Standards and Frameworks

Christos Kanellopoulos

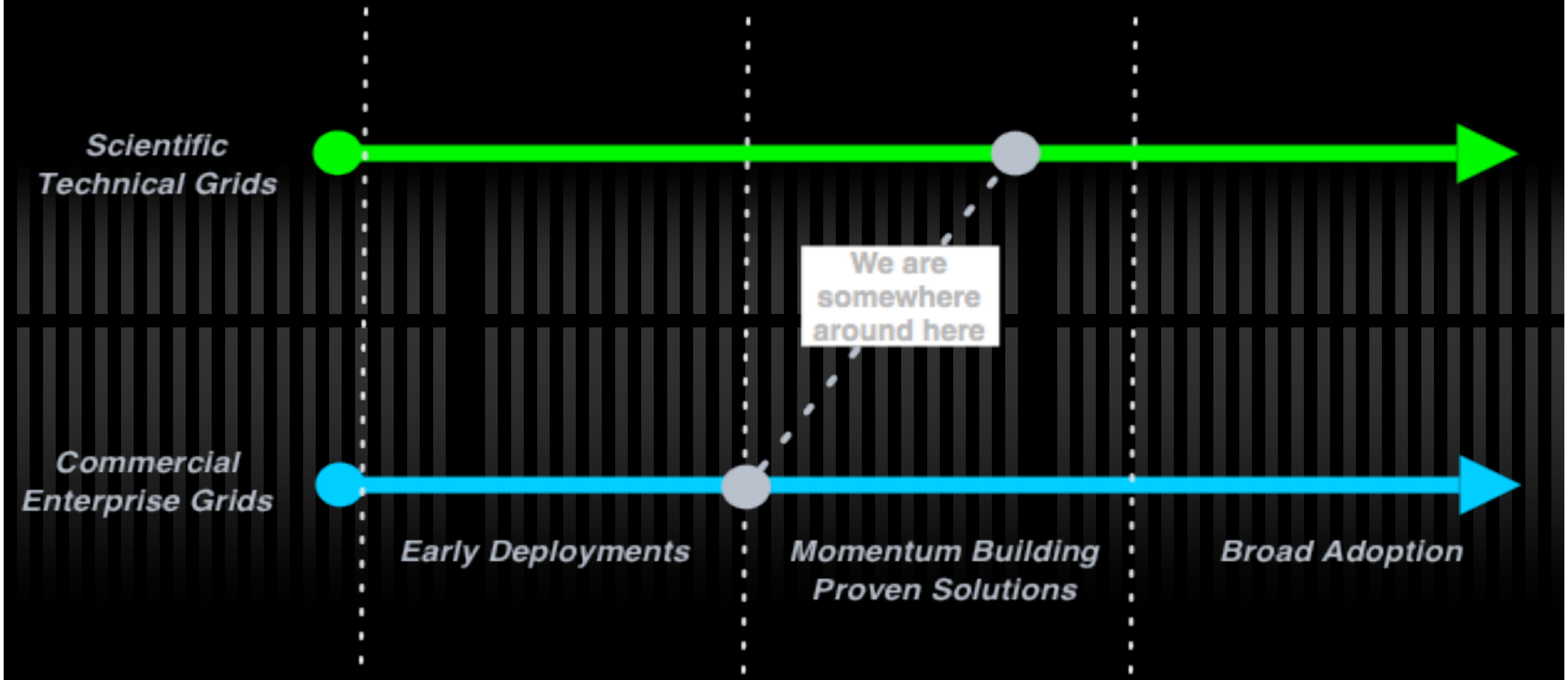
GGF CAOPS WG Co-chair

EGEE Workshop on Management of Rights in Production Grids

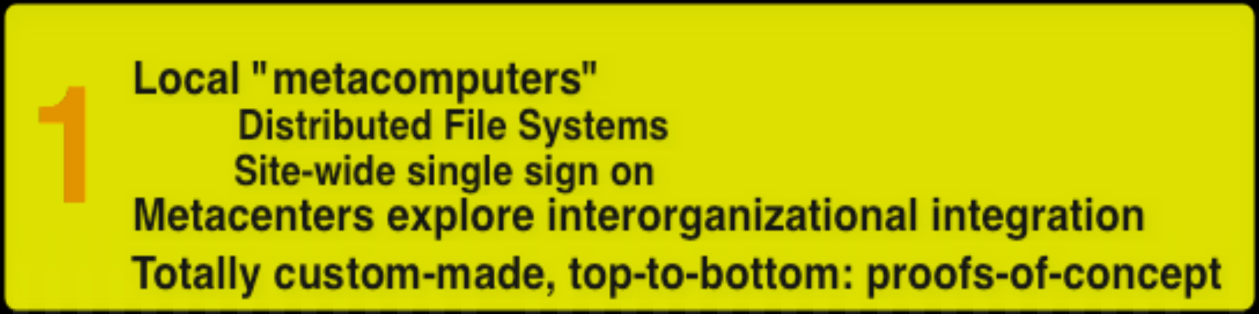
Outline

- ✓ Where we stand today
- ✓ Essentials in Grid Security
- ✓ Federated Grid Authentication
- ✓ OGSA AuthZ Model

