Adoption of a token-based authentication model for the CMS Submission Infrastructure

Marco Mascheroni\textsuperscript{1}, Jeff Dost\textsuperscript{1}, Saqib Haleem\textsuperscript{2}, A. Pérez-Calero Yzquierdo\textsuperscript{3}, Edita Kizinevic\textsuperscript{4}, Farrukh Aftab Khan\textsuperscript{5}, Hyunwoo Kim\textsuperscript{5} and Nikos Tsipinakis\textsuperscript{4} on behalf of the CMS Collaboration


CHEP 2023, May 11th 2023
Outline of the talk

● Why tokens?
● Token-based authentication in CMS Submission Infrastructure
● Current deployment status:
  ○ HTCondor CEs
  ○ ARC CEs
● Conclusions and Next steps
The CMS Submission Infrastructure

- **The CMS Submission Infrastructure:** team in CMS Offline and Computing in charge of:
  - Organizing HTCondor Software Suite (HTCSS) and GlideinWMS operations in CMS,
  - Maintaining a **Global Pool**, an infrastructure of distributed compute resources where reconstruction, simulation, and analysis of physics data takes place
  - Communicate CMS priorities to the development teams of glideinWMS and HTCondor

- **In practice:**
  - We operate a set of federated HTCSS pools which aggregate **resources from 70 Grid sites**, plus non-Grid resources
  - We regularly hold meetings with HTCSS and glideinWMS developers where we discuss current operational limitations, new feature requests and future scale requirements
The CMS Submission Infrastructure

- CERN
  - WMAgent T0 schedds
  - CRAB schedds
  - WMAgent schedds
  - WMAgent schedds
  - External CMS schedds
  - CERN Pool (Collector Negotiator)
  - CERN
  - BEER
  - HLT
  - WLCG
  - OSG
  - DODAS
  - HEPCloud
  - HEPCloud
  - Volunteer Pool (Collector Negotiator)
  - BOINC
  - BOINC
  - HPC/Cloud/Other

- FNAL
  - WMAgent schedds
  - External CMS schedds
  - External Pool (Collector Negotiator)

Submission Infrastructure Overview

submit flock
Overall SI architecture

CRAB Task Workers

SCHEDDs

GlideinWMS FRONTEND

COLLECTORS

CCB

GlideinWMS Factories

Compute Elements (CE)

Startds (GWMS Pilots)

Startds (Pilots)
Why tokens?

Motivations:

● Use de facto **standard** like OAuth in place of Grid specific ones (GSI)
  ○ Part of a general **WLCG campaign**

Advantages:

● Authorization based on token **capability** (vs identity) allows for finer handling of communications between entities

● Easier to follow **principle of least privilege**
  ○ **Limited impact** in case of credential leak, for example
  ○ Only affect Factory<=>CE communication

- Old pilot proxies were used in more places, e.g.: WN<=>Central Manager
Two different technologies

- **IDTOKENS** for HTCondor Software Suite components
  - New *native* condor authentication mechanism
  - JWT tokens signed with a *simmeric key*
  - Tokens generated with condor *command line interface* (even remotely)

- **SCITOKENS** for Grid sites (HTCondor-CEs + ARC-CEs)
  - Uses WLCG IAM go generate tokens
    - A client is registered and can fetch tokens on the GWMS Frontend
  - JWT tokens signed using *private/public schema*
  - Compute Elements (CEs) verify authenticity of tokens and authorize pilot job submission
Internal CMS Submission Infrastructure:
token authentication with IDTOKENS
WM to SI schedulers authentication

- Authentication of **Workload management tools** to schedulers switched almost **transparently**
  - Local authentication
- **User’s proxy** used for **remote** authentication (CRAB)
  - Switched to single service IDTOKEN
  - Development was necessary in CRAB to **switch from multiple users** mapped with Argus to **single user**
Condor components

- The whole Global pool is using IDTOKENS for authentication
  - HTCSS version 10 with no GSI fallback installed early April
- Multiple keys and tokens to minimize impacts in case of security incidents

Token transferred to WN by GWMS
Token manually requested
gn-glidelinWMS resources
/HPC/Vacuum STARTDs

WM Agents

T0 Schedd

Global CM

Backup CM

T0 CM

Backup CM
GlideinWMS authentication

- Lots of work to make GWMS ready to use tokens as well
  - New features for additional configuration in the next version
Overall authentication in SI

