Mytoken

Goal

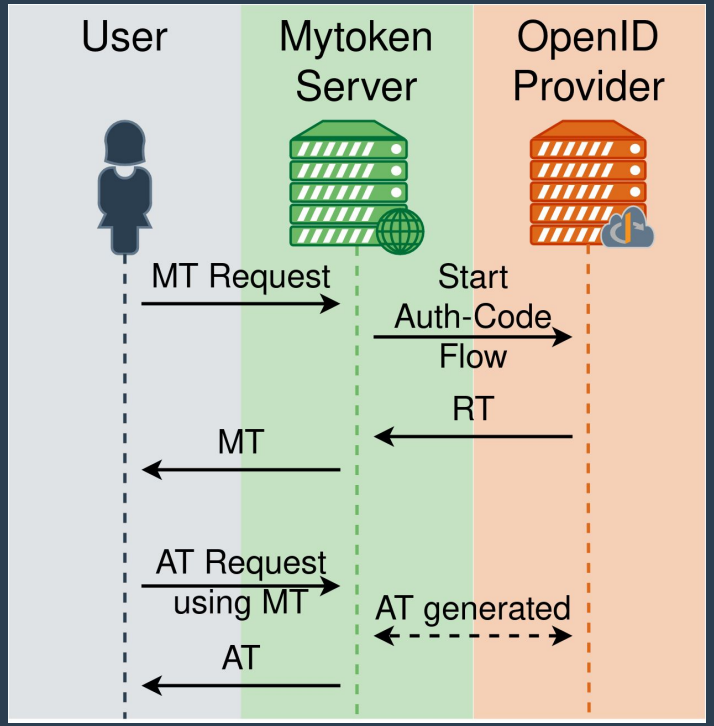
- Support for the “Long-running Jobs” requirements
- Other: Easy and secure way to obtain Access Tokens for Long-term Authorisation where Refresh Tokens are not suitable.

