

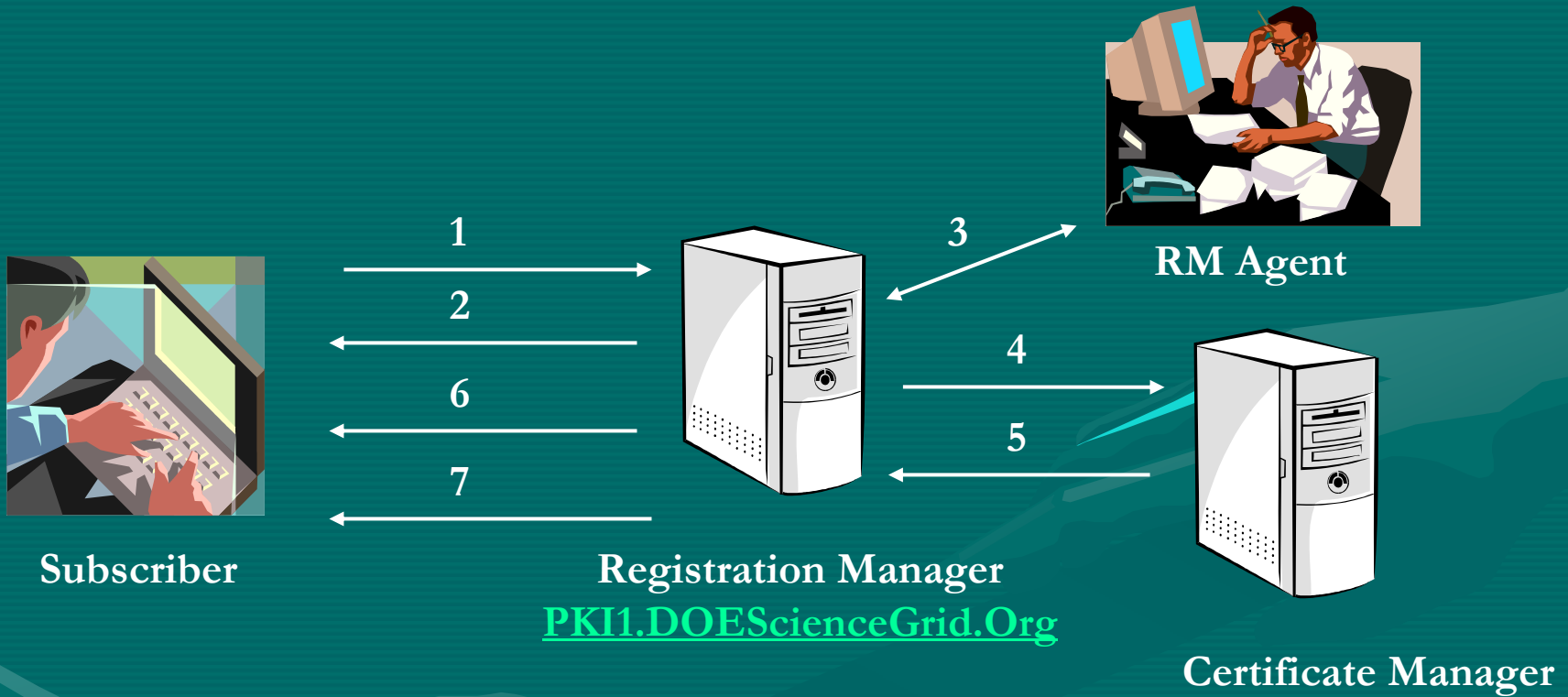
DOEGrids Public Key Infrastructure

DOEGrids PKI is funded by DOE
MICS and operated by ESnet

PKI achievements

- Policy Management Authority
 - PMA, currently has 15 members.
- Currently 9 Virtual Organizations and Sites supported
 - **PPDG** Doug Olsen, Ruth Pordes
 - **Fusion Grid** Mary Thompson
 - **PNNL** Scott Studham
 - **ORNL** Kasidit Chanchio
 - **ANL** John Volmer
 - **NERSC** Steve Lau, Steve Chan
 - **DOESG** Keith Jackson
 - **LBL** Joshua Boverhof
 - **iVDGL** Scott Koranda – Just added
- PPDG setting the pace
 - First Registration Authority Agent
 - First Trans Atlantic use of certificates with European Data Grid member
- European Data Grid
 - Broad acceptance by their PKI working group
 - Actively working with them on: PKI requirements, Certificate Policies and Directory

