



Enabling Grids for E-science

# PKI, Certificates and CAs – Oh My!

*Hank Nussbacher*

*Israel InterUniversity Computation Center*

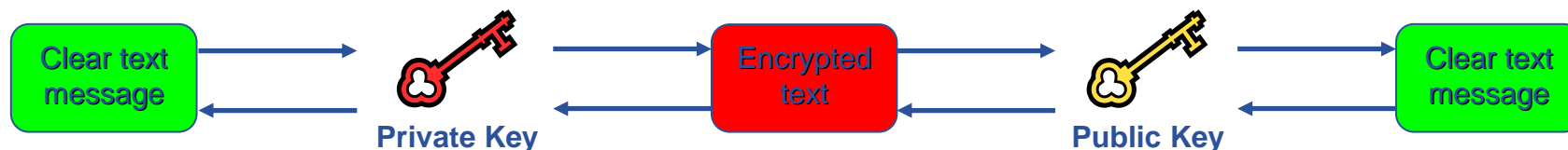
**Ra'nanna, 28 September 2005**

[www.eu-egee.org](http://www.eu-egee.org)

[iaq.iucc.ac.il](http://iaq.iucc.ac.il)



- **Public Key Infrastructure: Basis for authentication, integrity, confidentiality, non-repudiation**
- **Asymmetric encryption**



- **Digital signatures**
  - A hash derived from the message and encrypted with the signer's private key
  - Signature checked decrypting with the signer's public key
- **Allows key exchange in an insecure medium using a trust mode**
  - Keys trusted only if signed by a trusted third party (Certification Authority)
  - A CA certifies that a key belongs to a given principal
- **Certificate: held in two parts**
  - Public key + principal information + CA signature
  - Private key: only the owner (should) use this

- **A's digital signature is safe if:**
  1. A's private key is not compromised
  2. B knows A's public key
- **How can B be sure that A's public key is really A's public key and not someone else's?**
  - *A third party* guarantees the correspondence between public key and owner's identity, by signing a document which contains the owner's identity and his public key (**Digital Certificate**)
  - Both A and B must trust this third party
- **Two models:**
  - X.509: hierarchical organization;
  - PGP: "web of trust".

- **X 509 Digital certificate is the basis of AA in EGEE**
- **Certification Authorities (CAs)**
  - ~one per country; builds network of “Registration Authorities” who issue certificates
- **CAs are mutually recognized – to enable international collaboration**
  - International Grid Trust Federation <http://www.gridpma.org/>
- **For Europe region CAs:**
  - <http://eugridpma.org/>
  - <http://marianne.in2p3.fr/datagrid/ca/ca-table-ca.html>
- **CA certificates – issued to**
  - Users: you get a Certificate and use it to access grid services
  - Sites providing resources
- **Uses Public Key Infrastructure**
  - Private key – known only to you
  - Public key included in your certificate

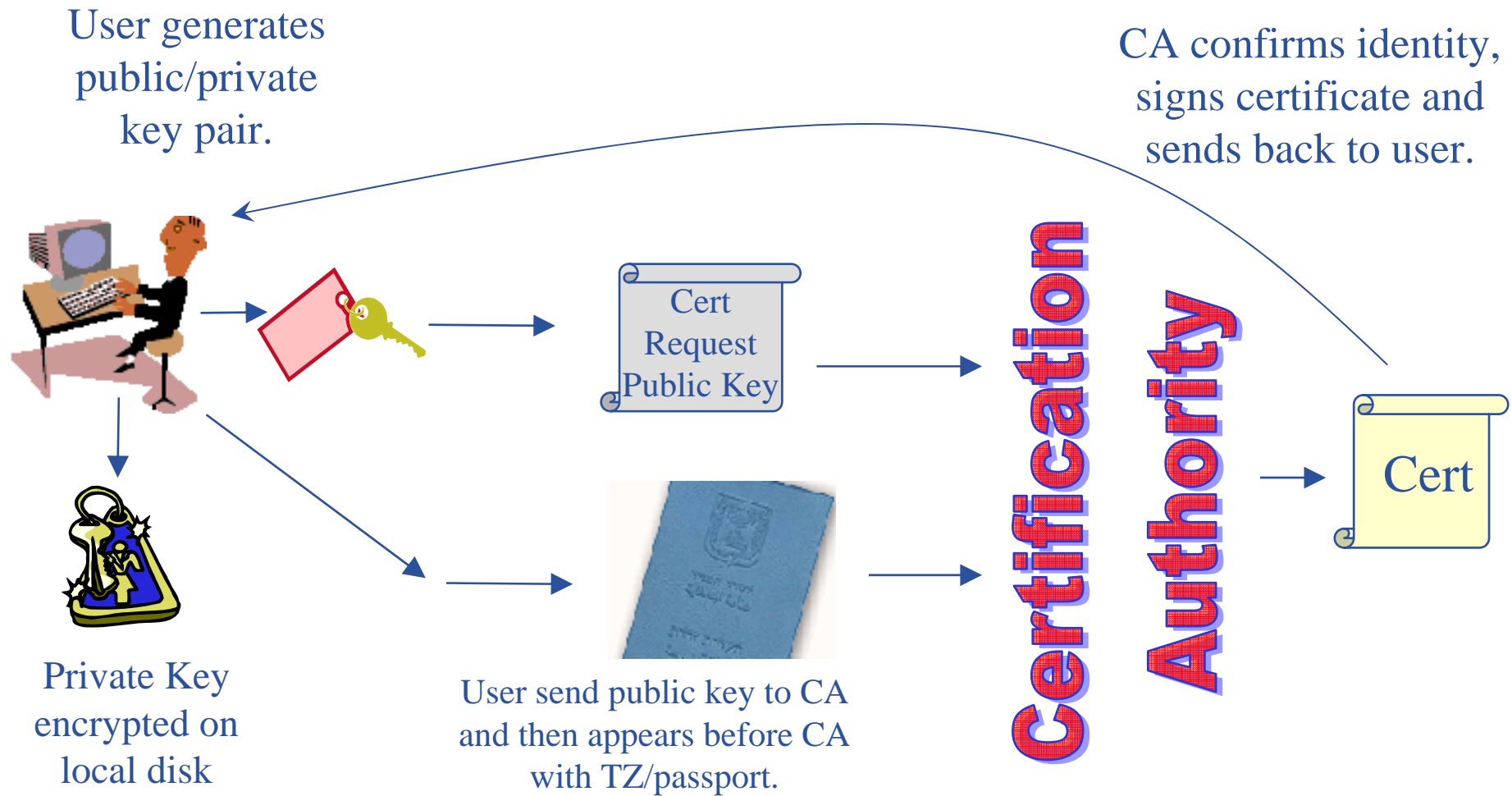
Certification Authorities - Testbed - Microsoft Internet Explorer