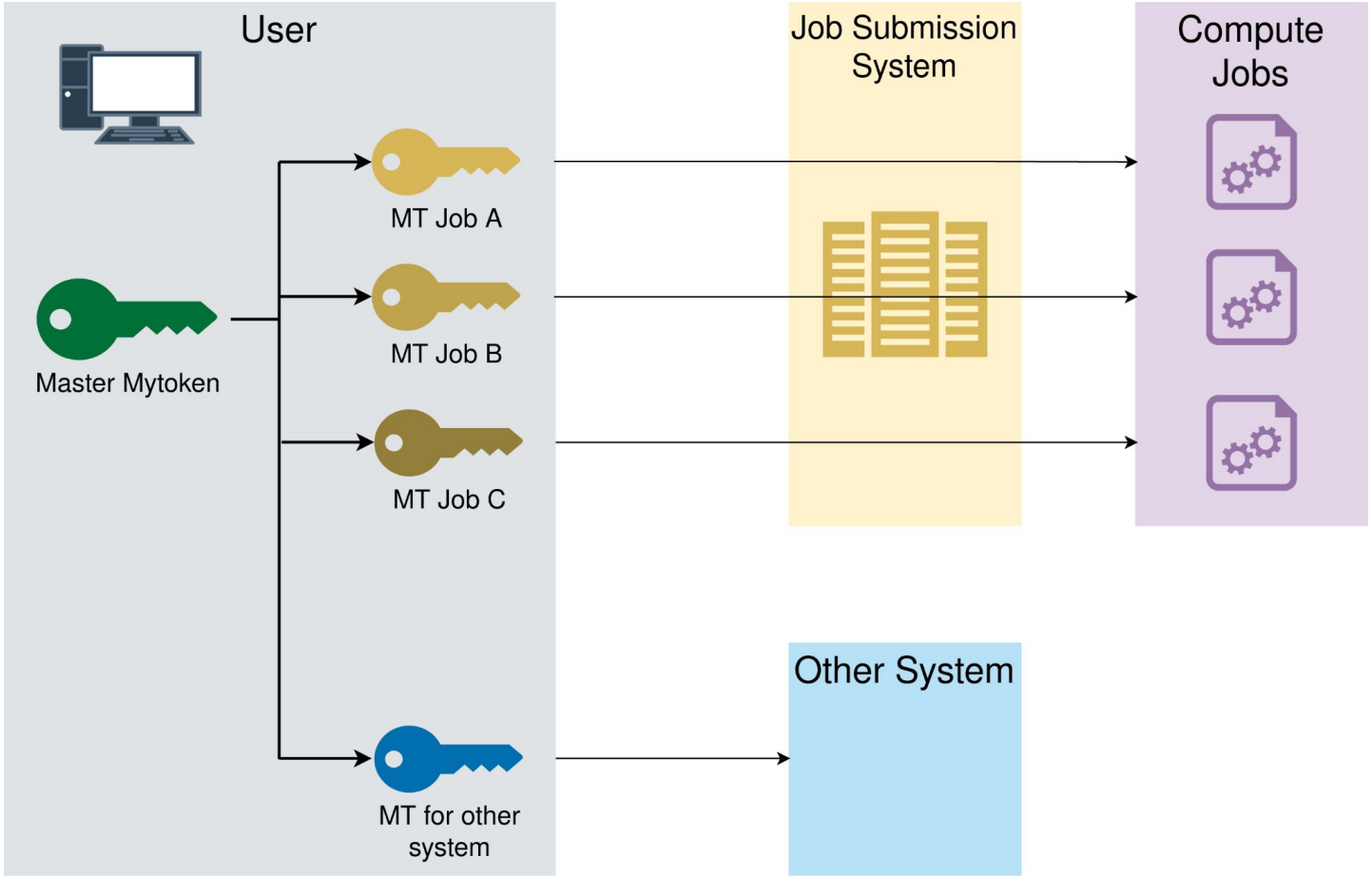
Basic Concept

- Similar concept to *myproxy* (i.e. secure storage of credentials)
- Mytoken can used as a Bearer Token that can be passed around
- Mytokens can be restricted (e.g. IP, aud) or used to obtain (restricted) AT

Mytoken can be created:

- From Authorization Code Flow
- From an existing Mytoken
- Other extensions possible





mytoken

Dedicated Mytoken for each usage can be easily created

Restrictions

- Using Bearer Mytokens as securely as possible
- Usage of each Mytoken can be restricted independently
- Very flexible approach
  - Different restriction dimensions (extensible)
  - Multiple privilege stages in one token possible

