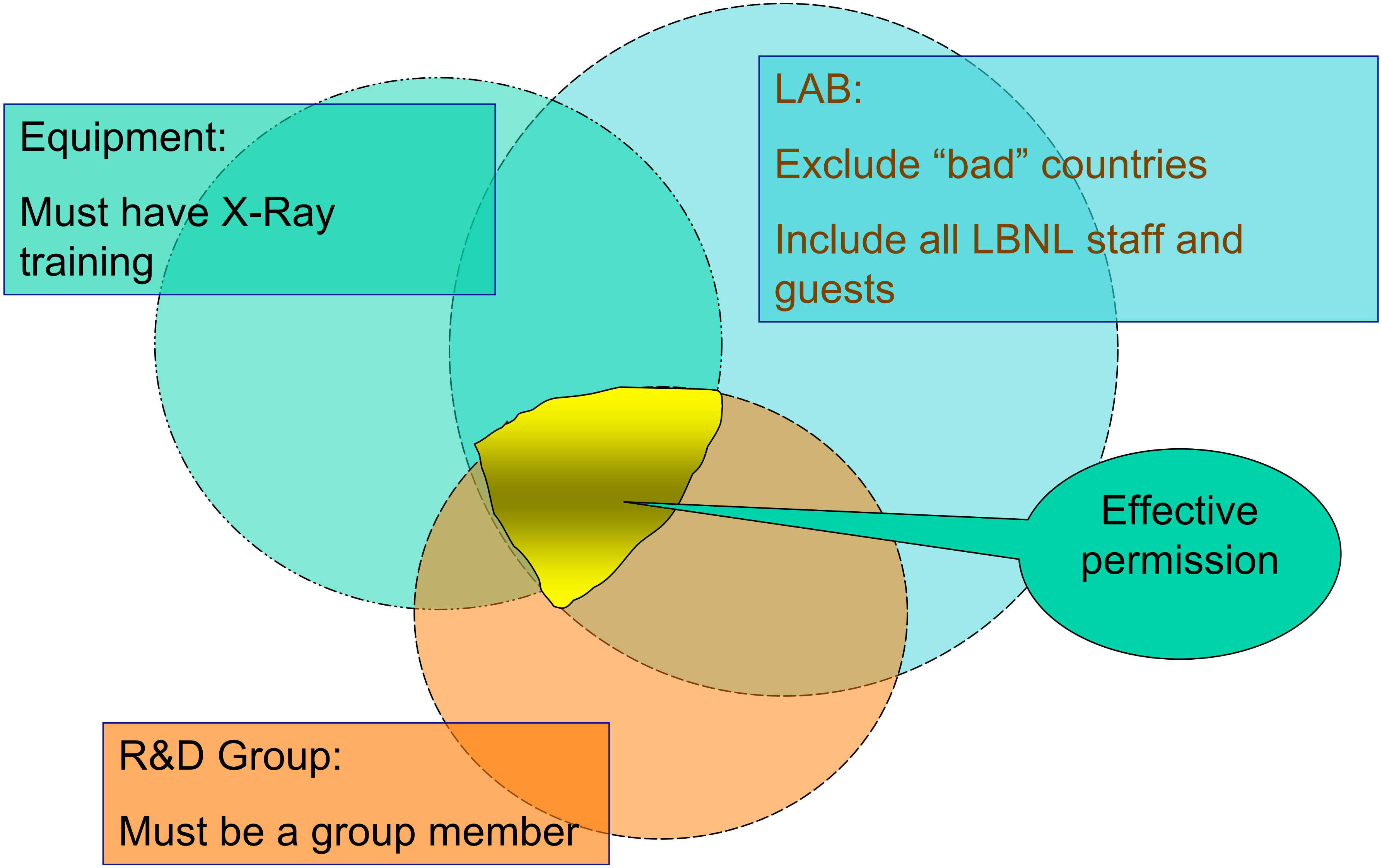
Grid Security

Grid Security Concerns

- Control access to shared services
  - Address autonomous management, e.g., different policy in different work groups
- Support multi-user collaborations
  - Federate through mutually trusted services
  - Local policy authorities rule
- Allow users and application communities to set up dynamic trust domains
  - Personal/VO collection of resources working together based on trust of user/VO

Virtual Organization (VO) Concept

- VO for each application or workload
- Carve out and configure resources for a particular use and set of users



Equipment:

Must have X-Ray training

LAB:

Exclude “bad” countries

Include all LBNL staff and guests

Effective permission

R&D Group:

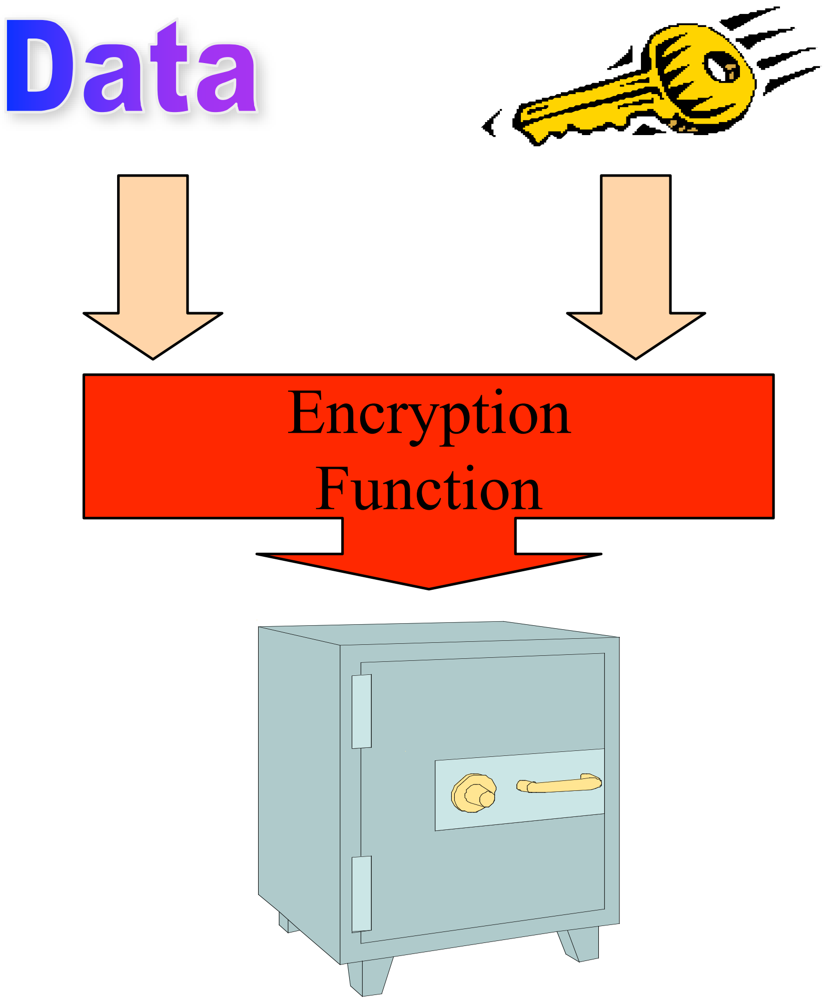
Must be a group member

Security Basics

- Privacy
  - Only the sender and receiver should be able to understand the conversation
- Integrity
  - Receiving end must know that the received message was the one from the sender
- Authentication
  - Users are who they say they are (authentic)
- Authorization
  - Is user allowed to perform the action

