# LCG/GDB
Security Update
(Report from the LCG Security Group)

Barcelona
18 May 2004

David Kelsey
CCLRC/RAL, UK
d.p.kelsey@rl.ac.uk
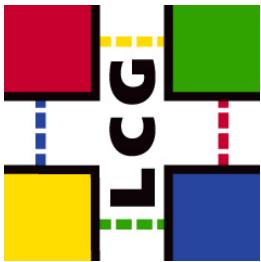
Overview

- LCG Security Group meetings
  - 22 March & 11 May 2004
  - Next meeting: 19 May 2004
- Policy documents: status and plans
- CA status
- EGEE security
  - Site requirements
  - Relationship to LCG, OSG etc
- User Registration/VO management
  - Requirements document
  - Task force

D.P.Kelsey, LCG-GDB-Security
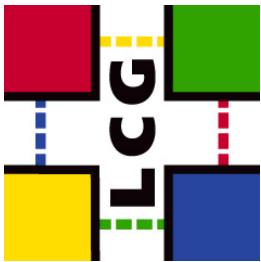
LCG Policy documents

- LCG Security and Availability – top level policy
  - Approved by GDB in October 2003
  - To PEB soon (minor changes still to be done)
- 3 new GOC guides presented at March 2004 GDB
  - Resource Administrators Guide
  - Service Level Agreement
  - Procedure for Site Self Audit
- Network and Application Security Guide (aim for June GDB)
- Many documents now need re-writing (task for LCG SEC)
  - Aim for larger scope
 - worldwide HEP and even eScience (EGEE, EiRG, OSG,…)
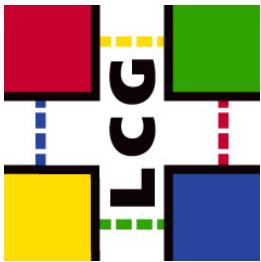
CA status

- The new EU Grid PMA formed and met 1st/2nd April 2004
  - takes over from EDG CACG
- http://www.eugridpma.org
- DPK is LCG representative on the PMA
- TERENA CA repository also active now (TACAR)
  - Independent 3rd part store of roots of trust
- EiRG endorsed EU GridPMA and TACAR (Dublin, 16 Apr)
  - For use in EGEE, DEISA and SEE-Grid, ... (& LCG!)
- Pakistan CA now granted interim approval (by EU Grid PMA)
  - They have to present in person in September
- Hungary and Estonia also presented in April
- US DOE CA close to acting as LCG "catch-all"
  - CNRS CA continues as EGEE (non-LCG) catch-all
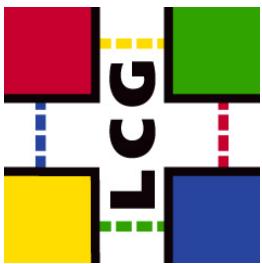
EGEE Security

- Why mention this at an LCG GDB meeting?
  - We (EGEE *and* LCG SEC) are now discussing
  - Depends on the GDB relationship to EGEE
  - LCG SEC Group is compiling a list of Site Security Requirements for input to EGEE

- So… plan for today:
  - Security in EGEE
  - Site Security Requirements
  - LCG, EGEE, OSG security relations

D.P.Kelsey, LCG-GDB-Security
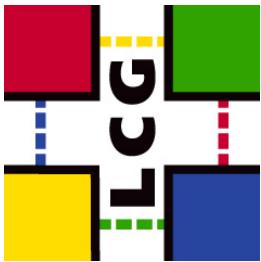
EGEE security groups

- JRA3 (Ake Edlund and NEG) is in charge

At the Cork EGEE kick-off meeting (April):

- Two coordination groups proposed

  - *EGEE Middleware Security* (Ake Edlund)

  - *SA1 Site Security Group* (DPK)

    - Builds on LCG Security Group experience

    - Responsible for preparing and maintaining policy and procedures

      - collect Sites (and VOs?) requirements and constraints

- EGEE Middleware Security met 5/6 May

- EGEE Site Security Group yet to be formed

18-May-04

D.P.Kelsey, LCG-GDB-Security

6

Workflow - Overview

egee

Enabling Grids for
E-science in Europe

NA4

Req.

Req.

Solutions/Recommendations

JRA1

Req.

Req.

Site
Security Group

Req.

