

New open source CA development as Grid research platform.

National Research Grid Initiative in Japan

Takuto Okuno.

About NAREGI PKI Group (WP5)

WP4 :
Packaging

WP2 :
Grid
Programming
- Grid RPC
- Grid MPI

WP3 : Grid Visualization

WP3 : Grid PSE

WP3 : Grid Workflow

WP1 :
SuperScheduler

WP1 :
Grid Monitoring &
Accounting

(Globus, Condor, UNICORE → OGSA)

WP1 : Grid VM

WP5 :

High-Performance & Secure Grid Networking

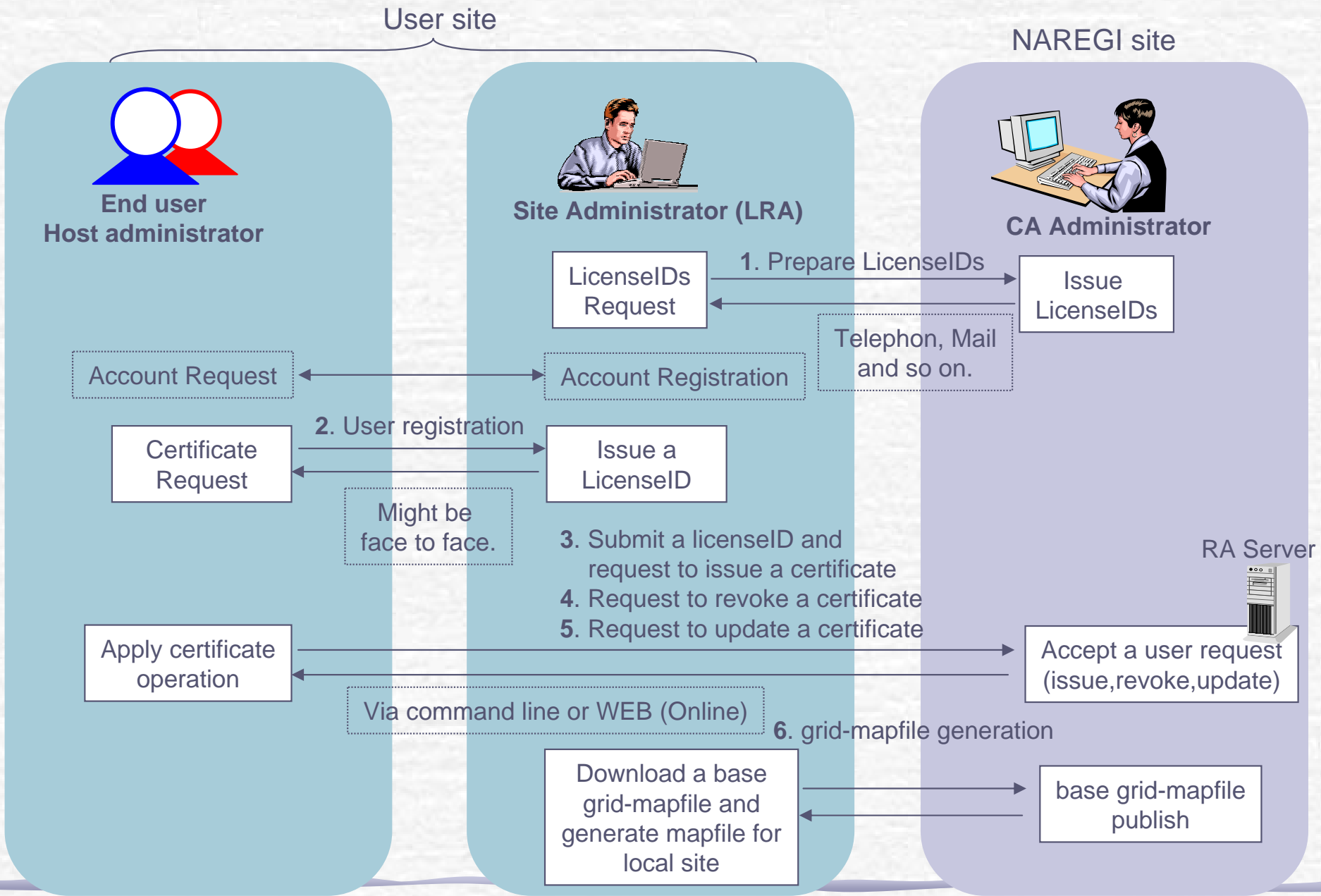
NAREGI Authentication Service Perspective

- To develop CA and RA server software that supports grid environment.
- To develop CA/RA policy and authentication service policy satisfied with basic assurance level by GGF.
- To experiment the operation of PKI authentication service (CA server software and CP/CPS) for UNICORE and Globus grid environment.
- To consider multi domain policy, and create an authentication mechanism for such environment.