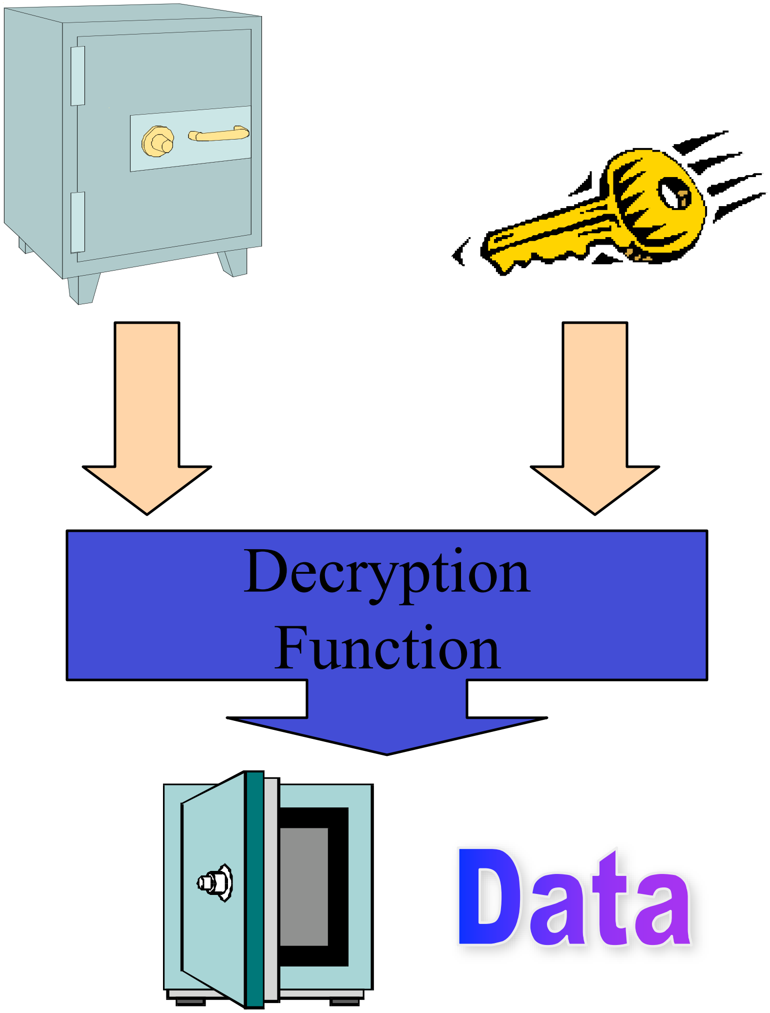
Encryption

- 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



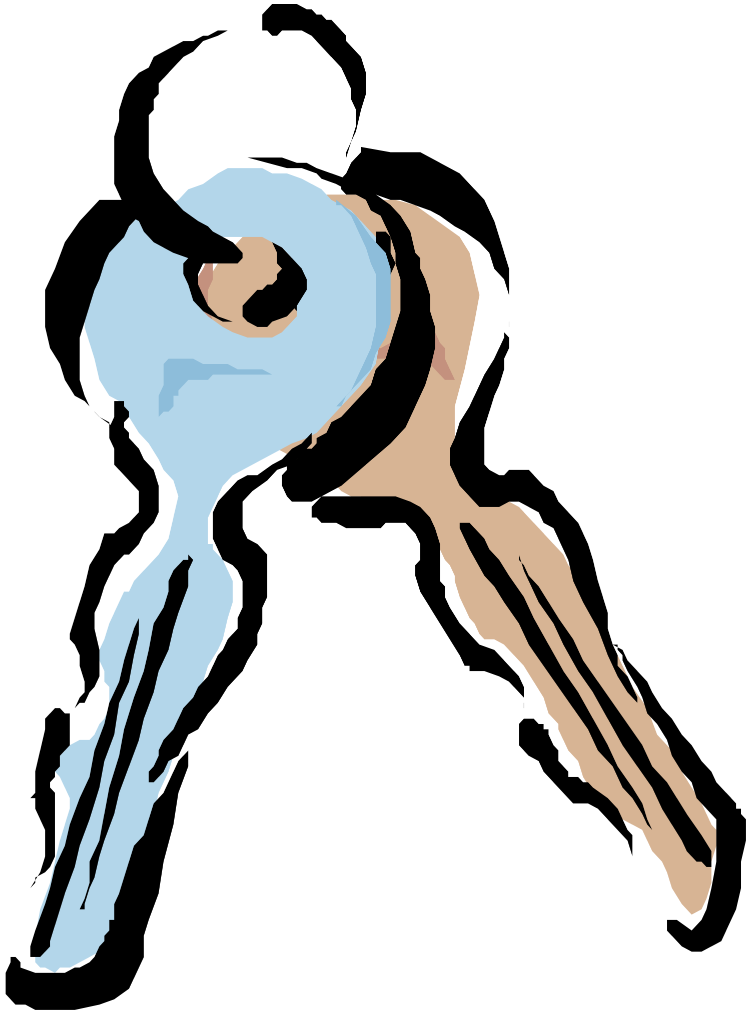
Decryption

- 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



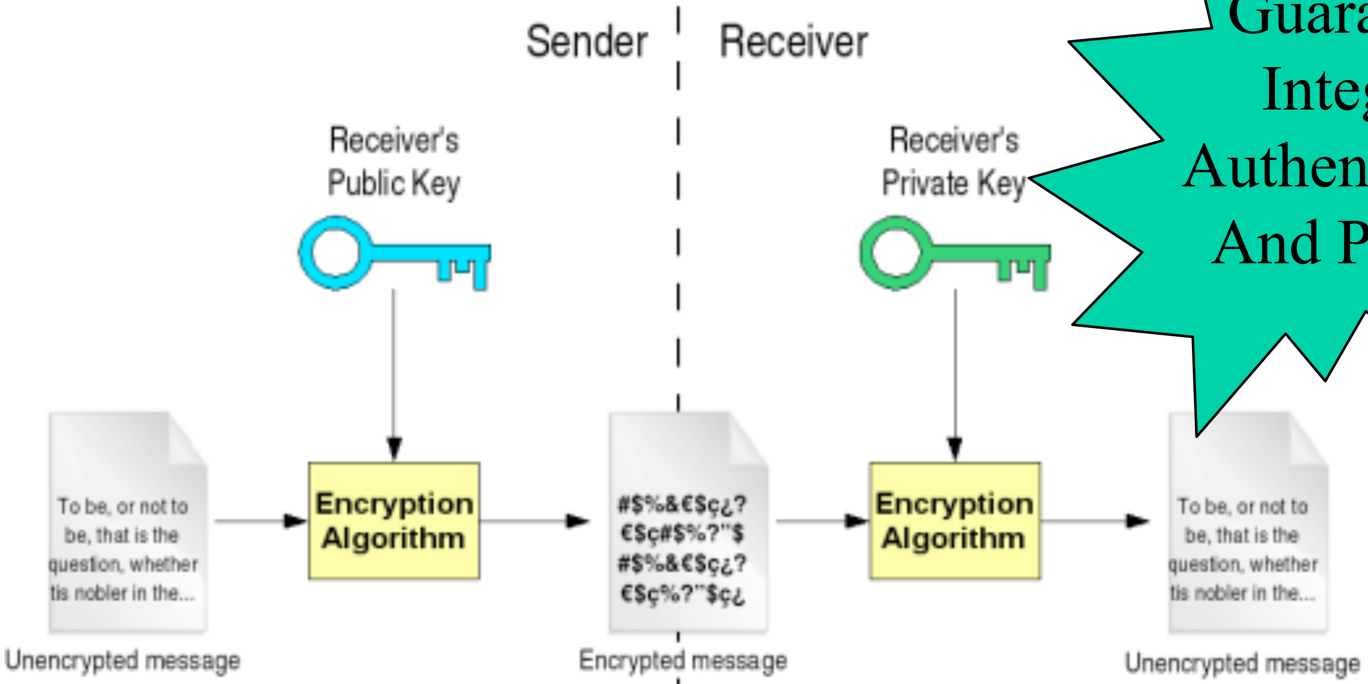
Asymmetric Encryption

- Encryption and decryption functions that use a key pair are called asymmetric
  - Keys are mathematically linked



Authentication

- Private Key - known only by owner
- Public Key- known to everyone
- What one key encrypts, the other decrypts

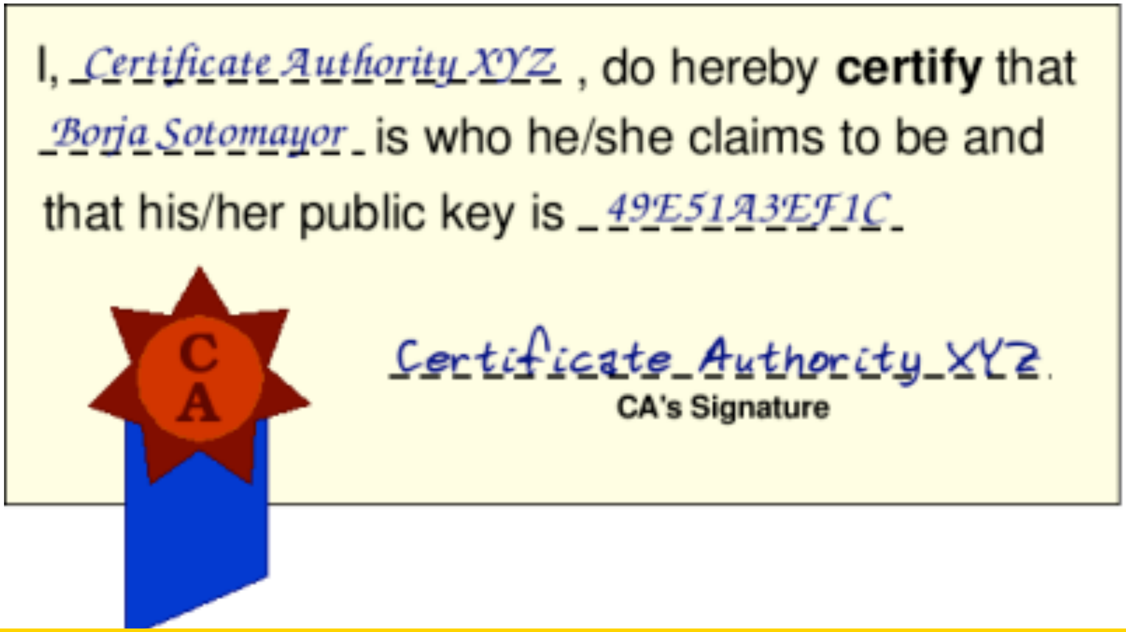

Sender
Receiver
Receiver's Public Key
Receiver's Private Key
To be, or not to be, that is the question, whether tis nobler in the...
Encryption Algorithm
#$%&€$ç¿? €$ç#$%?"$ #$%&€$ç¿? €$ç%?"$ç¿
Encryption Algorithm
To be, or not to be, that is the question, whether tis nobler in the...
Unencrypted message
Encrypted message
Unencrypted message

Guarantees Integrity Authentication And Privacy

Borja Sotomayor , http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s03.html

Authentication using Digital Certificates

- Digital document that certifies a public key is owned by a particular user
- Signed by 3rd party – the Certificate Authority (CA)



I, Certificate Authority XYZ , do hereby **certify** that Borja Sotomayor is who he/she claims to be and that his/her public key is 49E51A3EF1C

Certificate Authority XYZ

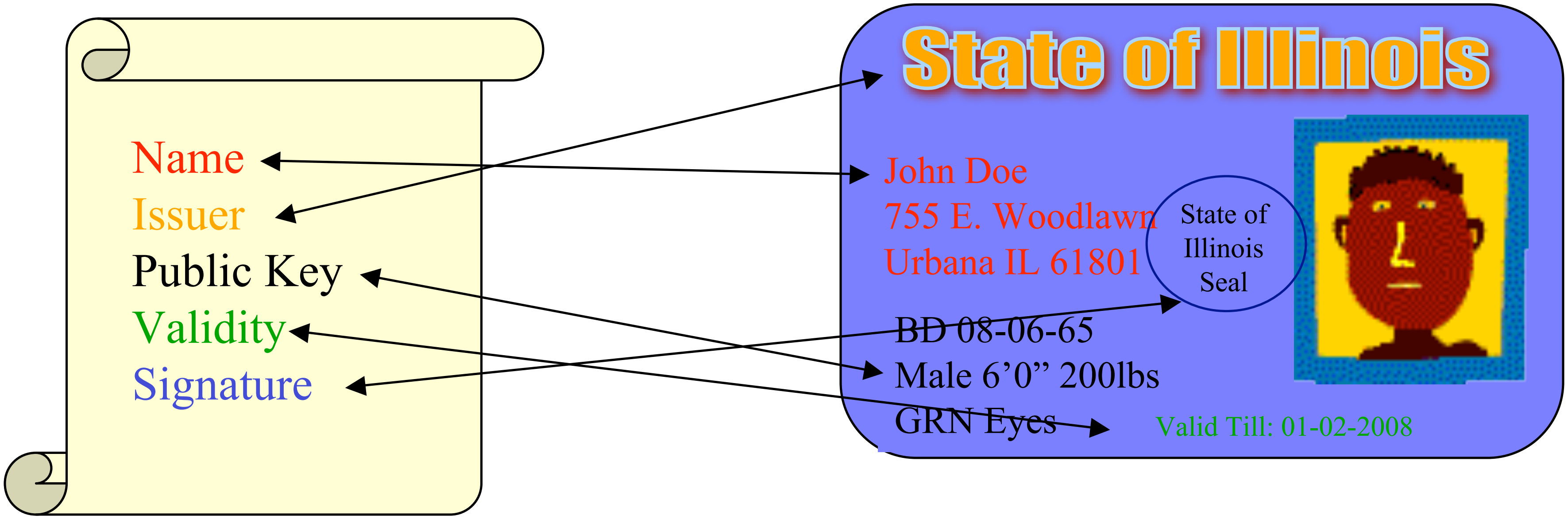
CA's Signature

To know if you should trust the certificate, you have to trust the CA

Borja Sotomayor , http://gdp.globus.org/gt4-tutorial/multiplehtml/ch09s04.html

Certificates

- Similar to passport or driver’s license

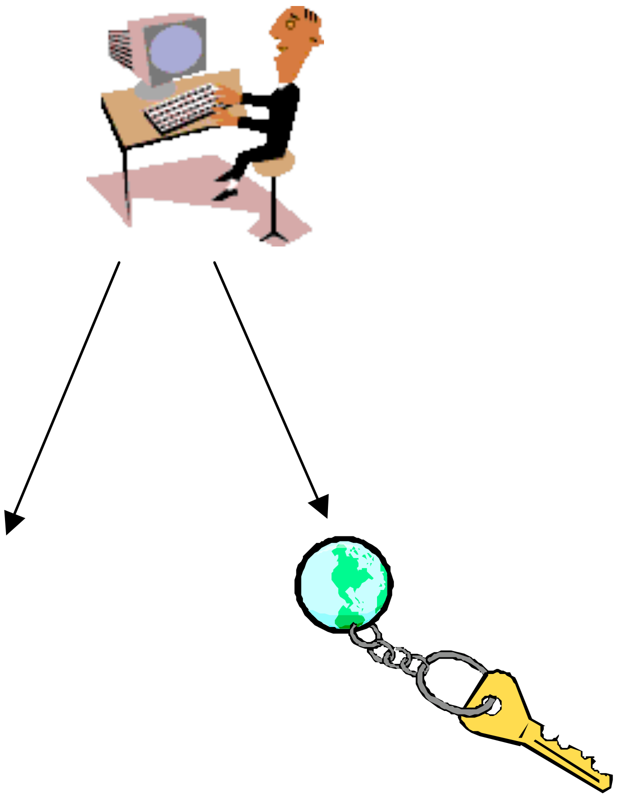


Globus Security

- Globus security is based on the Grid Security Infrastructure (GSI)
  - Set of IETF standards for security interaction
- Public-key-based authentication using X509 certificates

