

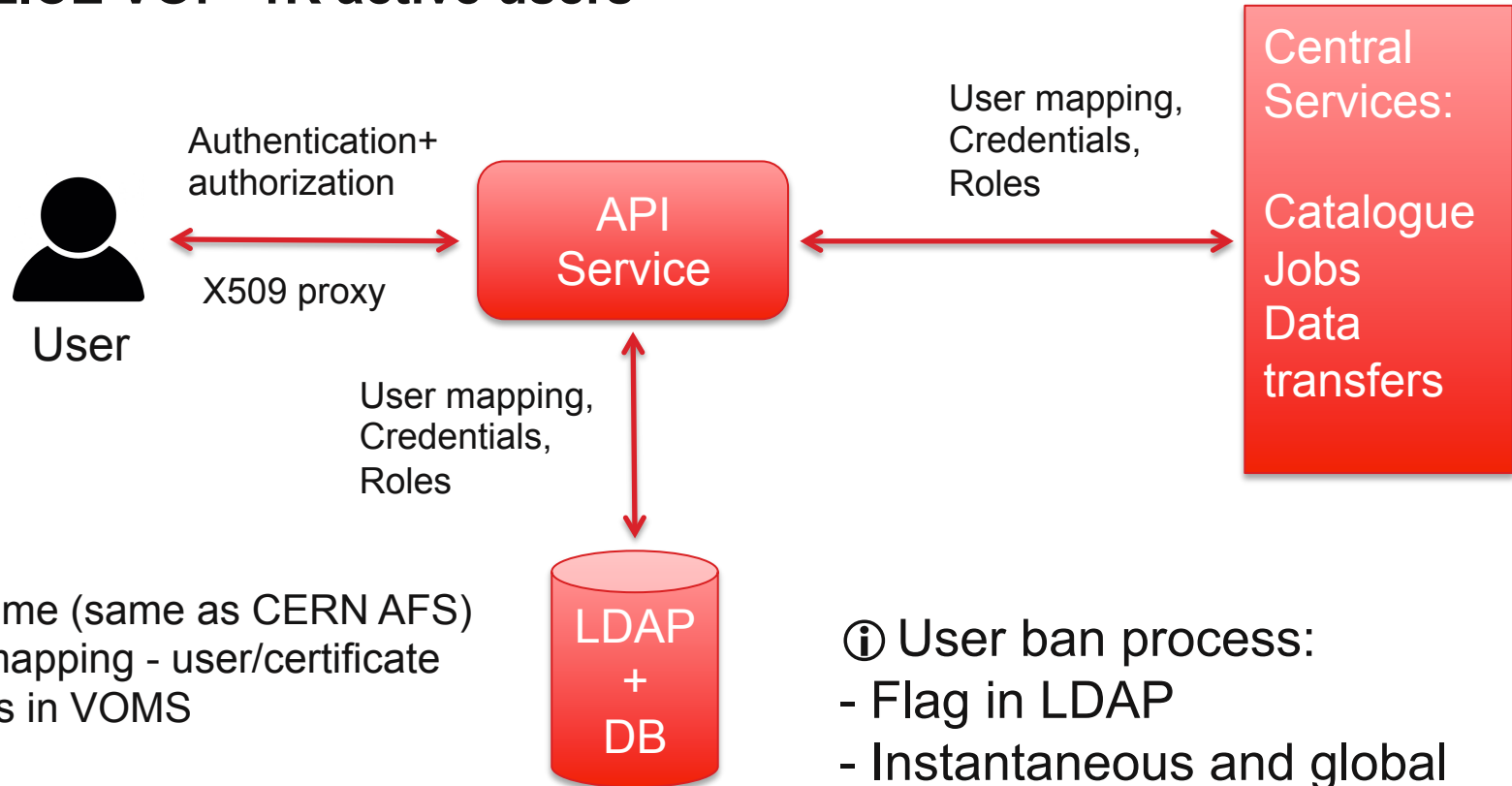


ALICE GRID SECURITY MODEL



ALICE GRID MODEL: USERS

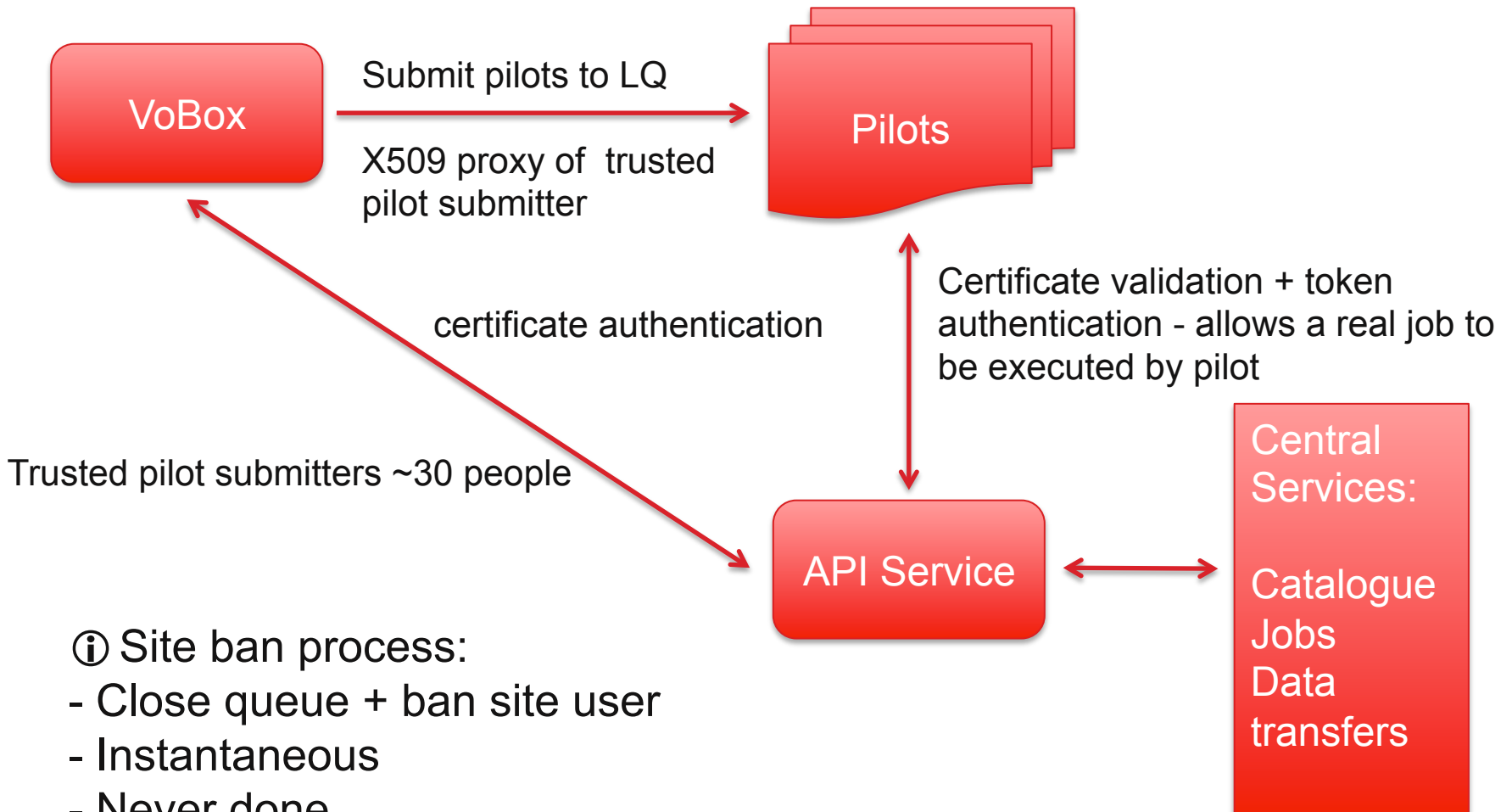
ALICE VO: ~1K active users



User name (same as CERN AFS)
1-to-1 mapping - user/certificate
All users in VOMS

- ⓘ User ban process:
- Flag in LDAP
 - Instantaneous and global
 - Never done

ALICE GRID MODEL: PILOT JOBS



TRACEABILITY

Users

- Logs with timestamp-command-user
- Logs IP/user request

Sites

- Job trace

Includes: Job data (TTL, job ID, JDL...), node, job status changes, errors, exit codes, batch job ID, and more (with timestamps)

- Pilot trace

Job IDs-Batch job IDs (if available), TTLs, total number of payloads ran

All logs kept since beginning of production.

ISOLATION

- Provided by the system
 - Sandboxed payloads [+ VMs in some cases]
- Clear isolation of VO services and data
 - Through the security layers shown in previous slides
- Pilot monitors and controls the payload (cpu, memory, disk)
 - Sending monitoring information periodically as well
- DB backups and monitorization
 - Load, operations: anomaly detection

ISOLATION

- Need to have more control
 - Filesystem (isolate key files and avoid payload interaction)
 - Memory, CPU, disk usage (force limit)
 - Some sites already partly implementing: CERN, KIT
- Working on **cgroups** / **containers** based configuration
 - **Positive** remark: mature, well-known, extended and accepted tools, big community (Docker, HTCONDOR, Mesos and more...)
 - Pilot able to generate its own isolated environment (e.g. Docker as requirement?)
 - VOs know exactly what they need to protect and avoids relying on site config
 - We could want different requirements depending on payload
 - Need to verify that both performance and integration of other software works OK
 - i.e. disk I/O + network, or CVMFS mounts
 - Already have a site using Docker within HTCONDOR
 - PhD working on Docker + AI integration
 - Algorithm to detect intrusions



SUMMARY

- ALICE has been stable since the beginning of operations
- Developments on Traceability & Isolation to improve the current status
- Questions / comments ?
- Thanks!