Where we stand today


Scientific Technical Grids
Commercial Enterprise Grids
We are somewhere around here
Early Deployments
Momentum Building Proven Solutions
Broad Adoption

Three Generation of Grids



1

Local "metacomputers"

Distributed File Systems

Site-wide single sign on

Metacenters explore interorganizational integration

Totally custom-made, top-to-bottom: proofs-of-concept

Three Generations of Grids

1

Local "metacomputers"

Distributed File Systems

Site-wide single sign on

Metacenters explore interorganizational integration

To [illegible]

2

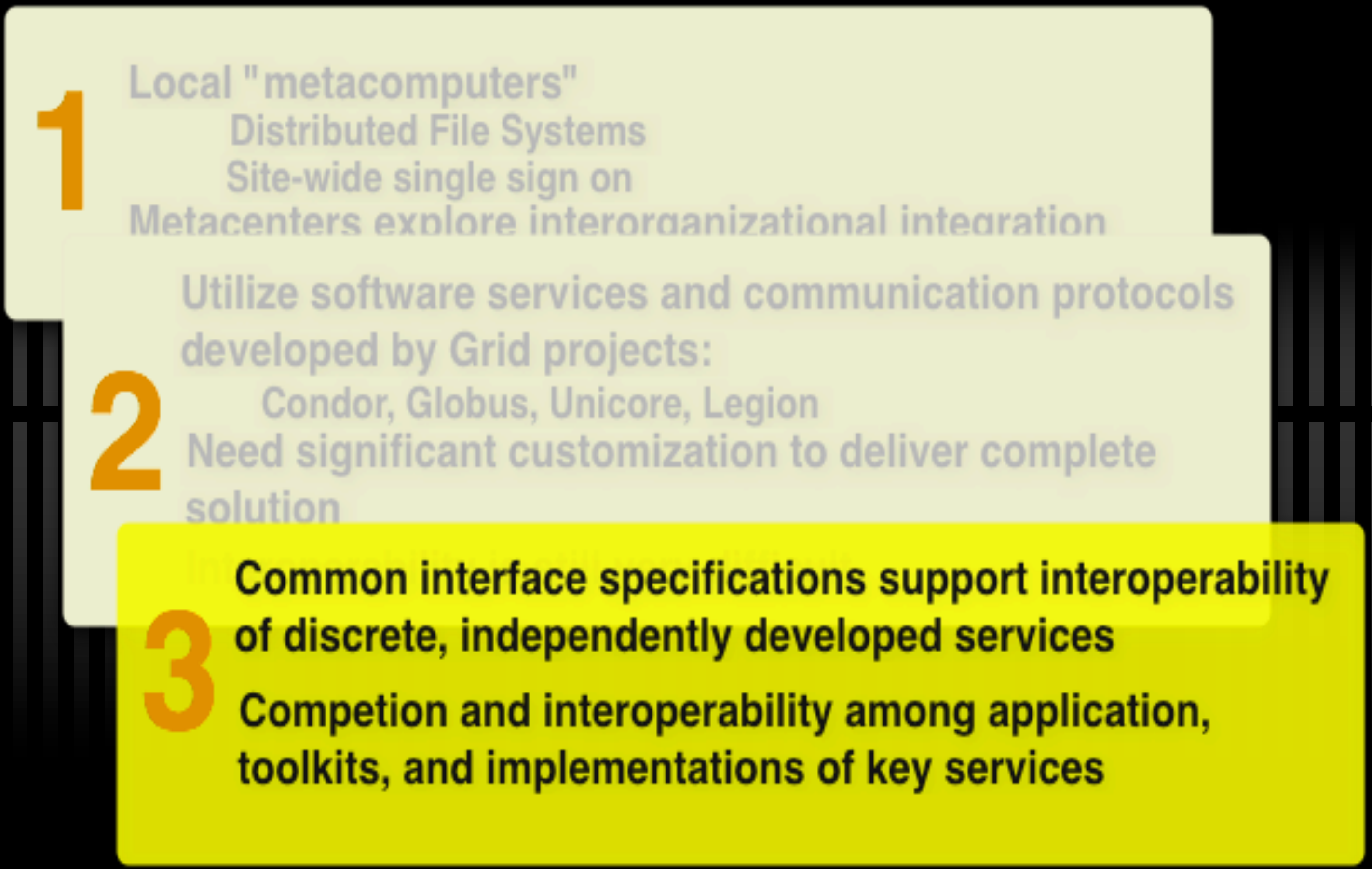
Utilize software services and communication protocols developed by Grid projects:

