the globus toolkit™
www.globustoolkit.org

Grid Security Overview

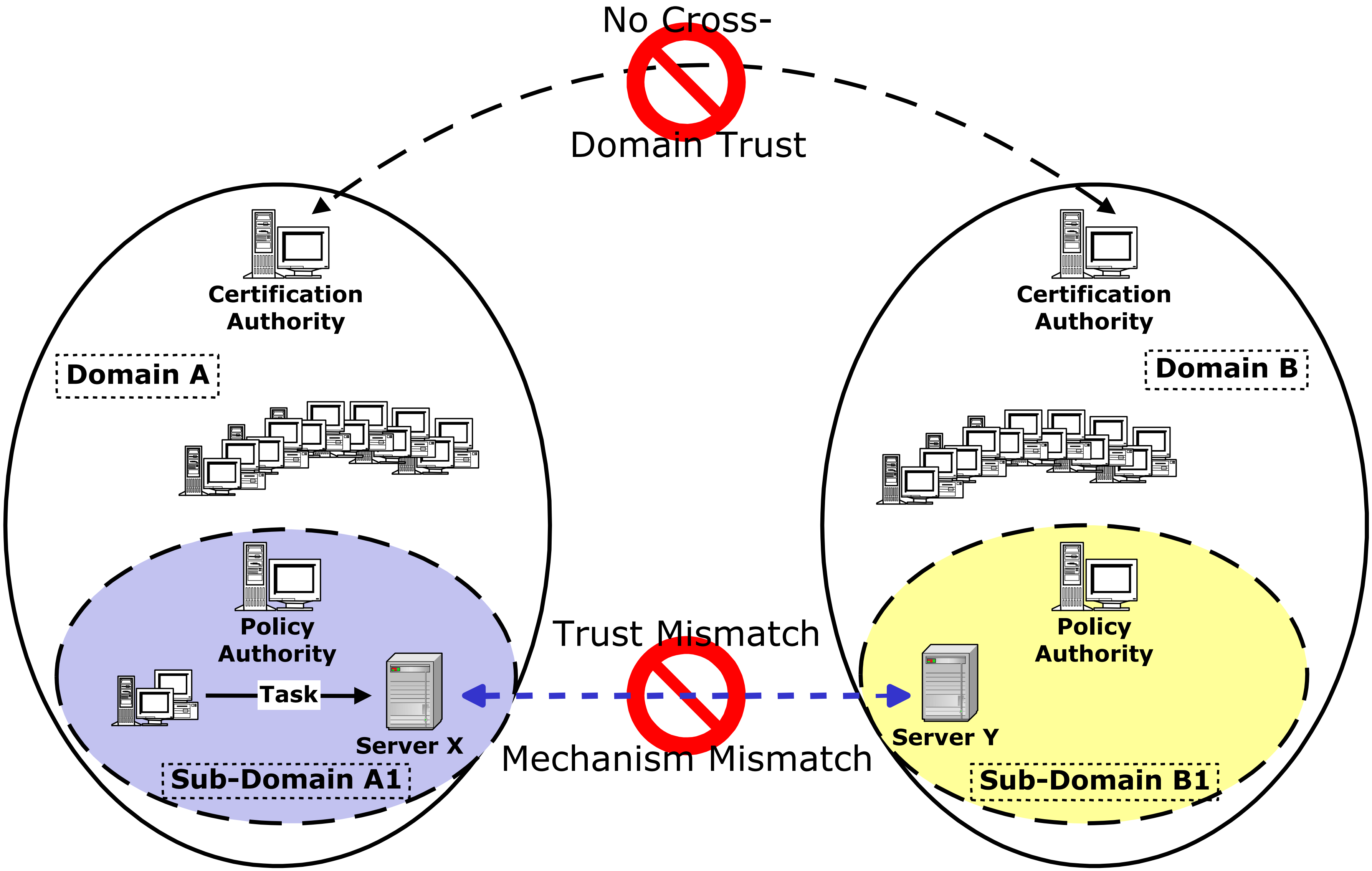
The Globus Project™

http://www.globus.org/

Security Terminology

- Authentication: Establishing identity
- Authorization: Establishing rights
- Message protection
  - Message integrity
  - Message confidentiality
- Non-repudiation
- Digital signature
- Accounting
- Delegation

Multi-Institution Issues



Why Grid Security is Hard

- Resources being used may be valuable & the problems being solved sensitive
  - Both users and resources need to be careful
- 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
    - X.509 vs Kerberos, SSL vs GSSAPI,
      X.509 vs. X.509 (different domains),
    - X.509 attribute certs vs SAML assertions

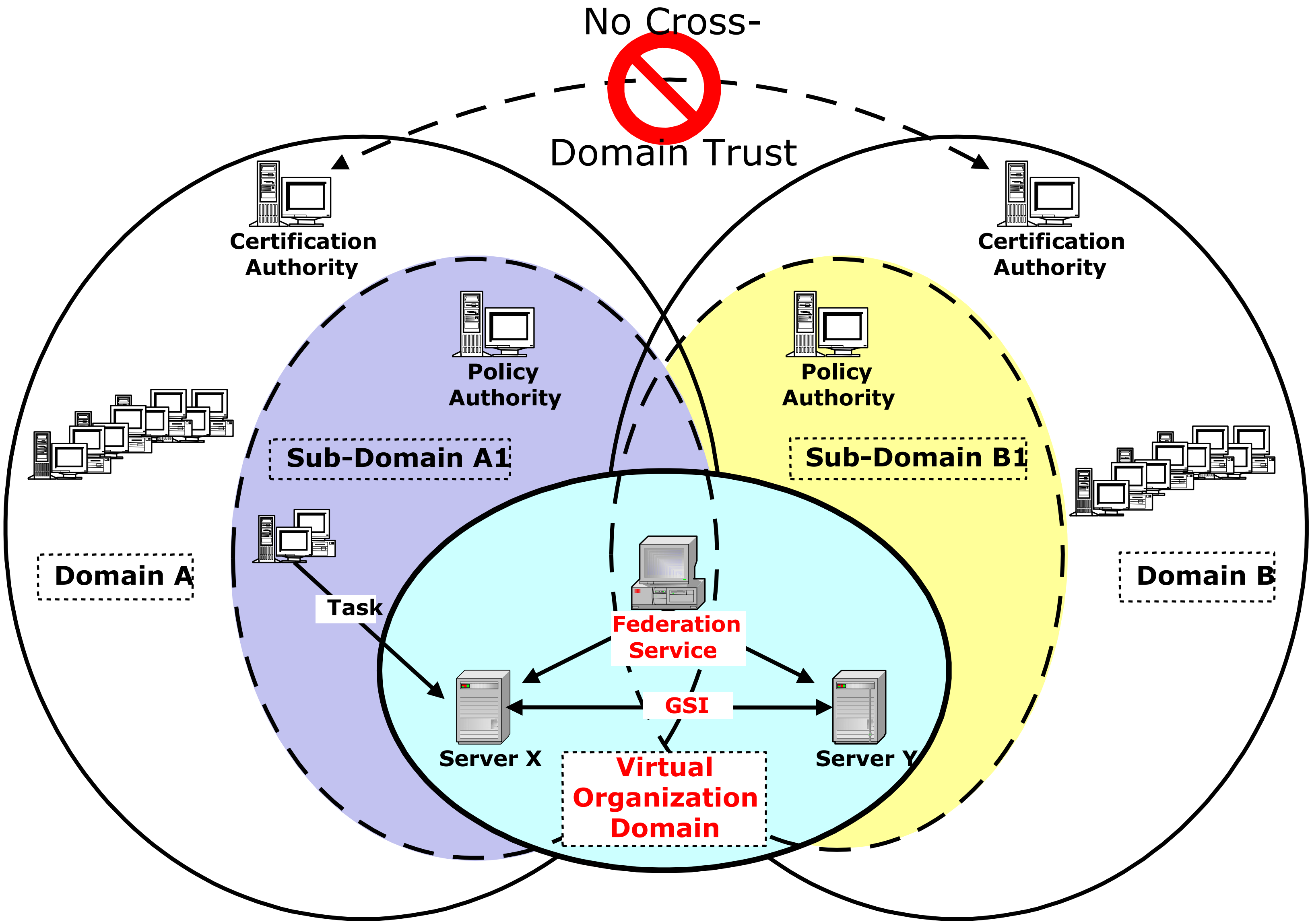
Why Grid Security is Hard…

- 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
- Standardization of interfaces to allow for discovery, negotiation and use
- Implementation must be broadly available & applicable
  - Standard, well-tested, well-understood protocols; integrated with wide variety of tools
- Policy from sites, VO, users need to be combined
  - Varying formats
- Want to hide as much as possible from applications!

