Architecture Review
September Release

Piotr Poznanski

Piotr.Poznanski@cern.ch

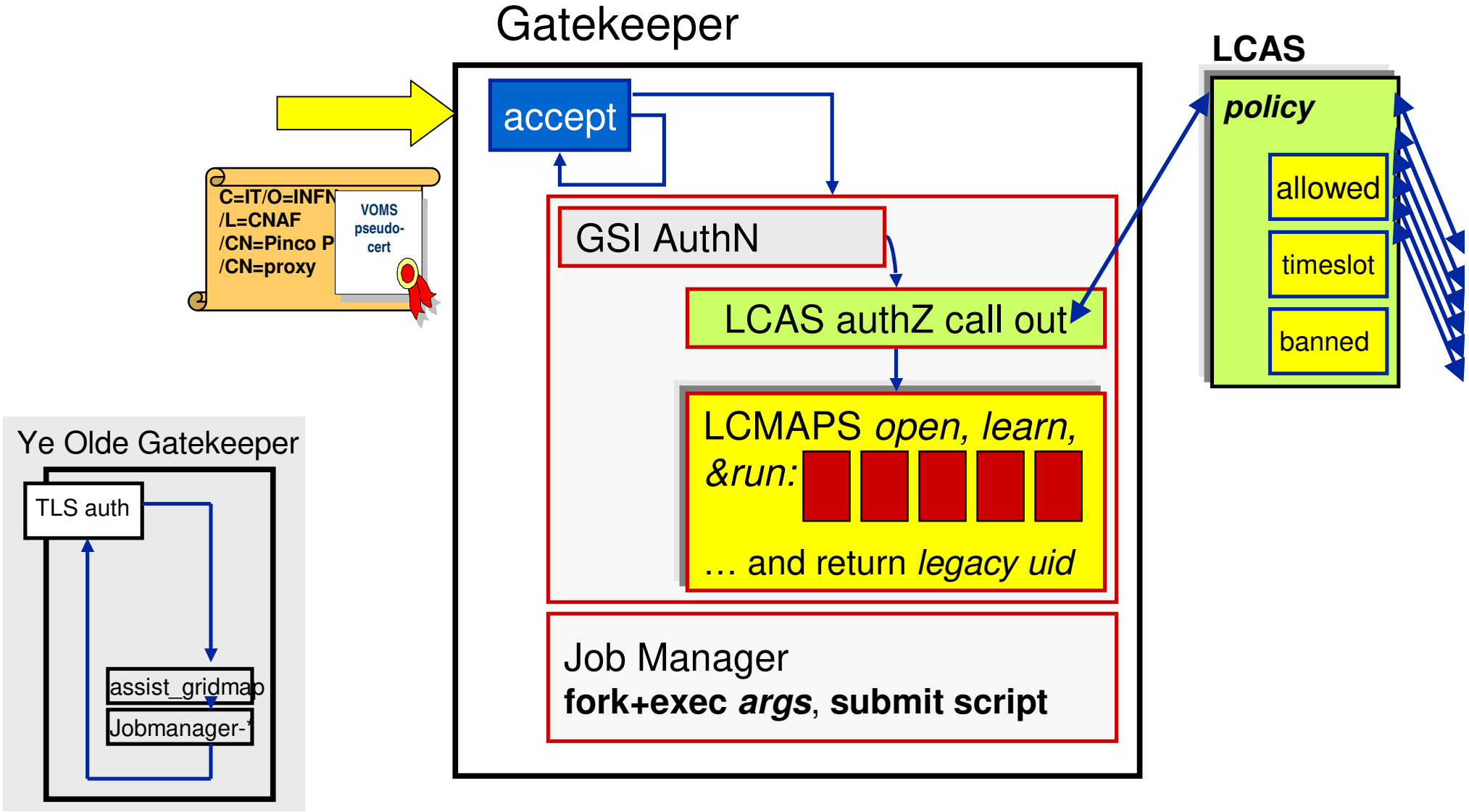
WP4 Priorities

- LCAS 2.0 - July/August
  - server implementation (does not require root privilege, one per many CEs)
  - use of Policy Description Language (PDL)
  - API plug-in upgraded to LCMAPS plug-in API,
- VOMS plug-in (end of June)
  - authorization decision based on VO, (sub)group, role
- LCMAPS 1.0 - end of June (with plug-ins)
  - plug-in framework, driven by PDL
  - supports standard UNIX credential (incl. pool accounts, VO affiliation, site local policy
- RMS
  - support for LSF, Condor
  - advance reservations
- Monitoring/Fault Tolerance
  - Relational DB backends (Oracle, MySQL)
  - GUIs (Alarm Display, AnaMon)
  - Fault Tolerance integrated
- Installation & Configuration
  - outside main TB
  - No involvement of MW WPs

