Enabling Grids for E-science in Europe

International Summer School for Grid Computing , Vico Equense, 10 - 22.6.2005

Security

NeSC Training Team

Why security?

- Information has value
  - Copyright
  - Patent
- Responsibility
  - To ensure good behavior on resources held in common requires that actions can be linked to individuals – audit trails
- Confidence
  - Users will not use a system which is not trusted
  - Resource providers will not allow their resources onto an insecure system
    - Not just hardware resources, data resources are crucial too.

The value of information

- Small pieces of information may seem of little value
  - However in large groupings may reveal valuable patterns
  - - Traffic analysis in military intelligence
  - - Individual genetics -> population genetics
  - - Analysis of spending patterns from receipts
- People value privacy
  - Although mostly when noticeably removed

Is this new?

- Communities and organisations have been managing access to common resources for millennia
  - Although frequently not successfully
    - “tragedy of the commons”
    - Over grazing – dustbowl, Mediterranean environments ? (goats)
  - Because this is a HARD problem

- States continually struggle with the idea of authentication
  - Balance the need for authentication with the need for freedom/privacy

- Should/can computing solutions be different?

Security Concepts (triple A)

- 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?

The Virtual Organisation

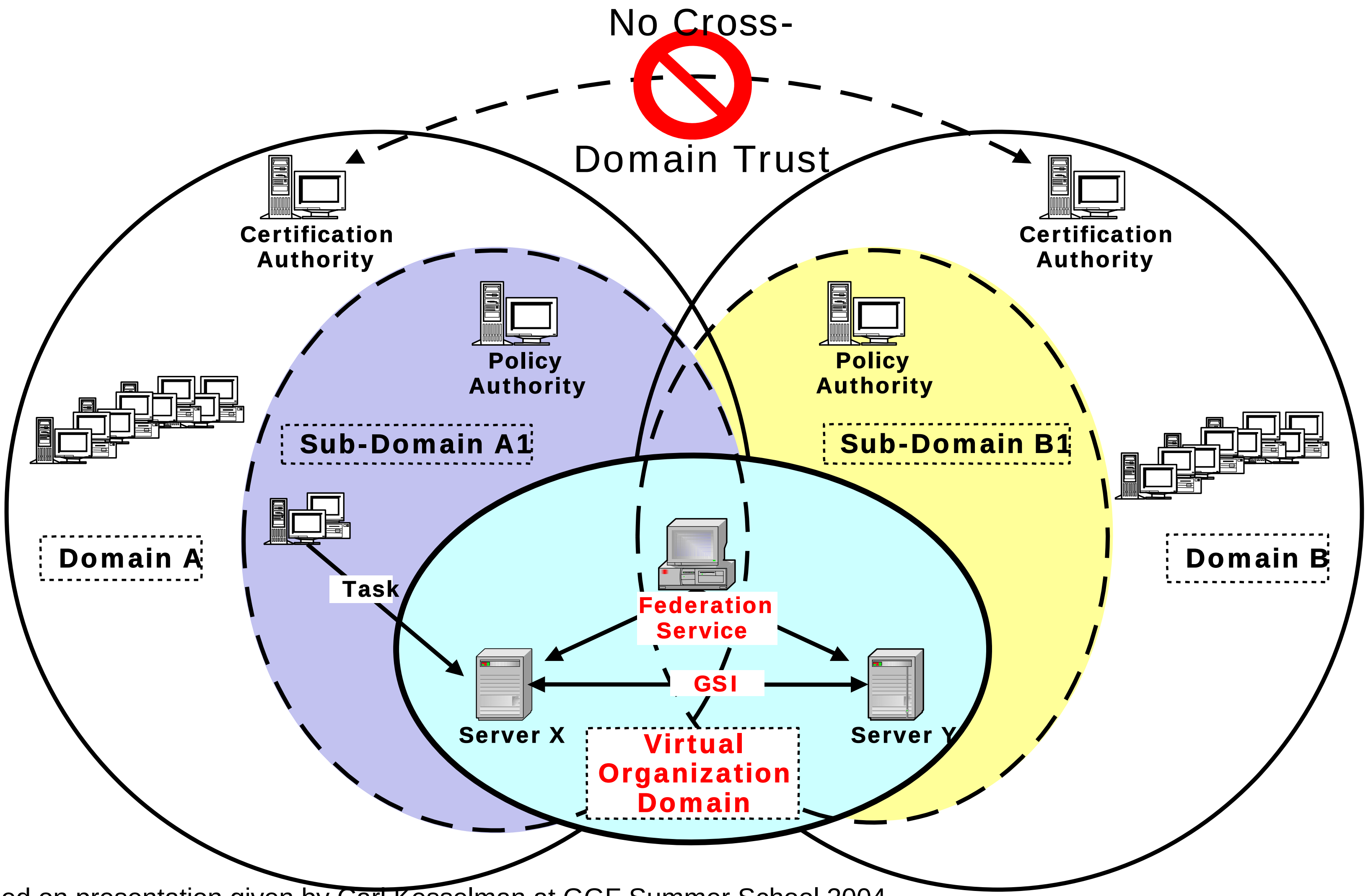
- This term was coined to describe a distributed organisation which has the task of managing access to resources which are accessed through computer network
- Implementations have been created which have their own more specialised definitions of the term
  - Eg. EGEE