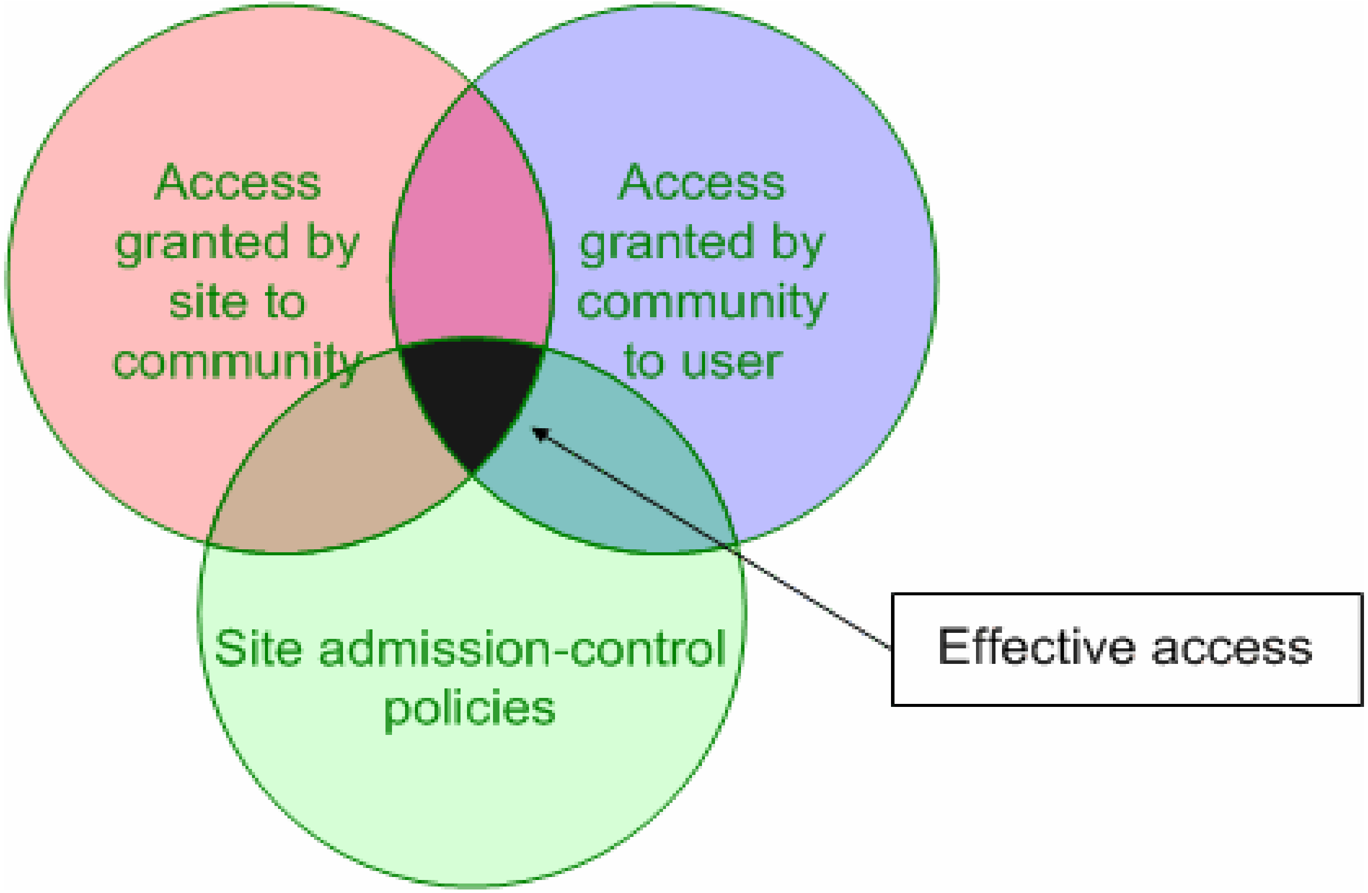
The Grid Trust solution

- Instead of setting up trust relationships at the organizational level (lots of overhead, possible legalities - expensive!) set up trust at the user/resource level
- Virtual Organizations (VOs) for multi-user collaborations
  - Federate through mutually trusted services
  - Local policy authorities rule
- Users able to set up dynamic trust domains
  - Personal collection of resources working together based on trust of user

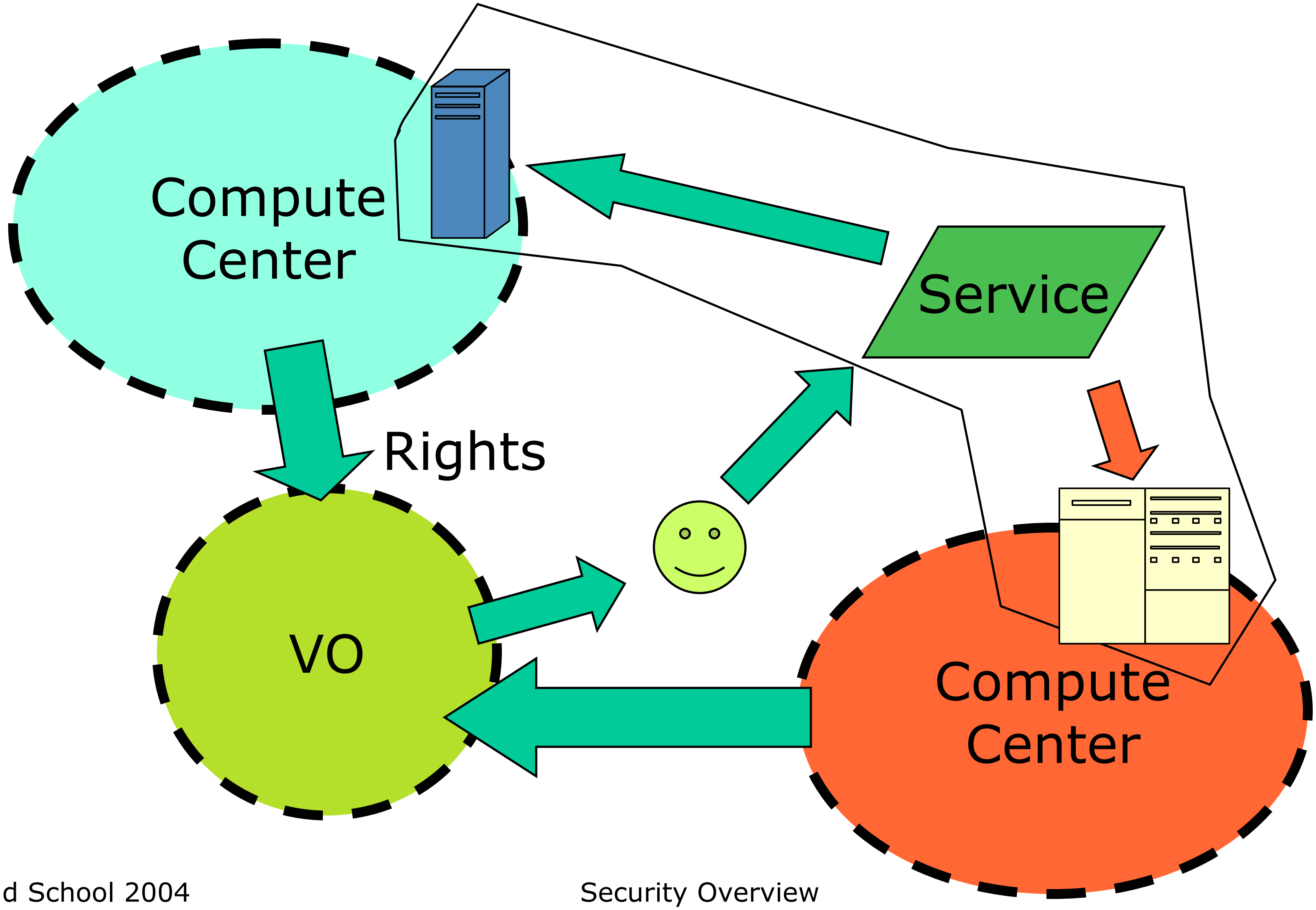
Grid Solution: Use Virtual Organization as Bridge