Local Site Authorization Services

- **Local Centre Authorization Service (LCAS)**
  - Handles authorization requests to local fabric
    - Authorization decisions based on proxy user certificate and job specification
    - Supports grid-mapfile mechanism
  - Plug-in framework (hooks for external authorization plug-ins)
    - Allowed users (grid-mapfile or allowed_users.db)
    - Banned users (ban_users.db)
    - Available timeslots (timeslots.db)
    - Plugin for VOMS (to process Authorization data)
- **Local Credential Mapping Service (LCMAPS)**
  - Provides local credentials needed for jobs in fabric
  - *Plug-in* framework, driven by comprehensive *policy language*
  - Mapping based on user identity, VO affiliation, site-local policy
  - Supports standard UNIX credentials (incl. pool accounts), AFS tokens, Krb5

EDG Gatekeeper (release 2.1)



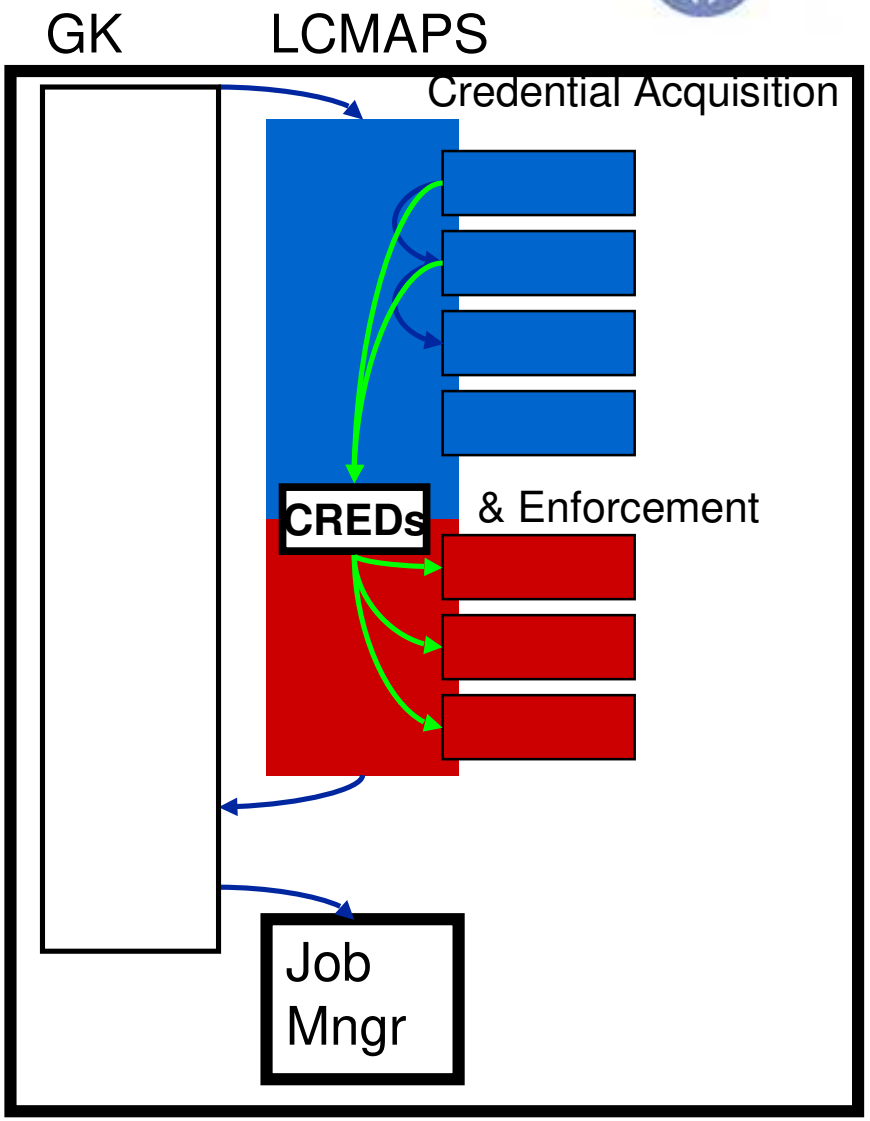
LCMAPS – requirements

- Backward compatible with existing systems (grid-mapfile, k5cert)
- Support for multiple VOs per user (and thus multiple UNIX groups)
- Mimimum system administration
  - Poolaccounts
  - Pool”groups”
  - Understandable configuration
- Extendible

