CRYPTOGRAPHY AND ENCRYPTION (CY 371)

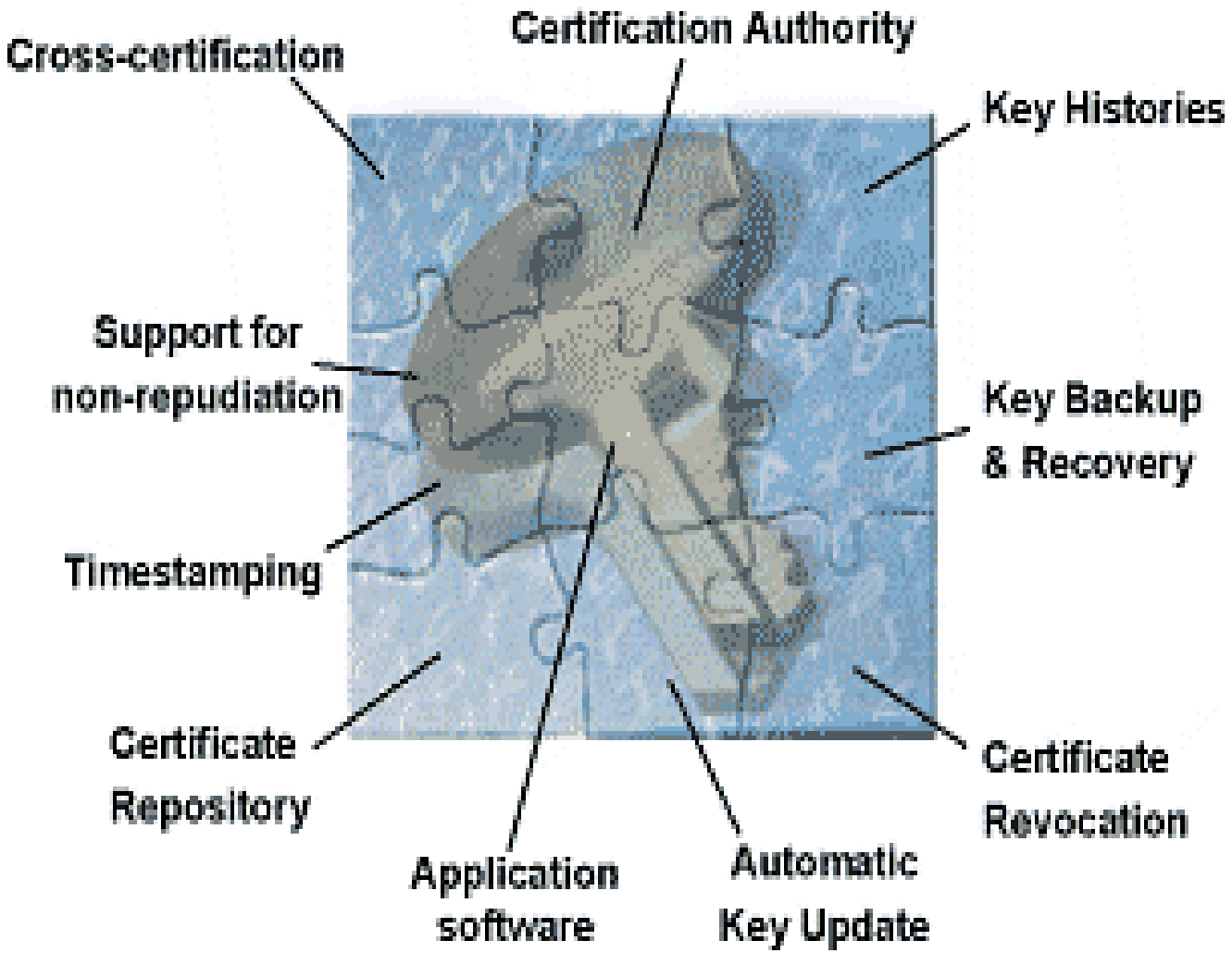
Dr Eric Affum

What is Public Key Infrastructure? (also known as PKI)

