JobSub Authentication & Authorization

Table of Contents

Table of Contents

1 REVISION HISTORY 3

2 JOBSUB ARCHITECTURE 4

2.1 ARCHITECTURE DIAGRAM 4

3 JOBSUB SECURITY MODEL 4

3.1 USE CASES & DESIGN DECISIONS 4

3.2 JOBSUB CLIENT SECURITY & PROCESS FLOW 6

3.3 JOBSUB SERVER SECURITY & PROCESS FLOW 7

1 Revision History

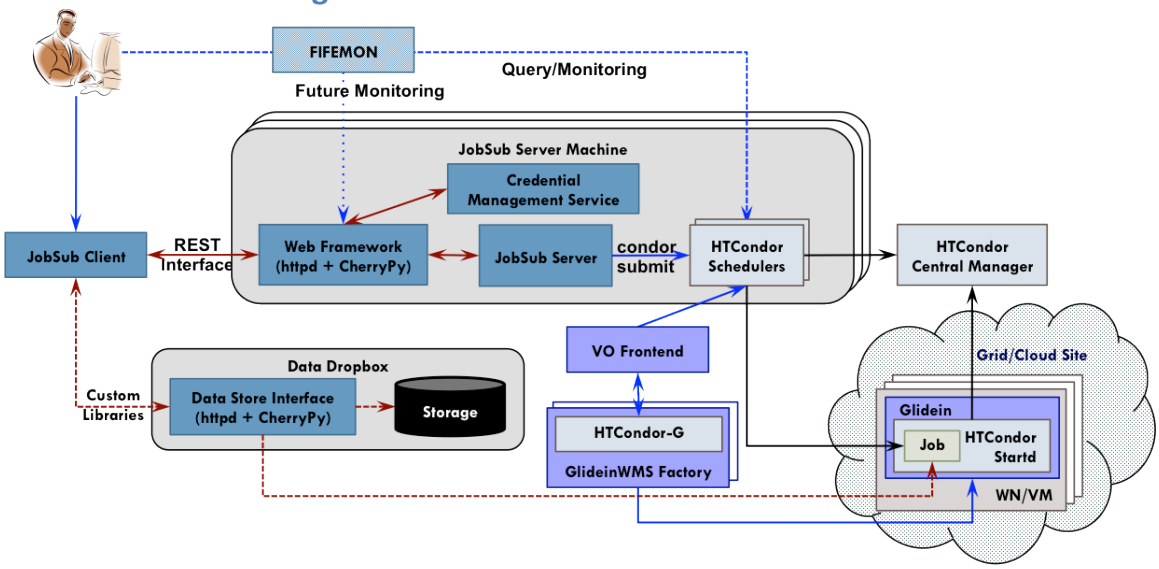
Version	Date	Author	Comments
V0.1	09/24/2014	Parag Mhashilkar	First draft
V0.2	10/01/2014	Parag Mhashilkar	Incorporated feedback from Dave Dykstra
V0.3	11/03/2014	Parag Mhashilkar	Clarified the admin group for job management as per Gerard's suggestions

2 JobSub Architecture

Additional documentation can be found in the JobSub project wiki.

Project Wiki	https://cdcvs.fnal.gov/redmine/projects/jobsub
Arch & REST API	https://cdcvs.fnal.gov/redmine/projects/jobsub/documents

2.1 Architecture diagram



3 JobSub Security Model

3.1 Use Cases & Design Decisions

The current security model in JobSub is designed to accommodate a wide range of use cases and user communities. These are highlighted below –

1. Client credentials
   a. User will provide JobSub client with one of the following credentials –
      i. Fermilab KCA issued krb5 ticket
      ii. X509 proxy
      iii. X509 user/service certificate
      iv. **FUTURE:** Ci-Logon token (?)
   b. Jobs will be submitted using X509 credentials. This restriction maybe lifted in future, however, it requires storage and WMS to work using some form of alternate secure method.

DESIGN DECISION:
If the X509 credentials are not provided to the JobSub client, it will convert user's krb5 ticket to X509 certificate-key pair using currently available tools like *kx509.*

2. JobSub is responsible for renewing the credentials used for job submission.

   DESIGN DECISION:
   The JobSub server needs access to the user's private key or use different set of credentials than that of the user to submit jobs. When different credentials are used, they will be added to the user's VOMS registration info automatically as part of the group/experiment on-boarding process. Additional details are in 5 below.

3. Analysis Jobs:
   a. Users submitting analysis jobs should be protected from each other.
   b. All users belonging to same group (aka experiment) should be able to read logs from group's jobs.
   c. Analysis jobs should be queued as individual users.
   d. A group of users from each experiment should be given admin privileges. This group should be allowed to manage their group's jobs and job priorities. One way to create this group is to assign VOMS Role ***admin*** to selected individuals. Details on admin group needs further discussion with FIFE working group and the service operations group.

