Authentication, Authorization & Grid Security Infrastructure

Von Welch

Distributed Systems Laboratory

Univ. Of Chicago and Argonne National Laboratory

What do we want from security?

- Identity
- Authentication
- Privacy
- Integrity
- Authorization
- Single sign-on
- Delegation

Identity & Authentication

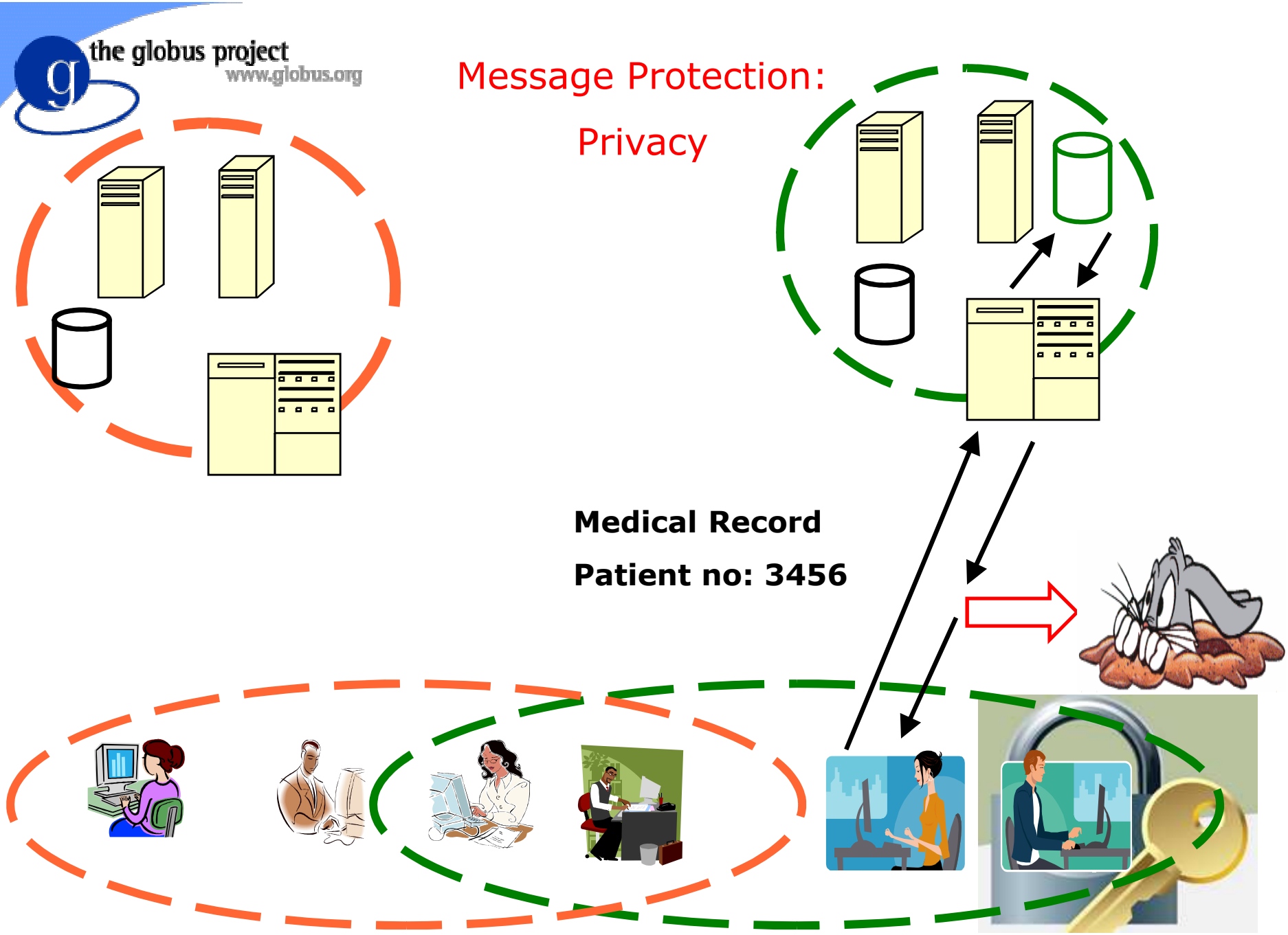
- Each entity should have an identity
  - Who are you?
  - Example: Unix login name
- Authentication:
  - Prove your identity
  - Stops masquerading imposters
- Examples:
  - Passport
  - Username and password

Message Protection

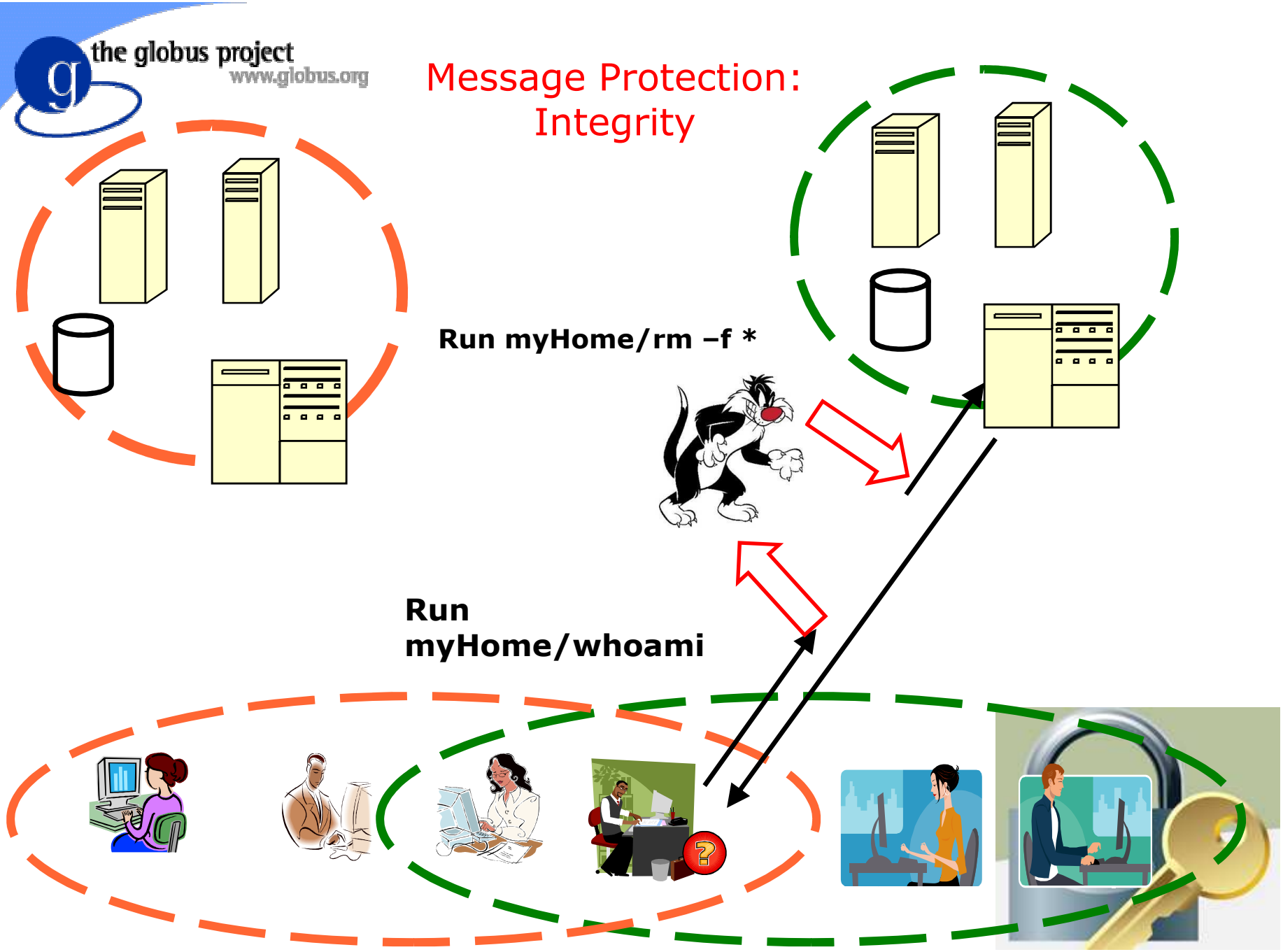
- Sending message securely
- Integrity
  - Detect whether message has been tampered
- Privacy
  - No one other than sender and receiver should be able to read message

Message Protection:

Privacy



Message Protection: Integrity



Authorization establishes rights to do actions

- Establishing rights
- What can a particular identity do?

Examples:

  - Are you allowed to read this file?
  - Are you allowed to run a job on this machine?
  - Unix read/write/execute permissions

- Must authenticate first
  - Authentication != authorization

Authorization

Examples:

- Are you allowed to be on this flight ?
  - Passenger ?
  - Pilot ?
- Unix read/write/execute permissions