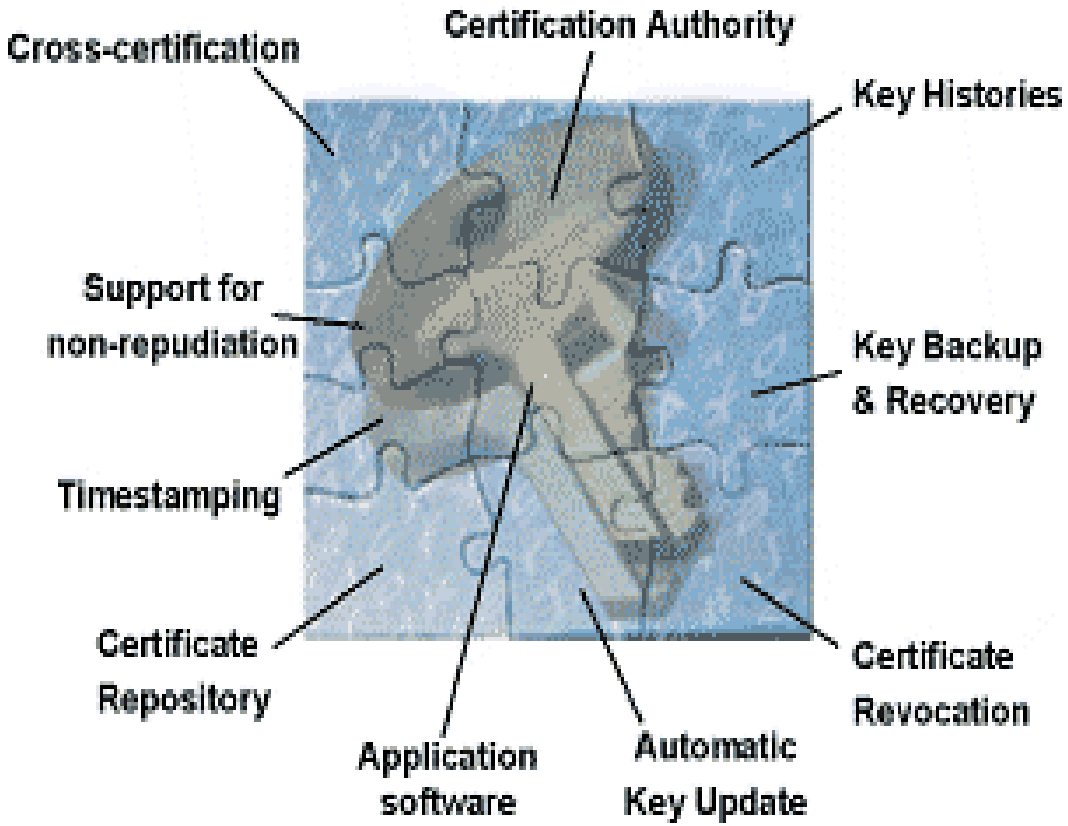
- Technology that enables users to securely and privately exchange data over an unsecured medium without the loss of integrity or confidentiality

- Also manages how user and network resources are identified and given access to online information and services

Functions and Components of PKI

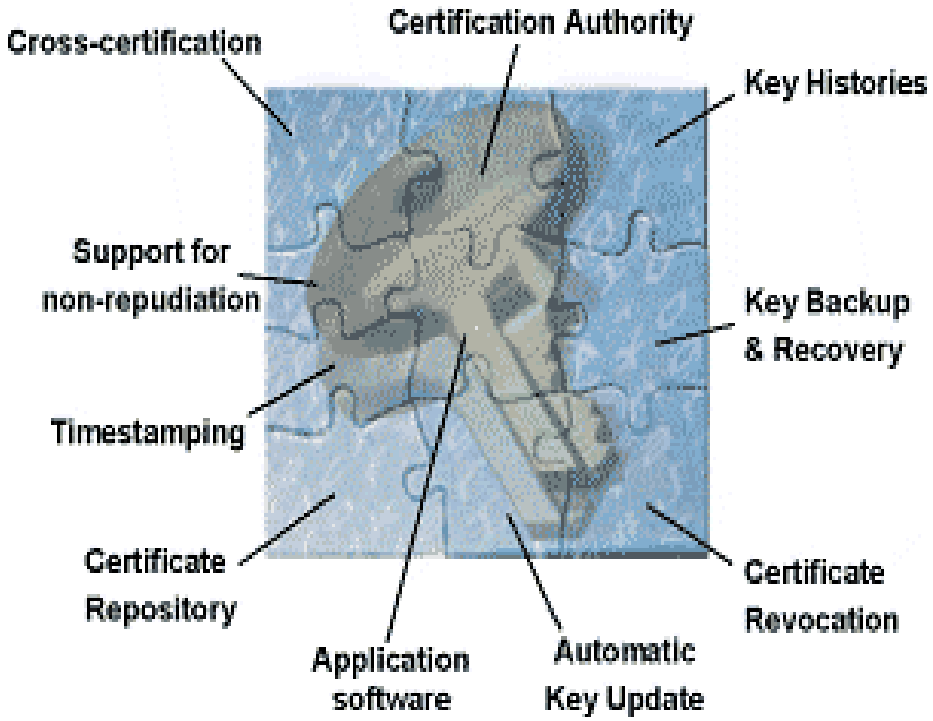


Functions and Components of PKI



- Certification authority (CA)
- Registration authority (RA)
- PKI clients
- Digital certificates
- Certificate Distribution System or repository
- Keys (Public and Private)

Functions of PKI (cont.)

