



AF- CYBERSEC 2008

Public Key Infrastructure (PKI)

November 17, 2008



Imo Ukpong

Agenda

- Introduction
- PKI Overview
- Why implement PKI?
- Uses and Benefits of PKI
- PKI Framework
- PKI Challenges
- Conclusion
- Q&A

Agenda

Introduction

Introduction

- **Apace Innovative Solutions** – a technology consulting and system integration startup firm providing innovative solutions, services and capabilities that address current and future needs of organizations
- **Contact Details**

Imo Ukpong

(Managing Partner)

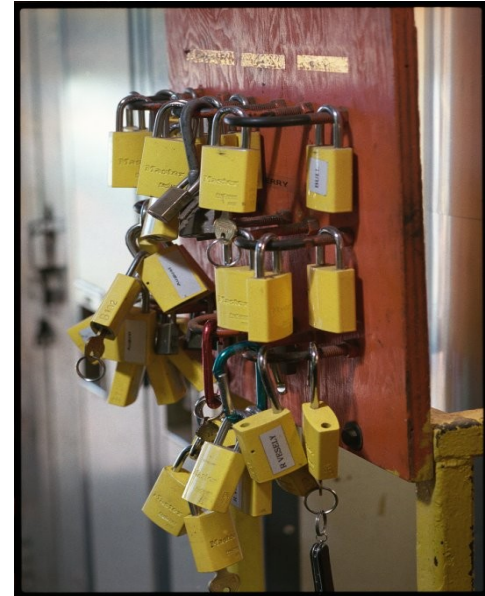
Mobile: +234 802 314 6080

Website: www.apace.com.ng

E-mail: imo@apace.com.ng

Agenda

PKI Overview



PKI Overview

- Public Key Infrastructure (PKI)
 - a foundation on which other applications, system, and network security components are built
 - keys and digital certificates used to address data access and communication issues
 - an essential component of a security strategy
 - Standards-based - example IETF X.509
 - Environment-specific

PKI Overview Cont'd

PKI supports security mechanisms such as

- Confidentiality: secrecy and privacy of data is provided with encryption mechanisms
- Integrity: data cannot be corrupted or modified and transactions cannot be altered
- Authentication: identity of entities is provided by the use of public key certificates and digital signature envelopes
- Non-repudiation: ensuring that data cannot be renounced or a transaction denied

to create a trusted environment for online transactions

Agenda

Why Implement PKI?

Why Implement PKI?

- Widespread deployment of e-government solutions to improve service delivery and interaction between G2G, G2B, G2C communities and therefore need for secure e-mail, cross-institutional use of secure web servers / databases, access control, etc
- To encourage online transactions, stakeholders (businesses, agencies, citizens, etc) must be assured of trust value
- To provide mechanisms to ensure trusted relationships are established and maintained

Why Implement PKI – Policy ?

- **US Federal PKI Technical Working Group**
A Subcommittee of the Federal Public Key Infrastructure Steering Committee
- ***Federal Public Key Infrastructure Policy Authority, or the***
- ***Federal Identity Credentialing Committee.***
- Solve a challenge: Provide users with new capabilities that help them to get their jobs done, not just PKI certificates

Why Implement PKI - Law?

- US Paperwork Reduction Act of 1998 – provide electronic services by Oct 21, 2003; no PKI mentioned
- Single Root US Fed KPI proposed : Issues raised –
 - Privacy advocates – challenge to individual privacy Vs European strong privacy protection laws
 - US Postal Service – early adopter of US Fed PKI - saw first class mails decline, thus raising concerns
 - Single root Fed PKI run by a single agency cannot satisfy other agencies
 - Single Fed PKI a vendor concern as it happened in Canada – violation of anti-competition laws
 - Costs – why not PIN-password option as (in ATM, Network, ISP logon) compared with expensive PKI-based security?

Why Implement PKI - Law?

- **The Federal Bridge Certification Authority**

- Political and technical solution – a consolidated PKI infrastructure consisting of discrete Federal Agency PKIs
- Interoperating through a *non-hierarchical* Bridge certification authority (or CA).
- Known as the Federal Bridge CA and following a hub-and-spoke model, it sits at the center of the U.S. Federal PKI design architecture.
- It has been created using commercial, off-the-shelf products with some special code written to allow different CA products to cross-certify and interoperate within the “membrane” of the Bridge CA.
- The Federal Bridge CA does not operate as a root. It does not issue certificates to subordinate CAs or relying parties.
- Rather, it exchanges a pair of cross-certificates with each participating Federal Agency CA. It has been designed to create trust paths among the individual Federal Agency PKIs.