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



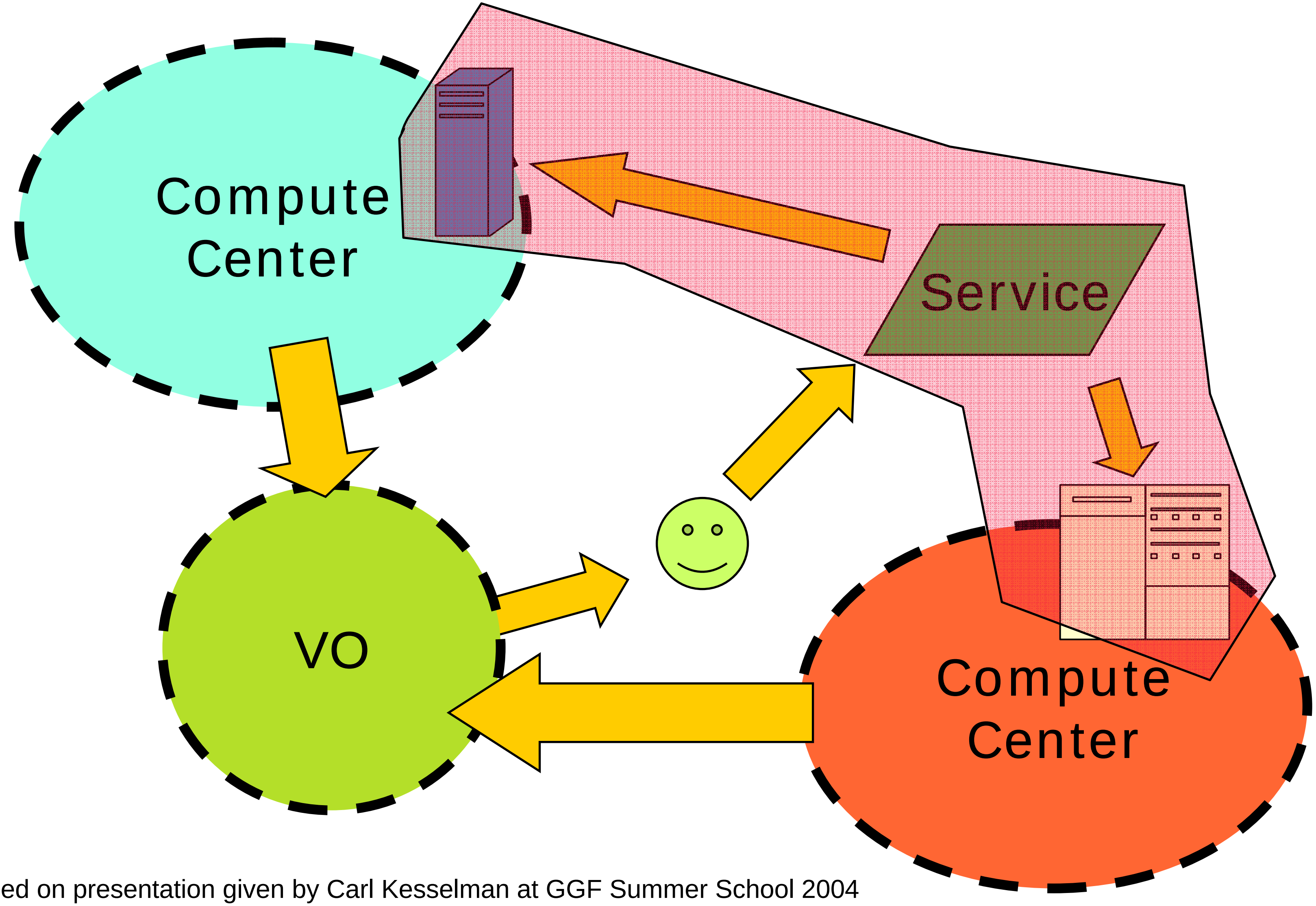
slide based on presentation given by Carl Kesselman at GGF Summer School 2004

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.
- An organisation delegates its rights to a user.
- A user delegates their authentication to a service to allow programs to run on remote sites.