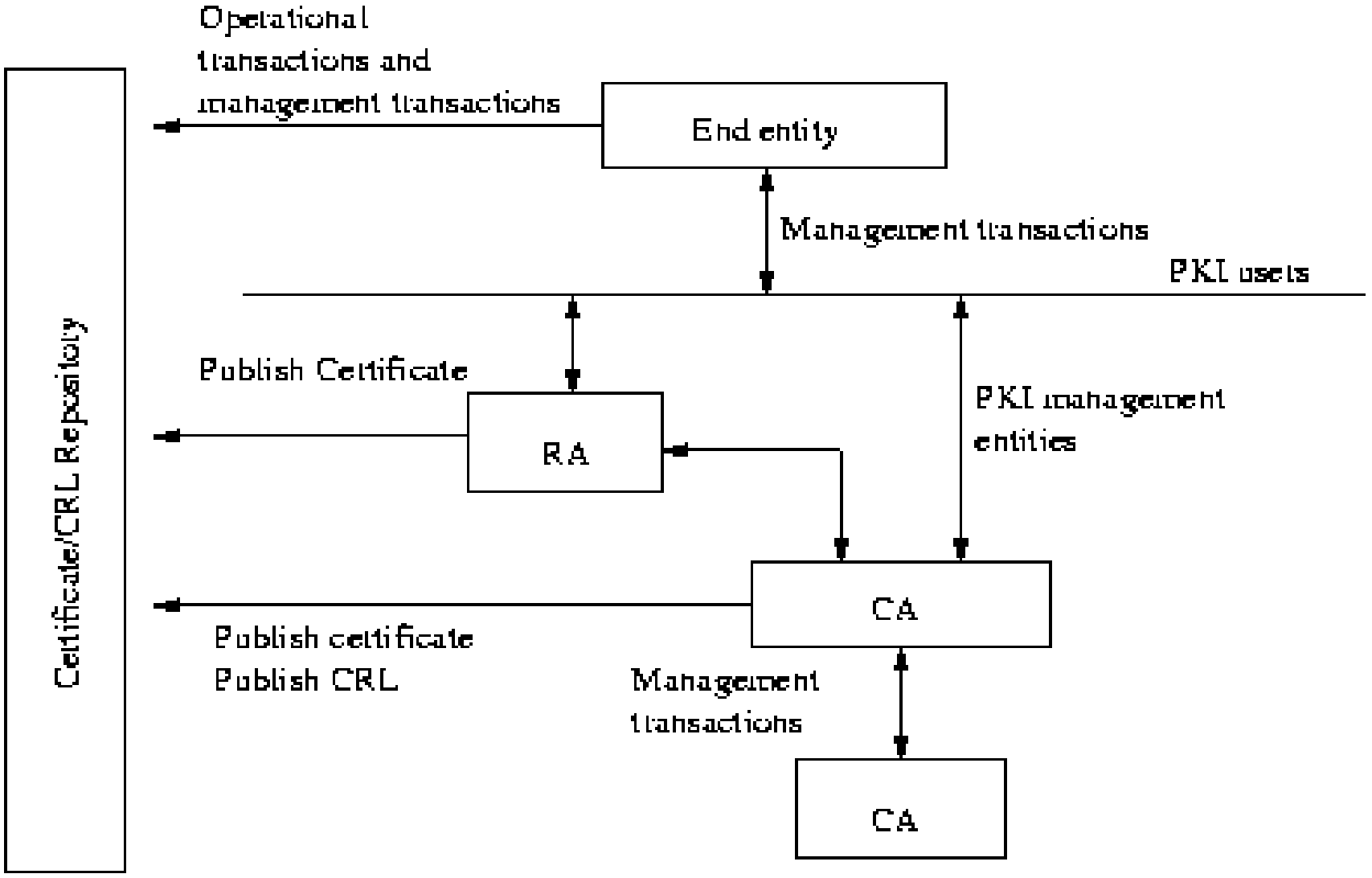


- Certificate Requests
- Certificate Revocation
- Client to Client Interaction
- Timestamping
- Non-repudiation
- Cross-certification

