



Enabling Grids for  
E-science in Europe

*Induction to Grid Computing  
and the EGEE Project, Vilnius, 5-6.10.2004*

# Authorisation, Authentication and Security

**Guy Warner**  
NeSC Training Team



# User Concepts

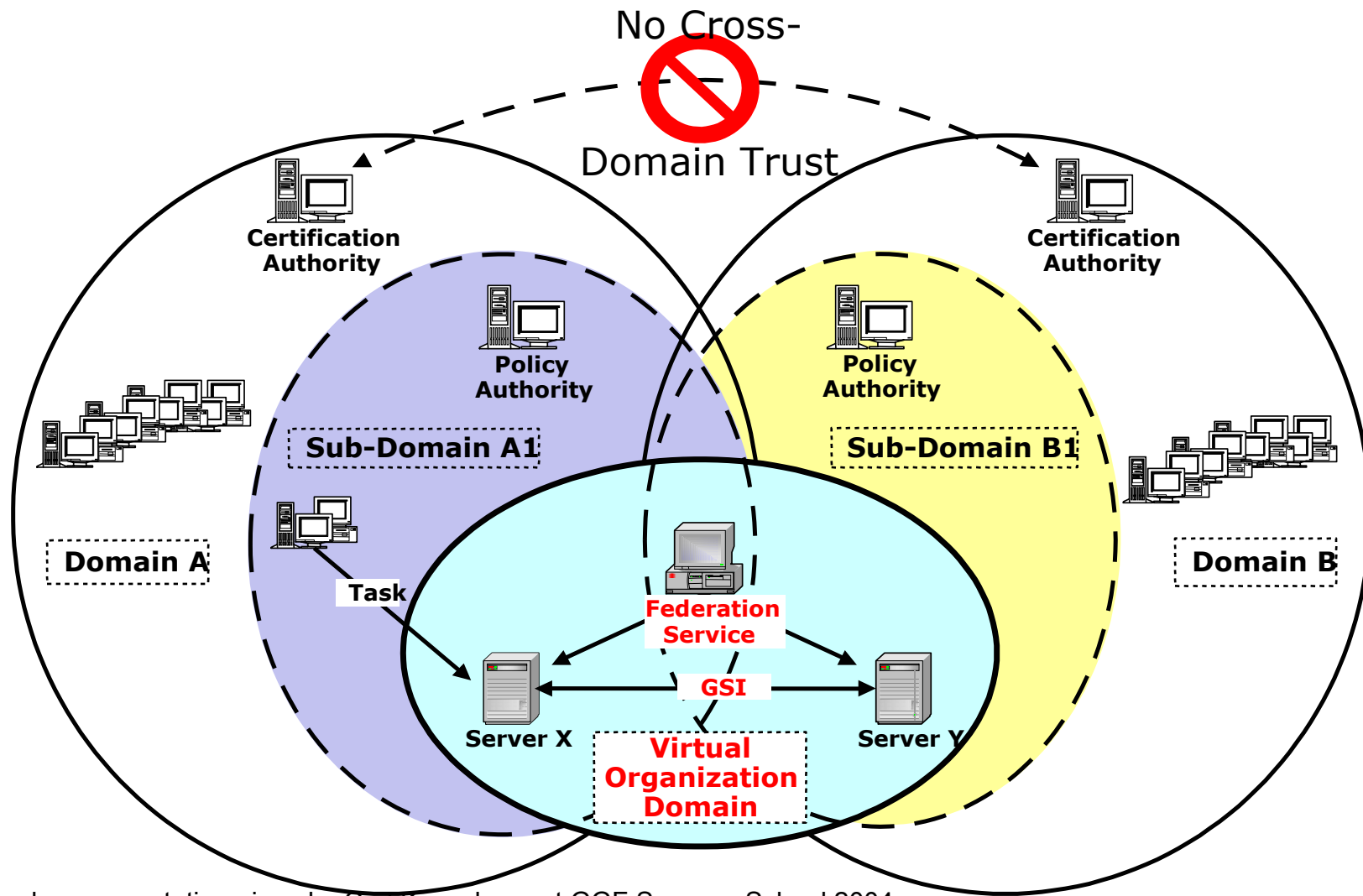
- Authentication
  - Are you who you claim to be?
- Authorisation
  - Do you have access to the resource you are connecting to?
- Accounting
  - What did you do, when did you do it and where did you do it from?

