Hierarchical Organization of Certification Authorities for Secure Environments

EUIT de Telecomunicación

Departamento de Ingeniería y Arquitecturas Telemáticas

Universidad de Madrid

Lourdes López Santidrián

Justo Carracedo Gallardo

Objectives

MAIN OBJECTIVE

To propose a Hierarchical Organization of CAS

Aims:

- General MODEL
- Open MODEL
- Easy solution for Certificate Path Validation

Pilot Experiment

EUIT de Telecomunicación

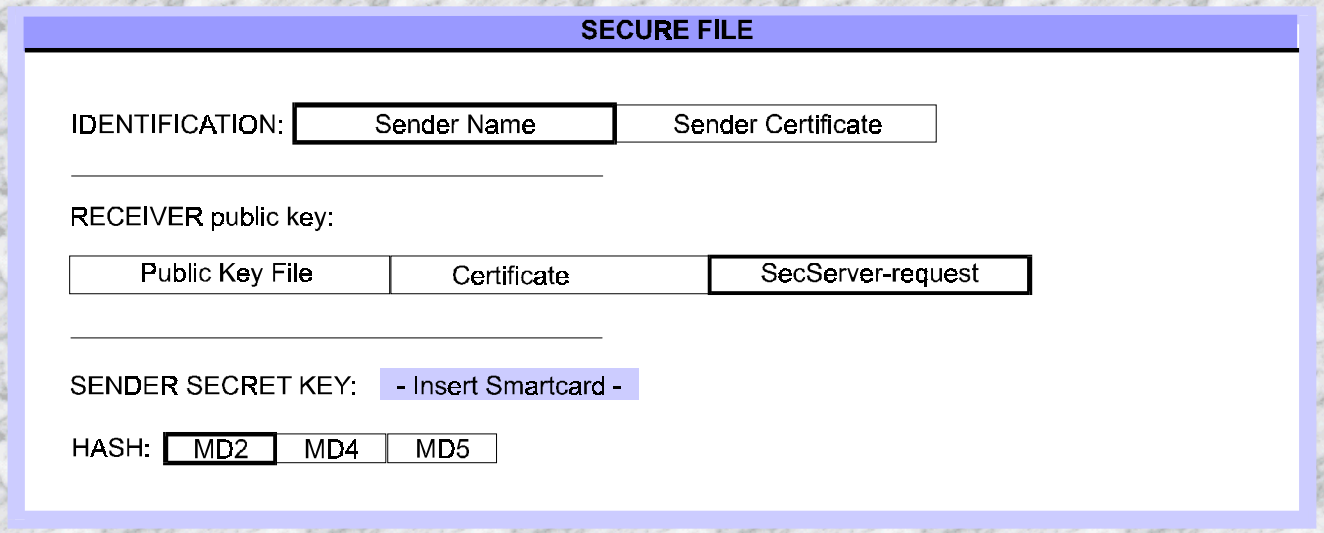
UNIVERSIDAD DE MADRID

Developments:

