CYS401: Fundamentals of Cybersecurity

Lecture 6.2:

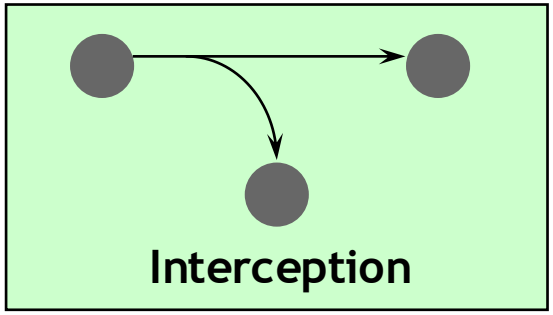
Public Key Infrastructure
and Applications

Agenda

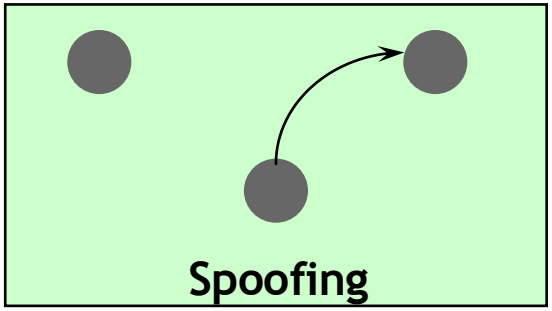
- PKI Overview
- Digital Signatures
  - What is it?
  - How does it work?
- Digital Certificates
- Public Key Infrastructure
  - PKI Components
  - Policies