# Aspects of Grid Security

- Resources being used may be valuable & the problems being solved sensitive
- Dynamic formation and management of virtual organizations (VOs)
  - Large, dynamic, unpredictable...
- VO Resources and users are often located in distinct administrative domains
  - Can't assume cross-organizational trust agreements
  - Different mechanisms & credentials
- Interactions are not just client/server, but service-to-service on behalf of the user
  - Requires delegation of rights by user to service
  - Services may be dynamically instantiated

slide based on presentation given by Carl Kesselman at GGF Summer School 2004

# The Trust Model



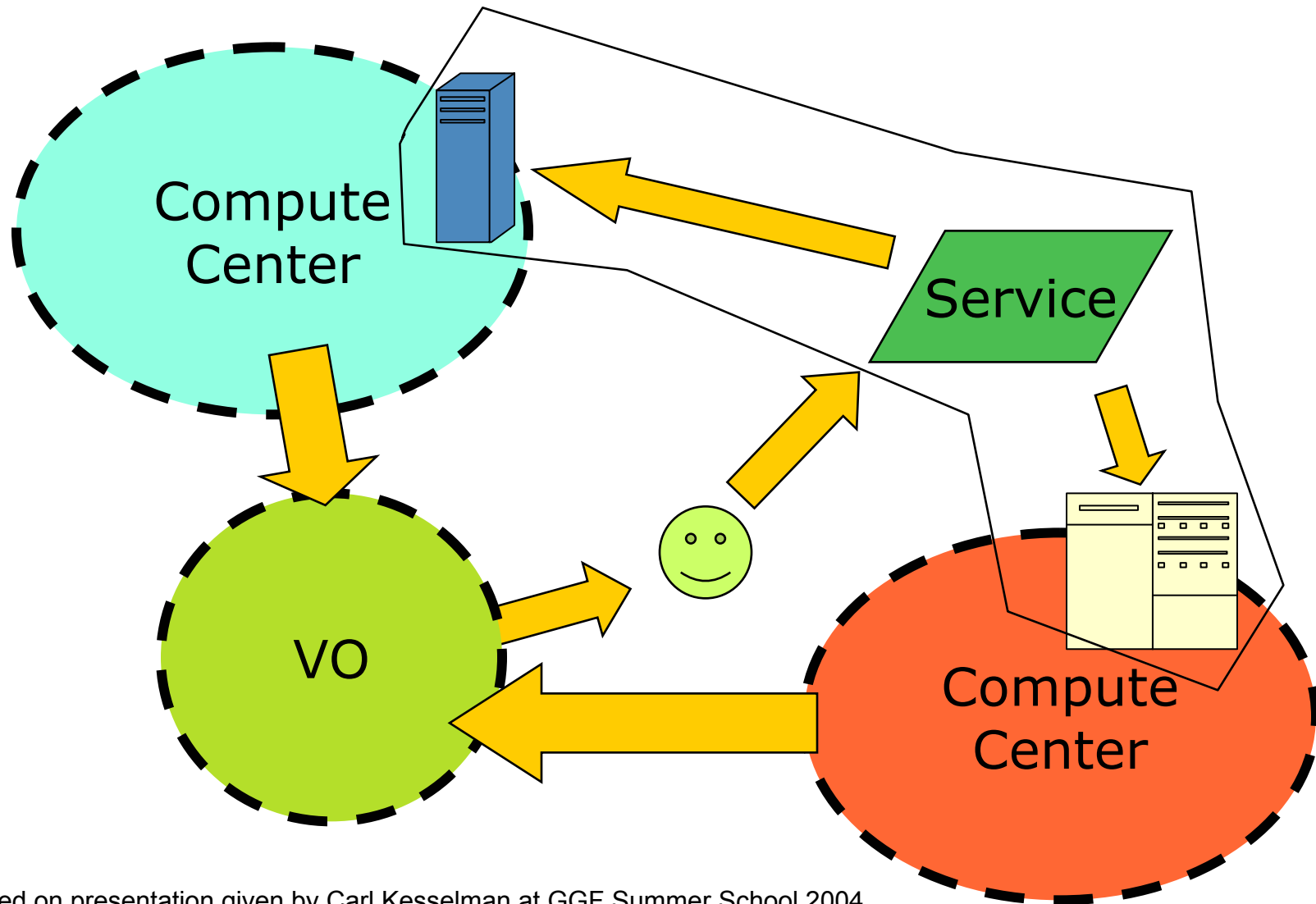
slide based on presentation given by Carl Kesselman at GGF Summer School 2004

# Delegation

Delegation : The act of giving an organisation, person or service the right to act on your behalf.

