Protecting Networks and Data with Public Key Infrastructure (PKI)

MARK B. COOPER
PRESIDENT & FOUNDER

MARK@PKISOLUTIONS.COM
WWW.PKISOLUTIONS.COM
@PKISOLUTIONS

What is PKI?

Organizations need enhanced security for data and strong credentials for identity management. You can use certificates to secure data and manage identification credentials from users and computers both within and outside your organization.

The combination of software, encryption technologies, processes, and services that enables an organization to secure its communications and business transactions.

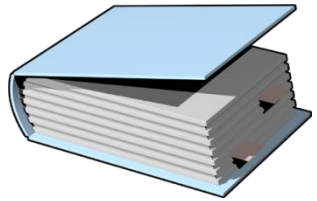
Confidentiality	Integrity	Authenticity	Nonrepudiation	Availability
Data Encryption	Digital Signature	Hashing, Message Digests, Digital Signature	Digital Signature, Audit Logs	Redundancy

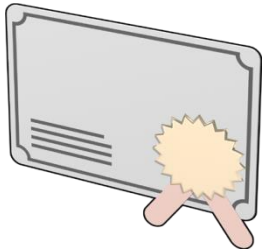
What are the components?

Certificate and CA Management Tools

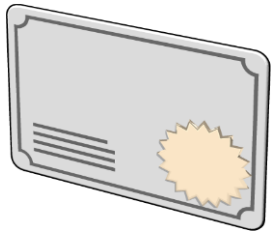
Certification Authority

Certificate and CRL Distribution Points





Certificate Template



Digital Certificate

Certificate Revocation List

Public Key-Enabled Applications and Services

Common PKI authentication solutions

- Smart card authentication
  - Organization wide
  - Tactical Two-Factor
- Wireless authentication – 802.11x
  - Variations
- VPN authentication
- Code signing

Smart card authentication

Password based user authentication

- Based on user knowledge only
  - Authentication name & passphrase
- No controls on this knowledge
- Requires server-side storage of credential details
- Easy to share, relatively easy to find
- Easy to refute

User authentication – smart cards

- Two-Factor authentication
  - Have – certificate
  - Know – passphrase
- Single instance/location
- Nonrepudiation available
- Protected against MITM, Pass-the-Hash, etc.

User authentication – organization wide

- Large capital investment
- User training and behavior modification
- Process and procedures
- Potentially impacts ALL authentication, devices, and services
- 90% process, 10% technology

Tactical two-factor authentication

- Focus on most vulnerable and highest value assets
  - Administrative and elevated accounts
- Perimeter systems
- High value corporate assets (database servers, manufacturing, etc.)
- Procedures still important, but significantly smaller scope
- Smaller capital investment
- Gain experience and comfort prior to larger rollout

Tactical two-factor authentication

- REQUIRE Smart card authentication
  - No impact to email and other difficult to incorporate services
  - Active Directory managed password significantly harder to break*
- USB token Smart card form factor
  - Greater portability
  - No dedicated reader on each device

Wireless authentication

Wireless authentication

- Pervasive adoption by organizations around the world
  - Convenience over security considerations
- Open Networks and Username/Password authentication (PEAP)
- Bypasses physical security and controls
- Internal and external actors
- Lost/stolen devices present significant risk

Wireless authentication – 802.11x

- Mutual authentication (EAP-TLS)
- Leverages device and/or user certificates
  - Generally not a bounded authentication
- Seamless as password based authentication
- Provides identity assurance
  - Knowledge of internal credentials is insignificant
- Easy to switch from PEAP to EAP-TLS
- Similar credential for other client authentication needs

Network authentication variations

- Wired authentication
- Microsoft DirectAccess
- IPSEC and other tunnels
- NAC/NAP integrated solutions

VPN authentication

VPN authentication

- Most common access technology employed
- Bypasses all traditional physical security controls
- Security is dependent on strength and integrity of authentication

VPN security

- Common ports
- Common security mechanisms
- By nature, remote authentication
  - Ripe for exploitation
- Traditionally secured with username/password

VPN PKI authentication

- Identifies and authenticates users or devices
- Previously determined to be trusted entity
- Can’t be shared
- Can’t be socially engineered
- High level of integrity
- Combined with Smart card, offers nonrepudiation

Code signing

Code signing uses

- Attests to the organization or individual creating data
- Internal and externally distributed software
- Macros and scripts
- Data can be re-signed by relaying party
- Software policy restrictions in Active Directory

Code signing implementation

- Can integrate with code build process (Visual Studio, etc…)
- Software installer packages (EXE, MSI)
- Manual invocation and scripted signing
- Timestamping provides historical integrity of signing

Code signing security concerns

- Access to code signing private key must be controlled
- Private key access jeopardizes organization’s reputation
- Control and invocation of signing must be auditable