HIPAA Security Regulations: Assessing Vendor Capabilities and Negotiating Agreements re: PKI and Security

March 2, 2001

Cy D. Ardoin, Ph.D.

Agenda

- Quick View of Security
- Strategy for Security
- Quick View of PKI
- Strategy for PKI

Quick View of Security Range of Attacks

	Script Kiddy	Hacker	Industrial Espionage	Electronic Warfare
Methods	Runs tools	Good tools Some homegrown	Good tools Many homegrown	Good tools Most homegrown
Motivation	Wants to brag about the break-in	Anger, Revenge, Profit	Profit, Compromise Business, Trade Secrets	Profit, Damage Industry, Damage Critical Infrastructure
Funding	No Funding	No Funding	Funding proportional to profit potential	Funding by foreign government may be proportional to profit
Stealth	Quick In and Out	Stealthy, trying to not be seen	Very Stealthy, will not be seen	Very Stealthy, will not be seen
Avenues	Internet mostly, Phone sometimes	Internet or Phone	Internet, Phone, Social Engineering, Physical, Electronic	Internet, Phone, Social Engineering, Physical, Electronic

Strategy for Security

- Establish a Security Program
  - Policy, Procedures, Mechanisms (Security Controls)
  - Assign Authority and Responsibility (Security Officer)
  - Focus on Critical Data (e.g. Medical Records and Financial Data)
  - Train employees and contractors
  - Monitor Activities and Report Problems
- Periodic Evaluation of the Program
- Maintain the Security Posture

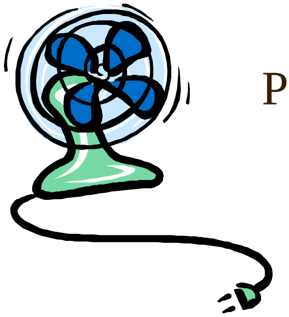
Vendor Capabilities

- Shop around, meet with three or more vendors
- Vendor investigation
  - Experience, stability, reputation, independence, etc.
- More than automated tools - good people are needed
- Know the methodology to be used
- Clearly state restriction on behavior and scope of work
- Penetration tests require protection of both parties
- Recommendations must be practical

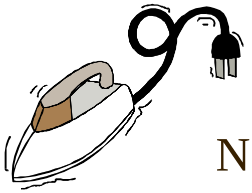
- Vendors should not play the role of Security Officer

Quick View of PKI

- Public Key Infrastructure
  - Support the implementation of a set of security functions



Privacy



Non-Repudiation

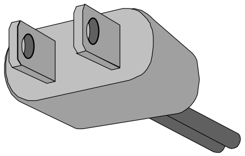
Digital Signatures

Data Integrity

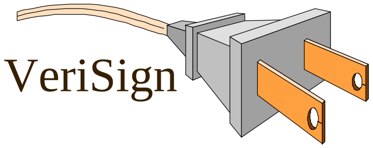
Authentication

Quick View of PKI

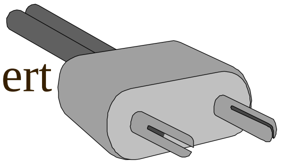
- PKI product vendors
  - Offer several options to implement security functions