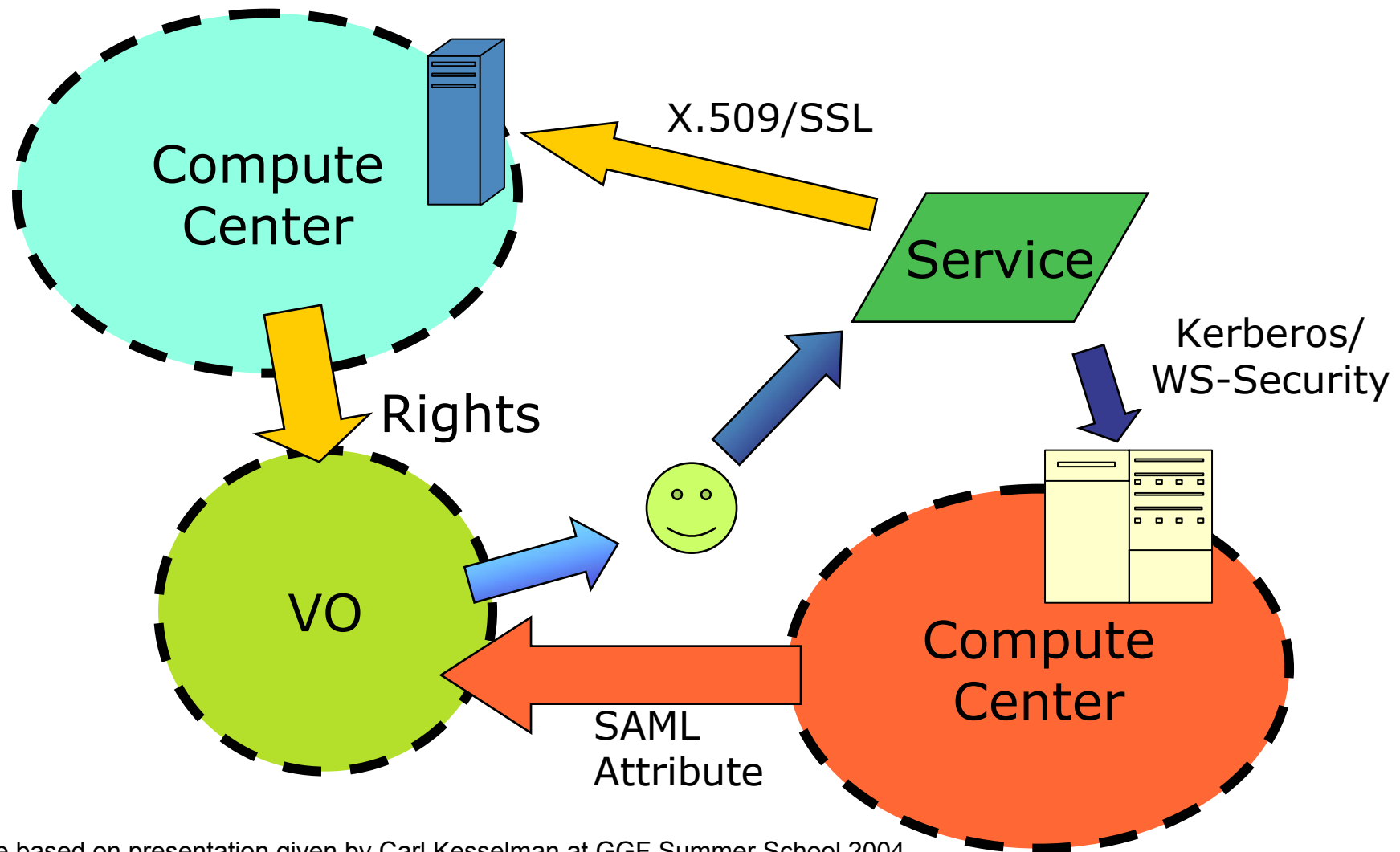
- A Site delegates responsibility for the users that may access its resources to the managers/management system of a VO.
- A VO delegates its rights to a user.
- A user delegates their authentication to a service to allow programs to run on remote sites.