- Seckit
- SecServer

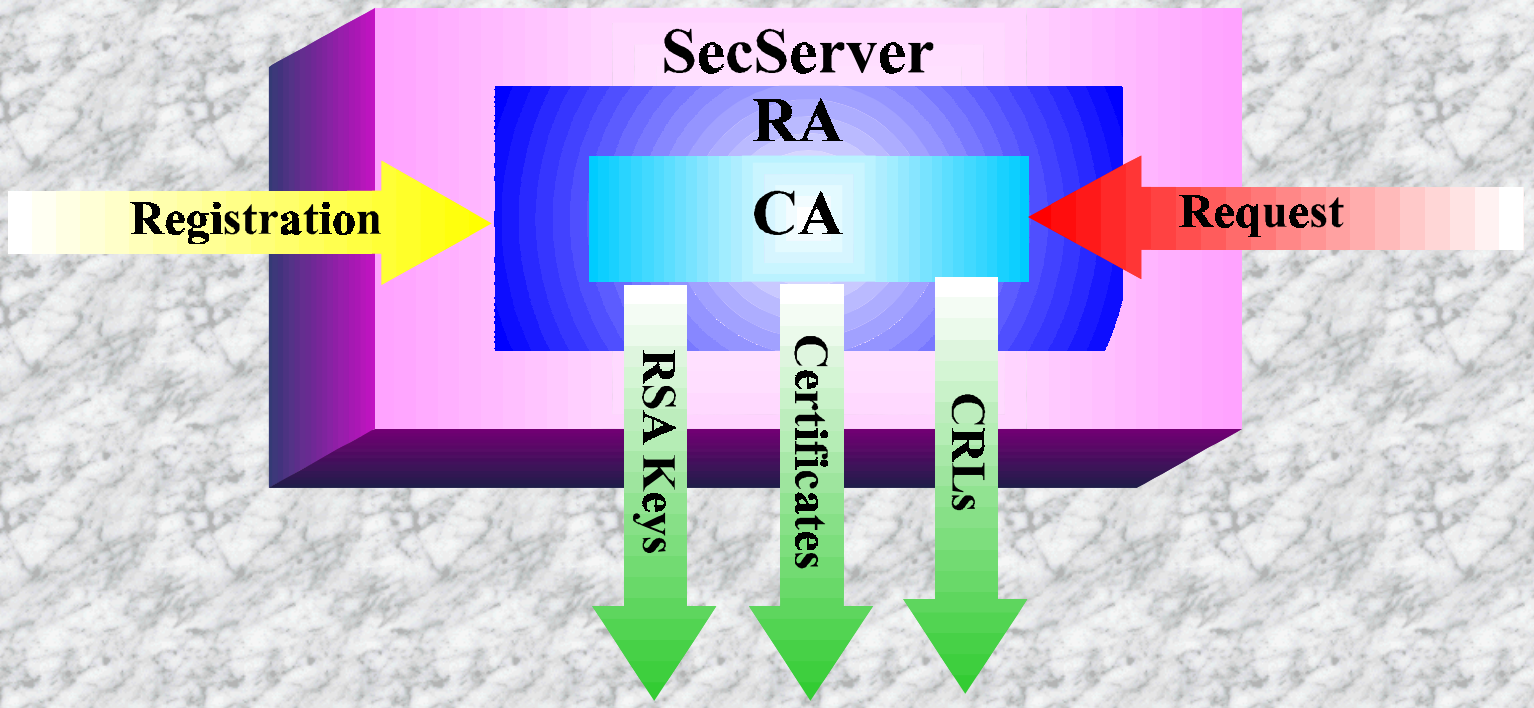
SecKit

- Generation of keys (DES, RSA)