Multiple Security Issues

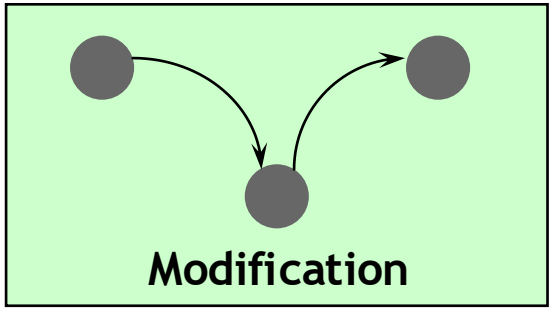
Privacy



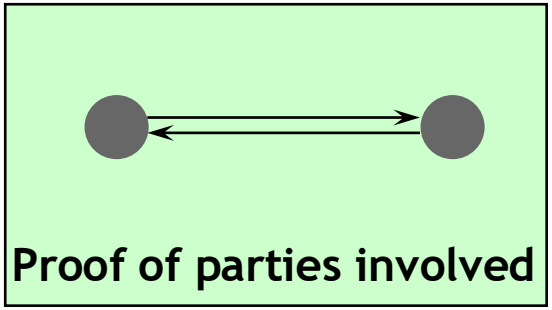
Authentication



Integrity



Non-repudiation

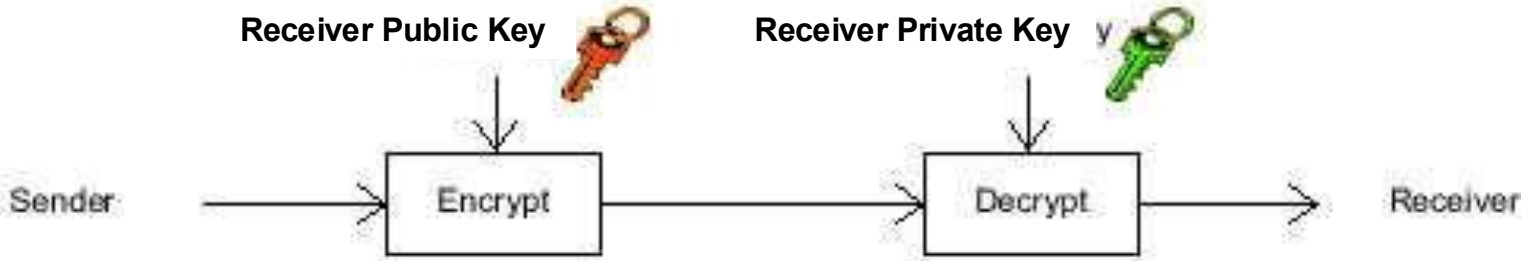


The Critical Questions

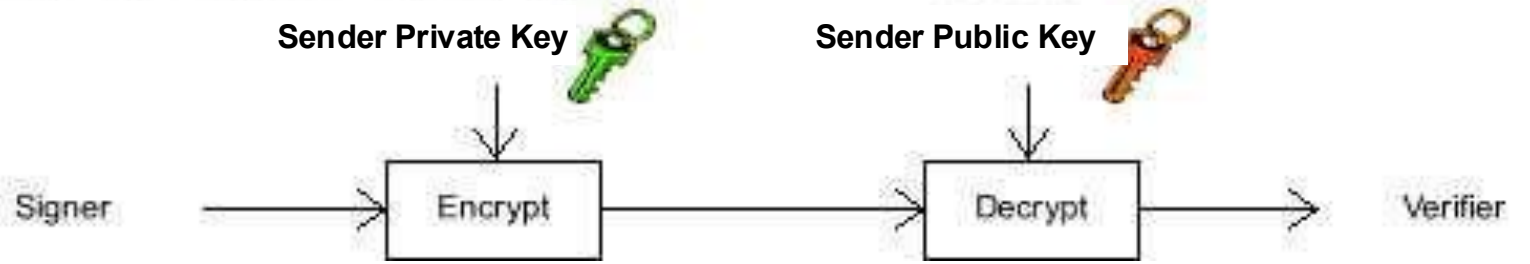
- How can the recipient know with certainty the sender's public key? (to validate a digital signature)
- How can the sender know with certainty the recipient's public key? (to send an encrypted message)