Requesting a Certificate

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

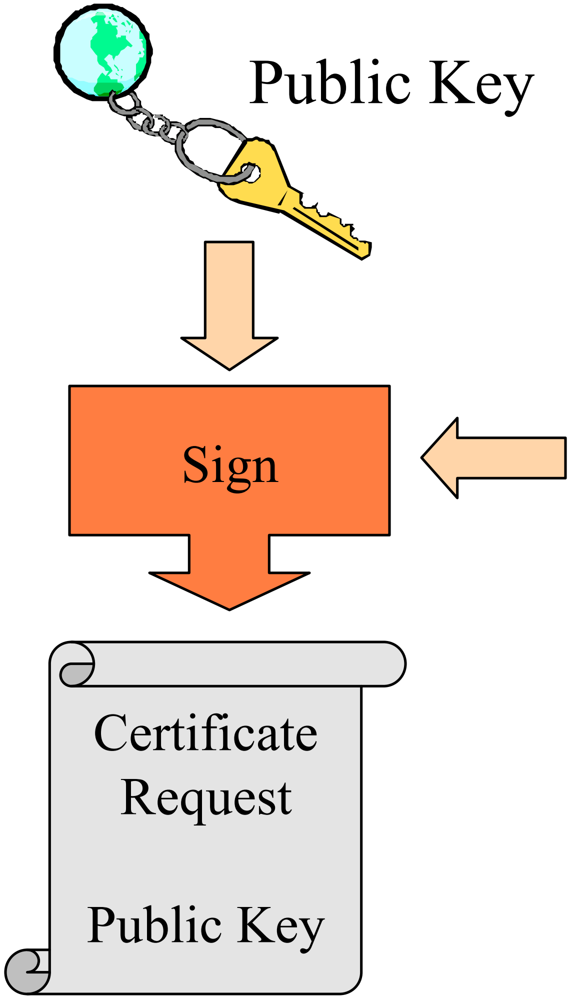


Private Key

Public Key

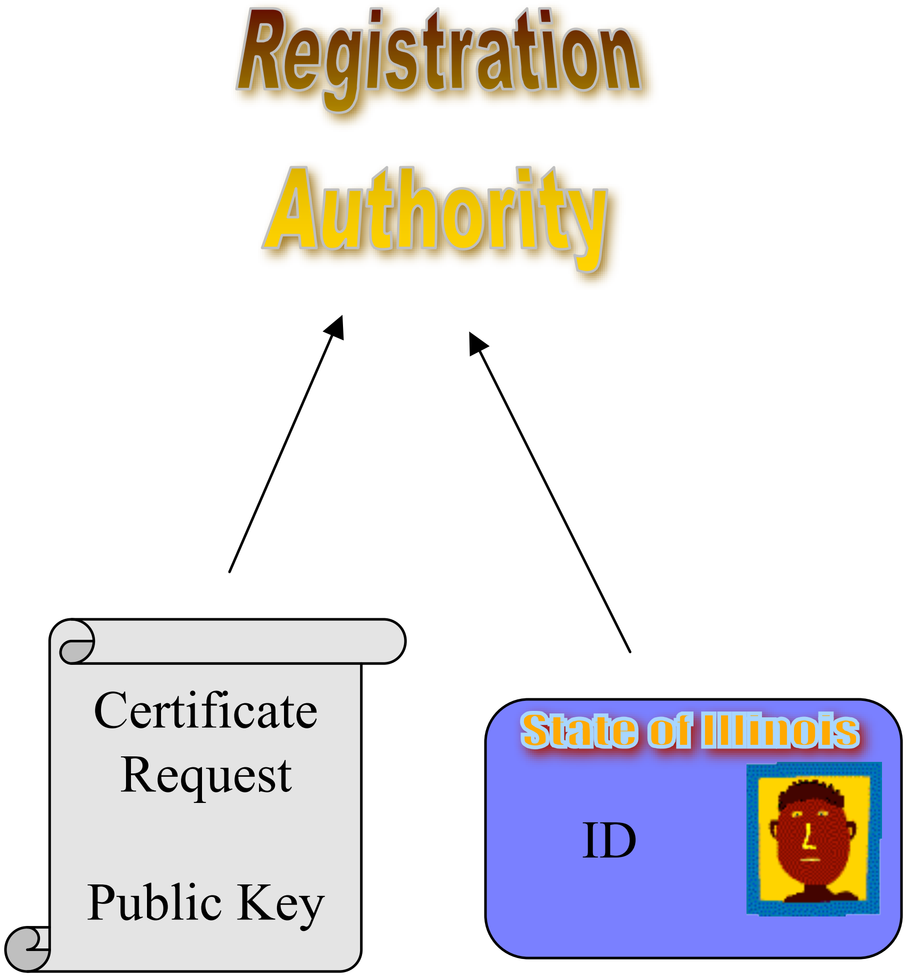
Certificate Request

- The user signs their own public key to form what is called a Certificate Request
- Email/Web upload
- Note private key is never sent anywhere



Registration Authority (RA)

- The user then takes the certificate to a Registration Authority (RA)
- Vetting of user’s identity
- Often the RA coexists with the CA and is not apparent to the user



Registration Authority

Certificate Request

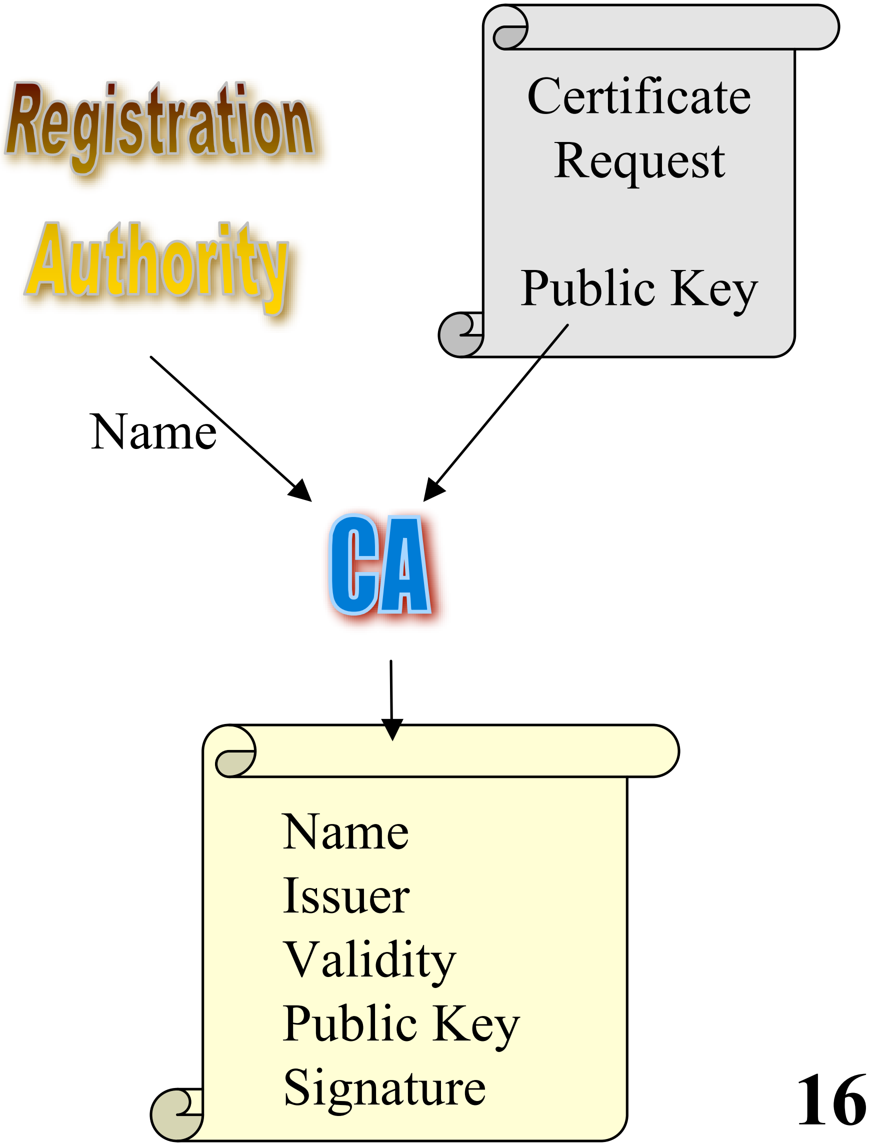
Public Key

State of Illinois

ID

Certificate Issuance

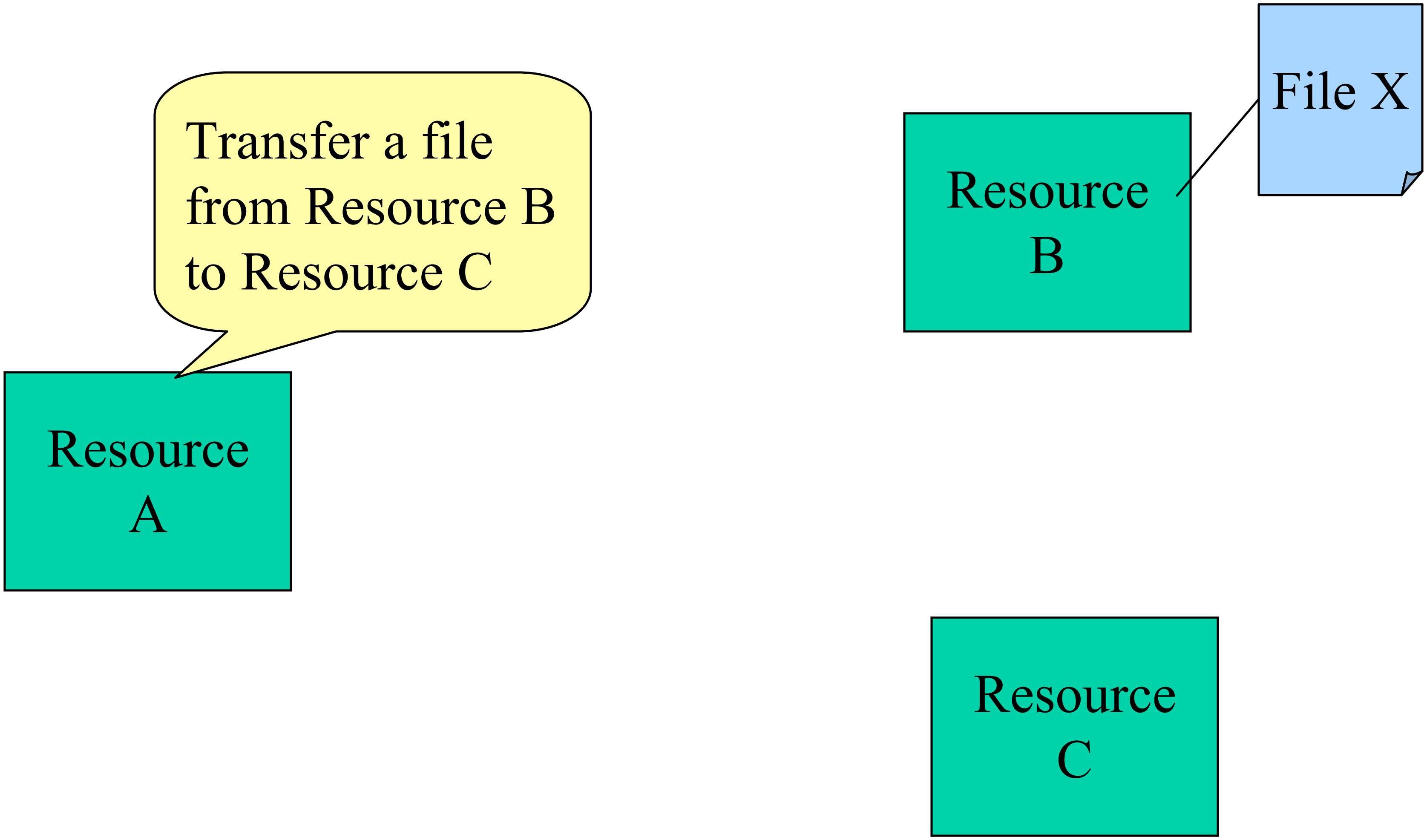
- The CA then takes the identity from the RA and the public key from the certificate request
- It then creates, signs and issues a certificate for the user



