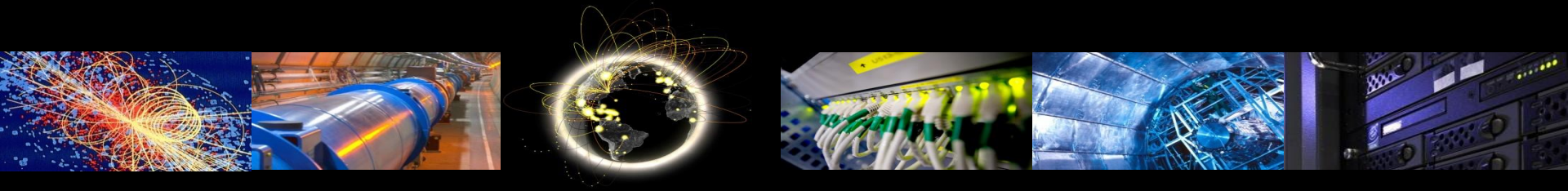
Authored by the WLCG AuthZ WG

Tokens in WLCG - Introduction

WoTBAn&Az

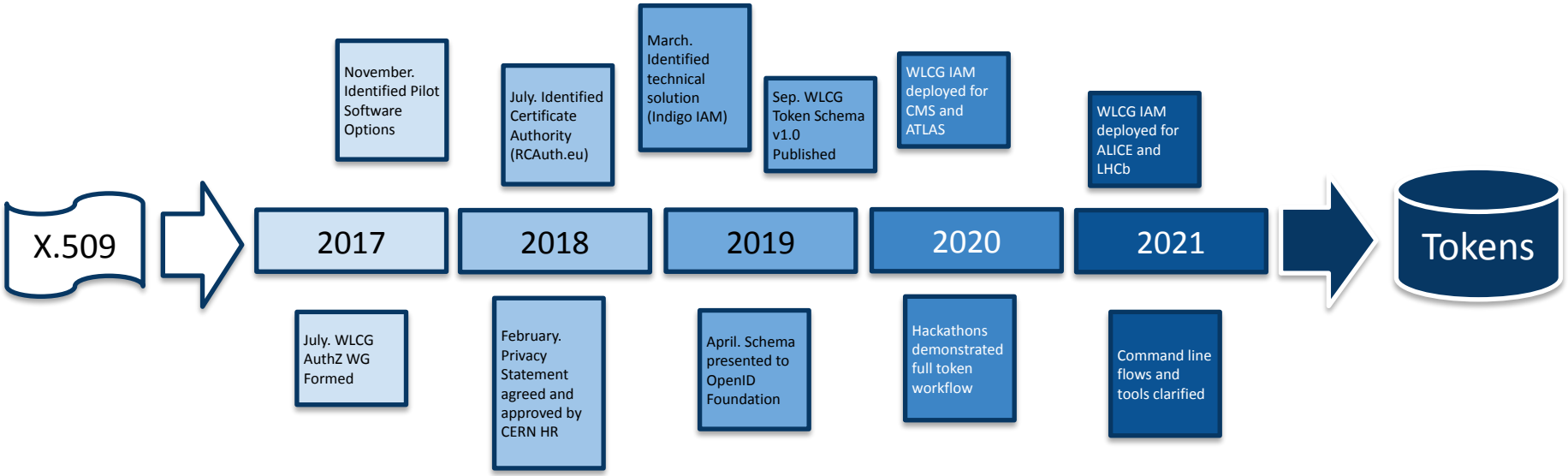
October 18th 2021



Overview

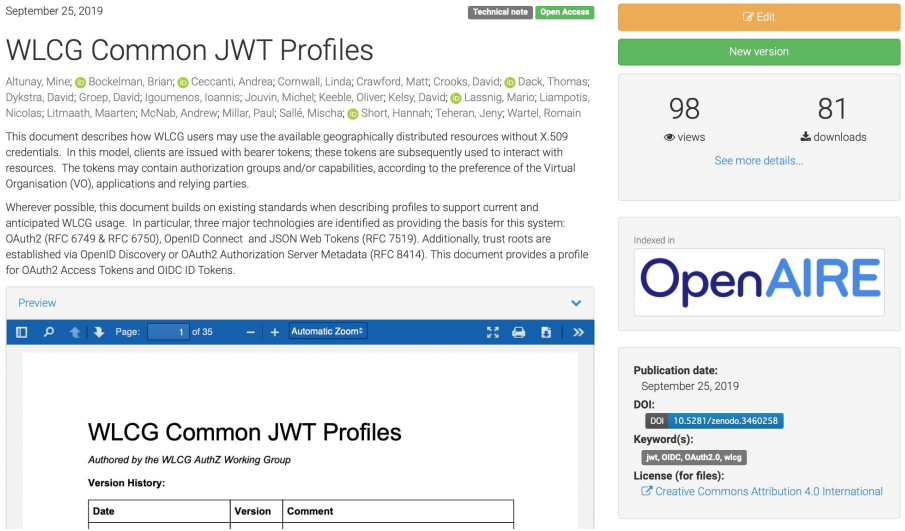
- WLCG (Worldwide LHC Computing Grid) used for high energy physics data analysis
- Since 2000s has relied on X.509 certificates for client and user authentication, and VOMS for authorization
- Since 2017 have been looking to move to JWT tokens over OAuth2.0
  - WLCG Authorization Working Group meets every 2 weeks