A - Private or symmetric key cryptography

B - Public or asymmetric key cryptography

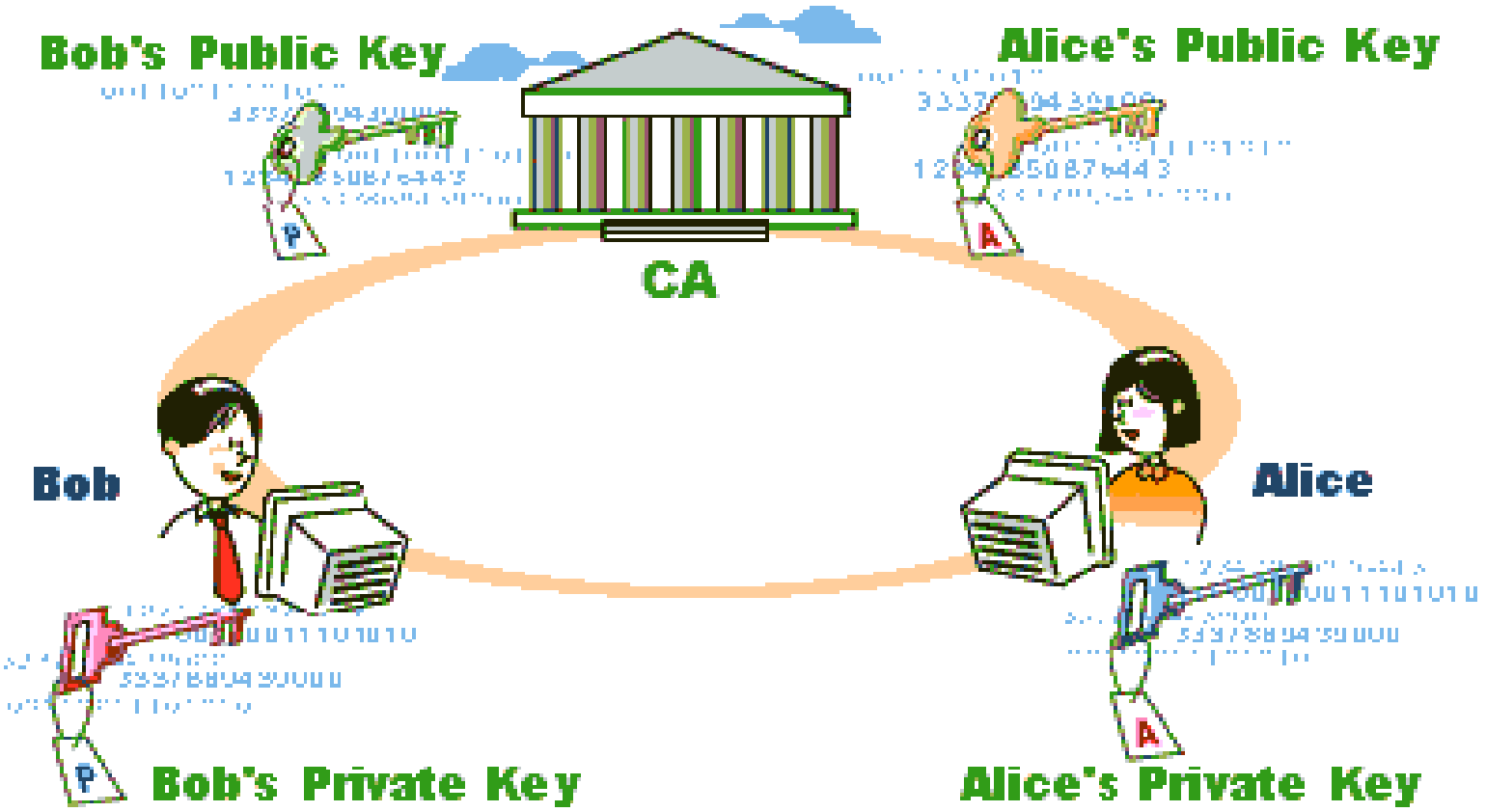


C - Signing using public key cryptography



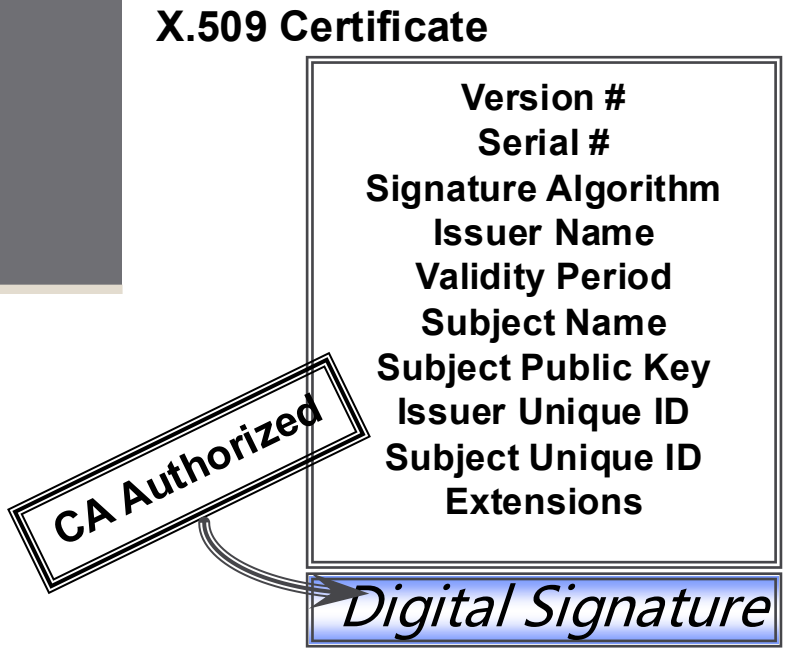
Digital Certificates

- 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**.


Bob's Public Key
Alice's Public Key
CA
Bob
Alice
Bob's Private Key
Alice's Private Key

