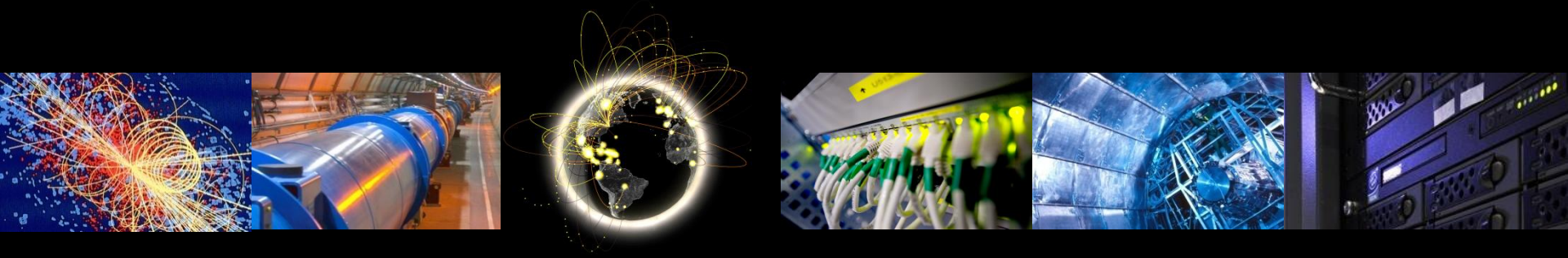
TEG Security
<Worker Node Security>

steffen.schreiner@cern.ch

7.2.2012 TEG Status, CERN



WLCG
Worldwide LHC Computing Grid

Worker Node Security

Is actually

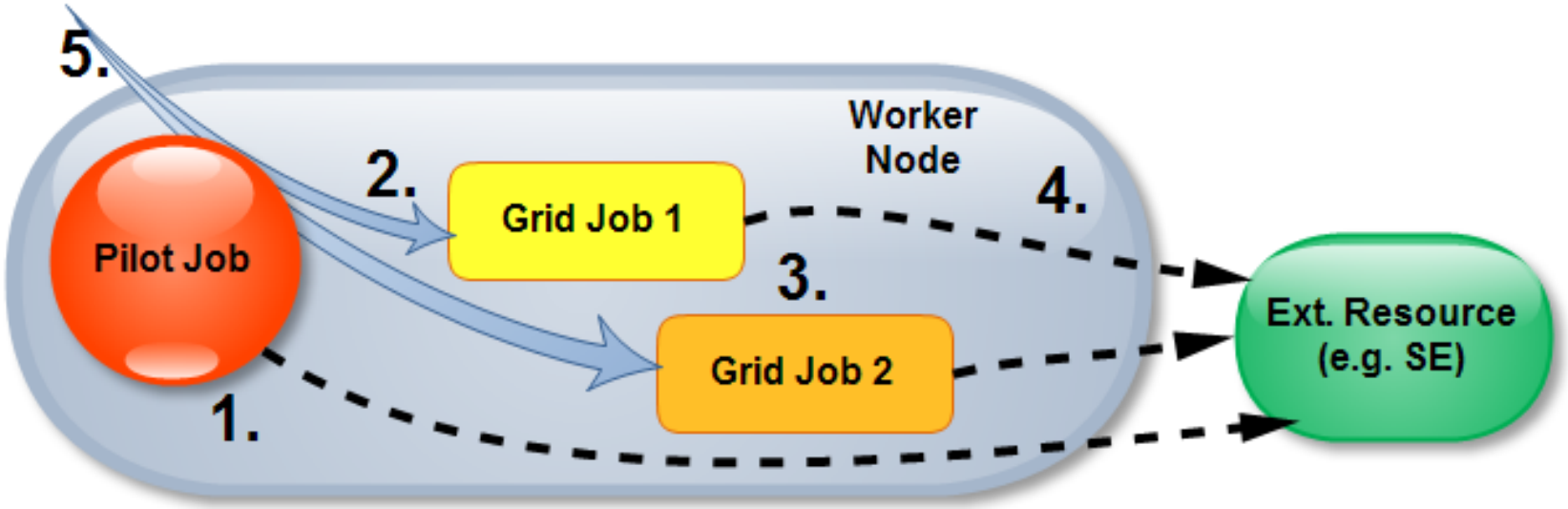
- Security of the Pilot Job
- Security of the Grid jobs
- Traceability (+ Accountability)

This brought us to five general

security requirements...

WN Sec Requirements

1. **Reduce a pilot job's credential to the minimum**
2. **Protect the pilot job**
3. **Mutually isolate jobs**
4. **Provide a minimal credential for the job**
5. Prove a job's authenticy, audit and log before execution.



Protection & Isolation

- We did (and will further) analyse the different options
  - Virtualization
  - ID Switching (gLExec, sudo)
  - SELinux
  - and more (e.g. Linux Containers in the future)
- Only serious option to take for the short-term is ID switching with gLExec
  - SELinux not usable right now
  - Virtualization would require further development

Short-term ID switching

Using gLExec ...

