Highlights (1)

- The Belle II experiment uses the DIRAC system to manage all its distributed computing resources, including cloud/grid sites and local clusters.
- BelleII@home aims at harnessing a big amount of volunteer computers which becomes part of the Belle II distributed computing resources.
- The DIRAC system requires user credentials stored on its computer nodes to communicate with the DIRAC services. The implementation of its pilot is extremely closely coupled with credentials requirements.
- Volunteer computers are not trustable. No credentials should be placed on them.
- Other similar projects which interact with DIRAC choose to place a user credential with minimum privileges on the volunteer computers. This is still **Dangerous**!

Highlights (2)

- We explore the possibility of detaching the payload running from the Belle II DIRAC pilot, so a gateway service can be deployed on a secure server and handle all the credential required operations of the job, also the payload can be executed on the volunteer computer without having any credentials.

- The prototype of BelleII@home proves the feasibility of this approach.

- With subtle modification, this can be applied generally to all volunteer projects and HPC systems which interact with the DIRAC system. It solves the security challenge for the volunteer projects, and outbound connectivity issues of HPC systems.