# Use Delegation to Establish Dynamic Distributed System



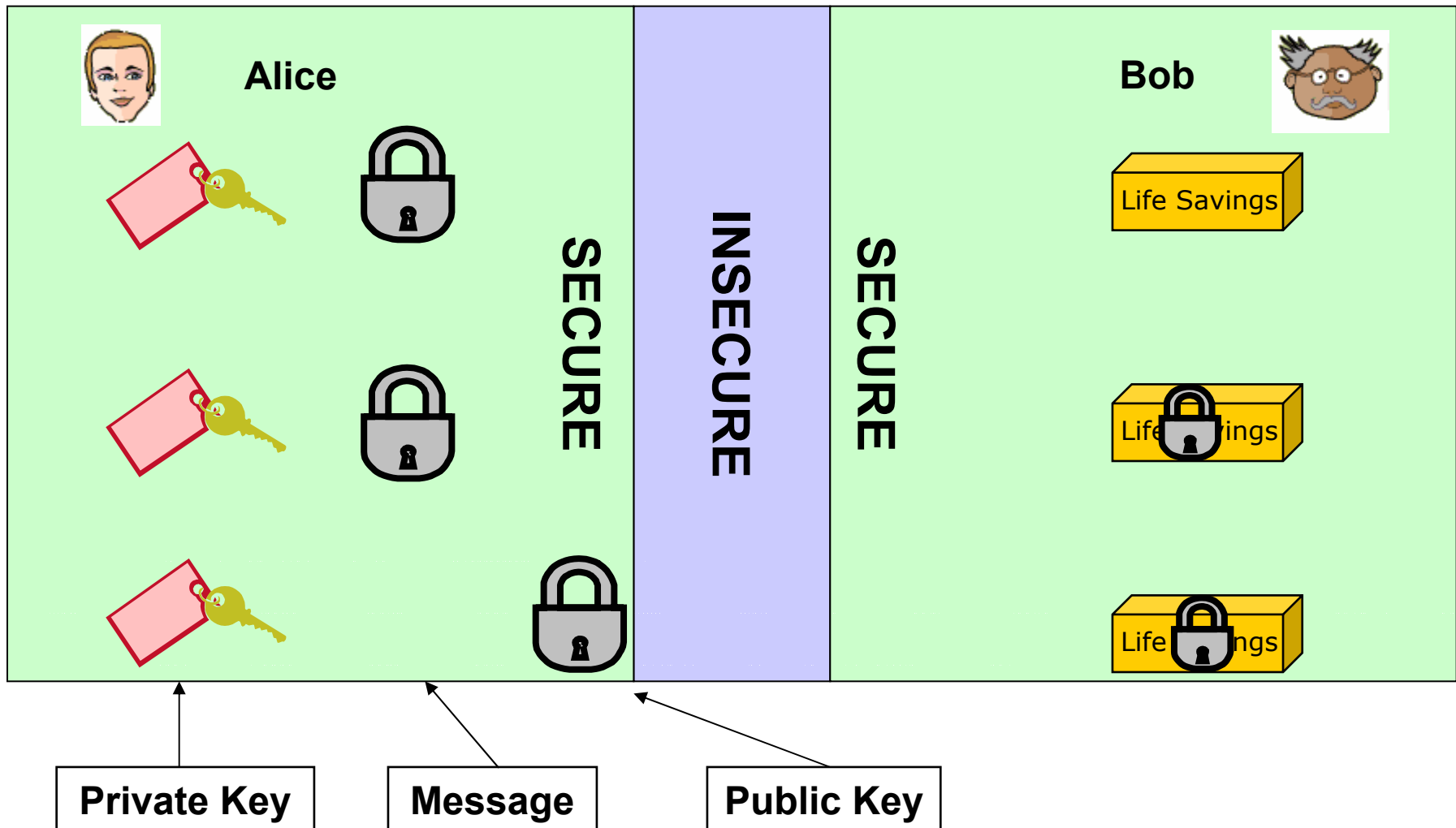
slide based on presentation given by Carl Kesselman at GGF Summer School 2004