Certificate Request Workflow



1. Subscriber request Certificate
2. A notice request has been queued
3. The RA for the Subscriber reviews request – approves or rejects request
4. The Signed Certificate Request is sent to CA.

5. CM issues certificate
6. RM sends Email notice to Subscriber
7. Subscriber picks up new certificate

Certificate stats as of 6/20/2002

- ~ 40 – 80 Certs per month issued
- Total Certificates issued: 258
- Certificates revoked: 29
- People Certificates 101
- Services Certificates 100
- Host (internal usage) 12
- Requests in Queue: 5

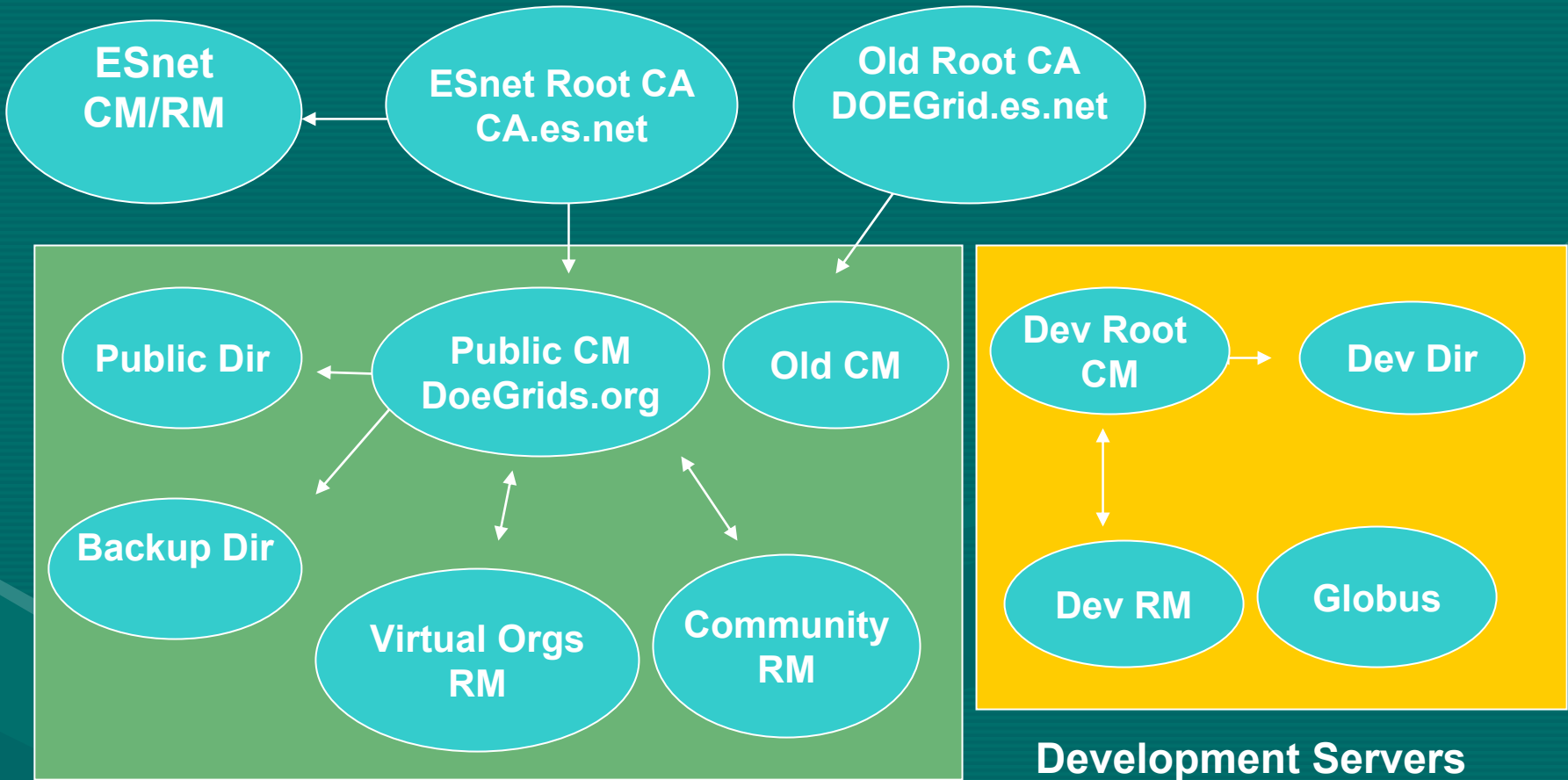
V2.0 DOEGrids Name Space

- Root CA
 - CN=Certificate Manager, OU=Certificate Authorities, O=DOE Science Grid
- Subordinate CAs
 - CN=pki1, OU=DOE Science Grid, OU=Certificate Authorities, DC=ES, DC=net
- End Entity (Subscriber)
 - CN=Mike 123, OU=People, O=doesciencegrid.org
- Service
 - CN=LDAP/foo.bar, OU=Services, O=doesciencegrid.org

V2.x DOEGrids Name Space

- Root CA
 - CN=Root, OU=Certificate Authorities, O=ESnet, DC=ES, DC=Net
- Subordinate CAs
 - CN=DOEGrids Community, OU=Certificate Authorities, DC=DOEGrids, DC=org
- End Entity (Subscriber)
 - CN=Mike 123, OU=People, DC=DOEGrids, DC=org
- Service
 - CN=LDAP/foo.bar, OU=Services, DC=DOEGrids, DC=org

Architecture for 10/15/02 deployment



DOEGrids Production Servers

Development Servers