   DESIGN DECISION:
   There should be privilege separation between the users when submitting & managing the analysis jobs. This can be achieved since the HTCondor daemons will be started as root. When a client sends request to the server with FQAN for non-production (Analysis) roles, the server can change privileges to mapped user login to perform any action. Given the DN+FQAN information to the GUMS server, call to, *'gums mapUser'* returns this user login. Initial testing demonstrated that querying GUMS server using the GUMS client is quite slow and not scalable. Another client tool *llrun* is scalable and provides the required functionality.

4. Production Jobs:
   a. Users belonging to production should be able to submit and manage jobs submitted with the production role.
   b. Jobs should be queued as production account.
   c. A group of users from each experiment should be given admin privileges. This group should be allowed to manage their group's jobs and job priorities.

   DESIGN DECISION:
   When a client sends request to the server with FQAN for production roles, multiple users will be mapped to same local (production) account on the server. Any user with that FQAN can perform any action on the jobs with this role.

5. HTCondor Daemons on the JobSub server
    a. HTCondor daemons will be started as user root.
    b. Based on the type of jobs, jobs should be queued as production account or individual user account.
    c. Users do not have login access to the server nodes.

DESIGN DECISION:
User accounts will be made available on the Jobsub server machine but the login access will be restricted. Also, each account has X509 certificate-key pair with a distinguish name ***DN'*** that is different than the ***DN*** of the user's X50 credential. This cert/key pair is used to generate VOMS proxy, which will be periodically refreshed and is used for job submission & management. The certificate-key pair will be derived from the special keytab generating KRB5 keytab file for individual account mapping or a Digi-Cert for group accounts.

3.2 Jobsub Client Security & Process Flow

- User provides credentials to the client in the form of X509 or KRB5 credentials.
- Non-X509 credentials are converted to X509. For this explanation lets assume the distinguish name is ***DN***.
  DN = '/DC=gov/DC=fnal/O=Fermilab/OU=People/CN=Parag A. Mhashilkar/CN=UID:parag'
- VOMS extensions maybe provided in the form of VOMS proxy or through command line options. For this explanation lets assume they are ***FQAN***
  FQAN (prod) = '/fermilab/fife/Role=prod/Capability=NULL'
  FQAN (analysis) = '/fermilab/fife/Role=analysis/Capability=NULL'
  FQAN (admin) = '/fermilab/fife/Role=admin/Capability=NULL'