- Sending of secure files

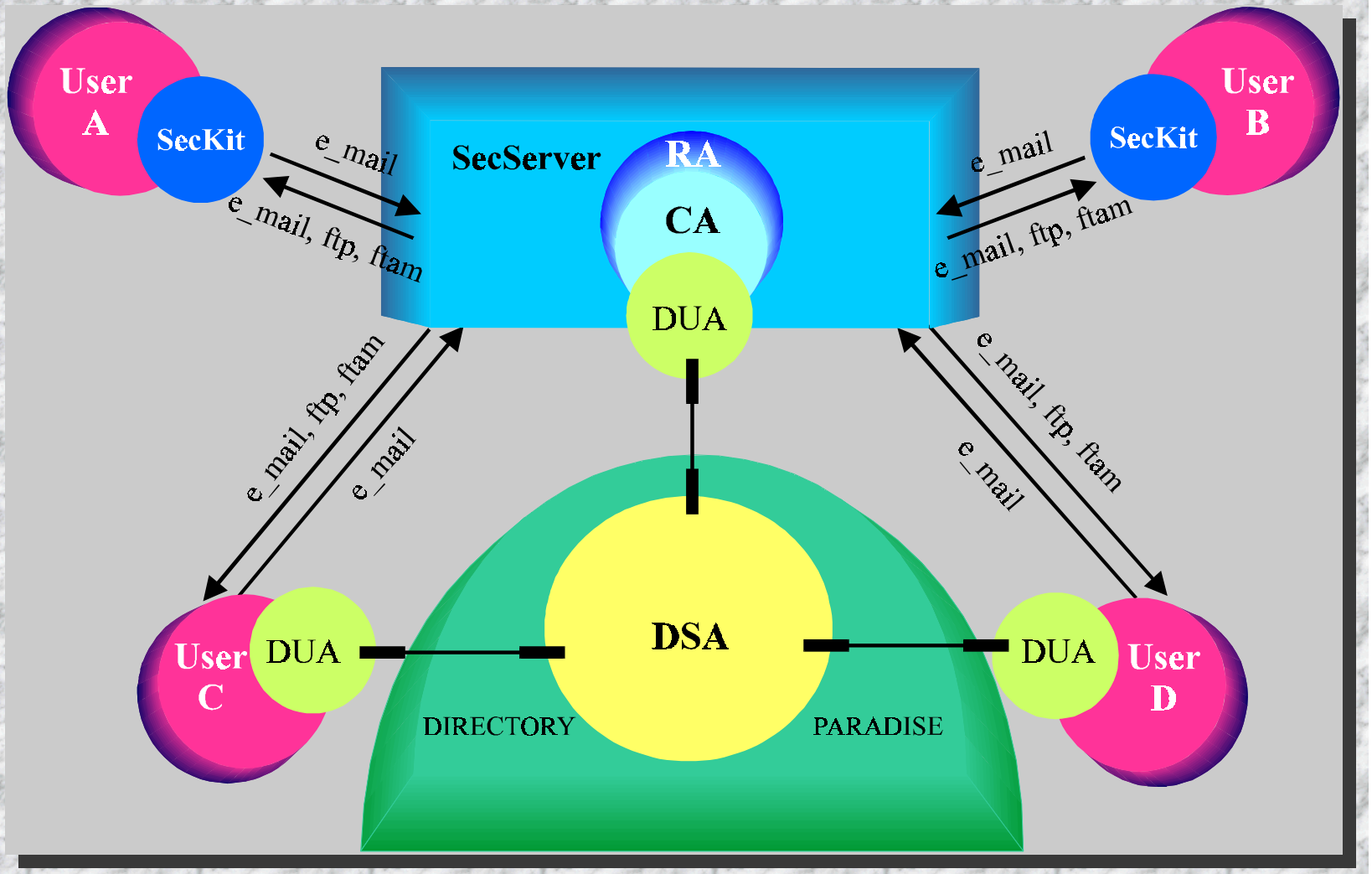


- Reception of secure files
- Access to the Directory