SA1

Middleware
Security Group

JRA3

Req.
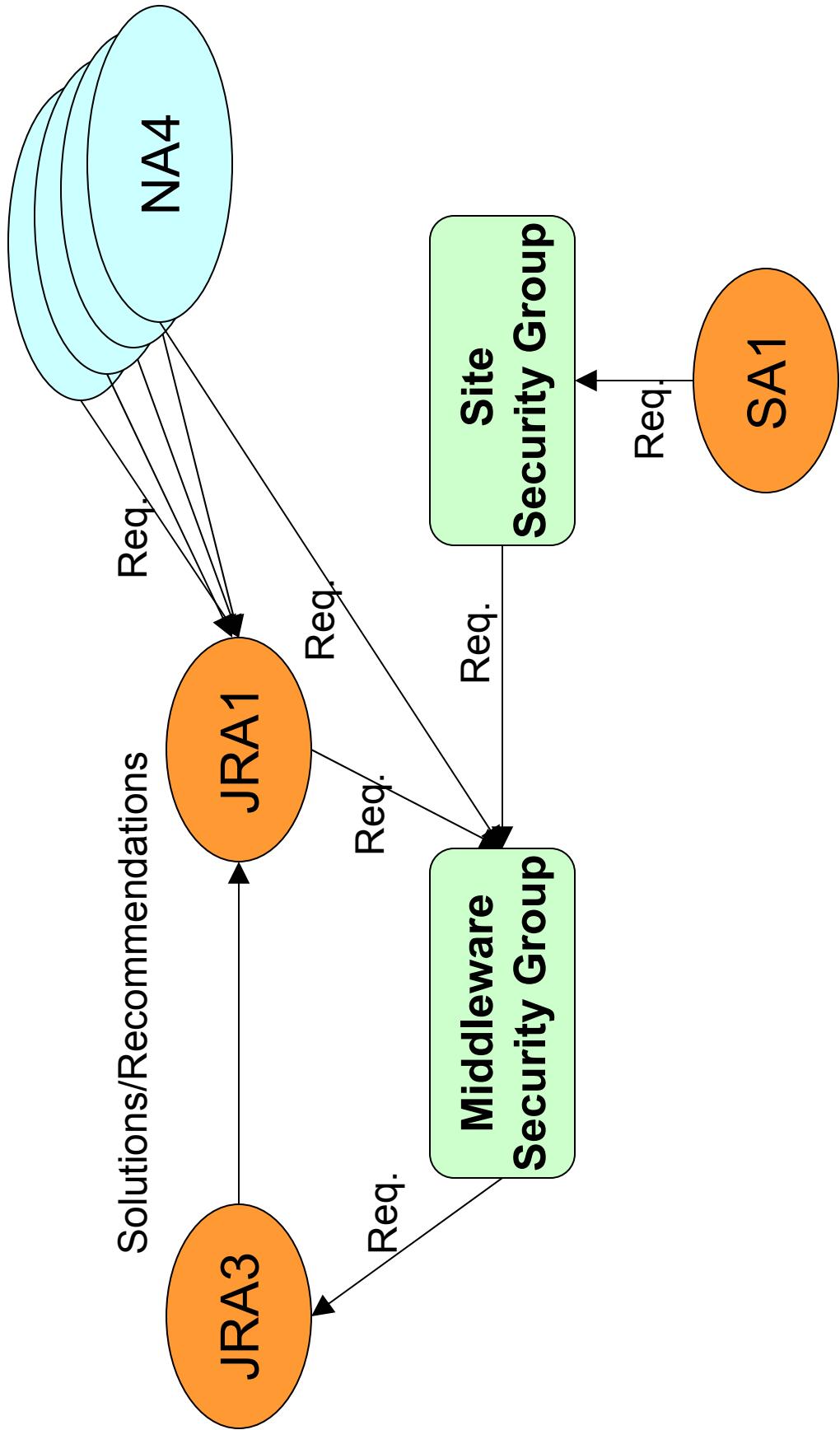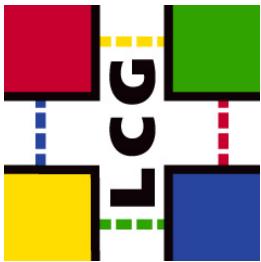
EGEE Site Security Requirements

