Public Key Infrastructure

A presentation to ISACA

Vincent LeVeque

October 1999

Information Security

- Information constitutes important corporate asset
- Enterprise information system involves external organizations
- Enterprises face greater risks from more sophisticated attackers
- A basic trust model is prerequisite to conducting electronic commerce

By 2002, 90% of all enterprises will have experienced significant financial loss as the result of an information security breach (70% probability)*

* ***Source: Gartner Group, Information Security in a Networked World, April 1998***

Security Services

Authentication	Provides assurance of the identity of some entity (a person or a system)
Access Control	Protects against unauthorized use or manipulation of resources.
Data Integrity	Protects against data being changed, deleted, or substituted without authorization.
Confidentiality	Protects against information being disclosed or revealed to unauthorized entities.
Non-Repudiation	Protects against a person denying later that a communication or transaction took place as recorded.

Security Services

Access Control	Discretionary Access Control Firewall Filter Router Single Sign-On Plant Control	Authentication Server Proxy Mandatory Access Control (Data Labelling) Kerberos
Authentication	Biometric Technology Basic UserID/Password Logon Tokens and Smartcards	**Public Key** One-Time Password w/2 factor authentication RADIUS
Data Integrity	Simple Checksum Data Base Referential Integrity	**Digital Signature (hashed message digest)**
Confidentiality	Database Encryption Virtual Private Network	**Public Key**
Non-Repuditation		**Digital Signature (Private Key)**

Information Security

- A basic trust model is prerequisite to conducting electronic commerce

Trust Model Components

- When two parties engage in a transaction they must:
  1. Mutually trust each other's identity
  2. Trust that both parties are allowed to engage in the transaction
  3. Trust that no third party can know the details of the transaction
  4. Trust that no third party can change any part of the transaction
  5. Trust that neither party can deny having engaged in the transaction
  6. Trust that a record of the transaction is kept for future reference

Threats and Defenses

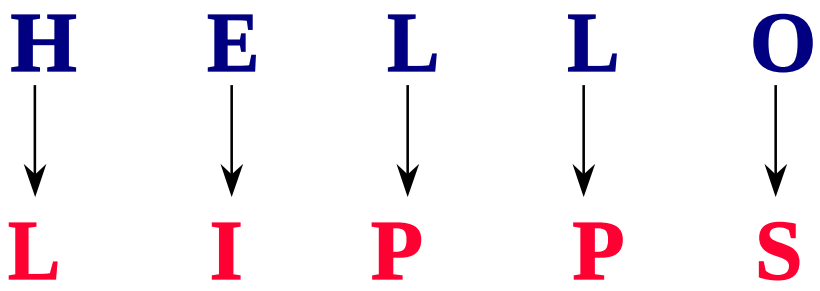
- Who are you?
- What can you do?
- For your eyes only.
- Can’t touch this!
- You can’t say “I didn’t do it.”
- What happened?
- I am always here

- Authentication
- Access Control
- Confidentiality
- Integrity
- Nonrepudiation
- Audit
- Availability

Traditional Implementation of Security

- Based on the notion of ***shared secrets***
- Issues
  - Requires pre-agreement on the shared secret
  - Each client must maintain a shared secret with each server
  - Not scaleable to a very large enterprise
  - Does not follow business model
- Some issues mitigated by network based solutions
  - The Kerberos Authentication System

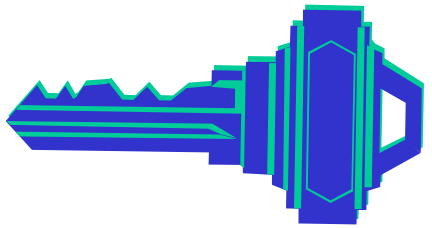
Foundation



- Encryption
  - The process of disguising a message in such a way as to hide its substance
  - Requires an encryption ALGORITHM and an encryption KEY