# Goal is to do this with arbitrary mechanisms



slide based on presentation given by Carl Kesselman at GGF Summer School 2004

# Public Private Key



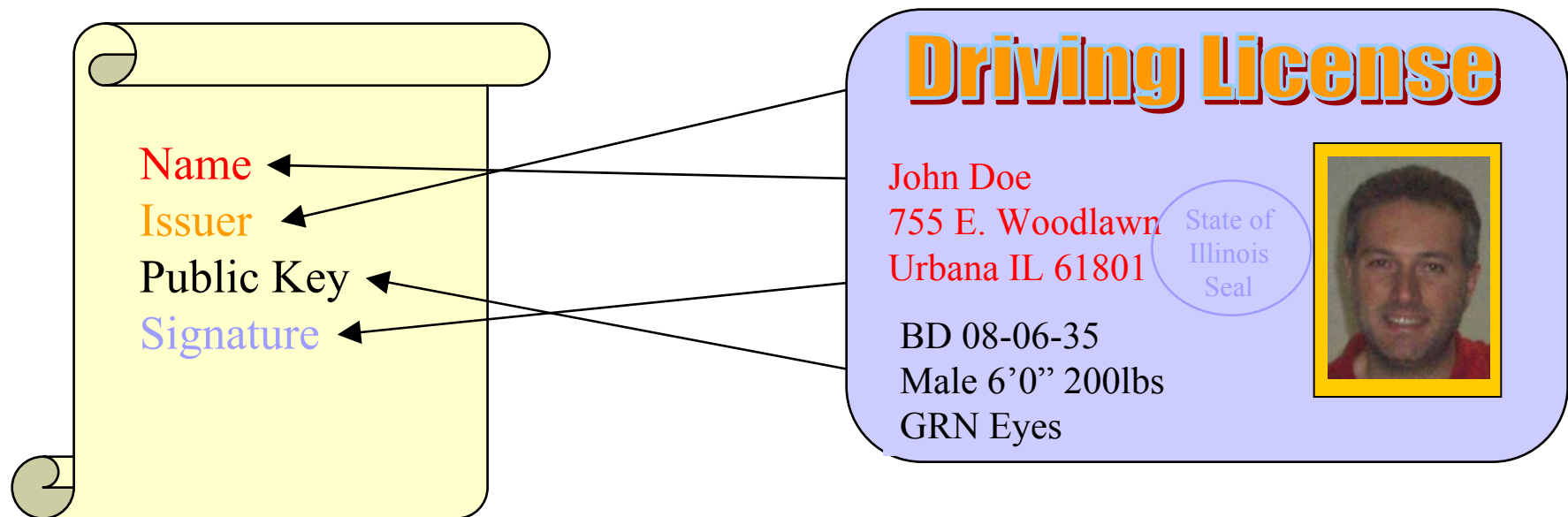


# Public Key Infrastructure (PKI)

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

# Certificates

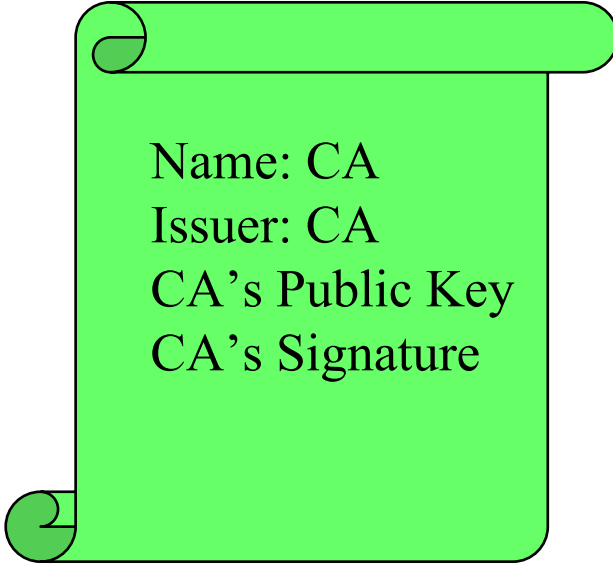
- Similar to passport or driver's license: Identity signed by a trusted party



