An evolving document that intends to capture all deployment intricacies
• We are aiming for transparent replacement of X509 + VOMS with tokens in a steadily increasing number and variety of workflows
• Deployment started during LS2, to be completed during Run 3

Presents a provisional timeline with tentative milestones

Steady progress, though several milestones had to be postponed
• See next pages
INDIGO IAM recap

- **INDIGO IAM** will replace VOMS(-Admin)
  - Identity and Access Management

- Integrates federated identities through CERN SSO plugin

- Obtains LHC experiment membership details from the CERN HR DB
  - Just like VOMS-Admin

- Can issue fine-grained tokens to users and services
  - Details depend on the configuration per VO and per workflow

- Also has a VOMS endpoint for backward compatibility
  - Users will still have their X509 certificates linked for now

- It does **not** have a VOMS-Admin endpoint
  - Classic grid-mapfiles etc. have to be constructed using the IAM SCIM API
  - For any IAM instance, all SCIM API clients have to be **registered**
Deployment state of affairs

- IAM is in production for ATLAS and CMS
  - Contents automatically replicated from VOMS-Admin
  - IAM VOMS endpoints are used alongside the legacy VOMS services
  - Legacy services will be switched off when IAM services look mature
    - See later

- ATLAS, CMS and SAM ETF can use tokens to submit jobs to HTCondor CEs
  - In particular the CEs on OSG, which will stop supporting X509 by May 1st

- Those jobs still use X509 VOMS proxies for data management etc.

- For ALICE and LHCb these matters are WIP and less urgent
Other near-term aspects

- HTCondor CE: **X509 support EOL** planned for November this year
  - Token configuration details are documented *and* under discussion
  - A deployment campaign will be launched after that has converged

- ARC CE: no plans for X509 support EOL yet
  - Tokens currently are supported for jobs without ARC data handling

- Agreements have been reached on token workflows involving FTS and/or Rucio
  - Details are being looked into by development teams and discussed in the WG
    - For example in the Rucio meeting on March 3
  - Prototype implementations and workflows are expected this year and will be integrated into production during Run 3 as they mature
Auxiliary services

- Services resembling MyProxy will help simplify things for users and robot workflows

- HashiCorp Vault + `htgettoken` already in production at FNAL
  - Presented in the April GDB, 2021
  - To be tried out at CERN
    - A Vault service already exists

- *MyToken* already in use for EOSC Synergy infrastructure monitoring
  - Presented in the AuthZ WG meeting of 2 Sep 2021
  - It allows tokens and workflows to be restricted in more ways
Smoothing the transition

- Several measures were agreed to help smooth the transition from X509 to tokens in the coming months (notes)

- HTCondor CE X509 support on OSG has been extended to May 1st

- The IAM service support level at CERN currently is envisaged to be “8/7” by then
  - 8/5 plus daily checks during weekends and holidays

- Pilot job submission tokens will initially have lifetimes of a few days
  - Some development is needed to make that more configurable

- Long lifetimes will be reduced when sufficient positive experience has been obtained with the reliability and the support level of the IAM services

- In the future, data management tokens will require much shorter lifetimes for the desired level of security

- The service deployment will be made as HA as feasible
  - Thanks especially to the development team at CNAF!
Globus retirement implications & prospects

- By May 1st, OSG should no longer depend on “Globus”, i.e. the Grid Community Toolkit (GCT)
  - No more X509 support for job submissions to OSG
  - Only dCache *can* still support GridFTP

- By November, no supported HTCondor release depends on the GCT ([link](#))
  - No more X509 support for job submissions to HTCondor CEs in EGI
  - HTCondor-G can still use X509 to submit jobs to ARC CEs via their REST interfaces

- The GridFTP protocol has mostly been phased out in WLCG
  - DOMA Bulk Data Transfer WG to follow up on remaining usage
  - Sites may need to keep supporting it for other VOs until those have also switched to HTTPS+WebDAV and/or Xrootd

- The GCT is maintained by the [Grid Community Forum](#) at best-effort level
  - Latest updates were released on 3 Sep 2021
  - RPMs are even published already in EPEL 9
  - We will need various components until the transition to tokens has been completed