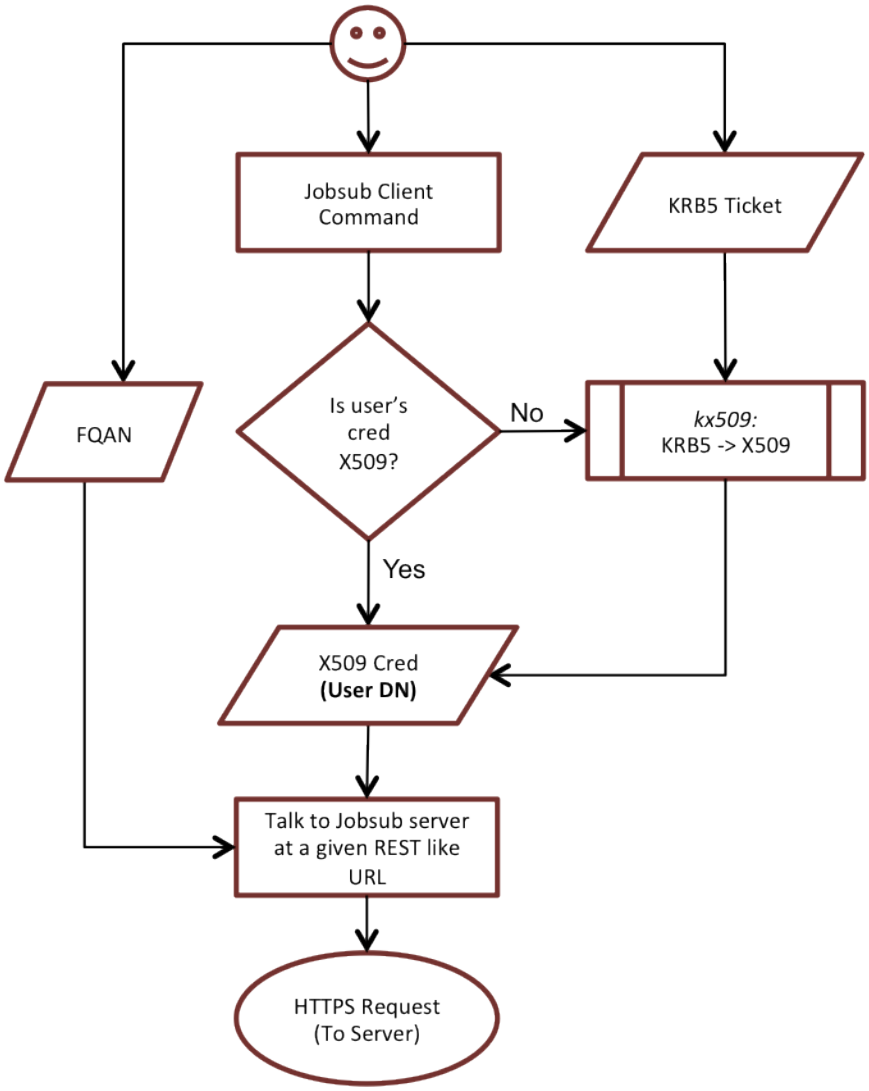


Figure 1: JobSub Client Security Flow

3.3 Jobsub Server Security & Process Flow

- Jobsub client presents server with the above mentioned credentials that have ***DN+FQAN***
- Given this ***DN+FQAN*** the Jobsub server gets the mapping from the GUMS server.
  Local Account (prod) = fifeprod
  Local Account (analysis) = parag
  Local Account (admin) = fifeadmin
- Based on the mapping, the Jobsub server
  - Identifies the X509 certificate-key pair with distinguish name ***DN'*** to use. In case of analysis, a special keytab is used to generate user specific robot keytab file. This user's robot keytab file is converted to X509 cert-key pair using tool *kx509*.

DN' (analysis) = '/DC=gov/DC=fnal/O=Fermilab/ OU=Robots/CN=fifegrid/CN=batch/CN=Parag A. Mhashilkar/CN=UID:parag'
DN' (prod) = '/DC=com/DC=DigiCert-Grid/O=Open Science Grid/OU=Services/CN=fifeprod/fermicloud383.fnal.gov'
DN' (admin) = '/DC=com/DC=DigiCert-Grid/O=Open Science Grid/OU=Services/CN=fifeadmin/fermicloud383.fnal.gov'

- Generates VOMS proxy from cert with ***DN'+FQAN***
- sudo to appropriate local account

- Jobsub server uses this VOMS proxy with ***DN'+FQAN*** to service client's request.

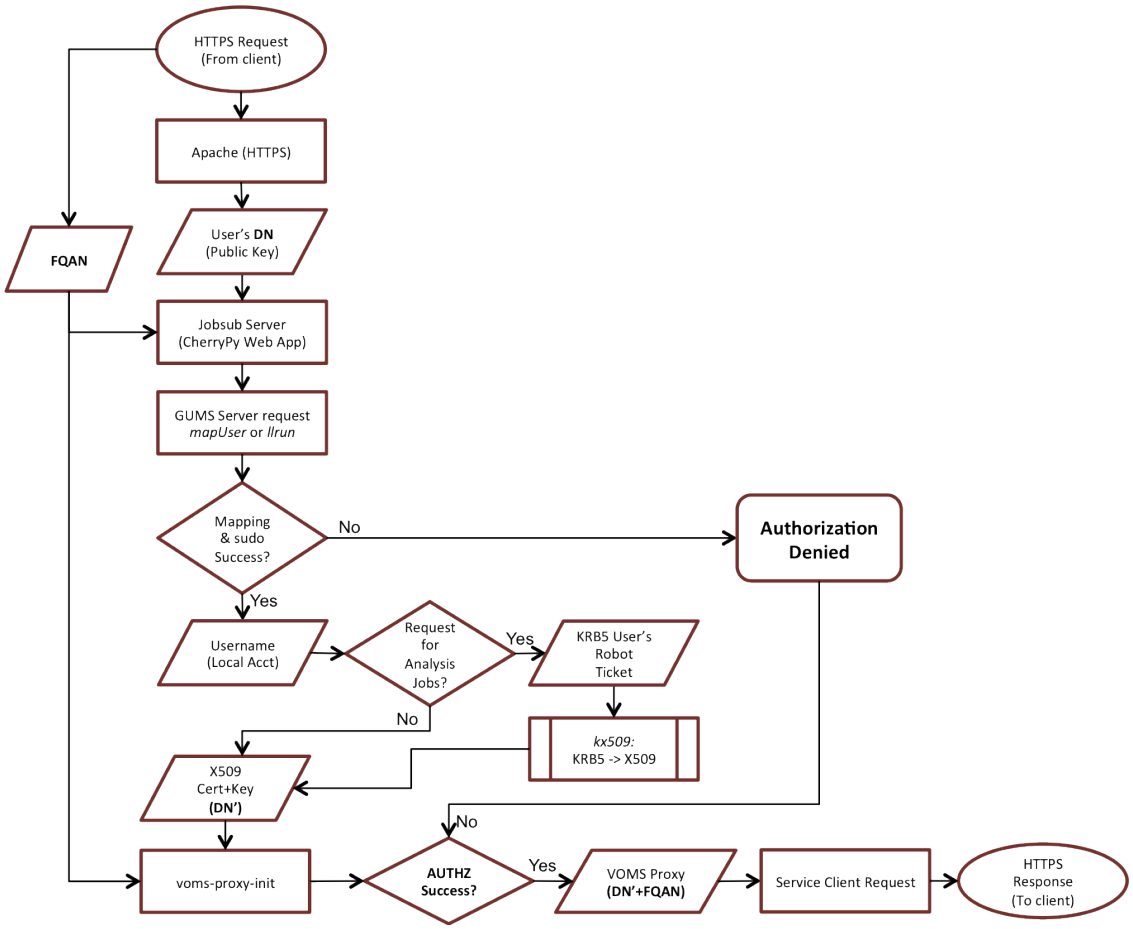


Figure 2: JobSub Server Security Process Flow