Address: <http://marianne.in2p3.fr/datagrid/ca/ca-table-ca.html>

## Certification Authorities

- **EGEE Users:**
  - Must obtain a certificate from their national or organisation certificate authority (see links below).
  - **These certificates are strictly personal and are not to be shared.**
  - Note that Globus certificates are not valid.
- **For users not covered by one of the CAs below:**
  - CNRS Datagrid-fr CA will act as the **EGEE catch-all CA** and DOE Grids CA will act as **LCG catch-all CA**.
  - EGEE catch-all CA procedure:
    - Users have to contact the [Registration Authority](#) of CNRS Datagrid-fr CA to setup a procedure.
  - LCG catch-all CA procedure:
    - [More information](#)
- **EGEE Site Administrators:**
  - Host certificates and service certificates may be obtained from the same national or organisation certificate authorities (see links below).
  - Note that Globus certificates are not valid.
- **CA RPMs and tar.gz download**
  - [Current distribution](#) of certificates, CRLs and signing policy file
  - [Tools to fetch CRLs, convert certificate,...](#) edg-utils-cert
- **EGEE CA administrators:**
  - [EU Grid PMA site](#).
- **EGEE CAs:**  
*Last update: August 30th 2005*

CA	Contact	How to obtain a certificate	CA Certificate		CA CRL		CP/CPS	Subject MD5 Finge. SHA1 Finge
			Download file	Import into browser	Download file	Import into browser		
<a href="#">Armenia - ArneSfo</a>	<a href="#">Ara Grigoryan</a> <a href="#">Artem Harutyunyan</a>		<a href="#">d0c2a341.0</a>		<a href="#">d0c2a341.r0</a>		X	/C=AM/O=ArneSfo/CN=ArneSfo CA MD5 Fingerprint=63:B3:08:9F:57:76:4A:B0:FC: SHA1 Fingerprint=9A:C4:99:EE:D5:73:3B:77:01
<a href="#">Austria AustrianGrid</a>	<a href="#">Willy Weisz</a> <a href="#">ca@austriangrid.at</a>	User	<a href="#">6e3b436b.0</a>		<a href="#">6e3b436b.r0</a>		X	/C=AT/O=AustrianGrid/OU=Certification Auth MD5 Fingerprint=A6:91:4F:6E:A8:55:0E:AF:74: SHA1 Fingerprint=A7:A7:FD:95:B6:06:FF:FC:7
<a href="#">Belgium - BEGrid</a>	<a href="#">gridca@belnet.be</a>	User Host	<a href="#">03aa0ecb.0</a>	X	<a href="#">03aa0ecb.r0</a>	X	X	/C=BE/O=BELNET/OU=BEGrid/CN=BEGrid MD5 Fingerprint=E3:90:39:1B:3C:E9:89:57:86:5 SHA1 Fingerprint=76:D6:39:F7:6C:12:45:9B:DE
<a href="#">Canada</a>								/C=CA/O=Grid/CN=Grid Canada CA



The goal of authorization and authentication of users and resources is done through digital certificates, in X.509 format

## Certification Authority (CA)

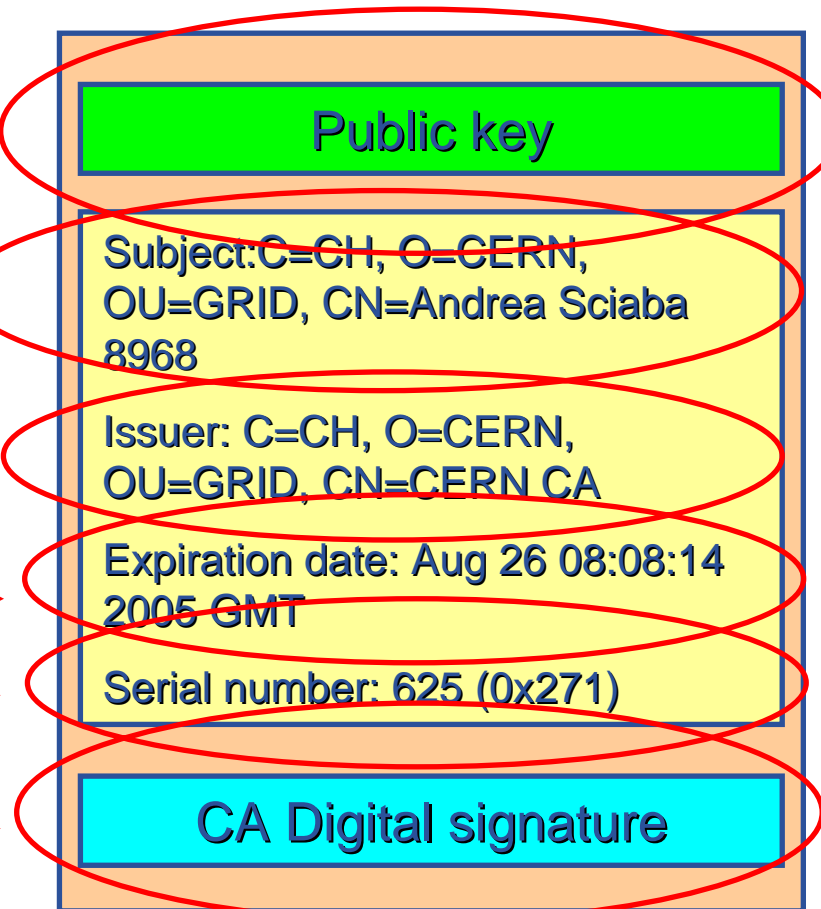
- Issue Digital Certificates for users and machines
- Check the identity and the personal data of the requestor
  - Registration Authorities (RAs) do the actual validation
- CA's periodically publish a list of compromised certificates
  - **Certificate Revocation Lists (CRL)**: contain all the revoked certificates yet to expire
- CA certificates are **self-signed**