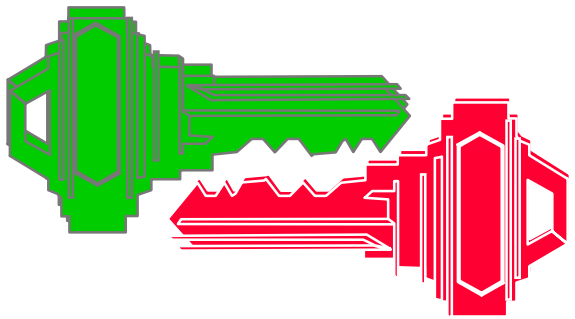
Symmetric Encryption Algorithms

- The same key must be used for encryption and decryption
- The sender and receiver must know this SHARED key
- The shared key must only be known to the sender and the receiver
- Examples
  - Data Encryption Standard (DES)
  - Rivest Ciphers (RC2, RC4, RC5)
  - International Data Encryption Algorithm (IDEA)



Asymmetric Encryption Algorithms

- Two different, but related keys: a PUBLIC key and a PRIVATE key
- Anything encrypted with the public key can only be decrypted with the private key
- Anything encrypted with the private key can only be decrypted with the public key
- Examples
  - Rivest-Shamir-Adelman (RSA)
  - Digital Signature Algorithm (DSA)
  - Elliptic Curve Cryptosystem (ECC)



Practical Considerations

- Encrypting an arbitrary large message using an asymmetric algorithm can be prohibitive
  - Use the asymmetric key pair to negotiate a symmetric, short-lived, session key
- For non-repudiation there is really no encrypt the entire message
  - Encrypt a digest of the message
- The authenticity of a public key must be ascertained
  - Use a Certification Authority to establish a chain of trust

