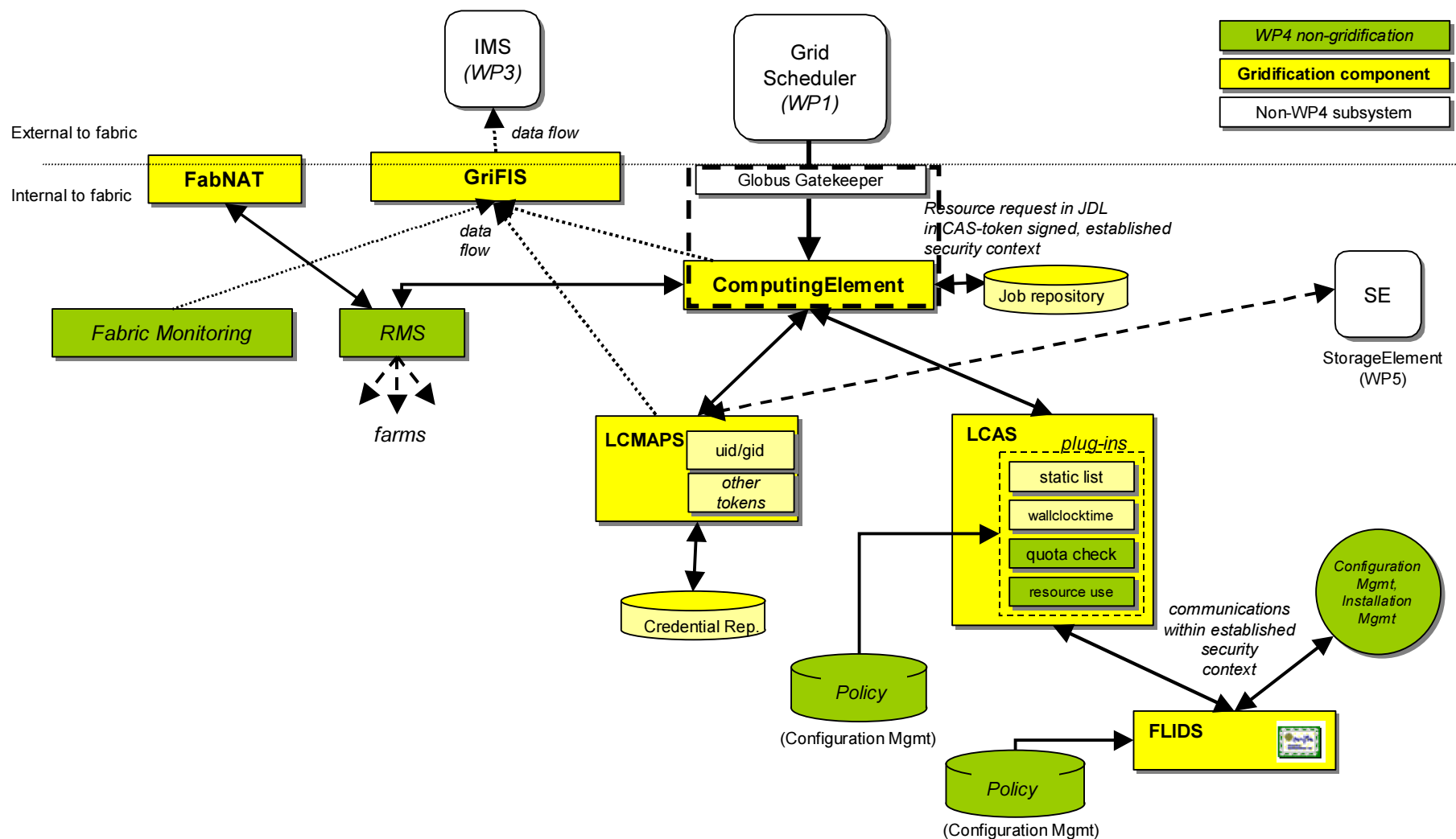# WP4 Gridification

Subsystem overlap & existing systems

for Gridification Task: David Groep

hep-proj-grid-fabric-gridify@cern.ch

WP4 Subsystems and relationships (D4.2)

IMS
(WP3)

Grid
Scheduler
(WP1)

WP4 non-gridification

Gridification component

Non-WP4 subsystem

External to fabric

data flow

Internal to fabric

FabNAT

GriFIS

Globus Gatekeeper

*Resource request in JDL
in CAS-token signed, established
security context*

*data
flow*

Fabric Monitoring

RMS

ComputingElement

Job repository

SE

StorageElement
(WP5)

farms

LCMAPS

uid/gid

*other
tokens*

LCAS

plug-ins

static list

wallclocktime

quota check

resource use

*communications
within established
security
context*

*Configuration
Mgmt,
Installation
Mgmt*

Credential Rep.