For each player, a CA guarantees its authenticity with a certificate

- **An X.509 Certificate contains:**

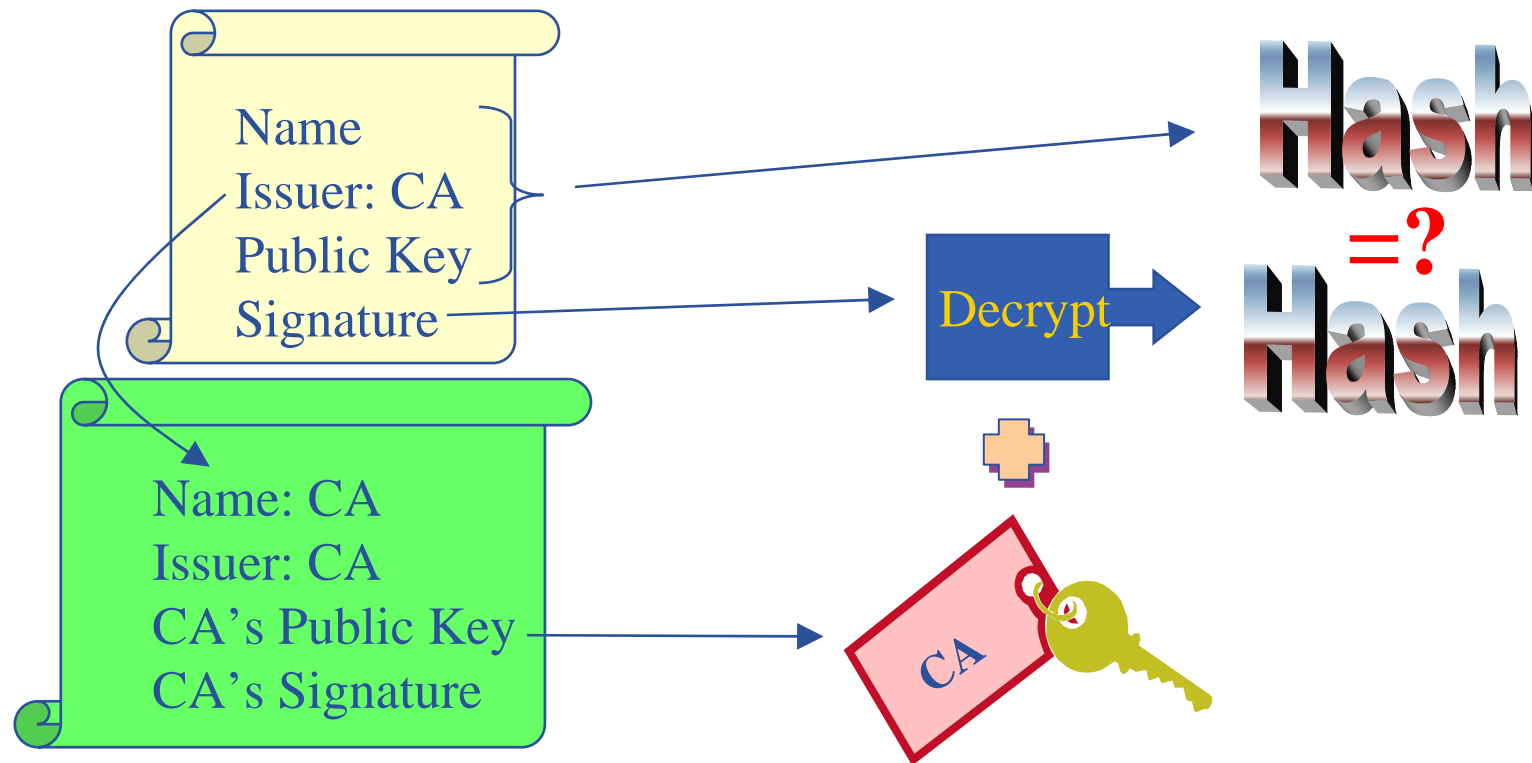
- owner's public key;
- identity of the owner;
- info on the CA;
- time of validity;
- Serial number;
- digital signature of the CA