Condor, Globus, Unicore, Legion

Need significant customization to deliver complete solution

Interoperability is still very difficult

Three Generations of Grid



1

Local "metacomputers"

Distributed File Systems

Site-wide single sign on

Metacenters explore interorganizational integration

2

Utilize software services and communication protocols developed by Grid projects:

Condor, Globus, Unicore, Legion

Need significant customization to deliver complete solution

Interoperability is still very difficult

3

Common interface specifications support interoperability of discrete, independently developed services

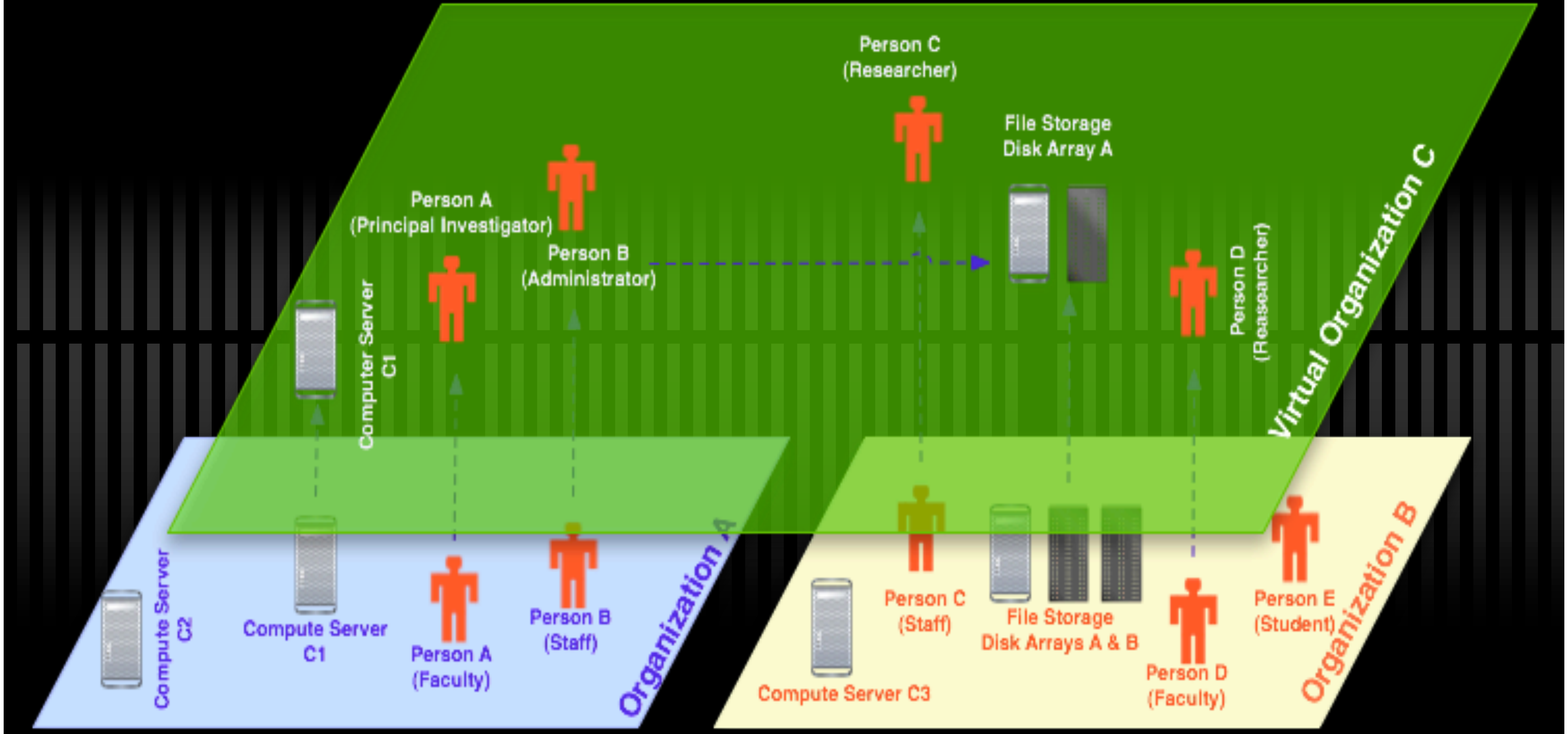
Competion and interoperability among application, toolkits, and implementations of key services

Standardization is key for 3rd Generation Grids

Essentials

- ✓ Access to shared resources
  - ✓ Cross domain authentication, authorization, accounting billing
  - ✓ Common generic protocols for collective services
- ✓ Support multi user collaborations
  - ✓ Organized in Virtual Organizations
  - ✓ International Grid Trust Federation
- ✓ Easy Single Sign On
- ✓ Resource owners must always be in control