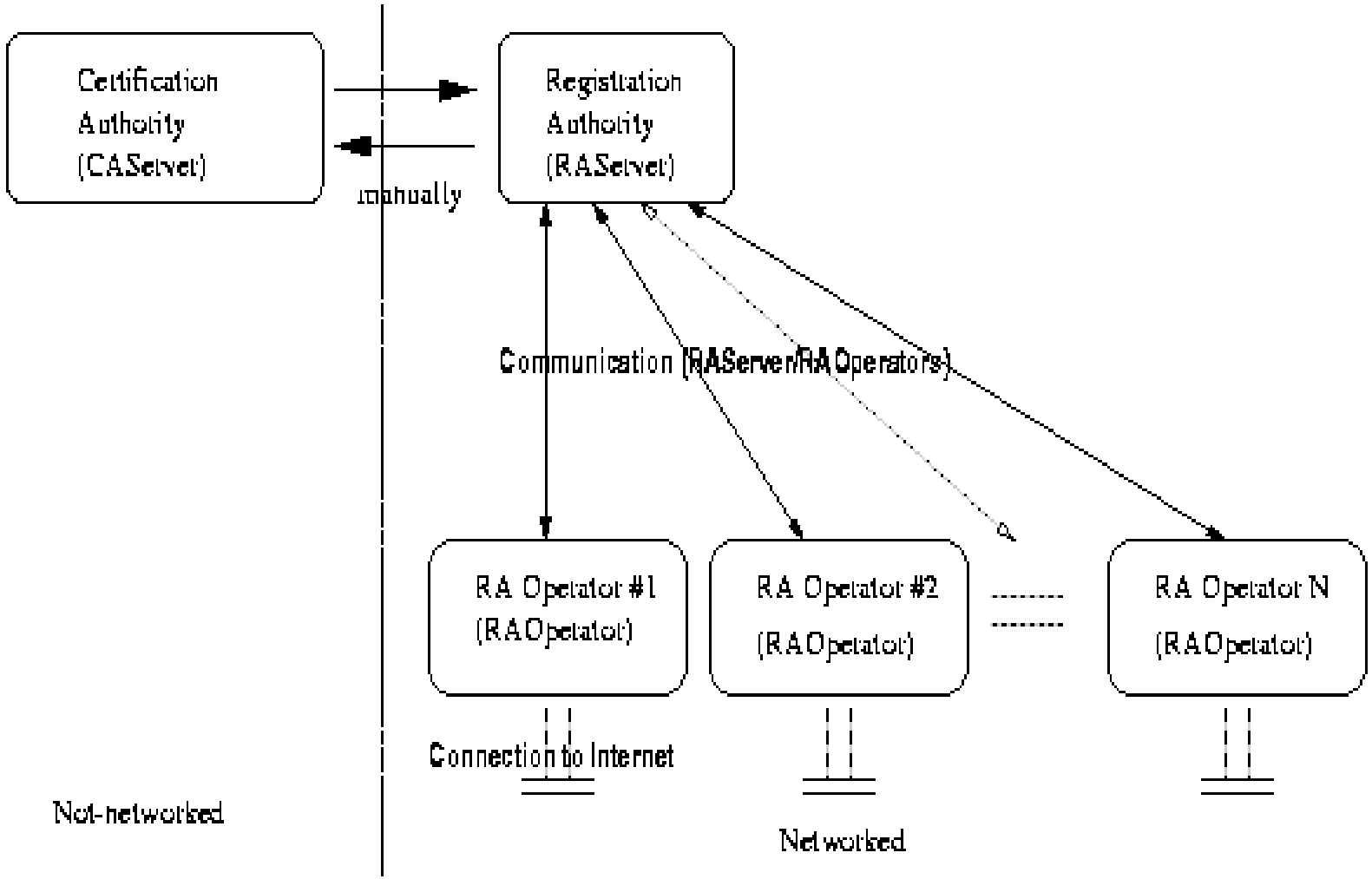
How does PKI work?

- Entities
  - Host A, B
  - RA, CA
- Objects
  - Public Keys for all entities
  - Private Keys for all entities
  - Digital Certificate
  - Hash Function
  - Message