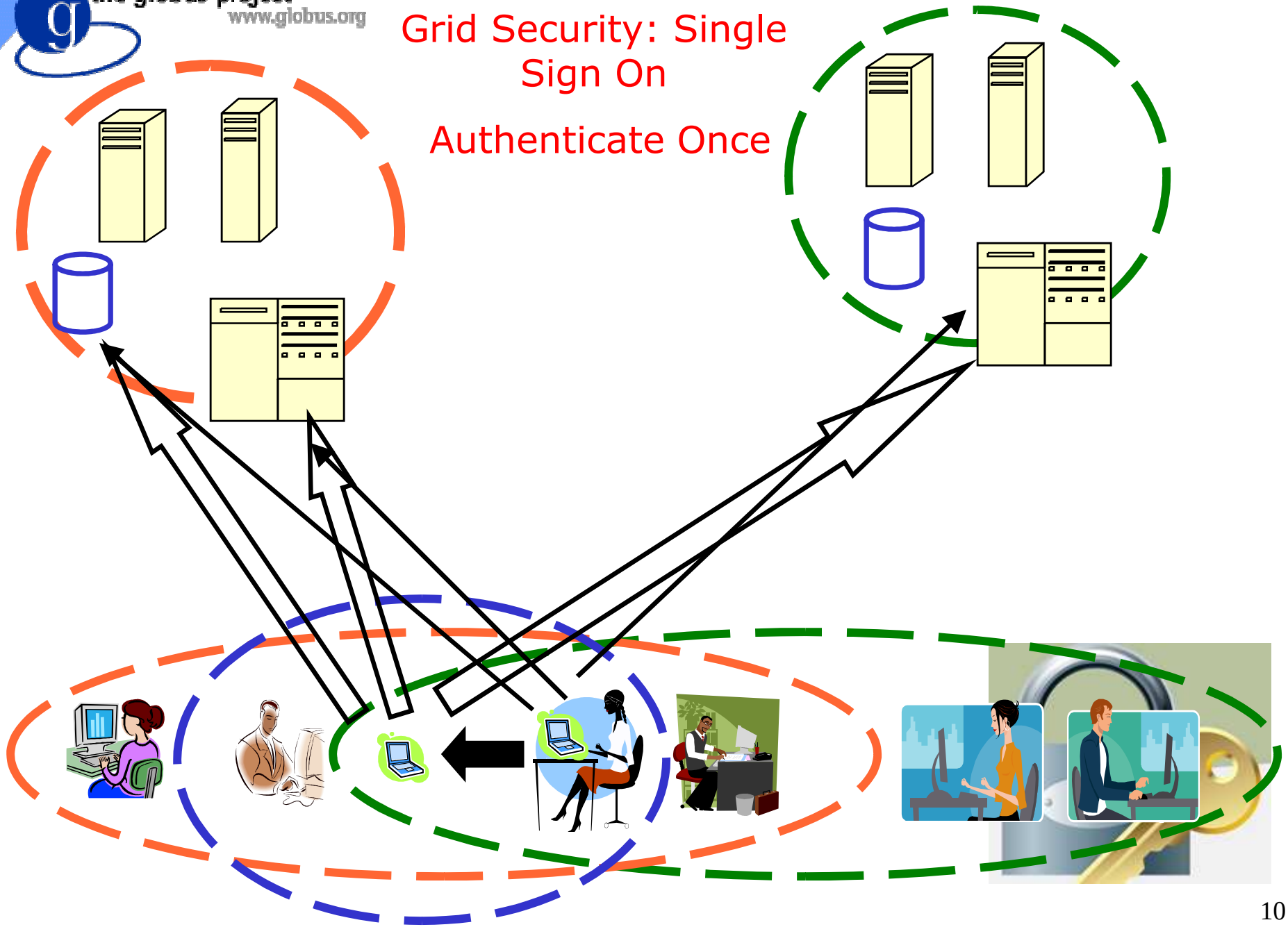
- Must authenticate first

Single sign on

- Log on once
  - Type password once
- Use any grid resource without typing password again.
- Important for complex applications that need to use Grid resources
  - Enables easy coordination of varied resources
  - Enables automation of process
  - Allows remote processes and resources to act on user's behalf
  - Authentication and Delegation

Grid Security: Single Sign On

Authenticate Once

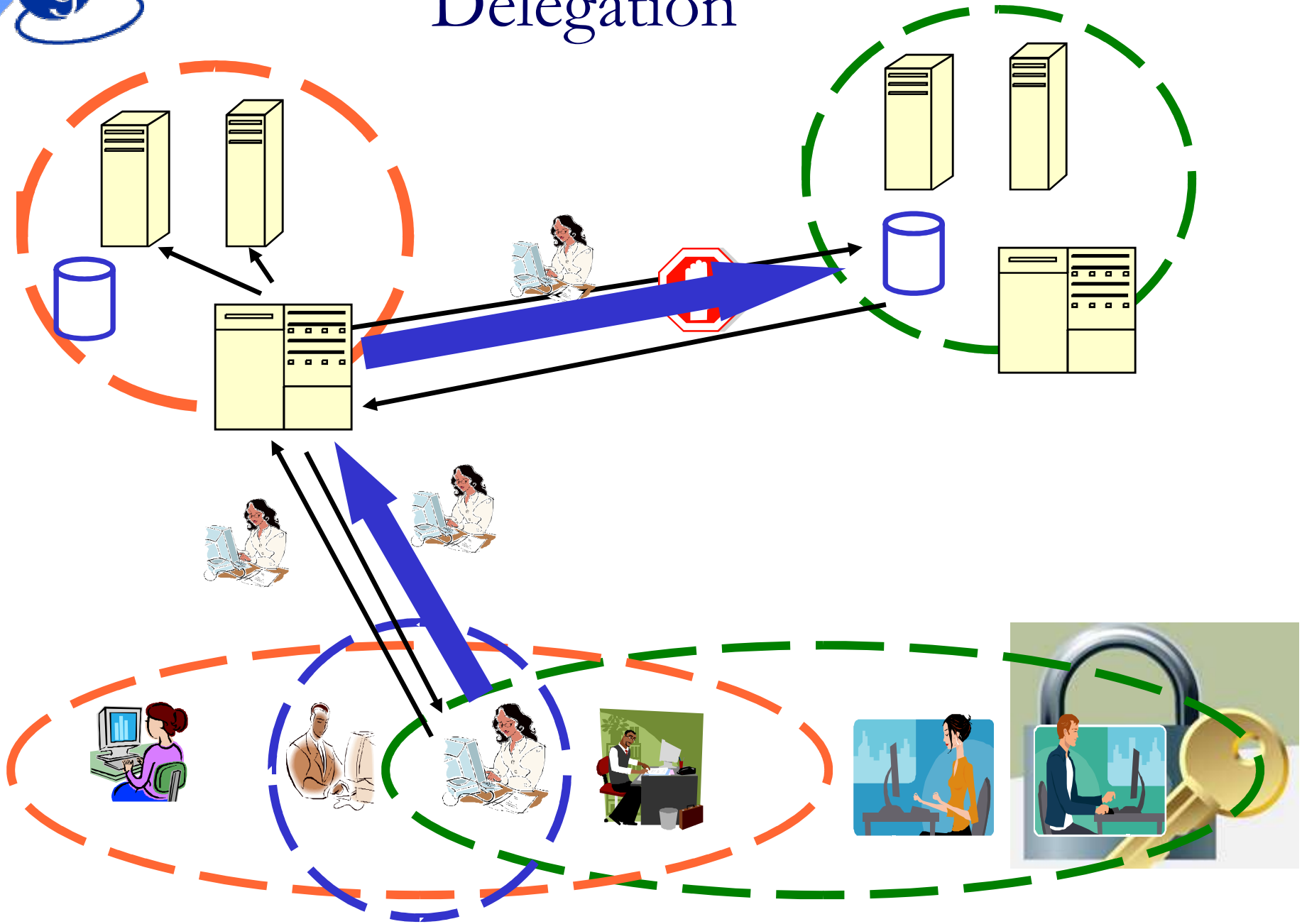


Delegation

- Resources on the grid can act as you
- Example: Execution jobs can transfer files
- Delegation can be restricted
  - For example: Delegation only valid for a short period of time

the globus project
www.globus.org

Delegation



Solutions

- **Cryptography Overview**
- Public Key Infrastructure (PKI) Overview
- Secure Socket Layer (SSL) Overview
- Grid Security Infrastructure (GSI) Overview

Cryptography Overview

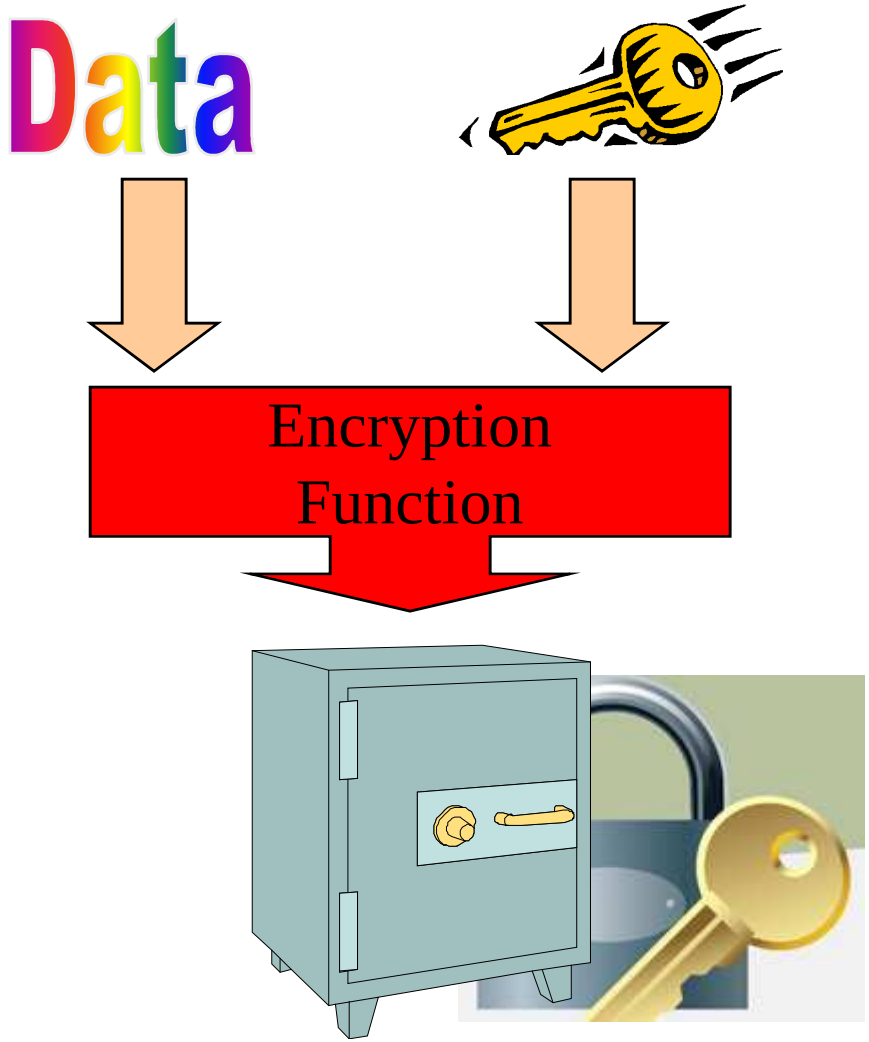
- Keys, Encryption and Decryption
  - Symmetric and Asymmetric
  - Public and Private keys
- Digital Signatures
  - Secure hashes

Keys

- A key can be thought of as simply a collection of bits
- The more bits, the stronger the key
- Keys are tied to specific encryption algorithms
- Lengths vary depending on the encryption algorithm
  - e.g. 128 bits is long for some algorithms, but short for others

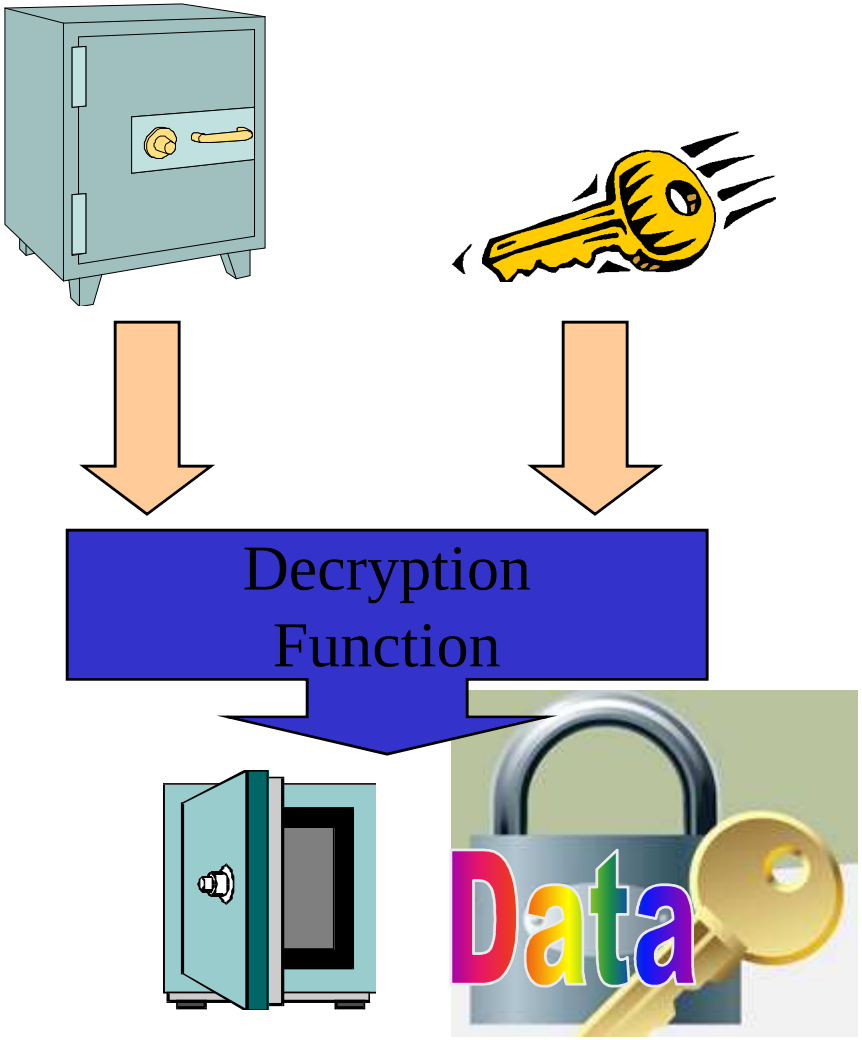
Encryption

- Encryption is the process of taking some data and a key and feeding it into a function and getting encrypted data out
- Encrypted data is, in principal, unreadable unless decrypted