GridMap File

- Maps distinguished names (found in certificates) to local names (such as login accounts)
  - schopf@mcs.anl.gov
  - jms@nesc.ed.ac.uk
  - u11270@sdsc.edu
- Can also serve as a access control list for GSI enabled services

Delegation



Transfer a file from Resource B to Resource C

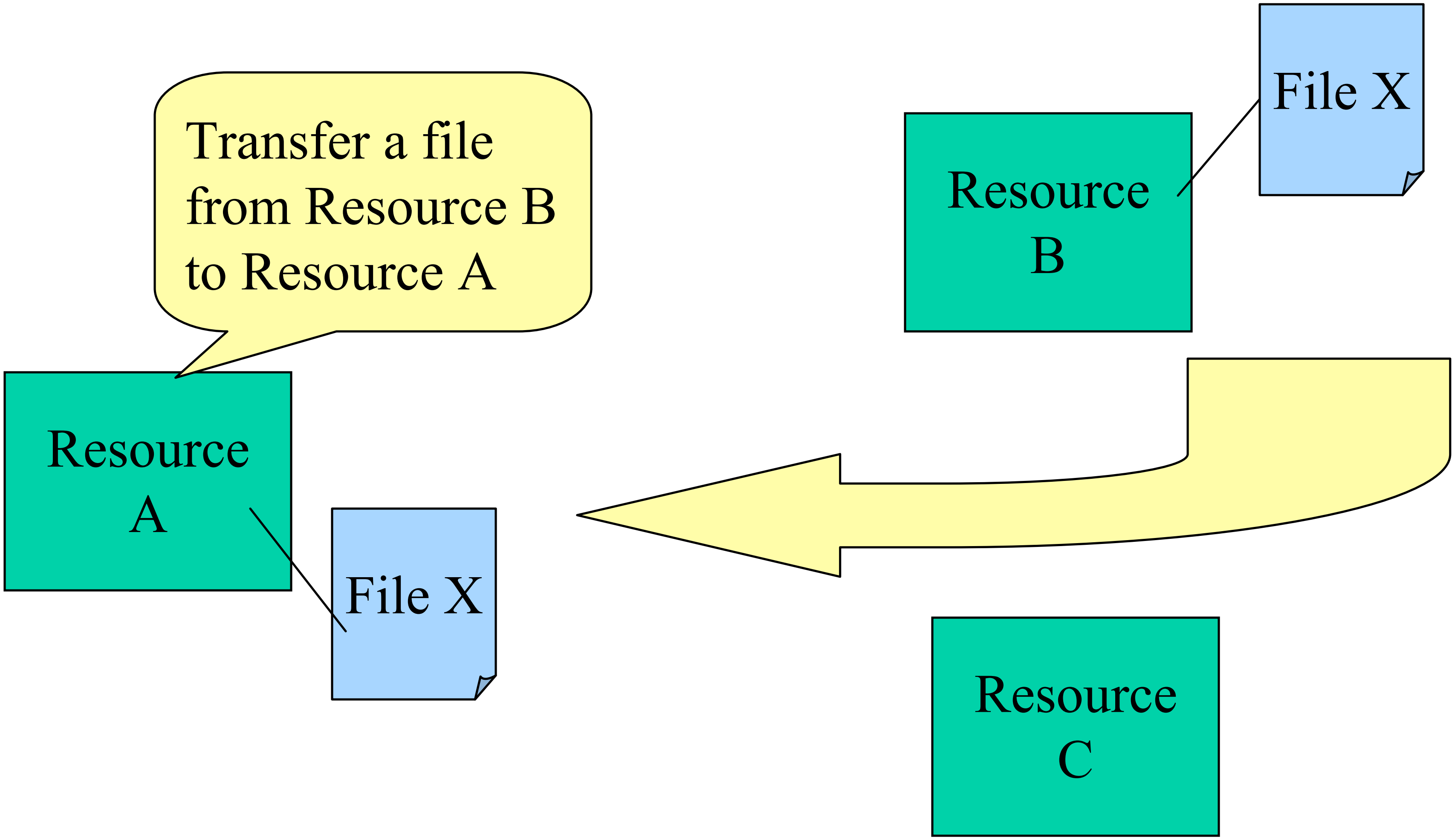
Resource A

Resource B

File X

Resource C

Delegation



Transfer a file from Resource B to Resource A

Resource B

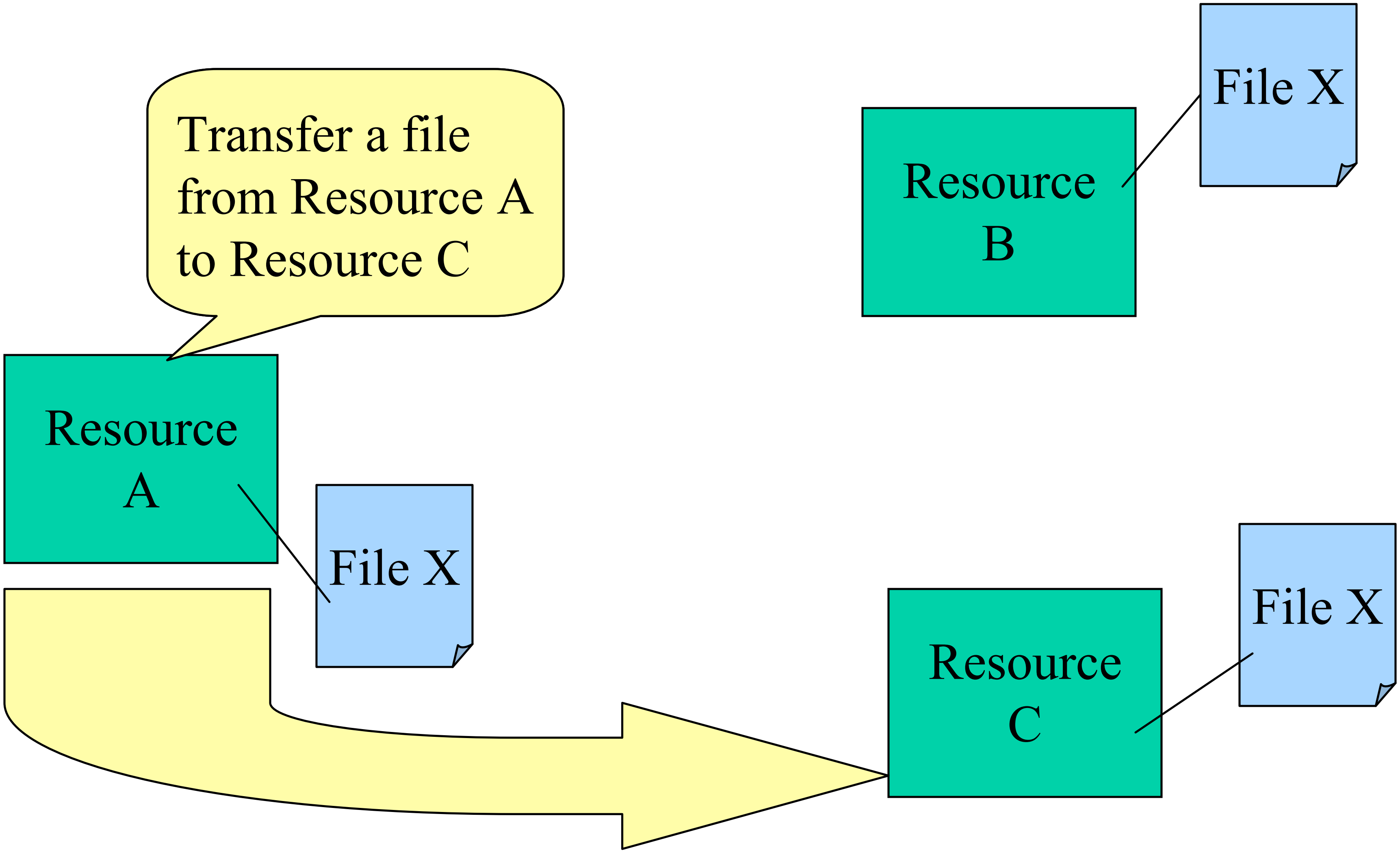
File X

Resource A

File X

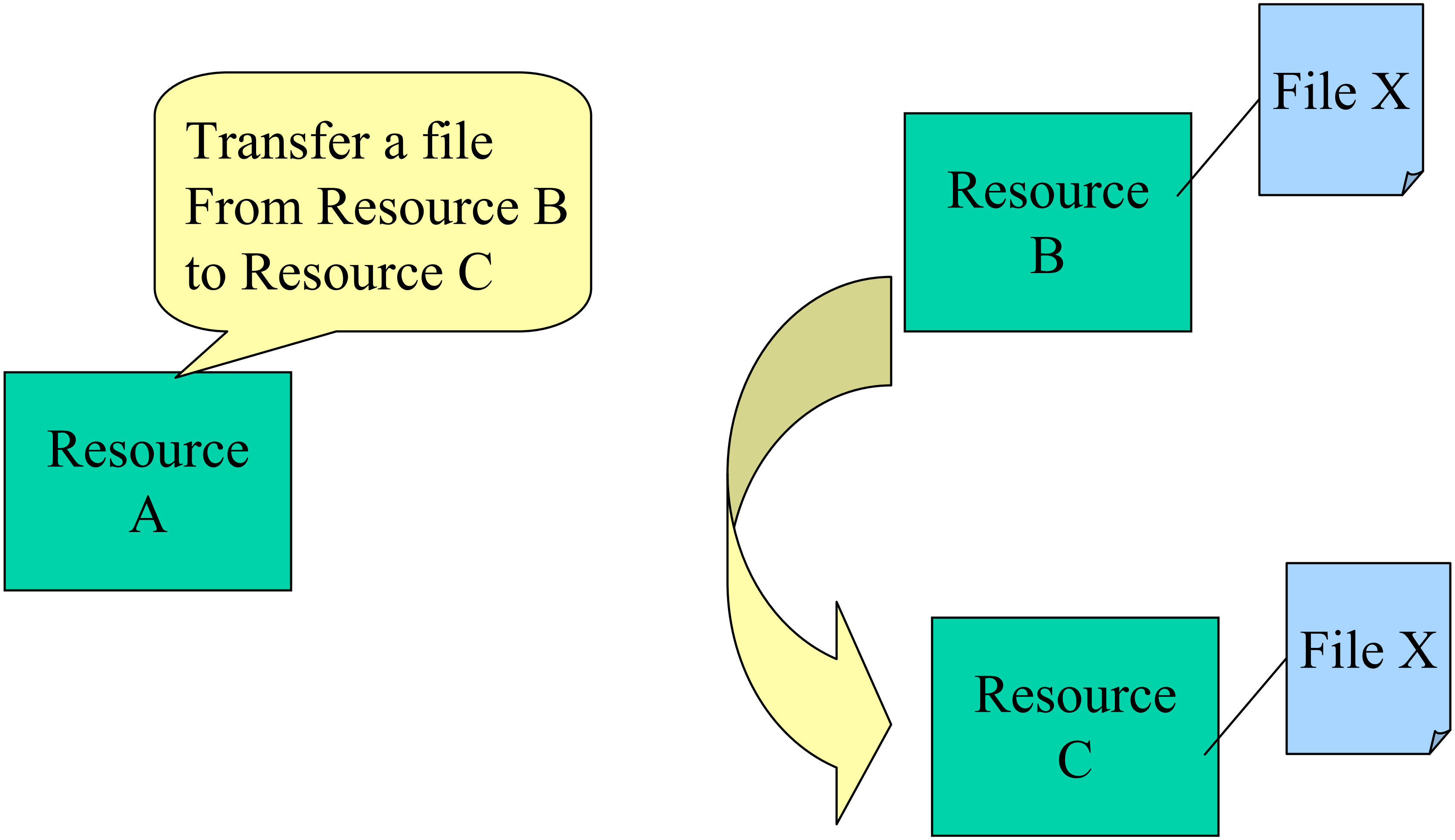
Resource C

Delegation



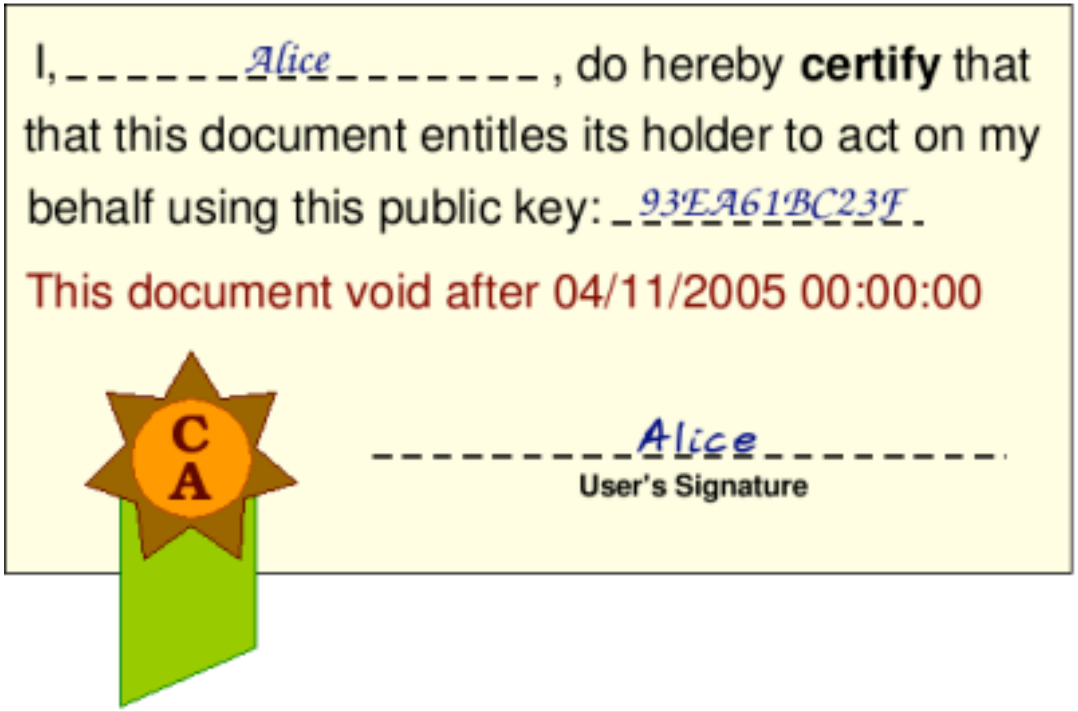
Transfer a file from Resource A to Resource C

Delegation


Transfer a file
From Resource B
to Resource C
Resource A
Resource B
File X
Resource C
File X

Proxy Certificate

- Proxy Certificate allows another user to act upon their behalf
  - Credential delegation



I, _______Alice________, do hereby **certify** that that this document entitles its holder to act on my behalf using this public key: _93EA61BC23F_

This document void after 04/11/2005 00:00:00

_________Alice_________
User's Signature

Borja Sotomayor , http://gdp.globus.org/gt4-tutorial/multiplehtml/ch10s05.html

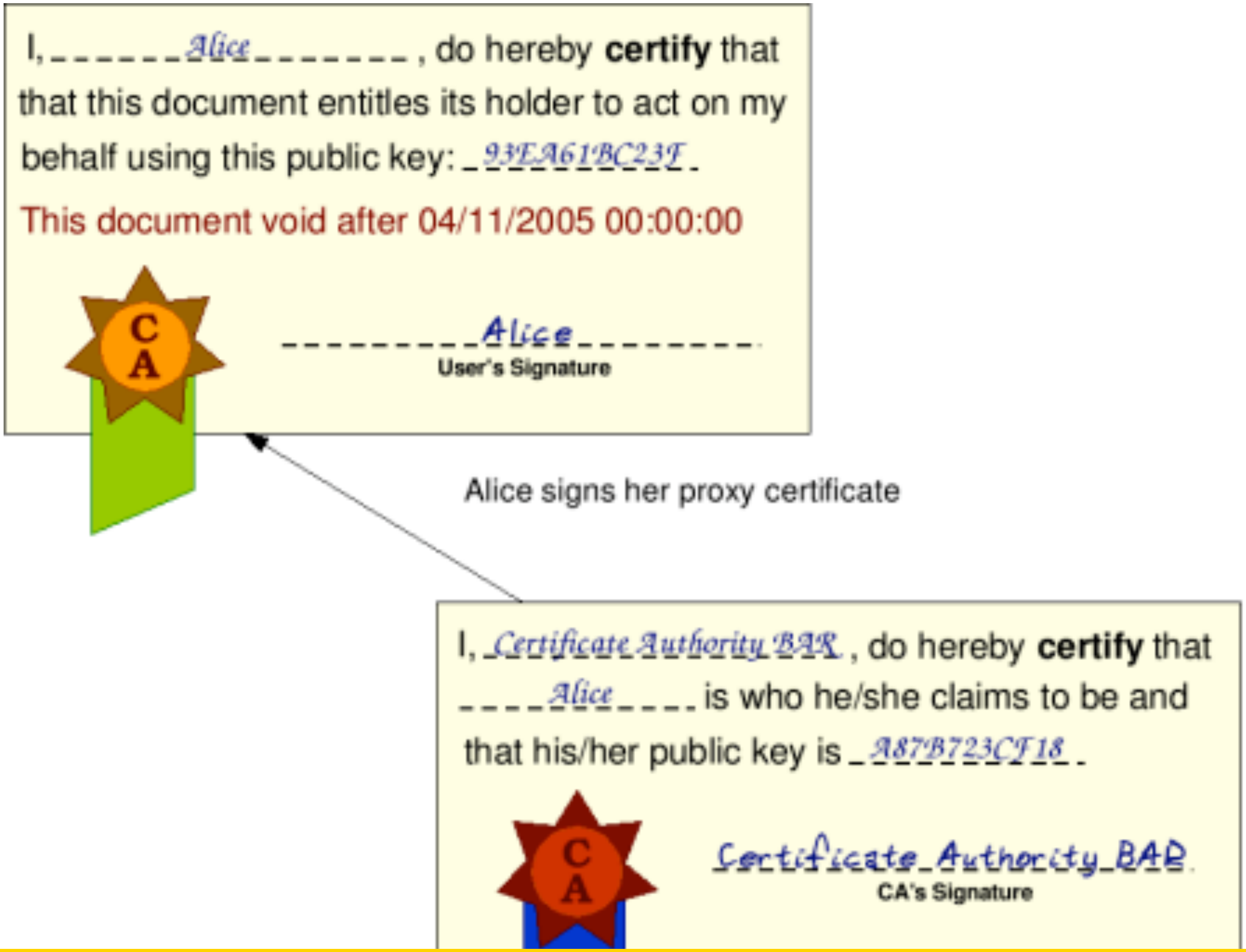
Proxy Certificate

- Proxy empowers 3rd party to act upon your behalf
- Proxy certificate is signed by the end user, not a CA
- Proxy cert’s public key is a new one from the private-public key pair generated specifically for the proxy certificate
- Proxy also allows you to do single sign-on
  - Setup a proxy for a time period and you don’t need to sign in again