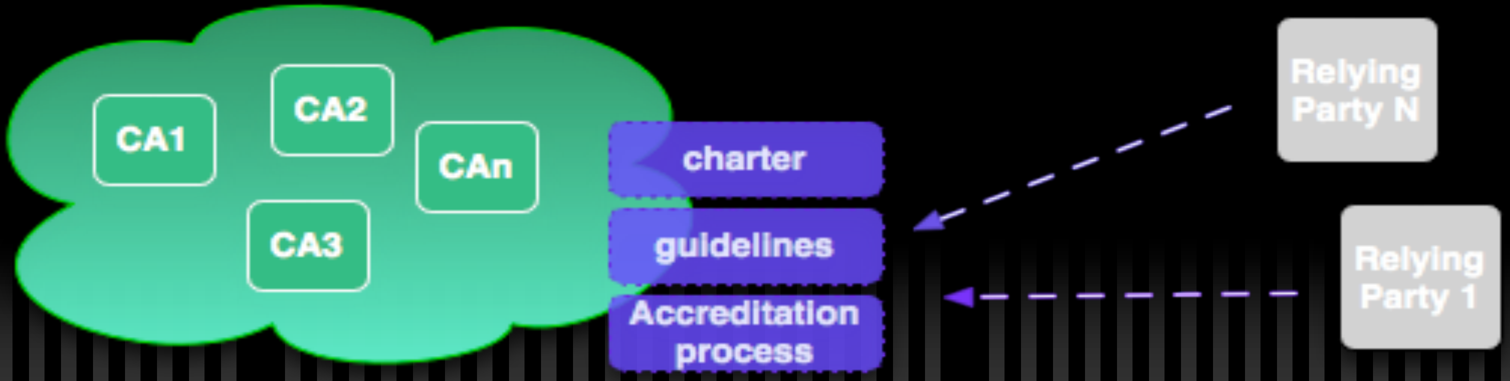
Virtual vs Organic



AuthN vs AuthZ

- ✓ Single Authentication Token («Passport»)
  - ✓ Issued by a trusted IdP
  - ✓ Recognised by many RPs, Users and Vos
  - ✓ Persistant & traceable
- ✓ Per VO Authorizations
  - ✓ Granted to a person - service via a VO
  - ✓ Based on the «passport» name
  - ✓ Provides provide access to VO, but still can deny access to individual users

Federation Model for Grid Authentication



- ✓ A Federation of many independent Cas
  - ✓ Common minimum requirements
  - ✓ Trust domain as required by users and relying parties
- ✓ No single hierarchy with a single top
  - ✓ Spread for reliability and failure containtment
  - ✓ Maximum leverage of national efforts

Building the Federation

- ✓ Identity Providers ('CAs') and Relying Parties ('sites') together shape the common requirements
  - ✓ Several profiles for different identity management models
  - ✓ Authorities testify to comply with profile guidelines
  - ✓ Peer review process within the Federation to (re)evaluate members on entry & periodically
  - ✓ Reduce efforts on the Relying Parties
  - ✓ Single document to review and assess for all CAs
  - ✓ Reduce cost on Identity Providers
  - ✓ No audit statement needed by certified accountants
  - ✓ But participation in the Federation comes with a price
  - ✓ Requires that the Federation remains manageable in size

International Grid Trust Federation

TAGPMA
eu gridpma

Profile: Secured X509 CAs

- ✓ RFC 3280 and 3820 Certificates:
  - ✓ Client - Server authentication
  - ✓ Single Sign On
  - ✓ Credential Delegation
  - ✓ SSL/TLS communications
- ✓ One single CA per country, large region or international treaty organization
- ✓ Users have to perform face to face identification with an RA

New things coming in…

- ✓ OCSP
- ✓ 1SCP
- ✓ Audits
- ✓ Long Lived Credential Services?

But….

- ✓ Users do not understand certificates
  - ✓ They are used to the standard username and password mechanism
- ✓ Many organizations have existing directories in place

Profile: Short Lived Credential Services

- ✓ Users authenticate by tranditional means to their directory
- ✓ The retrieve short lived grid proxies in order to be able to access Grid enabled services

