CipherQuest

The *key* to security

New Tools for Broadcasters:

Certificates, Digital Signatures & Certification Authorities

Michael Garceau

Agenda

- Business Need
- Principles of Cryptography
- Public Key Infrastructure
- X.509v3 Certificates
- How it Works
- Challenges

Business Need

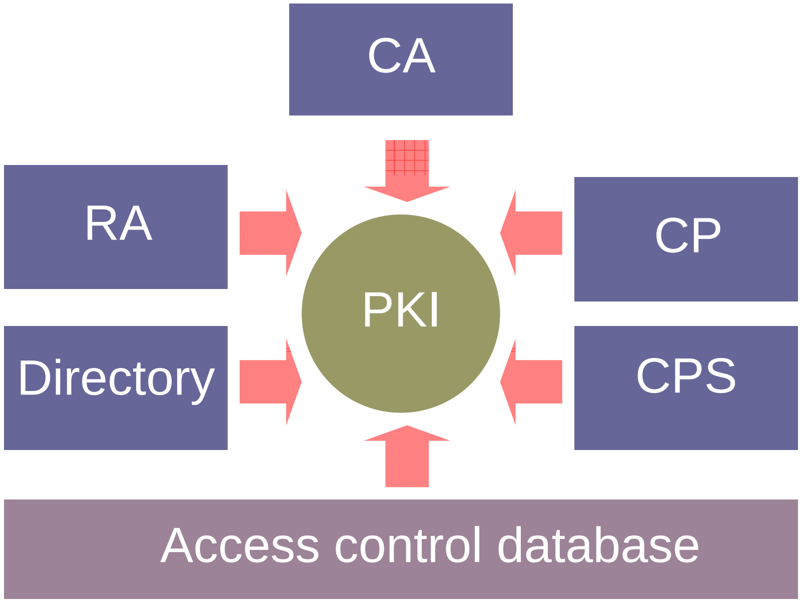
- *Identity/Integrity* - mechanisms that enable a business or individual to establish the identity of the other party to the extent necessary to *accept* the risk of doing business, that support the underlying business processes and that confirm that important information has not been tampered with.
- *Asset protection/IPR/Ownership* - as the value of a business is increasingly vested in information assets in electronic form, mechanisms need to be in place to prevent those assets being forged, stolen, or otherwise compromised.
- *Secrecy* - the need to conceal from those not authorized sensitive commercial, personal or other information in electronic form.

Based on Cryptography

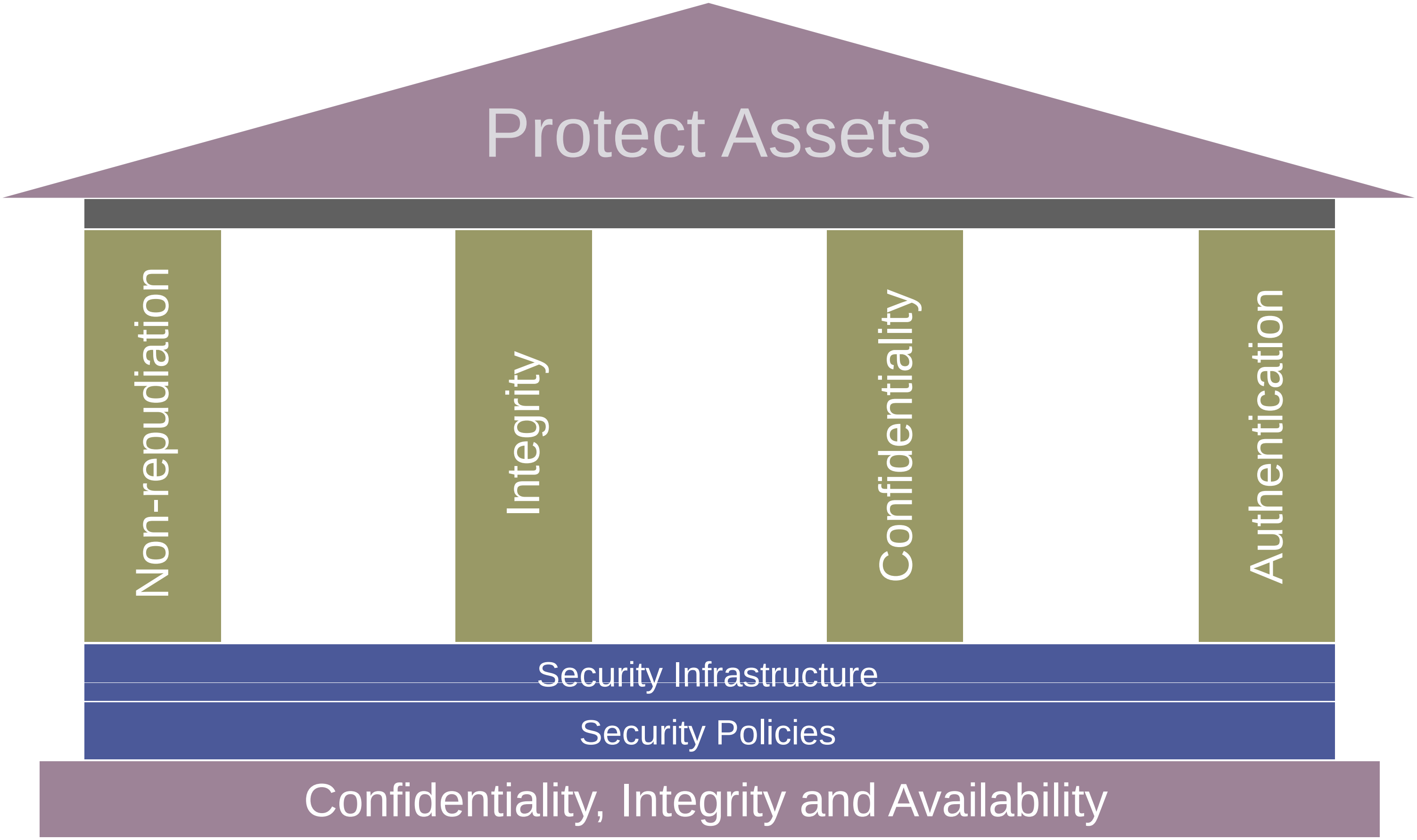
- The science of converting the original message “plain-text” into a scrambled message “cipher-text”
- Based on symmetric and asymmetric cryptography
  - Symmetric cryptography protects the data (confidentiality) -- referred to as a session key
  - Asymmetric cryptography (public key cryptography) provides authentication, integrity and digital signature -- consists of a public and private key pair
- Binding of a key pair to an entity provided by a digital certificate
- Certificates issued and managed by the PKI