- Boundary conditions
  - Has to run in privileged mode
  - Has to run in process space of incoming connection (for *fork* jobs)

LCMAPS – control flow

- User authenticates using (VOMS) proxy
- LCMAPS *library* invoked
  - Acquire all relevant credentials
  - Enforce credentials on current process tree at the end
- Run job manager
  - Fork will be OK by default
  - Batch systems may need primary group explicitly
  - Batch systems will need updated (distributed) UNIX account info
- Order and function: policy-based

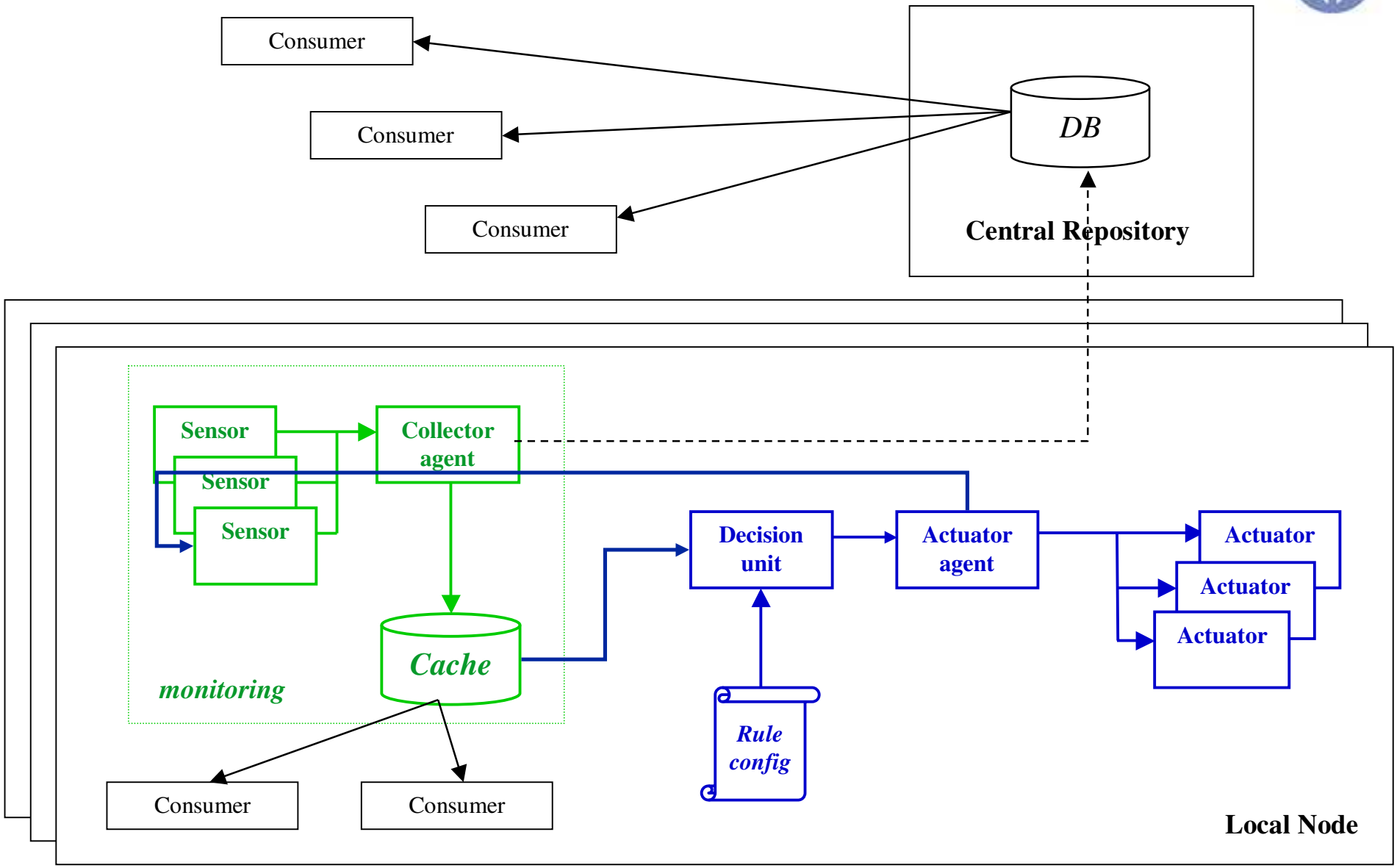