Policy

(Configuration Mgmt)

FLIDS

Policy

(Configuration Mgmt)

Job submission protocol & interface

- ◆ Current Globus design
  - ▪ Client tools connect to gatekeeper
  - ▪ GRAM (attributes over HTTPS)
  - ▪ Gatekeeper does authentication, authorization *and* user mapping
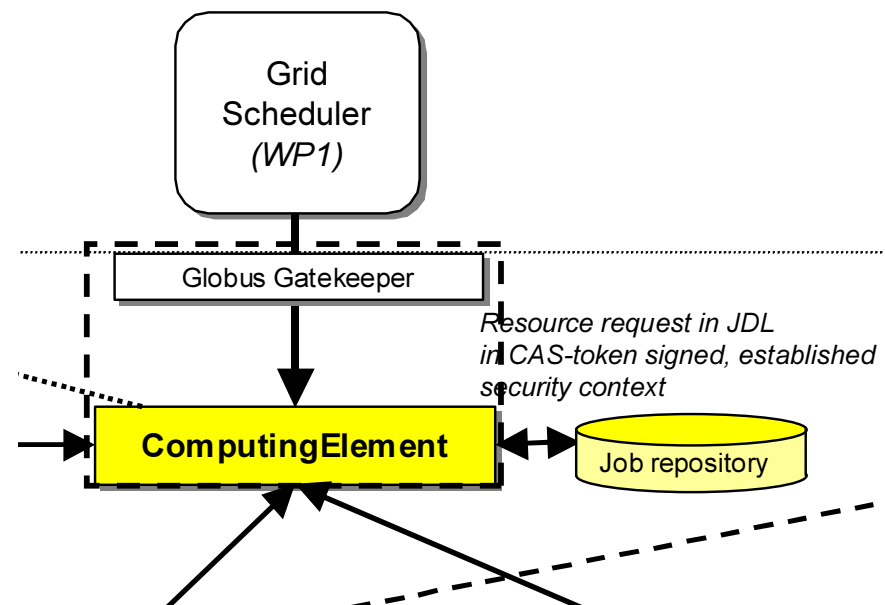 - ▪ RSL passed to JobManager

- ◆ Identified design differences
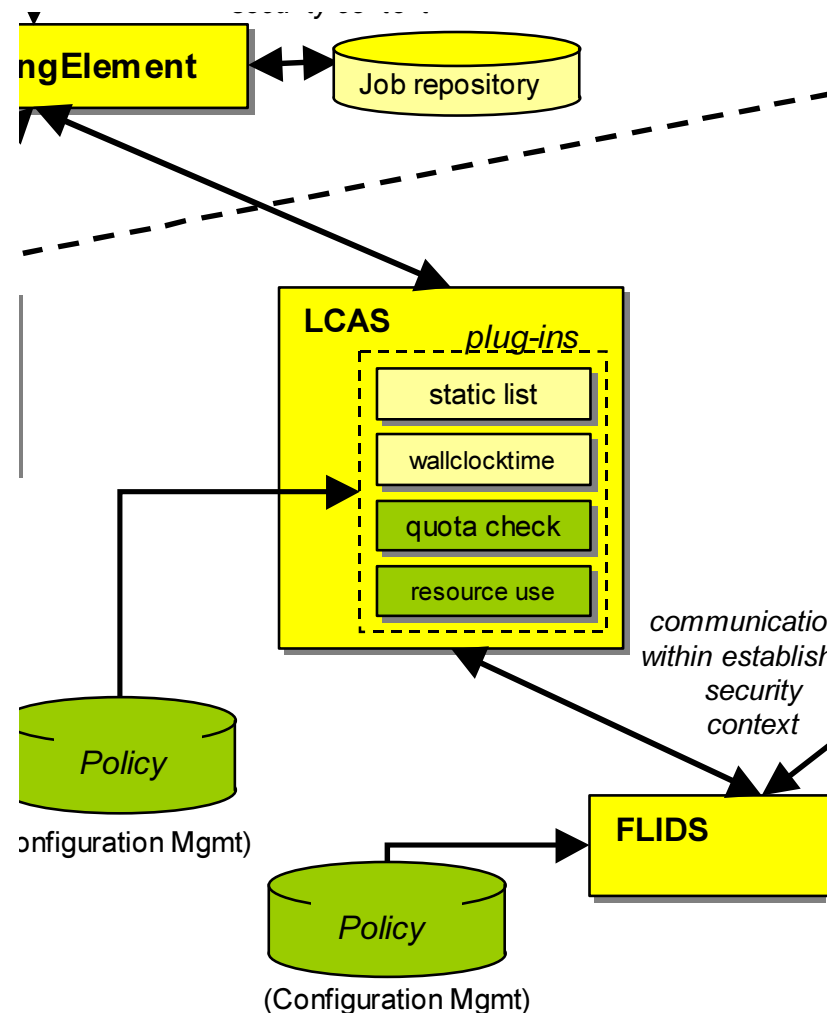 - ▪ authorization and user mapping done too early in process