Public Key Infrastructure

- An infrastructure that provides a set of security services to protect application and network resources through cryptography and X.509v3 digital certificates.
- It includes people, policies, procedures, software, and hardware.
- Trust and security are paramount!

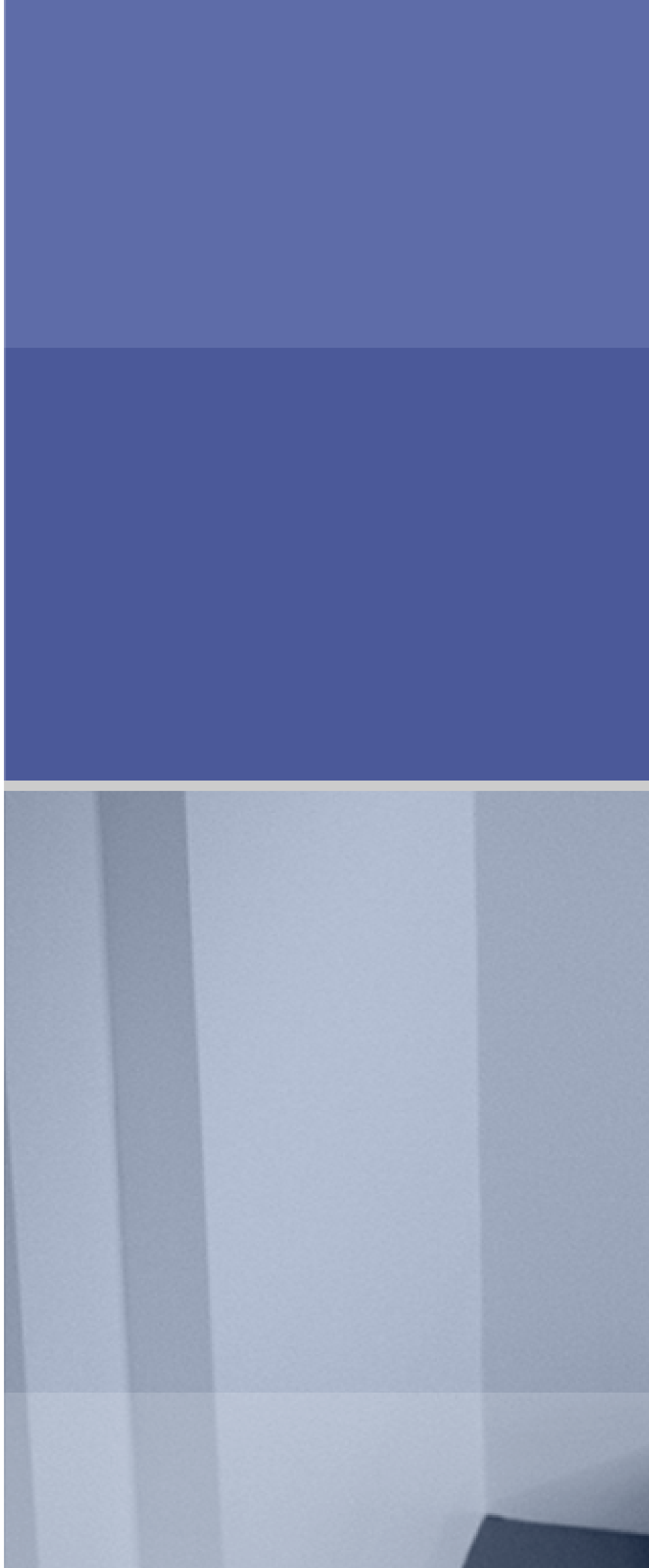


Security Services



Certification Authority

- Operates the Public Key Infrastructure
  - Authenticates users and distributes public keys
  - Issues certificates to authenticated individuals or organizations
  - Revokes certificates and maintains status
  - Provides directory/repository services
  - Optionally provides key generation, backup and recovery, token and smart-card initialization, and time-stamping
- Defines and embodies the trust policies for a community
  - Establish, publish, and follow sound practices to engender trust