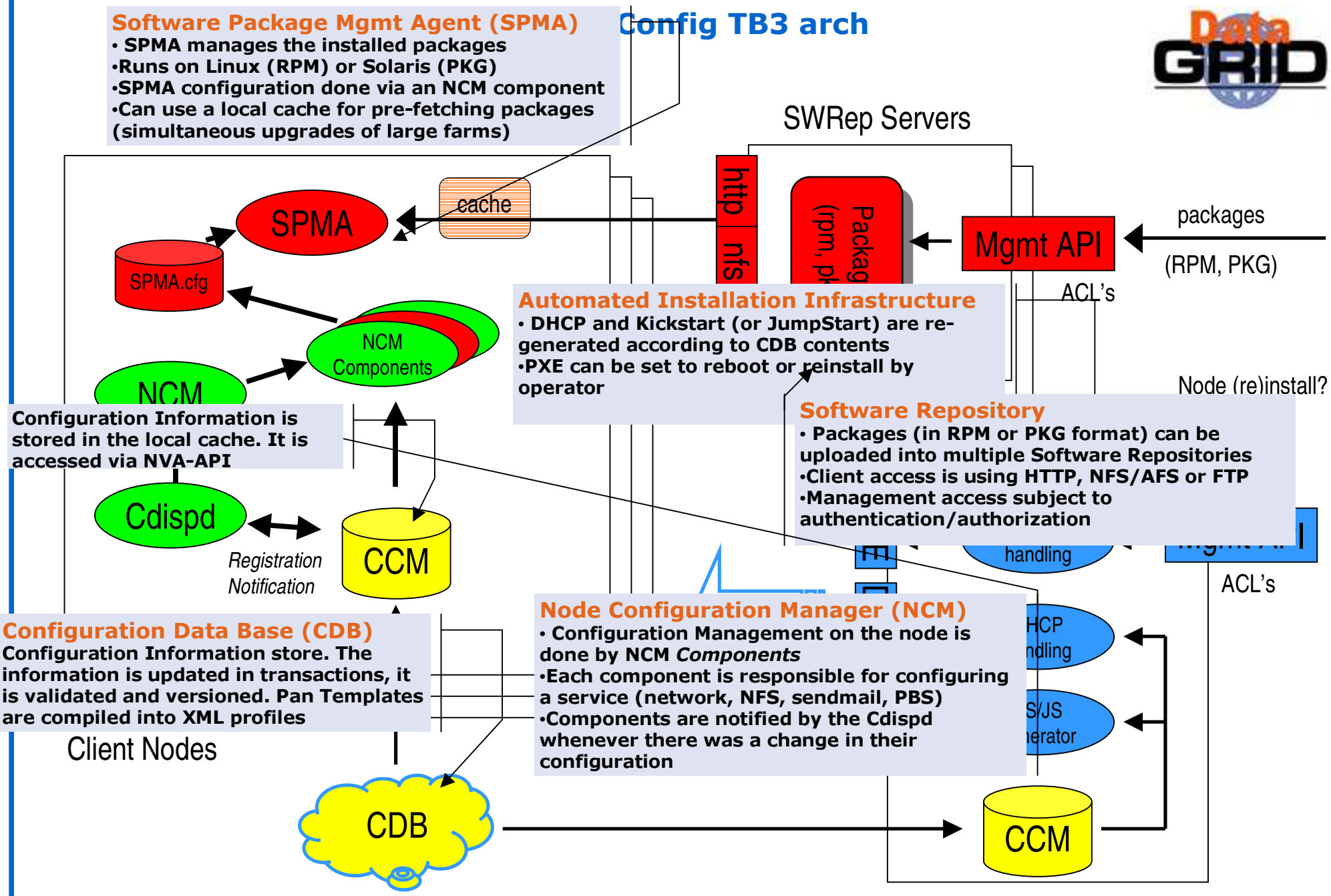


LCMAPS – modules

- Modules represent *atomic* functionality

- **VOMS** from role info and local mapfile assign gid (A)
- **PoolAccounts** from username assign unique uid (A)
- **PoolGroups** from (VOMS) groupname assign unique gid (A)
- **LocalAccount** from username assign local existing unique uid (A)
- **AFS/Krb5** get token based on user DN info (A)
- **POSIX *process*** setuid() and setegid() (E)
- **POSIX LDAP** update distributed user database (E)
- **Krb5** run job via k5cert (E)
- **…**

Fabric Monitoring & Fault Tolerance



Config TB3 arch