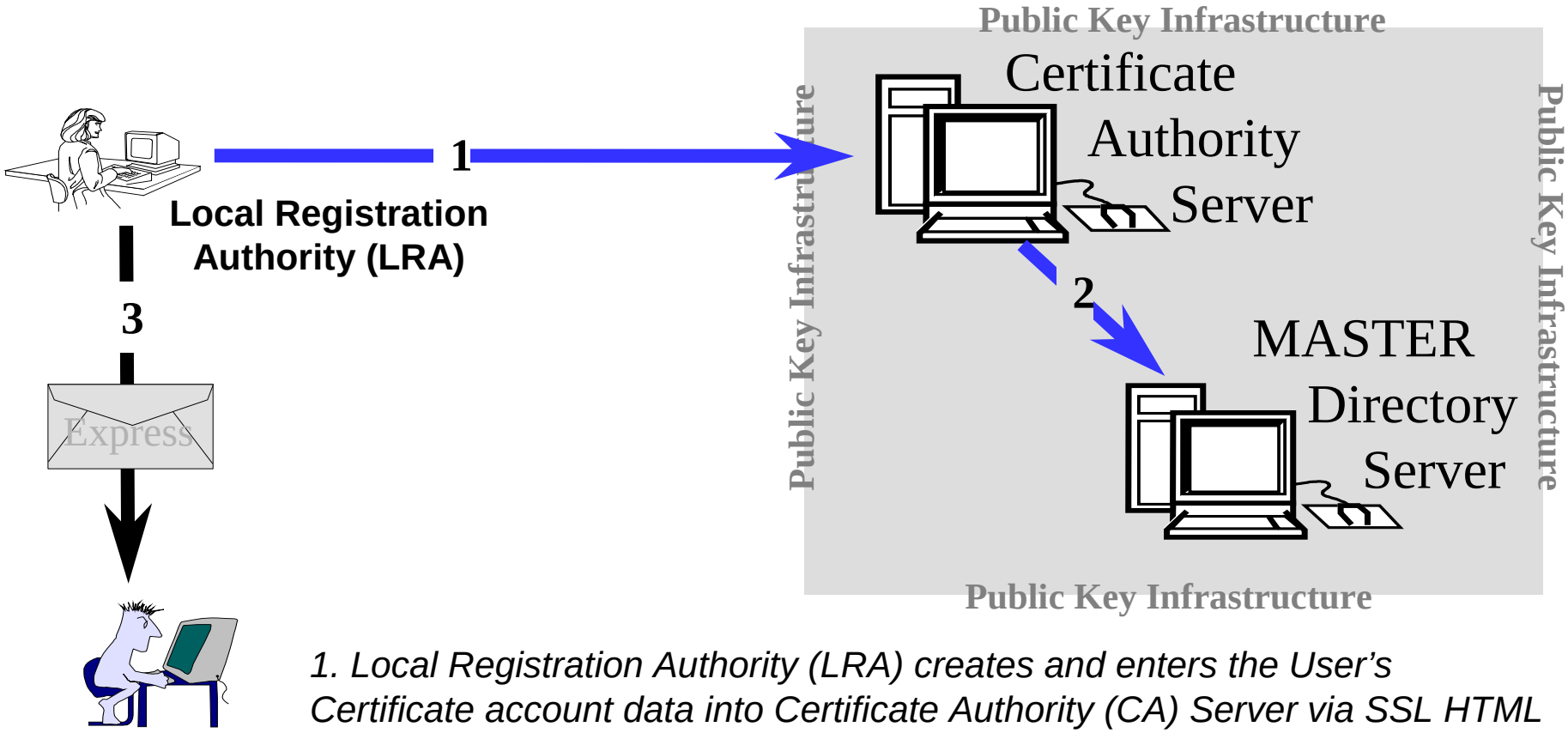
Considerations

- Effective use of public key cryptography requires resolution of the trust issue (“is this really Joe’s key?”)
- Building trust is not a simple task
  - Technology
  - Law
  - Administrative infrastructure
- Public Key Infrastructure attempts to create trust

Essential PKI Processes

- Creation of cryptographic key pair
- Creation of Public Key Certificate
