KENET Certification Authority

Ronald Osure

Applications Developer - KENET

rosure@kenet.or.ke

EUGridPMA Meeting September 8-10 2014, Poznan, Poland

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Agenda

- About Kenya
- About KENET
- Introduction
- KENET CA Re-design
- New Policy and technical details
- CA administration and KENET technical capacity
- Who can apply for a certificate?
- Research programs
- Importance of CA to KENET Community

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

About Kenya

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Governance structure of KENET

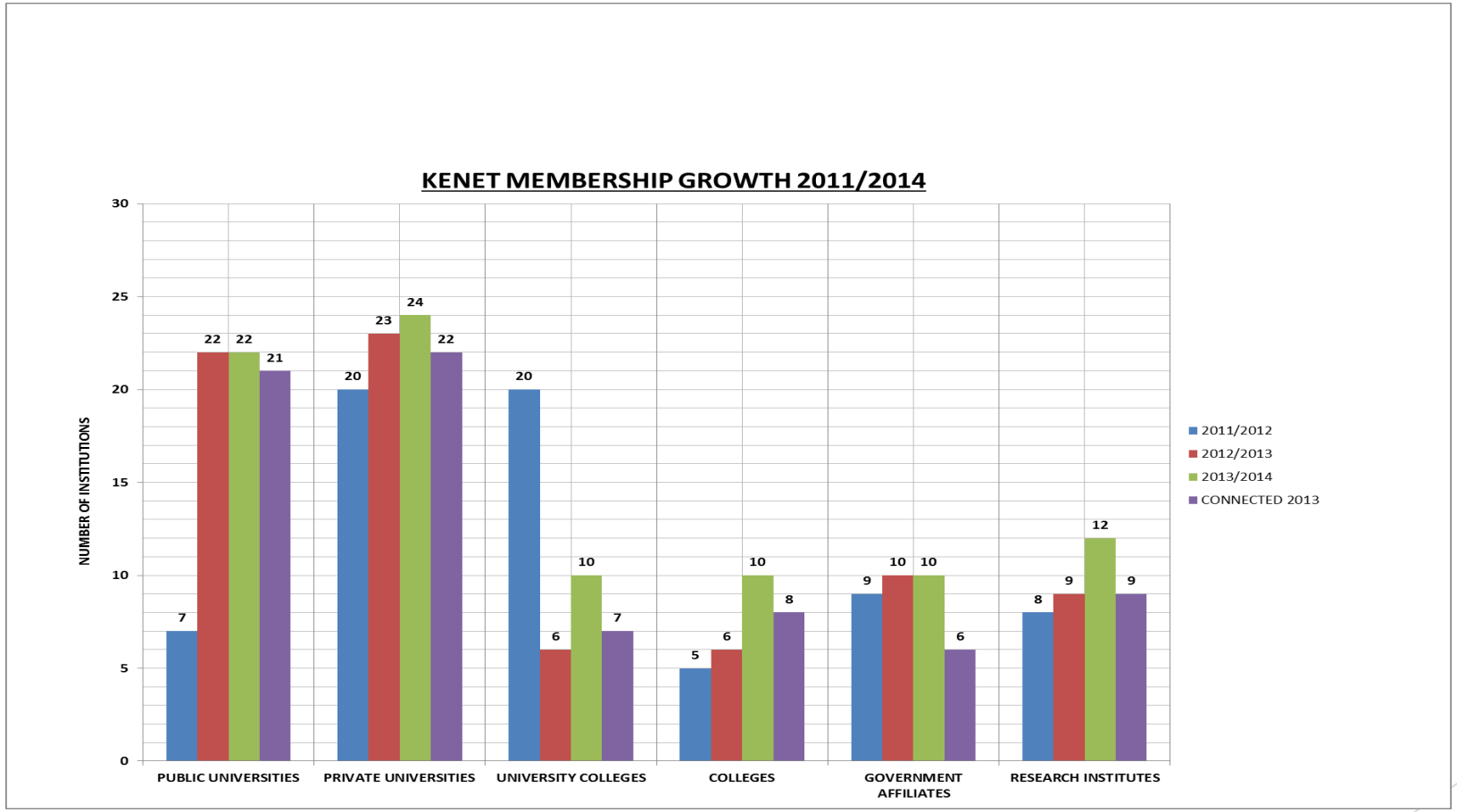
- Strong governance structure with founder members as Trustees. Keeps KENET close to the members , focused on their needs and listening to their problems.
- Recognized as NREN by the government of Kenya