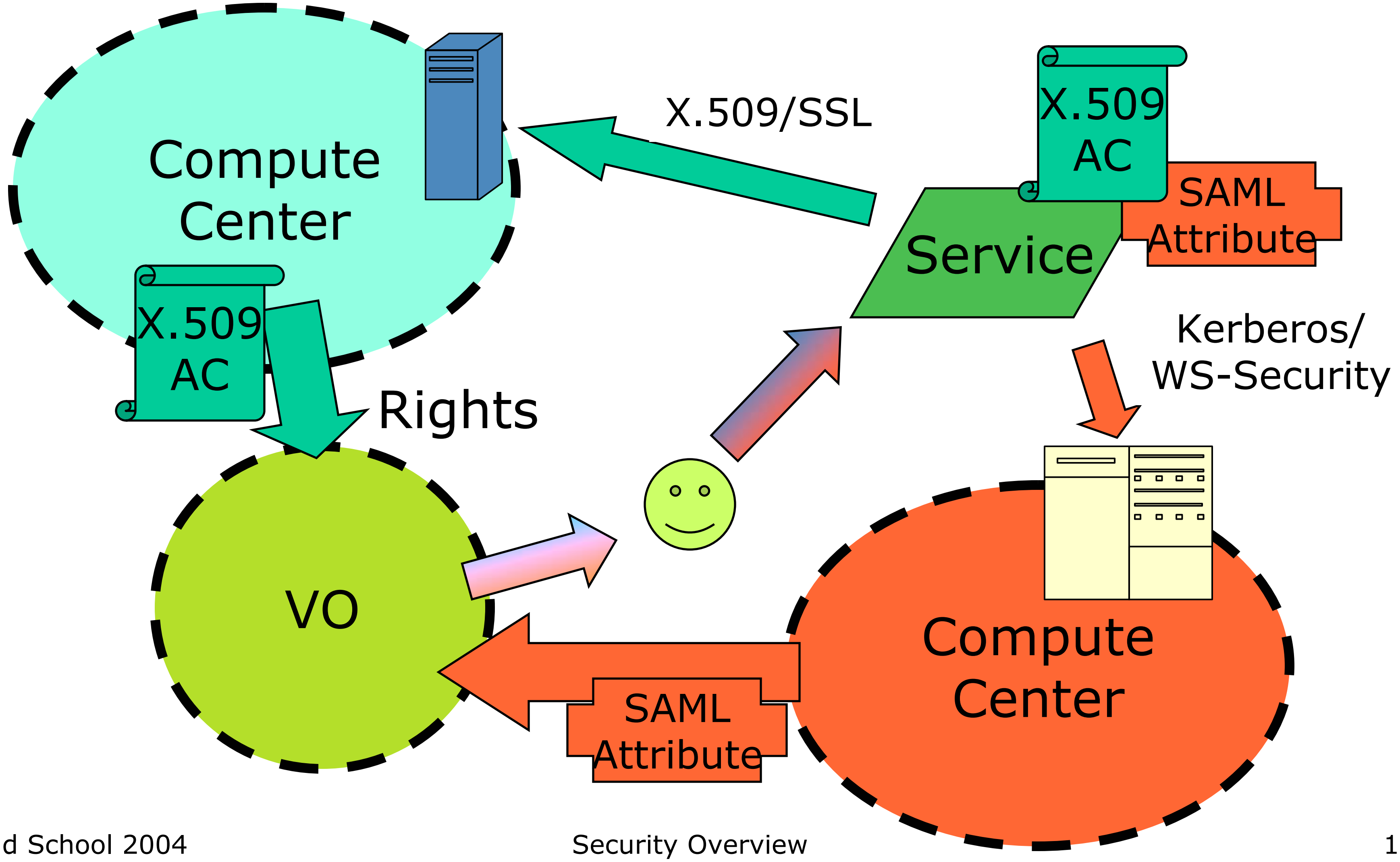
Effective Policy Governing Access Within A Collaboration


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

Use Delegation to Establish Dynamic Distributed System



Goal is to do this with arbitrary mechanisms



Grid Security Infrastructure (GSI)

- Use GSI as a standard mechanism for bridging disparate security mechanisms
  - Doesn't solve trust problem, but now things talk same protocol and understand each other's identity credentials
  - Basic support for delegation, policy distribution
- Translate from other mechanisms to/from GSI as needed
- Convert from GSI identity to local identity for authorization

GSI

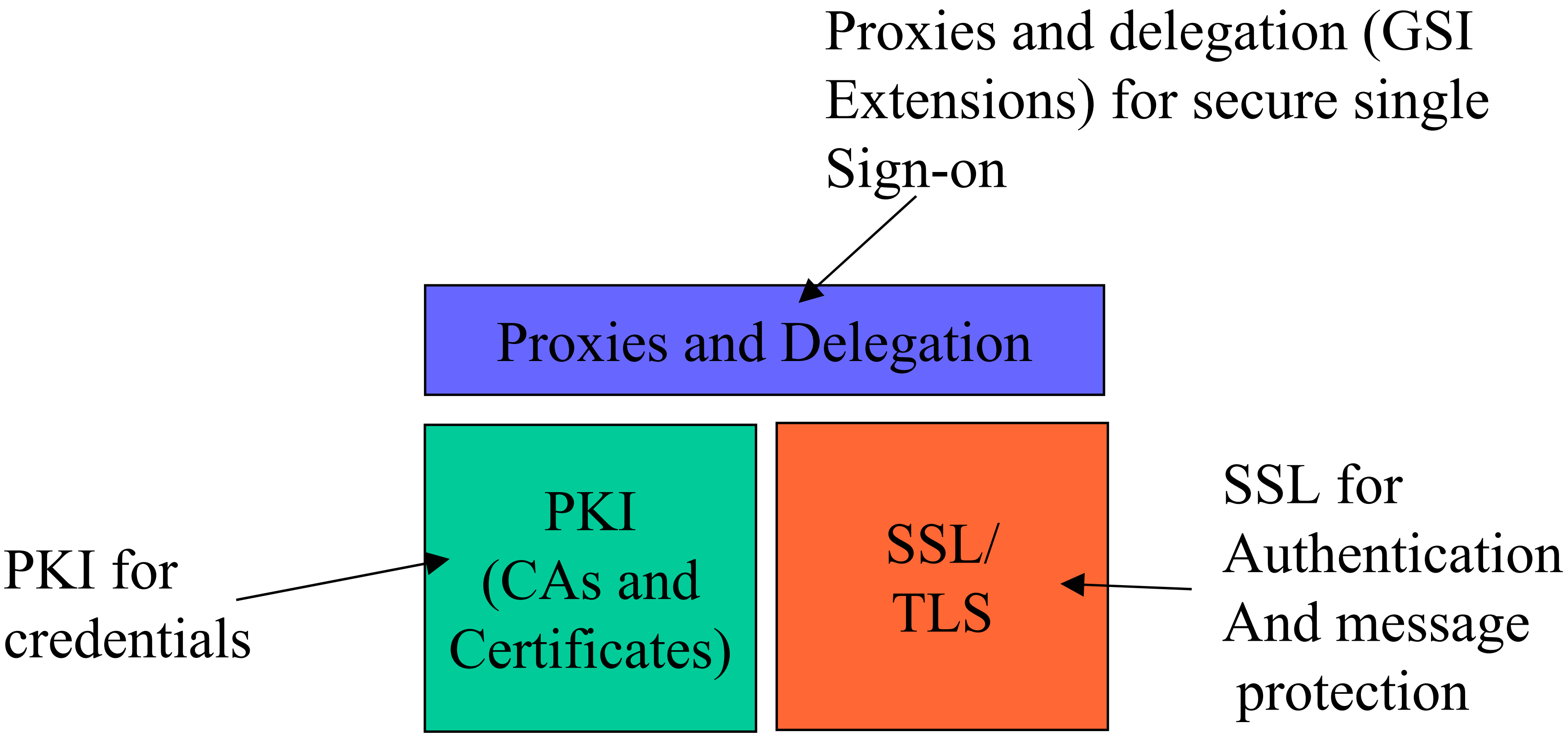
- GSI implements X.509 Proxy Certificates as extensions to these standards to support dynamic naming of services, delegation of rights and single sign-on
- After authentication, GSI identity is mapped by administer configuration to a local identity for authorization.
  - Local identity controls access to local files, job startup rights, etc.