- LCG Security Group asked to give rapid input to the EGEE Middleware security group
  - input for design of EGEE middleware
- We aim to submit this week
  - will discuss again 19 May phone conference
- Requirements include ….
  - Audit (consistent logs and identify individuals)
  - In control of local AuthZ policy (at individual user level)
  - User Reg/VO management procedures
  - Network connectivity (e.g. outgoing IP!)
  - Intrusion Detection hooks in middleware
  - Middleware security design and documented test procedures

18-May-04

D.P.Kelsey, LCG-GDB-Security

EGEE and LCG and OSG relations? (Ruth Pordes)

OSG

Applications

Engineering Group

Storage Technical Group

Operations Technical Group

Monitoring Technical Group

Facility Technical Group

Security Technical Group

Facilities

EGEE

NA4

JRA1

JRA3

SA1

Middleware Security Group

Site Security Group

Solutions/Recommendations

Req.

Interoperability

LCG Security Group

RP 5/12/04

9

18-May-04

D.P.Kelsey, LCG-GDB-Security

LCG
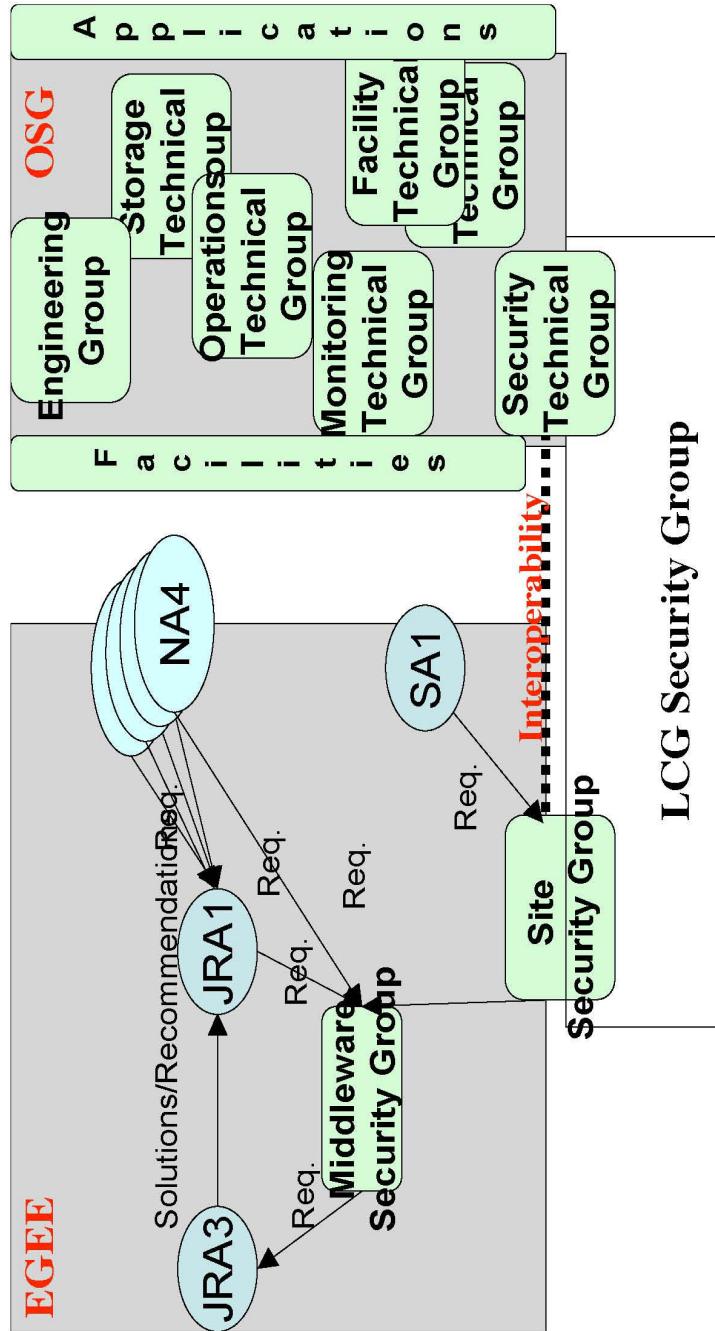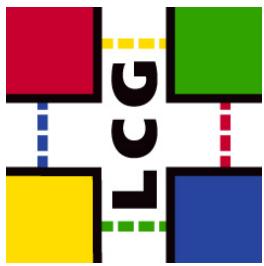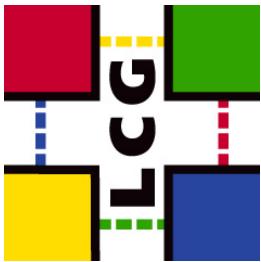
User Registration and VO Management