Structure of a X.509 certificate

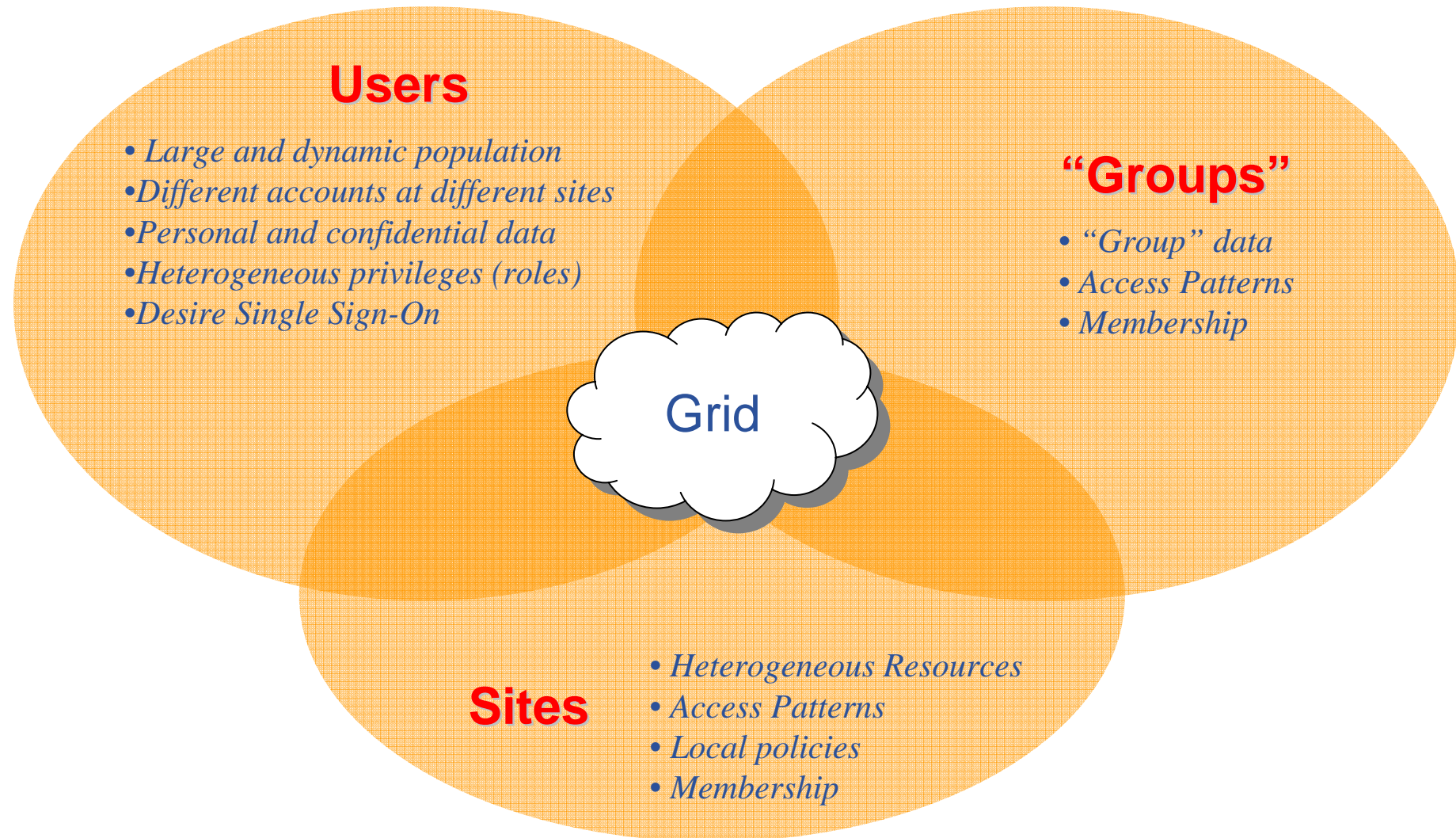




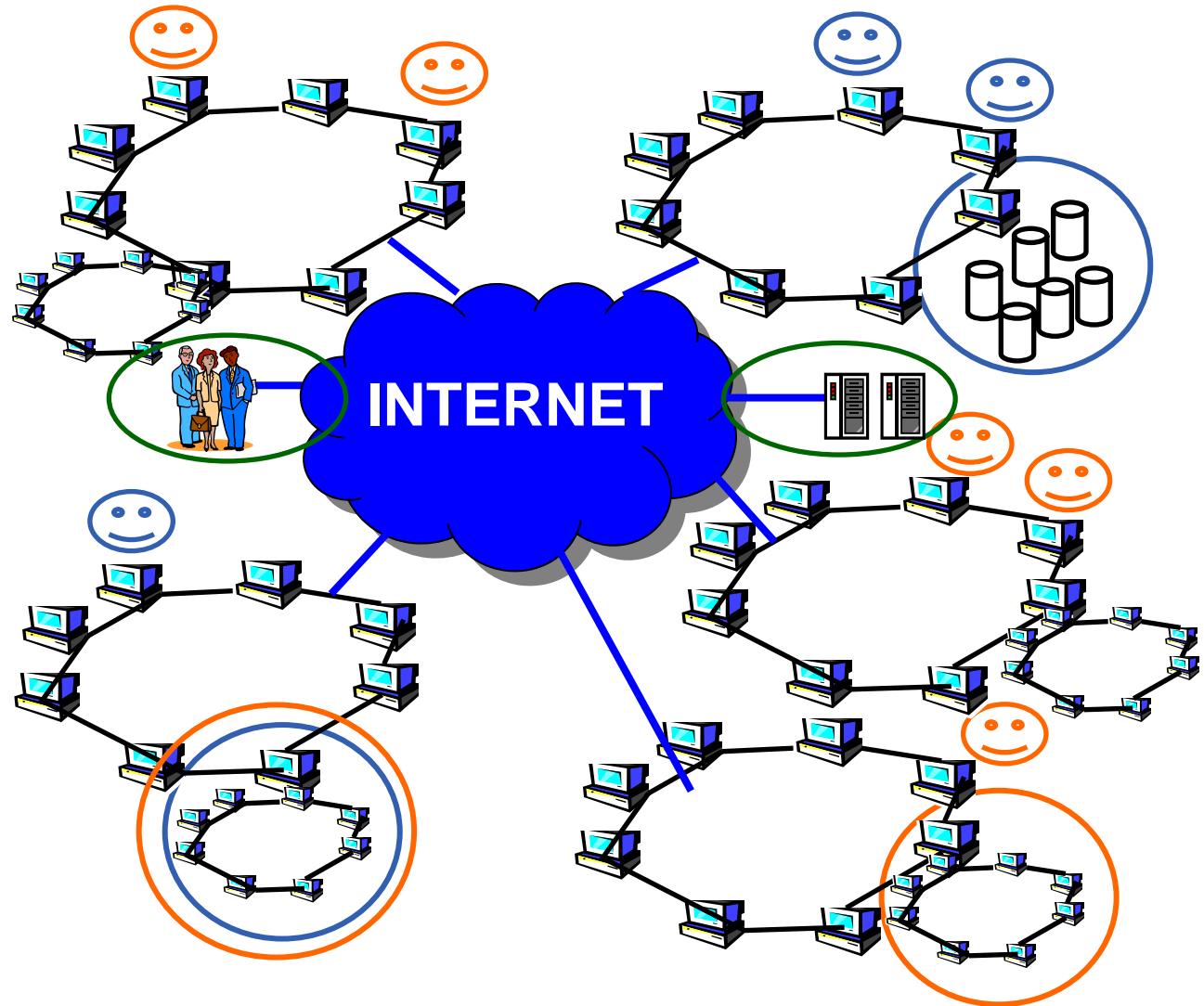
- The public key from the CA certificate can then be used to verify the certificate.



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



- **Support multiple VO's across**
  - Administrative domains
  - National borders
  - Via Internet
- **Single sign-on**
  - Multiple services
  - Delegation
- **Scalability:**
  - N,000 users
  - M,000 CPUs
  - Without M\*N million usernames / passwords...
- **Security**



- **46 CA's so far**
  - Armenia, Austria, Belgium, Canada, CERN, France (4), China, Cyprus (2), Czech Republic (2), Estonia, Germany (4), Greece, Hungary, Ireland, Israel, Italy, Netherlands, Nordics, Pakistan, Poland, Portugal (2), Russia (2), South East Europe (Balkans), Slovakia, Slovenia, Spain, Switzerland (4), Taiwan, UK, US(3)
- **All required to have a CP/CPS**
  - Certificate Policy/Certificate Practice Statement

- **Israel's is located at:**

- [http://certificate.iucc.ac.il/ca/IUCC\\_CP-CPS\\_1\\_5.pdf](http://certificate.iucc.ac.il/ca/IUCC_CP-CPS_1_5.pdf)

