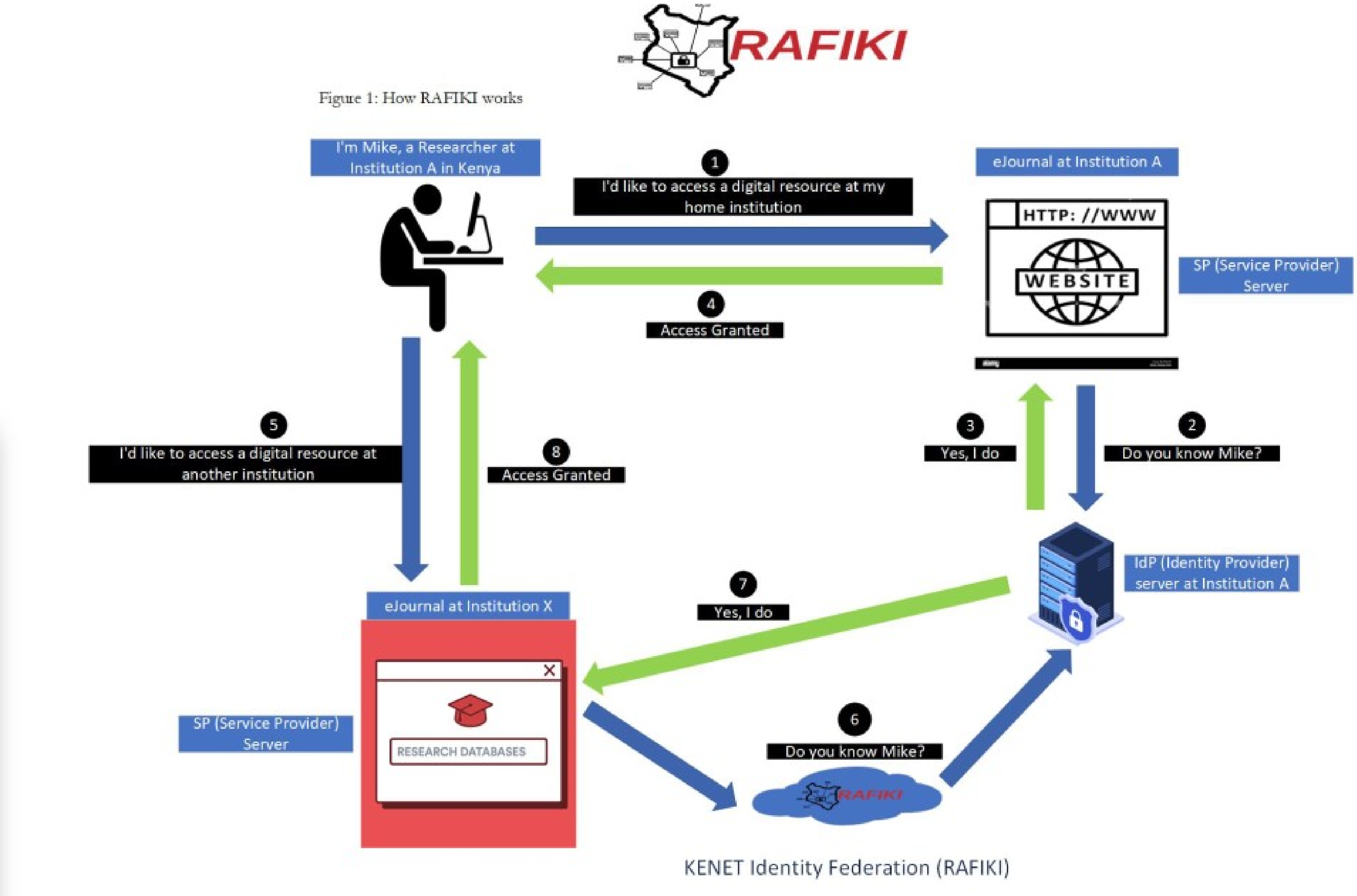
KENET Identity and Trust Services

- KENET promotes research and education collaboration and partnerships at national, regional and global levels.
- Two important services managed by KENET are:
  - Federation – RAFIKI (https://Rafiki.ke)
  - Eduroam