Restrictions

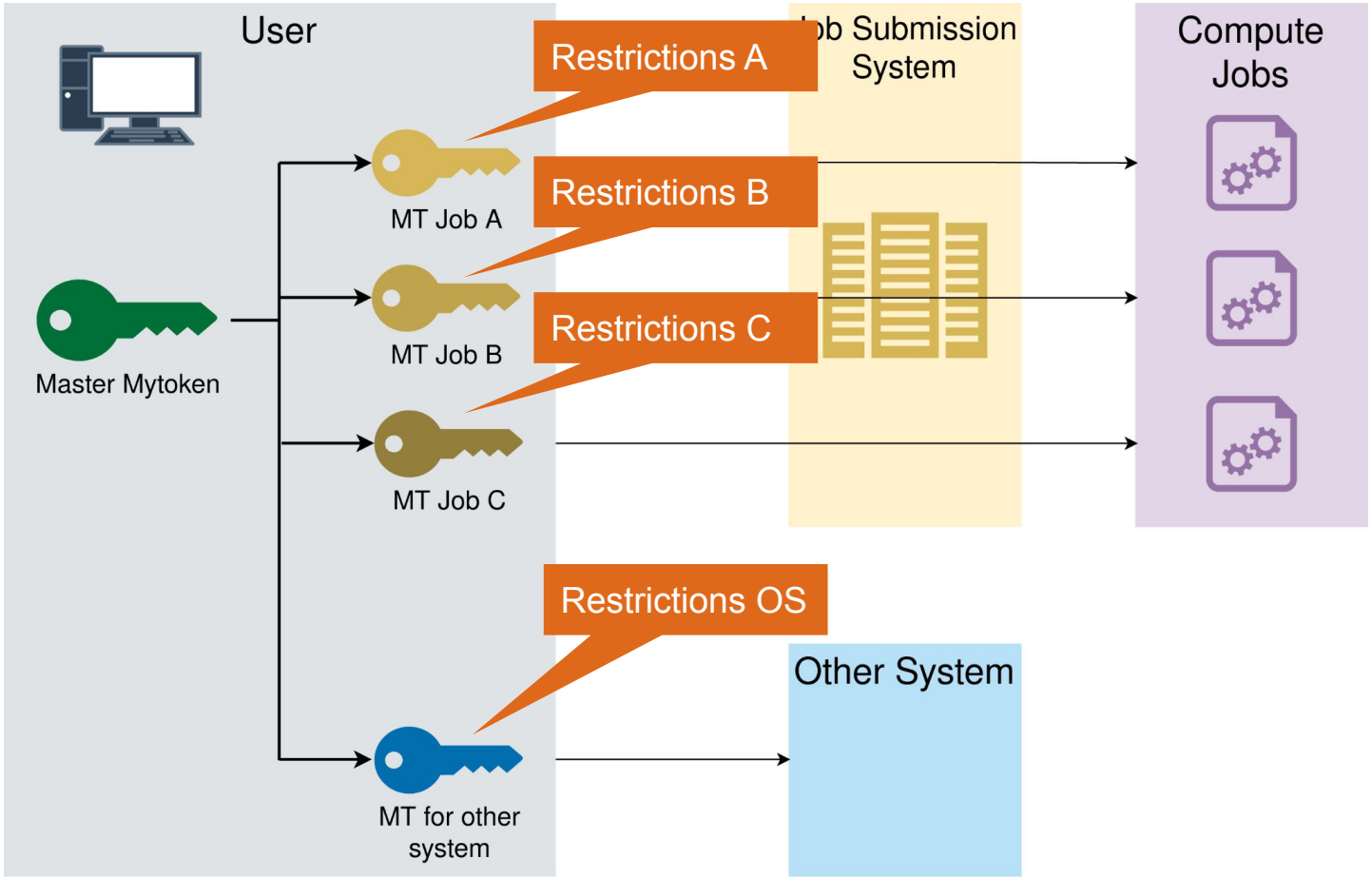
- Using Bearer Mytokens as securely as possible
- Usage of each Mytoken can be restricted independently
- Very flexible approach
  - Different restriction dimensions (extensible)
  - Multiple privilege stages in one token possible

- Time
  - **exp**: Only before this time
  - **nbf**: Only after this time
- Location
  - **ip**: Only from these IPs / Subnets
  - **geoip_allow**: Only from these countries
  - **geoip_disallow**: Not from these countries
- OIDC
  - **scope**: Only ATs with these scopes
  - **audience**: Only ATs with these audiences
- Usages
  - **usages_AT**: Only X ATs can be obtained
  - **usages_other**: Only X other actions can be performed