It was necessary for developing new CA software to satisfy our functional and security requirement.

NAREGI Registration Sequence

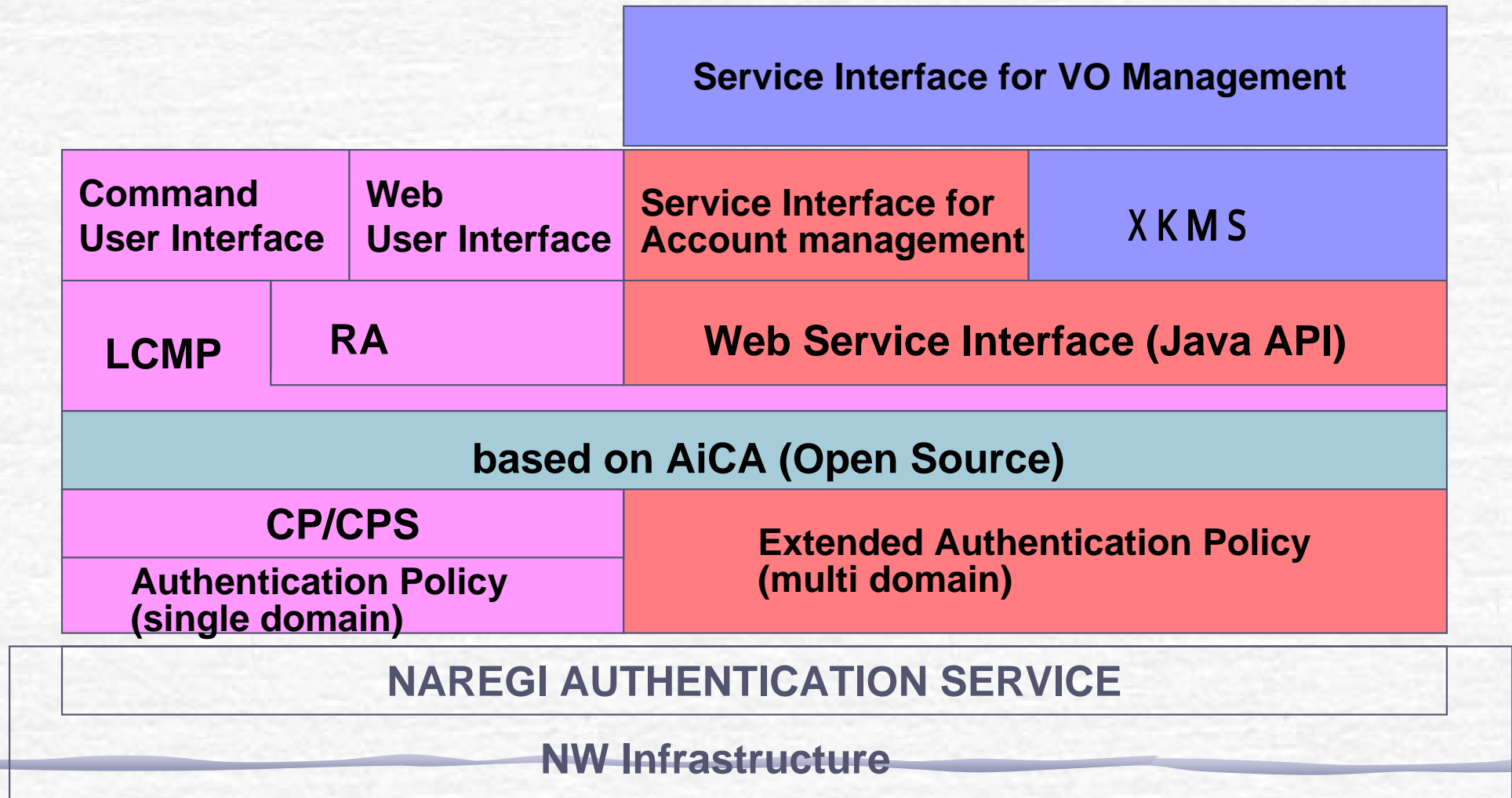


NAREGI CA – roadmap & function layer