Grid Security Infrastructure (GSI)

- Based on standard PKI technologies
  - SSL protocol for authentication, message protection
  - CAs allow one-way, light-weight trust relationships (not just site-to-site)
- X.509 Certificates for asserting identity
  - for users, services, hosts, etc.
- Proxy Certificates
  - GSI extension to X.509 certificates for delegation, single sign-on

Grid Security Infrastructure (GSI)

- GSI is:



Proxies and delegation (GSI Extensions) for secure single Sign-on

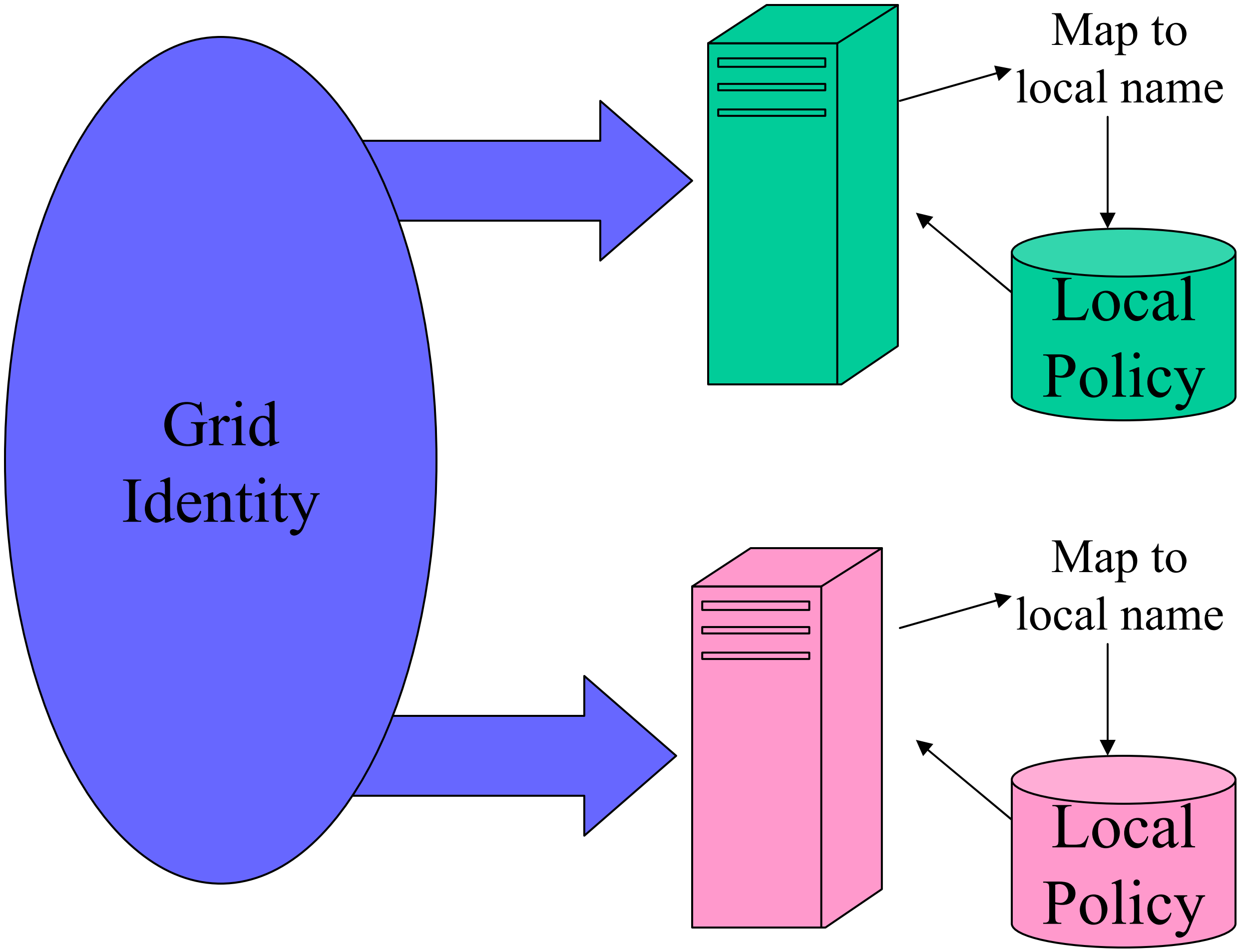
PKI for credentials

SSL for Authentication And message protection

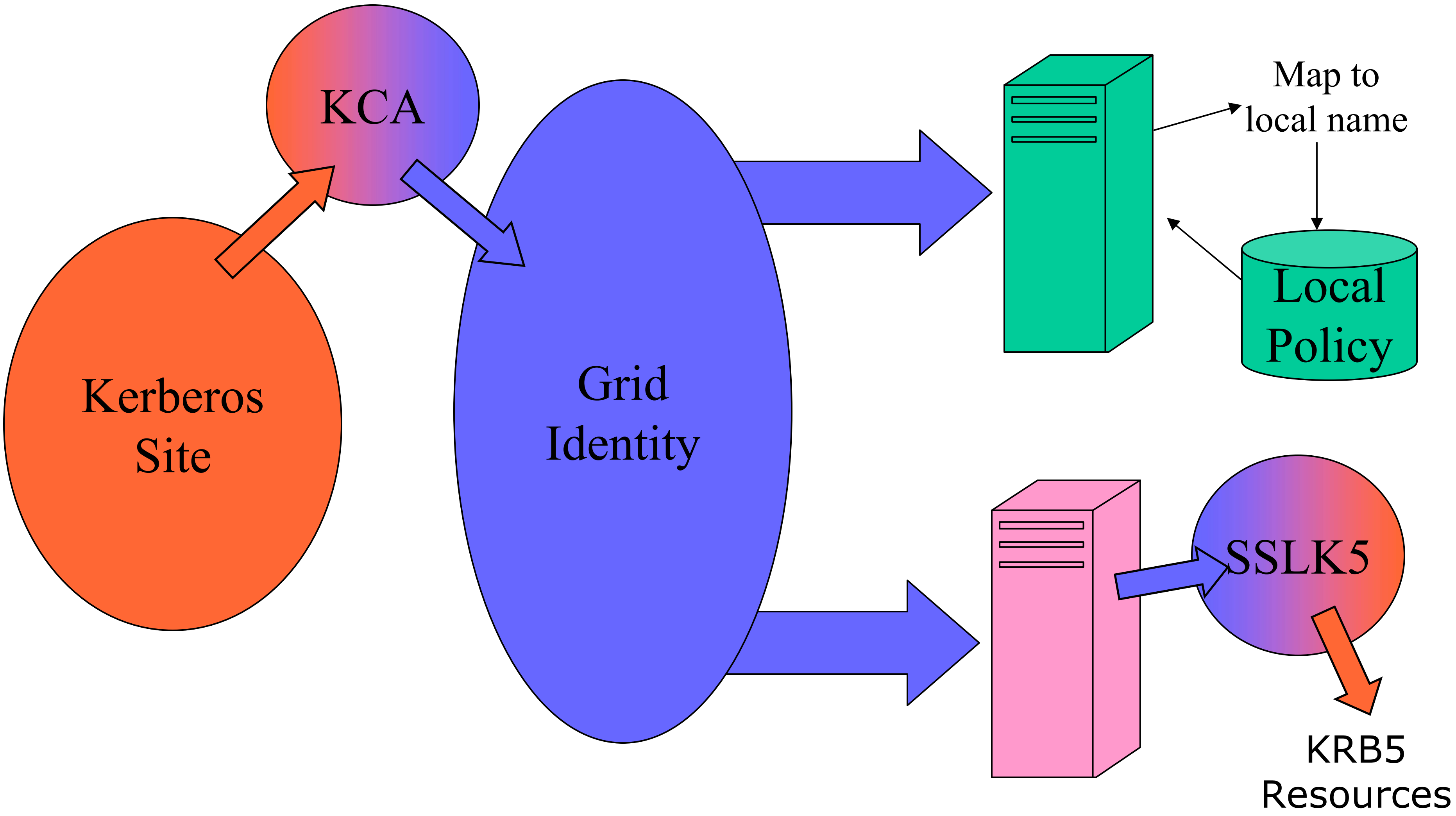