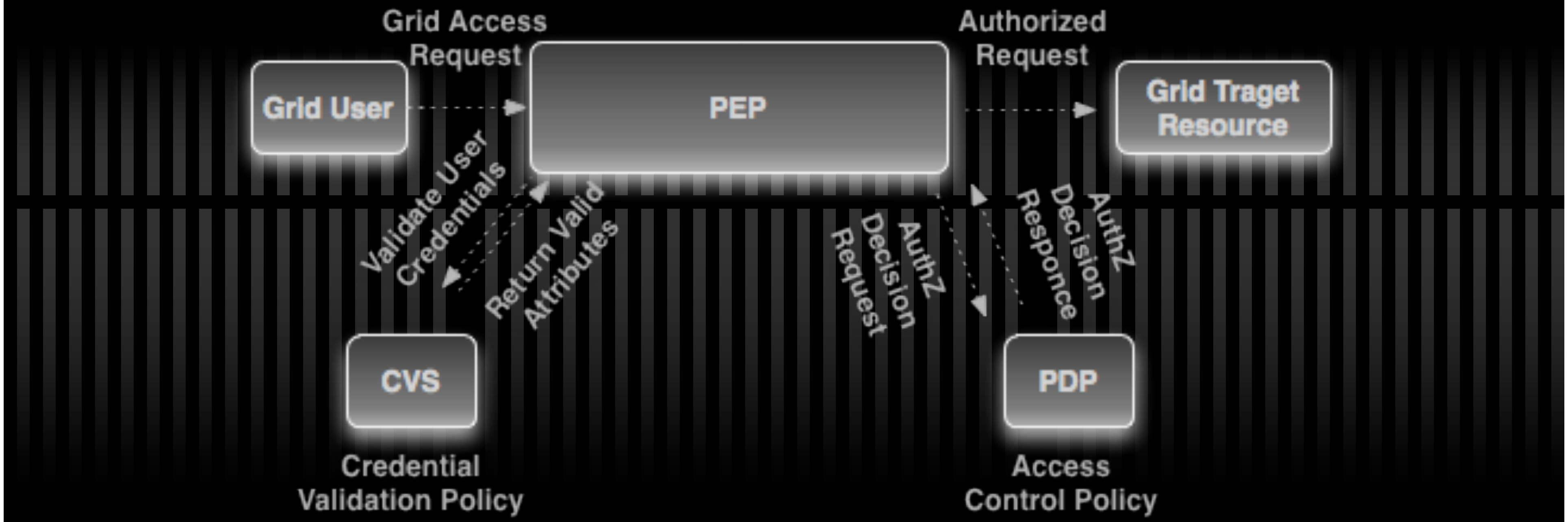
The rise of SAML

- ✓ There is no SAML vs PKI war
  - ✓ Two coplimentary technologies
  - ✓ One is not replacement of the other
- ✓ Many crossover efforts under way
  - ✓ GridShib, ShibGrid, SHEBANGS, GridShibPermis, MAMS, EGEE, BRIDGES, VOTES
  - ✓ inCommon and TAGPMA have discussed common requirements / authentication profile

Grid Authorization

- Key Elements
  - Grid User
  - Attribute Authority
  - Grid Resource
- Push Model:
  - The Grid User passes it’s credential to the Grid Resource
- Pull Model
  - The Resource fetches the user’s credential from the AA

OGSA Authorization Group



The request is a set of SAML attribute assertions embeded in a WS-Trust request protocol message

CVS, STS and PIP

- ✓ WS-Trust enables security token interoperability by defining a request/response SOAP protocol whereby clients can request from some trusted authority that a particular security token be exchanged for another one
- ✓ The security token service (STS) is the trusted authority that responds to WS-Trust requests.

CVS, STS and PIP

- ✓ STS Functionalities
  - ✓ Security token exchange
  - ✓ Security token issuing
  - ✓ Security token validation
- ✓ CVS Corresponds to the validation functionality of the STS

