LCG/GDB
Security Issues and Planning

(Report from the LCG Security Group)

CERN, 8 May 2003

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

Introduction

- LCG Security Group meetings
  - Phone conference 29 April 03
  - Meeting (CERN) 7 May 03
- Concentrating on the planning and implementation for start-up of LCG-1 (July 03)
  - But keep Jan 2004 in mind
- Many topics discussed (as presented at April GDB)
  - Many can be dealt with within the group and LCG operations
  - Policy items require GDB discussion, consultation and decision
    - Concentrate on these today

Membership of Security Group

Changes and additions:

- Experiment reps
  - ATLAS: Gilbert Poulard replaced by Rich Baker (BNL) and Anders Waananen (NBI)
- Security middleware experts
  - Roberto Cecchini (INFN)
  - Akos Frohner (CERN)
- Still under-represented (nominations welcome)
  - Geographical (Only EU and US to date)
  - Resource/Site managers

Topics discussed

http://agenda.cern.ch/age?a031170

- Authentication - trusted CA's for this GDB
- Incident response
- Audit and Accounting
- User Rules/AUP/LCG Security Policy
- User Registration
  - Personal information for this GDB
  - Procedures for this GDB
  - Pre-registration and account creation
- US CMS VOMS Extension project (VOX)
- VO Management
- Not discussed: Firewalls, network connectivity

Issues for GDB

- Start with those topics requiring GDB discussion
  - Initially today and decisions at June meeting
- Authentication-Trust
- User Registration – personal information
- User Registration – procedures

Authentication - Trust

- Two main issues
  - Who defines the list of trusted CA's?
    - LCG or other Grid projects?
  - How to introduce new types of CA (online)?
    - E.g. Kerberos CA at FNAL
- LCG-1 and EDG Application testbed
  - closely linked (at many sites)
  - Common approach desirable (for this year)
- For Jan 2004 onwards
  - Forum for CA best practice and trust evolving
    - EGEE, GGF
    - Community larger than just HEP

EDG CA's

18 on the trusted list (today)

- Canada, CERN, Cyprus, Czech Republic, France, Germany, Greece, Ireland, Italy, Netherlands, Nordic, Poland, Portugal, Russia, Slovakia, Spain, UK, USA
- "Catch-all" operated today by CNRS/France

Under development/consideration

- Belgium, FNAL (KCA), Hungary, Israel, Japan, Taiwan

Next meeting of the CA group is 12/13 June (CERN)

Recommendations to GDB Certificate Authorities

GDB is asked to agree for LCG-1 operations during 2003 that…

1) The LCG-1 Security Group defines the list of accepted CA's from two sources
   a) The list for traditional CA's comes from the EDG CA Group
   b) The list for additional CA's (online short-lived, special cases) is generated by the LCG-1 Security Group
2) That proposed additions to these lists above be circulated to the LCG-1 site security contacts for objection prior to implementation
3) That the LCG-1 operations group maintains the necessary information (certificates, signing policy, CRL's) and distribution mechanisms for CA's on both lists
4) All LCG-1 resources will install this information

User Registration
Personal Information

- The process for July 03
  - User registers with the LCG-1 Reg. Web
  - This list of users (the LCG-1 Guidelines VO) starts from an empty list (no inherited users)
  - Registration will have an initial short expiry date
    - Propose 6 months (2004 – new AUP/Policy, new procedures)
  - Information collected (fields on the web form) is ideally the super-set of that required by the sites
    - But this may not be possible
- Aims
  - Avoid user having to register at multiple sites
  - Avoid situation where users jobs will only run at subset of sites (but technically possible)

User personal info (2)

- Current common list (discussed on Security Contacts list)
  - Full name, Institute, Institute telephone number, e-mail address, Certificate DN, Experiment(s)
  - But only 4 sites responded to date
- OK so far, but some sites have requirements for additional fields
- FNAL requires
  - Nationality, date of birth and place of birth
  - Info required up-front for pre-registration
- BNL requires Nationality
- These items raise significant privacy concerns
  - Can be used for Identity theft
  - Users rightly concerned about the distribution/use of their data

User personal info (3)

- Karlsruhe and BNL expressed concerns about the distribution of and access to the data (privacy and legal issues)
- CERN expressed concerns about having to collect and manage such private data.
- AUP/reg web will request users consent to use the personal data
- We need LCG policy in this area
  - Who has access to the data and for what purpose

User personal info (4)

Ask GDB to consult their sites, countries

- replies from all sites, please

- What user information is required?
- Is this required for pre-registration
  - i.e. before creation of an account?
  - Or just access following some incident?
- Why do you need the (particularly sensitive) info?
- Can your policy be changed?

