Ronald Osure

Applications Developer

KENET CA

35th EUGridPMA Meeting, Amsterdam

Agenda

- Background and Introduction
- Online CA Architecture
- Gemalto HSM & EJBCA
- Key Generation Ceremony
- Setup costs
- Challenges
- KENET CA Overview
- Expectations

About Kenya

Rabat
El Djazair (Algiers)
Tunis
TUNESIA
MOROCCO
Tripoli
Cairo
ALGERIA
LIBYA
EGYPT
El-Aaiun
WESTERN SAHARA
MAURITANIA
Nouakchott
MALI
NIGER
CHAD
SUDAN
Asmara
ERITREA
Al-Khartum (Khartum)
Dakar
SENEGAL
Banjul
GAMBIA
Bissau
Niamey
BURKINA FASO
Ouagadougou
Bamako
N'Djamena
DJIBOUTI
Djibouti
GUINEA
BENIN
NIGERIA
Abuja
SOMALIA
Conakry
SIERRA LEONE
Freetown
COTE D'IVOIRE
Yamoussoukro
TOGO
Lome
CENTRAL AFRICAN REP.
Addis Ababa
ETHIOPIA
Monrovia
LIBERIA
GHANA
Accra
Porto Novo
CAMEROON
Jaunde
Bangui
EQUATORIAL GUINEA
Muqdisho (Mogadishu)
KENYA
Nairobi
SAO TOME & PRINCIPE
Labreville
CONGO
DEMOCR. REP. OF THE CONGO
Kampala
RWANDA
Kigali
GABON
Brazzaville
Bujumbura
BURUNDI
SEYCHELLES
Victoria
Kinshasa
Dodama
TANZANIA
Luanda
ATLANTIC
COMOROS
Moroni
ANGOLA
MALAWI
ZAMBIA
Lilongwe
Lusaka
MADAGASCAR
Antananarivo
Harare
NAMIBIA
ZIMBABWE
MOSAMBIK
MAURITIUS
OCEAN
Windhuk
BOTSWANA
Port Louis
Gaborone
Maputo
Johannesburg
Mbabane
SWAZILAND
Lesotho
LESOTHO
SOUTH AFRICA
Cape Town

About 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

Online CA Architecture

Gemalto HSM

- Components
  - Gemalto ID Prime MD 3810 smart card (FIPS 140-2 Level 3)
  - Gemalto ID Bridge K30 (Card Reader)
  - IDGO 800 Minidriver for Ubuntu Linux 12.04

Order of events

- Virtual servers in the beginning (Ei4Africa)
- Migration to physical servers
- Installation of EJBCA (recommendation from DFN)
- EUGridPMA online CA guidelines
- The HSM experience/saga
- Collaboration with NIIF CA (Use Gemalto Token)

Order of events

- Purchase of Gemalto HSM
- Attempt at open source drivers
- IDGo 800 mini driver for Ubuntu Linux 12.04
- Re-installation of OS, EJBCA and configuration
- Installation and configuration of driver appropriately
- Key Generation Ceremony

KENET CA Key Generation Ceremony

- CA Key (2048 bits) securely generated in offline laptop and exported to HSM
- Key is protected by pass phrase
- Copies of the private key backed up in offline medium

Setup Costs

- CA Server → $2,500
- VA Server → $2,500
- HSM bundle → $760
- Offline Laptop → $700
- Total → $6,460

Challenges

- Splitting of CA
- HSM integration

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
- CA system consists of 2 servers
  - 'Offline' CA signing server
  - Public repository / Validation Authority

KENET CA CP/CPS

- Version 1.0.1 – June 2nd 2015
- Structured as per RFC 3647
- Under review

KENET CA General Provisions

- KENET CA will operate in accordance with all provisions of CP and CPS
- KENET CA operates a secure on-line repository (https://ca.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 CA Name Forms

- **Issuer**: DC=ke, DC=kenet, O=Kenya Education Network Trust, OU=Research Services, CN=KENET CA
- **Subject (users)**: dc=ke, dc=kenet, O=INSTITUTE, OU=INSTITUTE DEPT/UNIT, CN=*commonName*
- **Subject (Hosts)**: dc=ke, dc=kenet, O=INSTITUTE, OU=INSTITUTE DEPT/UNIT, CN=*commonName*
- **Subject (services)**: dc=ke, dc=kenet, O=INSTITUTE, OU=INSTITUTE DEPT/UNIT, CN=*commonName*

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
- Both servers (including HSM) running off the same cabinet

Expectations

- Added value to our R&E network
- Transform and improve research

Questions

rosure@kenet.or.ke