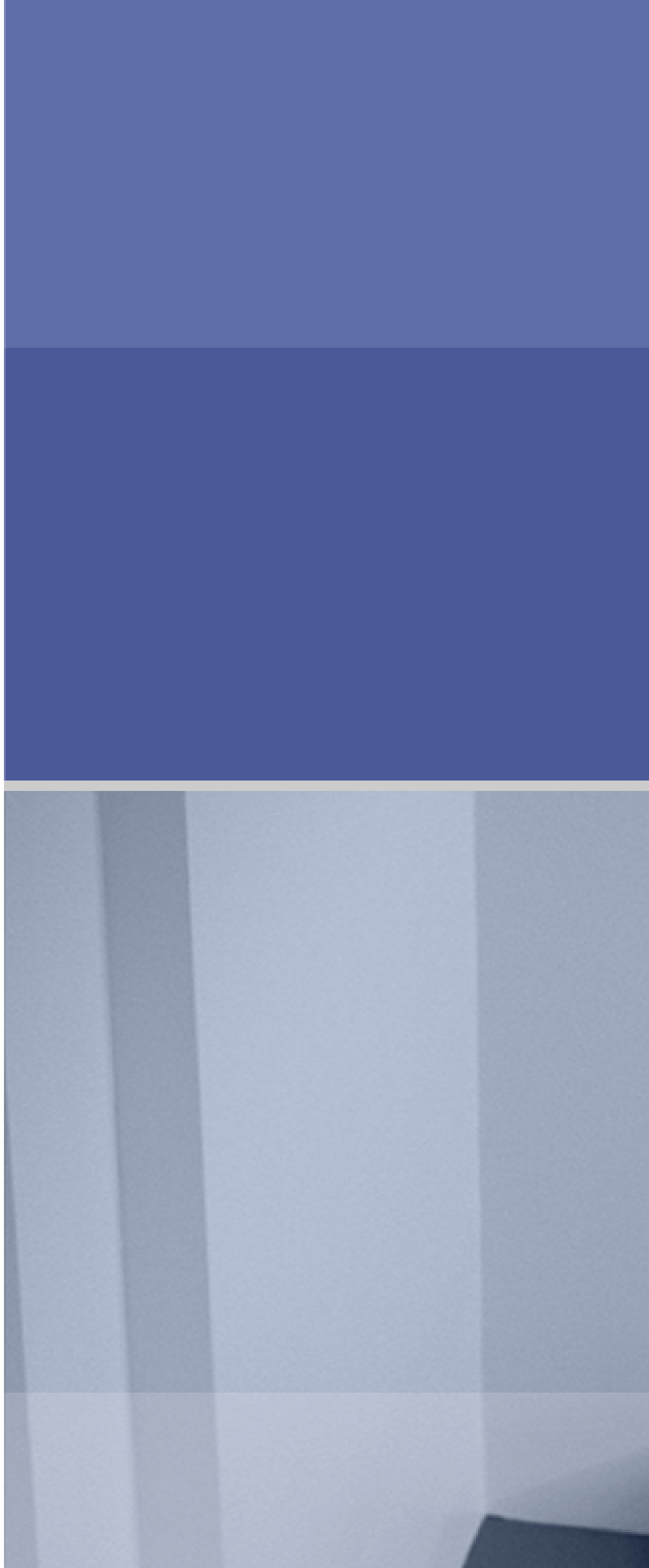


Registration Authority

- An entity that is delegated certain tasks by the CA such as identification and authentication of certificate subscribers, but does not sign or issue certificates
- Depending on the geographical distances between the issuing party (CA) and the business partner, the CA may delegate certain tasks to a Local Registration Authority (LRA)
  - LRAs are responsible for identification and authentication of their user community

