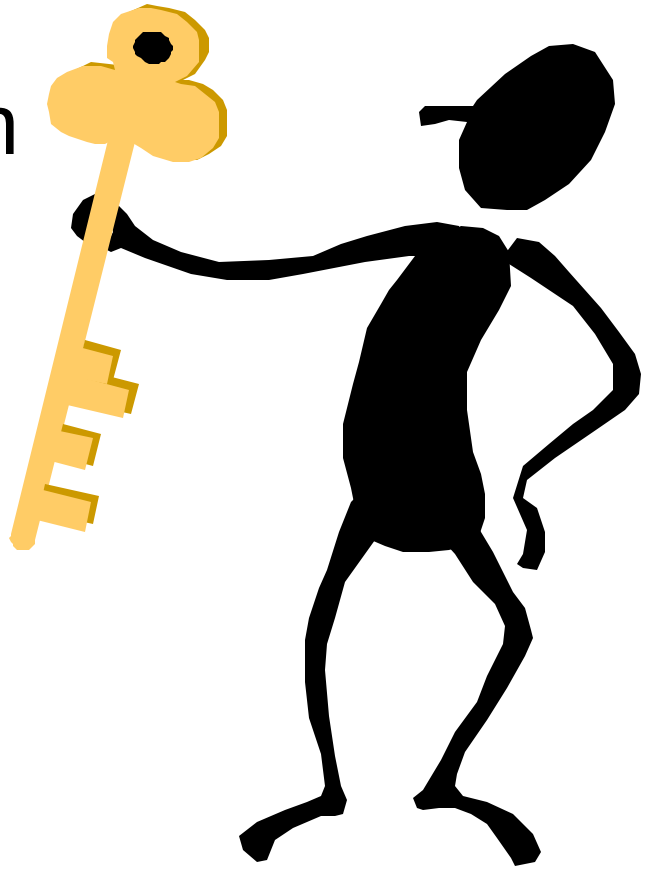
PKI Challenges

Michelle A. Ruppel
Saffire Systems
P.O. Box 11154
Champaign, IL 61826-1154
217 359-7763

Agenda

- Introduction
- Certificate Registration
- PKI Policy
- PKI Architecture
- Vision
- Envisioned usage
- Conclusion



Introduction

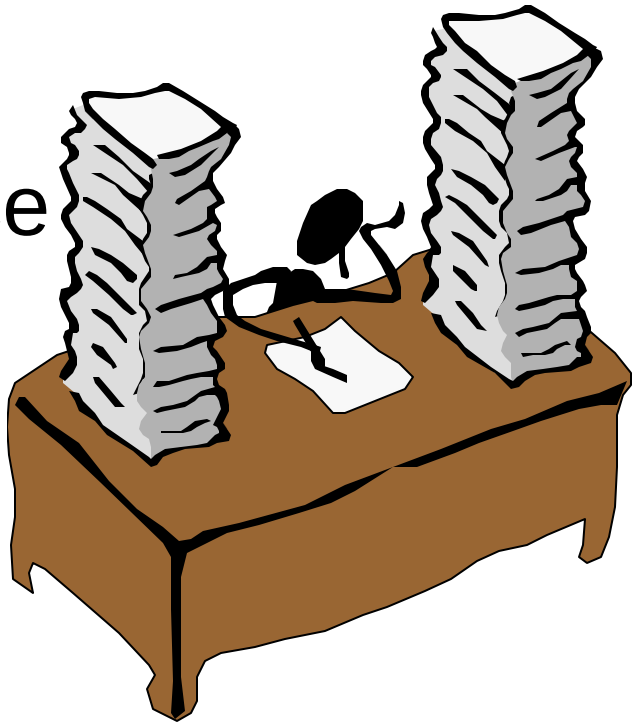
- Public Key Infrastructure (PKI) technology is fairly straight forward, well understood, and easy to install.
- Securely implementing PKI in an organization is none of these things.
- There are multiple issues and approaches surrounding this technology that need to be addressed before installing a PKI solution.