Grid Identity, Local Policy

- In current model, all Grid entities assigned a PKI identity.
- User is mapped to local identities to determine local policy.

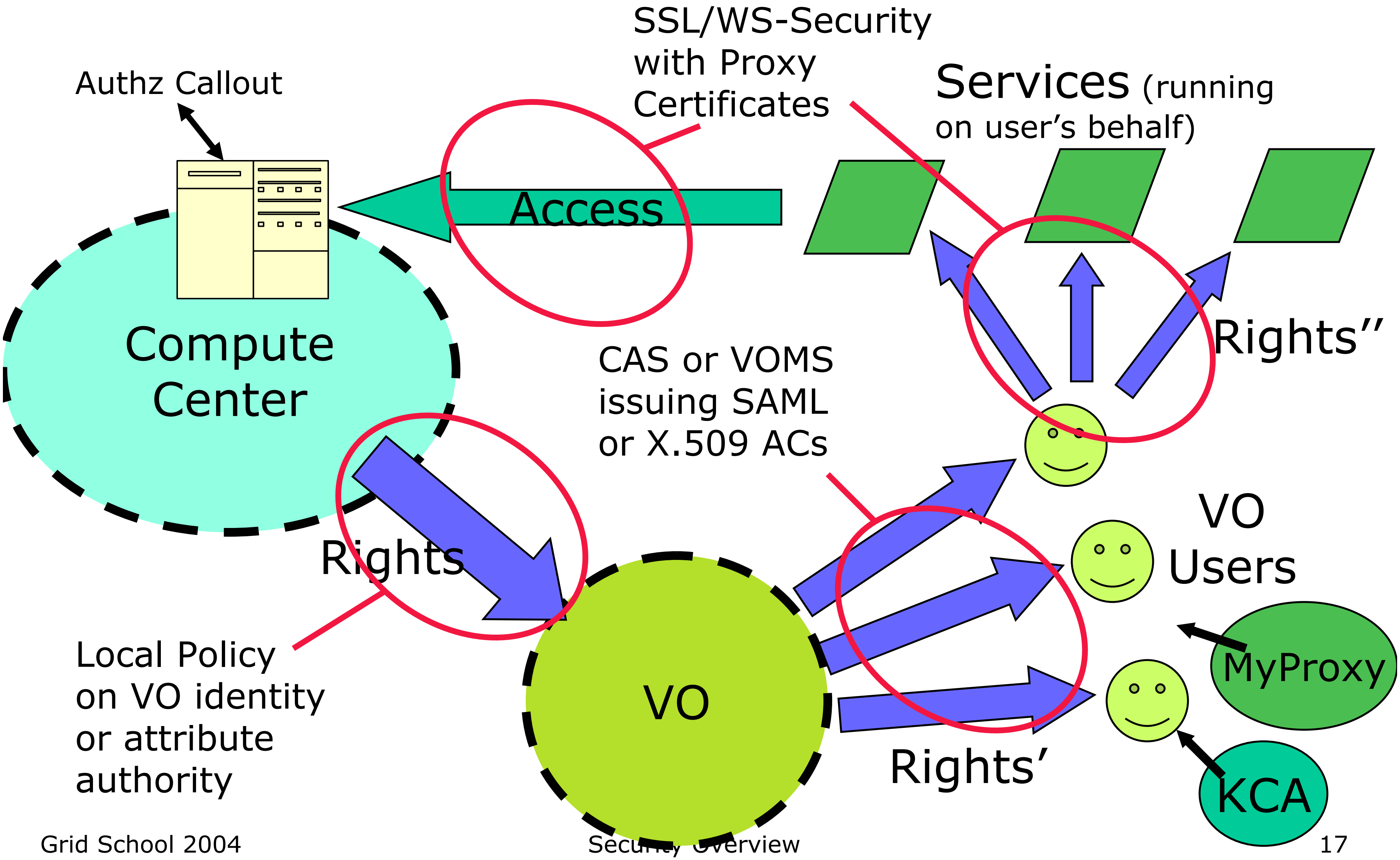
.



Local Identity, Grid Identity, Local Policy



GSI Implementation



SSL/WS-Security with Proxy Certificates

Services (running on user's behalf)

Authz Callout

Access

Compute Center

Rights''

CAS or VOMS issuing SAML or X.509 ACs

Rights

VO Users

MyProxy

Local Policy on VO identity or attribute authority

VO

Rights'

KCA

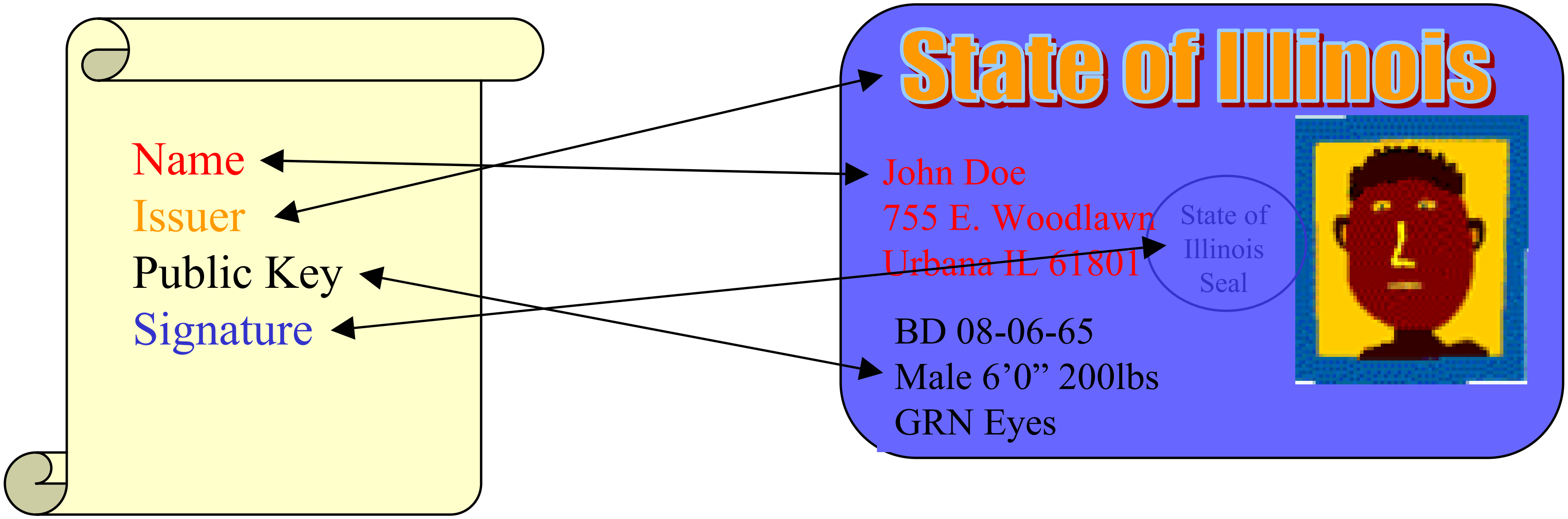
Public Key Infrastructure (PKI)

