CMS Token Transition

Strategy and Status

Brian Bockelman, on behalf of the co-authors and the CMS Collaboration



Many thanks to the co-authors

- Moving an experiment's authorization model forward is not a light lift! I'd like to start by acknowledging the co-authors.
 - Alan Malta Rodrigues (University of Notre Dame (US))
 - Brian Paul Bockelman (University of Wisconsin Madison (US))
 - Chan-Anun Rungphitakchai (University of Wisconsin Madison (US))
 - Dave Dykstra (Fermi National Accelerator Lab. (US))
 - Diego Ciangottini (INFN, Perugia (IT))
 - Edita Kizinevic (CERN)
 - Eric Vaandering (Fermi National Accelerator Lab. (US))
 - Marco Mascheroni (Univ. of California San Diego (US))
 - Panos Paparrigopoulos (CERN)
 - Rahul Chauhan (CERN)
 - Sarun Nuntaviriyakul (Chulalongkorn University (TH))
 - Stephan Lammel (Fermi National Accelerator Lab. (US))
 - Vaiva Zokaite (Vilnius University (LT))





Authorization, authentication, and credentials: A recap

Three important terms for this presentation:

- Authorization: Deciding whether an entity is permitted to perform an action.
- Authentication: Mapping an entity to an identifier.
 - Note: Authentication is often part of an authorization scheme.
- Credential: knowledge that establishes a fact (e.g., identity).
 - Not too far off from the 'credentials' the university provides: a diploma establishes the bearer has particular knowledge.
 - Classic example: a username/password is used as a credential to perform authentication.





Moving from identity mapping to capabilities

- Authorization on WLCG was always based on identity mapping*:
 - A request was authenticated to a global identity.

REARLES

SCIENCE

- The global identity was mapped to a local identity.
- The request was <u>authorized</u> if the local identity was authorized to perform the action.

<u>Scheme</u>	Credentials	Authentication	Authorization
Gmail login	Password, 2FA	Username	Access to your inbox
Building access	ID card	Identity in HR database	Elevators
International Travel	Passport	Identity according to US Government	Enter Switzerland
Baseball Game	Ticket	NONE!	Sit in section 4, seat 34B
Workshop	Zoom URL	NONE!	Attend this wonderful talk!

