Public Key Infrastructure 101:
A Security Manager's Survival Guide

Tim Polk

November 29, 2001

Why, What, How, and How-not

- What a manager needs to know about PKI:
  - *Why* build a PKI?
  - *What* is a PKI?
  - *How* do I deploy a PKI?
  - What are some common pitfalls to avoid? (The *How-Not* of PKI)

Symmetric, or Secret Key, Cryptography

- Sharing secret keys is
  - Difficult to get started: Alice needs to go see Bob before she can send him a secret message.
  - Hard to scale: If Alice wants to send a message to Carol, she has to start over with a new secret.
  - An oxymoron: If Alice and Bob both have the key is it really secret? Alice has to trust Bob completely

Asymmetric, or Public Key, Cryptography

- There are no shared secret keys
- There are lots and lots of public keys
  - Each person has their own key pair(s), with a private (really!) key and a public key
- Alice has two burning questions
  - “Who’s key is this anyway?”
  - “Is this key still valid?”

Public Key Infrastructure

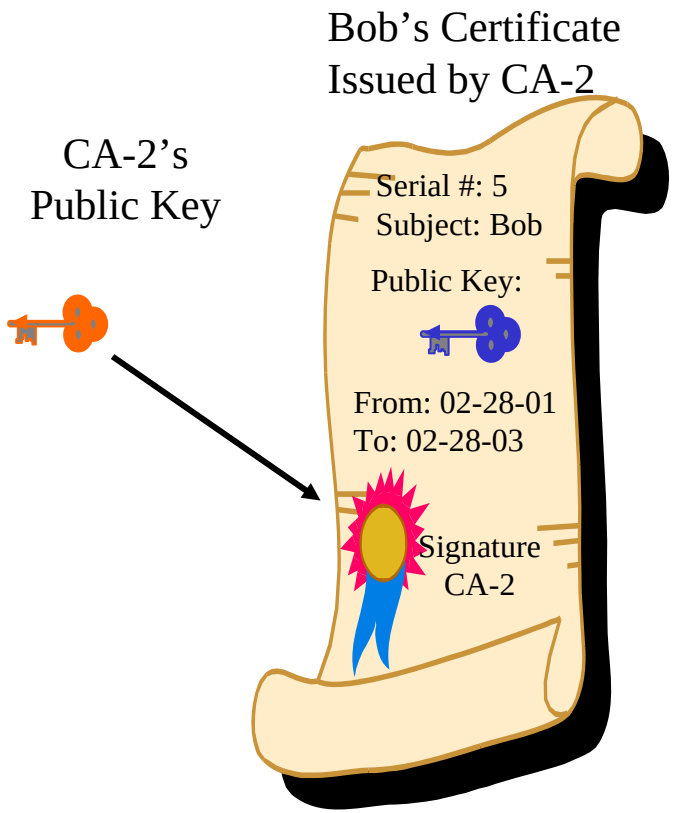
- A PKI answers Alice's burning questions so she can use public key cryptography to achieve security with lots of people
  - Certificates bind an identity to a public key
    - This is Bob's RSA public key
  - Certificate Revocation Lists (CRLs) are the list of certificates Alice shouldn't trust

Public Key Infrastructure Components

- There are four basic infrastructure components
  - Certification Authority (CA) – generates certificates and CRLs
  - Registration Authority (RA) – checks users identity to ensure binding is correct
  - Directory – database of certificates and CRLs
  - Archive – keeps old certificates and CRLs for use in distant future
- If Alice trusts a particular CA, she can use its certificates to protect information