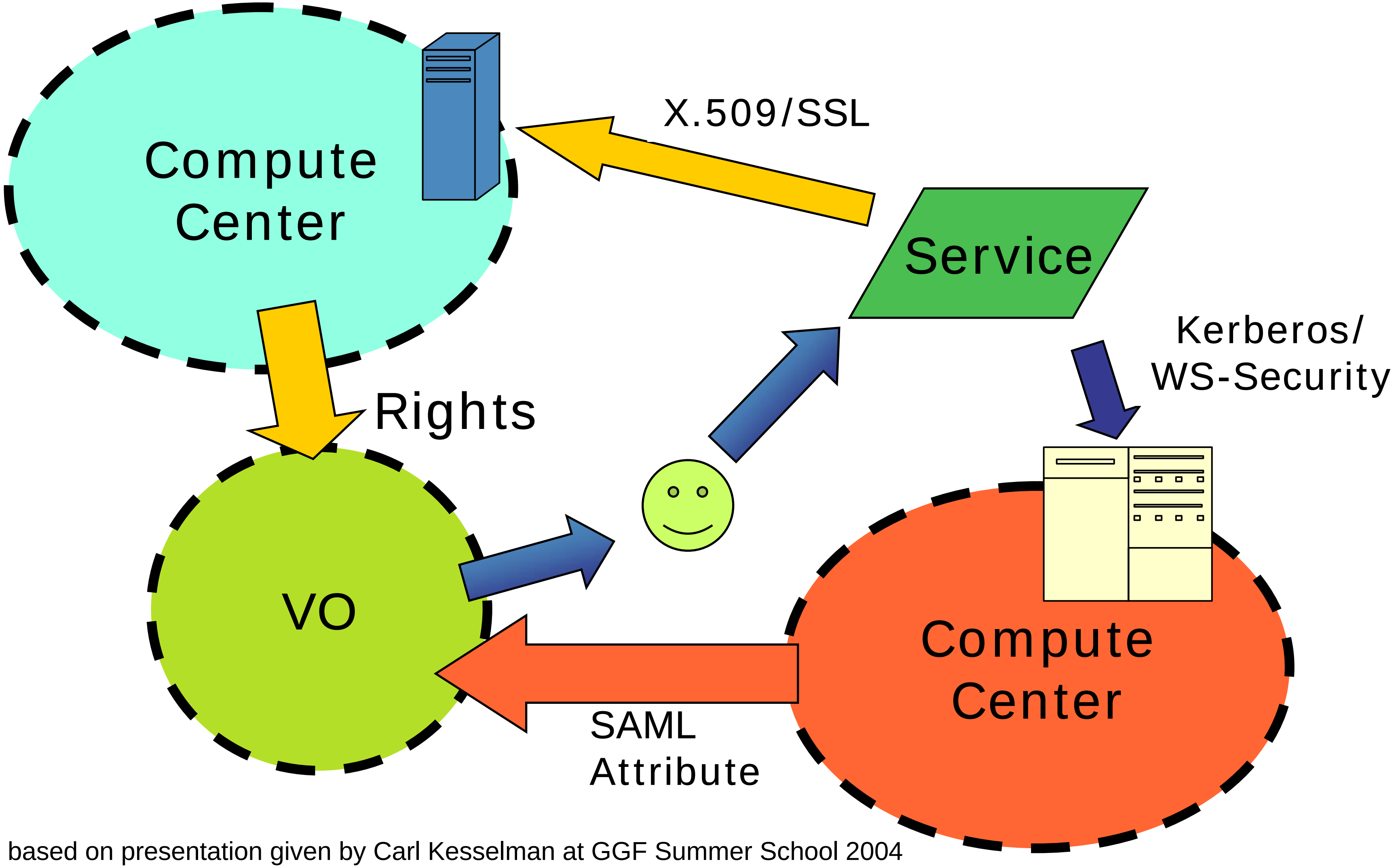
Use Delegation to Establish Dynamic Distributed System