- **78 certificates issued so far**

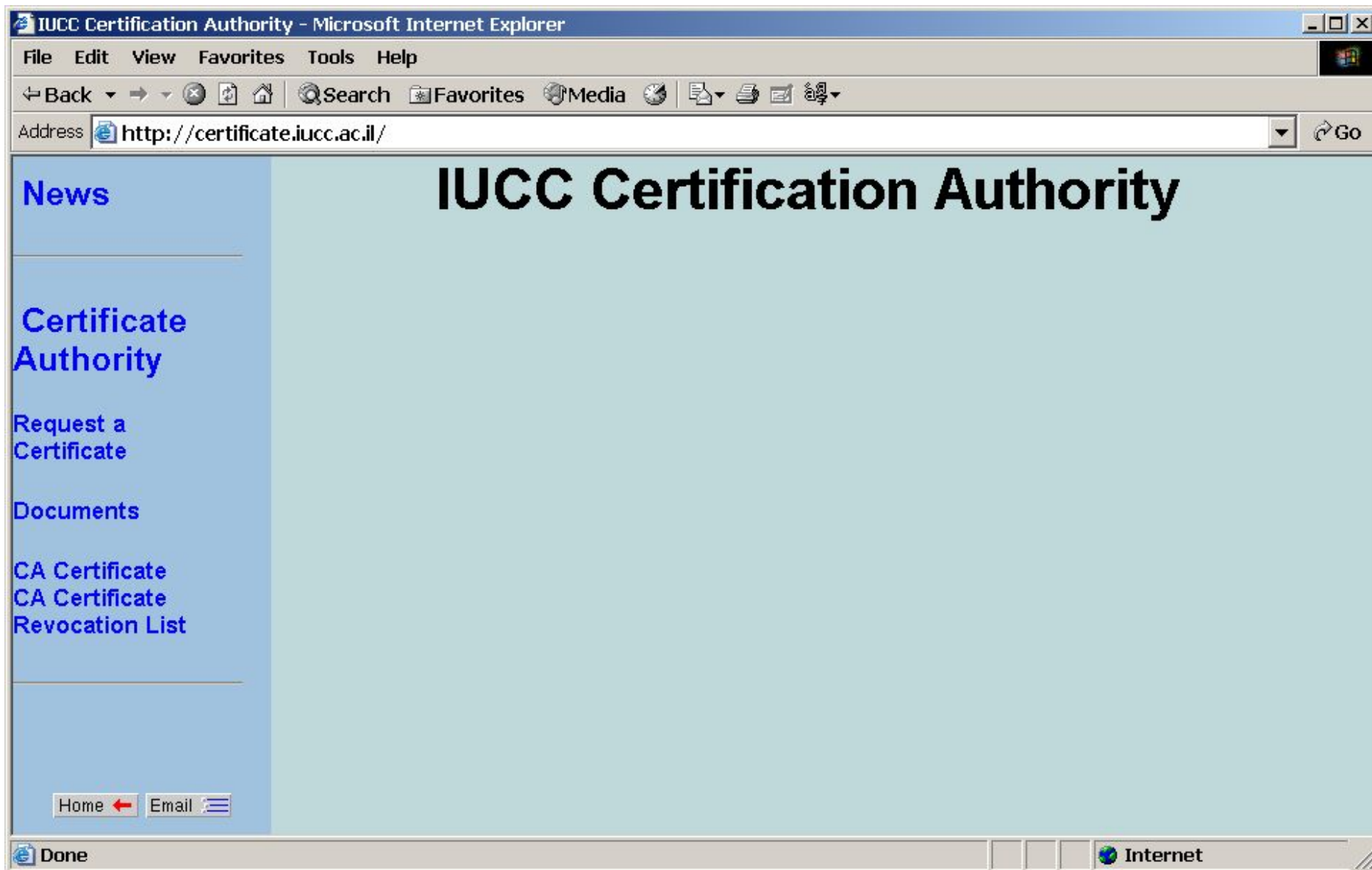
- 22 computer
  - 56 human

- **Authentication**
  - TZ or Passport
  - Visual identification (only in person) via CA (no RAs yet)
- **Key sizes (minimum)**
  - User and host: 1024 bit
  - IUCC CA: 2048 bit
- **Validity**
  - IUCC CA: 5 years
  - Entity: maximum 1 year