GDB will need to decide (June) whether to

- Agree to a common set of info for single registration or to
- allow some sites to require separate registration or to
- Allow some users' jobs not to run everywhere

Registration procedures

- In the April GDB report, we proposed
  - improve and document the Experiment VO RA procedures
  - with no checks when joining the LCG-1 VO
- Long-term aim still ("Experiments" do the work)
  - move the registration process to the Experiment User offices
- Short-term (Sites do the work)
  - necessary to have robust checks at the first stage in the registration process (joining the LCG-1 Guidelines VO)
    - This is where the user info is collected and stored
  - can delay improvements to the experiment VO procedures
    - Until ready to take over the management of user info

Registration procedures (2)

- Implement a distributed LCG-1 registration authority
  - Hierarchical scales best (i.e. use Tier-1 centres)
- The web-form will have pull-down lists of institute names (per country) – to enforce format etc
- Need to map Institutes to Registration Authorities
- The Registration Authority confirms
  - The person issuing the request is allowed to join LCG-1 and they did indeed complete the reg form
  - That the info provided is correct
- In most cases this will (eventually) need distributed RA's behind each Tier-1

Registration procedures (3)

- We ask GDB to consider
  - Ask each Tier-1 to
    - nominate one (or two) individuals as the regional RA
      - Process needs defining plus suitable training
    - Define a list of Institutes to be supported by the RA
  - Users from institutes not associated to a Tier-1 RA should be checked by the Experiment (or institute makes arrangements with a Tier-1)
    - Will need experiment RA's

Summary

Issues for GDB

- Agree procedure for definition of trusted CA's
- Required User Personal Info fields
  - And related aim of single registration
- Tier-1 Registration Authorities

Acceptable Use Policy

- Users agree to this when they join the LCG-1 VO
- We start with the current EDG User Rules
  - Aim to make minimal changes
- This includes User Rules, responsibilities of the Sites and rules for access to personal data
- Eventually we aim to have separate User Rules and a LCG Security Policy (but not for July)
- The AUP will be submitted to the GDB at the end of May
  - Next Security Group phone conference is 28th May