- LCG User Registration and VO Management (V2.1) was presented at the March GDB

- Aim
  - Improve the robustness and scalability
    - Procedures and technology
    - To allow sites to open up resources to VOs
  - Allow for non-LHC VOs (BaBar, D0, Biomed …)
  - Registration (logically) at the VO level

- Conclusion then was
  - GDB members to provide feedback
  - DPK to create task force to propose the solution(s)
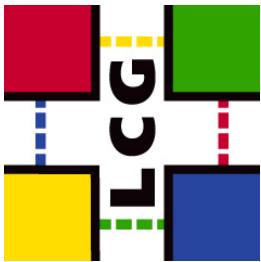
User Reg Requirements

- Lots of feedback received – thanks!
- Several versions of document and discussion
  - Now concentrate on Requirements
- V2.6 distributed to GDB on 13th May
- Important requirement is the use of existing VO databases
- Task Force created and made good progress
- Current concerns
  - Procedures for External users
    - Those who never come to CERN
  - need to handle exceptions (those not able to register)
  - VO Audit trail required
  - "Control" over users
    - team leader not necessarily this person
  - Experiments vary re regular review of DB entries

D.P.Kelsey, LCG-GDB-Security
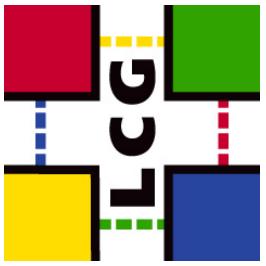
Requirements (2)

- Do we consider the document in more detail?

D.P.Kelsey, LCG-GDB-Security

18-May-04
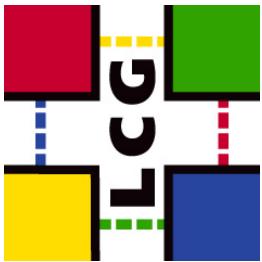
User Registration Task force

- A Task Force (TF) was formed after the March GDB

- Mission: To propose (to GDB through the LCG SEC group) procedures and technology to meet the LCG User Registration and VO Management requirements

  – In particular, to investigate the possibility to use CERN HR database (HR db) information to obtain Registration data for LCG users.

Members of the task force

- Ian Neilson (TF coordinator, LCG Security Officer)
- Maria Dimou (LCG Registrar and DTeam VO manager)
- Joni Hahkala (VOMS admin. development Leader)
- David Kelsey (LCG Security Group chairman)
- Tanya Levshina (VOX Project leader)
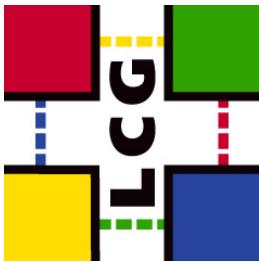
User Reg Task Force (2)

- Progress to date: met with the technical experts of the
  - CERN HR db
  - PIE db (HR db view for experiment members' registration)
  - Head of the Users Office

- Pending actions
  - May: Meet with the project leaders of the new CCDB project to discuss possible interfacing to HR db and CCDB data
  - Early June: Tel. conference with all members of the TF to formulate proposal
  - In June: Discuss at the LCG Security Group meeting the TF's proposal

- Present the TF's proposal to the July GDB meeting

D.P.Kelsey, LCG-GDB-Security
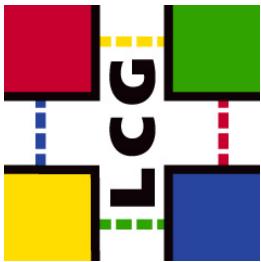
GDB approval and input

- *Approve* 3 policy documents presented in March GDB?

- *Approve* User Registration/VO Management Requirements (V2.6) document?

- *Input* to task force from experiments

  - To what extent do current procedures meet these requirements?

- *Guidance* on relationship with EGEE and OSG

- *Input* security requirements (for EGEE)