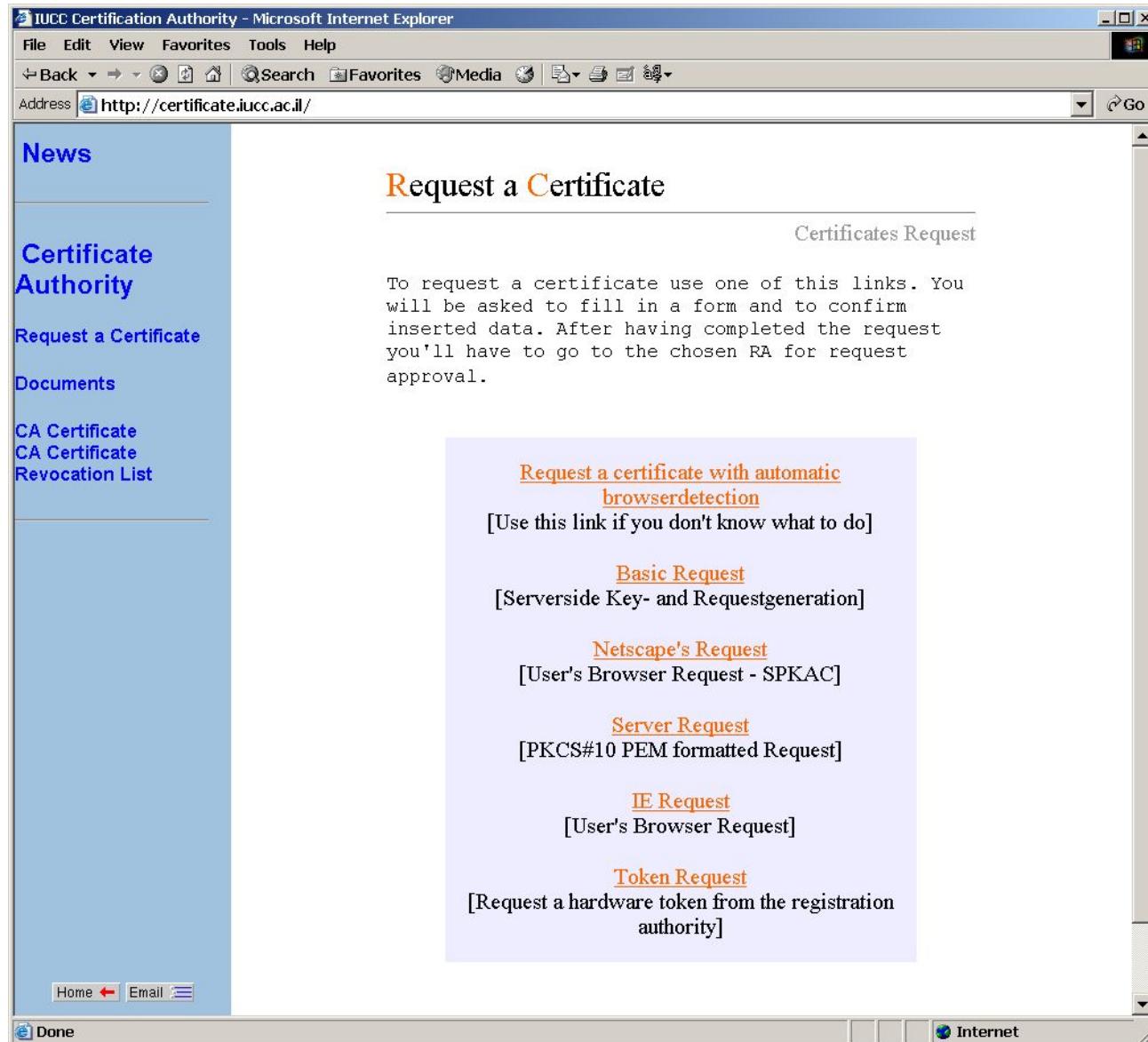
# LIST of Israeli CA and RAs

- **Eddie Aronovich, Certificate Authority Manager**  
**[eddiea@tau.ac.il](mailto:eddiea@tau.ac.il), 03-6406915**

University	Name	e-mail	phone
Hebrew	Ayelet Hashachar Drori	ayeleth@savion.cc.huji.ac.il	<b>02-6584475</b>
Haifa	Herakel Endrawes	herakel@univ.haifa.ac.il	<b>04-8249249</b>
Technion	Anne Weill	anne@tx.technion.ac.il	<b>04-8294997</b>
Weizmann	Pierre Choukroun	pierre@weizmann.ac.il	<b>08-9343038</b>
BGU	Amir Zofnat	zofnat@bgu.ac.il	<b>08-6479449</b>
Open-U	Reuven Aviv	aviv@openu.ac.il	<b>09-7781252</b>
TAU	Avi Raber	avir@tauex.tau.ac.il	<b>03-6409117</b>







**Request a Certificate**

Certificates Request

To request a certificate use one of this links. You will be asked to fill in a form and to confirm inserted data. After having completed the request you'll have to go to the chosen RA for request approval.

[Request a certificate with automatic browserdetection](#)  
[Use this link if you don't know what to do]

[Basic Request](#)  
[Serverside Key- and Requestgeneration]

[Netscape's Request](#)  
[User's Browser Request - SPKAC]

[Server Request](#)  
[PKCS#10 PEM formatted Request]

[IE Request](#)  
[User's Browser Request]

[Token Request](#)  
[Request a hardware token from the registration authority]

IUCC Certification Authority - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://certificate.iucc.ac.il/>

**News**

---

**Certificate Authority**

[Request a Certificate](#)

**Documents**

[CA Certificate](#)

[CA Certificate Revocation List](#)

**Basic Certificate Request**

Please enter your data in the following form.

<b>Certificate Data</b>	
E-Mail	<input type="text"/>
Name	<input type="text"/>
Institution	IUCC <input type="text"/>
alternative email	<input type="text"/>
<b>User Data</b>	
Name (first and Last name)	<input type="text"/>
Email	<input type="text"/>
Department	<input type="text"/>
Telephone	<input type="text"/>
Level Of Assurance chose the LOA you would like to be authenticated against.	Test <input type="text"/>
Role	CA Operator <input type="text"/>
Registration Authority chose the RA where you will be authenticated.	IUCC <input type="text"/>
PIN [used to verify the certification request, min 10 chars (please write it down for later usage)]	<input type="text"/>
Re-type your PIN for confirmation	<input type="text"/>
Choose a keysize	1024 <input type="text"/>

Home  Email

Done Internet

Cyprus Grid Certification Authority - Microsoft Internet Explorer

File Edit View Favorites Tools Help

← Back → Stop Home Search Favorites Media

Address <http://grid.ucy.ac.cy/CyGridCA/>

---

## CyGrid Certification Authority

---

### General information

The CyGrid Certification Authority (CyGridCA) is the top-level certification authority for Grids in Cyprus. It provides X.509 certificates for identification and authentication purposes related to Grid activities in Cyprus. The CyGridCA has been established within the EU project [CrossGrid](#), and now extended to cover the latest EU project [EGEE](#) (Enabling Grids for E-science in Europe). Its duty is to certify, with its digital signature, the following:

- the public keys belonging to the certification authorities;
- the public keys of the registration authorities which act for and on behalf of CyGridCA;
- the public keys of end entities (users and machines).

CyGridCA is mutually recognized by the Certification Authorities of most European countries and the USA. It has been certified by the [EUGridPMA](#), the European Policy Management Authority for Grid Authentication in e-Science. For more information, please check also the [Acceptance Matrix](#) maintained by Dr. Coghlan of Trinity College, Dublin.

### Certification Policy

The latest CyGridCA Certification Practice Statement (CPS, version 1.0.4) is available online in [pdf](#) format.



**CyGrid Certification Authority**

---

**Registration Authorities managed by CyGridCA**

**1. HPCLUCY**

RA - HPCL (High Performance Computing systems Lab - Registration Authority)  
C=CY, O=CYGRID, O=HPCL, CN=\*

**Instructions for users:**

Please follow the "[user how to](#)" short guide for creating a user private key and certificatio

**Instructions for site administrators:**

Please follow the "[host how to](#)" short guide for creating a machine private key and certific how to receive the signed certificate and how to setup your grid nodes.

**Contact information:**

HPCL Registration Authority  
Computer Science Department  
University of Cyprus  
P.O.Box 20537  
CY-1678 Nicosia, CYPRUS

Tel: +357-22.89.26.63  
Fax: +357-22.89.27.01  
Email: [hpcl@ucy.ac.cy](mailto:hpcl@ucy.ac.cy)

- **Every CA must provide a CP/CPS (combined)**
  - RFC2527 preferred
- **Cross-evaluation of CP/CPS by every CA Manager**
  - tries to make up for lack of auditing
  - provide trust guidelines for “local” site administrators
  - Every CA Manager should inspect **all** other CP/CPSs

- **Security**

- machine with CA private key not connected to any network
- All CA’s issue a CRL (Certification Revocation List) with a 30-day lifetime (updated ~ weekly)
- Relying parties must update every 24 hrs
- Audit logs must be kept

- To get cert information run **grid-cert-info**

```
[scampana@grid019:~]$ grid-cert-info -subject
```

```
/C=CH/O=CERN/OU=GRID/CN=Simone Campana 7461
```

- Options for printing cert information
  - all
  - subject
  - issuer
  - startdate
  - enddate
  - help

