PKI Tutorial

Jim Kleinsteiber

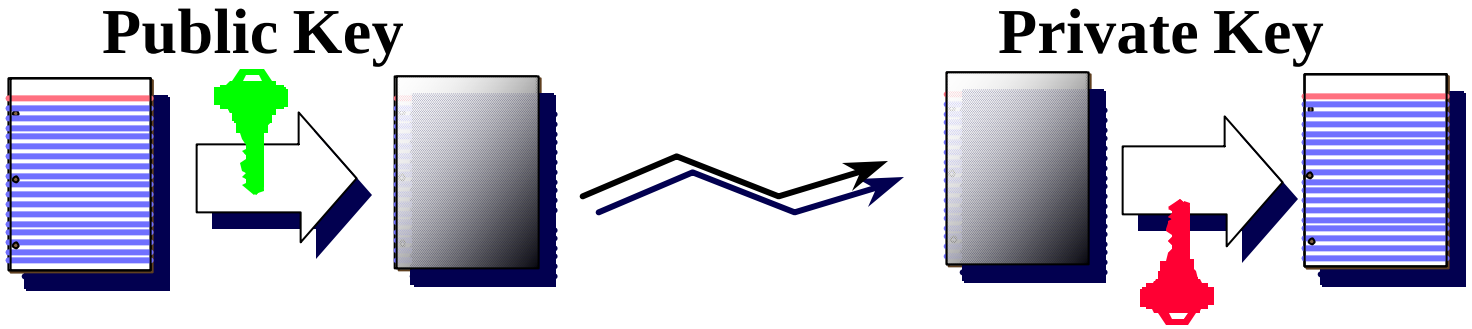
February 6, 2002

BROCADE

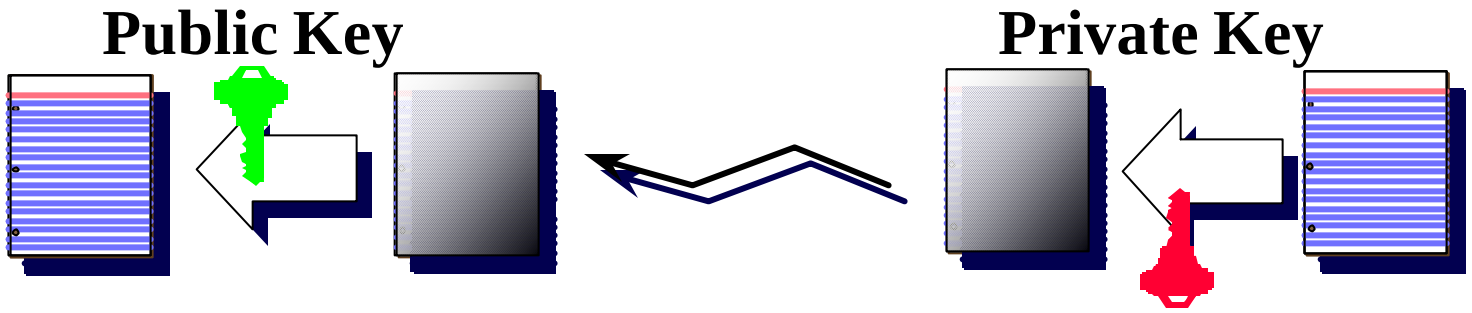
Outline

- Public Key Cryptography Refresher Course
- Public / Private Key Pair
- Public-Key – Is it really yours?
- Digital Certificate
- Certificate Authority

Public Key Cryptography Refresher Course



Each user has 2 keys - What one key encrypts, only the other key in the pair can decrypt



It works both ways!

BROCADE

Public / Private Key Pair

- **Public Key Cryptography provides the basis for:**
  - **Digital Envelopes – anyone can encrypt data with the public key; only the holder of the private key can decrypt.**
  - **Digital Signatures – the holder of the private key can encrypt (sign); anyone can verify that the owner of the private key did the encryption (signature).**
- **The Private key must be kept secret by its owner.**
- **The Public Key is freely distributed for others to use.**