slide based on presentation given by Carl Kesselman at GGF Summer School 2004

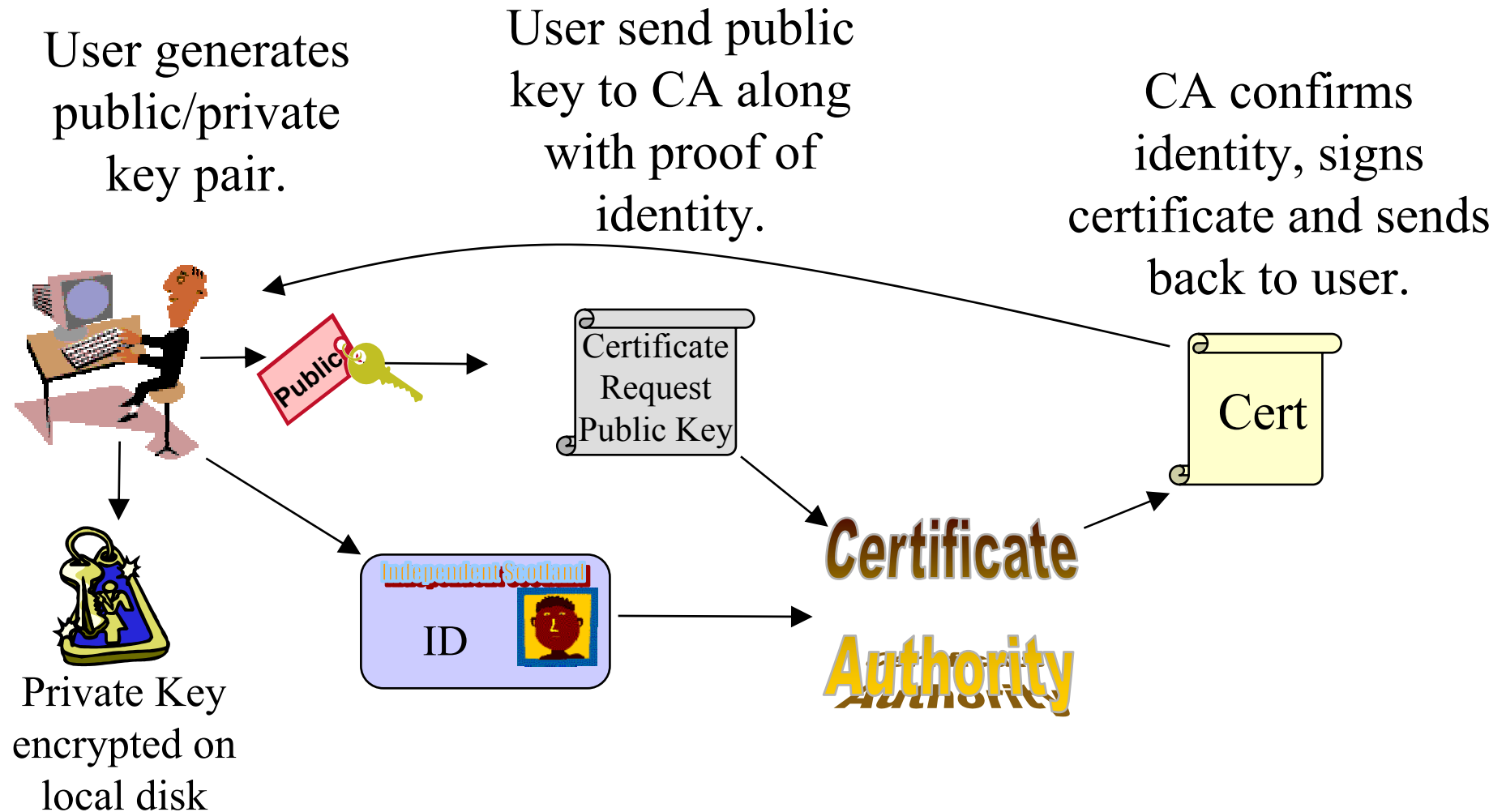
# Certificate Authorities

- A small set of trusted entities known as Certificate Authorities (CAs) are established to sign certificates
- A Certificate Authority is an entity that exists only to sign user certificates
- Users authenticate themselves to CA, for example by use of their Passport or Identity Card.
- The CA signs it's own certificate which is distributed in a secure manner.



Name: CA  
Issuer: CA  
CA's Public Key  
CA's Signature

# Certificate Request



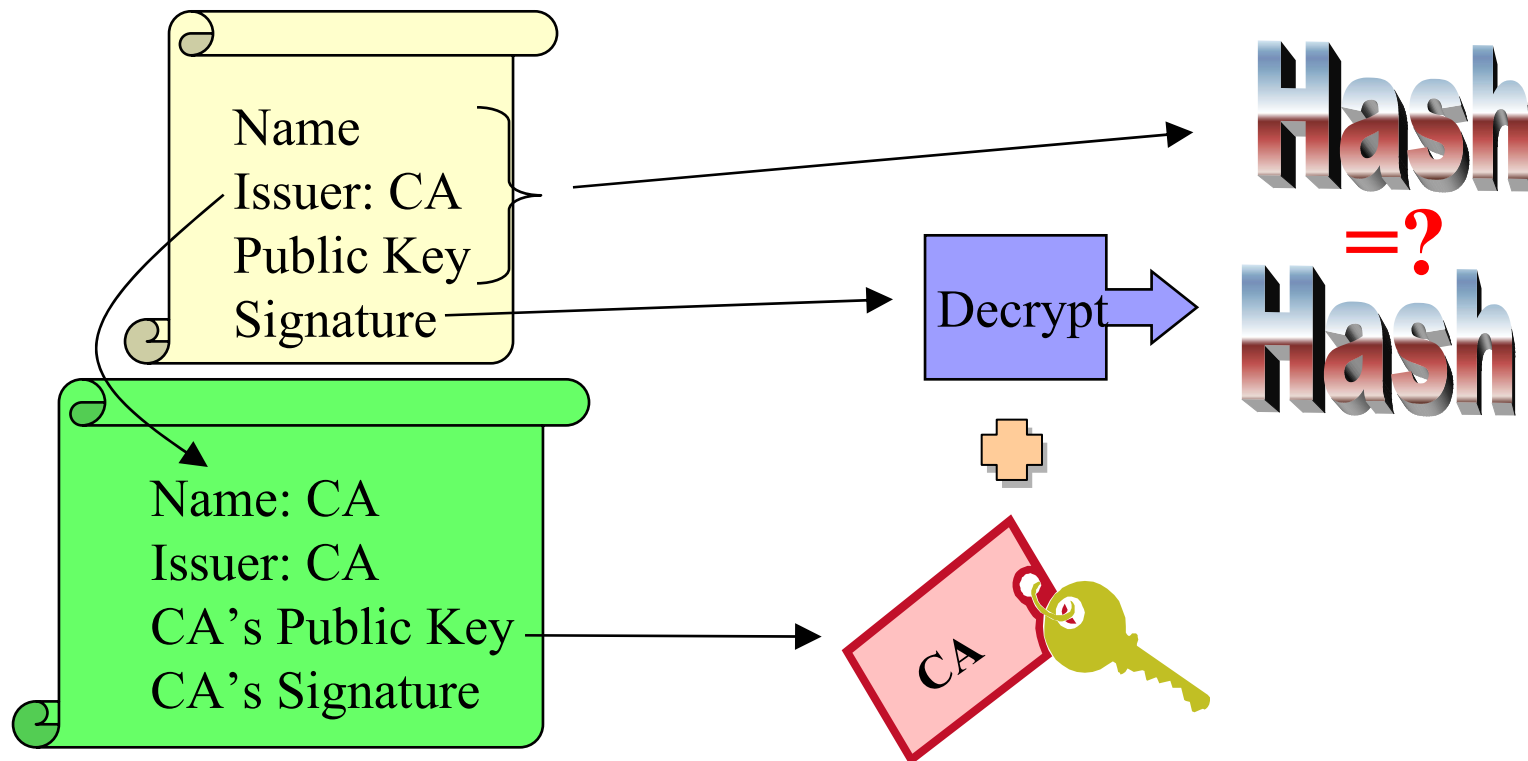
slide based on presentation given by Carl Kesselman at GGF Summer School 2004