- 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

the globus toolkit™
www.globustoolkit.org

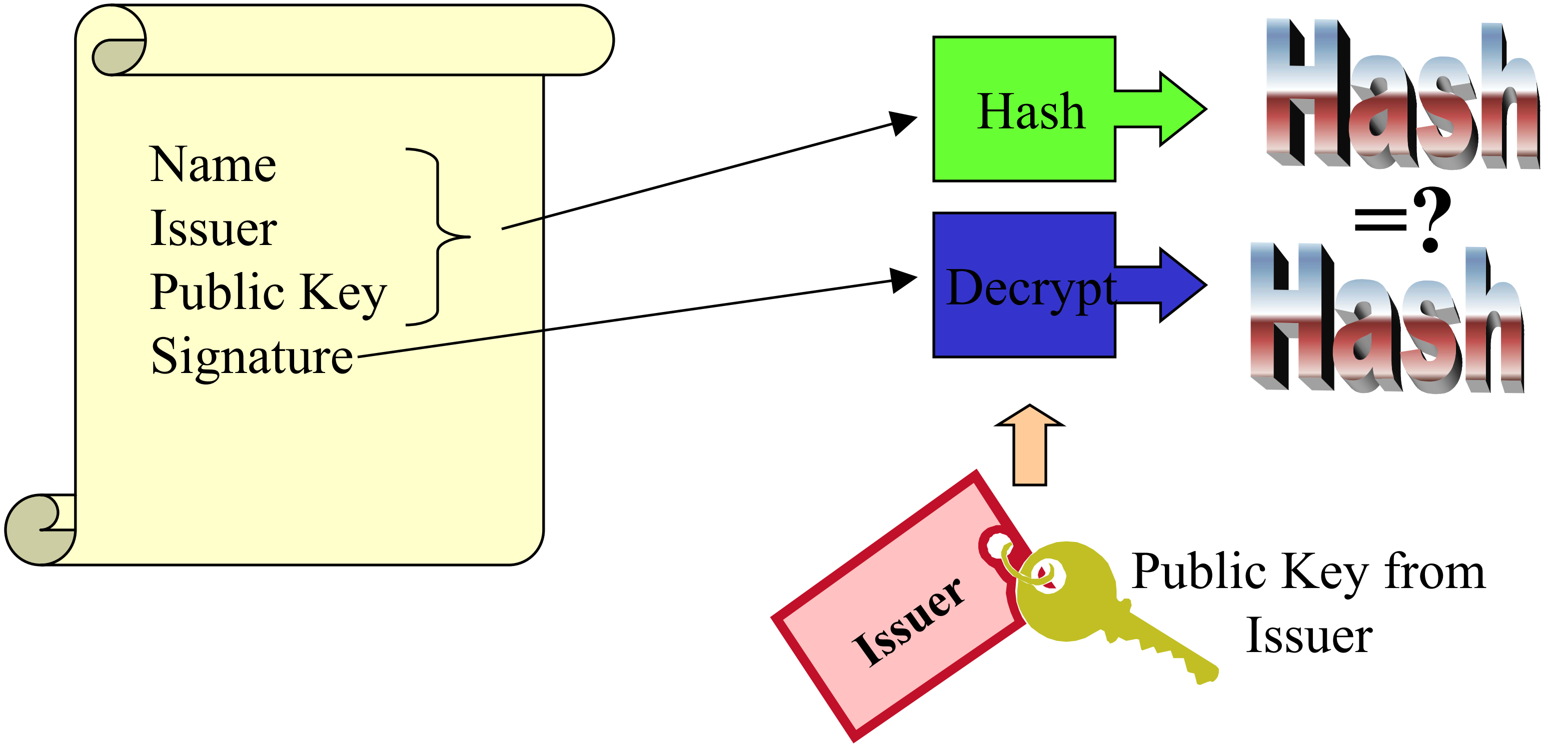
Certificates

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



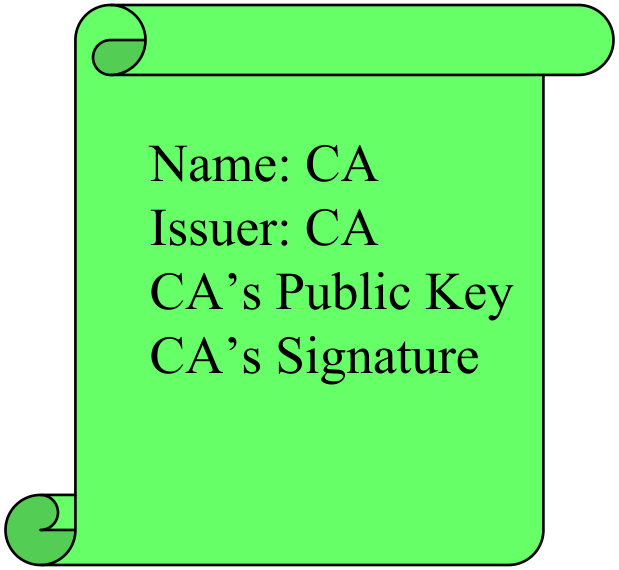
Certificates

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



Certificate Authorities (CAs)

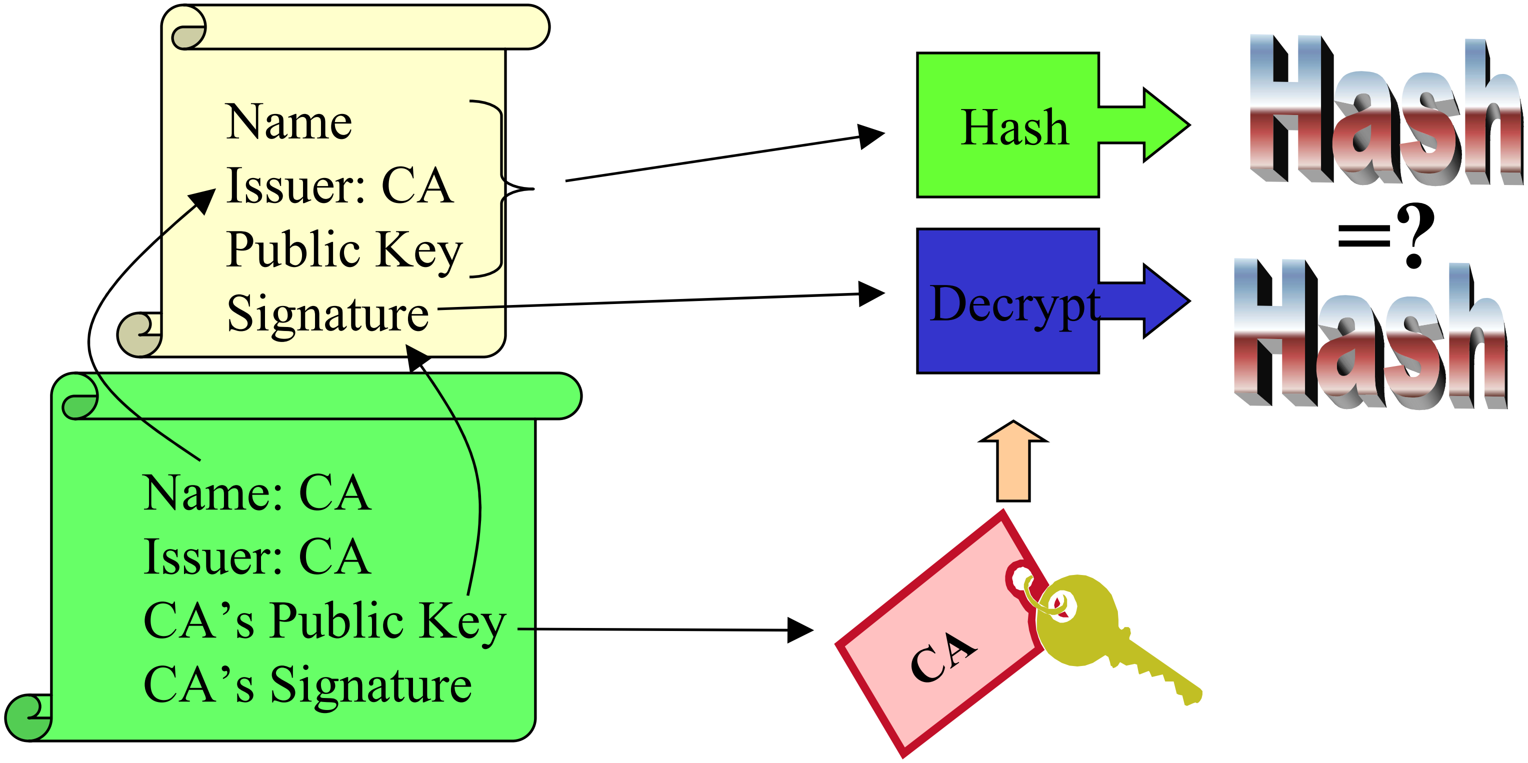
- A small set of trusted entities known as Certificate Authorities (CAs) are established to sign certificates
- A Certificate Authority is an entity that exists only to sign user certificates
- The CA signs it’s own certificate which is distributed in a trusted manner