PKI Entities

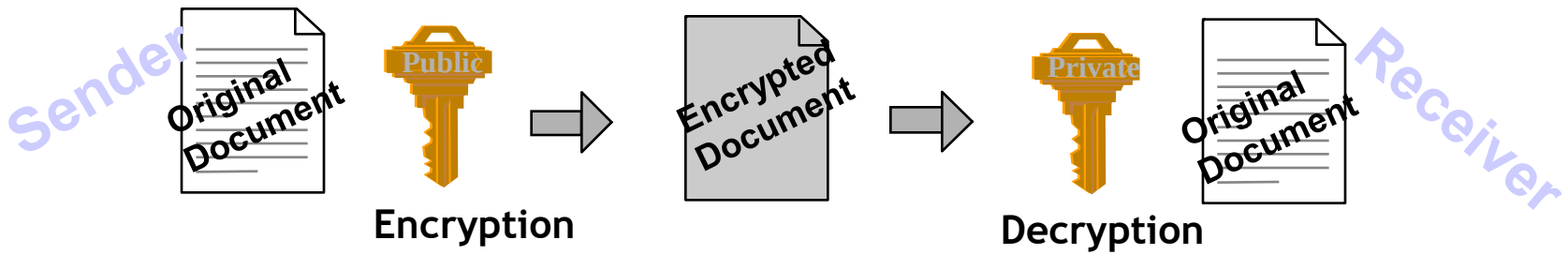


Example of Certificate Request and Distro Architecture



Public Key Cryptography

- **Public-Key Cryptography is an encryption scheme that uses mathematically related, but not identical keys.**
- **Each user has a key pair (public key/private key).**

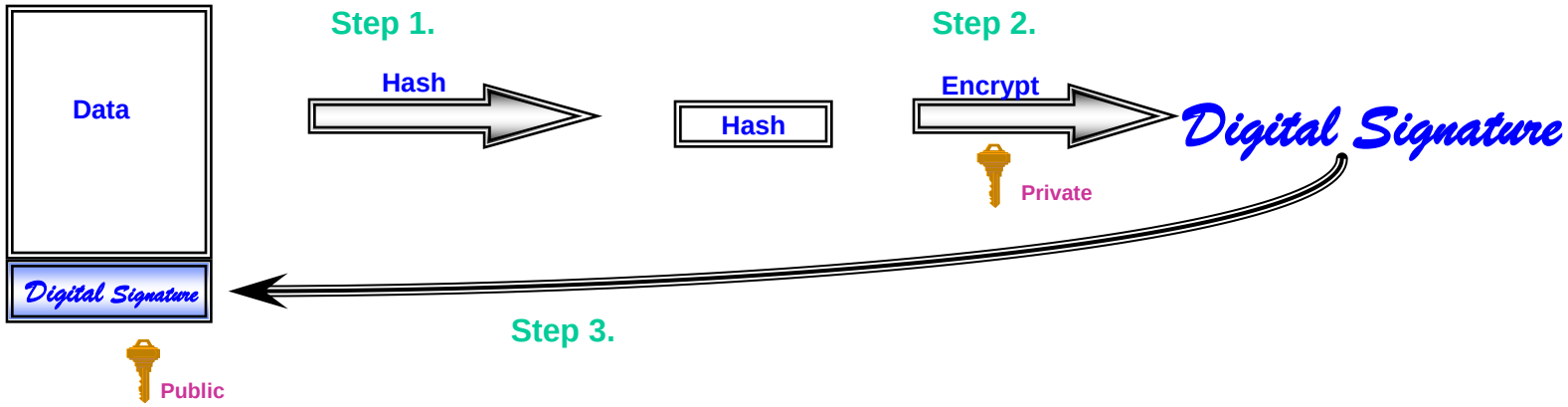


  - **Information encrypted with the public key can only be decrypted using the private key.**

What is a Digital Signature ?

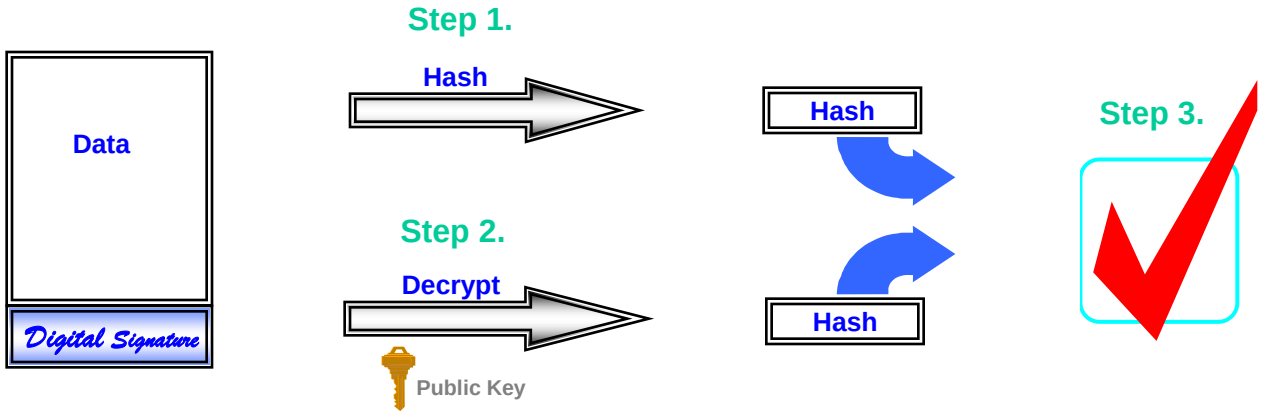
- A Digital Signature is the result of encrypting the Hash of the data to be exchanged.
- A Hash (or Message Digest) is the process of mathematically reducing a data stream down to a fixed length field.
- The Hash uniquely represents the original data.
- The probability of producing the same Hash with two sets of different data is <.001%.
- Signature Process is opposite to Encryption Process
  - Private Key is used to Sign (encrypt) Data
  - Public Key is used to verify (decrypt) Signature