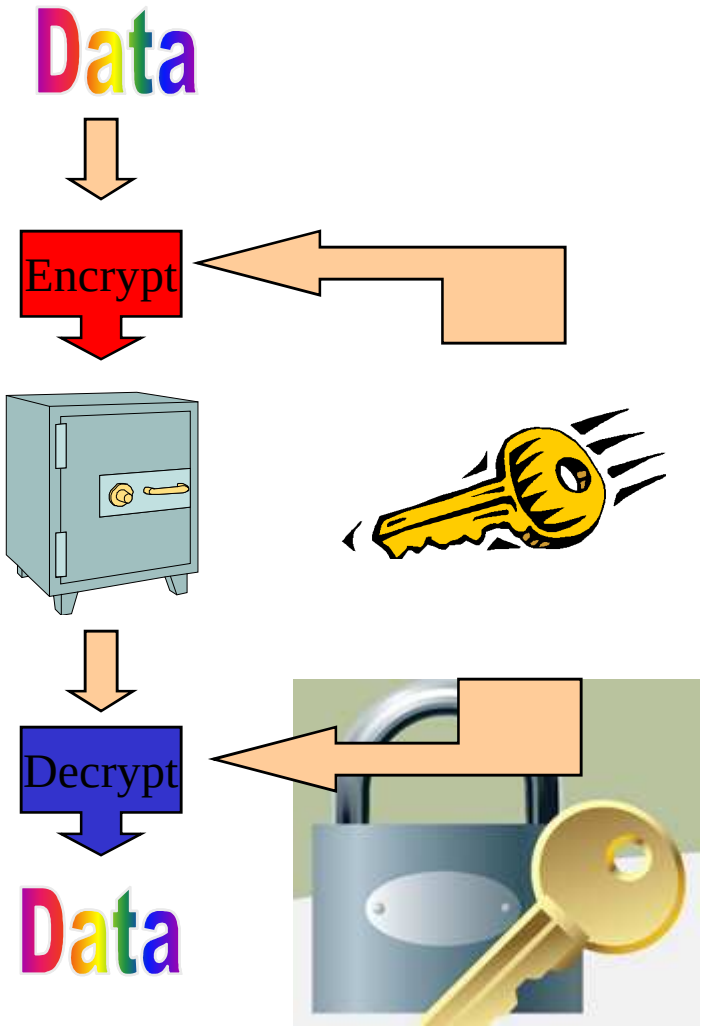
Decryption

- Decryption is the process of taking encrypted data and a key and feeding it into a function and getting out the original data
  - Encryption and decryption functions are linked



Symmetric Encryption

- Encryption and decryption functions that use the same key are called symmetric
  - In this case everyone wanting to read encrypted data must share the same key
- DES is an example of symmetric encryption

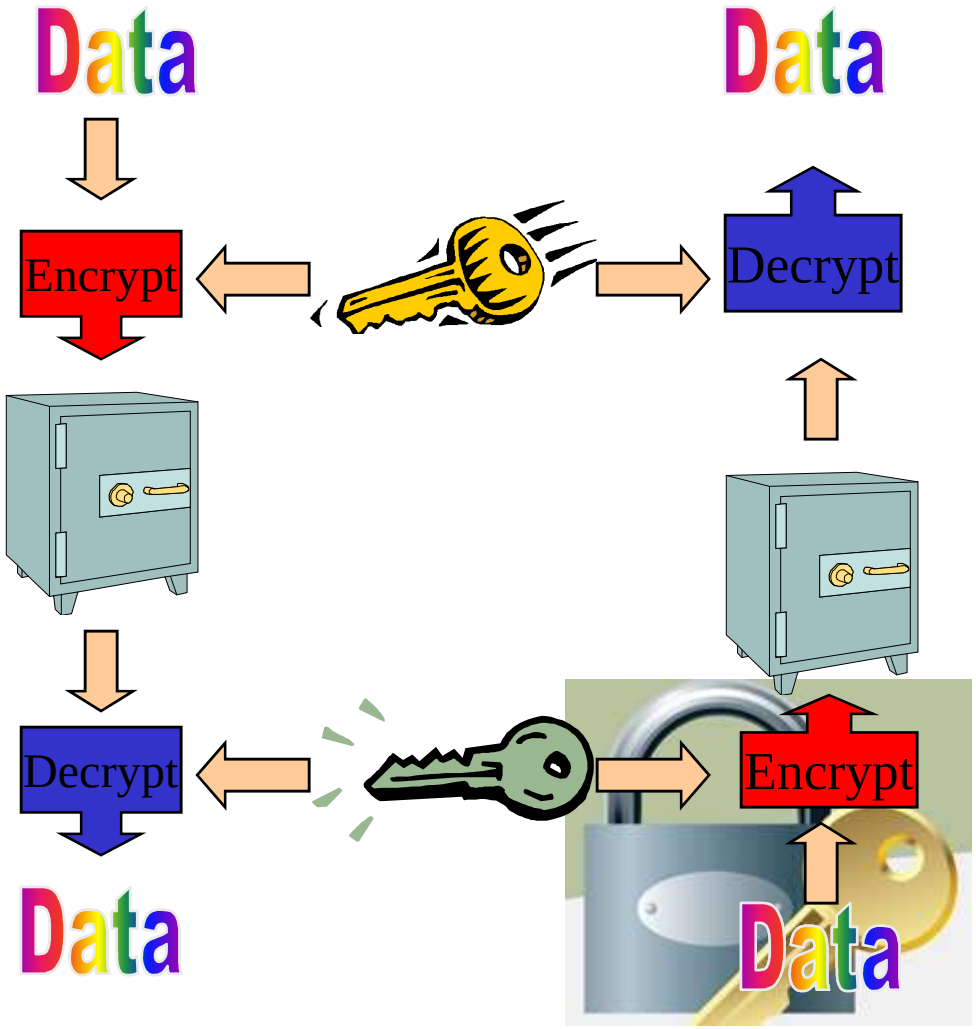


Asymmetric Encryption

- Encryption and decryption functions that use a key pair are called asymmetric
  - Keys are mathematically linked
- RSA is an example of asymmetric encryption

Asymmetric Encryption

- When data is encrypted with one key, the other key must be used to decrypt the data
  - And vice versa



Public and Private Keys

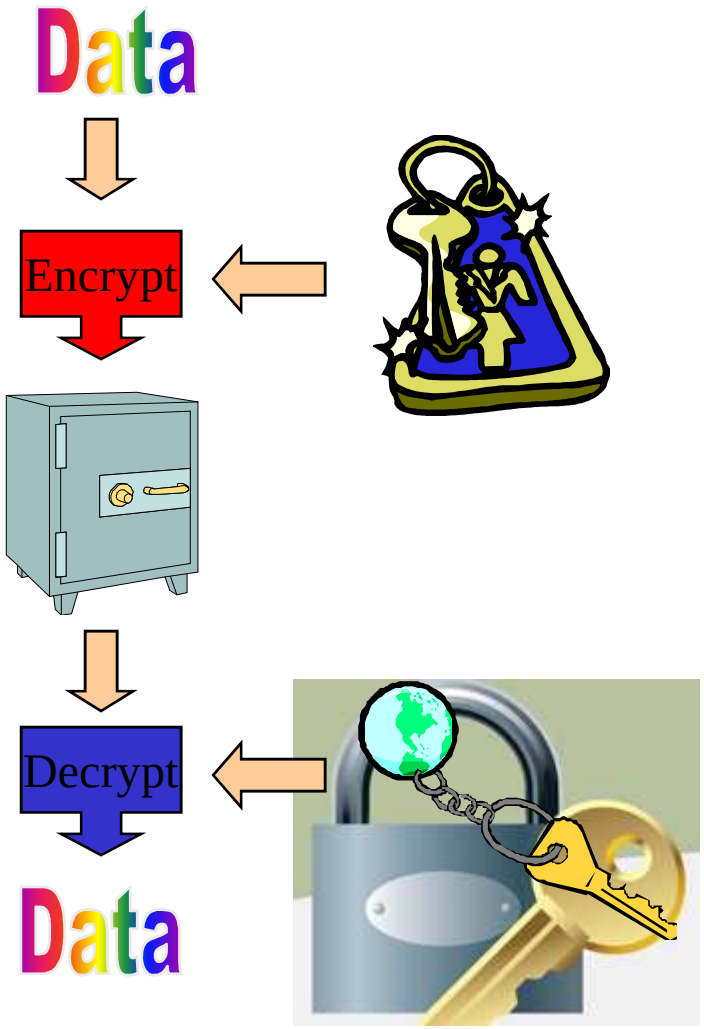
- With asymmetric encryption each user can be assigned a key pair: a private and public key

Private key is known only to owner

Public key is given away to the world

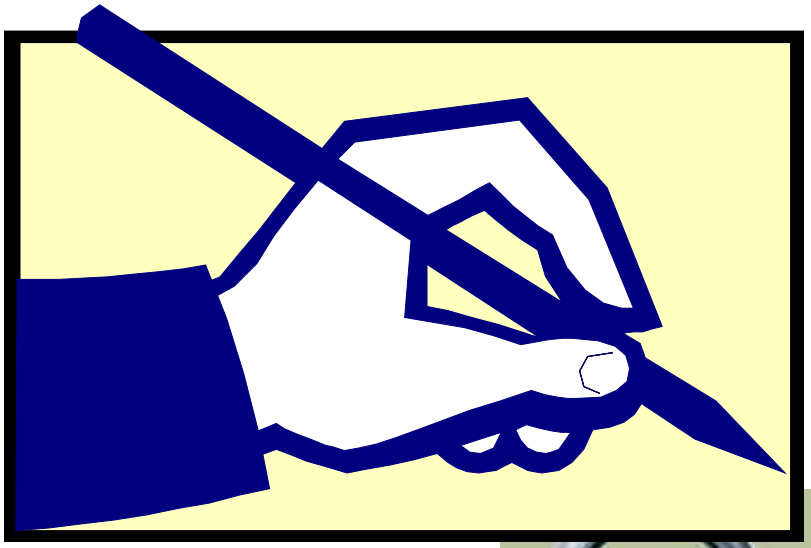
Public and Private keys

- Anything encrypted with the private key can only be decrypted with the public key
- And vice versa
- Since the private key is known only to the owner, this is very powerful…