Introduction

- Resolving these issues correctly requires:
  - *shift in priorities (privacy versus I want it now & I want it simple)*
  - *managed expectations*
  - *education of executives*
  - *education of users*
  - *defining roles and responsibilities*
  - *defining the vision for the organization*
  - *understanding the current structure and culture of the organization*

Certification Registration

- Identity Theft
- Initial process for issuance of a certificate
- Level of Assurance
  - *Encryption (Low)*
  - *Authentication (Medium)*
  - *Legally Binding Signatures (High)*



Certification Registration

- Registration Authority
  - *Human*
  - *Electronic*
- Re-key / Recovery
  - *issuing a new certificate*
  - *different request method than registration*
    - perhaps using info obtained during registration (challenge questions)
  - *equivalent level of assurance as used in registration*

Certification Registration

- Registration Process Examples
  - *Callback*
  - *Face-to-face*
  - *Registration codes distributed via 2 separate mechanisms*
  - *Third-party verification (TRW, Equifax, Experian)*
  - *Secret/private information*

PKI Policy

- Private Key Protection
- Uptimes
- Separation of Duties
- Backups/Restores
- Certification Revocation Timeframes
- Public Attributes of Certificates
- Personnel Requirements

PKI Architecture

- Physical Protection
- Layered Security (Zones)
- Automated Registration Authorities
- Fault Tolerance
- High Availability
- Intrusion Detection

PKI Architecture

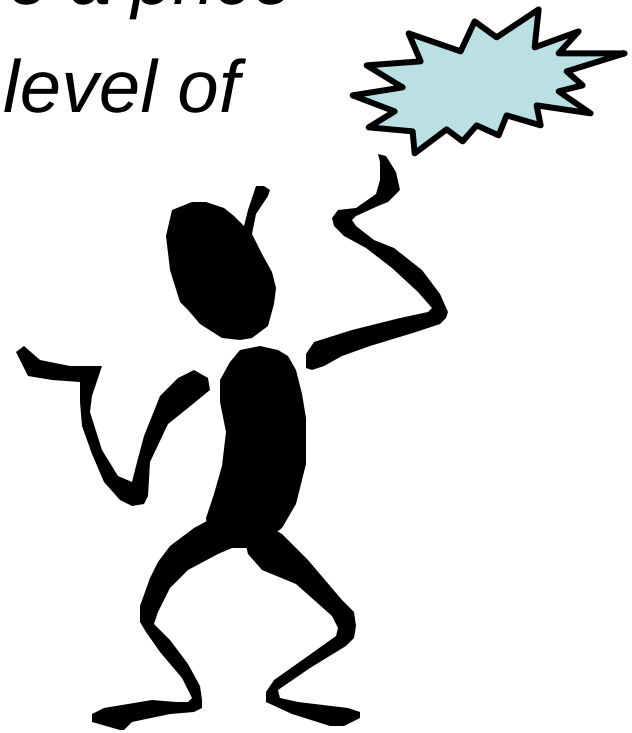
- Phased Approach
  - *Usage may initially be low risk*
  - *Assurance cannot always be added later without rebuilding*
  - *The Infrastructure must be built to the highest expected level of assurance*
- Enterprise-wide architectural components may conflict with a PKI

Envisioned Usage

- Disk & Packet Encryption
- VPN
- Authentication (single sign-on)
- Digital Signatures
- Legally-binding digital signatures
- Risk of impersonation
  - *Legal*
  - *Reputation*
  - *Loss via recovery time*

Vision

- Executive Education
  - *Electronic operations have a price*
  - *Misunderstood accepted level of risk*
- PKI vs. HTTPS



Government Involvement

- Guidelines on Securing Important Infrastructures
  - *Federal Bridge*
  - *NIAP Guidelines*
- Certification Standards
  - *Common Criteria Certification*
    - *Certificate Issuing and Management Components (CIMC) Family of Protection Profiles*
  - *System Accreditation & Certification*

Conclusion

- Security Expertise
- Planning
- Education
- Priority Shift