Why Implement PKI – Some PKI Development efforts in Africa

- South Africa (Private Sector : Thawte, SACA,)
- Tunisia (ANCE)
- Egypt (ITIDA)
- Mauritius (ICT authority CCA)
- The African PKI Forum
- Challenges faced by most African countries:
 - Policy Requirements
 - Legal and Regulatory Requirements
 - Infrastructural Challenges
 - Skilled Resources

Why Implement PKI – African Country Examples

Tunisia

- (ANCE – National Commission for Electronic Commerce and Electronic Exchanges 1997)
- Ecommerce and Electronic Exchanges Law, Aug 2000
- National Digital Certification Authority (root CA; Jan 2001, controller of CAs and cross certification with foreign CAs)

Why Implement PKI – African Country Examples

- **Egypt**
- E-signature Law, April 2004
- E-signature regulatory authority: ITIDA – Information Technology Industry Development Agency, who is the root CA and controller for Egypt CA / responsible for cross certification with foreign CAs

Why Implement PKI – African Country Examples

- **South Africa**
- Electronic Communications and Transactions Act, Aug 2002
- Led by private sector (Thawte – a CA for X.509 certification – an ITU-T standard for PKI, etc)

Agenda

Uses and Benefits of PKI

Uses and Benefits of PKI

- Some typical applications are e-mails, chip card applications (GMPC), online value exchange (debit / credit cards), Voting, Students ID, Citizen ID systems (Passports, Driver's licence), Ticketing, etc
- Forms part of the overall data and information security strategy to provide the comfort and confidence to move from face-to-face systems and transactions to the online arena
- Identity Assurance – it allows for identification of entities

Uses and Benefits of PKI Cont'd

- Reduces risk
- Reduces transactional processing expenses
- Enhances efficiency and performance of systems and networks
- Reduces the complexity of security systems
- Allows distribution and use of security mechanisms – keys and certificates – with integrity

Agenda

PKI Framework

PKI Framework

- Consists of
 - security and operational policies
 - security services
 - interoperability protocols supporting the use of public-key cryptography for the management of keys and certificates.
- Enables and supports secured exchange of data, credentials, and value (such as monetary instruments) in various environments that are typically insecure

PKI Framework Cont'd

- The generation, distribution, and management of public keys and associated certificates occur through the use of Certification Authorities (CAs), Registration Authorities (RAs), and Directory Services, which can be used to establish a hierarchy of trust
- The CA provides this trust relationship between the entities

PKI Framework Cont'd

Certificate Authority functions as follows:

- Entities that are unknown to one another, each individually establish a trust relationship with a CA.
- The CA performs some level of entity authentication, according to its established rules as noted in its Certificate Practices Statement (CPS), and then issues each individual a digital certificate
- That certificate is signed by the CA and thus vouches for the identity of the entities
- The unknown individuals can now use their certificates to establish trust between themselves because they trust the CA to have performed an appropriate entity authentication irrespective of their network environments

PKI Framework Cont'd

PKIs perform :

- *Public key cryptography* – Includes the generation, distribution, administration, and control of cryptographic keys e.g RSA composite numbers cryptographic system
- *Certificate issuance* – Binds a public-key to an entity, or to data — example an email
- *Certificate validation* – Verifies that a trust relationship or binding exists and that a certificate is still valid for specific operations
- *Certificate revocation* – Cancels a previously issued certificate and publishes the cancellation notice in a timely manner

Agenda

PKI Challenges

PKI Challenges

➤ PKI / cryptographic solution challenges:

- Initial identification / authentication of a user or a remote entity for the first time e.g. National ID issuance without a birth / death registry systems

➤ It requires:

- **Careful planning** – requires detailed evaluation of business and technical environments and specific threats to the organisation
- **Interoperability** – available systems, platforms, standards and protocols must be taken into consideration
- **PKI system and vendor selection** – Multi-vendor PKI / cryptographic solution could cause problems along the lines of protocols, certificate formats, integration, etc
- **Performance and capacity** – dependent on amount of data involved, algorithms and number of certificates to be issued

Conclusion

- UN ECA and partners continued assistance and experience sharing
- Policy, Legal and Regulatory Frameworks
- Roll out of E-government, Cybersecurity and Information Security Laws
- Training and Capacity Building
- Infrastructure Development
- Support for the African PKI Initiative