Restrictions

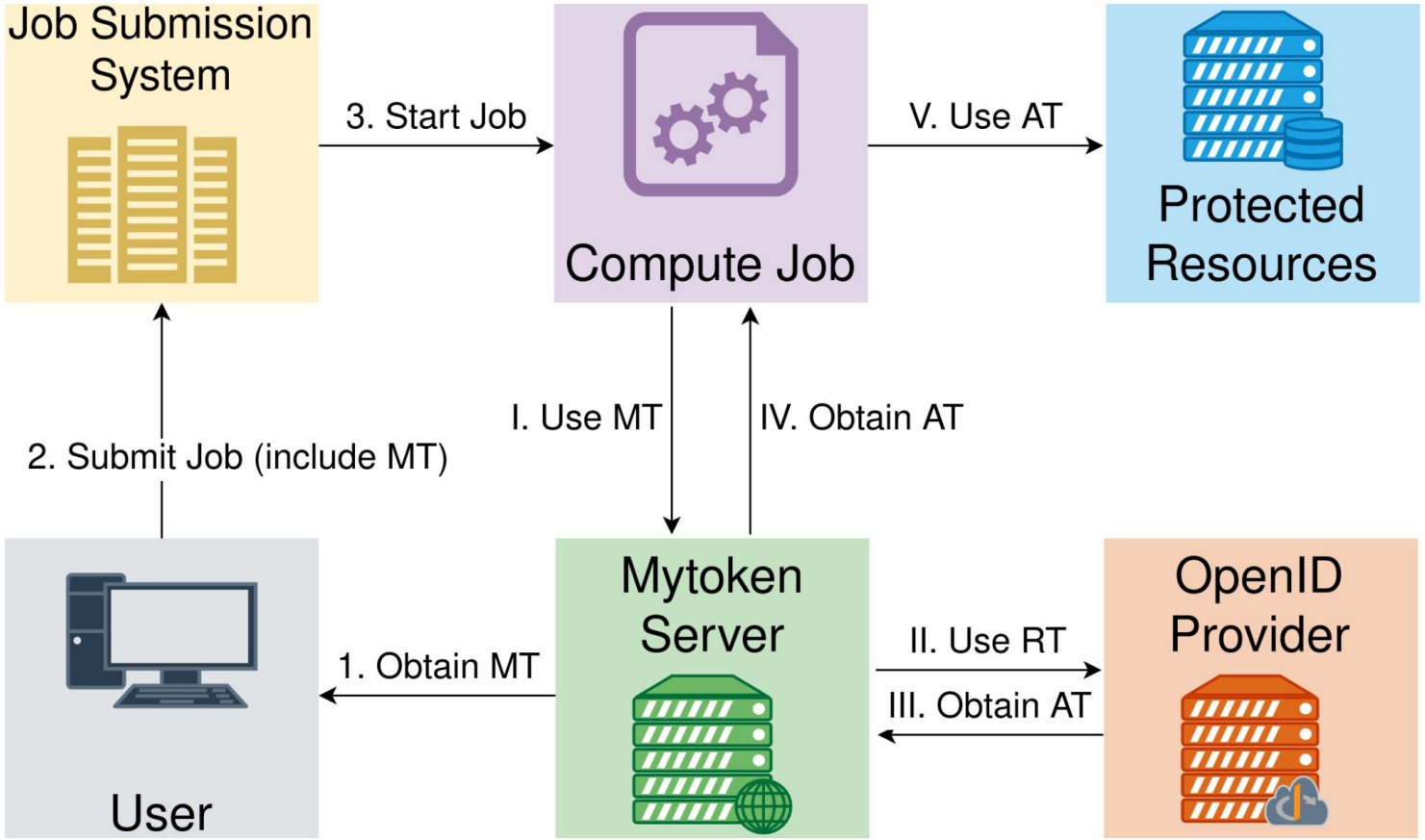
- Using Bearer Mytokens as securely as possible
- Usage of each Mytoken can be restricted independently
- Very flexible approach
  - Different restriction dimensions (extensible)
  - Multiple privilege stages in one token possible

- Job Submission
  - Only single AT with compute.create scope and https://hpc.example.com audience can be obtained
- Begin Job
  - Only single AT with storage.read and https://storage.example.com audience can be obtained
- During Job
  - No actions allowed
- End Job (after some time)
  - AT with storage.write and https://storage.example.com audience can be obtained



mytoken

Each Mytoken can (and should) have its own Restrictions


Job Submission System
3. Start Job
Compute Job
V. Use AT
Protected Resources
mytoken
2. Submit Job (include MT)
I. Use MT
IV. Obtain AT
User
1. Obtain MT
Mytoken Server
II. Use RT
III. Obtain AT
OpenID Provider

Backup-Slides