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

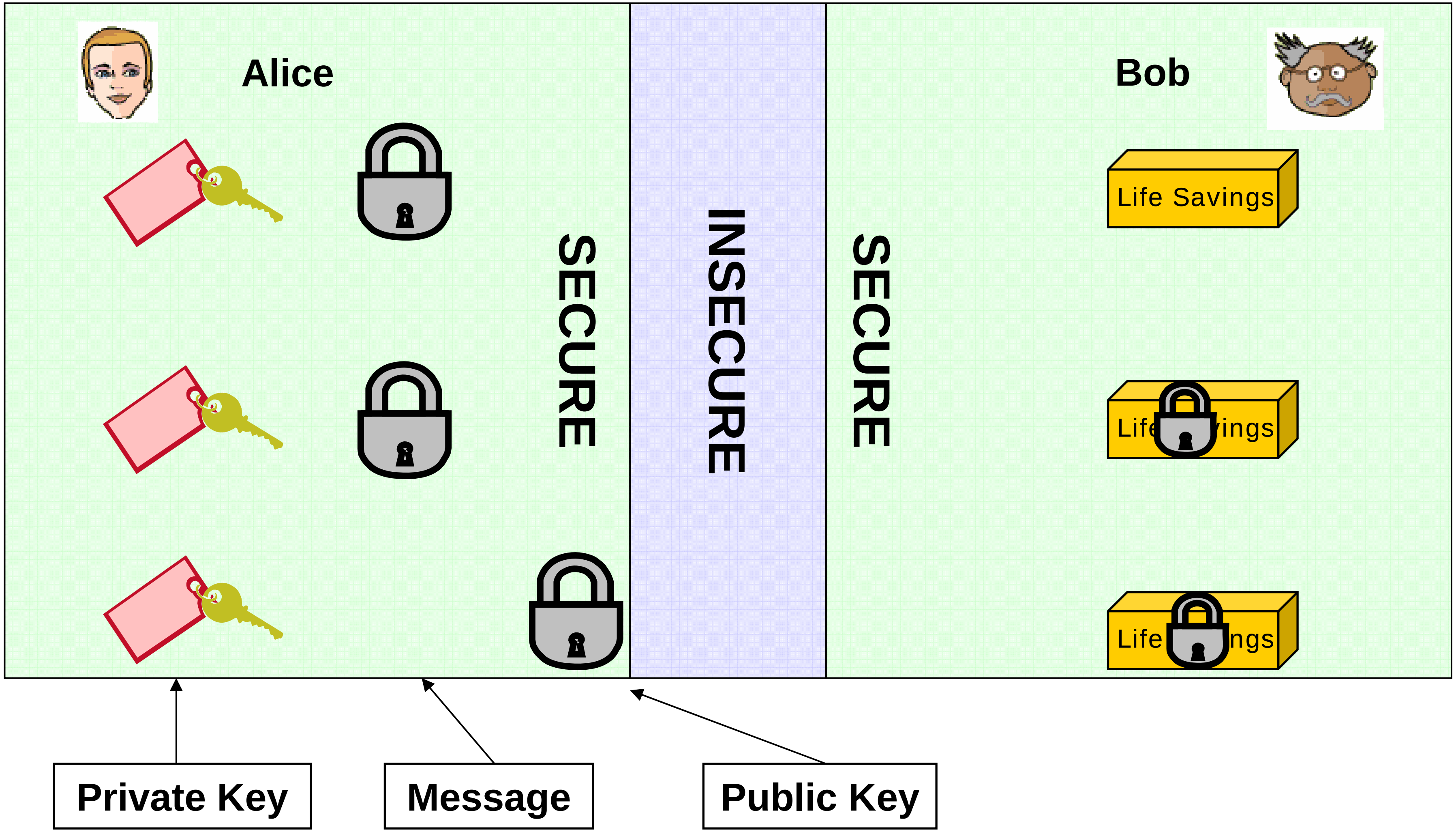
Goal is to do this with arbitrary mechanisms

Enabling Grids for E-science in Europe



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

Public Private Key



Private Key

Message

Public Key

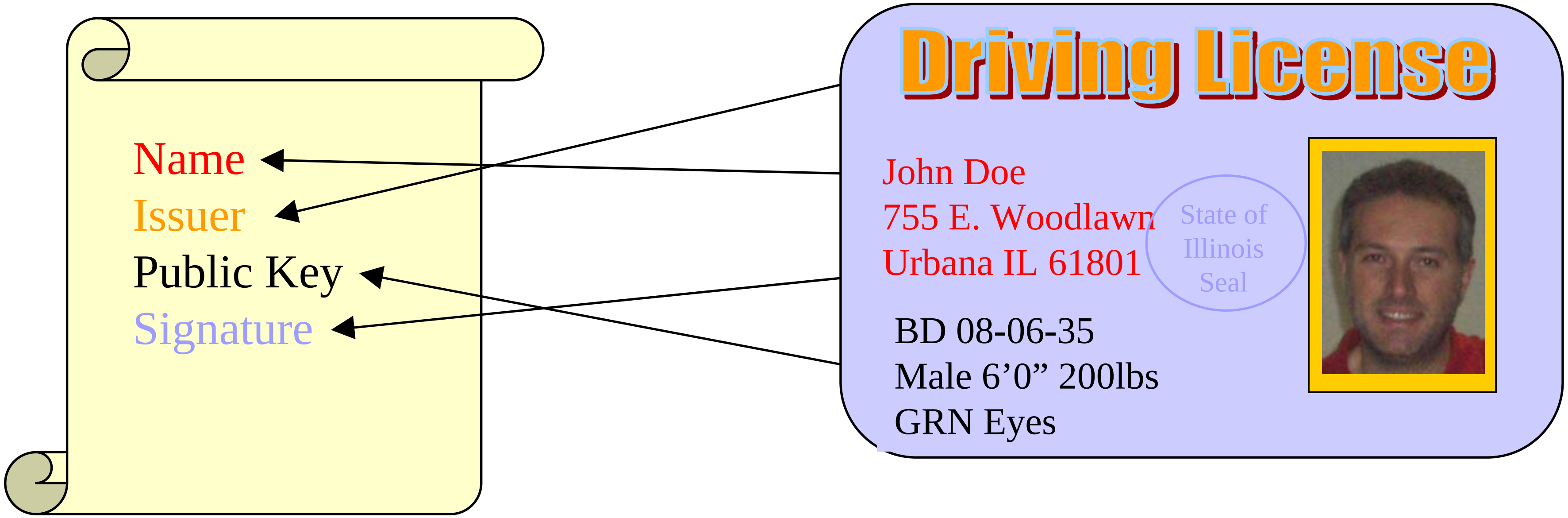
Public Key Infrastructure (PKI)

- 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.