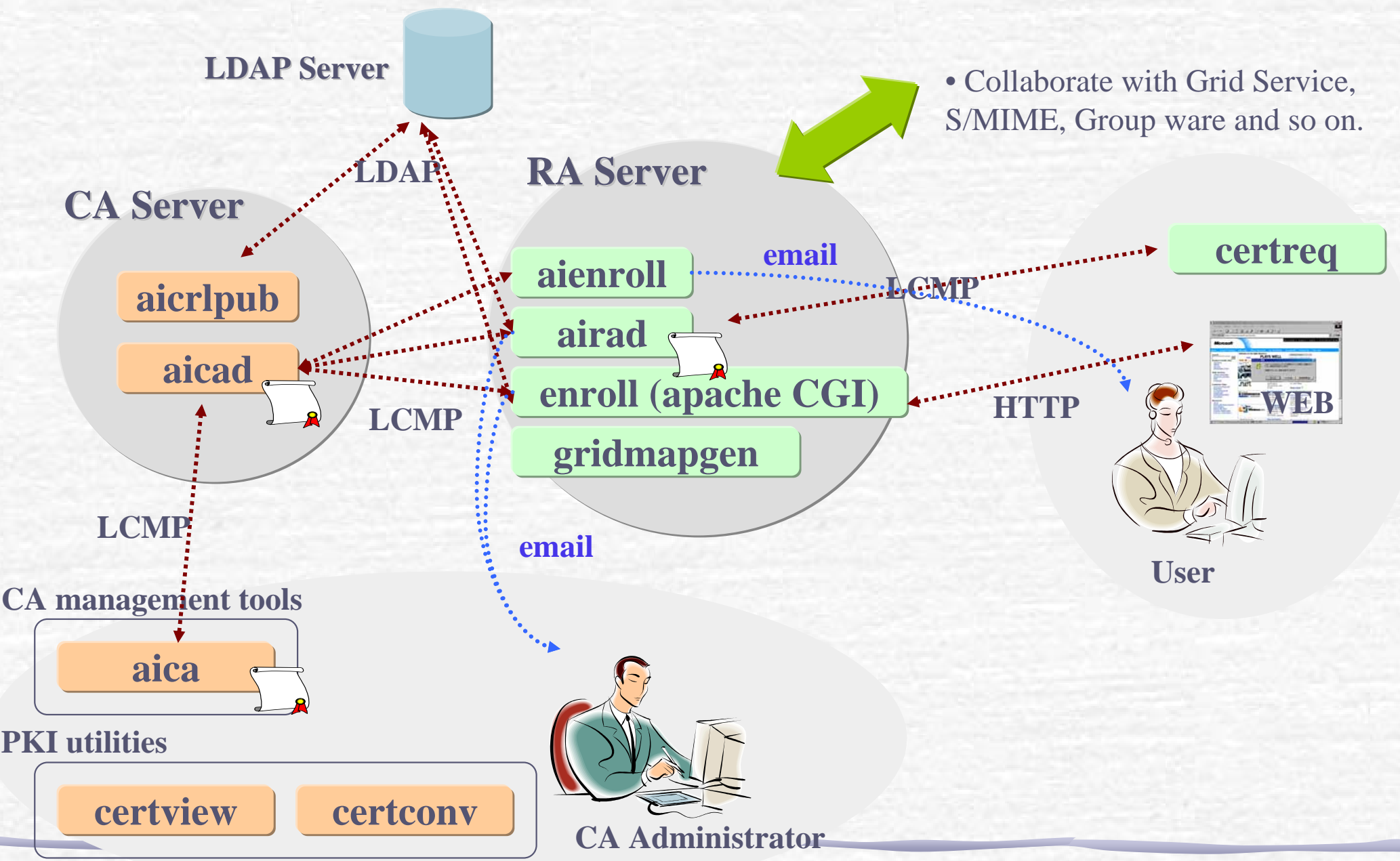
Development in 2003

in 2004 - 2005

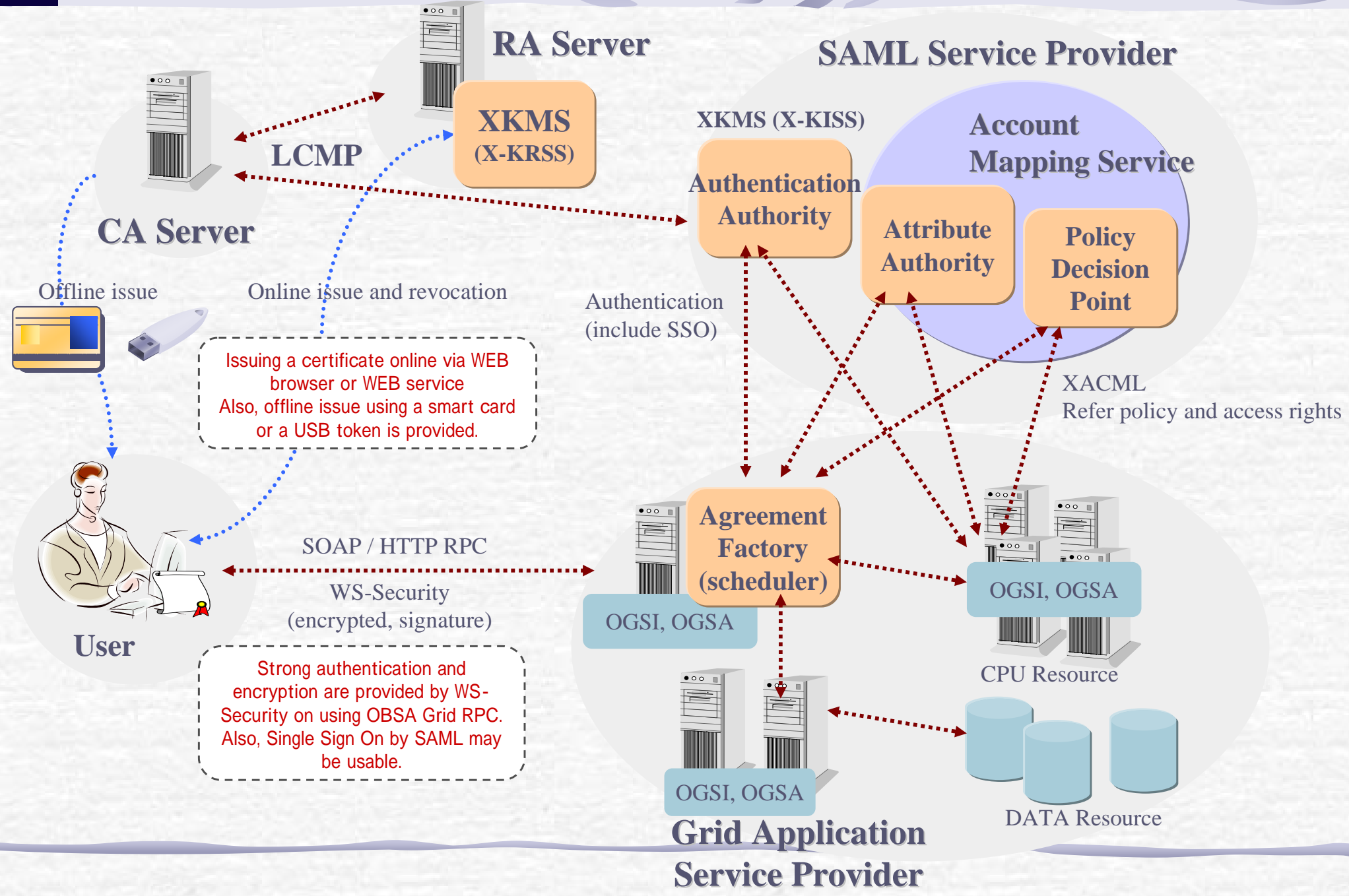
After 2005



NAREGI CA – server components