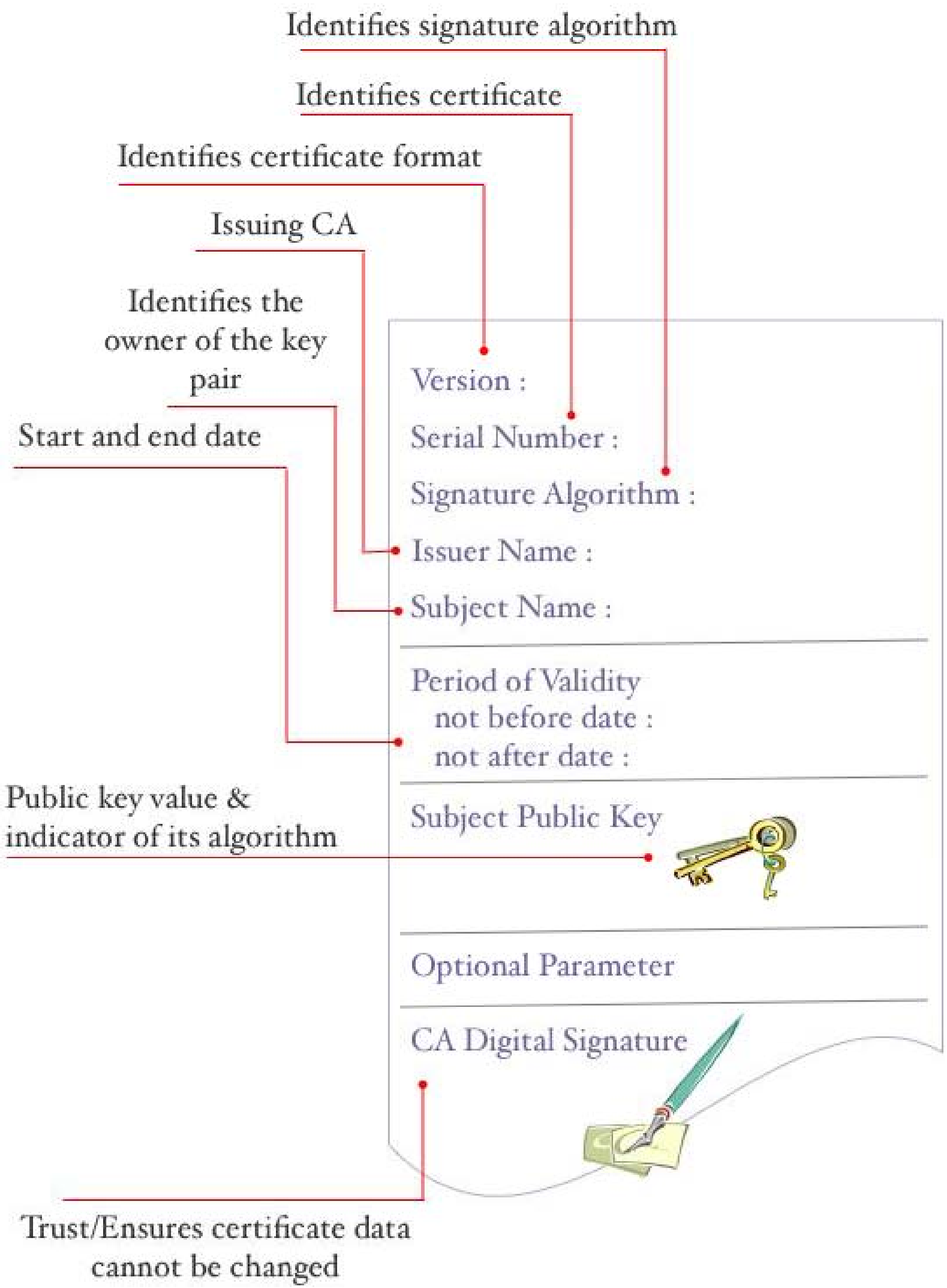
Directory

- A directory or repository is an online database used for
  - storing and distributing all public key certificates, information of certificate status (CRL) and other PKI related information
  - Broadening the certificate base of the PKI through Internet standards
  - Increasing the strength of legacy application authentication
- In order to work with a PKI, directories must
  - Support storage of X.509v3 certificates and CRLs
  - Support for Lightweight Directory Access Protocol (LDAP) for accessing directory information



Digital Certificate

- An electronic document that identifies an individual or entity through the binding of a name to a public and private key pair
- Contains relevant information
- Is notarized or validated by a trusted third party
- The entire digital record is digitally signed by the CA
- The CA's signature prevents tampering with any data in the certificate



Identifies signature algorithm

Identifies certificate

Identifies certificate format

Issuing CA

Identifies the owner of the key pair

Start and end date

Version :

Serial Number :

Signature Algorithm :

Issuer Name :

Subject Name :

Period of Validity
not before date :
not after date :