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

Certificate Authorities (CAs)

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

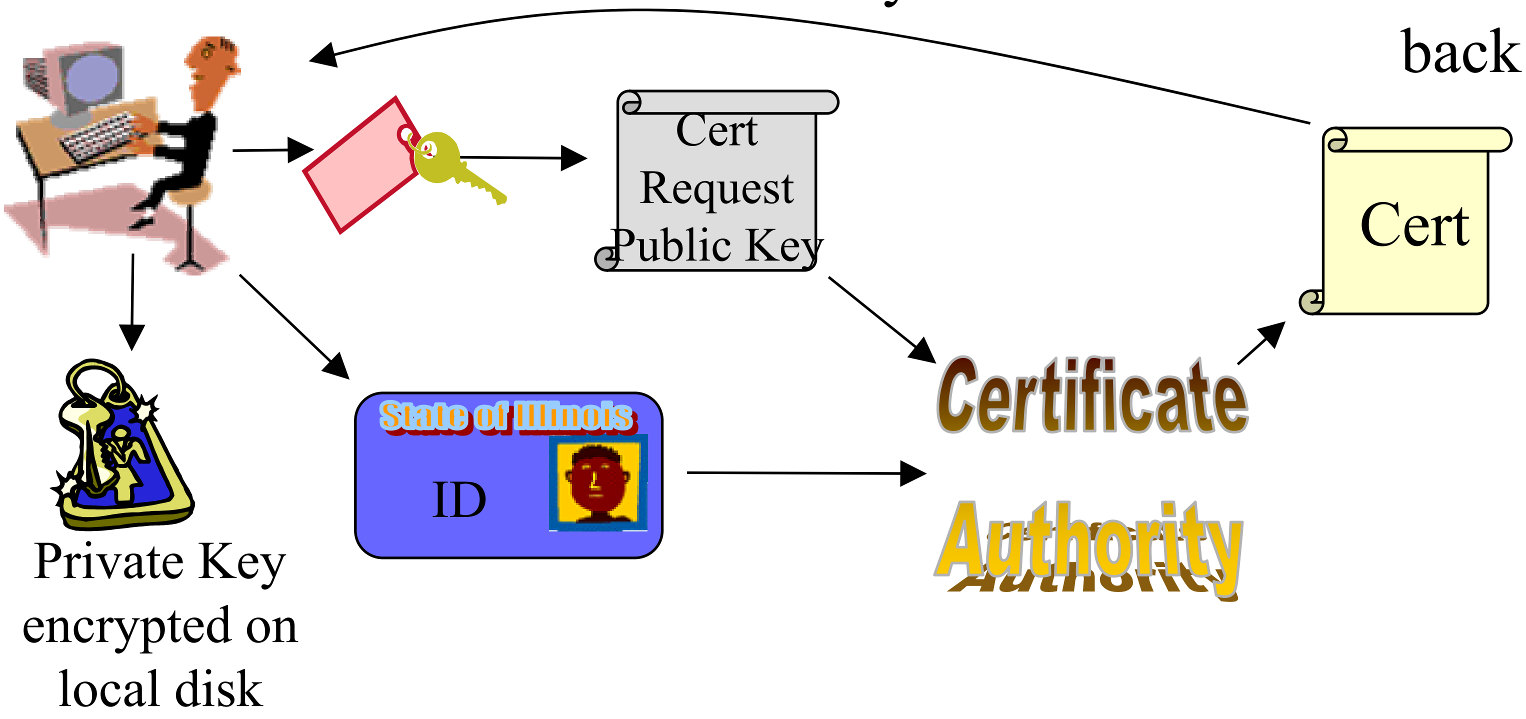


Certificate Request

User generates public/private key pair.

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

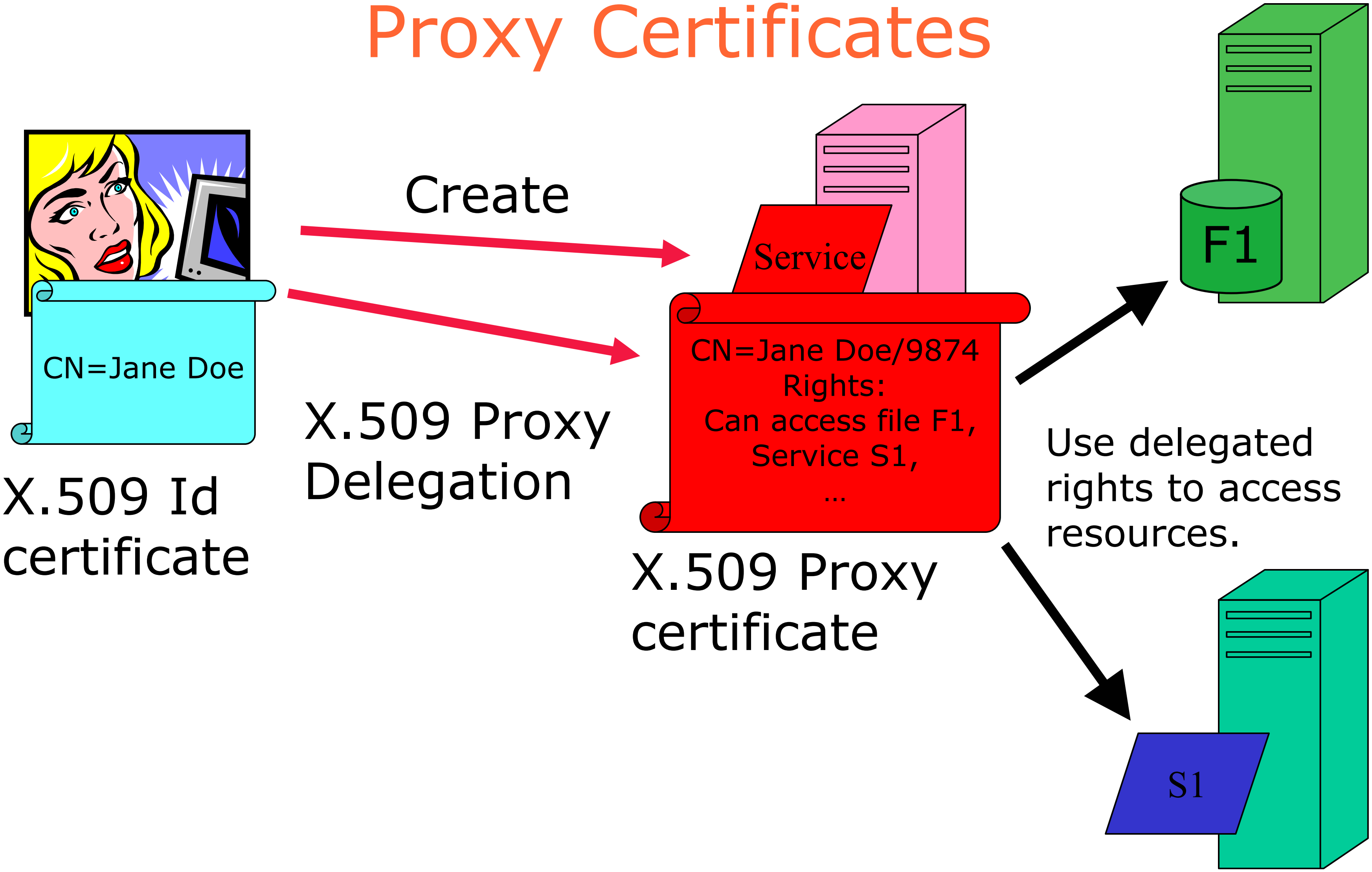
CA confirms identity, signs certificate and sends back to user.



