Nigeria Computer Society 11th International Conference
Theme: e-Government & National Security
24th – 26th July, 2013

Public Key Infrastructure

Taofeeq Olatinwo
Harmony Worldwide Inc.
www.harmonycanada.com
www.hwwgs.com

25th July 2013

Table of Contents

Introduction

- Nigeria's economy is growing fast resulting in:
  - growing middle class, and more reliance on technology and the internet.
    - Nigeria is expected to support 70 million internet users by 2015, up from just 45 million today.
  - Increase in cyber crime, as more and more citizens connect to the internet and the web using smart phones, high capacity 3G and 4G cellular networks.

- Internet penetration is far lower in Africa- just 29% in Nigeria and 14% in South Africa, compared to 78% in the United States of America (USA).
  - From internetworldstats in October 2012, Security Intelligence Report

- But, Nigeria is reputed to be one of the leading cyber crime perpetrators in the world.

- In addition, Nigeria is susceptible to Cyber Espionage.

History of PKI

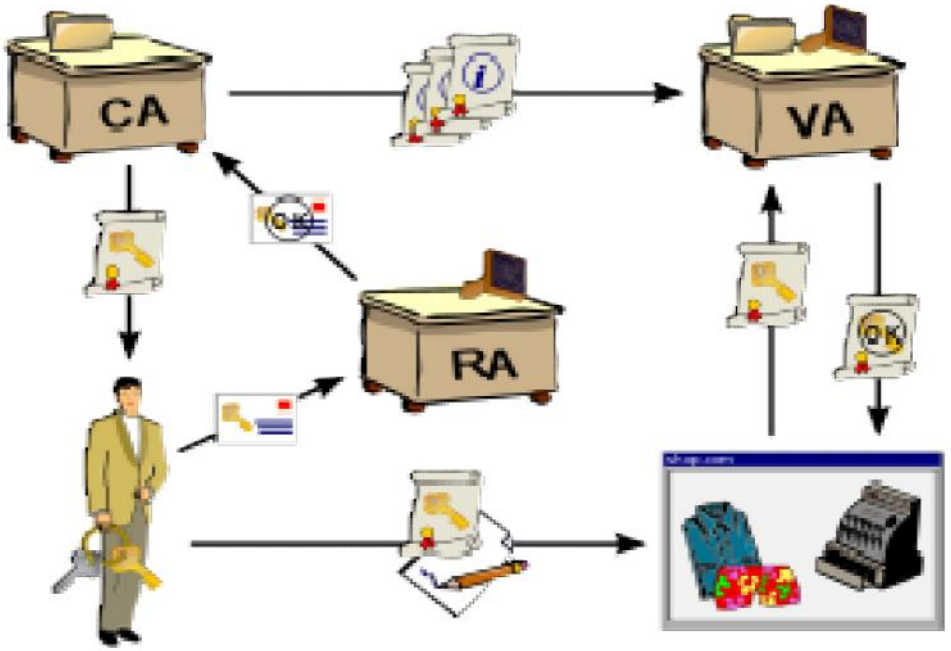
The public disclosure of both secure key exchange and asymmetric key algorithms in 1976 by Diffie, Hellman, Rivest, Shamir, and Adleman changed secure communications entirely. This has been influenced further by:

- development of high speed digital electronic communications (the Internet and its predecessors),
- a need to know which users could securely communicate with each other, and
- for users to be sure with whom they were actually interacting.

What is PKI?

- A **public-key infrastructure** (**PKI**) is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.

  - From Wikipedia



CA – Certificate Authority
VA – Validation Authority
RA – Registration Authority

Benefits of PKI

- Creates digital signatures detailing the information about a specific transaction in order to forestall electronic transaction crimes.
- Confirms or authenticate people or parties involved in the transaction
- Reduces or eliminates outrageous claims and legal tussles resulting from financial transactions
- Helps in ensuring confidentiality of data or information

PKI Areas of Application

- Online/mobile banking
- Online tax filing
- Land records
- Health
- Education
- e-procurement
- Import/export community/customs
- Online line vat returns
- Police
- Defense
- Judiciary details
- Government Press Releases
- Document management system

What's Going On in Nigeria?