Digital Signature Process



- Step 1. Hash (digest) the data using one of the supported Hashing algorithms, e.g., MD2, MD5, or SHA-1.
- Step 2. Encrypt the hashed data using the sender's private key.
- Step 3. Append the signature (and a copy of the sender's public key) to the end of the data that was signed.

Signature Verification Process



- Step 1. Hash the original data using the same hashing algorithm.
- Step 2. Decrypt the digital signature using the sender's public key. All digital signatures contain a copy of the signer's public key.
- Step 3. Compare the results of the hashing and the decryption. If the values match then the signature is verified. If the values do not match, then the data or signature was probably modified in transit.

The Critical Questions

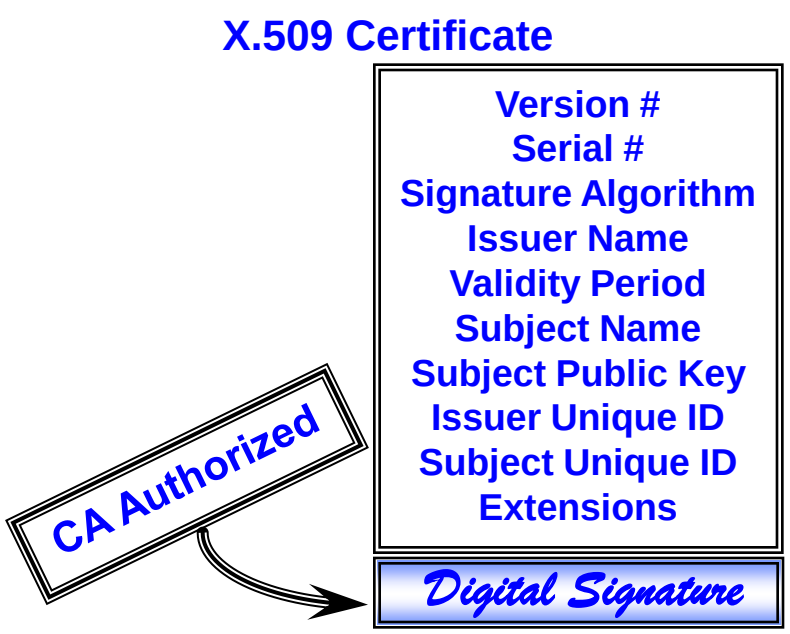
- How can the recipient know with certainty the sender's public key? (to validate a digital signature)
- How can the sender know with certainty
  the recipient's public ke[illegible] send an encrypted message)

Digital Certificates

- **Before two parties exchange data using Public Key cryptography, each wants to be sure that the other party is authenticated**
- Before B accepts a message with A's Digital Signature, B wants to be sure that the public key belongs to A and not to someone masquerading as A on an open network
- One way to be sure, is to use a trusted third party to authenticate that the public key belongs to A. Such a party is known as a Certification Authority (CA)
- Once A has provided proof of identity, the Certification Authority creates a message containing A's name and public key. This message is known as a Digital Certificate.