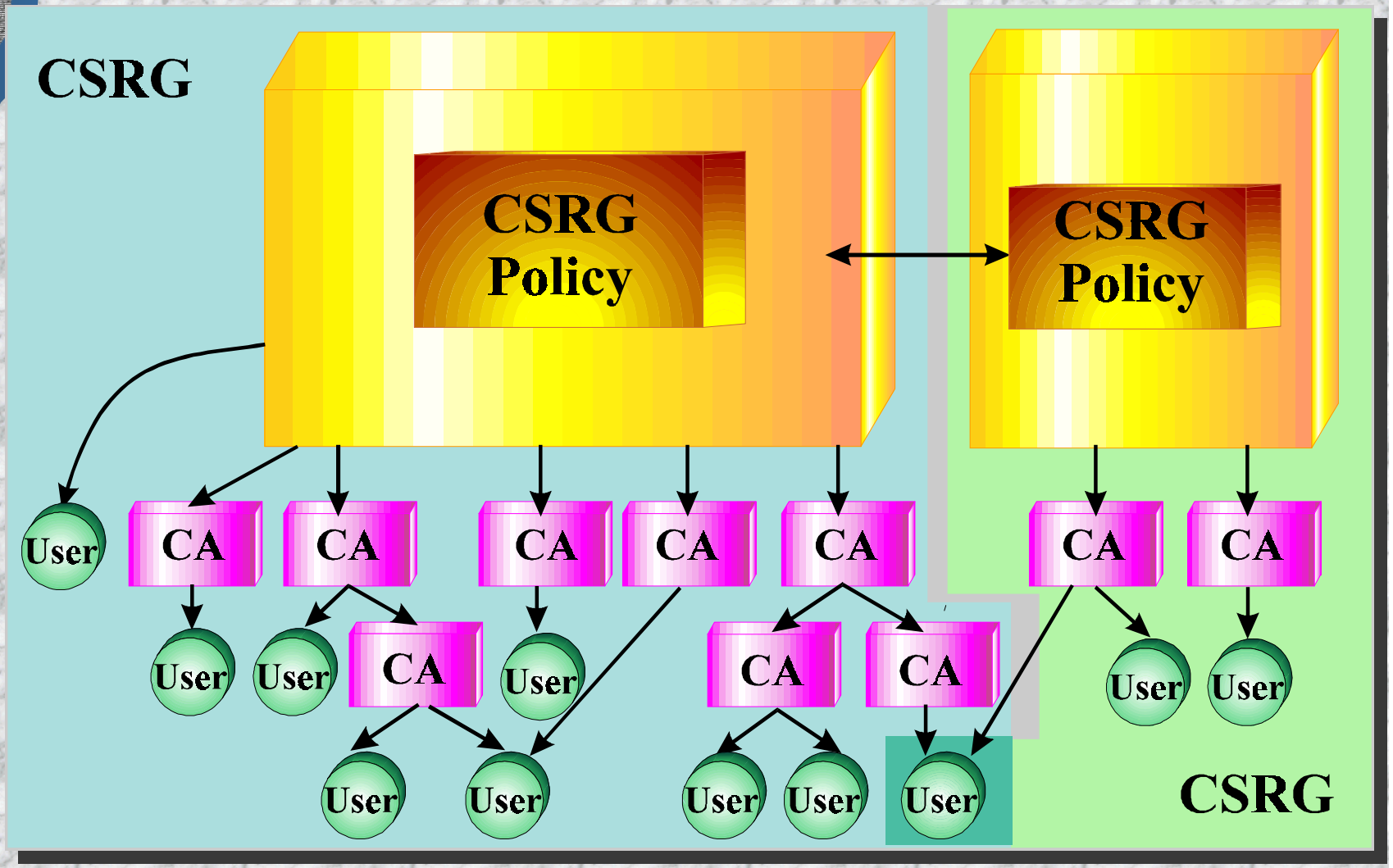
SecServer


SecServer
RA
CA
Registration
Request
RSA Keys
Certificates
CRLs