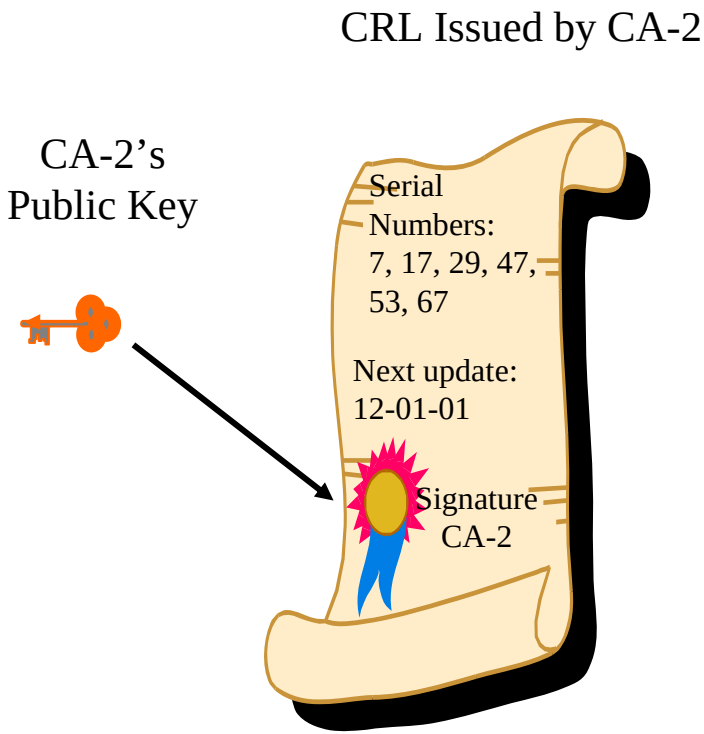
X.509 Certificate

- Tamper-evident package (CA's digital signature)
- Contents include
  - Serial number
  - Subject (user) name
  - Validity period
  - Optional information (*extensions*)

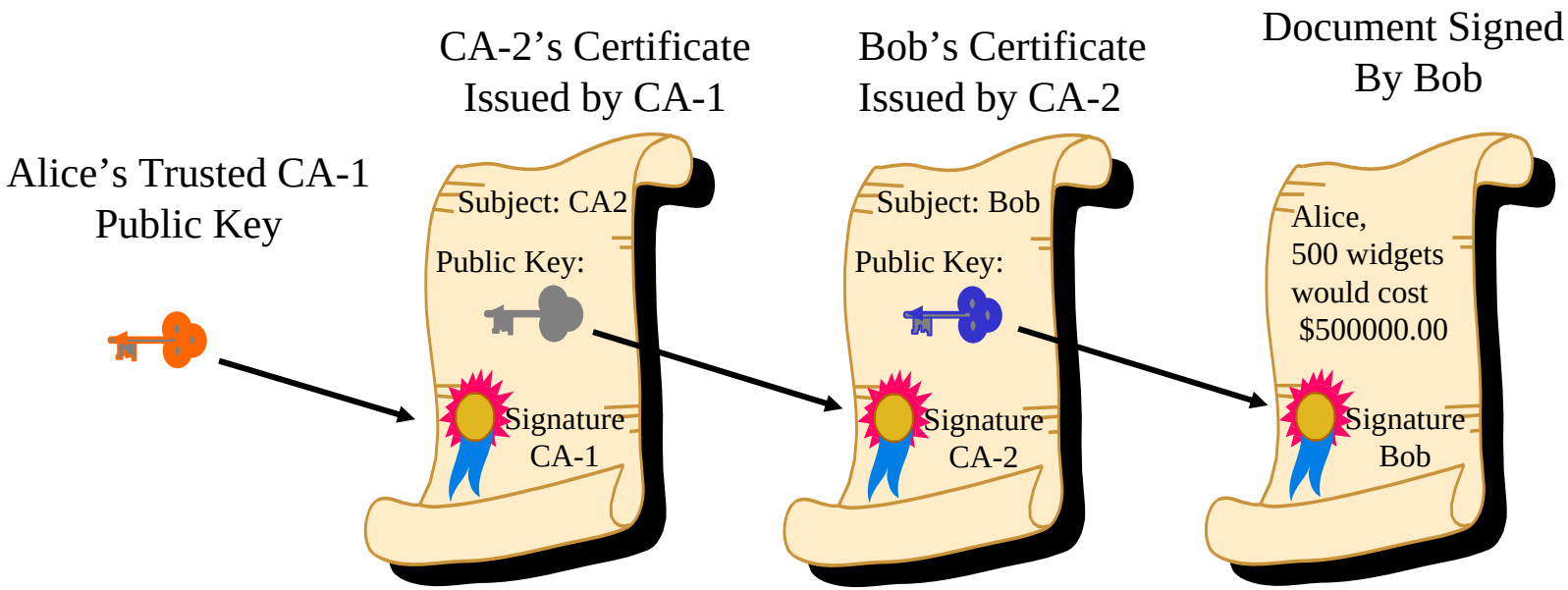


X.509 Certificate Revocation List

- Analogous to the credit card “hot list”
- Issuer’s un-expired certificates that aren’t trustworthy (a.k.a., “revoked”)