Public key value & indicator of its algorithm

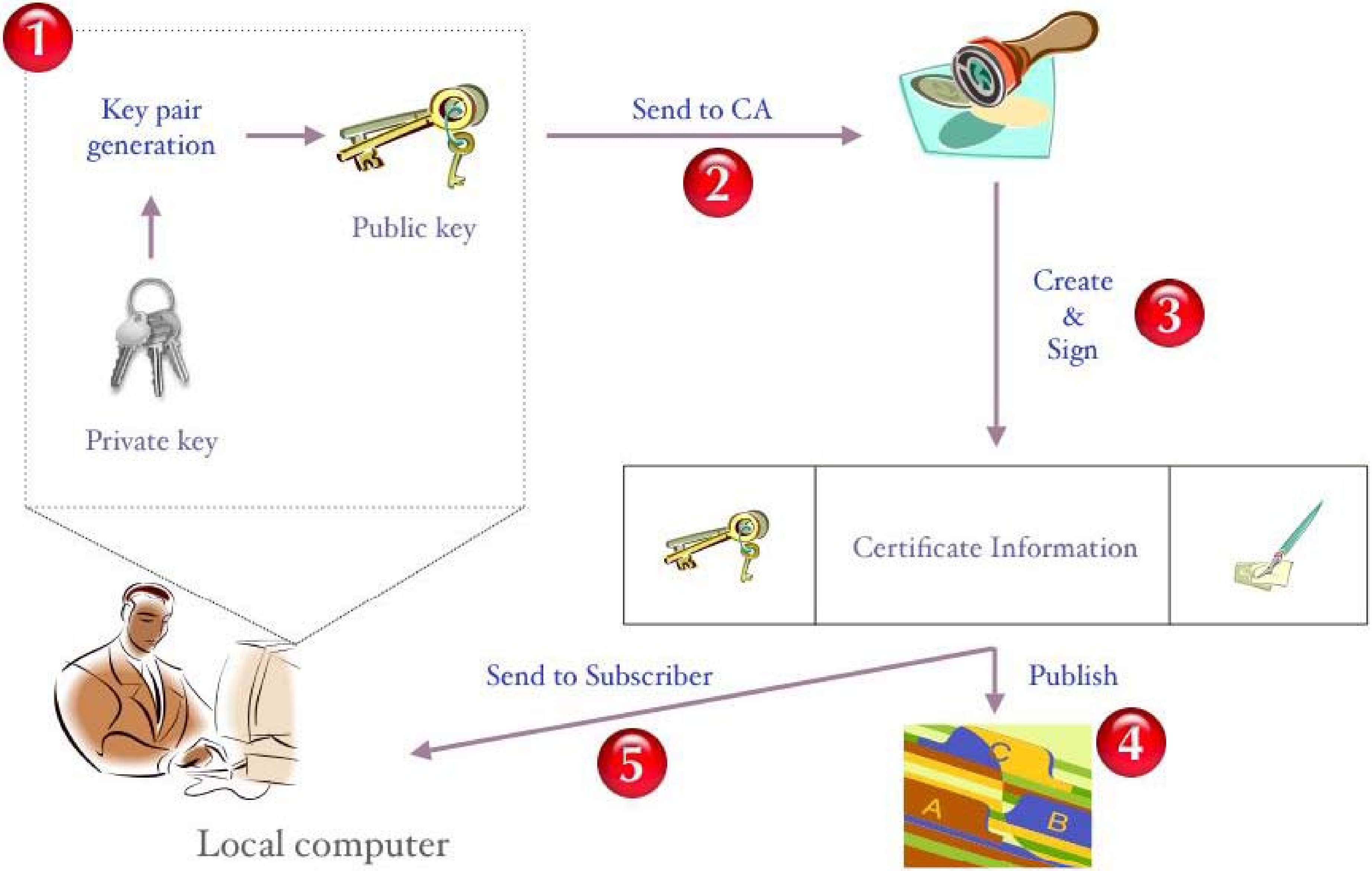
Subject Public Key

Optional Parameter

CA Digital Signature

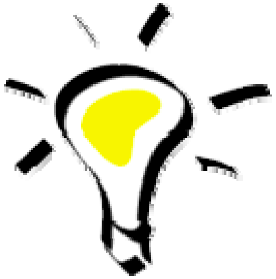
Trust/Ensures certificate data cannot be changed