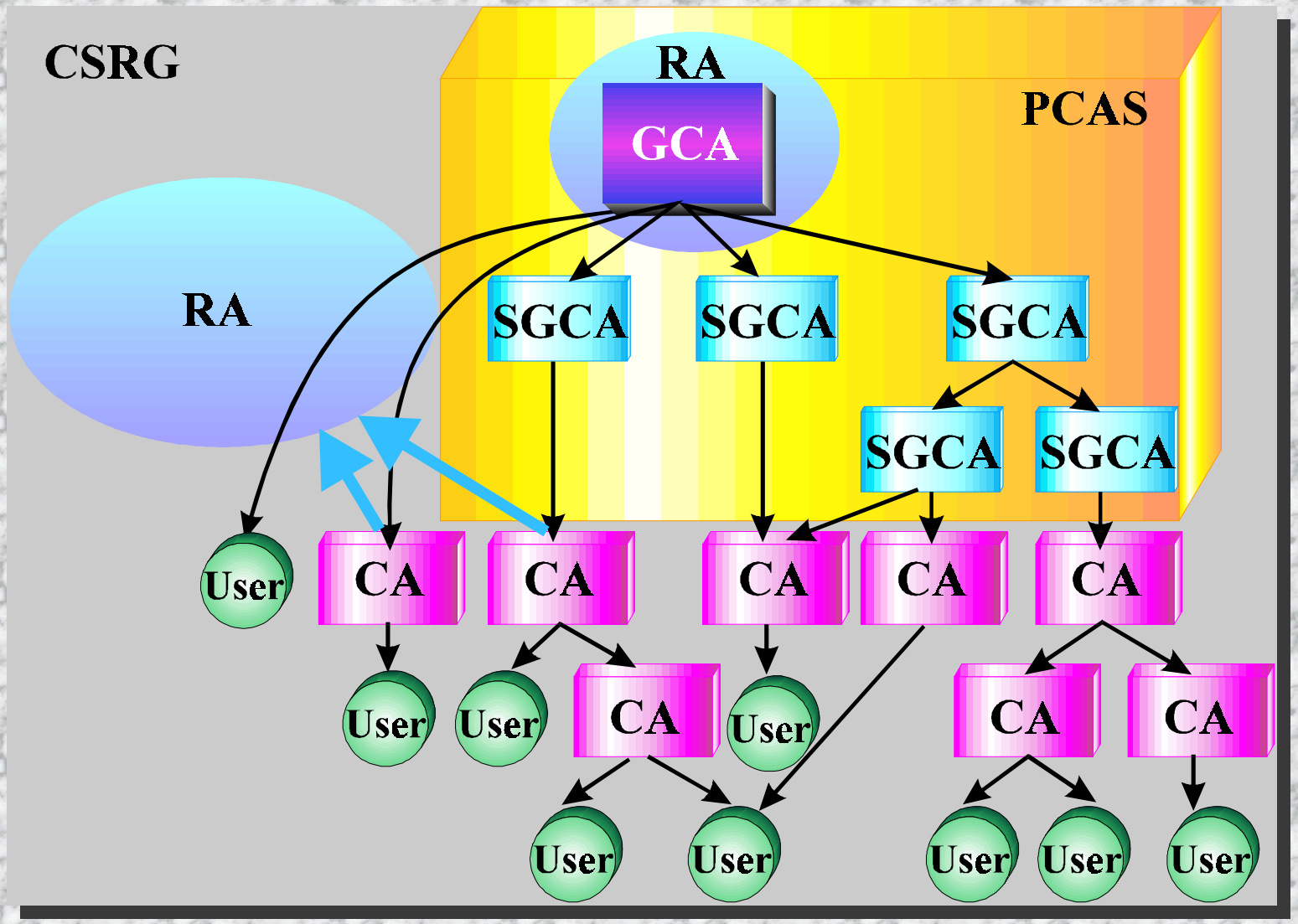
Pilot Environment



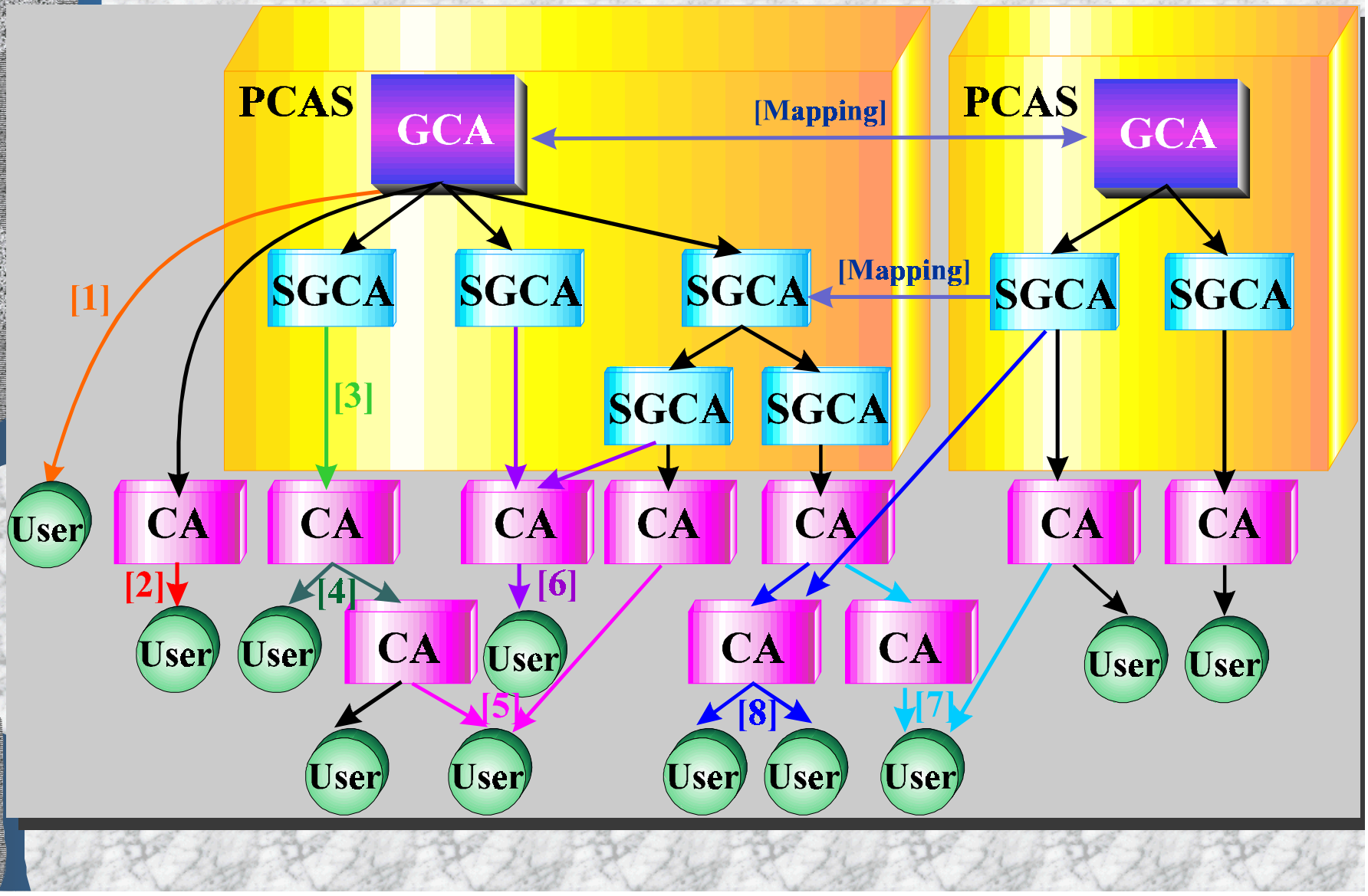
MODEL [1]


CSRG
CSRG Policy
CSRG Policy
User
CA
CA
CA
CA
CA
CA
CA
User
User
CA
User
CA
CA
User
User
User
User
User
User
CSRG