NAREGI CA – Secure grid web service perspective



NAREGI CA - CD contents

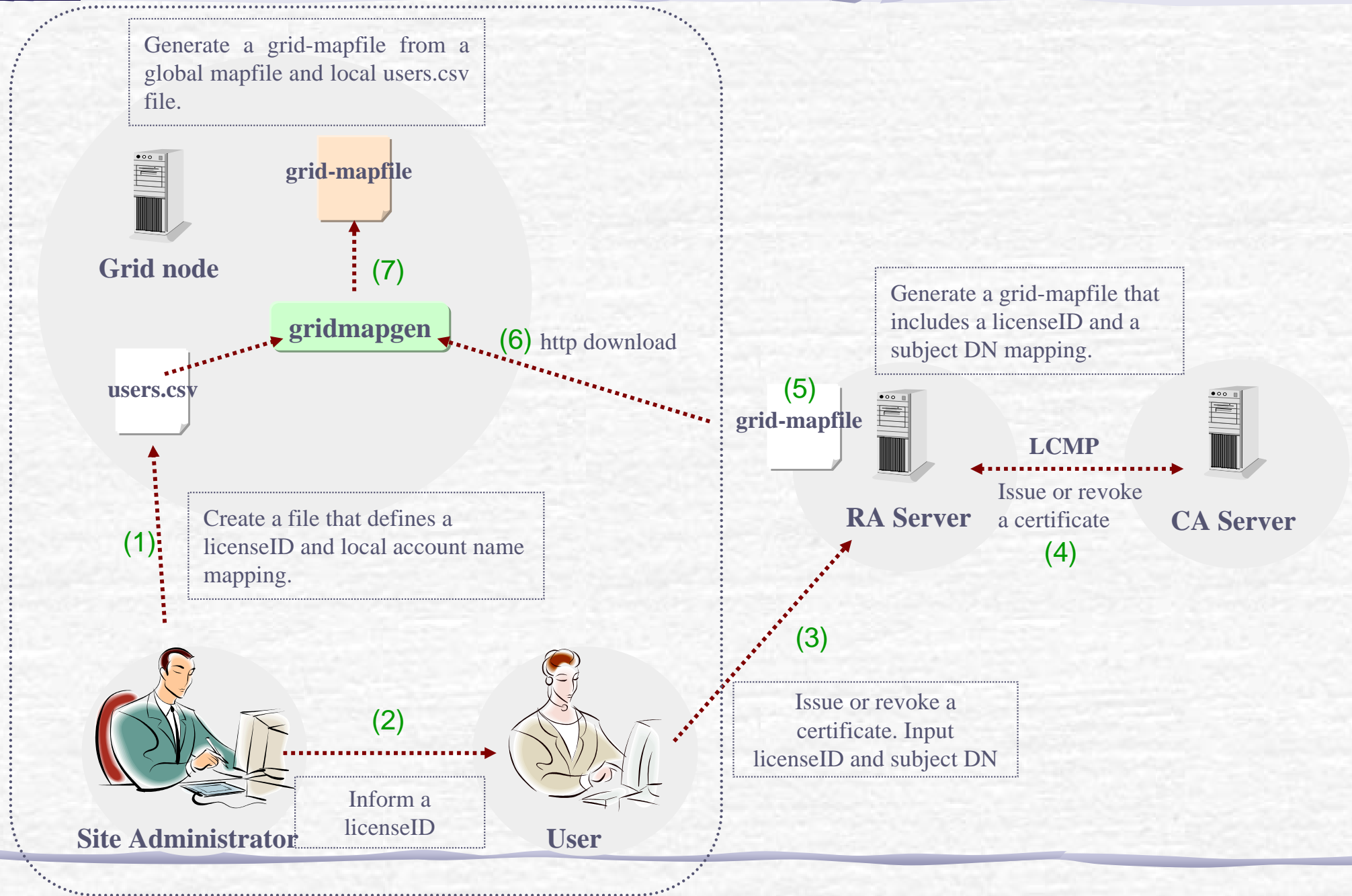
- **CD contents**
 - **README (Overview, install, etc..)**
 - **LICENSE**
 - **Release NOTE**
 - **naregi-ca-1.0.tar.gz**
 - **Source files**
 - **CP/CPS, Administrator Guide, etc..**
 - **naregi-project**
 - **naregi_pre.pdf (about NAREGI)**
 - **wp5_pre.pdf (about NAREGI Work Package 5)**