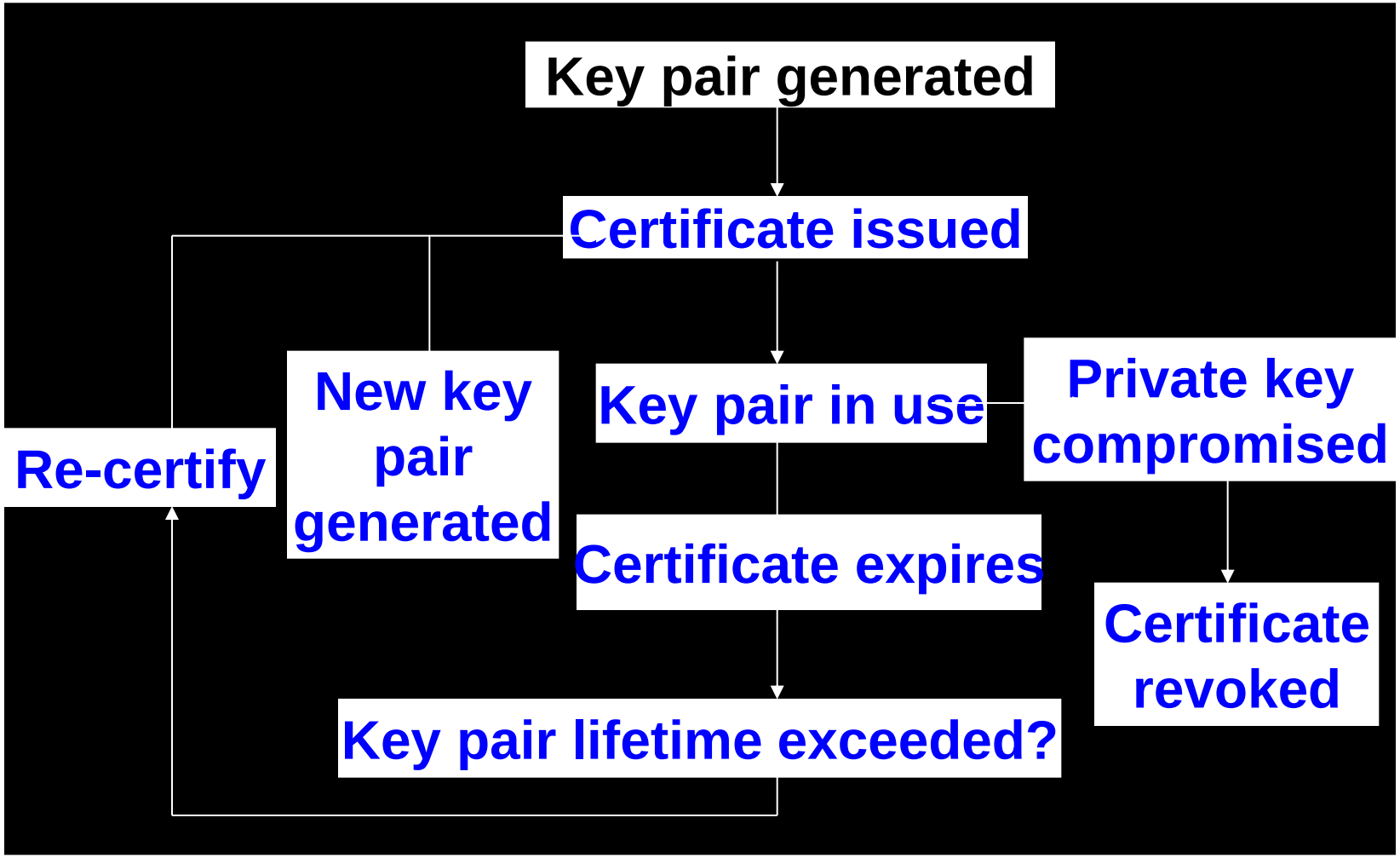
Digital Certificates

- A Digital Certificate is simply an X.509 defined data structure with a Digital Signature. The data represents who owns the certificate, who signed the certificate, and other relevant information



- When the signature is generated by a Certification Authority (CA), the signature can be viewed as trusted.
- Since the data is signed, it can not be altered without detection.
- Extensions can be used to tailor certificates to meet the needs of end applications.

Certificate Life Cycle



Certificate Revocation Lists

- CA periodically publishes a data structure called a certificate revocation list (CRL).
- Described in X.509 standard.
- Each revoked certificate is identified in a CRL by its serial number.
- CRL might be distributed by posting at known Web URL or from CA's own X.500 directory entry.

PKI Players

- Registration Authority (RA) to identity proof users
- Certification Authorities (CA) to issue certificates and CRL's
- Repositories (publicly available databases) to hold certificates and CRLs

Certification Authority (CA)

Certification Authority

- Trusted (Third) Party
- Enrolls and Validates Subscribers
- Issues and Manages Certificates
- Manages Revocation and Renewal of Certificates
- Establishes Policies & Procedures

What's Important

- Operational Experience
- High Assurance Security Architecture
- Scalability
- Flexibility
- Interoperability
- Trustworthiness