Certificate Distribution

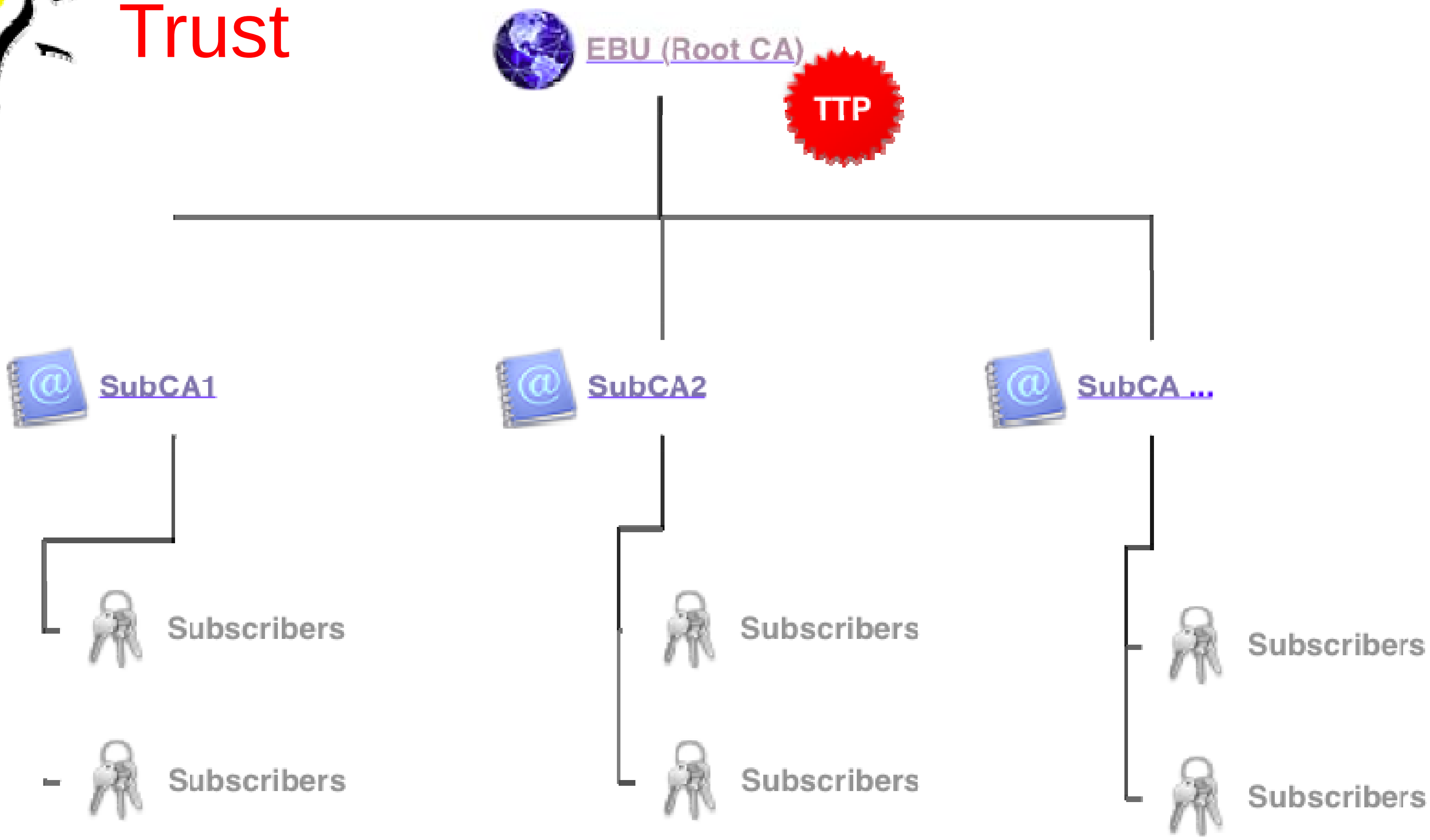


CipherQuest

Hierarchy CA



Trust



EBU (Root CA)

TTP

SubCA1

SubCA2

SubCA ...