  - CA signs key and publishes
- Policy Infrastructure to give operational meaning to cryptographic functions
  - Certificate Authority function
  - Certificate Policy
  - Certificate Practice Statement

Public Key
(Registration)



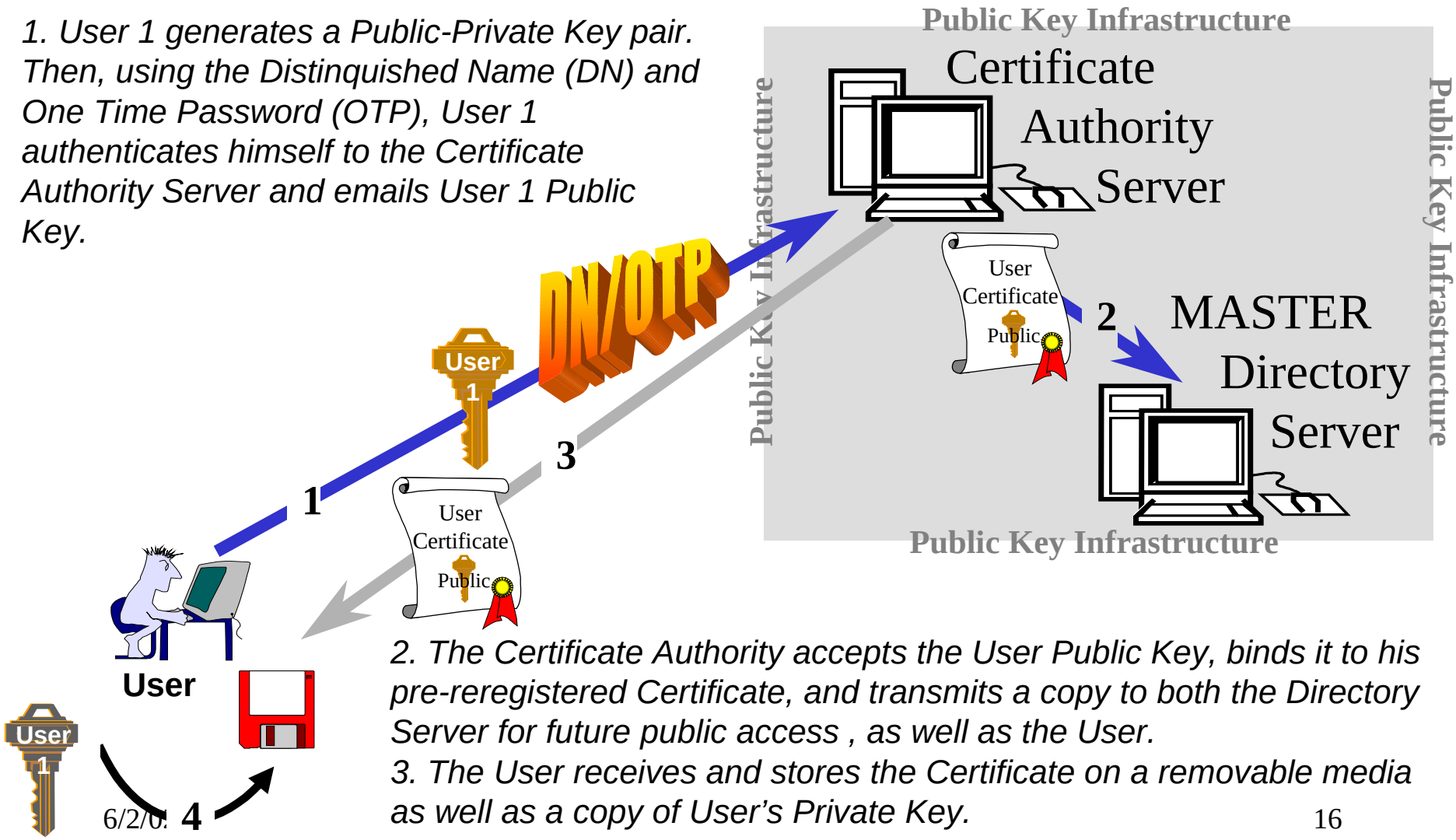
1. Local Registration Authority (LRA) creates and enters the User's Certificate account data into Certificate Authority (CA) Server via SSL HTML form.

