Secure gateway for Beauty@LHC
BOINC project for volunteer computing running LHCb simulation jobs

The problem:
- Pilot jobs need to contact central LHCbDirac services
  - Job matching
  - Job status update
- Jobs need to perform Data Management operations
  - Output file upload
- We don’t want to deploy real credentials (proxy or server certificate) on untrusted machines
- We need to check that the files to upload are clean
  - The machine owner might inject malicious data

The solution
- Split the world in two:
  - Untrusted world (the volunteer’s machine)
  - Trusted world (handled by LHCbDirac)
- Introduce a gateway between the two worlds
The two worlds and the gateway
In the untrusted world:
- Use fake credentials, using a fake CA (MrBoinc CA)
- Credentials are associated to the BOINC Id of the user
  - Their only role is to communicate between the VM and the gateway

In the trusted world:
- The GW uses server certificate to obtain jobs
- The GW uses the real credentials of the payload owner for DM operations
  - Obtained from the LHCbDirac proxy repository

The gateway (running on a CERN VOBox)
- Ensures the transition between the two worlds
- Queues Data Management request
  - Using the standard DIRAC Request Management System
  - Adding a special operation:
    - Validate output files (log files + output data)
    - Output data must be ROOT files
    - Logfiles must contain specific informations
Beauty@LHC is now ready for secure running

The secure gateway is operational and jobs are being run using internal volunteers

Next step: open to the general public
  - Before summer 2016