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

Certificates

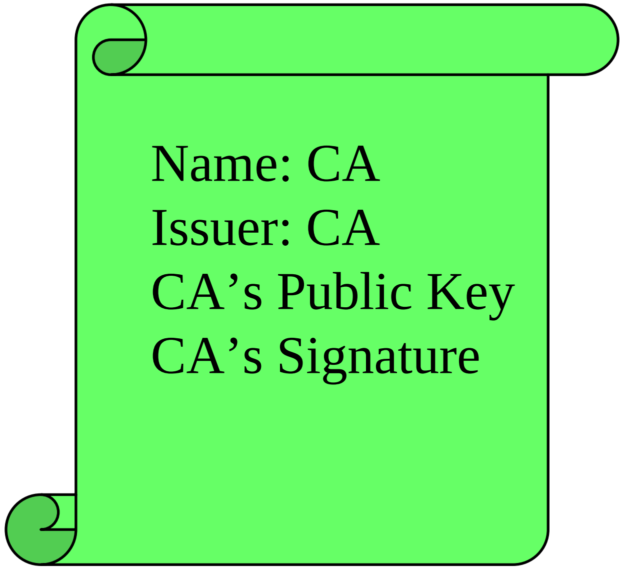
- Similar to passport or driver's license: Identity signed by a trusted party



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

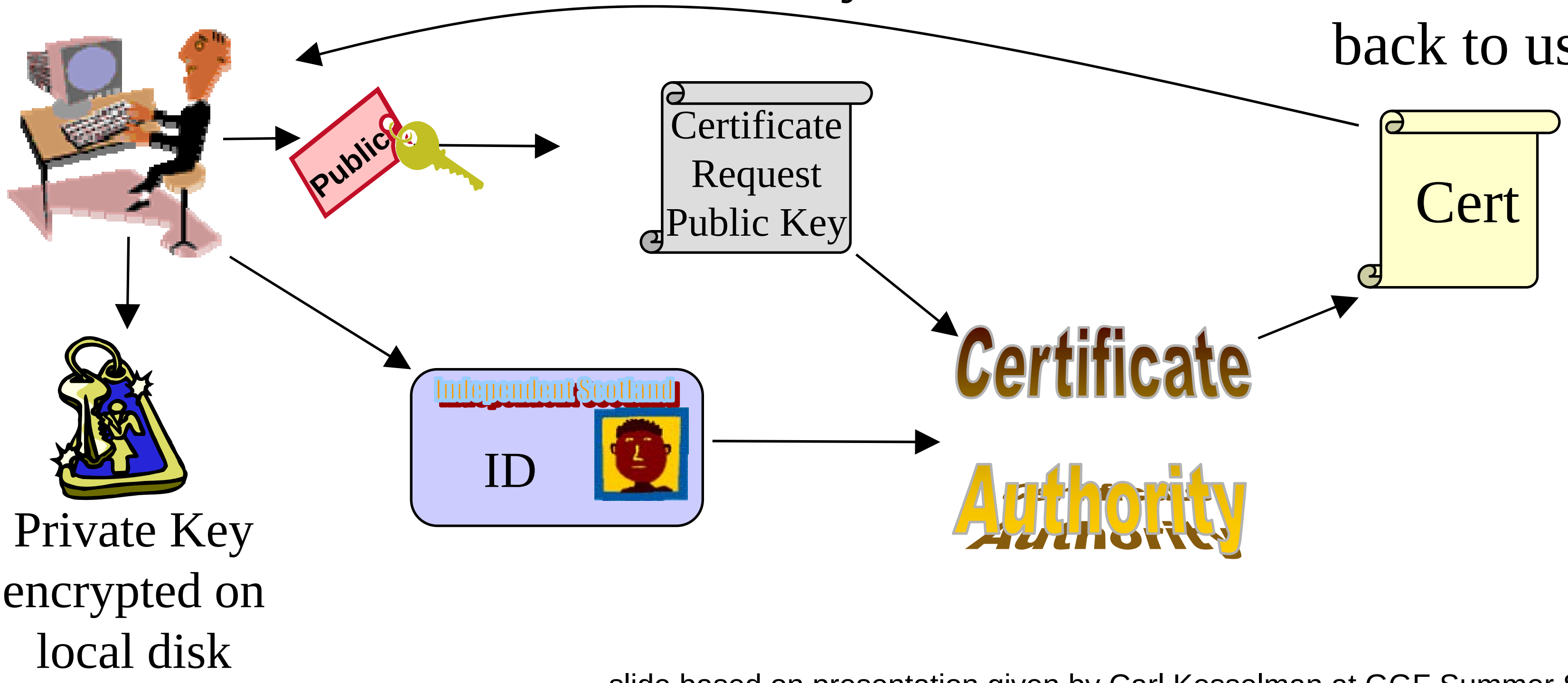
slide based on presentation given by Carl Kesselman at GGF Summer School 2004

Certificate Request

User generates public/private key pair.

User send public key to CA along with proof of identity.

CA confirms identity, signs certificate and sends back to user.