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

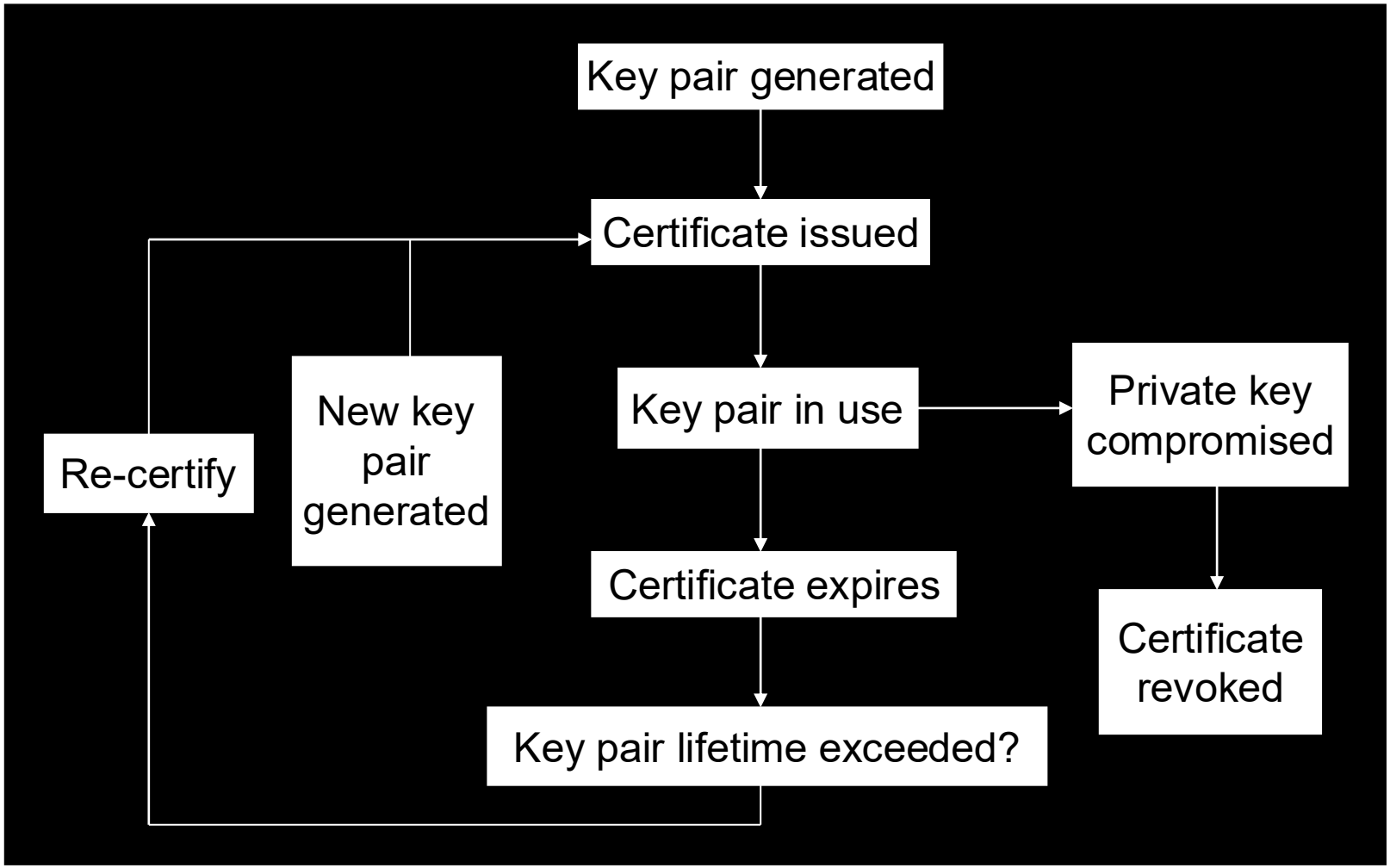


- When the signature is generated by a Certification Authority (CA), the signature can be viewed as trusted.
- Since the data is signed, it can not be altered without detection.
- Extensions can be used to tailor certificates to meet the needs of end applications.

Certificate Life Cycle

Three states for cert.