2. The Certificate Authority automatically creates User record in the Master Directory Server

3. Local Registration Authority (LRA) provides the User with a One Time Password (OTP) and Distinquished Name via Express Mail or in person.

Public Key (Cert Issuance)

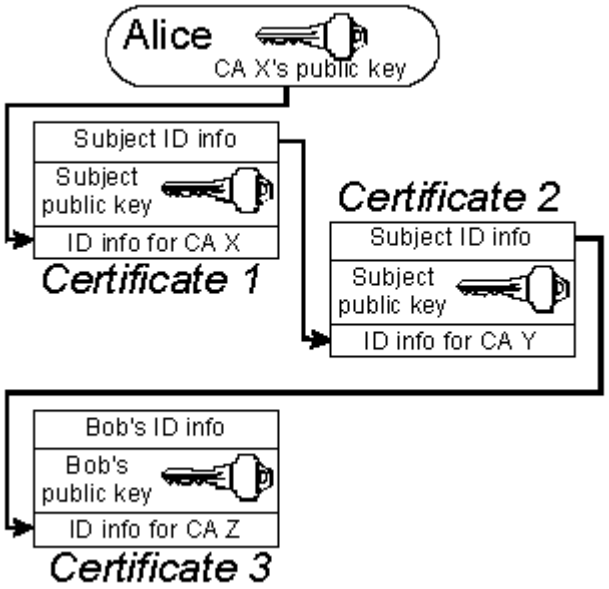
1. User 1 generates a Public-Private Key pair. Then, using the Distinquished Name (DN) and One Time Password (OTP), User 1 authenticates himself to the Certificate Authority Server and emails User 1 Public Key.



2. The Certificate Authority accepts the User Public Key, binds it to his pre-reregistered Certificate, and transmits a copy to both the Directory Server for future public access , as well as the User.

3. The User receives and stores the Certificate on a removable media as well as a copy of User's Private Key.

Public Key (Cert Validation)



What is a Key Certificate

- Exact format and content of an identity certificate is standardized by the X.509 Digital Certificate Standard

◆ **If the private key is compromised the certificate needs to be revoked**

—Certificate Revocation Lists (CRLs)

◆**Original certificate has a lifetime and must be renewed**

Certification Authority (CA)

- An entity whose public key you trust
  - Public key is transmitted via secure, non-electronic communication
  - Public key may also be obtained from numerous sources
  - The private key of the CA is used bind the identity of a principal to its public keys
- The CA issues *credentials* to other entities
  - Digital certificates is a form of credentials
- Types of digital certificates
  - Identity
  - Attribute
    - Role
    - Permission

Certificate Policy (CP)