CM: Certificate Manager

RM: Registration Manager

Dir: LDAP based Directory

DOEGrids LDAP DIT

6/15/2002

O= DOEScienceGrid.org



```
graph TD; O["O= DOEScienceGrid.org"] --- OU1["OU= Certificate Authorities"]; O --- OU2["OU= CRL issuing Point - Experimental"]; O --- OU3["OU= People"]; O --- OU4["OU= Services"]; O --- OU5["OU= Hosts (private)"];
```

OU= Certificate Authorities

OU= CRL issuing Point - Experimental

OU= People

OU= Services

OU= Hosts (private)

DOEGrids LDAP DIT

10/15/2002

DC= DOEGrids; DC=Org



```
graph TD; Root[DC= DOEGrids; DC=Org] --- OU1[OU= Certificate Authorities]; Root --- OU2[OU= CRL issuing Point - experimental]; Root --- OU3[OU= People]; Root --- OU4[OU= Services]; Root --- OU5[OU= Hosts (private)];
```

The diagram illustrates the LDAP Directory Information Tree (DIT) structure for DOEGrids. It starts with a root entry 'DC= DOEGrids; DC=Org' in a rounded rectangular box. A vertical line descends from this box and branches into five horizontal rounded rectangular boxes, each representing an Organizational Unit (OU). The OUs are listed from top to bottom: 'OU= Certificate Authorities', 'OU= CRL issuing Point - experimental', 'OU= People', 'OU= Services', and 'OU= Hosts (private)'.

OU= Certificate Authorities

OU= CRL issuing Point - experimental

OU= People

OU= Services

OU= Hosts (private)