Subscribers

Subscribers

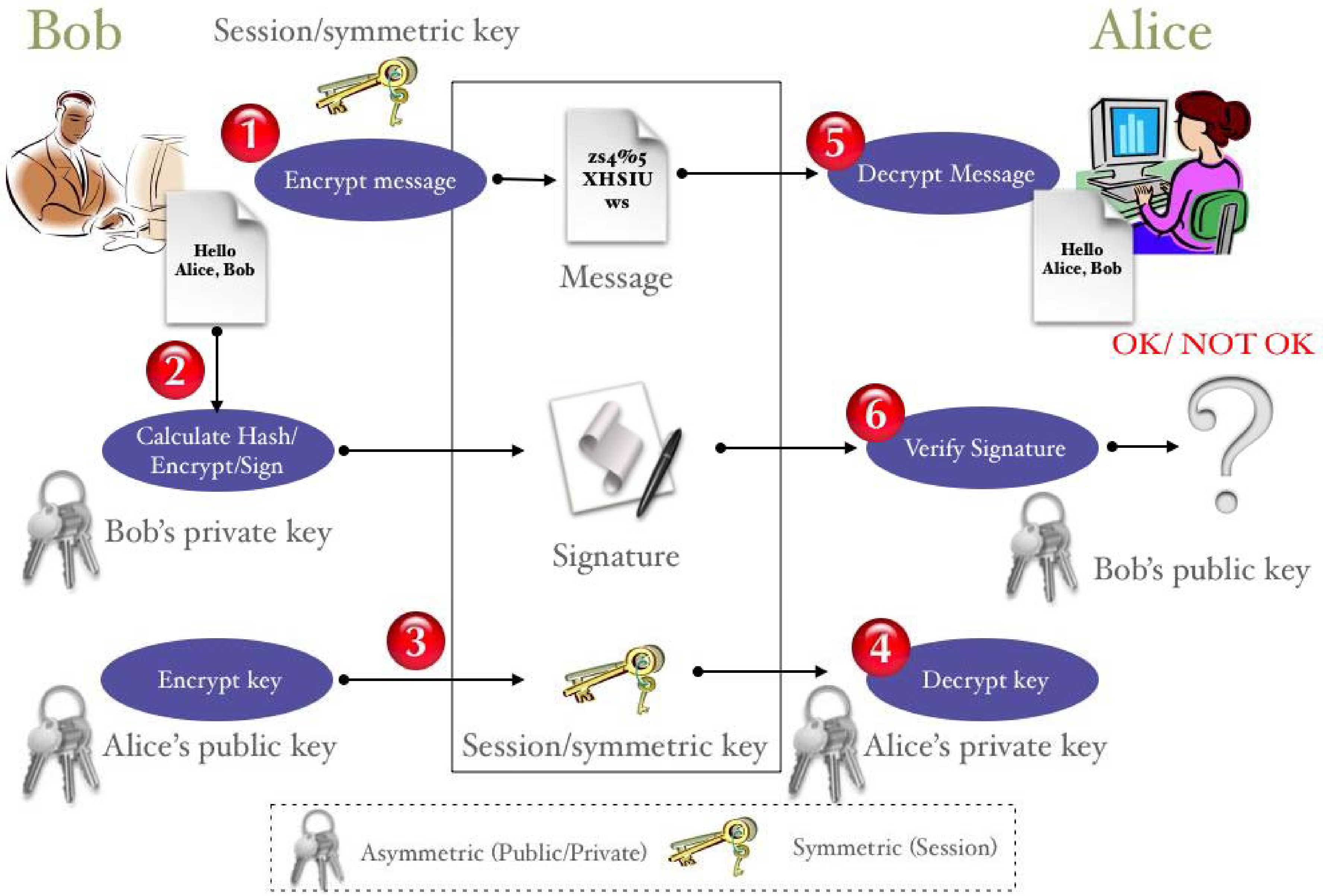
Subscribers

Subscribers

Subscribers

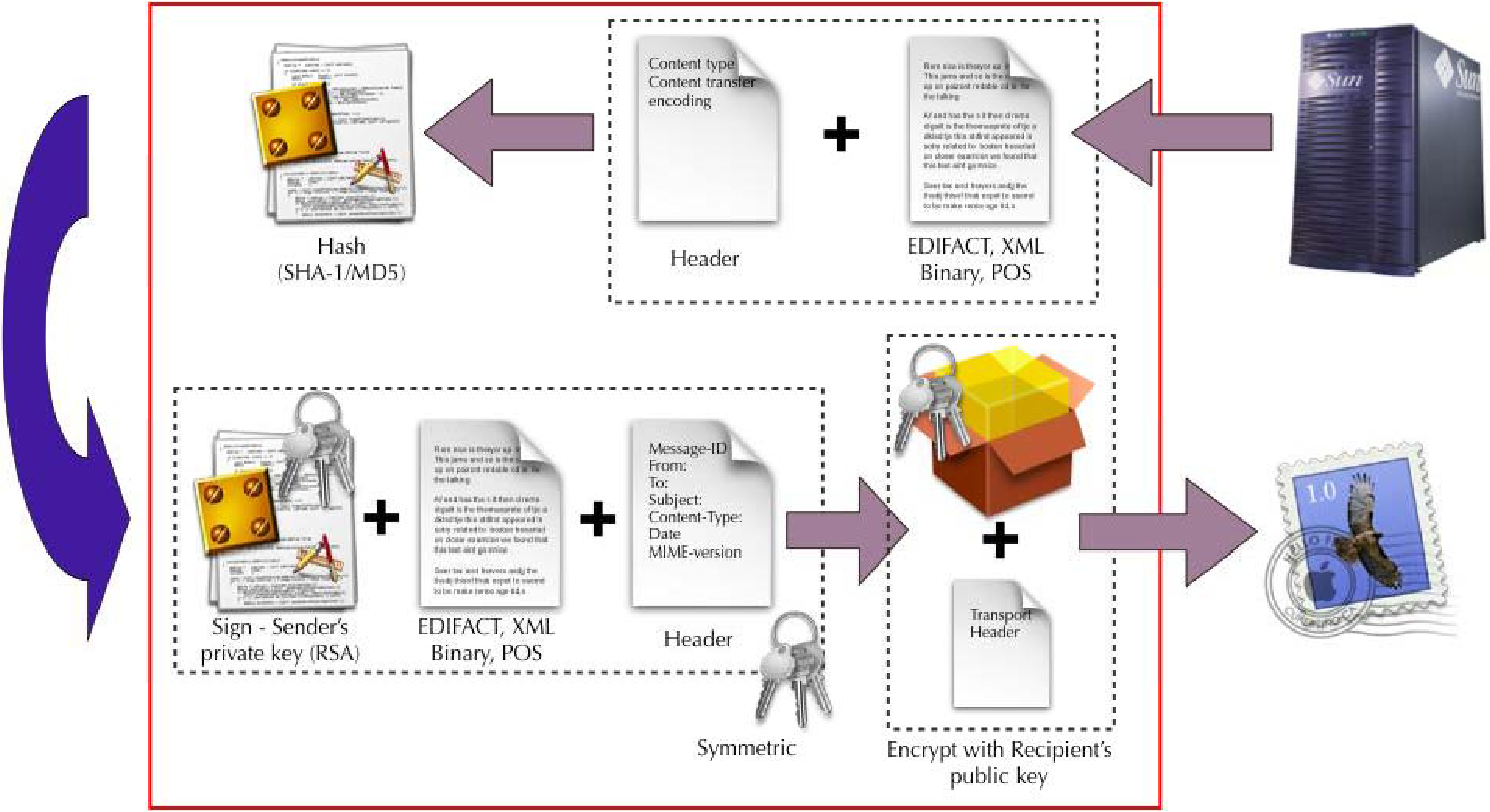
Subscribers

How it Works



CipherQuest

S/MIME



Hash
(SHA-1/MD5)