- IDTOKEN (WRITE) from CRAB TW to GWMS Frontend
- IDTOKEN READ from CRAB Schedd to Global CM
- IDTOKEN to Backup CM from Global CM
- IDTOKEN to T0 CM from Backup CM
- IDTOKEN to Backup CM from T0 CM
- IDTOKEN to CE from GWMS Factory
- IDTOKEN to CE from non-glideinWMS resources
- IDTOKEN to GWMS STARTDs from CE
- IDTOKEN to GWMS Factory from CE
- IDTOKEN to Glidein/Pilot Job from CE
- IDTOKEN to External Schedd from GWMS Factory
- IDTOKEN to T0 Schedd from GWMS Factory
- IDTOKEN to WM Agents from GWMS Factory
- IDTOKEN to CRAB Schedd from GWMS Factory

- scitoken from GWMS Frontend to GWMS Factory
- scitoken from CE to GWMS Factory
- scitoken from CE to non-glideinWMS resources
- scitoken from CE to GWMS STARTDs

Resources:
- CRAB TW
- Remote submission tool
- IDTOKEN
- GWMS Factory
- Global CM
- Backup CM
- T0 CM
- Backup CM
- WM Agents
- External Schedd
- T0 Schedd
- scitoken
- Glidein/Pilot Job
- non-glideinWMS resources
- /HPC/Vacuum
- STARTDs
Token authentication to sites with SCITOKENS
Ways to submit jobs to the Grid

- Factory submits pilots using HTCondor
  - Sites use two CE technologies
    - Completed 100% (both OSG and EGI sites, last site January)

- HTCondor submission
  - ARC-CEs submission:
    - Through LDAP interface and GSI proxies
      - Deprecated in HTCondor 10 series
    - New REST interface available
      - Support for tokens
      - Plain X509 proxies can be used (no GSI)
ARC CE REST interface

- **Current focus** in factory operations

- **Campaign with sites to enable ARC-CE REST** interface and configure them to accept tokens
  - Tests in ITB to not affect working sites
  - 12 CEs do not work out of 45 CEs (or 5 sites out of 25)

- **Split configuration with UCSD factory using REST** and **CERN using old LDAP interface**
  - To guarantee **seamless transition** (no fallback to proxy for pilot submission)

- **Few issues** found with **scale** usage
  - Memory leak of arc_gahp on rhel7
  - Job in run state forever under certain circumstances
  - Submission timeouts due to condor request serialization
Conclusions

- CMS Submission Infrastructure internal components fully switched to IDTOKENS in Spring 2022
- Communication to HTCondor-CE sites with SCITOKEN to 100% of the sites by Autumn 2022
- Improved secret management
  - GSI secrets needed minimal maintenance as they used one certificate per-host
  - IDTokens need to be securely generated, stored, and distributed to their intended user
    - Introduced usage of Teigi for secret storage

Future Work:

- Complete token transition
  - Disable GSI fallback in the global pool
- Retire ARC-CE LDAP interface
- Security “drill exercises”
Acknowledgements

Projects FPA2016-80994-C2-1-R, PID2019-110942RB-C21, BES-2017-082665 and PID2020-113807RA-I00 funded by:

US National Science Foundation
Grant No. 2121686
Backup Slides
The CMS Submission Infrastructure (SI) is the main computing resource provisioning system for CMS workloads. A number of HTCondor pools are employed to manage this infrastructure, which aggregates geographically distributed resources from the WLCG and other providers. Historically, the model of authentication among the diverse components of this infrastructure has relied on the Grid Security Infrastructure (GSI), based on identities and X509 certificates. In contrast, commonly used modern authentication standards are based on capabilities and tokens. The WLCG has identified this trend and aims at a transparent replacement of GSI for all its workload management, data transfer and storage access operations, to be completed during the current LHC Run 3. As part of this effort, and within the context of CMS computing, the Submission Infrastructure group is in the process of phasing out the GSI part of its authentication layers, in favor of IDTokens and Scitokens. The use of tokens is already well integrated into the HTCondor Software Suite, which has allowed us to fully migrate the authentication between internal components of SI. Additionally, recent versions of the HTCondor-CE support tokens as well, enabling CMS resource requests to Grid sites employing this CE technology to be granted by means of token exchange. After a rollout campaign to sites, successfully completed by the third quarter of 2022, the totality of HTCondor CEs in use by CMS are already receiving Scitoken-based pilot jobs. On the ARC CE side, a parallel campaign was launched to foster the adoption of the REST interface at CMS sites (required to enable token-based job submission via HTCondor-G), which is nearing completion as well. In this contribution, the newly adopted authentication model will be described. We will then report on the migration status and final steps towards complete GSI phase out in the CMS SI.