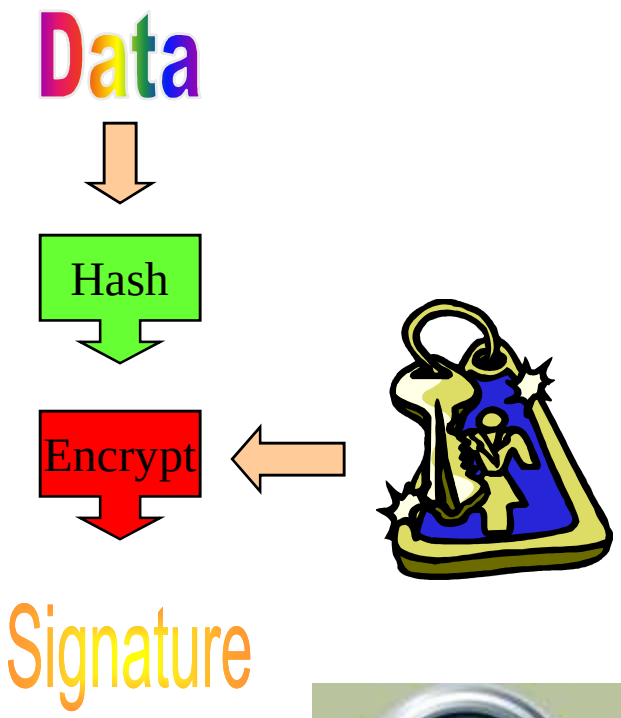
Digital Signatures

- Digital signatures allow the world to verify I created a chunk of data
  - e.g. email, code



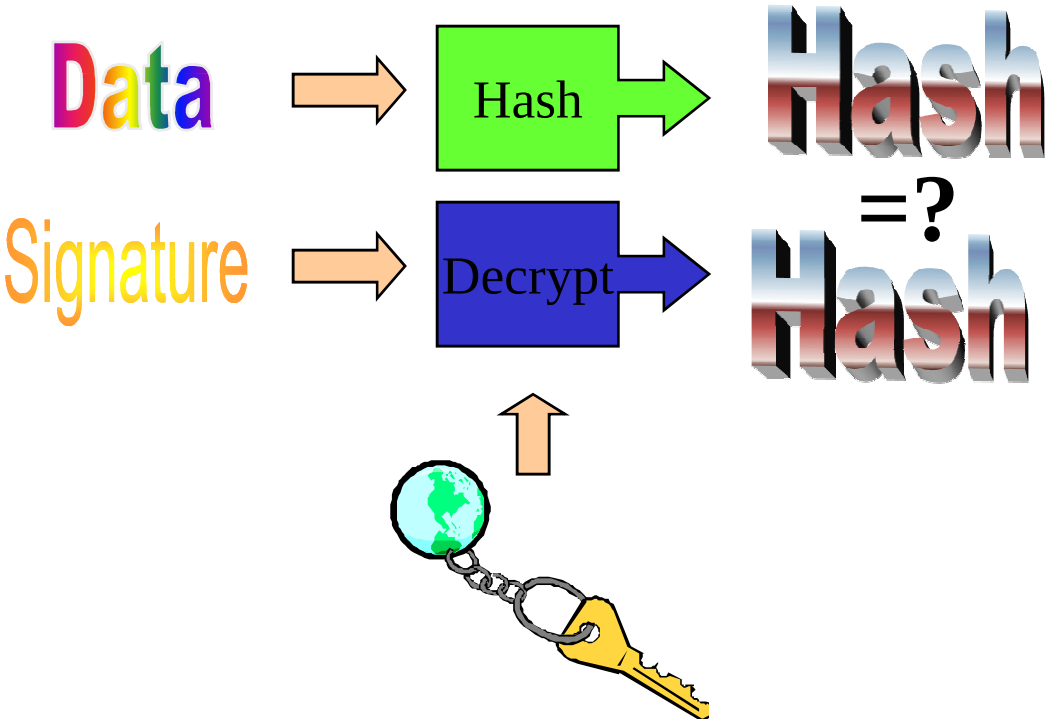
Digital Signatures

- Digital signatures are created by encrypting a hash of the data with my private key
- The resulting encrypted data is the signature
- This hash can then only be decrypted by my public key



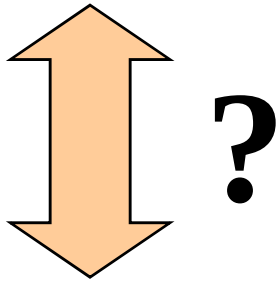
Digital Signature

- Given some data with my signature, if you decrypt a signature with my public key and get the hash of the data, you know it was encrypted with my private key



Digital Signature

- Since I'm the only one with access to my private key, you know I signed the hash and the data associated with it
- But, how do you know that you have my correct public key?
- Answer: A Public Key Infrastructure…



Solutions

- Cryptography Overview
- **Public Key Infrastructure (PKI) Overview**
- Secure Socket Layer (SSL) Overview
- Grid Security Infrastructure (GSI) Overview

Public Key Infrastructure (PKI)

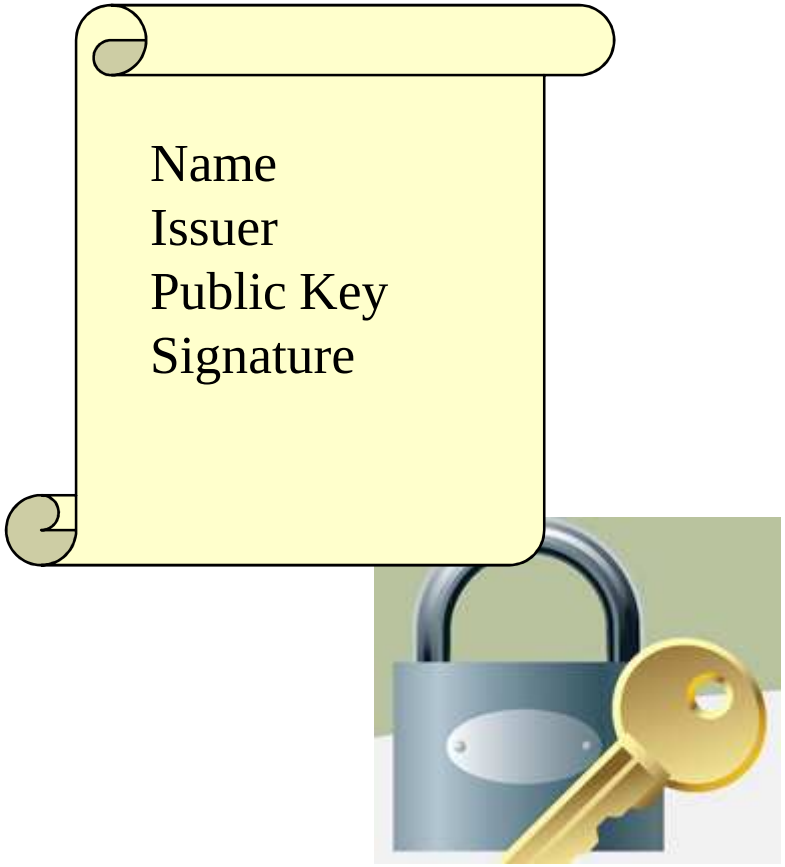
- PKI allows you to know that a given public key belongs to a given user
- PKI builds off of asymmetric encryption:
  - Each entity has two keys: public and private
  - The private key is known only to the entity
- The public key is given to the world encapsulated in a X.509 certificate

Public Key Infrastructure (PKI) Overview

- X.509 Certificates
- Certificate Authorities (CAs)
- Certificate Policies
  - Namespaces
- Requesting a certificate
  - Certificate Request
  - Registration Authority

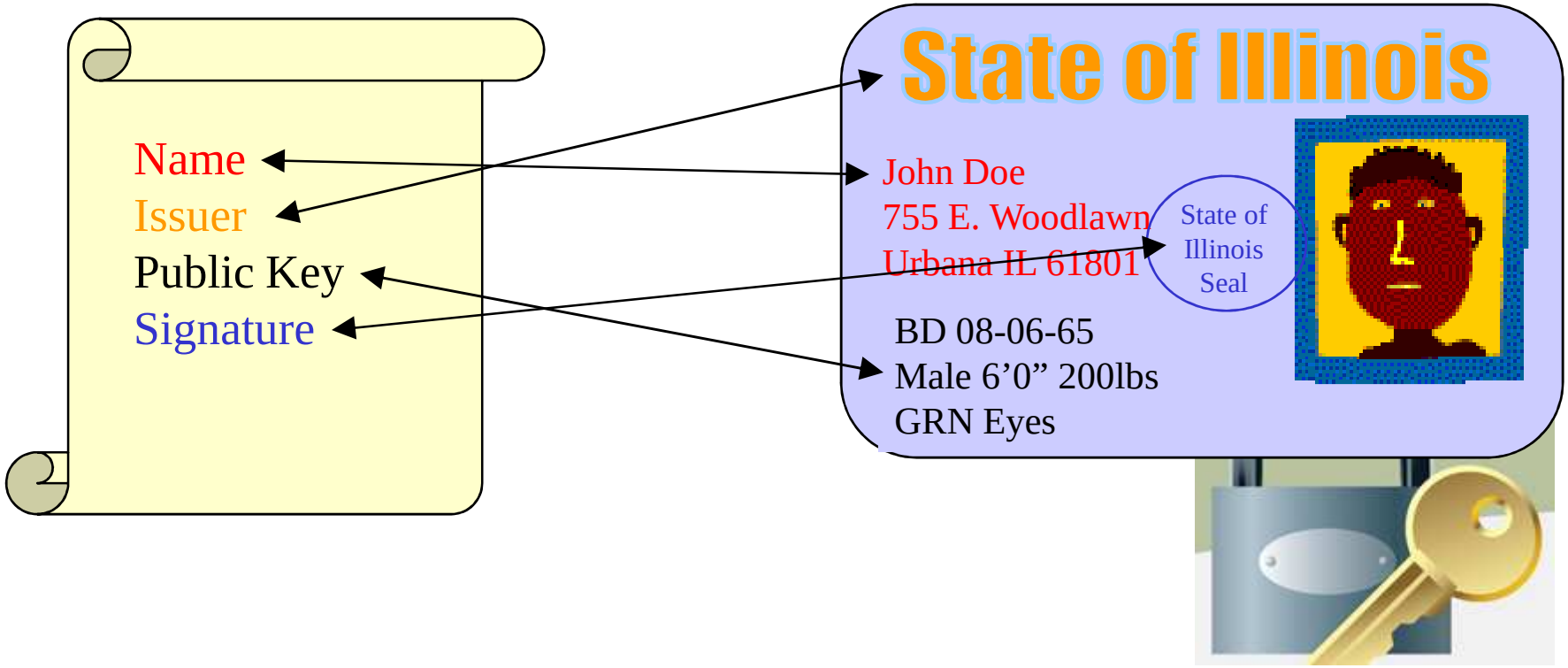
Certificates

- A X.509 certificate binds a public key to a name
- It includes a name and a public key (among other things) bundled together and signed by a trusted party (Issuer)