Benefits of Single Sign-on

- Don’t need to remember (or even know) ID/passwords for each resource.
- Automatically get a Grid proxy certificate for use with other Grid tools
- More secure
  - No ID/password is sent over the wire: not even in encrypted form
  - Proxy certificate expires in a few hours and then is useless to anyone else
  - Don’t need to write down 10 passwords
- *It’s fast and it’s easy!*

Proxy Certificate Chain



I, Alice, do hereby **certify** that that this document entitles its holder to act on my behalf using this public key: 93EA61BC23F

This document void after 04/11/2005 00:00:00

Alice
User's Signature

Alice signs her proxy certificate

I, Certificate Authority BAR, do hereby **certify** that Alice is who he/she claims to be and that his/her public key is A87B723CF18

Certificate_Authority_BAD
CA's Signature

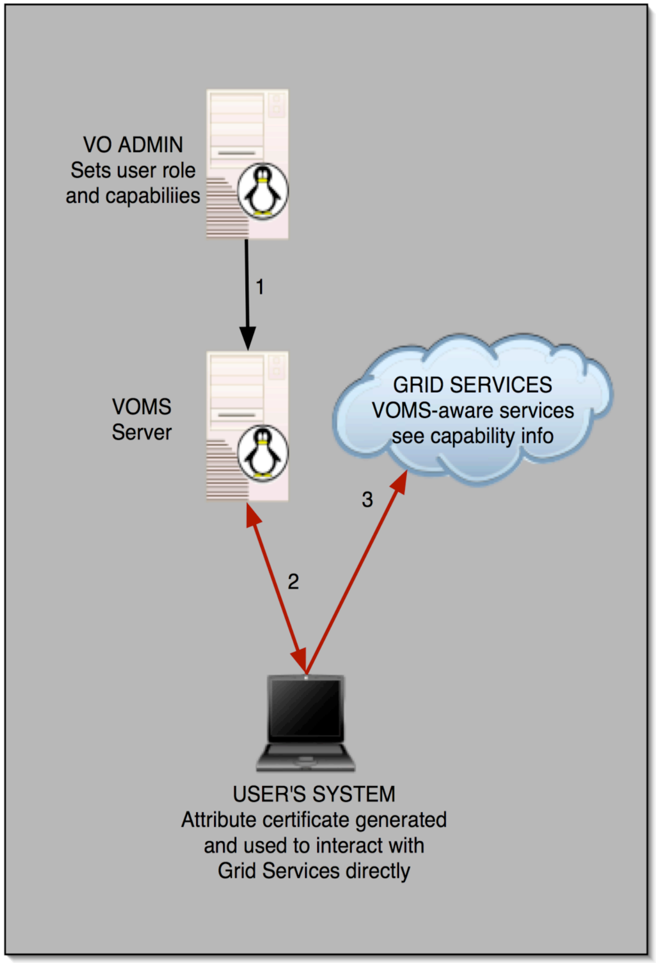
Borja Sotomayor , http://gdp.globus.org/gt4-tutorial/multiplehtml/ch10s05.html

Delegation

- Can delegate as part of protocol
- Extra round trip with delegation
- Types: Full or Limited delegation

- Single sign-on
  - one password for the whole grid
- Let services (eg RFT) act on your behalf

VOMS

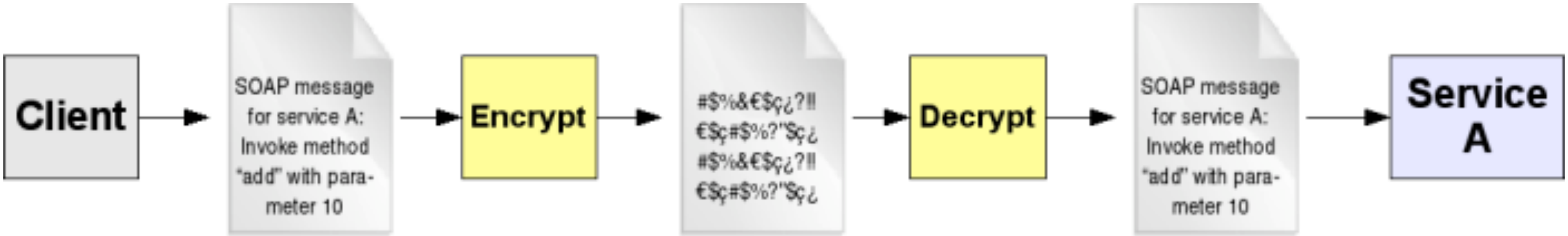


- A community-level group membership system
- Database of user roles
  - Administrative tools
  - Client interface
- voms-proxy-init
  - Uses client interface to produce an attribute certificate (instead of proxy) that includes roles & capabilities signed by VOMS server
  - Works with non-VOMS services, but gives more info to VOMS-aware services
- Allows VOs to centrally manage user roles