X.509 Proxy Certificates

- GSI Extension to X.509 Identity Certificates
  - RFC
- Enables single sign-on
- Allow user to dynamically assign identity and rights to service
  - Can name services created on the fly and give them rights (i.e. set policy)
- What is effectively happening is the user is creating their own trust domain of services
  - Services trust each other with user acting as the trust root

Proxy Certificates



CN=Jane Doe

X.509 Id certificate

Create

X.509 Proxy Delegation

CN=Jane Doe/9874
Rights:
Can access file F1,
Service S1,
…

X.509 Proxy certificate

Use delegated rights to access resources.

Obtaining a Certificate

- The program grid-cert-request is used to create a public/private key pair and unsigned certificate in ~/.globus/:
  - usercert_request.pem: Unsigned certificate file
  - userkey.pem: Encrypted private key file
    - > Must be readable **only** by the owner
- Mail usercert_request.pem to ca@globus.org
- Receive a Globus-signed certificate

  Place in ~/.globus/usercert.pem
- Other organizations use different approaches
  - NCSA, NPACI, NASA, etc. have their own CA

Certificate Information

- To get cert information run grid-cert-info

```
% grid-cert-info -subject
/C=US/O=Globus/O=ANL/OU=MCS/CN=Ian Foster
```

- Options for printing cert information

  -all
  -subject
  -issuer
  -startdate
  -enddate
  -help

"Logging on" to the Grid

- To run programs, authenticate to Globus:

```
% grid-proxy-init
Enter PEM pass phrase: ******
```

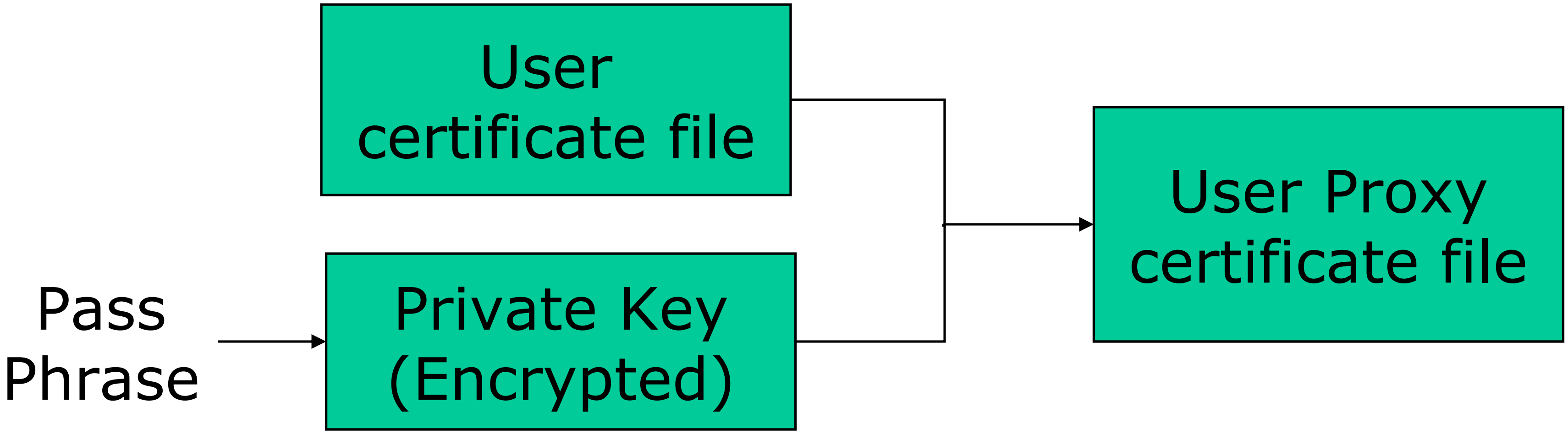
- Creates a temporary, local, short-lived proxy credential for use by our computations
- Options for grid-proxy-init:

```
-hours <lifetime of credential>
-bits <length of key>
-help
```

grid-proxy-init Details

- grid-proxy-init creates the local proxy file.
- User enters pass phrase, which is used to decrypt private key.
- Private key is used to sign a proxy certificate with its own, new public/private key pair.
  - User's private key not exposed after proxy has been signed
- Proxy placed in /tmp, read-only by user
- NOTE: *No* network traffic!
- grid-proxy-info displays proxy details

Grid Sign-On With grid-proxy-init



Destroying Your Proxy (logout)

- To destroy your local proxy that was created by grid-proxy-init:

```
% grid-proxy-destroy
```

- This does *NOT* destroy any proxies that were delegated from this proxy.
  - You cannot revoke a remote proxy
  - Usually create proxies with short lifetimes

Proxy Information

- To get proxy information run grid-proxy-info

```
% grid-proxy-info -subject
/C=US/O=Globus/O=ANL/OU=MCS/CN=Ian Foster
```

- Options for printing proxy information

  -subject
  -type
  -strength
  -issuer
  -timeleft
  -help

- Options for scripting proxy queries

  -exists -hours <lifetime of credential>
  -exists -bits <length of key>

  – Returns 0 status for true, 1 for false:

Delegation

- Delegation = remote creation of a (second level) proxy credential
  - New key pair generated remotely on server
  - Proxy cert and public key sent to client
  - Clients signs proxy cert and returns it
  - Server (usually) puts proxy in /tmp
- Allows remote process to authenticate on behalf of the user
  - Remote process “impersonates” the user

Limited Proxy

- During delegation, the client can elect to delegate only a “limited proxy”, rather than a “full” proxy
  - GRAM (job submission) client does this
- Each service decides whether it will allow authentication with a limited proxy
  - Job manager service requires a full proxy
  - GridFTP server allows either full or limited proxy to be used

Secure Services

- On most unix machines, inetd listens for incoming service connections and passes connections to daemons for processing.
- On Grid servers, the gatekeeper securely performs the same function for many services
  - It handles mutual authentication using files in /etc/grid-security
  - It maps to local users via the gridmap file

Sample Gridmap File

- Gridmap file maintained by Globus administrator
- Entry maps Grid-id into local user name(s)

```
# Distinguished name                                  Local
#                                                   username
"/C=US/O=Globus/O=NPACI/OU=SDSC/CN=Rich Gallup”       rpg
"/C=US/O=Globus/O=NPACI/OU=SDSC/CN=Richard Frost”     frost
"/C=US/O=Globus/O=USC/OU=ISI/CN=Carl Kesselman”       u14543
"/C=US/O=Globus/O=ANL/OU=MCS/CN=Ian Foster”           itf
```

Authorization

- GSI handles authentication, but authorization is a separate issue
- Authorization issues:
  - Management of authorization on a multi-organization grid is still an interesting problem.
  - The grid-mapfile doesn't scale well, and works only at the resource level, not the collective level.
  - Large communities that share resources exacerbates authorization issues, which has led us to CAS…

Security Summary

- Programs for credential management
  - grid-cert-info, grid-proxy-init, grid-proxy-destroy, grid-proxy-info
- GSS-API: The Globus Toolkit Grid Security Infrastructure (GSI) uses this API, which allows programs to easily add security
- globus_gss_assist: This is a simple wrapper around GSS-API, making it easier to use