- ◆ Identical components
  - ▪ Protocol must stay the same (GRAM)
  - ▪ Separation of JobManager (closer to RMS) and GateKeeper will remain

- ◆ Issue: scalability problems with many jobs within one centre (N jobmanagers)

Grid Scheduler *(WP1)*

Globus Gatekeeper

ComputingElement

Job repository

Resource request in JDL in CAS-token signed, established security context

Authorization and AAA
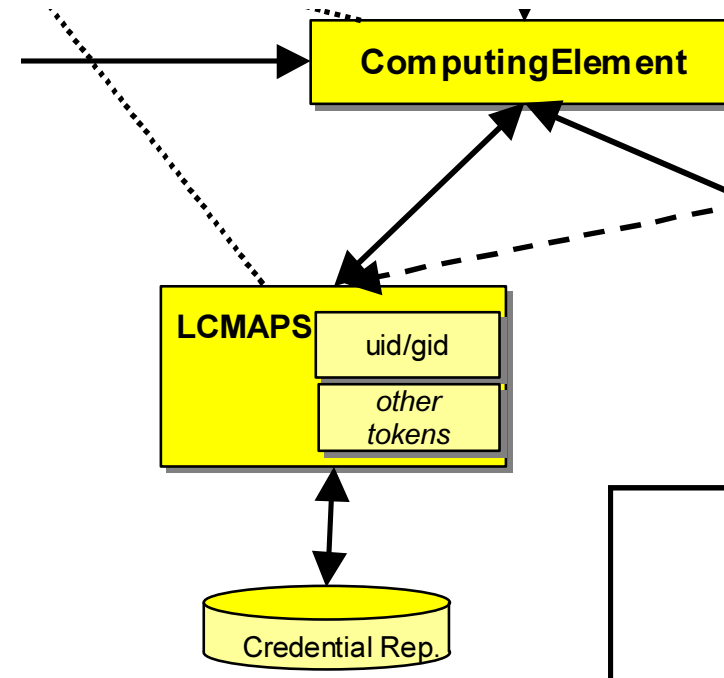
- Current Globus design:
  - Authorization and user mapping are intermingled
  - No scalable/dynamic per-site Authorization in Globus

- Identified design points
  - new design, taking concepts from generic AAA architectures
  - coordination with EDG security group

- Identical components
  - generic AAA architectures/servers
  - distributed AAA decisions/brokering
  - generic policy languages

ngElement

Job repository

LCAS *plug-ins*

static list

wallclocktime

quota check

resource use

*communicatio
within establish
security
context*

Policy

(onfiguration Mgmt)