Towards Tokens



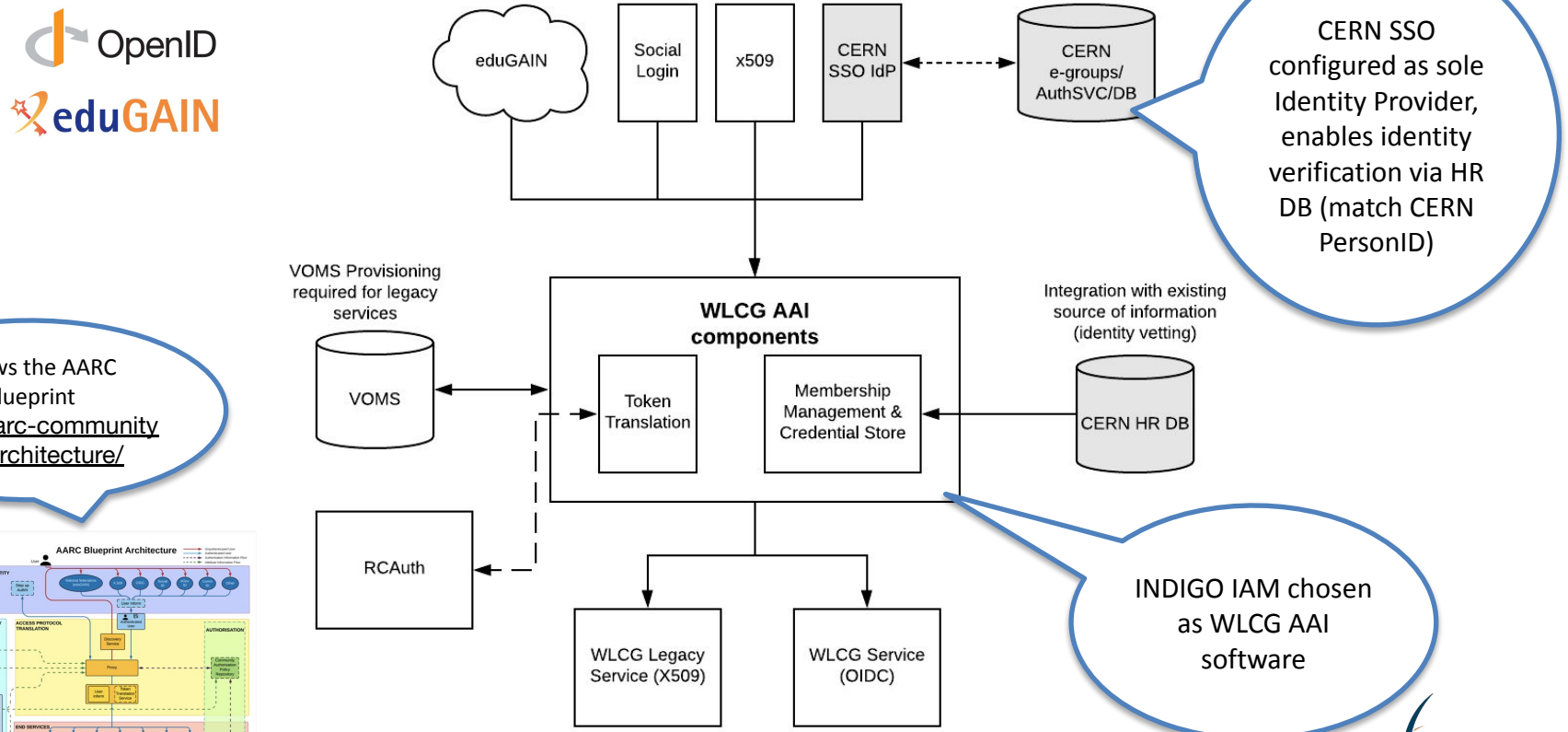
WLCG Token Schema V1.0

- Published on Zenodo, September 25th 2019
- Allows middleware developers to enable token based authorization to an agreed schema
- Working document at https://github.com/WLCG-AuthZ-WG/common-jwt-profile

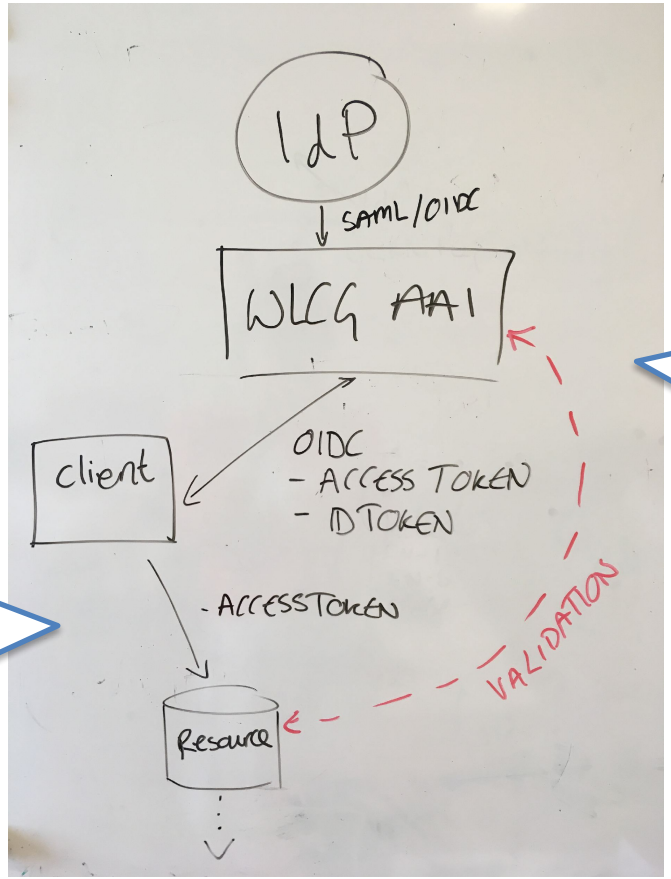


https://zenodo.org/record/3460258#.X8ED_i1Q1qs

AAI Design


eduGAIN
Social Login
x509
CERN SSO IdP
CERN e-groups/ AuthSVC/DB
CERN SSO configured as sole Identity Provider, enables identity verification via HR DB (match CERN PersonID)
VOMS Provisioning required for legacy services
VOMS
WLCG AAI components
Token Translation
Membership Management & Credential Store
Integration with existing source of information (identity vetting)
CERN HR DB
RCAuth
WLCG Legacy Service (X509)
WLCG Service (OIDC)
INDIGO IAM chosen as WLCG AAI software
Follows the AARC Blueprint https://aarc-community.org/architecture/
AARC Blueprint Architecture