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Members of KENET 2014

(*46 universities + 12 research institutes*)



kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Kenya ICT in Higher Education and ICT Context

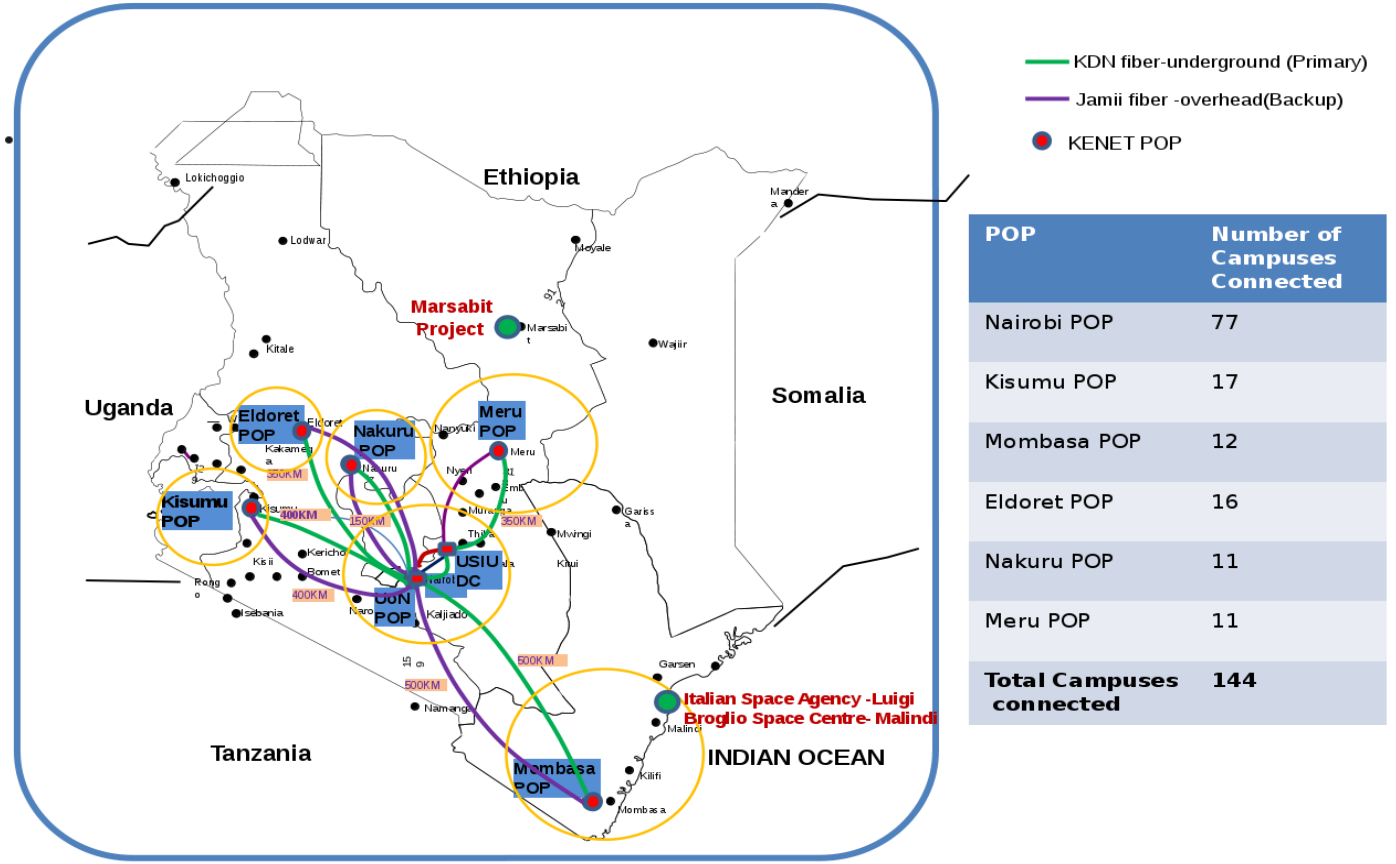
No	Parameter	Dimension
1	Size of Kenya (in Sq. KM)	582,646
2	Population (Millions)	43.18
3	Mobile Subscriptions (Millions)	31.3
4	Mobile Money Transfer Subscriptions (Millions)	21.1
5	Internet Users (Millions)	19.2
6	International Internet Bandwidth Available (Gb/s)	862.8
7	Number of Undersea fiber cables at Kenyan Coast	4