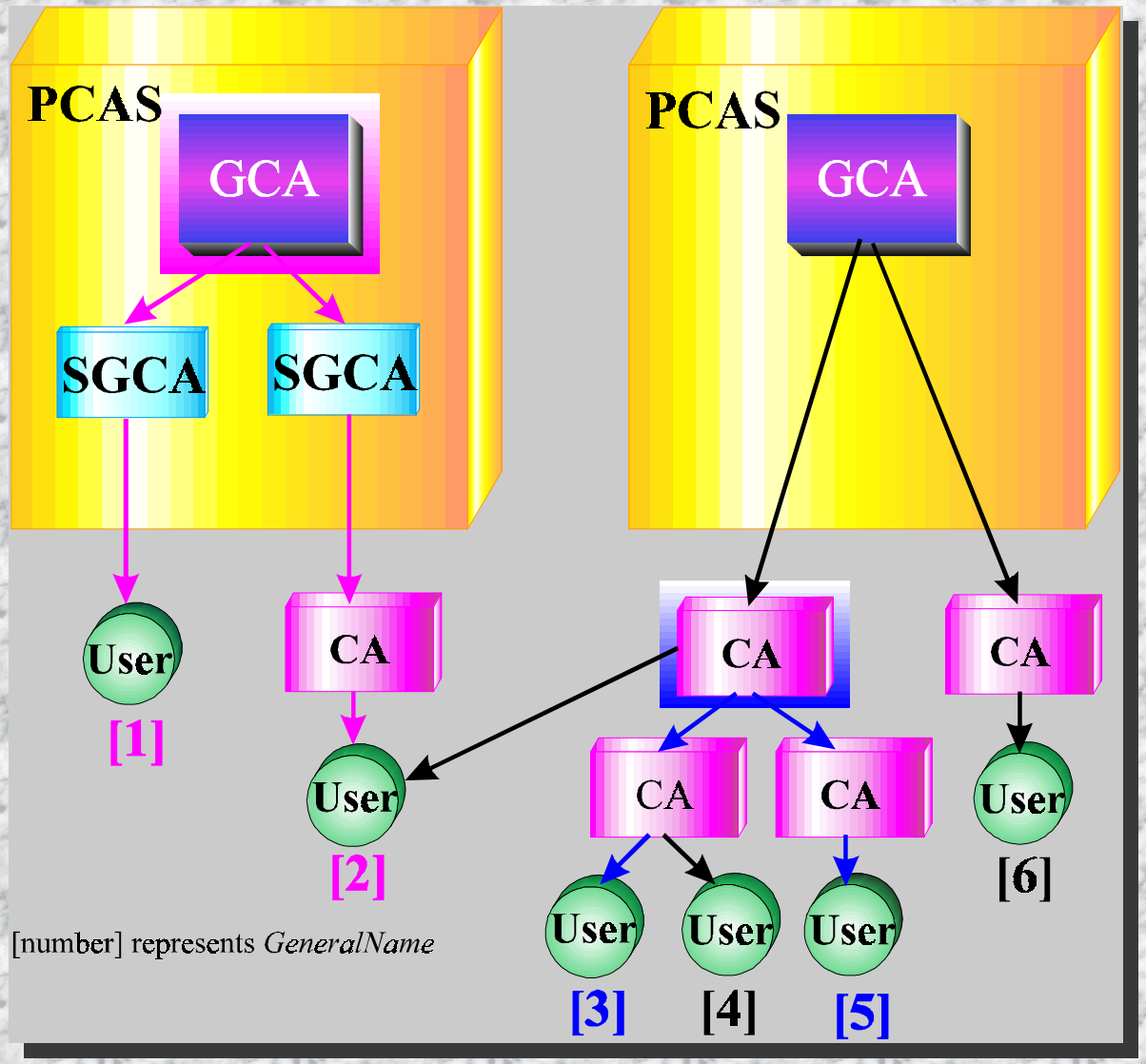
MODEL [2]


CSRG
RA
GCA
PCAS
RA
SGCA
SGCA
SGCA
SGCA
SGCA
User
CA
CA
CA
CA
CA
User
User
CA
User
CA
CA
User
User
User
User
User

MODEL [3]


PCAS
GCA
[Mapping]
PCAS
GCA
SGCA
SGCA
SGCA
[Mapping]
SGCA
SGCA
SGCA
SGCA
[1]
[3]
User
CA
CA
CA
CA
CA
CA
CA
[2]
[4]
[6]
User
User
CA
User
CA
CA
User
User
[5]
[8]
[7]
User
User
User
User
User

Certificate Path Validation [1]