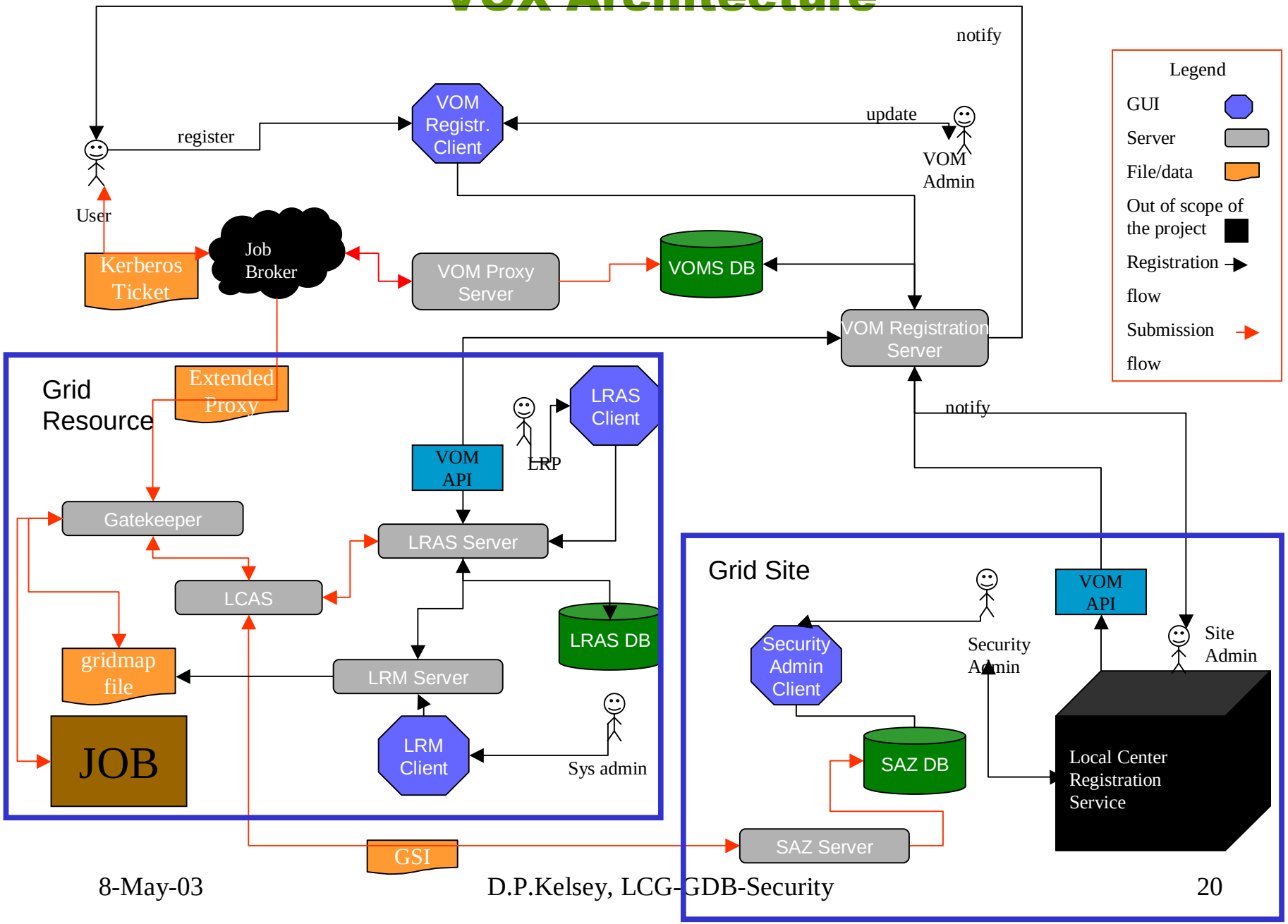
VO Management

- WG3 report, GDB and subsequent discussions
- One VO service per experiment
  - shared between LCG and EDG
- July 2003 (GDB approval?)
  - Continue with existing VO databases and servers run by NIKHEF (for EDG)
  - With existing VO managers
    - These approve the requests to join
- By Jan 2004
  - LCG will need to run its own servers
  - Perhaps sooner than January?

US CMS VOX

- Tanya Levshina (FNAL) presented the plans and status of this "VOMS Extension" project
- See slides and paper on the Security Group agenda page (7th May)
- Purpose
  - To facilitate the remote participation of US based physicists in effective and timely analysis of data from the LHC experiments during DC04 by designing, developing, and deploying Virtual Organization Management Service eXtension (VOX) for US CMS

VOX Architecture



VOX (2)

- Scope is US CMS (Tier-1/Tier-2) for July 2003
- Registration components clearly of interest to LCG
  - But not for July 2003
- An ambitious project with security middleware developments
- There is overlap between some of the proposed functionality and that being developed in EDG
  - Propose that VOX and EDG collaborate

Incident Response

- Draft document (Dane Skow)
  - being discussed on Security Contacts list (Dane Skow)
  - Incidents, communications, enforcement, escalation etc
  - Good working draft by end of May (for GDB)
- We already have a (mail) list of Contacts (these are people)
- While we wait for Grid Operations centres
  - We need/will create an ops security list
  - Default site entry is the Contact person but an operational list would be better
- for Site Security Ops use only (not for users)
- GDB should require sites to listen and react to the ops list
- Response will be no better than current cover
  - Varies from site to site
  - But not 24*7

Audit (and Accounting)

- LCG ops team (Ian Neilson) defining lists of what logs need to be kept for audit purposes
  - Mainly grid services (CE etc) and batch services
  - Some grid service logs are distributed
  - Logs may also contain non-grid jobs (no problem)
- List to be finalised at 5th June LCG Security meeting
- Format to be specified later (not July 2003)
- Tools to analyse and aggregate info will come later
- Security Group proposes minimum retention period is 3 months
- Some of the same logs will be needed for Accounting but this is not our responsibility

Summary (again)

Issues for GDB

- Agree procedure for definition of trusted CA's
- Required User Personal Info fields
  - And related aim of single registration
- Tier-1 Registration Authorities