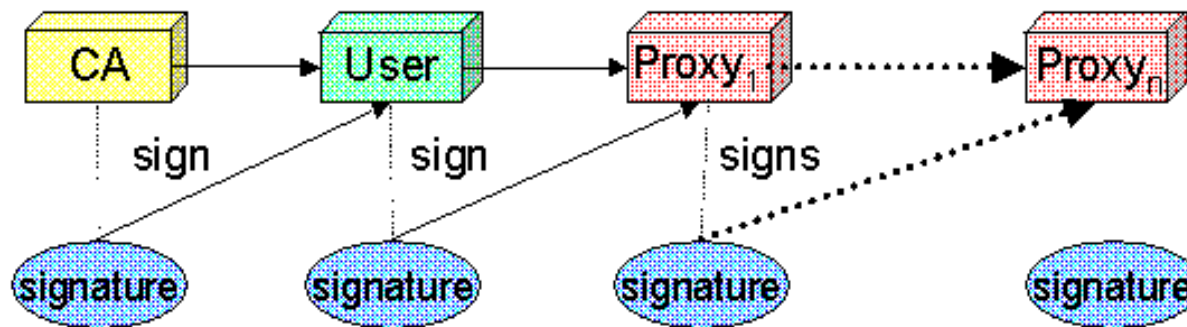
- **Keep your private key secure.**
- **Do not loan your certificate to anyone.**
- **Report to your local/regional contact if your certificate has been compromised.**
- **Do not launch a delegation service for longer than your current task needs.**