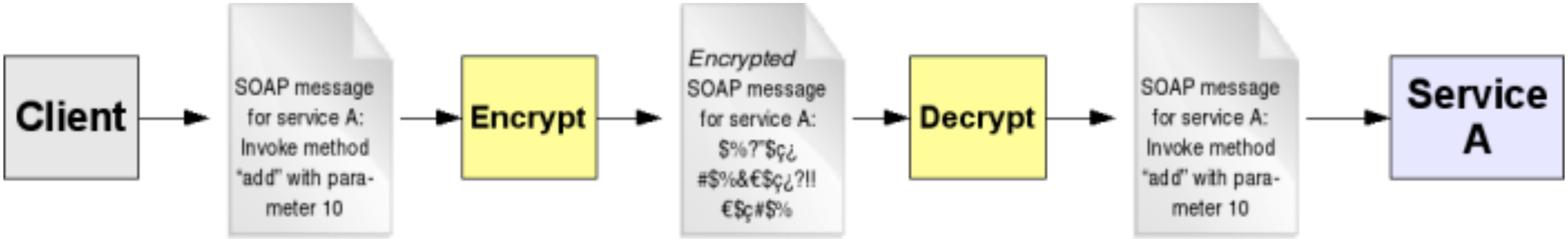
Enabling
Private Communication

GSI enables security at 2 levels

Transport-level Security (https)

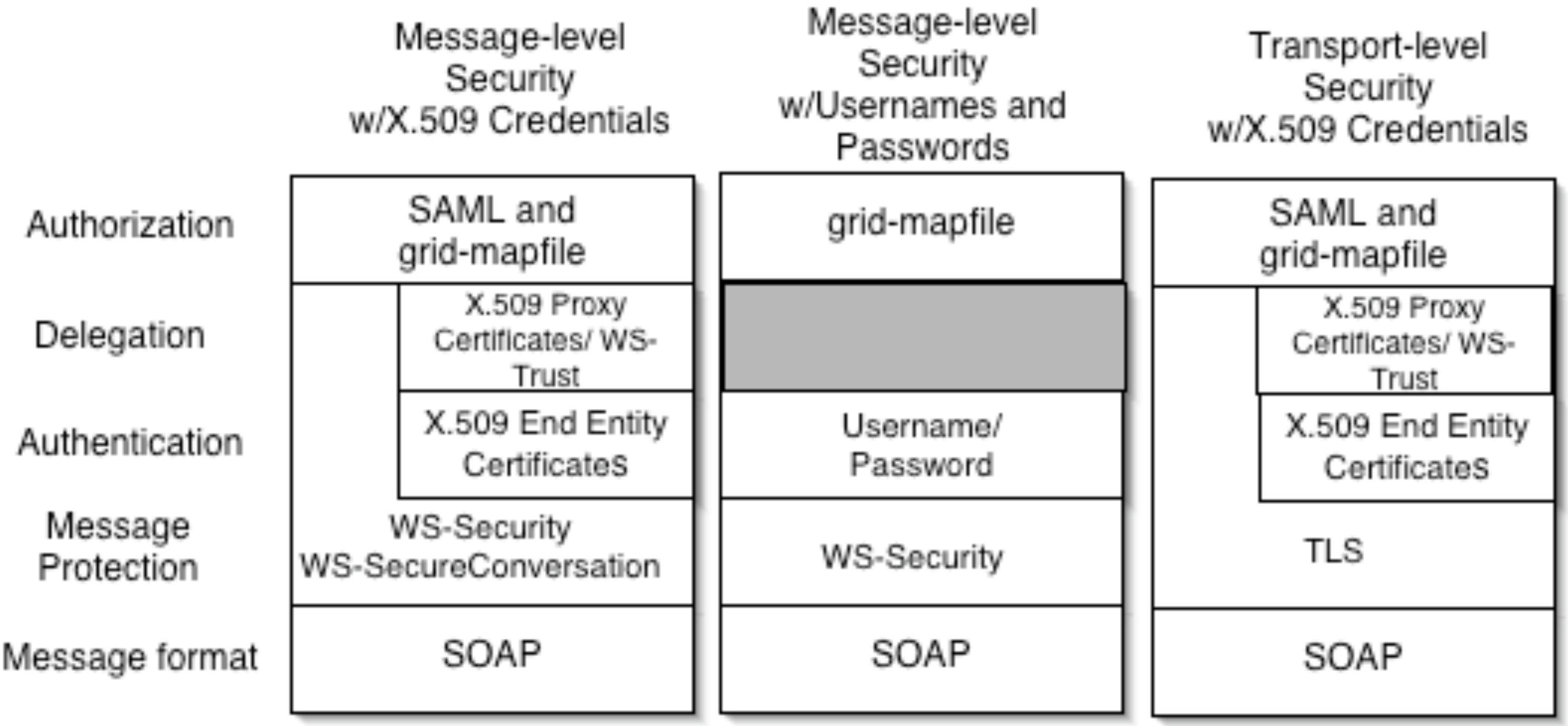

Client
SOAP message for service A: Invoke method "add" with parameter 10
Encrypt
#$%&€$ç¿?!!
€$ç#$%?"$ç¿
#$%&€$ç¿?!!
€$ç#$%?"$ç¿
Decrypt
SOAP message for service A: Invoke method "add" with parameter 10
Service A

Message-level Security


Client
SOAP message for service A: Invoke method "add" with parameter 10
Encrypt
Encrypted SOAP message for service A:
$%?"$ç¿
#$%&€$ç¿?!!
€$ç#$%
Decrypt
SOAP message for service A: Invoke method "add" with parameter 10
Service A

Borja Sotomayor , http://gdp.globus.org/gt4-tutorial/multiplehtml/ch10s02.html

Globus's Use of Security Standards



	Message-level Security w/X.509 Credentials	Message-level Security w/Usernames and Passwords	Transport-level Security w/X.509 Credentials
Authorization	SAML and grid-mapfile	grid-mapfile	SAML and grid-mapfile
Delegation	X.509 Proxy Certificates/ WS-Trust		X.509 Proxy Certificates/ WS-Trust
Authentication	X.509 End Entity Certificates	Username/ Password	X.509 End Entity Certificates
Message Protection	WS-Security WS-SecureConversation	WS-Security	TLS
Message format	SOAP	SOAP	SOAP

Supported, but slow

Supported, but insecure

Fastest, so default

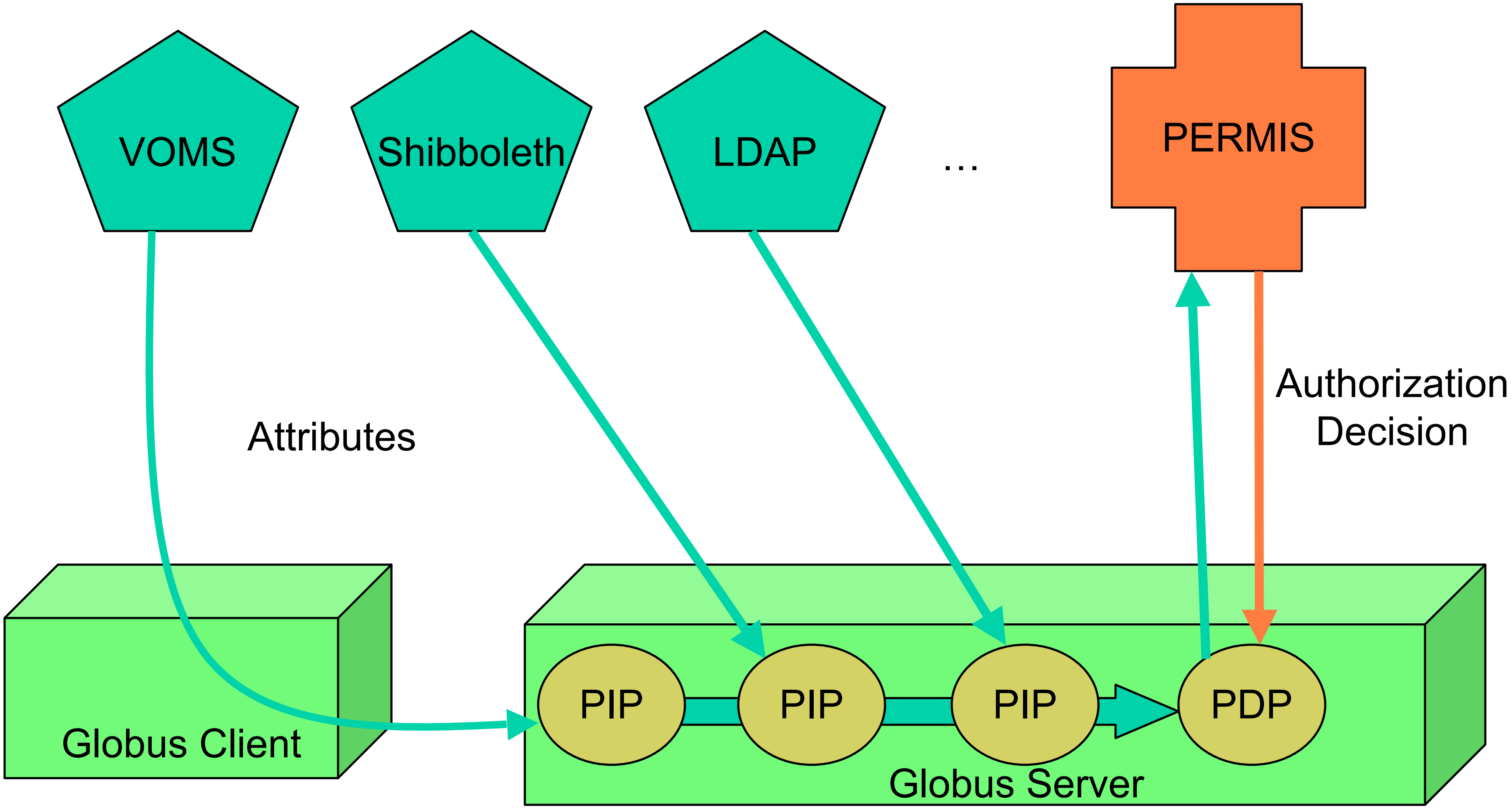
Globus Security

- Extensible authorization framework based on Web services standards
  - SAML-based authorization callout
    - Security Assertion Markup Language, OASIS standard
    - Used for Web Browers authentication often
    - Very short-lived bearer credentials
  - Integrated policy decision engine
    - XACML (eXtensible Access Control Markup Language) policy language, per-operation policies, pluggable