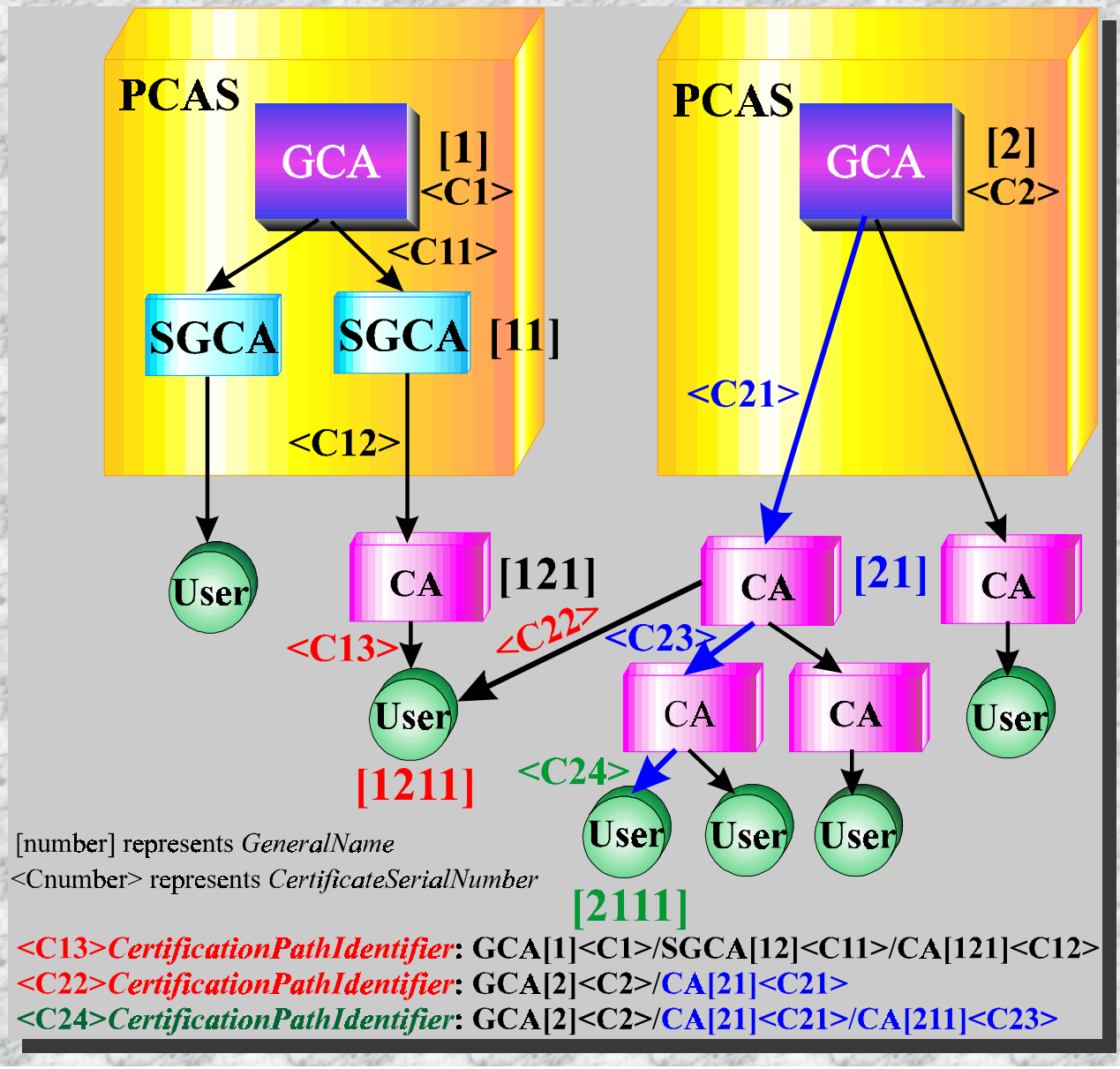


Certificate Path Validation [2]

```
CertificationPathIdentifier ::= SEQUENCE OF
NewAuthorityKeyIdentifier
NewAuthorityKeyIdentifier ::= SEQUENCE {
   autyType                    [0] CertificateType,
   autyKeyIdentifier           [1] KeyIdentifier   OPTIONAL,
   autyCertIssuer              [2] GeneralNames,
   autyCertSerialNumber        [3] CertificateSerialNumber}
CertificateType ::= BIT STRING {
   groupAuthority              (0),
   subgroupAuthority           (1),
   certificationAuthority      (2),
   user                        (3) }
```

```
NewSubjectKeyIdentifier ::= SEQUENCE {
subjectType       [0] CertificateType,
subjectKeyIdent   [1] KeyIdentifier OPTIONAL}
```

Certificate Path Validation [3]



Conclusions and Future Work

- Certificate v3 important step ahead
- Go to a general model
- Formal specification of the policy statements