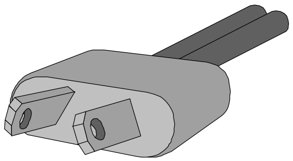
Entrust



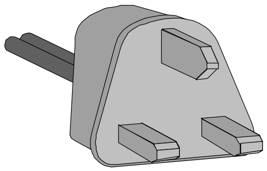
VeriSign



Xcert



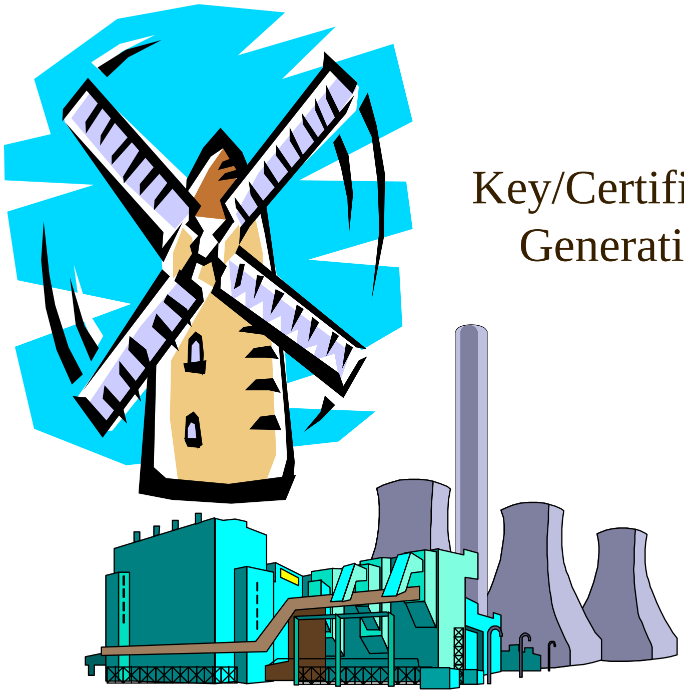
Baltimore



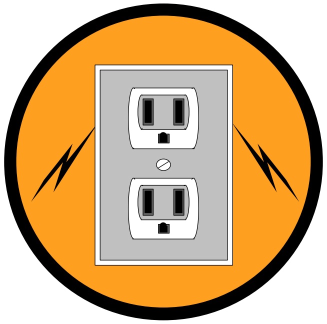
Netscape

Quick View of PKI

- Certificate Management Functions

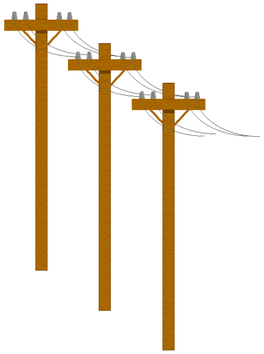


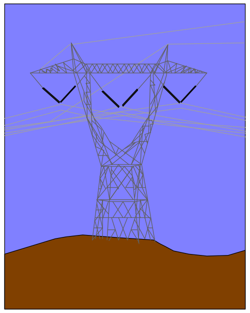
Key/Certificate Generation



Certificate Authority

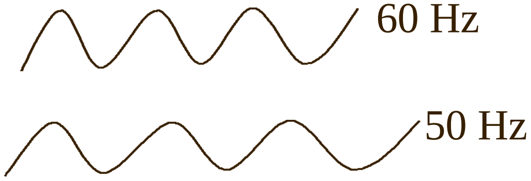
Certificate Format



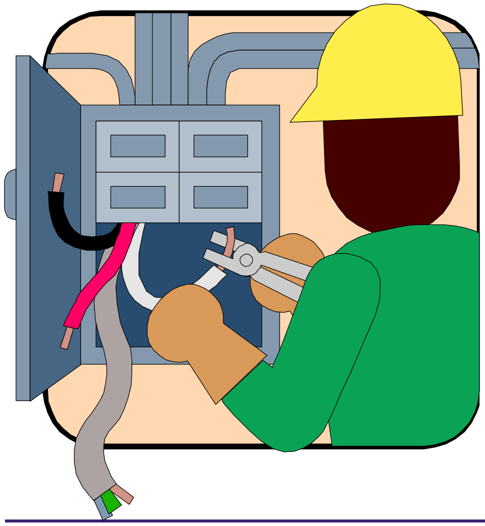


Quick View of PKI

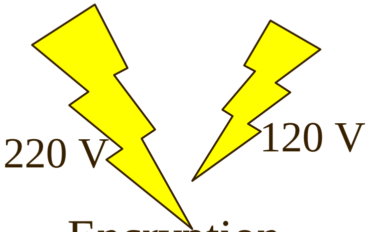
- Policies and Protocols



Security
Protocols



Key Management
Policies



Encryption
Algorithm

Key
Revocation

Strategy for PKI

- What is the business need for PKI?
- How do you acquire the services?

- Major topics to consider in developing a strategy
  - Build or Buy
  - Registration
  - Naming
  - Separate Keys
  - Types of Certificates
  - Tokens
  - Federal PKI and others
  - Number of users

Strategy for PKI

- Develop Requirements as a baseline for vendors
  - Who controls the registration process
  - Who can define the fields in the certificates
  - PKI shall satisfy the Class 3 criteria of the Federal PKI model
  - Define the standards, ITU, IETF, ANSI, PKCS
  - Define the CA requirements
    - CA will support registration, key generation, certificate generation, certificate revocation, certificate renewal, CRL generation and distribution, certificate and RRL archiving, on-demand private key recovery (for encryption keys), certificate and CRL retrieval.

Strategy for PKI

- Specify Algorithms (SHA-1 and PKCS #1 RSA to sign certificates and CRLs)
- Specify Key Lengths
- Hierarchy of the PKI (all subscribers fall under a specific subtree of the hierarchy)
- Certificate generation (X.509 version 3)
  - Define standard certificates (e-mail, encryption, code signing, server, etc)
- CRL requirements

– Registration Requirements

– Archiving Requirements

– Token Requirements

Strategy for PKI

- Estimate the number of users
- Get pricing and support data from vendors
- Compare Vendors to the Baseline Document
- Develop a PKI Certificate Policy
- Begin a prototype and staged deployment

Don’t Forget

- Interoperability
  - prototype interoperability with other organization
- Integration
  - PK-enabling applications may be difficult
  - prototype using several vendor products before making a large investment into software development
- Technical/Usability
  - different environments will have different demands for authentication mechanisms - a single solution for strong authentication will not work in a complex environment

A Few References

- NIST SP 800-12 An Introduction to Computer Security; The NIST Handbook.
- NIST SP 800-14 Generally Accepted Principals and Practices for Securing Information Technology Systems.
- NIST SP 800-18 Guide for Developing Security Plans for Information Technology Systems.
- X.509 Certificate Policy For The Federal Bridge Certification Authority (http://www.cio.gov/docs/FBCA_Policy_Document_1-17-01.htm)

Mitretek Systems

Cy Ardoin
Senior Manager
Information Security & Privacy Center
7525 Colshire Drive
McLean VA 22102-7400

Phone: 703-610-1946
Fax: 703-610-1699
Email: cy.ardoin@mitretek.org