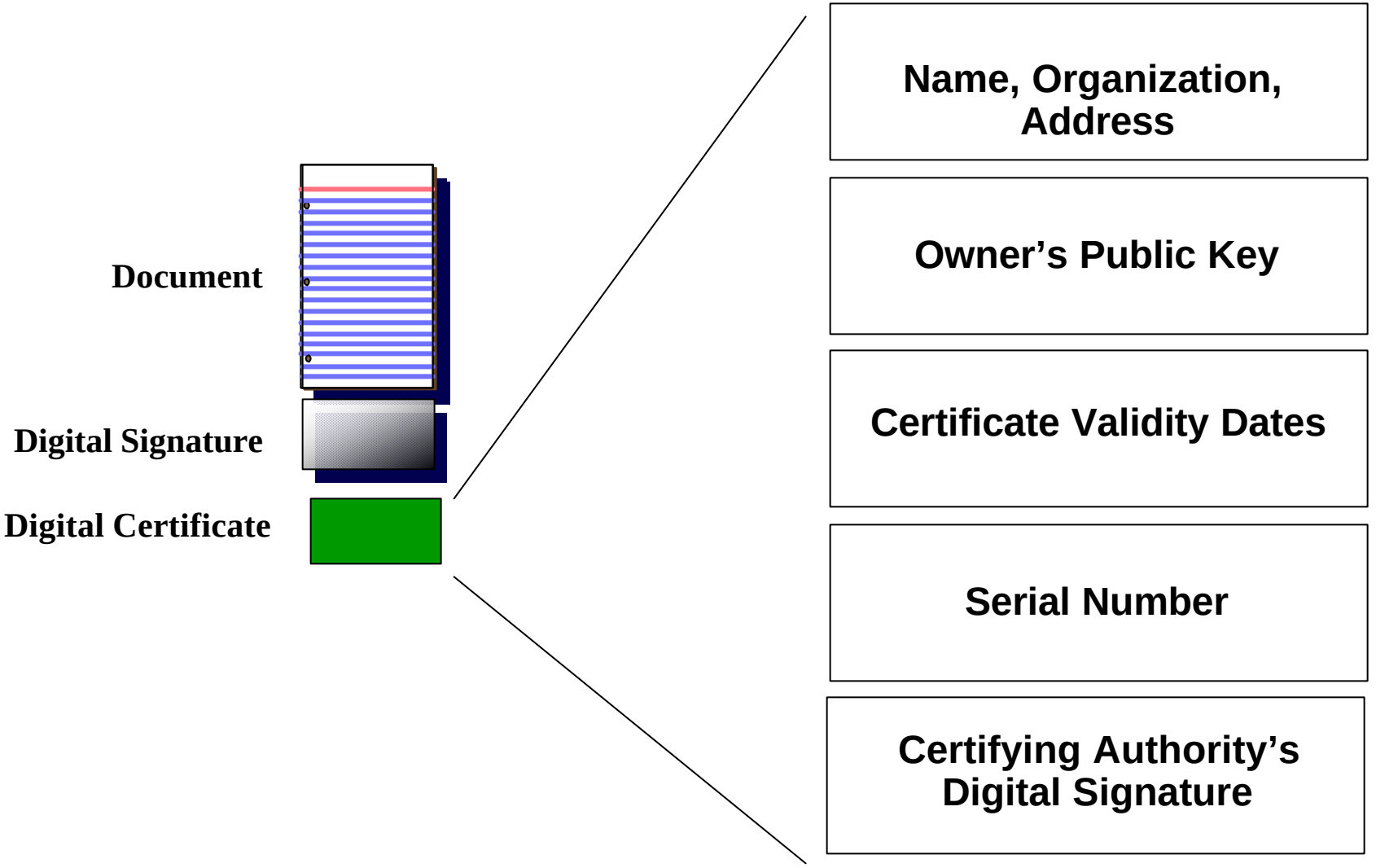
BROCADE

Public Key – Is it really yours?

- How to Find Out Someone's Public Key?
  - Send with message
  - Lookup From Database
- How to Trust the Result?
  - Digital Certificates
  - Trusted Certificate Authorities
- Signed Message that proves
  - "Bob's Key is N"

BROCADE

Digital Certificate



BROCADE

Certificate Authority

- What is a Certificate Authority (CA)?
- CA functions
- Responsibilities
- Delegation

BROCADE

What is a Certificate Authority (CA)?

- A fundamental component of PKI
- Collection of Software, Hardware and people managing it.
- Attributes
  - Name
  - Public key
- Issues a self-signed certificate
  - Root CA

BROCADE

Certificate Authority Functions

- Issue certificates
- Maintain certificate status and issue Certificate Revocation Lists (CRLs)
- Publish current certificates and CRLs
- Maintain archives of expired and revoked certificates

BROCADE

Issue Certificates – Root CA

Root CA

- Issue certificates to Other CAs
  - Level 1 CA
- Authorizes Level 1 CA to issue certificates
- Level 1 CA can issue other CA certificates if authorized.
- A CA chain is created in this manner

BROCADE

Issue Certificates

- Issue certificates to users
- Information in the certificate is binding to the entity
  - Name, Organization, Address
  - Public key
  - Validity Dates
  - Serial number
  - Certifying authority's digital signature

BROCADE

Issue Certificates – Process

- User Submits a Certificate Signing Request (CSR)
  - with name, public key and other information
- CA Follows Known Policies & Procedures to validate request as defined in the Certificate Practice Statement (CPS)
- CA Attaches Extra Information
  - Validity Dates, Key Usage, Account ID, Etc.
- CA Signs Certificate

BROCADE

Maintain Relevant Information

- Maintain certificate directory for Certificate lookup
- Maintain a List of Revoked Certificates (CRL)
- Manage User Changes

Publish Current Certificates and CRLs

- Distribute its certificates
- Distribute list of Revoked Certificates (CRL)
- Distribution need not be secure
  - But it should be made secure if required for privacy.