- e-Government initiatives
- ePassport – Immigration Application
- ASYCUDA – Customs Application
- Federal Government Web Portals
- State Government Web Portals
- Banks – Online transactions (Cashless policy)
- PKI Blueprint (NITDA)
- National Security Bill (Draft)
- etc

Challenges

- Adoption of Public Key Infrastructure (PKI) was initially
  - complex
  - costly
  - difficult to deploy and
  - time-consuming to maintain.

- Security is a chain; it is only as strong as the weakest link. The security of any CA-based system is based on many links, and they are not all cryptographic.

- People are involved.

Mitigating the Issues & Risks

- **Cost:** Use PPP to develop a business model for KPI implementation
- **Complex:** Engage IT Security & Project Management Professionals to implement
- **Time:** Be proactive by starting early and be focused
- **People:**
  - Change Management through transition and transformation
  - Develop a clear policy with metrics to measure performance and incorporate reward and consequence management

Some Examples

- Banks in Nigeria
- Government of Ontario, Canada
- Government of Saskatchewan, Canada
- Government of Michigan, USA
- University of Chicago Medical Centre, IL, USA
- Multi-National Enterprises
  - Shell, HP, Microsoft, IBM, SAP, etc
- USA Defense Information Systems Agency (DISA) - Common Access Cards program (considered the largest PKI implementation to date)

Overall, PKI has had the most success in government implementations

Recommendation

In our goal to attain vision 2020, the Government needs to take advantage of PKI to curb Cybercrime and improve our image .

- Approve the PKI Blueprint developed by NITDA and start the implementation for all e-Government systems
- Continue and complete the establishment of a fully functional national digital forensic laboratory in the office of the NSA
- Work with IT professionals, investors and entrepreneurs to develop a sustainable and secure platform for cyber accessibility, secured transaction and credible identity
- Establish steps to protect all critical information infrastructure and secure computer systems and networks in Nigeria
- Ensure adequate provision of Project Management, Transition and Transformation Management; and Sustainment

Conclusion

In conclusion, PKI

- provides an increased level of confidence in exchange of information
- is a network security that is essential in both public and private sectors entering the digital domain.
- is only as valuable as the policies, standards and practices that control the issuance of certificates
- robust identity management will help to protect our information, reduce Cybercrime and improve the image of Nigeria

Be proactive, start – NOW!!!

Last Words!

Thank you for listening attentively!!!

Taofeeq Olatinwo
Harmony Worldwide Inc.
www.harmonycanada.com
www.hwwgs.com

25th July 2013

Backup Slides

PKI Implementation - 1

- Complex grouping of security tools
- Roll out digital certificates to users (including employees, partners, and even customers) and then validate those certificates.
- Users need smart cards/keys/tokens, which require smart card readers/USB /Web services to access PKI applications

PKI Implementation - 2

- identifying the enterprise need for developing it,
- selecting the best technology and supporting infrastructure,
- writing governing policies,
- installing and testing the CA and supporting infrastructure for functionality,
- training administrative personnel and end users, and
- generating public/private CA signing keys and associated CA public key certificates.

Business Model

- Certificates provide an attractive business model. They cost almost nothing to make; and
- if you can convince someone to buy a certificate each year for $5, that times the population of the Internet is a big yearly income.
- If you can convince someone to purchase a private CA and pay you a fee for every certificate he issues, you are also in good shape.
- It is no wonder so many companies are trying to cash in on this potential market.
- With that much money at stake, it is also no wonder that PKI vendors produce almost all the literature and lobbying on the subject.

Methods of certification

Certificate Authorities (CA)

- CA digitally signs and publishes the public key bound to a given user
- CA that is third party separate from the user and the system is called the Registration Authority (RA)
- VA provides information on unique user identity within each CA domain
  - Temporary certificates & single sign-on

Web of trust

- Uses self-signed certificates and third party attestations of those certificates
  - PrettyGoodPrivacy, PGP
  - GnuPG

Simple public-key infrastructure

- *key* is what is trusted. Does not associate users with person