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

KENET Network Coverage March 2014

4.5 gb/s international capacity; 1,000 KM dark fiber



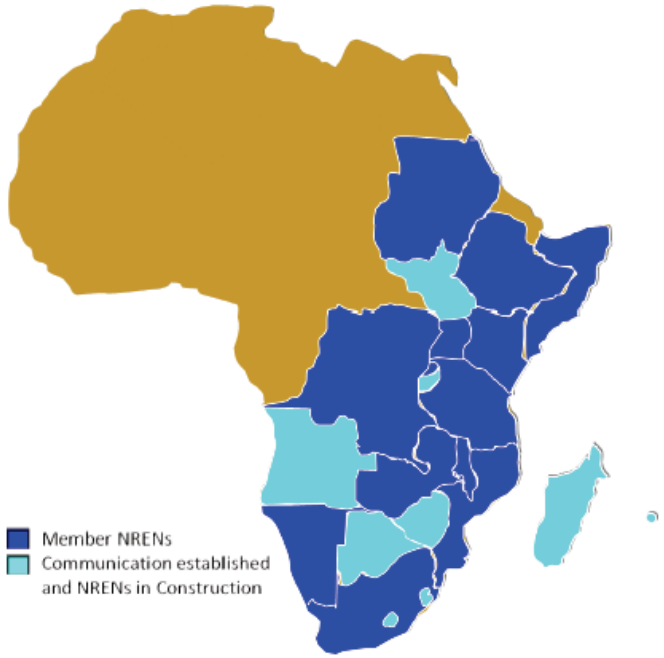
POP	Number of Campuses Connected
Nairobi POP	77
Kisumu POP	17
Mombasa POP	12
Eldoret POP	16
Nakuru POP	11
Meru POP	11
Total Campuses connected	**144**

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

UbuntuNet Alliance Regional REN

13 Member NRENs



Eb@le, DRC
EthERNet, Ethiopia
*KENET, Kenya
*MAREN, Malawi
*MoRENet, Mozambique
XNet, Namibia
*RwEdNet, Rwanda
SomaliREN, Somalia
SudREN, Sudan
*TENET, South Africa
TERNET, Tanzania
RENU, Uganda
ZAMREN, Zambia

** = founding member*

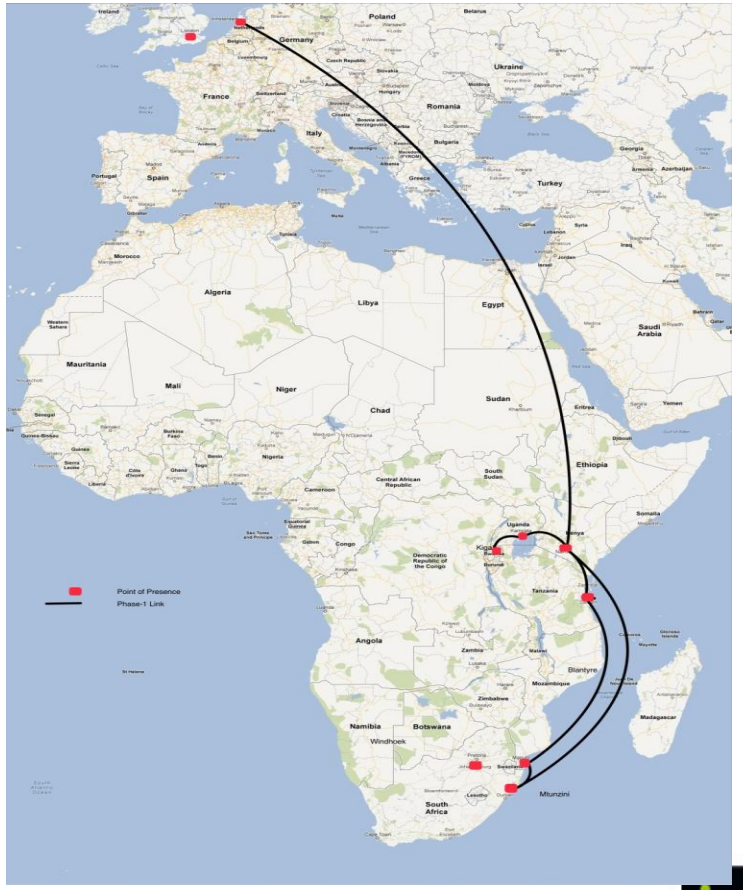
UbuntuNet Alliance

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

AfricaConect Phase 1 Map

- AfricaConnect aims to establish a high capacity internet network for research and education
- Provide gateway to global research collaboration for the South and Eastern Africa region
- http://www.africaconnect.eu



kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

KENET CA highlights

- Start of implementation on 3rd March 2013
- Deployment of CA at KENET starts guided by eI4Africa
- First Presentation in Tartu, Estonia 15/5/2014 (EUGridPMA meeting)
- CP/CPS re-structuring to RFC 3647
- CP/CPS Uploaded for review
- CA Setup re-design
- New setup using EJBCA (ejbca.org)