BROCADE

Maintain Archives

- **Maintain information about old certificates**
  - **Person or system named in certificate**
  - **Certificate request**
  - **Validity period of certificate**
  - **If certificate was revoked**
  - **Any other activity performed by CA in certificate's lifetime**

BROCADE

Certificate Authority Responsibilities

- Protect its private key
- Verify subject information in CSR
- Adhere to profile defined in CPS
- Maintain list of revoked certificates
- Distribute its certificates and CRLs
- Maintain certificate archives after expiration

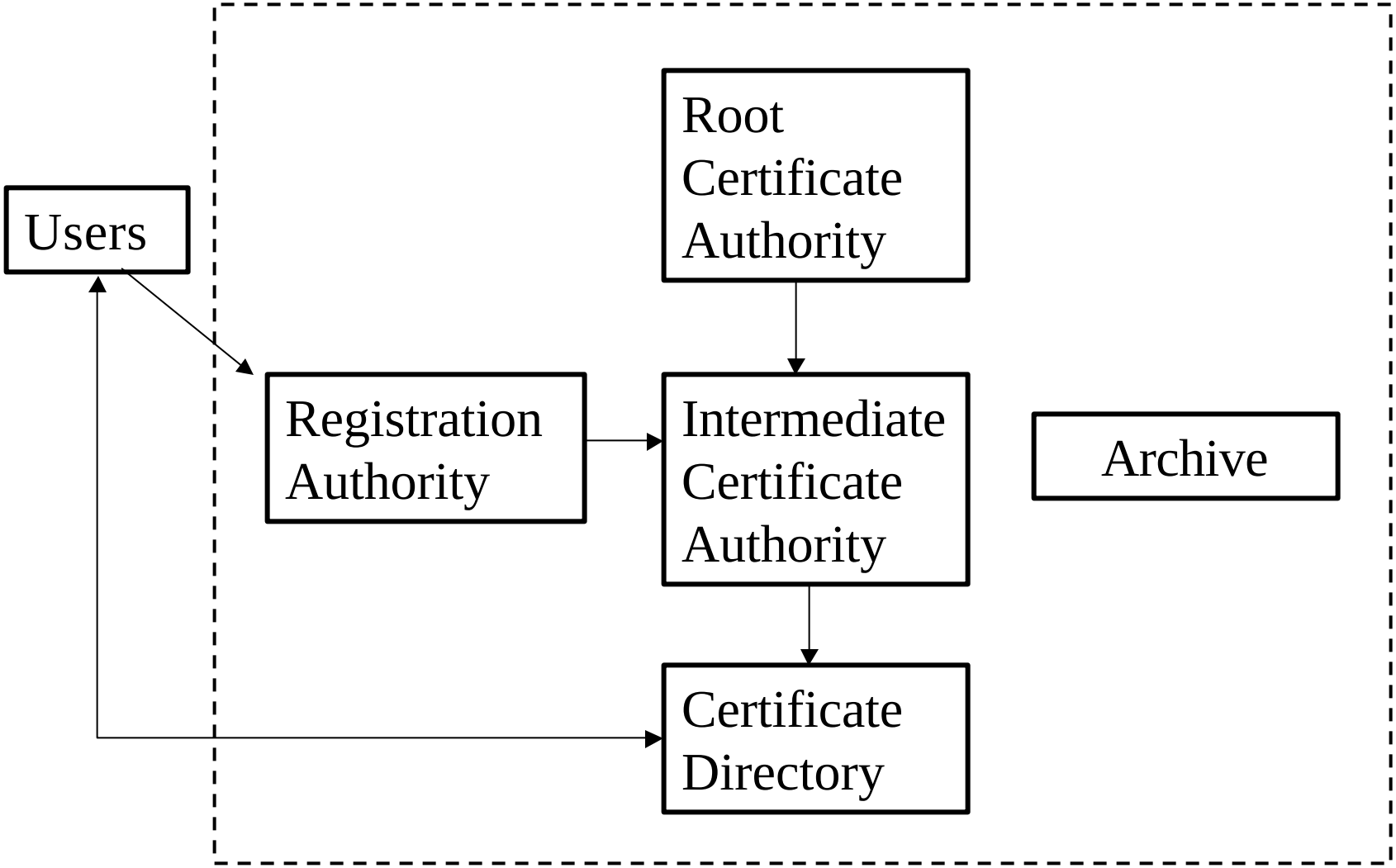
BROCADE

Certificate Authority - Delegation

- CA can delegate its responsibilities to
  - Registration authority (RA)
  - Repository (certificate directory)
  - Archive

BROCADE

Public Key Infrastructure



BROCADE

Certificate Authority Delegation

- Registration Authority (RA) verifies certificate request
- Repository distributes certificates and CRLs
- Archive provides long term secure storage

CA can create multiple of these entities to offload and distribute work