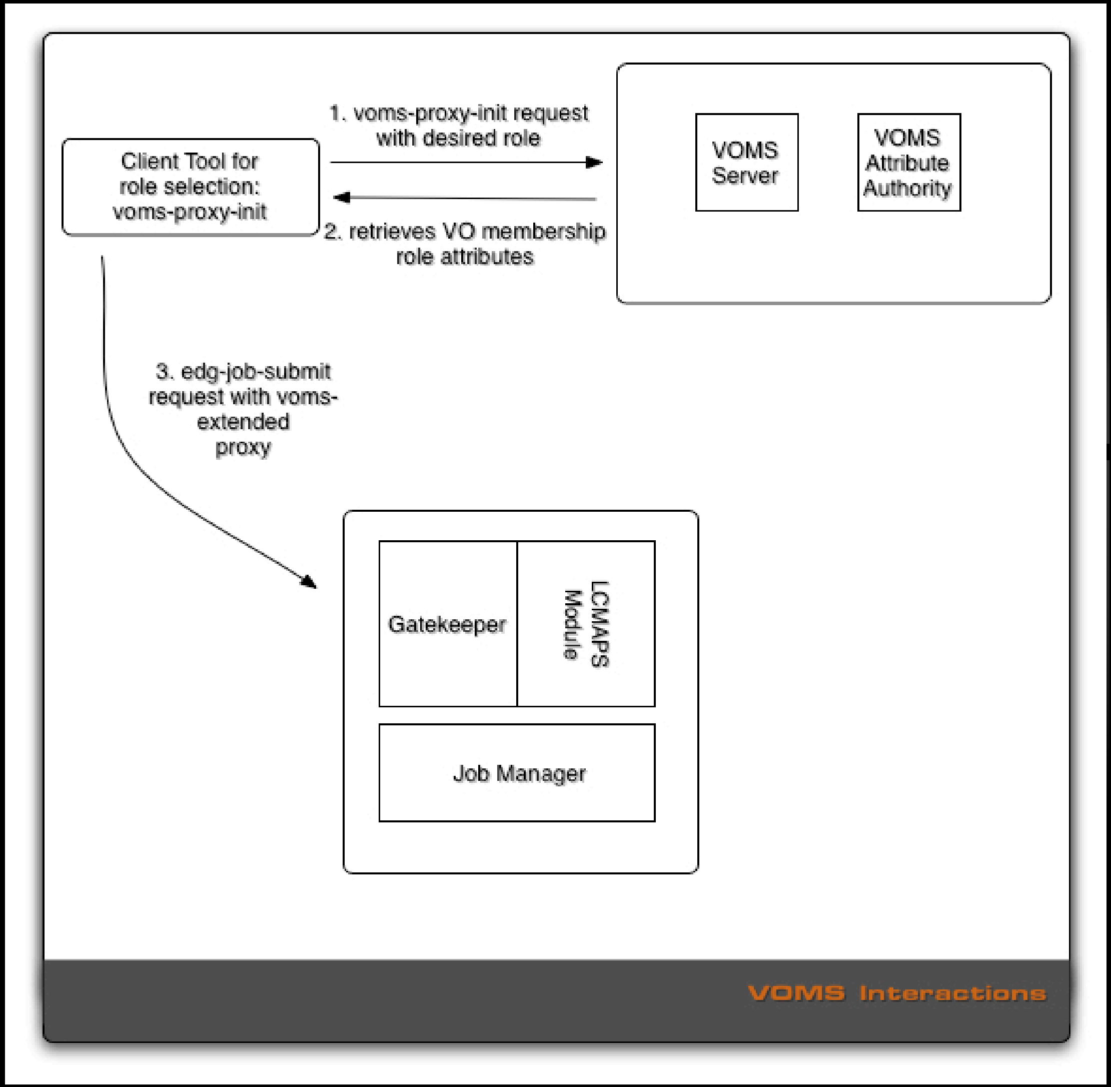
CVS, STS and PIP

- ✓ Policy Information Point (PIP) is the system entity that acts as a source of attribute values.
- ✓ CVS is a specialized type of PIP that can process credentials and/or security tokens according to a credential validation policy, and that can return valid attributes in exchange for the input credentials.

Virtual Organization Membership Service

- ✓ Maintains a database of members and members roles for a specific
- ✓ Uses Attribute Certificates (RFC 3281)
- ✓ Follows the Push Model:
  - ✓ User generates a voms proxy and passes it to the Resource
- ✓ The VOMS proxy attribute certificate format hass been submitted to GGF