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

KENET CA Overview

- KENET CA is a self signed root certification authority. It doesn't issue certificates to subordinate CA's
- KENET CA issues certificates to mainly research and higher learning institutions
- KENET CA is an online CA
- HSM not yet procured – in process
- CA system consists of 1 server
  - Repository and signing in one box
- Security implemented as per http://ejbca.org/docs/security.html

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

KENET CA CP/CPS

- Version 1.0.1 – August 2014
- Older version (1.0.0) was structured as per RFC 2527
- New structure for 1.0.1 is RFC 3647
- Object Identifier assigned: 1.3.6.1.4.1.43322.1.1.1.0
- Submitted for review

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

General Provisions

- KENET CA will operate in accordance with all provisions of CP and CPS
- KENET CA operates a secure on-line repository (https://cheti.kenet.or.ke).
- The on-line repository runs with an availability of 24x7, liable to reasonable scheduled maintenance
- Interpretation of CP and CPS is subject to Kenyan Law

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

KENET CA identification and authentication

- The subject name of the applicants shall be compatible to the X.500 standard
- Subscriber name must be meaningful and unique
- Subscriber identified in person by RA (member institution) or KENET
- Re-key before expiration provided the last identification in accordance with section 3.1.9
- Revocation request only through signed emails by owner or as described in section 3.2.3

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Who can apply for a certificate?

- Users affiliated to KENET member organization (Natural Persons)
- Hosts administered by the requesting KENET member and
- Services provided on a host that is administered by a KENET member institution

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Key pair and certificate usage

- Certificate to be used in accordance with section 1.4.1 and 1.4.2
- A certificate may be used for the following purposes:
  - Email signing and encryption
  - Server authentication
  - Authentication purposes in grid and computing infrastructures

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Physical, Procedural & Personnel Security Controls

- CA operates in a controlled environment at KENET University of Nairobi data centre
- Physical access restricted to authorized personnel
- Building under CCTV surveillance
- The building has fire alarm system
- Team of 4 engineers dedicated to managing CA
- All engineers have attended trainings on PKI infrastructure

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Certificate name forms

- Issuer: C=KE, O=KENET, CN=KENET CA
- Users: C=KE O=INSTITUTE, OU=KENET CN=*commonName*
  - commonName must be the full name of the subject
- Hosts: C=KE O=INSTITUTE OU=KENET CN=*commonName*
  - commonName must be the DNS FQDN of the host.
- Services: C=KE O=INSTITUTE OU=KENET CN=*commonName*
  - commonName must be the DNS FQDN of the host.

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Compliance and Audit

- All procedures and processes in accordance with CP/CPS
- Once a year self-assessment to check compliance
- KENET CA accepts to be audited by external CA or relying parties to verify compliance with CP/CPS

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

To-Dos

- Release new version of CP CPS that is compliant with online CA requirements
- Review setup to meet EUGridPMA guidelines for online CAs as explained in http://wiki.eugridpma.org/Main/GuidelinesForOnLineCAs

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Key Challenges and Questions

- Finding a well documented CA software (we have settled on EJBCA)
- Clear separation of Online and Offline in EJBCA?

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

How do we discover researchers?

- Through mailing lists tailored for particular sector e.g health, agriculture
- Through nominations by Institution Vice Chancellors /Principals
- Conferences
- Reputation – researchers approaching KENET

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

International research and doctoral programs in Kenya

- IBM Research Lab
- University partnerships with others abroad
- Research institutions in fields like medical, agriculture, marine

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Importance of CA to KENET Community

- Kenyan researchers can now access the Africa Grid Science Gateway
- KENET members can also deploy grid infrastructures and share
- Streamline business process of members by use of digital certificates

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa

Thank You!

kenet
Kenya Education Network

el4africa.eu
e-Infrastructures for Africa