Policy

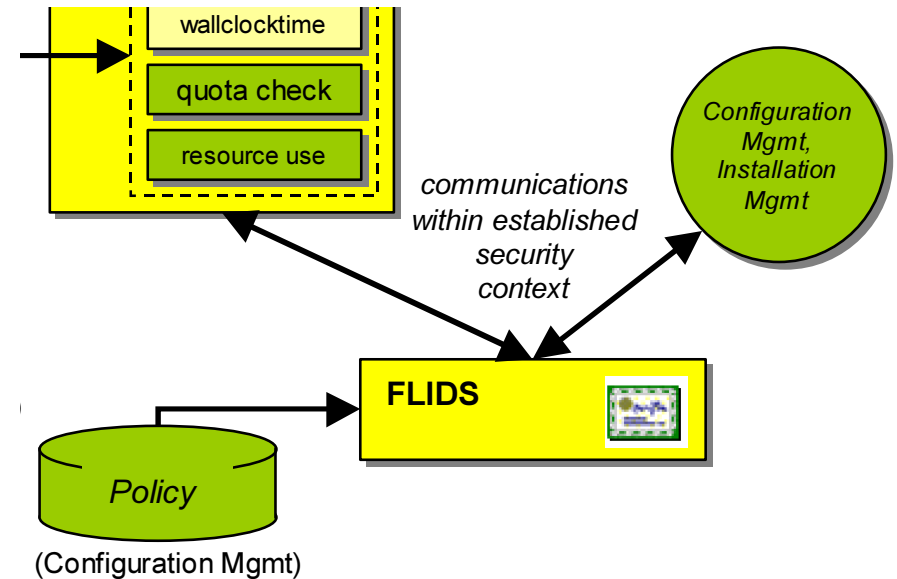(Configuration Mgmt)

FLIDS

Credential Mapping

- ◆ Current Globus design:
  - Authorization and user mapping are intermingled
  - Currently by GateKeeper (on connection establishment)
  - Kerberos by external service (sslk5)

- ◆ Identified design points
  - Extend for multiple credential types
  - move to later in the process (after AAA decision)

- ◆ Identical components
  - gridmapdir patch by Andrew McNab
  - sslk5/k5cert service

- ◆ Issues in current design
 - mapping may be expensive (updating password files, NIS, LDAP, etc.)

ComputingElement

LCMAPS
uid/gid
other tokens

Credential Rep.

Local security service (FLIdS)

- Current Globus design:
  - Component does not exist
  - Technology ubiquitous (X.509 PKI)

- Identified design points
  - Policy driven automatic service
  - policy language design (based on generic policy language or EACLs)

- Identical components
  - PKI X.509 technology (OpenSSL)
  - use by GSI and HTTPS

- Issues:
 - mainly useful in untrusted environments (e.g., outside a locked computer centre)

wallclocktime

quota check

resource use

communications
within established
security
context

Configuration
Mgmt,
Installation
Mgmt

FLIDS

Policy

(Configuration Mgmt)

Information Services (GriFIS)

- Current Globus design:
  - GIS: LDAP based with caching backend
  - Modular information providers

- Identified design points
  - Many more information providers (CDB)
  - Correlators between RMS, Monitoring and CDB (internal WP4 components)

- Identical components
  - GIS or EDG equivalent (GMA/R-GMA)
  - Some of the information providers

- Issues in current design
  - Evaluation of WP3 framework still in progress
  - Wide variety of frameworks in general, but all seem currently interchangeable

IMS
(WP3)