Public

Certificate Request Public Key

Cert

Private Key encrypted on local disk

Independent Scotland

ID

Certificate Authority

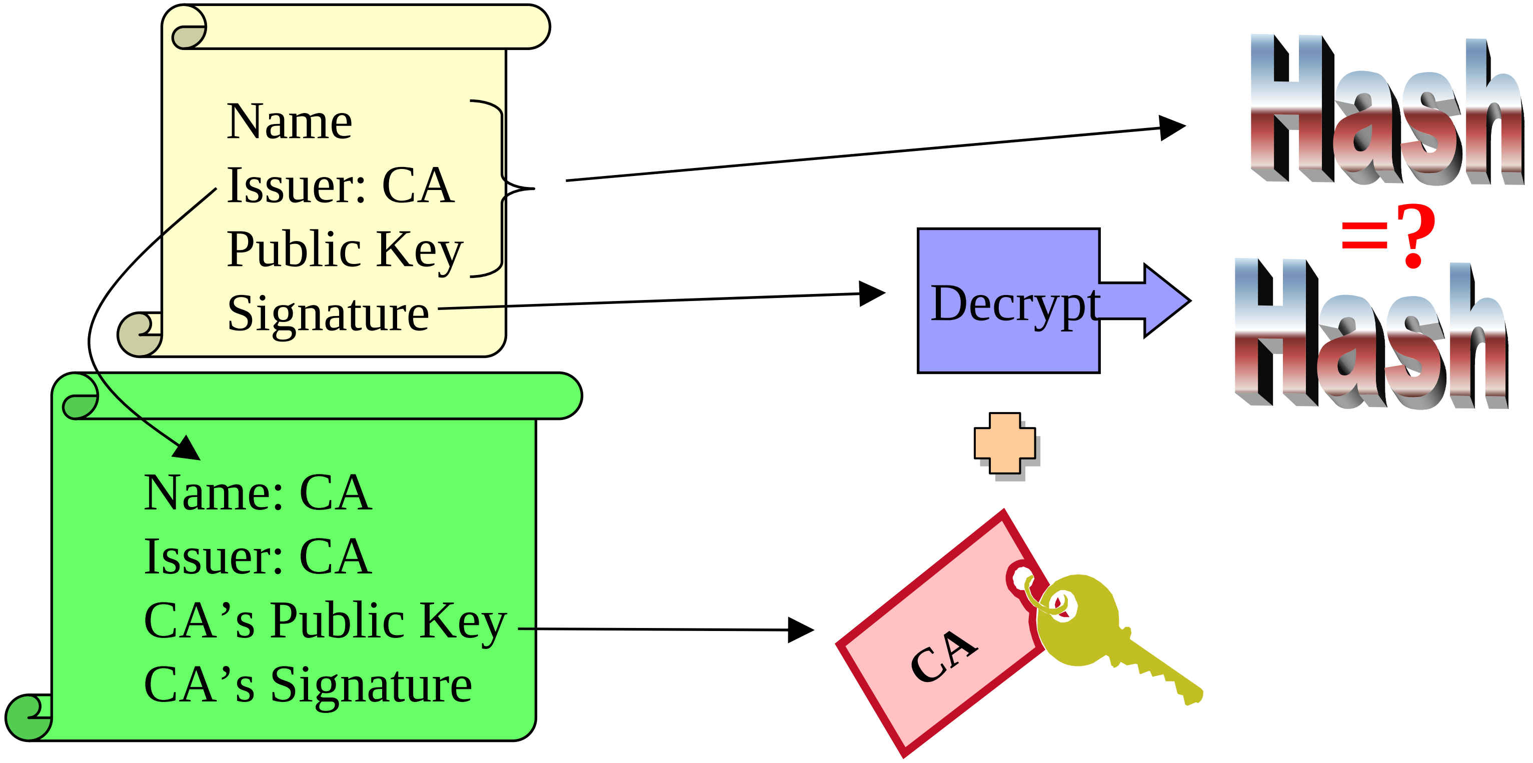
slide based on presentation given by Carl Kesselman at GGF Summer School 2004

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.