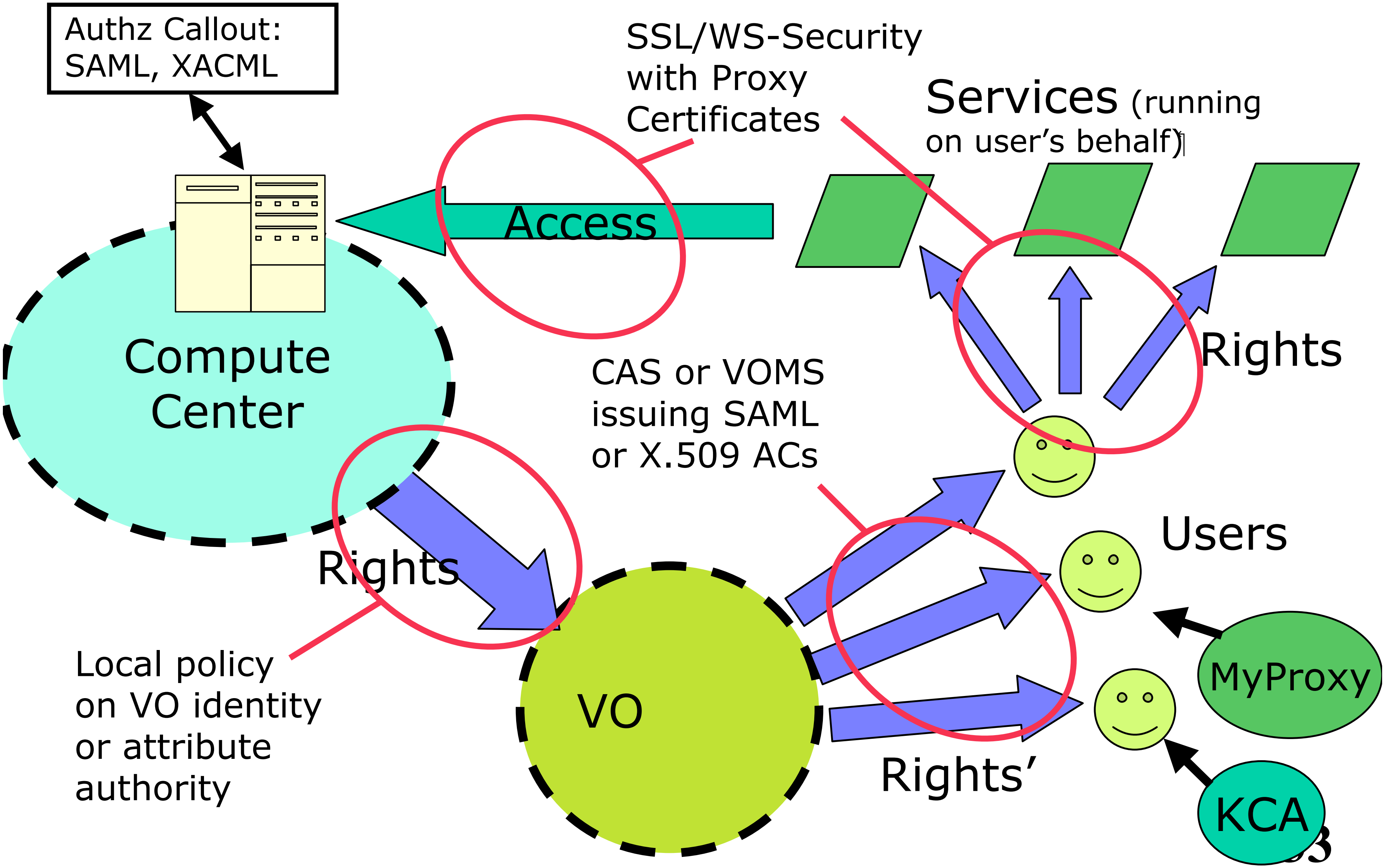
Globus-XACML Integration

- eXtensible Access Control Markup Language
  - OASIS standard, open source implementations
- XACML: sophisticated policy language
- Globus Toolkit ships with XACML runtime
  - Included in every client and server built on Globus core
  - Turned-on through configuration
- … that can be called transparently from runtime and/or explicitly from application …
- … and we use the XACML-”model” for our Authz Processing Framework

Globus Authorization Framework



Globus Security



Authz Callout: SAML, XACML

SSL/WS-Security with Proxy Certificates

Services (running on user's behalf)

Access

Compute Center

Rights

CAS or VOMS issuing SAML or X.509 ACs

Users

MyProxy

KCA

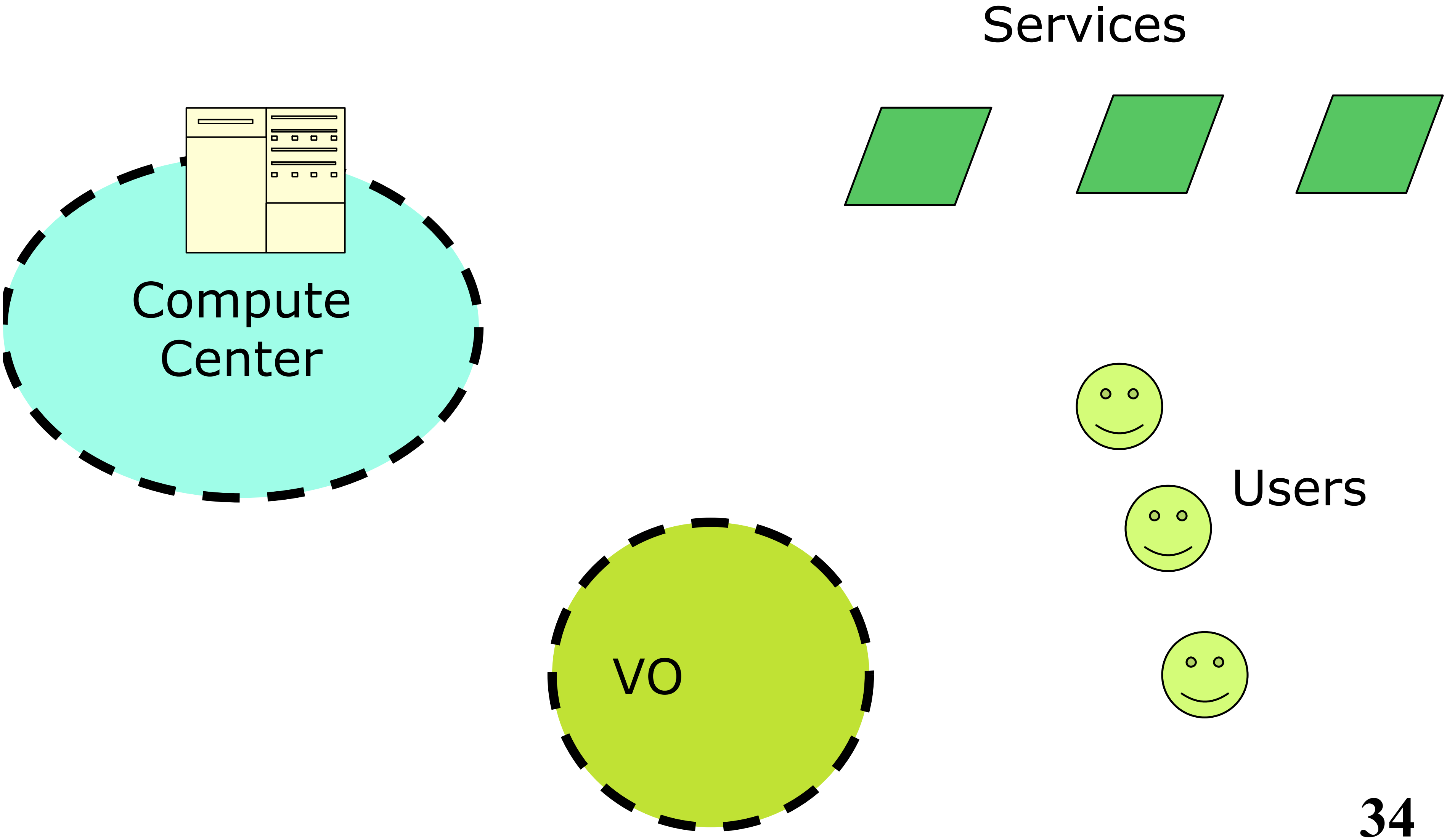
Rights

Local policy on VO identity or attribute authority

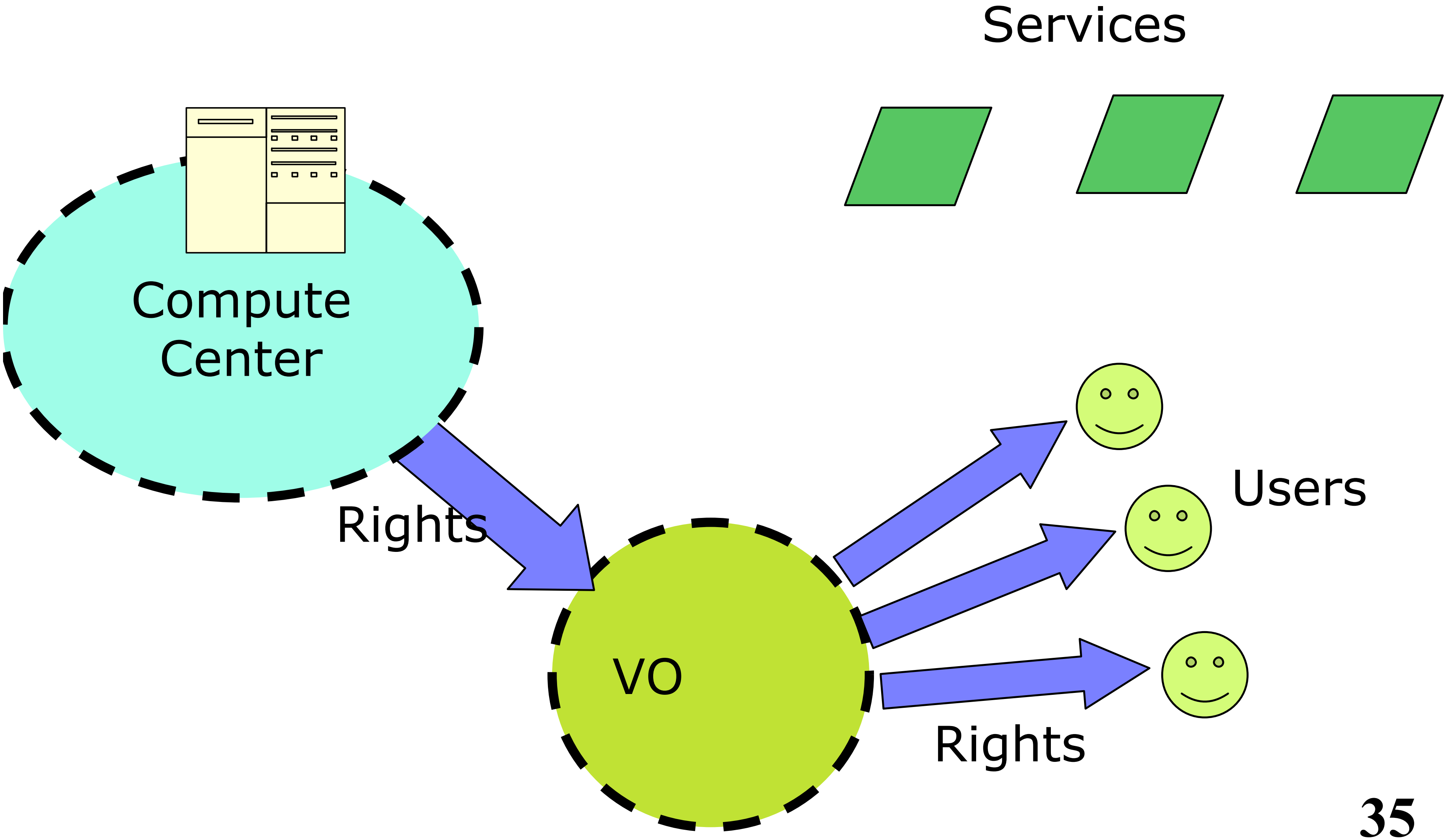
VO

Rights'