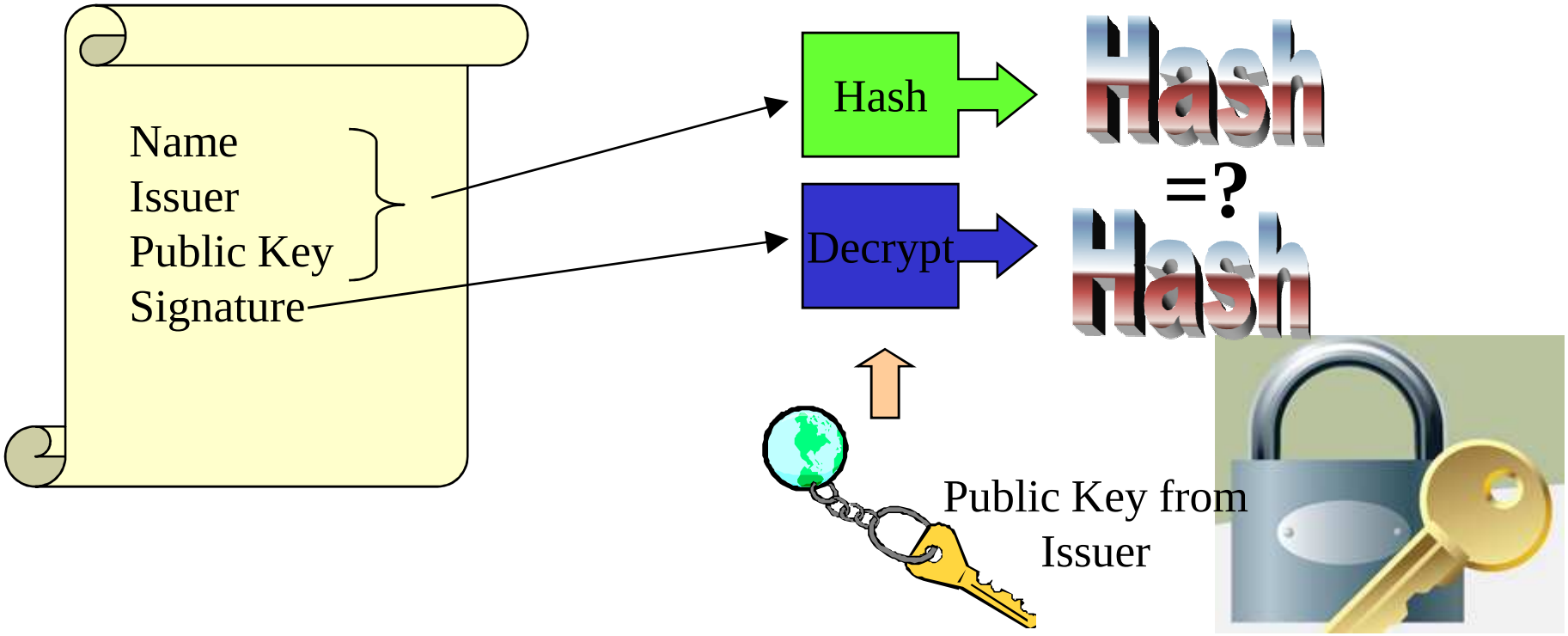
Certificates

- Similar to passport or driver's license



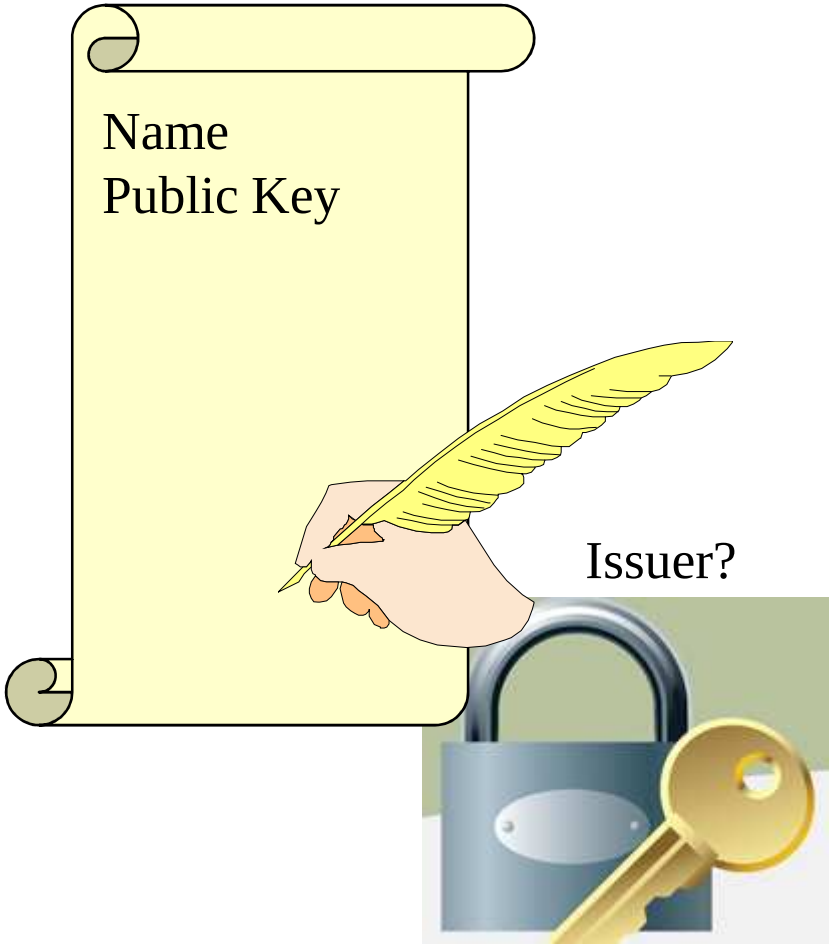
Certificates

- By checking the signature, one can determine that a public key belongs to a given user.



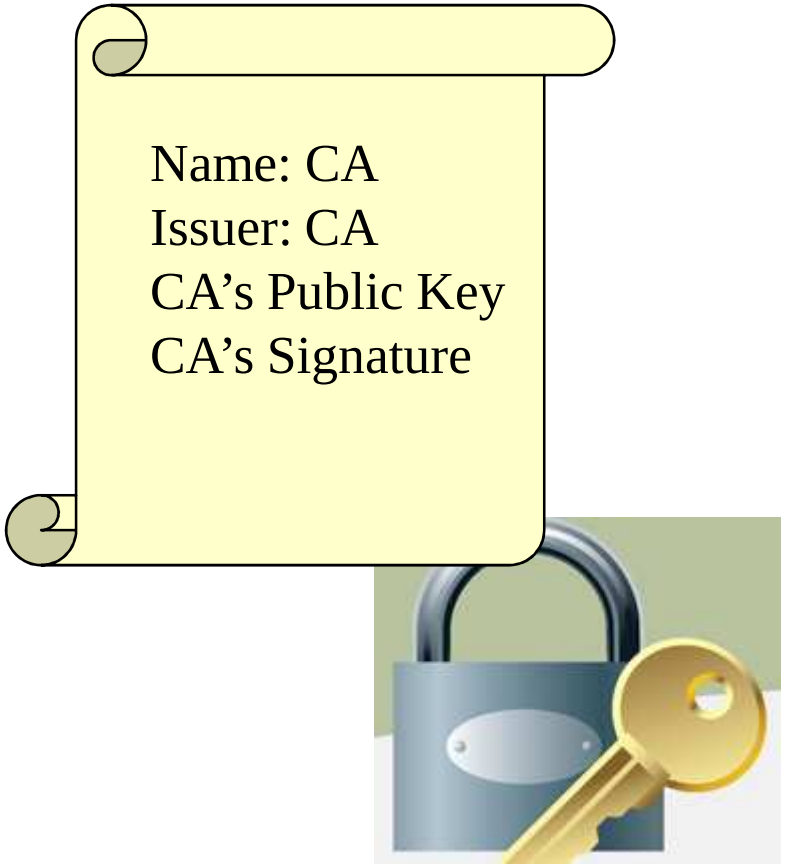
Certificates

- Question: Who signs certificates?
- Answer: A small set of trusted entities known as Certificate Authorities (CAs)



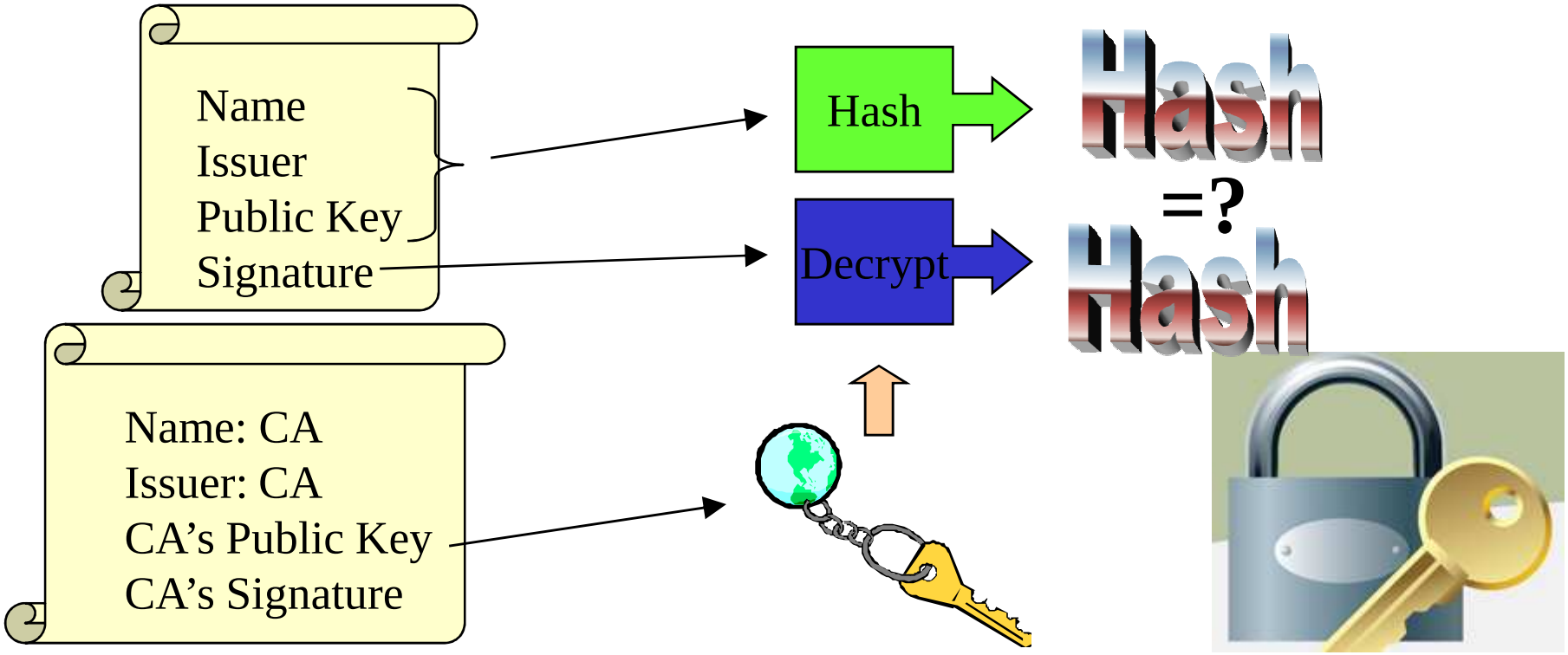
Certificate Authorities (CAs)