Certification Authority = Basis of Trust

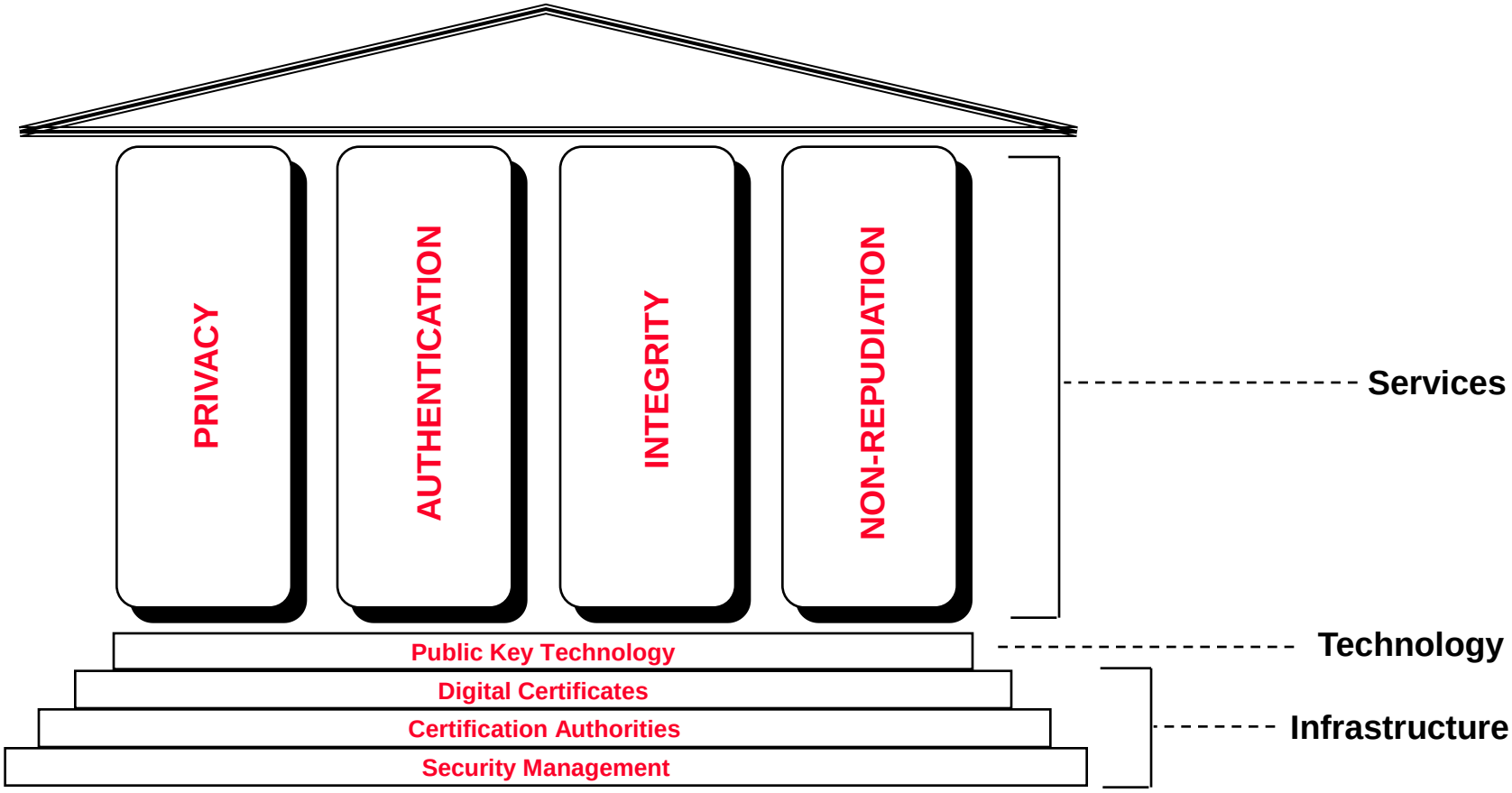
Registration Authority (RA)

- Enrolling, de-enrolling, and approving or rejecting requested changes to the certificate attributes of subscribers.
- Validating certificate applications.
- Authorizing requests for key-pair or certificate generation and requests for the recovery of backed-up keys.
- Accepting and authorizing requests for certificate revocation or suspension.
- Physically distributing personal tokens to and recovering obsolete tokens from people authorized to hold and use them.

Certificate Policy (CP) is …

- the basis for trust between unrelated entities
- not a formal “contract” (but implied)
- a framework that both informs and constrains a PKI implementation
- a statement of what a certificate means
- a set of rules for certificate holders
- a way of giving advice to Relying Parties

Public Key Security



- Public Key Technology Best Suited to Solve Business Needs
- Infrastructure = Certification Authorities

Authentication/Access Control

- **Can Public Key Technology be used to perform Authentication and Access Control?**

Sure Can

How?

Using Digital Signatures and Digital Certificates

SSL Protocol

- **Secure Socket Layer (SSL) is a Network Layer protocol used to secure data on TCP/IP networks.**