KENET Identity and Trust Services

- The Kenyan Identity Federation for Research and Education is introduced to facilitate and simplify the introduction of shared services across the Federation.
- This is accomplished by using Federation Technologies to extend the scope of a digital identity issued by one Federation Member to be valid across the whole Federation.
- Use of Federated Identity makes collaboration easier and fosters seamless access to research and academic resources.

Figure 1: How RAFIKI works


RAFIKI
I'm Mike, a Researcher at Institution A in Kenya
1
I'd like to access a digital resource at my home institution
eJournal at Institution A
HTTP: //WWW
WEBSITE
SP (Service Provider) Server
4
Access Granted
5
I'd like to access a digital resource at another institution
8
Access Granted
3
Yes, I do
2
Do you know Mike?
IdP (Identity Provider) server at Institution A
7
Yes, I do
eJournal at Institution X
RESEARCH DATABASES
SP (Service Provider) Server
6
Do you know Mike?
RAFIKI
KENET Identity Federation (RAFIKI)

KENET Identity and Trust Services

Terminologies

Identity Provider (IdP)

- An organization that manages a user's digital identity and authenticates users.
- Often the user's primary organization (e.g. university).
- Examples: Google, Microsoft, Universities with their own login systems.

KENET Identity and Trust Services

Terminologies

Service Provider (SP)

- An organization that offers resources (applications, services, data) to users.
- Relies on the IdP to verify user identities and grant access based on authorization policies.
- Examples: ERP, Learning Management Systems (LMS), WebConferencing Platforms

KENET Identity and Trust Services

Technologies Used:

- Commonly used protocols are SAML, OIDC, CAS, Oauth
- Open Source software, for example, Shibboleth, SimpleSAMLphp, KeyCloak

KENET Identity and Trust Services

What will you need to join the federation?

i. Fill and sign the RAFIKI Membership form

ii. A user database, for example, OpenLDAP/LDAP, Active Directory, Microsoft Azure, Googles Gsuite/Workspace