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

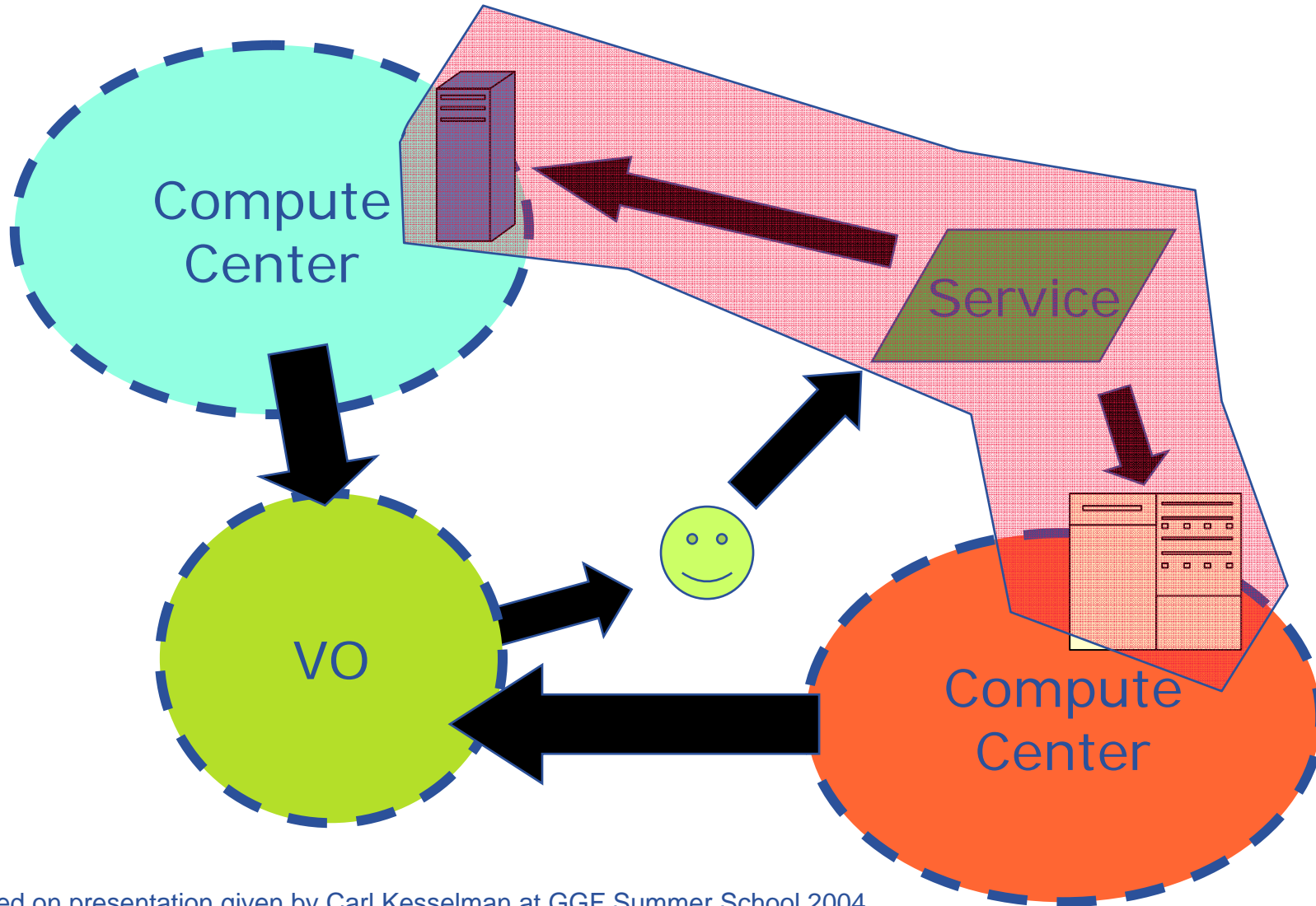
**IT IS YOUR PASSPORT AND CREDIT CARD**



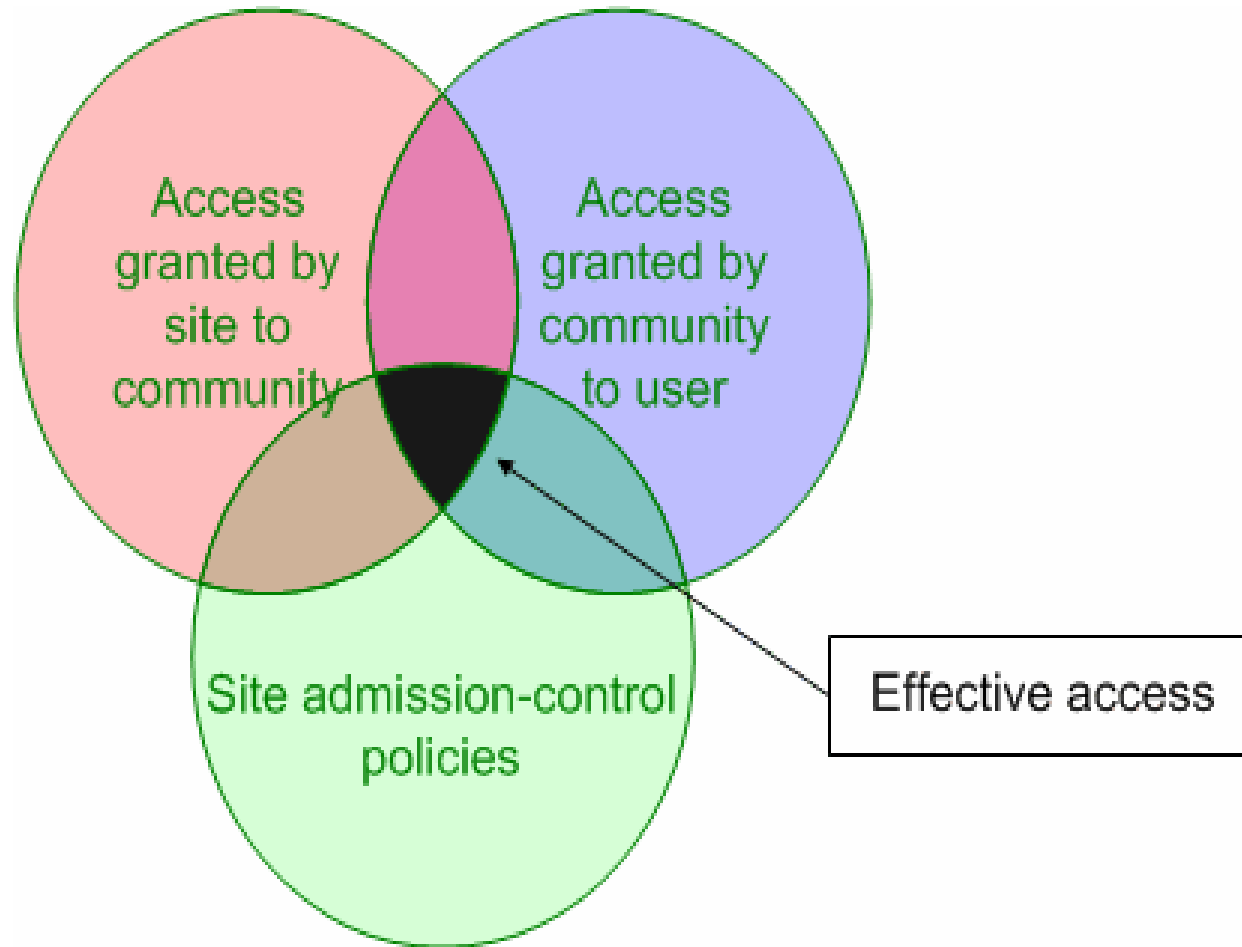
- *de facto* standard for Grid middleware
- Based on PKI
- To support....
  - Single sign-on: to a machine on which your certificate is held
  - Delegation: a service can act on behalf of a person
  - Mutual authentication: both sides must authenticate to the other
- ....GSI introduces **proxy certificates**
  - Short-lived certificates signed with the user's certificate or a proxy
  - Reduces security risk, enables delegation



- CA and user included in the proxy... See practical later



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



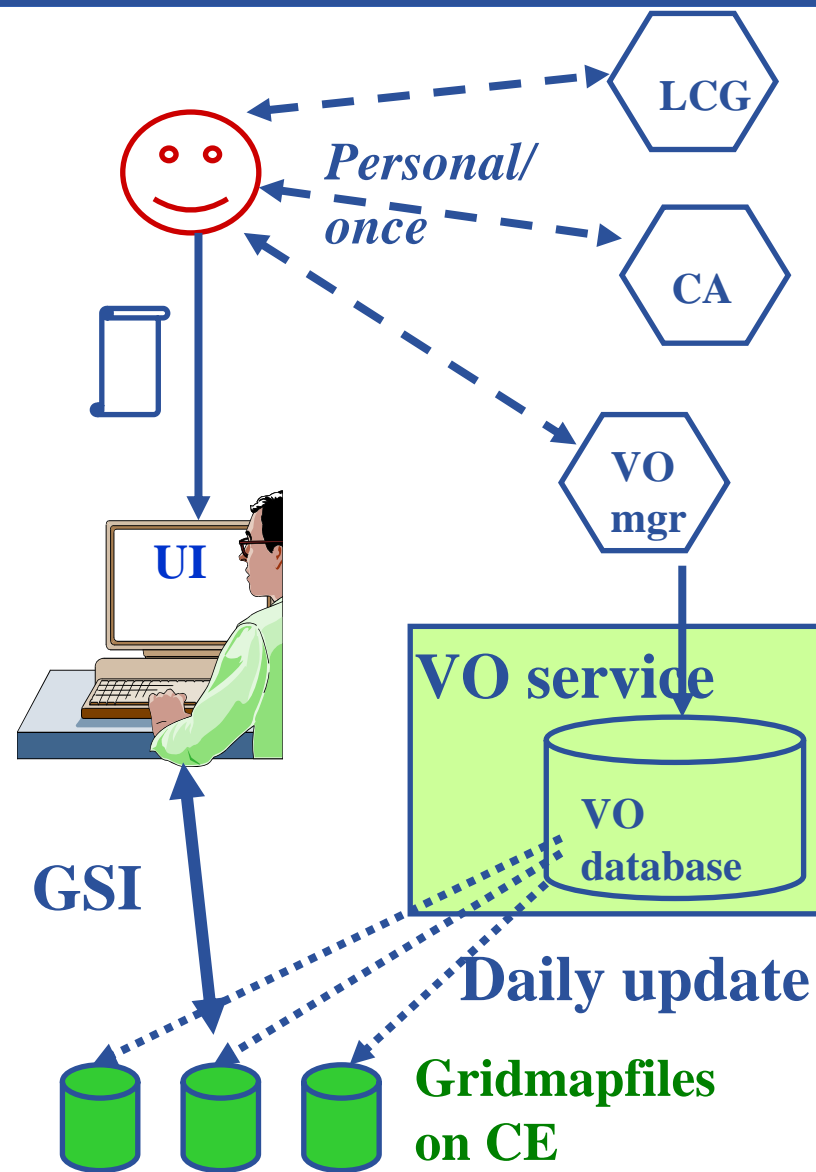
slide based on presentation given by Carl Kesselman at GGF Summer School 2004

- **Authentication**

- User certificate signed by CA
- Connects to UI by ssh
- Downloads certificate
- Invokes Proxy server
- **Single logon** – to UI - then **Grid Security Infrastructure identifies user to other machines**

- **Authorisation**

- User joins Virtual Organisation
- VO negotiates access to Grid nodes and resources
- Authorisation tested by CE
- **gridmapfile maps user to local account**



[hank@efes.iucc.ac.il](mailto:hank@efes.iucc.ac.il)