- **ALICE:** Proxy certificates that are limited to allow ID switching with gLExec only. This would allow to put (almost) no additional trust into the VO. (awaiting disussion and decisions by both gLExec and ALICE development, no time estimate).
- **ATLAS:** The GlideinWMS back-end engine for PanDA handles ID switching transparently via Condor (still being tested - no exact time estimate.)
- **CMS:** GlideinWMS already handles the ID switch transparently via Condor.
- **LHCb:** DIRAC can be configured to let the pilot make use of gLExec (retesting necessary due to potential changes since original development).

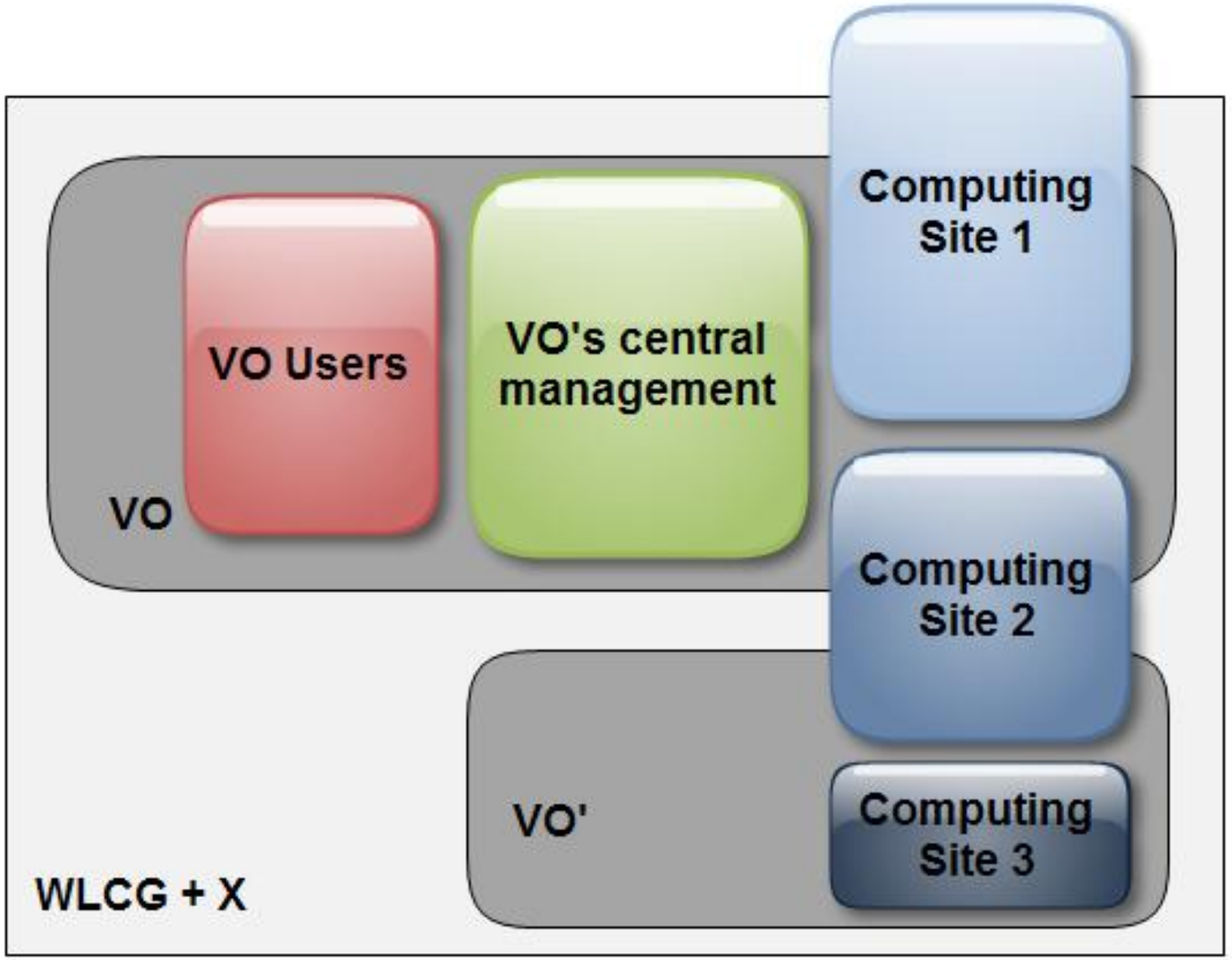
Beyond short-term

1. Reduce a pilot job's credential to the minimum
2. Protect the pilot job
3. Mutually isolate jobs
4. Provide a minimal credential for the job
5. Prove a job's authenticy, audit and log before execution.

We will work on...

1. A basic trust model
2. Requirements for a Grid job delegation credential providing strong accountability/traceability
3. Discussion and assessment of the different frameworks

Trust model outline



Grid Job Credential outline

Requirements for a delegation credential providing strong accountability/traceability

1. Prove the actual submission by the user (actually by someone possessing the private key of the user's certificate)
2. Be unusable for other purposes
3. As such, implement a restricted and definite delegation of a task (the job)