KENET Identity and Trust Services

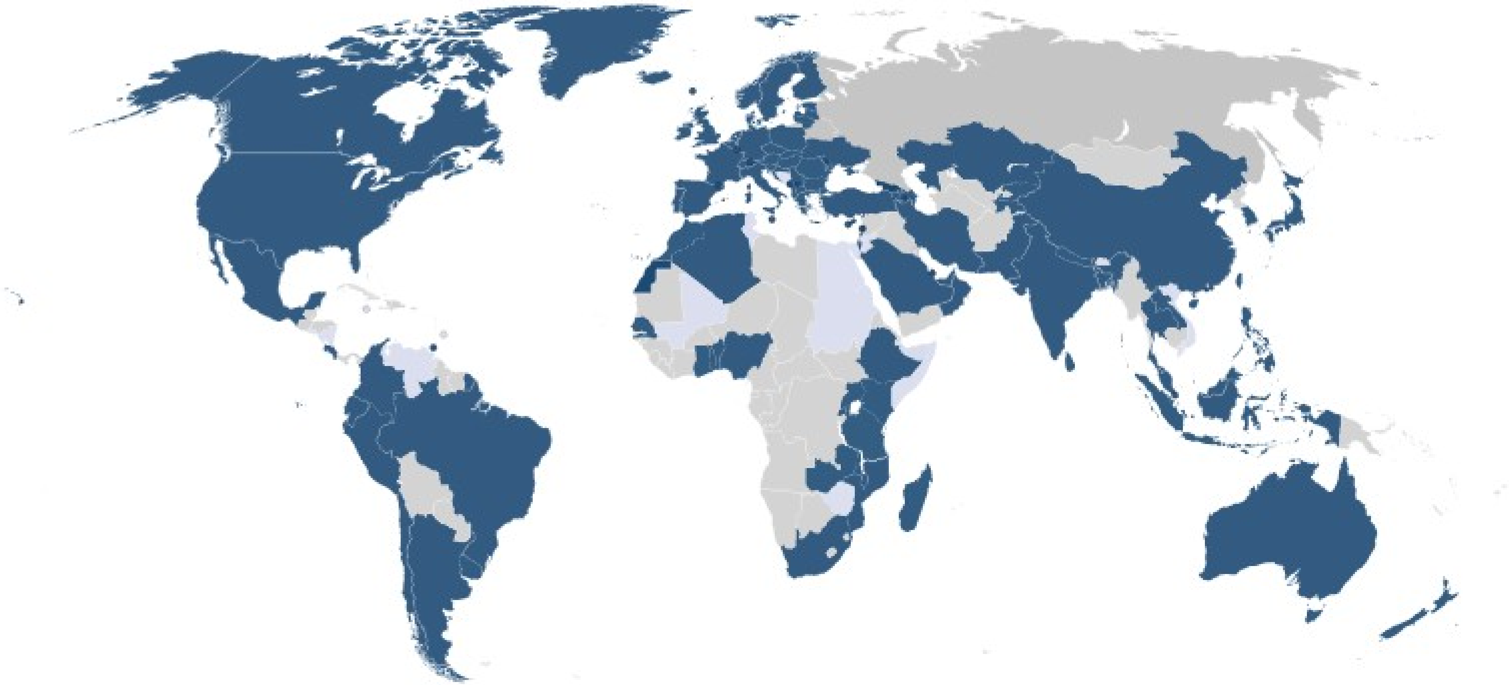
What is eduroam?

eduroam (EDUcation ROAMing) is the secure, world-wide roaming access service developed for the international research and education community

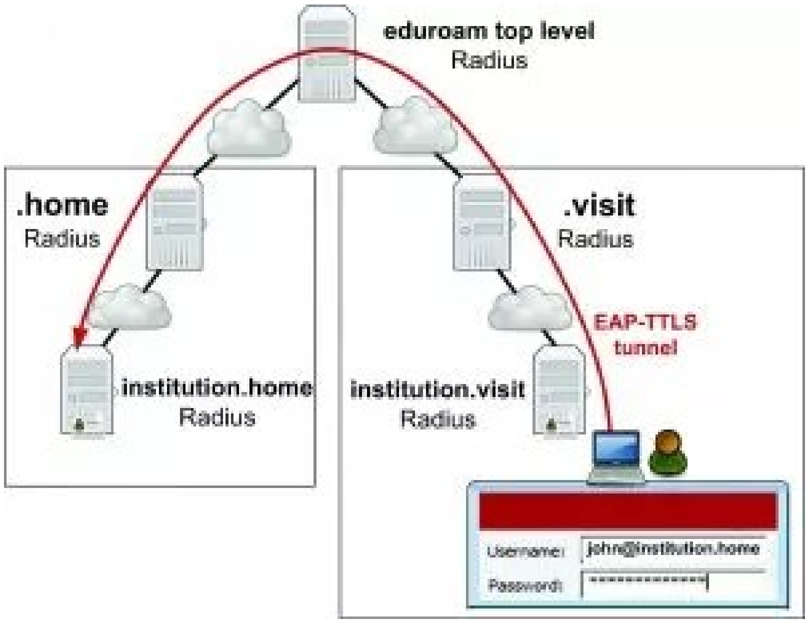
Eduroam is available in thousands of locations across over 100 countries worldwide

KENET Identity and Trust Services

Where can I Eduroam?



KENET Identity and Trust Services



Username: john@institution.home

Password: **************

eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions by simply opening their laptop.

KENET Identity and Trust Services

The user’s home institution is responsible for maintaining and monitoring user information, even when the user is at a guest campus. Thus, this data is not shared with other connected institutions.

QUESTIONS
And
Answers