- A Certificate Authority is an entity that exists only to sign user certificates
- The CA signs it's own certificate which is distributed in a trusted manner



Certificate Authorities (CAs)

- The public key from the CA certificate can then be used to verify other certificates



Certificate Policy (CP)

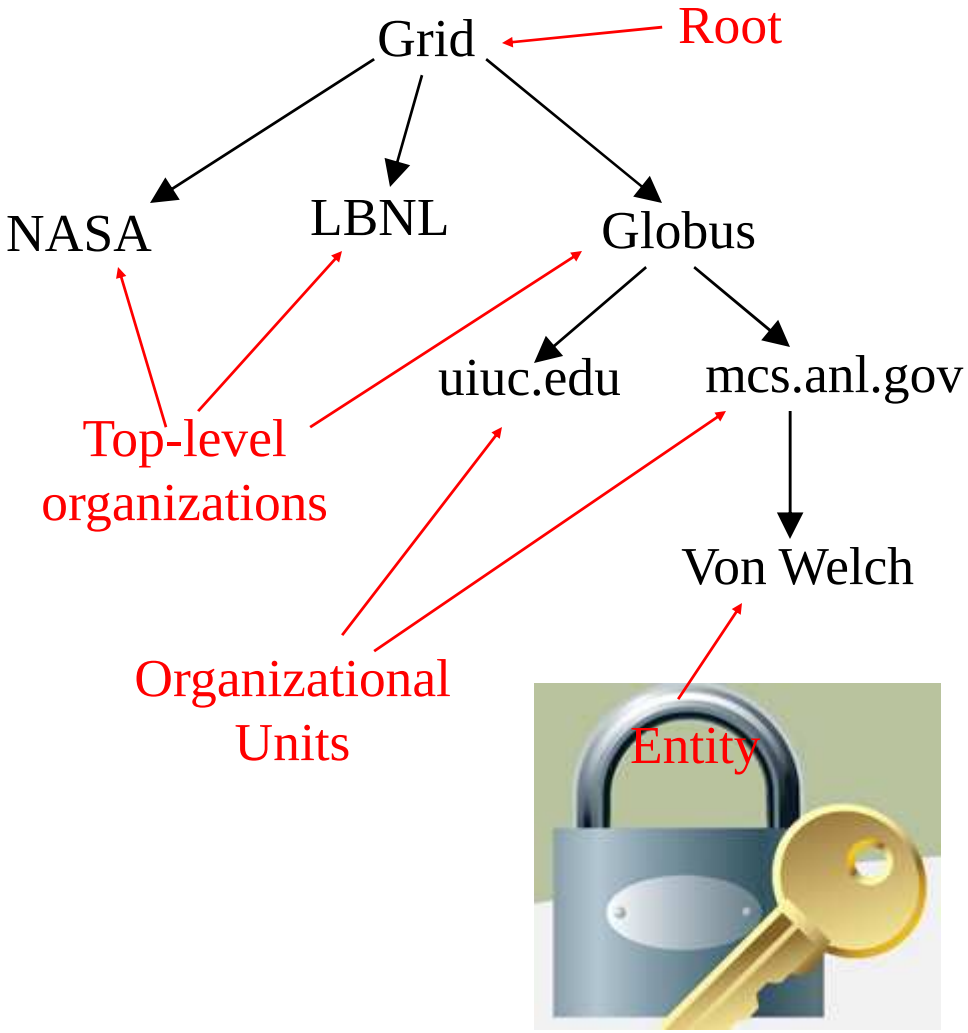
- Each CA has a Certificate Policy (CA) which states when and how a CA issues certificates.
- It states who it will issue certificates for
  - Just like the State of Illinois only issues driver's licenses' for residents of the state of Illinois
  - A CA for a grid typically only issues certificates for customers who are already approved to use resources on the grid

Certificate Policy (CP)

- A CA's CP states how it identifies the people it issues certificates to
  - Similar to having to show a birth certificate to get a driver's license
  - Some CA's are very stringent and require similar proof of identity
  - Others are lenient and only require proof via email

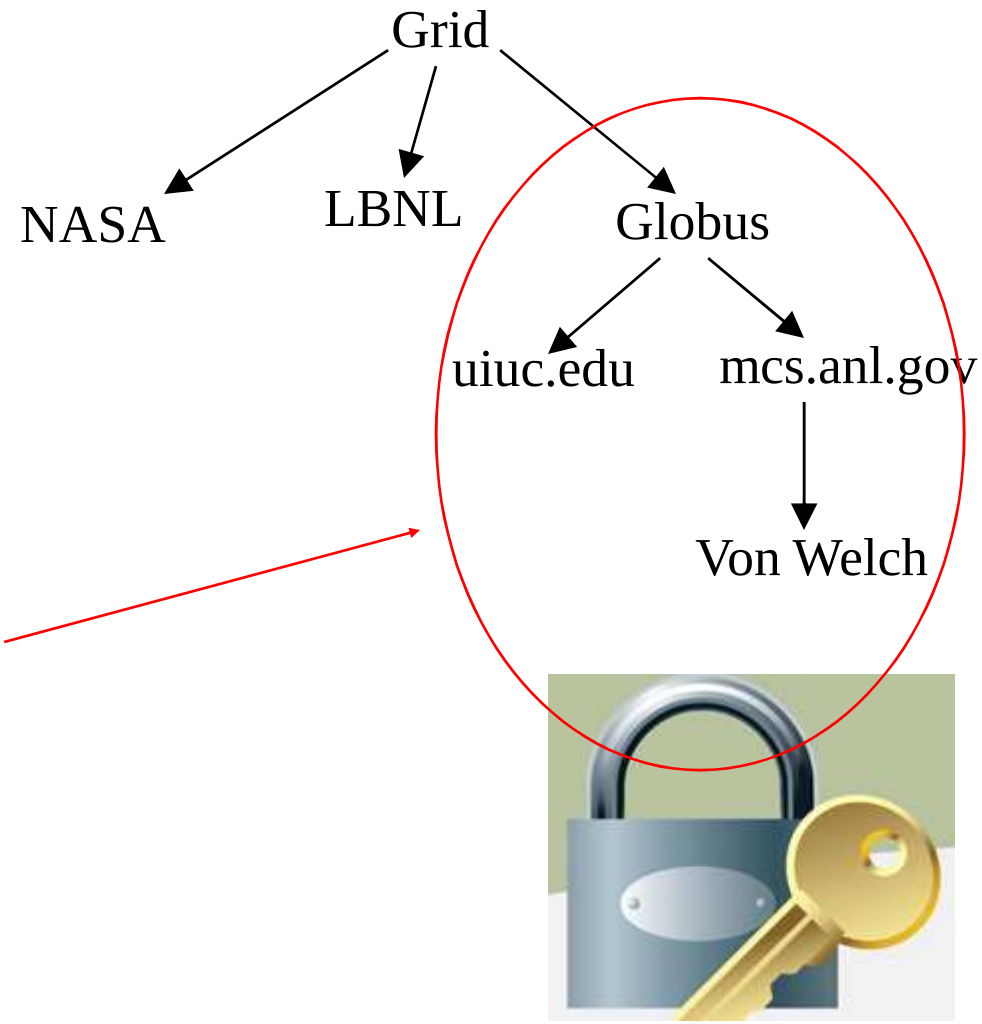
Namespaces

- Each CA's Certificate Policy also states the namespace of certificates issued by the CA
- A namespace is a hierarchy similar to the hierarchy used for Internet hostnames



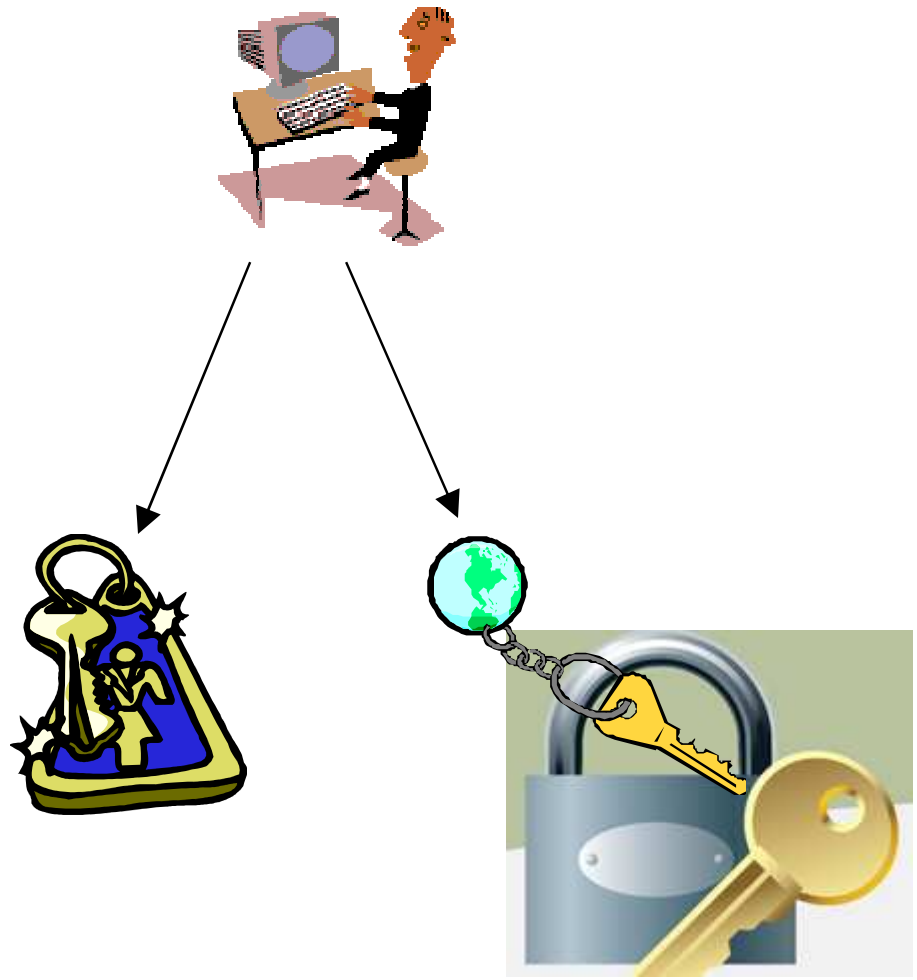
Namespaces

- Each CA constrains itself to signing certificates that are in a namespace that are a portion of the overall space
  - E.g. the Globus CA signs certificates only under the Globus organization