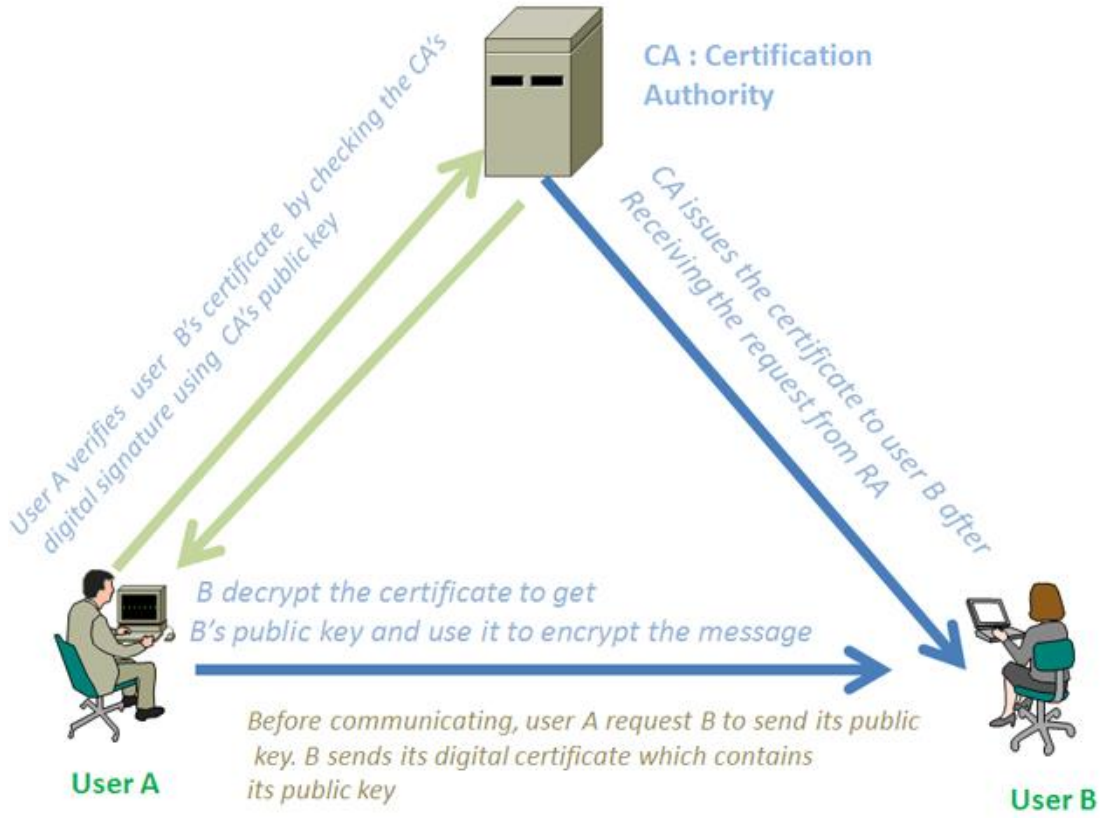
- **In use**
- **Revoked**
- **Expired**



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.

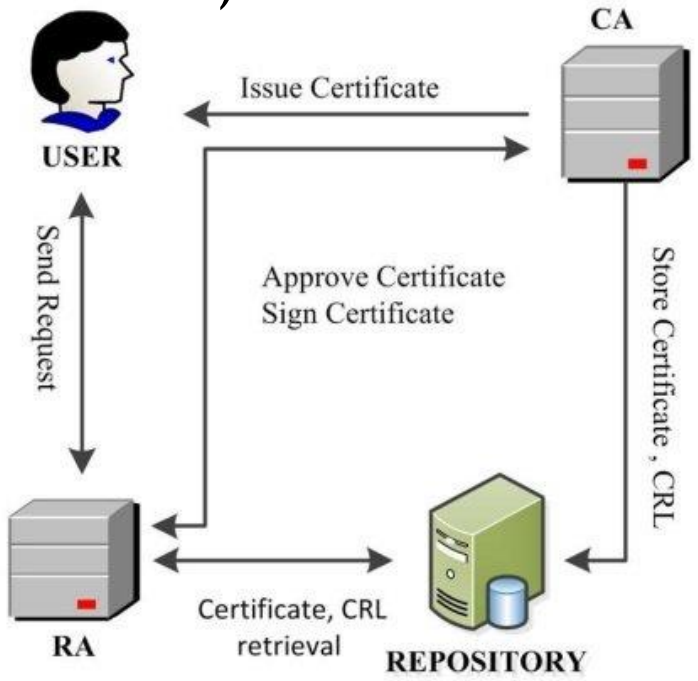
DC in reality



Simplified diagram: Secure communication with digital certificate

PKI Players

- Registration Authority (RA) to prove the user's identity& approve the policies.
- 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