# Inside the Certificate

- Standard (X.509) defined format.
- User identification (e.g. full name).
- Users Public key.
- A “signature” from a CA created by encoding a unique string (a hash) generated from the users identification, users public key and the name of the CA. The signature is encoded using the CA’s private key. This has the effect of:
  - Proving that the certificate came from the CA.
  - Vouching for the users identification.
  - Vouching for the binding of the users public key to their identification.

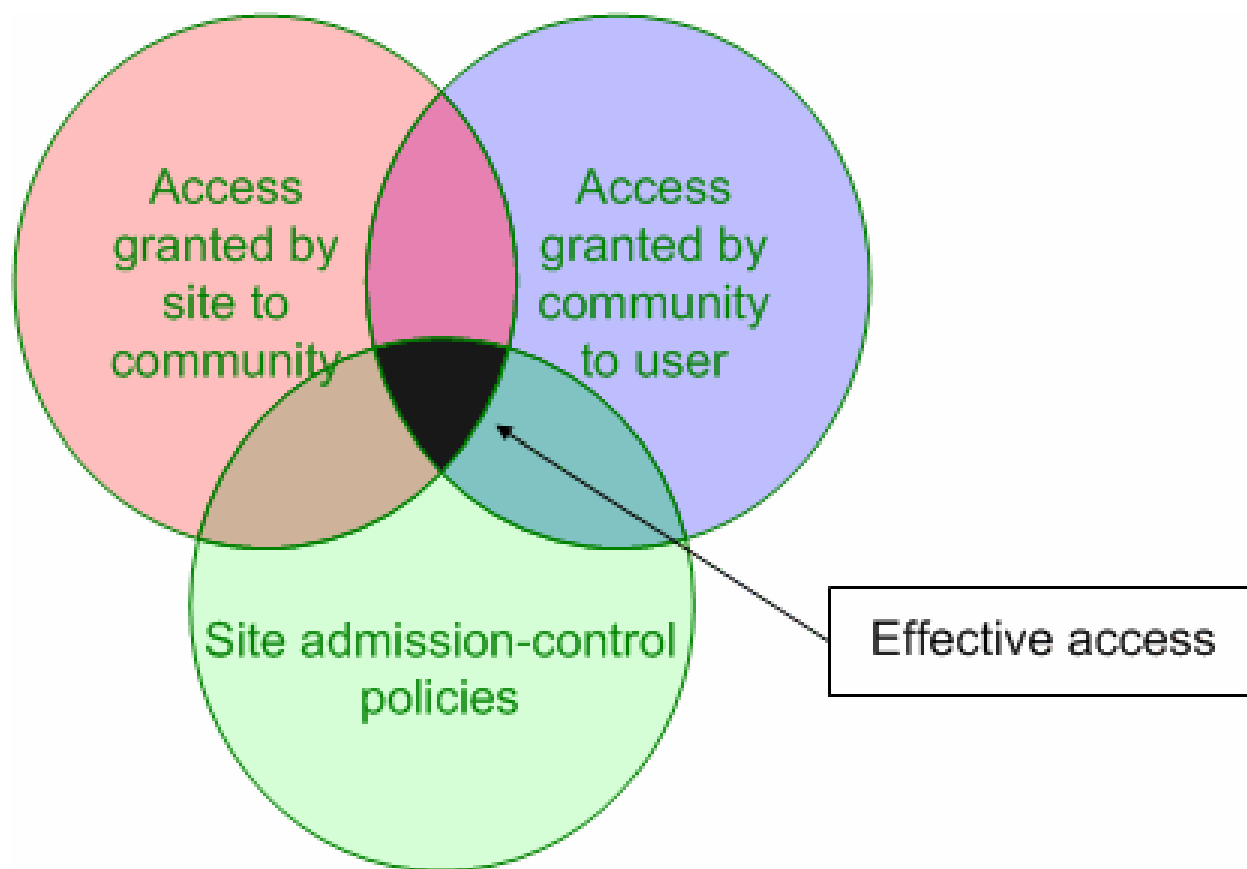
# Certificate Validity

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



slide based on presentation given by Carl Kesselman at GGF Summer School 2004

# User Authorisation to Access Resource



slide based on presentation given by Carl Kesselman at GGF Summer School 2004

# Authorisation Requirements

- Detailed user rights centrally managed and assigned:
  - User can have certain group membership and roles
- Involved parties:
  - Resource providers.
    - Keep full control on access rights.
  - The users Virtual Organisation.
    - Member of a certain group should have same access rights independent of resource.
- Resource provider and VO must agree on authorisation:
  - Resource providers evaluate authorisation granted by VO to a user and map into local credentials to access resources