Anticipated Token Flows



Small number of registered clients, large number of unregistered resources

Usability of command line flows proving more complex than anticipated! Discussions ongoing in the WLCG Authorization Working Group

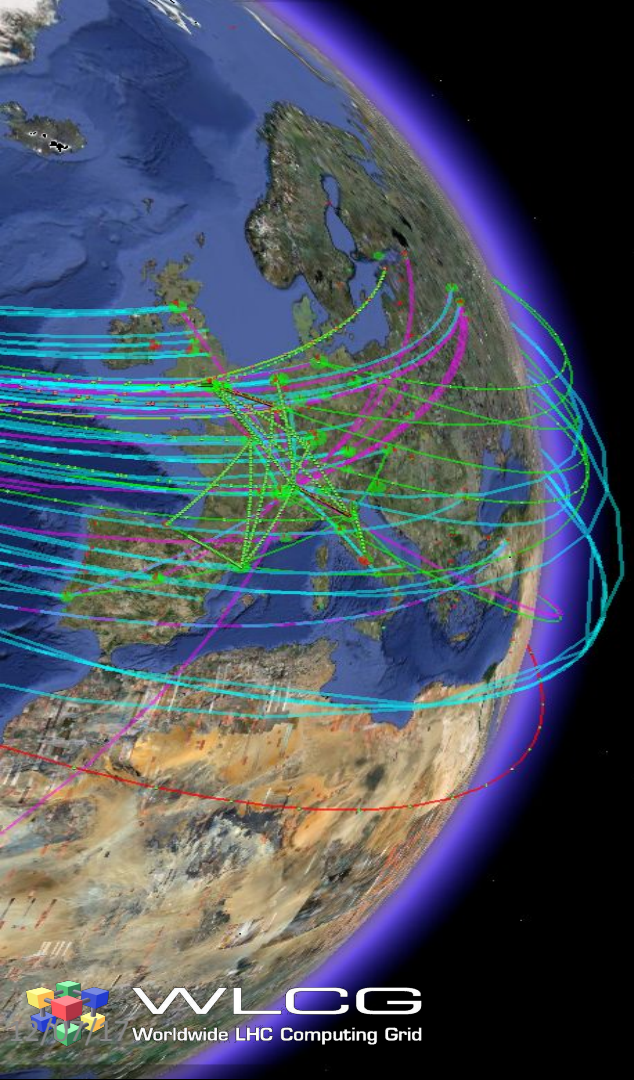
Certificate fadeout

- X.509 will continue to play a vital role in our infrastructure as host certificates, but users will no longer need to manage the certificate lifecycle themselves
- It is likely that power users, e.g. admins, may need to manage certificates for much longer
- This is a very early plan and significant changes are expected

	2019	2020	2021	2022	2023
Integrate RCAuth.eu for on-demand IOTA X.509					
Migrate VOs to IAM, retire VOMS Admin					
Add Token support to Middleware					
Dual mode (IAM issues X.509/VOMS and Tokens)					
Privilege Tokens, analyse remaining X.509 use					
Begin removing X.509 User Certificate Support					

Today's Talks

Time	Item	Speaker
5m	Introduction	Hannah Short (CERN)
20m	Lightning talk: Fermilab	Mine Altunay, Dave Dykstra (Fermilab)
	Lightning talk: CERN - WLCG IAM deployment	Hannah Short (CERN)
	Lightning talk: CiLogon and WLCG	Jim Basney (Uni Illinois)
	Lightning Talk: Condor with Vault	Dave Dykstra (Fermilab)
10m	IAM Development Roadmap	Andrea Ceccanti (INFN)



Questions?