Appendix. File Formats

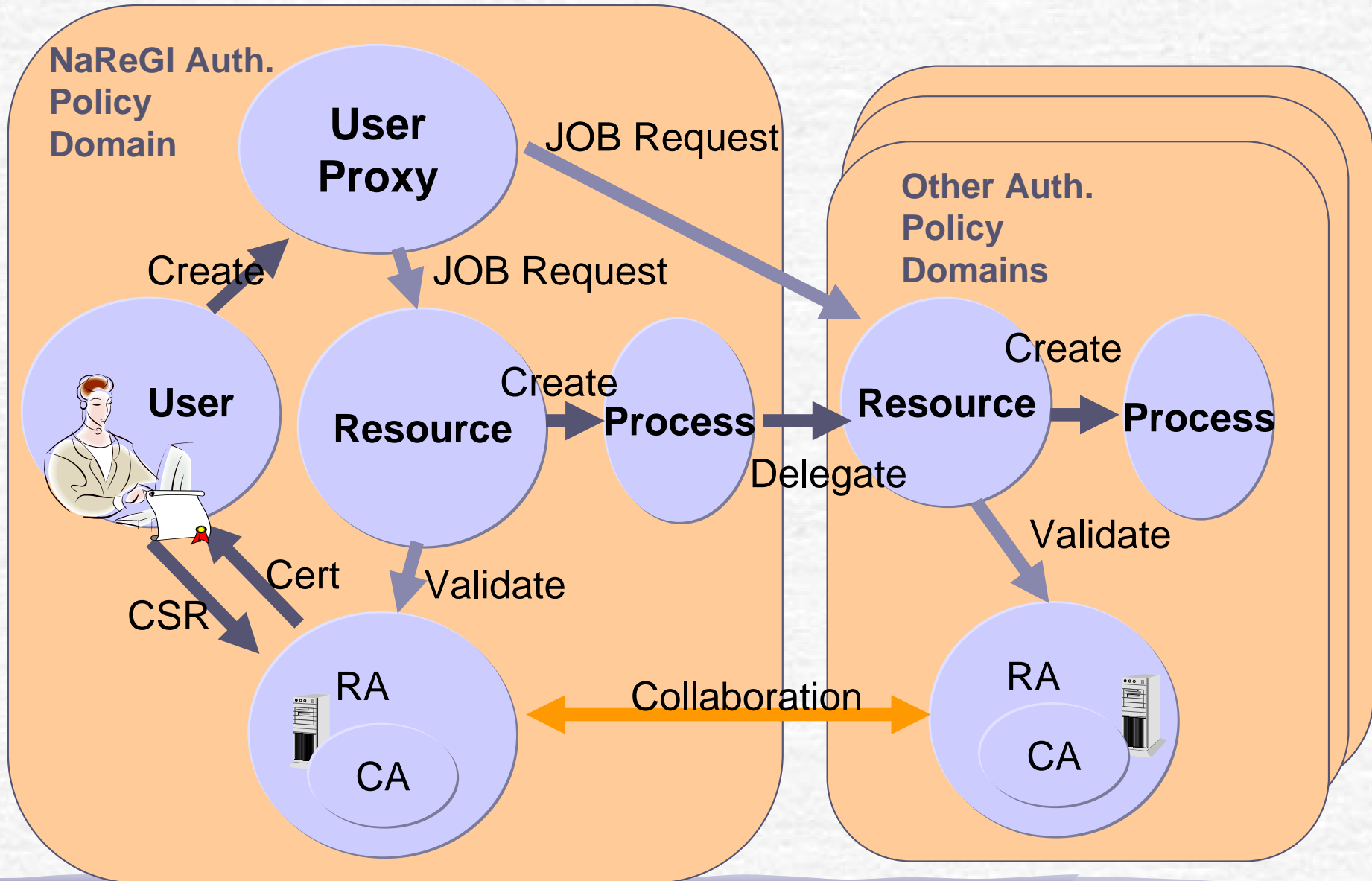
· Available PKI files

Certificate	X509 DER, PEM (*.cer,*.pem) PKCS#7 DER (*.p7b) PKCS#12 DER (*.p12, *.pfx)
Private Key	PKCS#1 PEM (*.key,*.pem) PKCS#8 DER (*.key,*.pem) PKCS#12 DER (*.p12, *.pfx)
CRL	X509 DER, PEM (*.crl,*.pem) PKCS#7 DER (*.p7b)
Cross certificate pair	X509 DER, PEM (*.ccp,*.pem)
Certificate Signing Request	PKCS#10 DER, PEM (*.crl,*.pem)

Appendix. grid-mapfile generation



Appendix. NAREGI Authentication Service



NAREGI CA – development roadmap

In 2003	In 2004	In 2005
<ul style="list-style-type: none"> ●LCMP protocol definition ●NAREGI CA development ●Start trial CA operation 	<ul style="list-style-type: none"> ●Optimize performance (10k certificates/h) ●LCMP Java API ●Service Interface for account management 	<ul style="list-style-type: none"> ●XKMS ●Feedback / improve server operation