# User Responsibilities

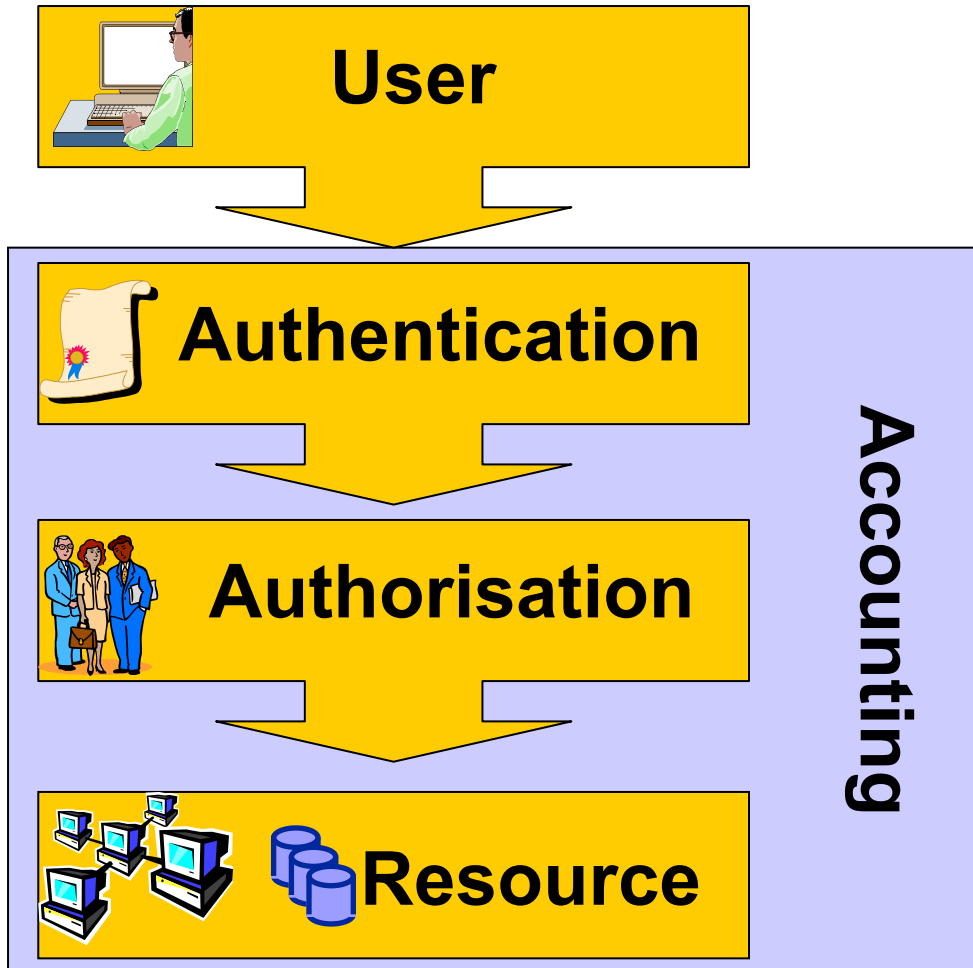
- Keep your private key secure.
- Do not loan your certificate to anyone.
- Report to your local/regional contact if your certificate has been compromised.
- Do not launch a delegation service for longer than your current task needs.

**If your certificate or delegated service is used by someone other than you, it cannot be proven that it was not you.**

# Summary

via Certificates and  
Delegated Services

delegated to VO.



# Acknowledgements



**Many slides in this presentation are based on the presentation given by Carl Kesselman at the GGF Summer School 2004. This presentation may be found at**

**<http://www.dma.unina.it/~murli/GridSummerSchool2004/curriculum.htm>**

# Grid Security Infrastructure (GSI)

- Globus Toolkit™ proposed and implements the Grid Security Infrastructure (GSI)
  - Protocols and APIs to address Grid security needs
- GSI protocols **extend standard public key protocols**
  - Standards: X.509 & SSL/TLS
  - Extensions: X.509 Proxy Certificates (single sign-on) & Delegation
- GSI extends standard GSS-API (Generic Security Service)
  - The GSS-API is the IETF standard for adding authentication, delegation, message integrity, and message confidentiality to applications.
- **Proxy Certificate:**
  - Short term, restricted certificate that is derived from a long-term X.509 certificate
  - Signed by the normal end entity cert, or by another proxy
  - Allows a process to act on behalf of a user
  - Not encrypted and thus needs to be securely managed by file system

# Example: VO-LDAP server for Authorisation