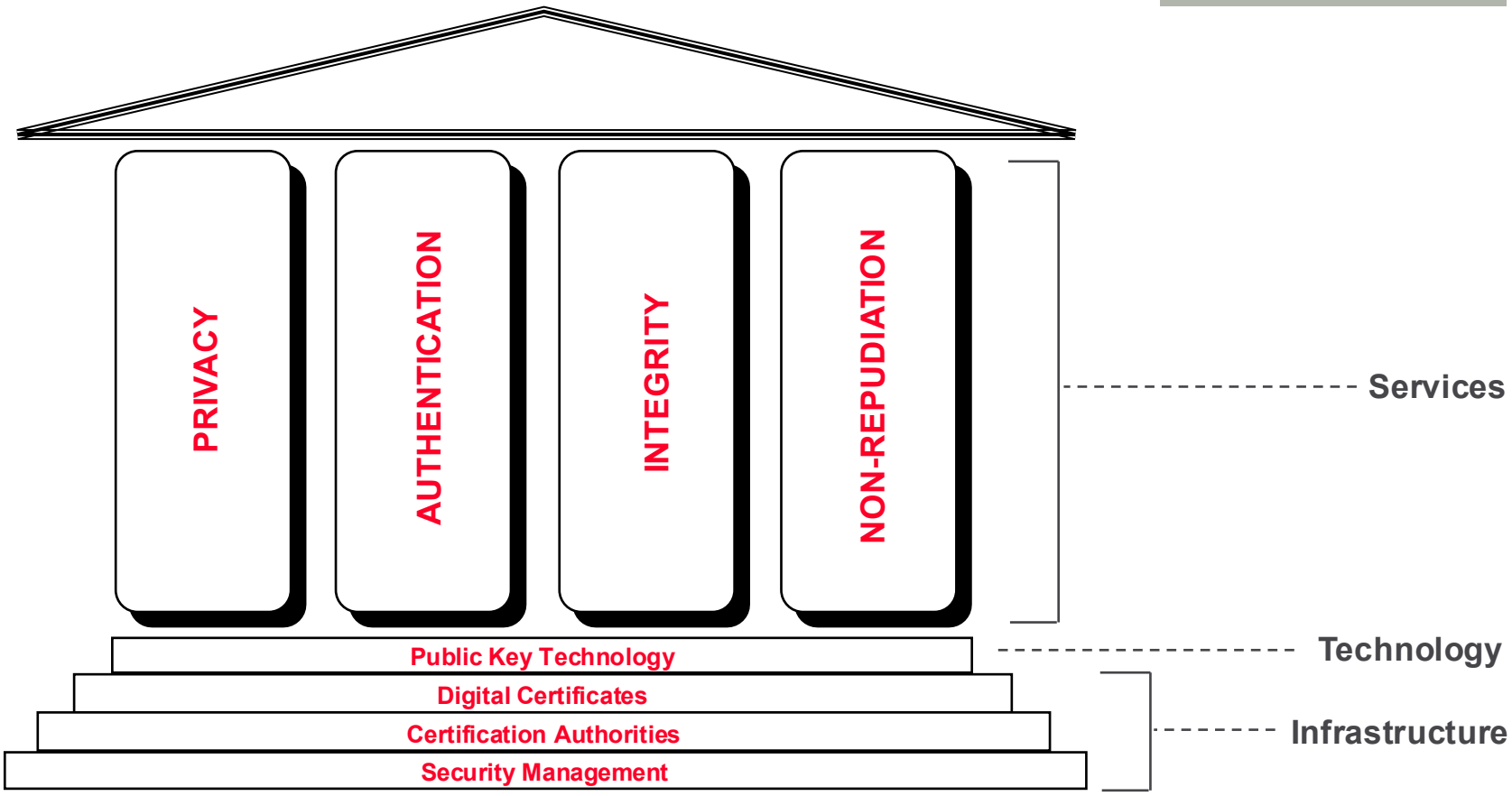
Registration Authority (RA)