X.509 Certification Path



Achieving Security with PKI: An Encryption Example

- Alice creates a key pair and goes to the RA to request a certificate
- The RA checks her ID and requests the certificate from the CA
- The CA posts it in the directory
- Bob gets the certificate from the directory
- Bob verifies her certificate, makes sure its not on the CRL, and uses her public key to send her a secret message

Achieving Security with PKI: A Digital Signature Example

- Alice creates a key pair and goes to the RA to request a certificate
- The RA checks her ID and requests the certificate from the CA
- The CA posts it in the directory
- Alice uses her private key to sign a message
- Bob gets the certificate from the directory
- Bob verifies her certificate, makes sure its not on the CRL, and uses the public key to verify her signature

Policy and Procedures

- A PKI is only as strong as the policies and procedures that govern its operations
  - Certificate Policy (CP)
    - Describes the security policy for issuing certificates and maintaining certificate status information
  - Certification Practice Statement (CPS)
    - Describes how a CA implements a particular CP
  - Compliance analysis
    - Verifies that a CPS meets a CP
  - Certification and Accreditation
    - Verifies that a CA is performing the procedures described in its CPS.

So, You Want To Deploy A PKI

- Simple Steps:
  - Categorize the information you're protecting
  - Develop an appropriate CP
  - Select your PKI products
  - Draft a CPS
  - Compliance analysis
  - Begin pre-production operations
  - Certification & Accreditation
- You're in business!

Categorize the information and applications you're protecting

- What can go wrong: Requirements Creep
  - Everyone wants a PKI to solve *all* the security problems in an organization
  - A PKI that is appropriate for million dollar fund transfers will be overkill for Alice's personal messages to Bob
- Solution: Solve the 80% that's easy

Develop an Appropriate CP

- What can go wrong:
  - There is a temptation for perfection, resulting in complex and expensive PKIs.
- Solution:
  - Examine the level of security afforded this data today. Strive for cost-effect *improvements*.

Select PKI Products

- What can go wrong:
  - Products do not include technical mechanisms to implement your CP (e.g., two person control)
  - CA product does not support your applications
- Solutions:
  - Compensate with physical and procedural controls in the CPS
  - Factor support for target applications into the procurement process

Draft a CPS

- What can go wrong:
  - No one wants to operate/house/support the CA
  - No one wants to be the RA
  - Everyone wants to use your directory for their applications
- Solutions:
  - Get upper management buy-in
  - Limit directory responsibility to PKI

Compliance Analysis (1 of 3)

- What can go wrong:
  - The CP was too specific and boxed you in to inappropriate procedures
- Solution:
  - Rewrite the CP to describe your goals, then write a CPS that meets those goals through sensible procedures

Compliance Analysis (2 of 3)

- What can go wrong:
  - The CP was too specific and PKI products just don't work that way
- Solutions:
  - If you wrote the CP first, use it as part of your procurement specification
  - If you bought the CA first, understand its mechanisms before writing the CP

Compliance Analysis (3 of 3)

- What can go wrong:
  - The CPS doesn't match the CP
- Solution:
  - Revise either the CP or CPS until you get it right

Certification and Accreditation

- What can go wrong:
  - System is not being operated according to the CPS
- Solutions:
  - Use the CPS as the basis for your own operations manuals
  - Training, Training, Training

Summary

- PKI enables ubiquitous security services through public key cryptography.
- The technical mechanisms for PKI are well understood and the products work.
- The policies and procedures that make PKI work can be complicated, and common mistakes compound the problems
- The problems are avoidable, and PKI can work for you and your agency

For More Information

Tim Polk 301-975-3348, tim.polk@nist.gov

Draft NIST publication: *An Introduction to Public Key Technology and the Federal PKI*
http://csrc.nist.gov/publications/drafts/pki-draft.pdf

The NIST PKI website http://csrc.nist.gov/pki

The Federal PKI Technical Working Group
http://csrc.nist.gov/pki/twg

The Federal PKI Steering Committee
http://www.cio.gov/fpkisc/