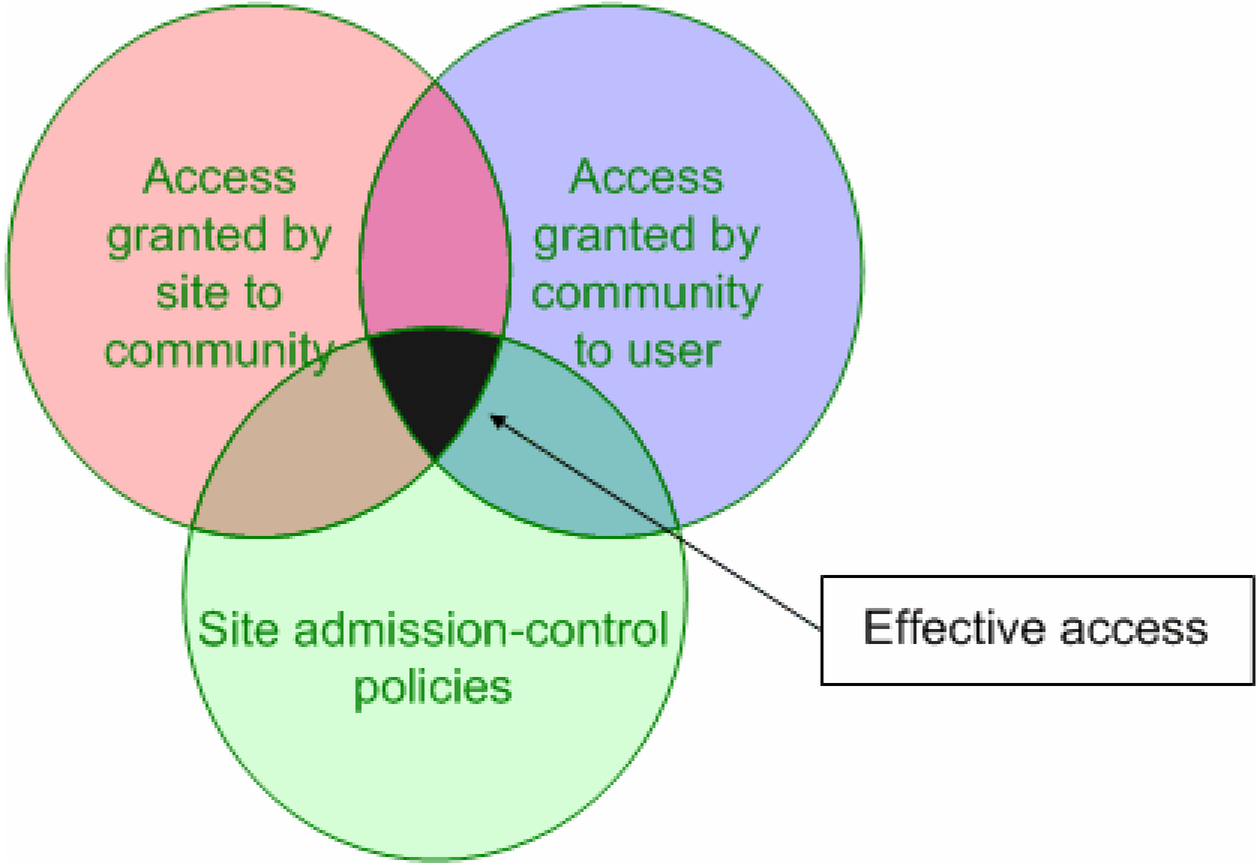
Certificate Validity

- 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


Access granted by site to community
Access granted by community to user
Site admission-control policies
Effective access

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

Authorisation Requirements

- Detailed user rights 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.

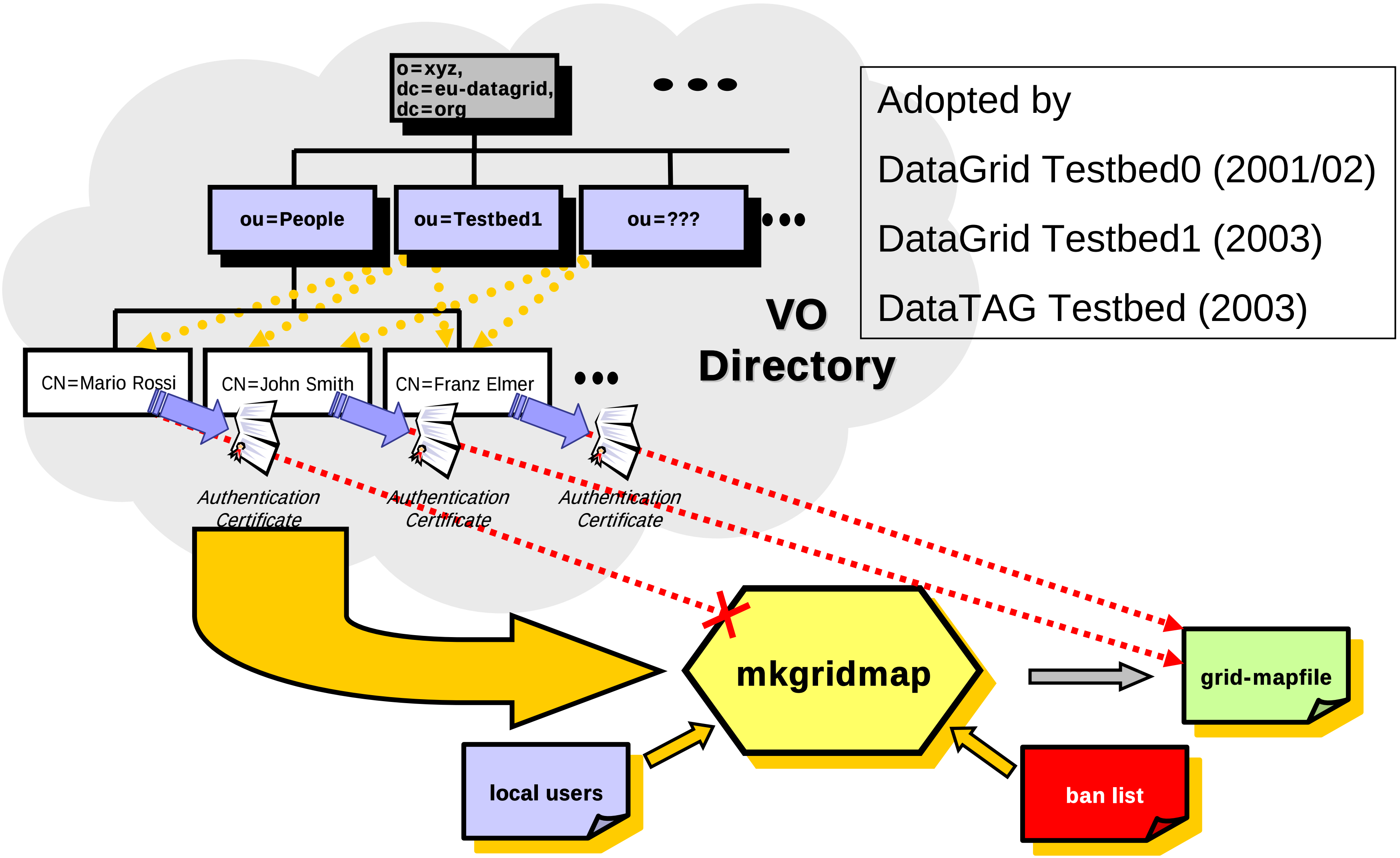
If your certificate or delegated service is used by someone other than you, it cannot be proven that it was not you.