Content type
Content transfer
encoding

Header

EDIFACT, XML
Binary, POS

Sign - Sender's
private key (RSA)

EDIFACT, XML
Binary, POS

Message-ID
From:
To:
Subject:
Content-Type:
Date
MIME-version

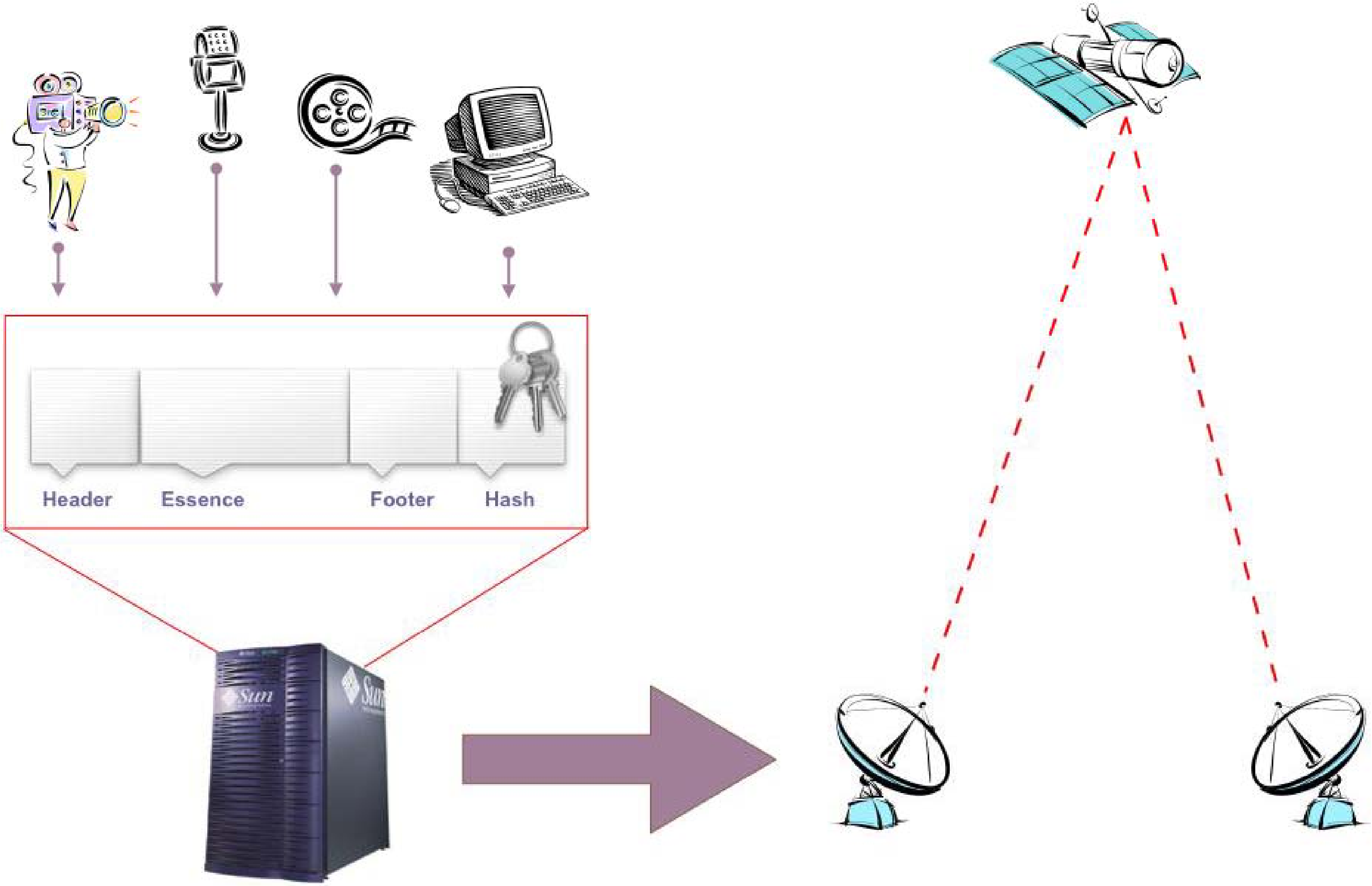
Header

Symmetric

Transport
Header

Encrypt with Recipient's
public key

Secure Communications



CipherQuest

Some Challenges

- Top-down commitment to security - awareness
- Policies, procedures and logistical considerations
- Message format and the need for security to protect assets - IPR and ownership
- Encryption and its impact on time sensitive data -- archiving

Thank you