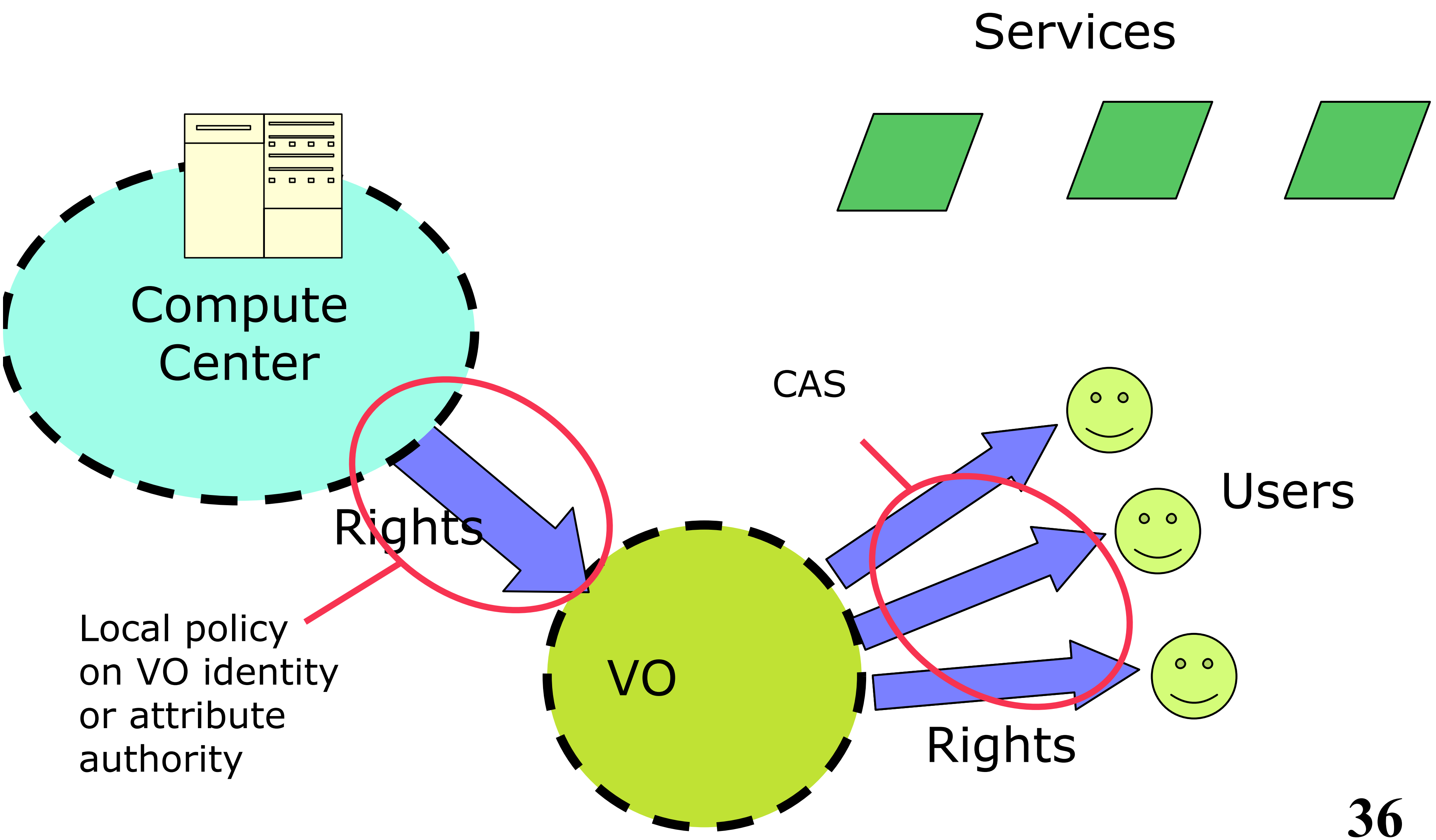
Globus Security: How It Works



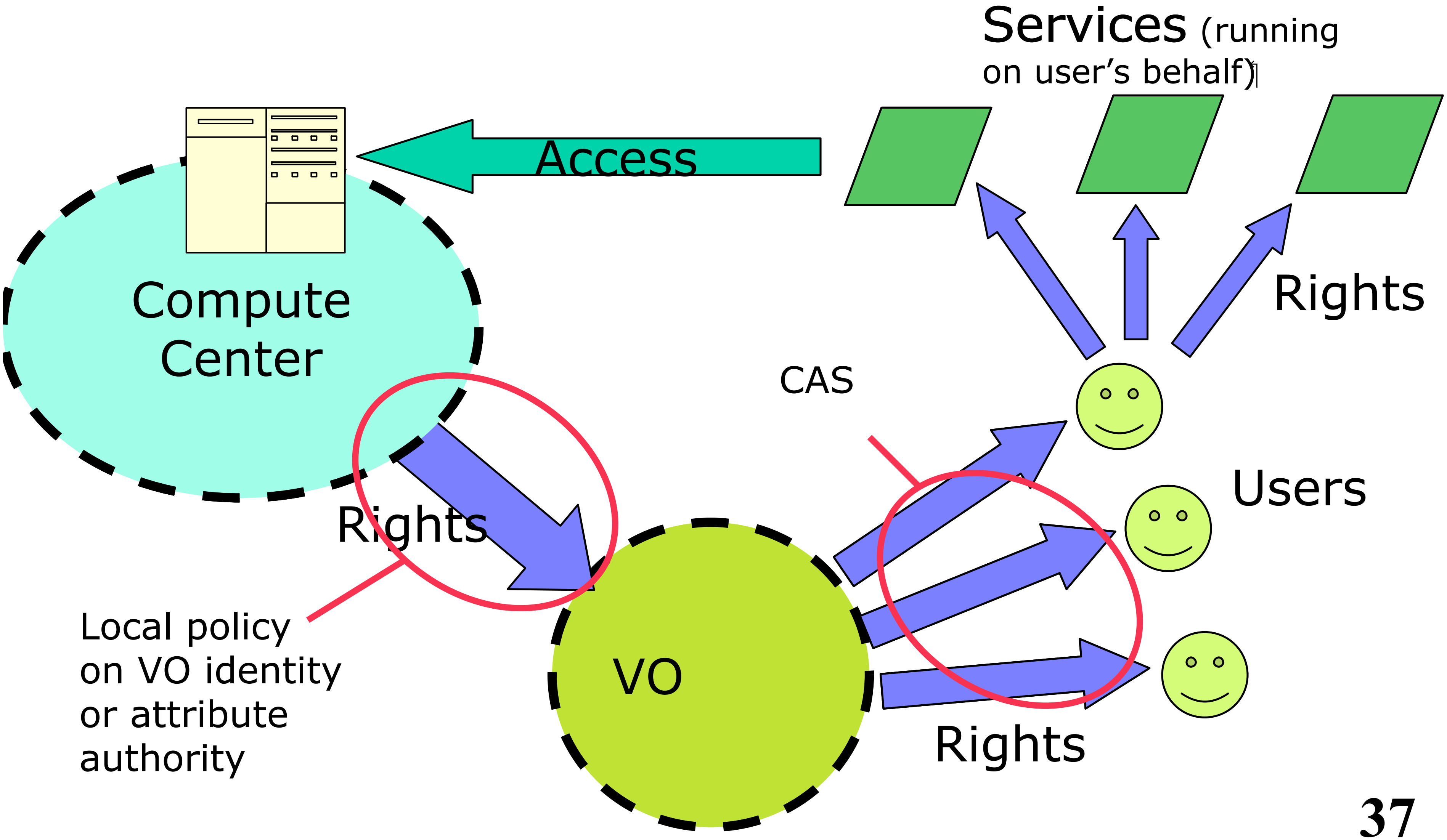
Globus Security: How It Works



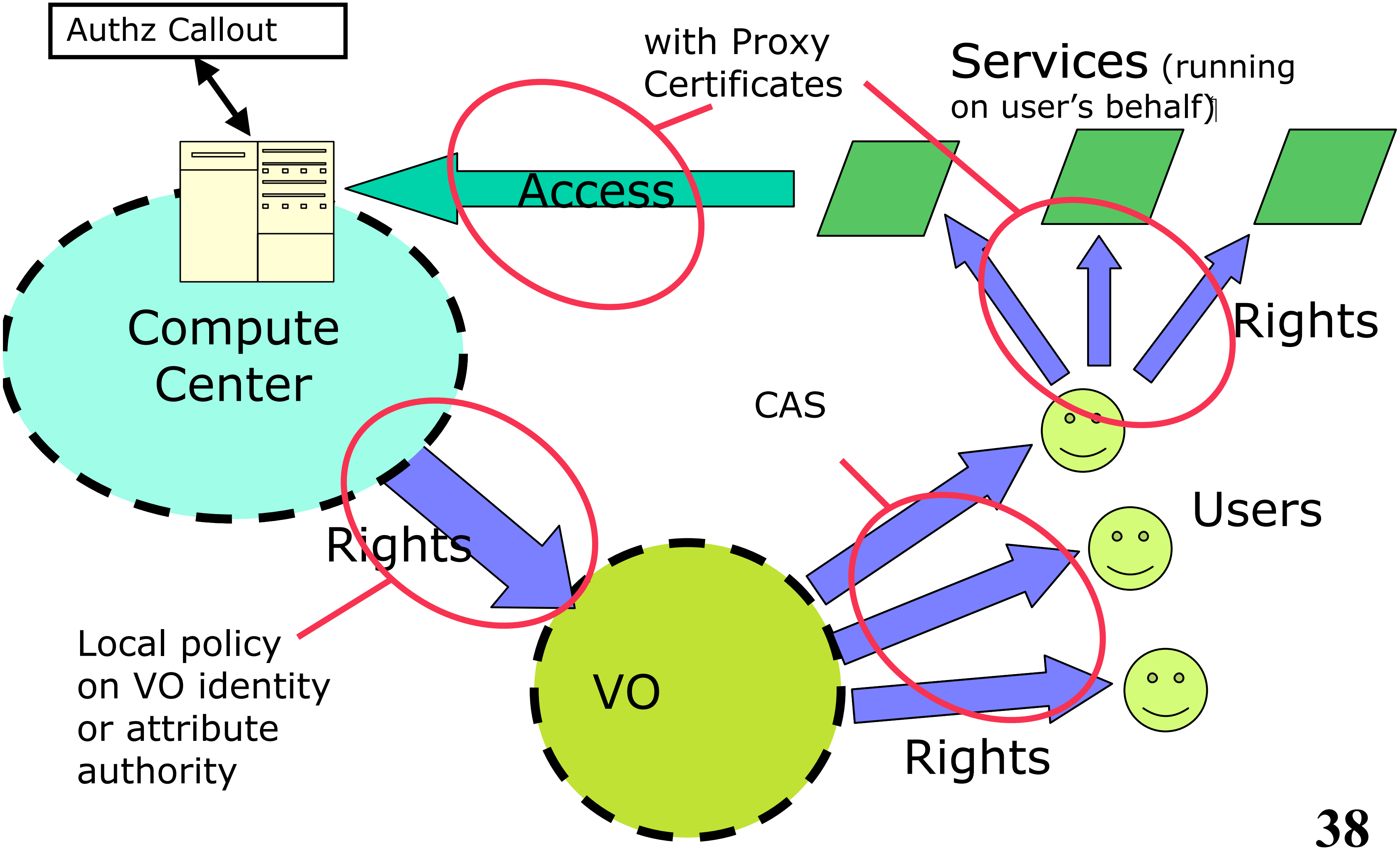
Globus Security: How It Works



Globus Security: How It Works


Services (running on user’s behalf)
Access
Compute Center
Rights
CAS
Users
Rights
Local policy on VO identity or attribute authority
VO
Rights

Globus Security: How It Works



Authz Callout
with Proxy Certificates
Services (running on user's behalf)
Access
Rights
Compute Center
CAS
Users
Rights
Local policy on VO identity or attribute authority
VO
Rights

A Cautionary Note

- Grid security mechanisms are tedious to set up
  - If exposed to users, hand-holding is usually required
  - These mechanisms can be *hidden entirely* from end users, but still used behind the scenes
- These mechanisms exist for good reasons.
  - Many useful things can’t be done without Grid security
  - It is unlikely that an ambitious project could go into production operation without security like this
  - Most successful projects end up using Grid security, but using it in ways that end users don’t see much