IT IS YOUR PASSPORT AND CREDIT CARD

Grid Security Infrastructure (GSI)

- Globus Toolkit^{TM} 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 form 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



Adopted by

DataGrid Testbed0 (2001/02)

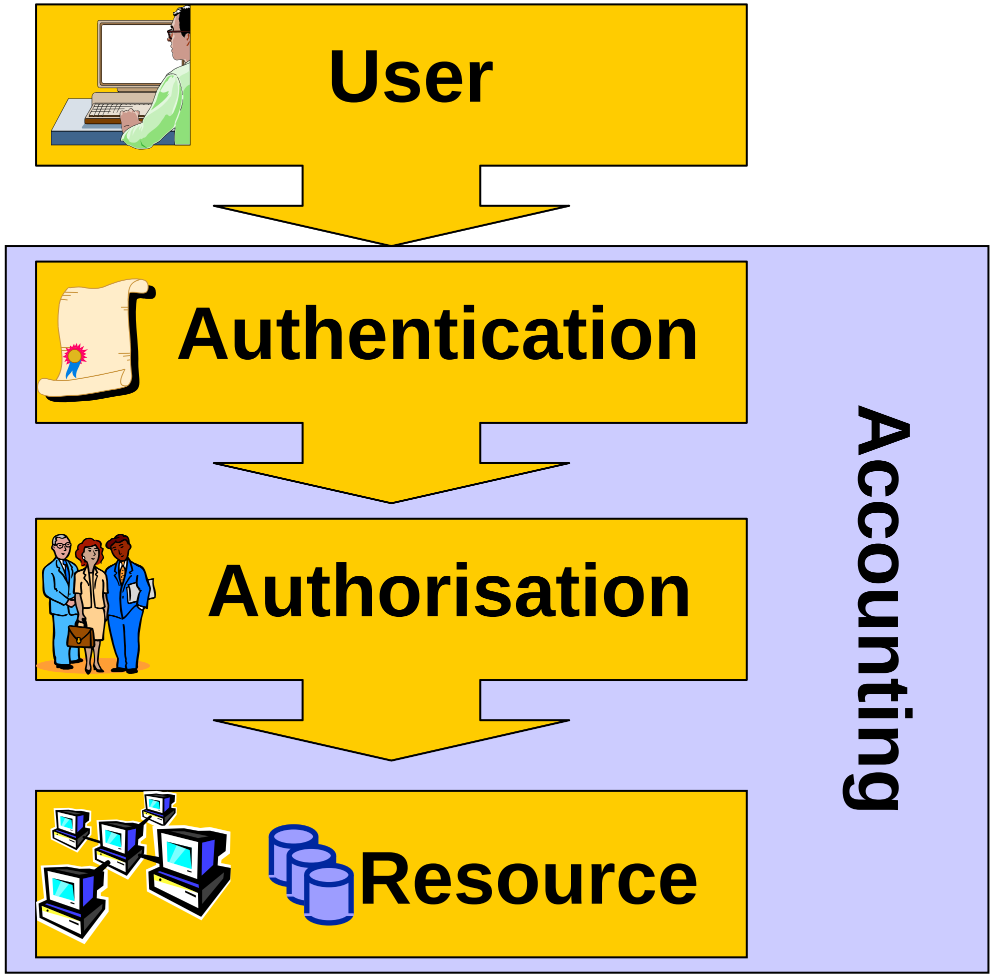
DataGrid Testbed1 (2003)

DataTAG Testbed (2003)

Summary

via Certificates and Delegated Services

delegated to VO



Finer grained security

- A user may have different rights in different contexts
- Systems being deployed which give finer grained access
  - Roles (eg. Sys admin, user, clinician, top secret clearance, etc)
  - VOMS, Permis

Acknowledgements

Enabling Grids for E-science in Europe

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