VOMS Interactions

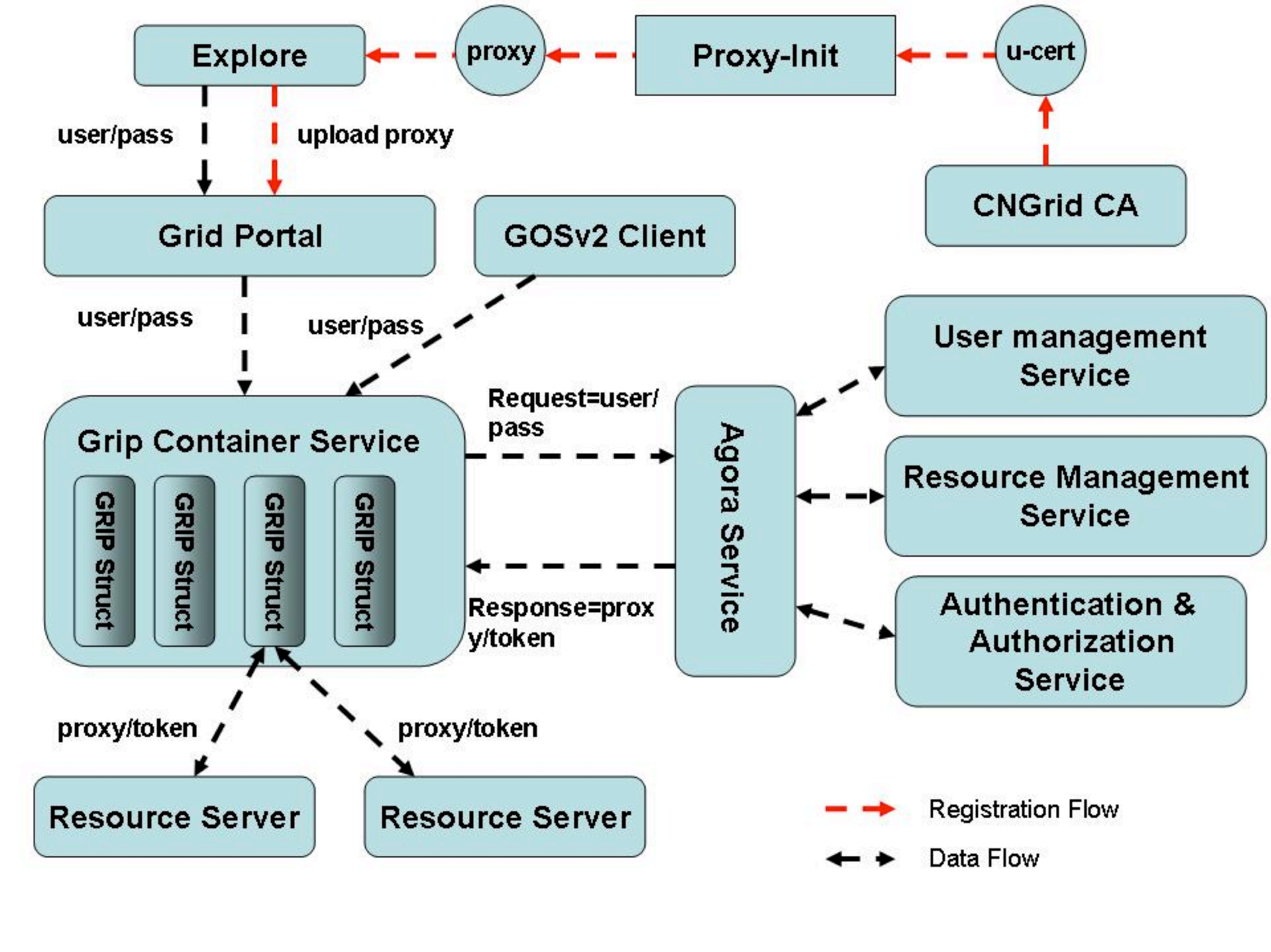


1. voms-proxy-init request with desired role
Client Tool for role selection: voms-proxy-init
VOMS Server
VOMS Attribute Authority
2. retrieves VO membership role attributes
3. edg-job-submit request with voms-extended proxy
Gatekeeper
LCMAPS Module
Job Manager
VOMS Interactions

Vega GOSv2 & GridShield

- ✓ Employed in CNGrid
- ✓ Uses the Agora Service as the front-end for the user management service, the resource management service and the authentication - authorization service.

Vega GOSv2 Interactions



The OSG Priviledge project

- ✓ See Gabriele’s presentation

Grid Interoperation Now (GIN)

- ✓ Effort between 18 production Grids to showcase interoperation (not interoperability)
- ✓ Several different middlewares
- ✓ IGTF CAs used for authentication
- ✓ VOMS used for authorization

Final Thoughts

- ✓ More Authentication Service Profiles start to appear (tendency to go to username, password scheme)
- ✓ PKI tends to get hidden into the middleware.
- ✓ Opens the door for SAML based implementions to interoperate with existing ones
- ✓ Credential Translation Services can provide such bridging