- A set of rules that indicates:
  - Common security requirements
  - The applicability of a certificate to a particular community
  - The applicability of a certificate to a particular application class of application
- A Certificate Policy is a blue print defining *what* must be done to meet the common security requirements

CP Contents

- Introduction
- General Provisions
- Identification and Authentication
- Operational Requirements
- Physical, Procedural and Personnel Security
- Technical Security Controls
- Certificate and CRL Profiles
- Specification Administration

Certification Practice Statement (CPS)

- A statement of practices that the Certificate Authority employs in issuing and revoking certificates
- Must follow the Certificate Policy
- A CPS complements the CP by describing *how* the Certificate Authority meets the common security requirements
- A CPS enumerates mutual rights and obligations of the CA as well as the subscribers

CPS Contents

- Background and Concepts
- Overview, CP Identification, Community, Applicability
- Legal Provisions, Obligations, Disputes and Compliance
- Initial Validation of Identity and Authority
- Certification Life Cycle Operational Requirements
- Private Key Recovery
- CA Facility and Management
- Procedural and Technical Security Controls
- Certificate and CRL Profiles
- Specification Change Procedures

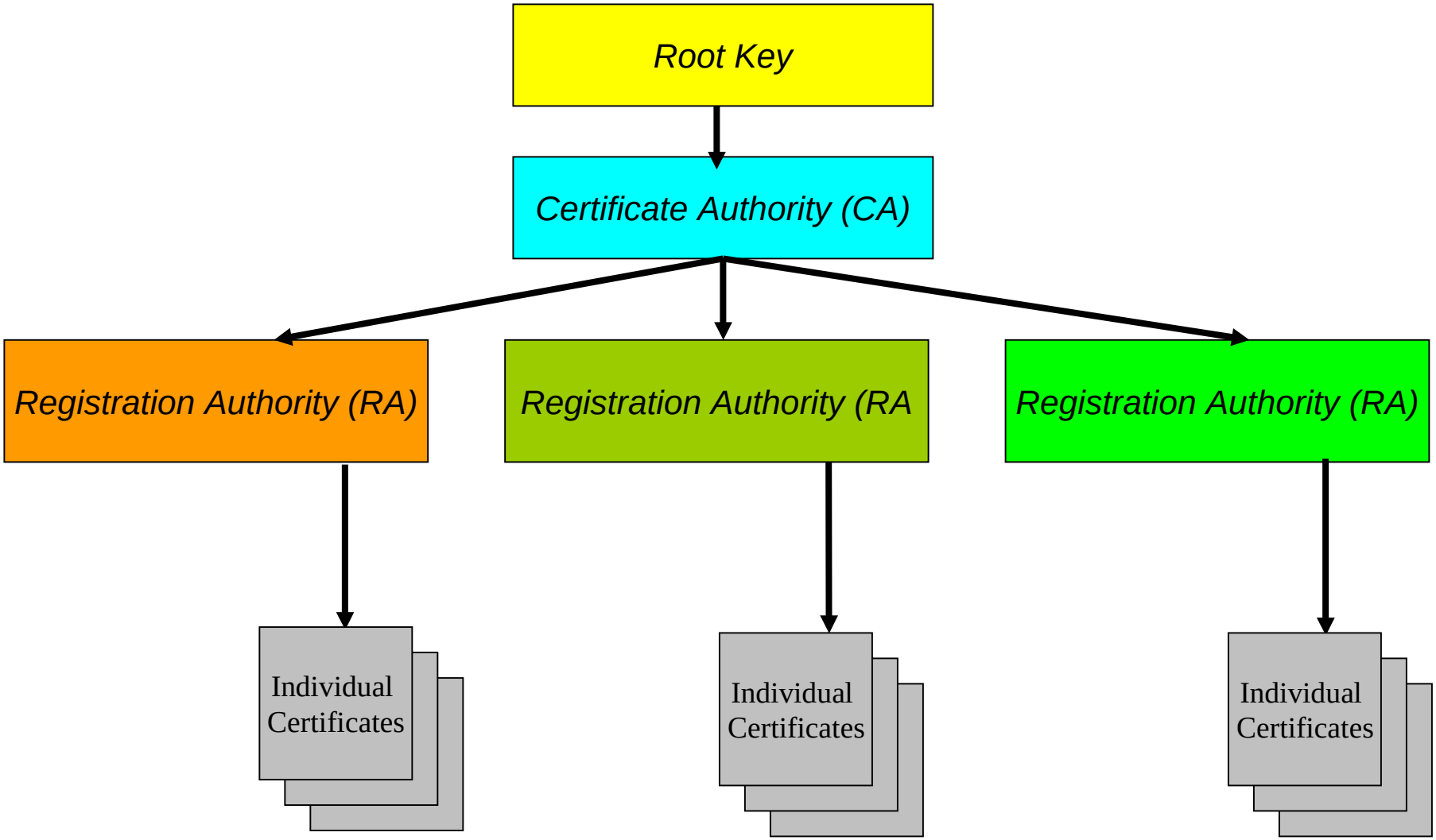
Highlights of Subscriber's Obligation as Defined in the CPS