- 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 …

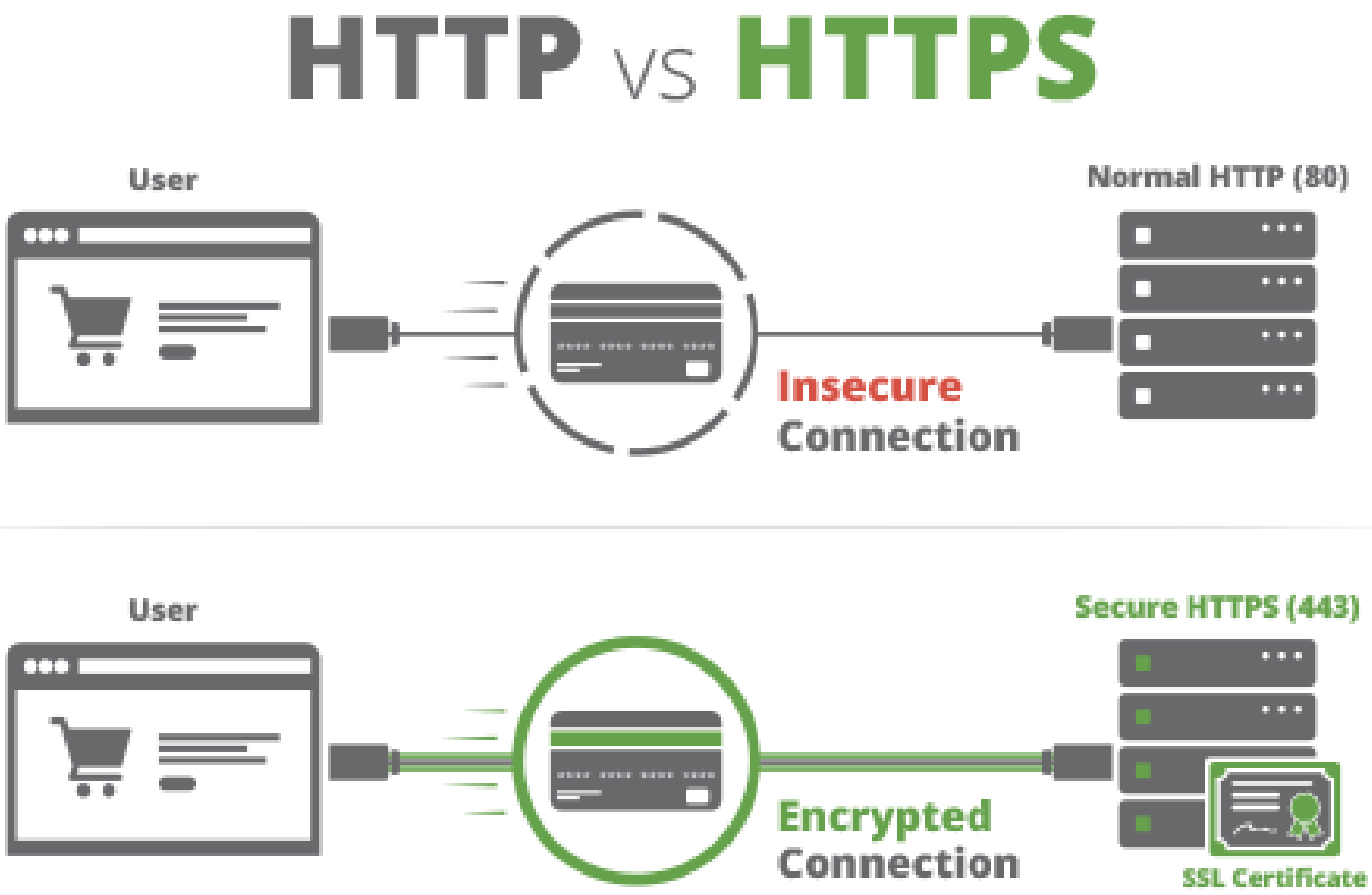
- the basis for trust between unrelated entities
- not a formal “contract” (but implied)
- a framework that both informs and constrains a PKI implementation
- a statement of what a certificate means
- a set of rules for certificate holders
- a way of giving advice to Relying Parties