data flow

FabNAT

GriFIS

data flow

Monitoring

RMS

farms

LCMAPS
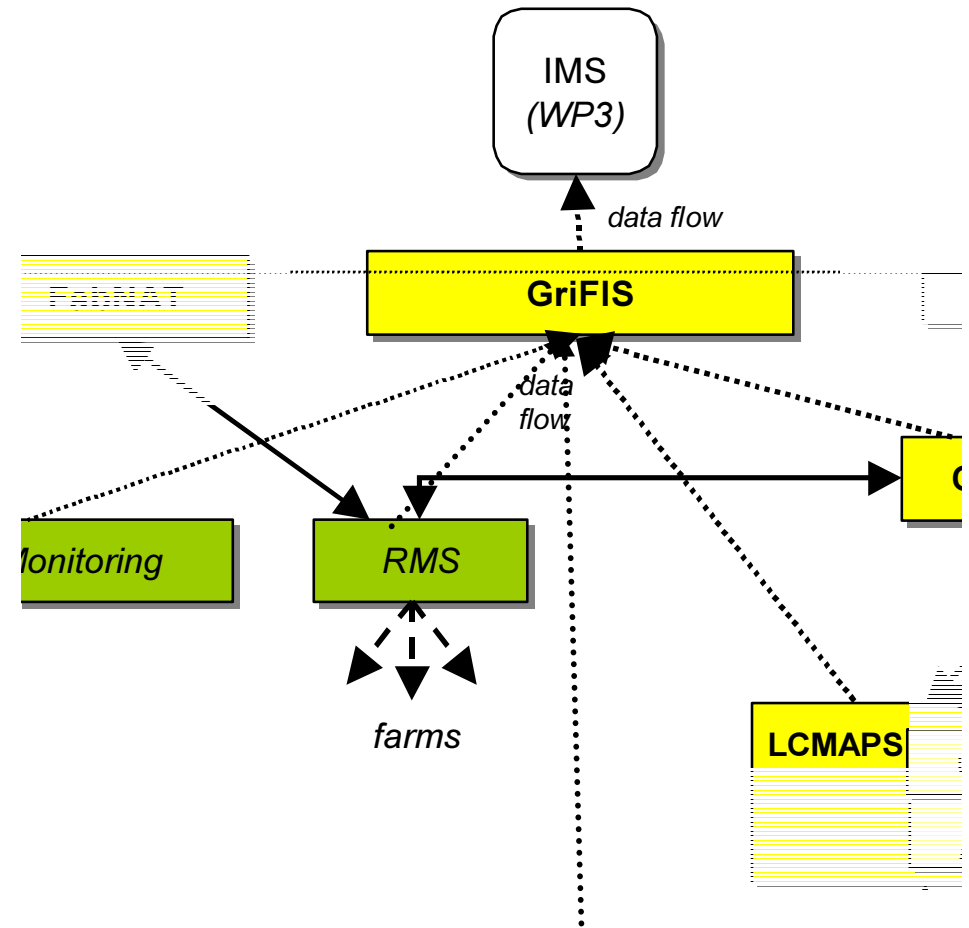
Network access to large fabrics

- ◆ Current Globus design
  - ▪ Is not in scope of Globus toolkit

- ◆ Identified design differences
  - ▪ Needed component for large farms
  - ▪ Needed for bandwidth brokerage and user/job based QoS

- ◆ Identical components
  - ▪ 0st order: no functionality
  - ▪ 1st order: IP Masquerading routers
  - ▪ 2nd order: IP Masq & protocol translation (IPv6 → IPv4 and v.v.)
  - ▪ use of intelligent edge devices, managed bandwidth (and connections) per job, AAA interaction (with LCAS)

External to fabric

FabNAT

Internal to fabric

Fabric Monitoring

RMS
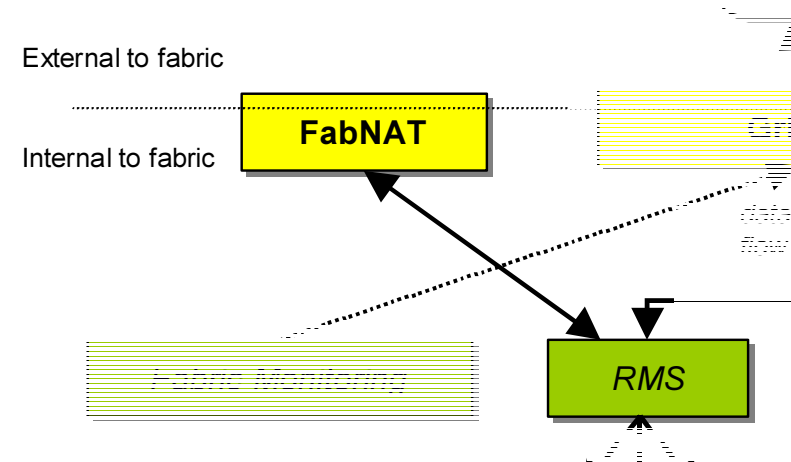
Key overlaps & differences

◆ Globus provides adequate prototypes for much of the functionality

◆ **Lacking components**

- Generic and distributed AAA

- too-early relinquishing of credential mapping capabilities in gatekeeper

- does not address intra-fabric security concerns (FLIdS)

- information providers for whatever the framework will be

- managed network access

◆ **Key components to be compatible**

- GRAM protocol & RSL forwarding [Globus]

- Information framework (GIS, GMA, R-GMA, …) [Globus and EDG WP3]

- Security methods and protocols (X.509, SSL, …)