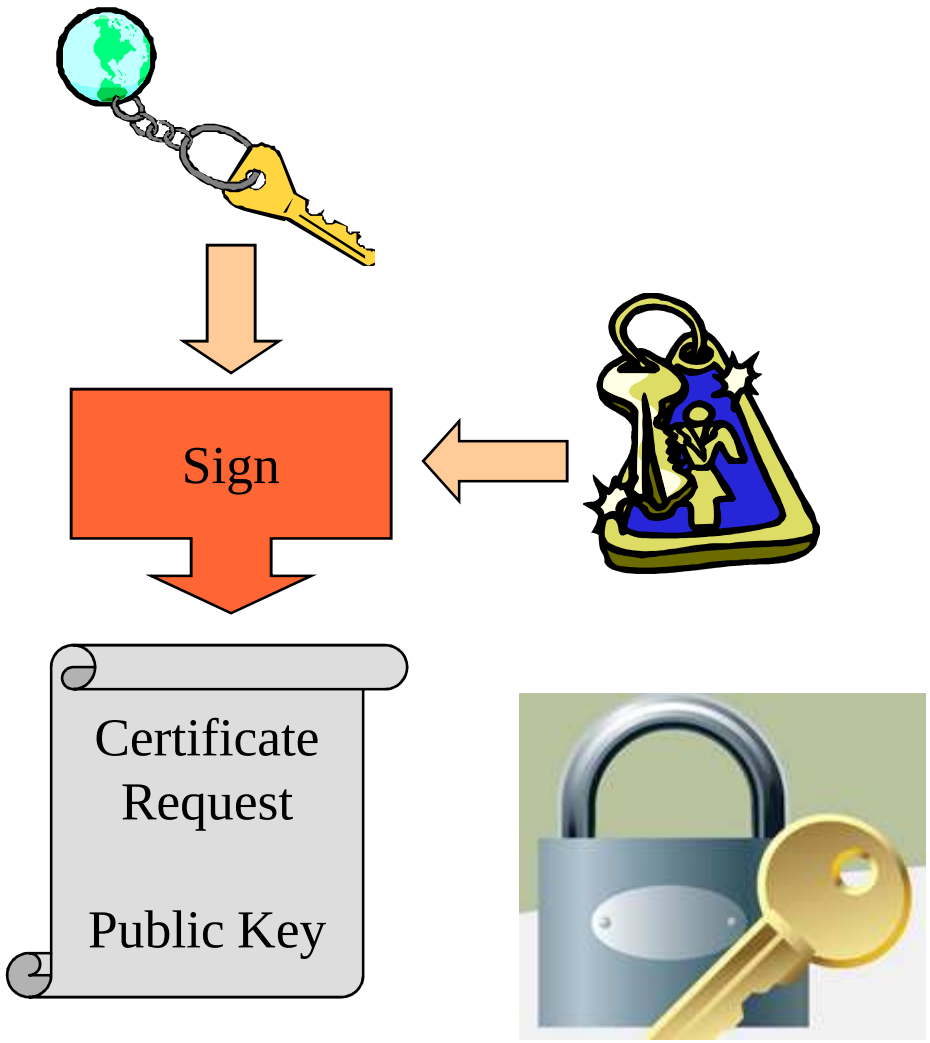
Requesting a Certificate

- To request a certificate a user starts by generating a key pair



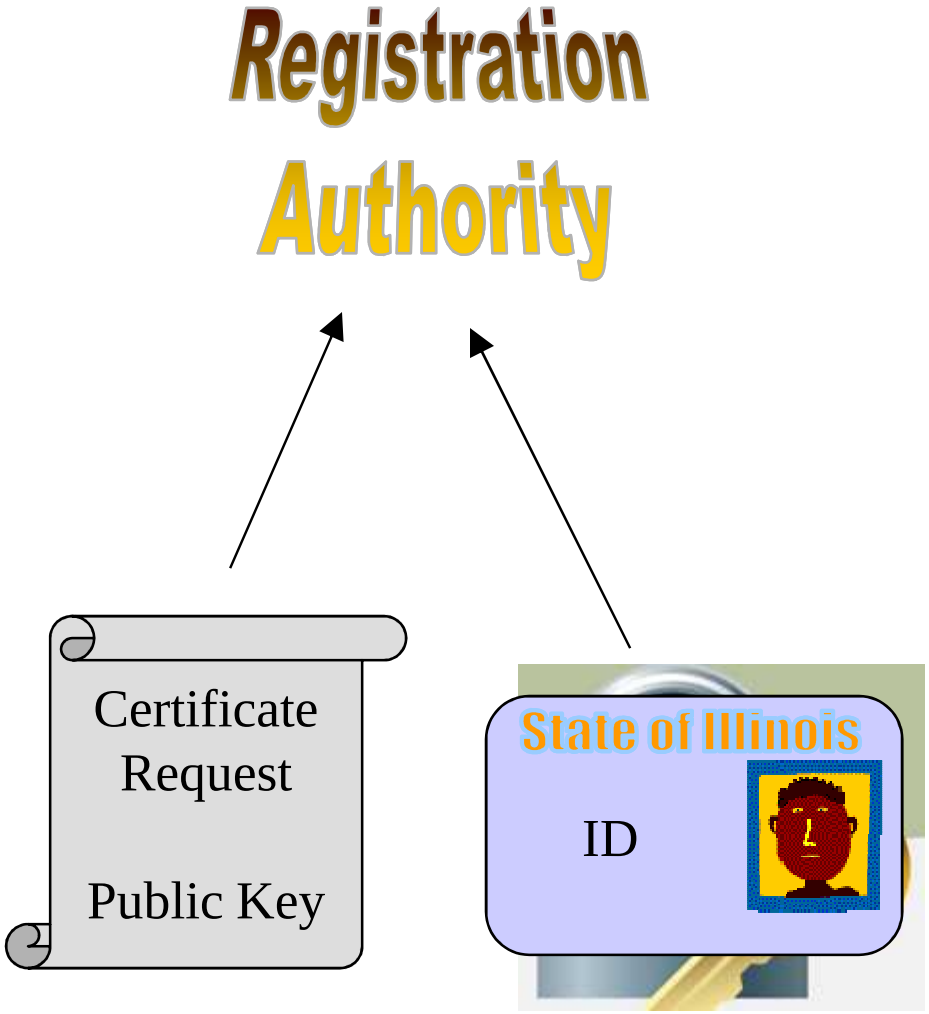
Certificate Request

- The user then signs their own public key to form what is called a Certificate Request



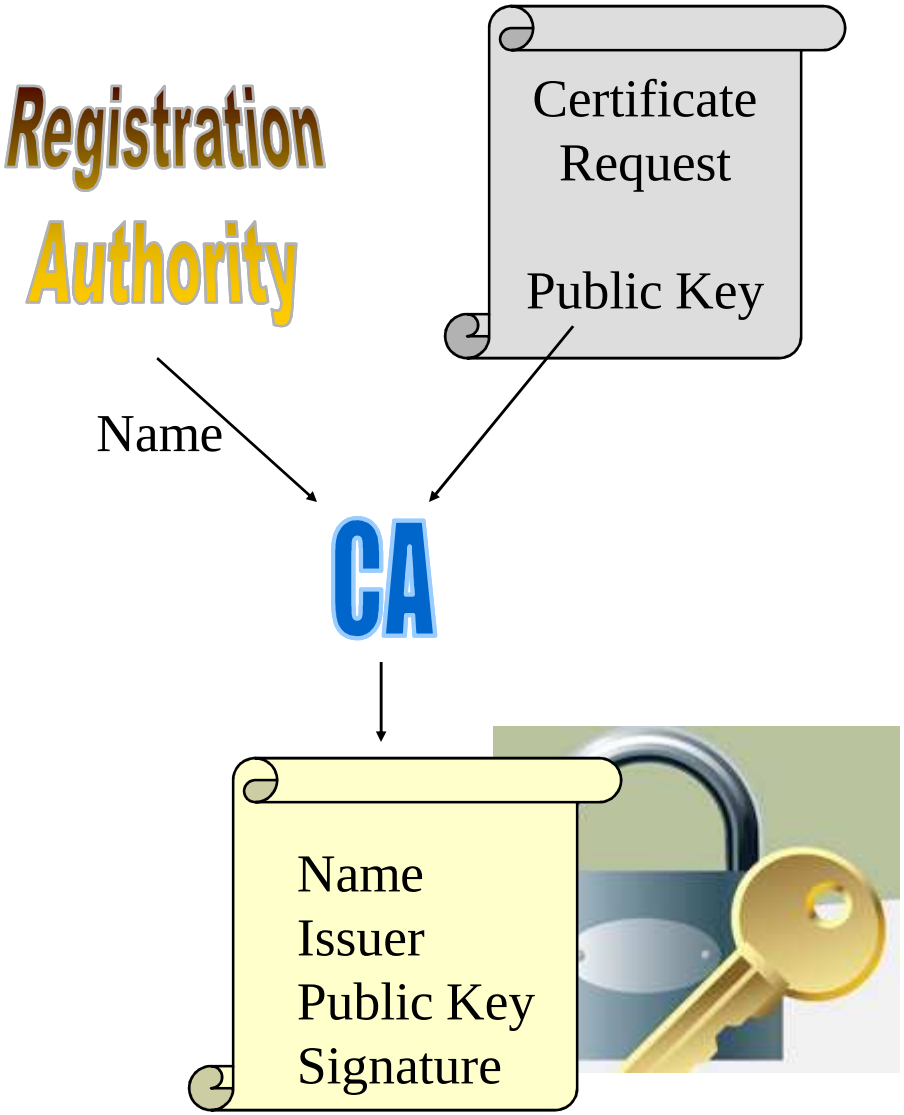
Registration Authority (RA)

- The user then takes the certificate to a Registration Authority (RA)
- A RA's responsibility is to verify the user's name
- Often the RA coexists with the CA and is not apparent to the user



Certificate Issuance

- The CA then takes the identity from the RA and the public key from the certificate request
- It then creates, signs and issues a certificate for the user