- Storage and safekeeping of the private key and other credentials
- Credentials must be renewed every year
- CA must be notified when
  - Storage medium (e.g., smart card) is lost is suspected to have been compromised
  - Holder of certificate is no longer authorized (e.g., employee is terminated)
  - Other situations when CAL ISO must revoke the certificate
- Refer to the specific CPSs for a complete description of rights and obligations

PKI Supporting System

- Certificate Authority Hierarchy
- Certificate Revocation List
- Directory Server

A Possible Certificate Infrastructure



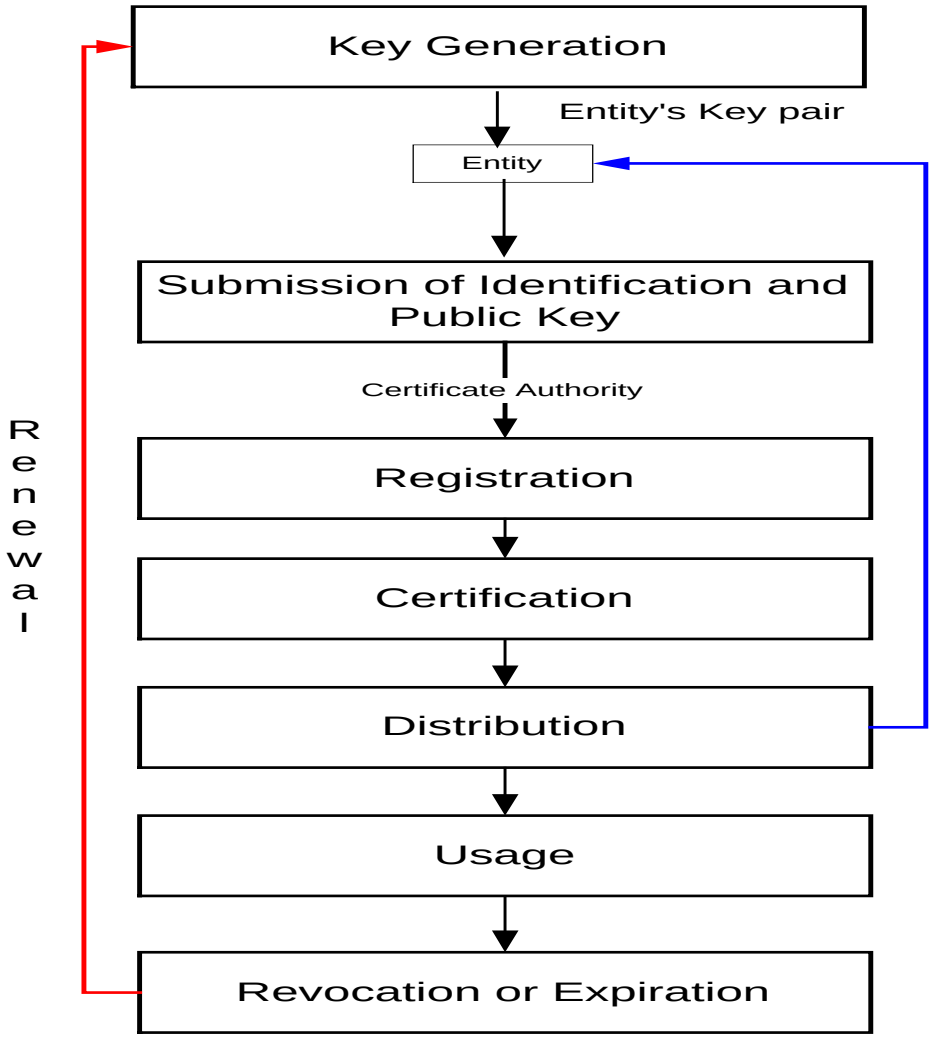
Certificate Revocation List

- A listing of public key certificates which are no longer valid
- Typically placed in public directories so that applications may check the revocation status of a certificate before trusting
- Examples
  - Expired
  - Explicitly revoked due to termination

Directory Server

- Central repository used to store information
  - For example: PKI certificates
- Information is made publicly available for consumption
- Based on X.500/LDAP standard
  - X.500 directories are hierarchical with different levels for each category of information, such as country, state, and city
  - Lightweight Directory Access Protocol is a set of protocols for accessing information directories

Certificate and Key Life Cycles



Implementing PKI

- Three pillars of a production PKI
  - Architecture
  - Certificate Policy
  - Certification Practice Statement
- One needs to treat the PKI as an *entire* system rather than individual pieces
- One must remain flexible
  - Migratory paths
  - Technology meeting operational requirements

PKI Requirements: Scalability and Usability of PKI

- Scalability
  - Number *objects* in supported by the
    - Certificates
    - CAs
    - RAs
- Usability
  - Different types of certificates
    - Authentication and key agreement
    - Nonrepudiation
    - Attribute
    - Data encipherment

PKI Requirements: Operational Impact

- Initial keys and certificates for all Individuals
- On-going renewal of keys and certificates
- Prompt notification in the event of a key compromise

PKI Requirements: Performance and Application Impact

- Minimal performance impact
- Little or no change to the user interface of applications
- No software development for existing applications
- Transparent software deployment for existing applications

Some Current CA Vendors

- Baltimore Technologies
- GTE Cybertrust (Enterprise and Outsource)
- Entrust
- Microsoft Certificate Server
- Netscape Certificate and Directory Servers
- VeriSign (Outsource Only)
- Certicom
- Spyrus
- CertCo / Digital Signature Trust
- Valicert (Validation only)
- Xcert
- Frontier Technologies
- Thawte (Outsource Only)
- PGP

Certificate Aware Applications

- Web Browsers (Netscape, MS)
- Web Servers (MS IIS, Netscape, Apache, Lotus Domino)
- E-mail Clients (MS Outlook, Eudora, Lotus, etc.)

PKI Product Feature List

- Certificate Format
- CRL Format
- Naming Support (x.500)
- Redundant CAs (Cloning)
- Graceful CA Key Rollover
- Certificate and Key Management
- Multiple Keys/Certs Per Person
- Support for Standard Key Algorithms
- Key Recovery
- LDAP Interface
- Incremental CRL Support
- Hardware Cryptographic Support
- Scalability into 100s of 1000s
- Cross-Certification Support
- Attribute Certificate Support
- GUI Mgmt Tools
- GUI based RA Tools
- Elliptic Curve Support

PKI Issues

- Interoperability Between Vendors
- Key Recovery (Forgotten Password)
- Key Renewal
- Directory Schema
- Cross Domain Trust
- Certificate Aware Applications

- Standards in Transition
- Scalability
- Reliability
- Cost

PKI Good News-Bad News

Good News

- Strong Authentication
- Non-repudiation
- Highly Portable
- Privacy over the Internet

Bad News

- Physical Protection of CA
- Initial User Identification
- Standards in Transition

Bottom-Line: Good News outweighs Bad News.

More info

- **http://selva.dit.upm.es/~pepe/catalogo/pki.htm -** Comprehensive listing of all kinds of PKI links
- **http://www.labcal.com -** “25 Steps to the Sucessful Implementation of a Corporate PKI”
- **http://csrc.nist.gov/pki/welcome.html -** US Federal Government PKI Resource Page
- **http://www.verisign.com/ -** Verisign’s Web Page