Public Key Security

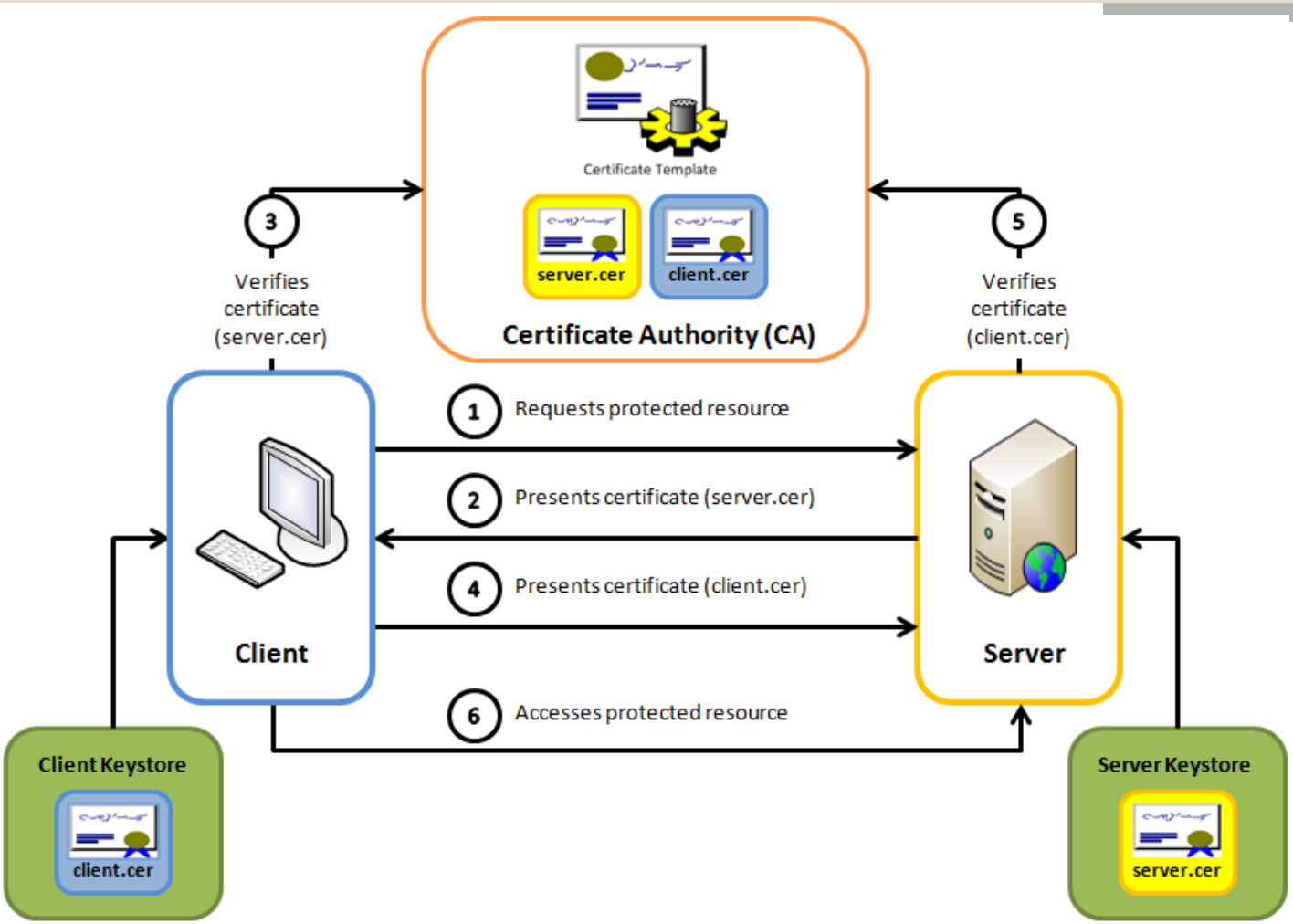


- Public Key Technology Best Suited to Solve Business Needs
- Infrastructure = Certification Authorities

Certificate and SSL



Certificate and SSL



Mutual SSL authentication / Certificate based mutual authentication

The End…