Solutions

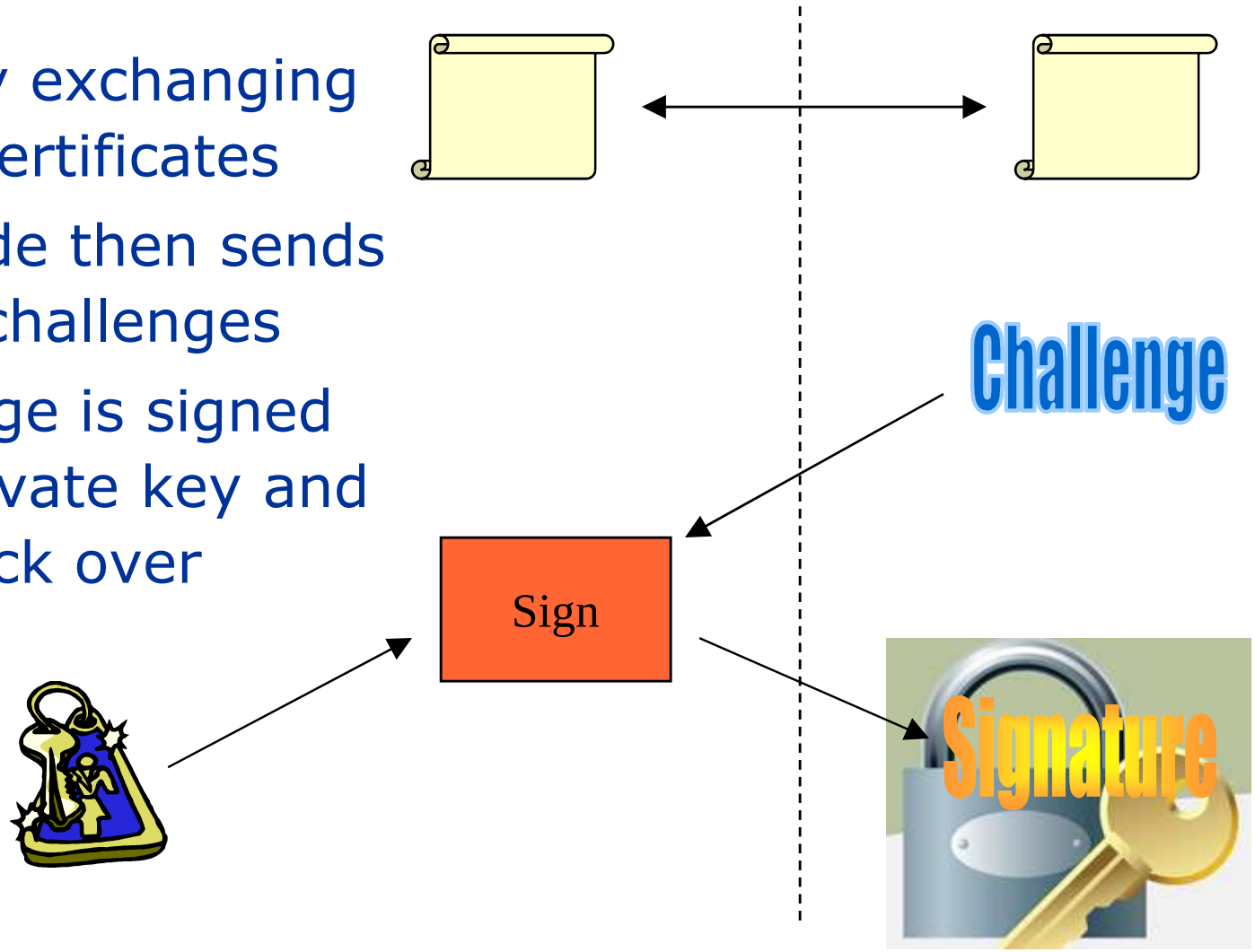
- Cryptography Overview
- Public Key Infrastructure (PKI) Overview
- **Secure Socket Layer (SSL) Overview**
- Grid Security Infrastructure (GSI) Overview

Secure Socket Layer (SSL)

- Protocol above a standard TCP/IP socket to provide security in the forms of:
  - Authentication
  - Message protection
    - Confidentiality
    - Integrity

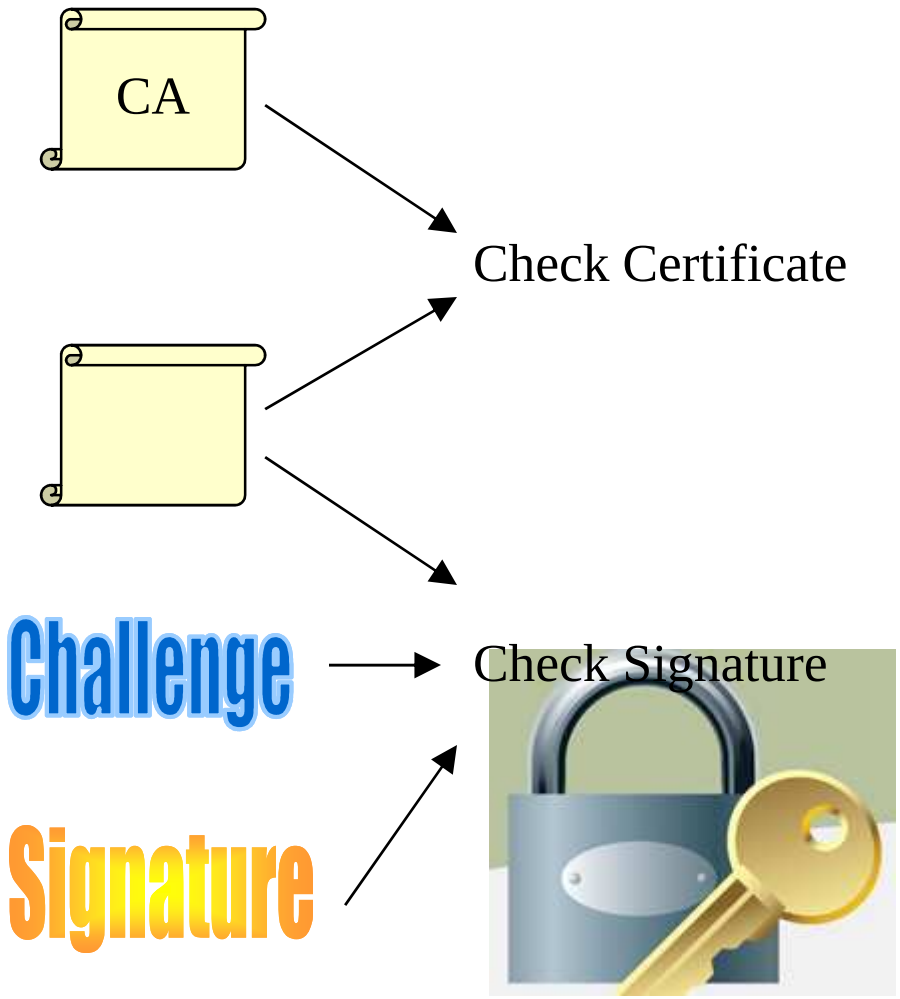
SSL Authentication

- Start by exchanging X.509 certificates
- Each side then sends over a challenges
- Challenge is signed with private key and sent back over



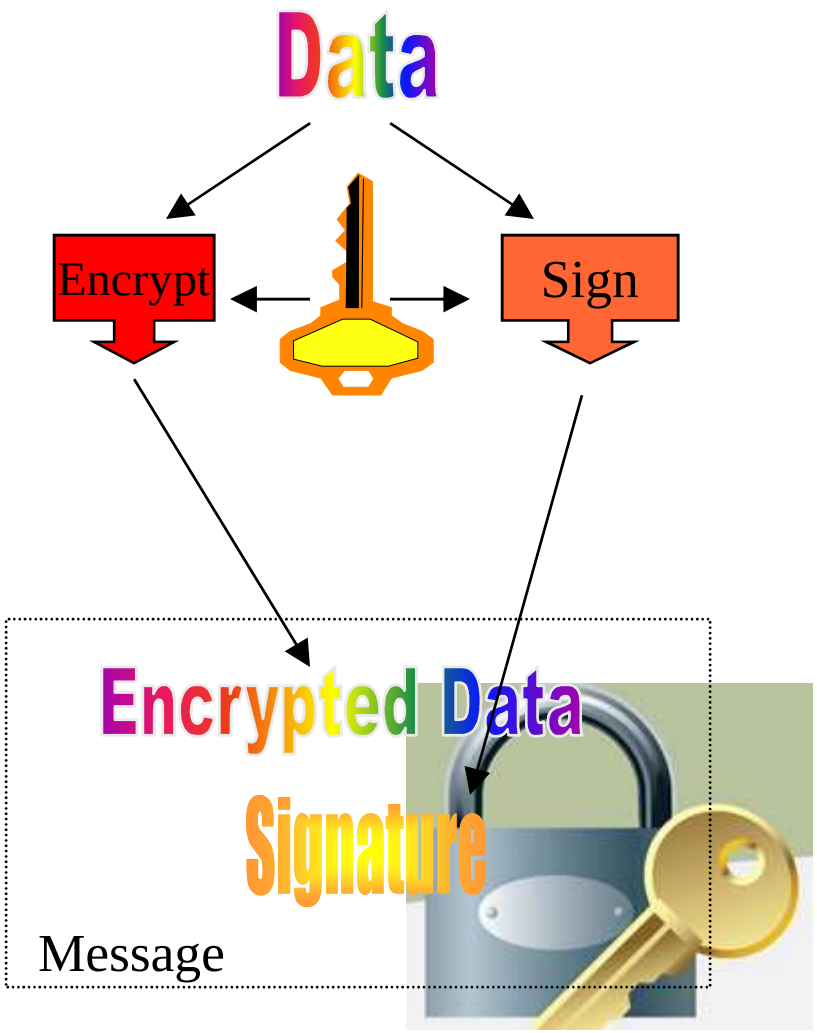
SSL Authentication

- Each side then verifies certificate using PKI and signature using certificate
- If everything checks then the identity from the certificate can be trusted



SSL Message Protection

- After authentication a shared session key is established to be used for message protection
- Confidentiality == Encryption of messages to prevent eavesdropping
- Integrity == Signing of messages to prevent modification



Solutions

- Cryptography Overview
- Public Key Infrastructure (PKI) Overview
- Secure Socket Layer (SSL) Overview
- **Grid Security Infrastructure (GSI) Overview**

Globus Security: The Grid Security Infrastructure

- The Grid Security Infrastructure (GSI) is a set of tools, libraries and protocols used in Globus to allow users and applications to securely access resources.
- Based on a public key infrastructure, with certificate authorities and X509 certificates

GSI

- Uses SSL for authentication and message protection
- Adds features needed for Single-Sign on
  - Proxy Credentials
  - Delegation

GSI: Credentials

- In the GSI system each user has a set of credentials they use to prove their identity on the grid
  - Consists of a X509 certificate and private key
- Long-term private key is kept encrypted with a pass phrase
  - Good for security, inconvenient for repeated usage

GSI: Single Sign-on

- Single-sign on is important feature for Grid Applications
  - Enables easy coordination of multiple resources
  - User authenticates themselves once, then can perform multiple actions without reauthentication
  - Can allow processes to act on their behalf

GSI: Single Sign-on

- To support single sign-on GSI adds the following functionality to SSL:
  - Proxy credentials
  - Credential delegation

GSI: Proxy Credentials

- Proxy credentials are short-lived credentials created by user
  - Short term binding of user's identity to alternate private key
  - Stored unencrypted for easy repeated access
  - Short lifetime in case of theft
  - Enables user to authenticate once then perform multiple actions without reauthenticating

GSI: Delegation

- GSI enables user to create and delegate proxy credentials to processes running on remote resources
- Allows remote processes and resources to act on user's behalf
- Important for complex applications that need to use Grid resources
  - E.g. jobs that needs to access data storage

Summary

- GSI is:
  - X.509 Certificates for authentication
  - PKI for verifying identities in Certificates
  - SSL as the protocol for authentication, confidentiality and integrity
  - Proxy Credentials and delegation to support single sign-on