morgridge.org



PRICE & ALL TAXES INCL

ADULT

55.00

EYS0416

55.00

SECTION / BOX

ROW / SEAT

A 18

513X CA 31MAR08 ZWS752

A

18 \$

New York Yankees

BOSTON RED SOX

YANKEE STADIUM

M20

23 2000

THE FINAL SEAS

MAIN RES SEC 20

A transition in Two Ways -> Credentials

X.509

JWT

BEGIN CERTIFICATE	Certificate:				
MIIIzjCCBragAwIBAgITbgBUyVBjktiAr/TUCAAAAFTJUDANBgkqhkiG9w0BAQ0F	Data:				
ADBWMRIwEAYKCZImiZPyLGQBGRYCY2gxFDASBgoJkiaJk/IsZAEZFgRjZXJuMSow	Version: 3 (0x2)				
KAYDVQQDEyFDRVJ0IEdyaWQgQ2VydG1maWNhdG1vbiBBdXRob3JpdHkwHhcNMjAw	Serial Number:				
ODE4MjA1NDI5WhcNMjEwOTIyMjA1NDI5WjCBlTESMBAGCgmSJomT8ixkARkWAmNo	6e:00:54:c9:50:63:92:d8:80:af:f4:d4:08:00:00:00:54:c9:50				
MRQwEgYKCZImiZPyLGQBGRYEY2VybjEWMBQGA1UECxMNT3JnYW5pYyBVbml0czE0	Signature Algorithm: sha512WithRSAEncryption				
MAwGA1UECxMFVXNlcnMxETAPBaNVBAMTCGJib2NrZWxtM08wD0YDV00DEwY2NTk4	Issuer: DC=ch, DC=cern, CN=CERN Grid Certification Authority				
NjkxHTAbBgNVBAMTFEJyaWFuIFBhdWwgQm9ja2VsbWFuMIIBIjANBgkqhkiG9w0B	Validity				
AQEFAAOCAQ8AMIIBCgKCAQEAi53glUNf5tPI4fslPo6HfFenSplb07sIa1fI2ug0	Not Before: Aug 18 20:54:29 2020 GMT				
M72LGOswDHj65P10MKEoh8YVhj8XW3jdnb3h45NxWiRqjR07pRW9LY5LsVkmJwt0	Not After : Sep 22 20:54:29 2021 GMT				
ØEHEM3VHnwjrhCjNpgg5aacYGUaD1d0deD91IAlSlKmBEoR5ZW/Y2meOymUzDVeV	Subject: DC=ch, DC=cern, OU=Organic Units, OU=Users, CN=bbockelm, CN=659869, CN=Brian Paul Bockelman				
/esj0BqN5VthJqhoxC3AfVJICVHY4BcoHA2wlA/sx3B4jADxSihy9vTM00cH9mbQ	Subject Public Key Info:				
MO+8CTszlholbxLs2ah8MB0BCK04wPY4f4uP9iv0Hf4FaNiYUcHAk008ftT0dTNs	Public Key Algorithm: rsaEncryption Public-Key: (2048 bit)				
0Iu+0awCIPMb/aIviX98+mav5P7MJXC/k0aljjl9hz9kx0IDA0ABo4IEUzCCBE8w	Public-Key: (2048 bit) Modulus:				
HQYDVR00BBYEFE8pv/HJDn60VikdQlP1MMAjZccDMB8GA1UdIwQYMBaAFKWg/WZY	00:8b:9d:e0:95:43:5f:e6:d3:c8:e1:fb:25:3e:8e:				
/bndeuGynZ+j0eV0GJTnMIIB0AYDVR0fBIIBLzCCASswagEnoIIBI6CCAR+GTmh0	87:7c:57:a7:4a:99:5b:d3:bb:08:6b:57:c8:da:e8:				
dHA6Ly9jYWZpbGVzLmN1cm4uY2qvY2FmaWx1cy9jcmwvQ0VSTiUyMEdyaWQ1MjBD	0e:33:bd:8b:18:eb:30:0c:78:fa:e4:fd:50:30:a1:				
ZXJ0aWZpY2F0aW9uJTIwQXV0aG9yaXR5LmNybIaBzGxkYXA6Ly8vQ049Q0VSTiUy	28:87:c6:15:86:3f:17:5b:78:dd:9d:bd:e1:e3:93:				
MEdyaWQ1MjBDZXJ0aWZpY2F0aW9uJTIwQXV0aG9yaXR5LENOPUNFUk5QS0kwNSxD	71:5a:24:6a:8d:13:bb:a5:15:bd:2d:8e:4b:b1:59:				
Tj1DRFAs0049UHVibGljJTIwS2V5JTIwU2VydmljZXMs0049U2VydmljZXMs0049	26:27:0b:74:d0:41:c4:33:75:47:9f:08:eb:84:28:				
029uZmlndXJhdGlvbixE0z1jZXJuLERDPWNoP2N1cnRpZmljYXRlUmV2b2NhdGlv	cd:a6:08:39:69:a7:18:19:46:83:d5:dd:1d:78:3f:				
bkxpc3Q/YmFzZT9vYmp1Y3RDbGFzcz1jUkxEaXN0cm1idXRpb25Qb2ludDCCAWIG	75:20:09:52:94:a9:81:12:84:79:65:6f:d8:da:67:				
CCsGAQUFBwEBBIIBVDCCAVawywYIKwYBBQUHMAKGV2h0dHA6Ly9jYWZpbGVzLmN1	8e:ca:65:33:0d:57:95:fd:eb:23:d0:1a:8d:e5:5b:				
cm4uY2gvY2FmaWx1cy9jZXJ0aWZpY2F0ZXMvQ0VSTiUyMEdyaWQ1MjBDZXJ0aWZp	61:26:08:68:c4:2d:c0:7d:52:48:09:51:d8:e0:17:				
Y2F0aW9uJTIwQXV0aG9yaXR5LmNydDCBwgYIKwYBBQUHMAKGgbVsZGFw0i8vL0N0	28:1c:0d:b0:94:0f:ec:c7:70:78:8c:00:f1:4a:28:				
PUNFUk41MjBHcmlkJTIwQ2VydGlmaWNhdGlvbiUyMEF1dGhvcml0eSxDTj1BSUEs	72:f6:f4:cc:38:e7:07:f6:66:d0:31:0f:bc:09:3b:				
Q049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29uZmln	33:96:1a:25:6f:12:ec:da:08:7c:30:1d:01:08:ad:				
dXJhdGlvbixEQz1jZXJuLERDPWNoP2NBQ2VydGlmaWNhdGU/YmFzZT9vYmp1Y3RD	38:c0:f6:38:7f:8b:8f:f6:2b:ce:1d:fe:05:68:d8:				
bGFzcz1jZXJ0aWZpY2F0aW9uQXV0aG9yaXR5MCQGCCsGAQUFBzABhhhodHRw0i8v	98:51:c1:c0:91:03:bc:7e:d4:f4:75:33:6c:740:8b:				
b2NzcC5jZXJuLmNoL29jc3AwDgYDVR0PAQH/BAQDAgWgMD0GCSsGAQQBgjcVBwQw	be:3a:ac:02:20:f3:1b:fe:a2:2f:89:7f:7c:fa:68:				
MC4GJisGAQQBgjcVCI090AmC7Y0Nhu2LK4He9TeFgNBiHoWK40yBtaoEAgFkAgEQ	2f:e4:fe:cc:25:70:bf:93:48:25:8e:39:7d:87:3f: 64:c5				
MCkGA1UdJQQiMCAGCisGAQQBgjcKAwQGCCsGAQUFBwMEBggrBgEFBQcDAjA1Bgkr	64:C5 Exponent: 65537 (0x10001)				
BgEEAYI3FQoEKDAmMAwGCisGAQQBgjcKAwQwCgYIKwYBBQUHAwQwCgYIKwYBBQUH	X509v3 extensions:				
AwIwSwYDVR0RBEOwOqAnBqorBqEEAYI3FAIDoBkMF2JyaWFuLmJvY2tlbG1hbkBj	X509v3 Subject Key Identifier:				
	Units/OU=Users/CN=bbockelm/CN=659869/CN=Brian Paul Bockelman/CN=1761602861	1			
	Units/OU=Users/CN=bbockelm/CN=659869/CN=Brian Paul Bockelman				
to be to be to be to be to be to be	Units/OU=Users/CN=bbockelm/CN=659869/CN=Brian Paul Bockelman				
BgkqhkiG9w0BAQ0FAA0CAgEAh type : RFC3820 compliant imperson					
cipe i in concertaire imperson	ation proxy				
Screngen . Loto		1			
puch . / cmp/ x305up_u1221		10000000 000 000 0			
culletere . 11.55.54	on%20Authority.crl				
key usage . Digital Signature, key Enc	<pre>I05,CN=CDP,CN=Public%20Key</pre>				
(Nae / RKulkacTycAnelda0Ch					
VU : Cms	VO : cms				
tijTcd2azfa05pET6Ki/MULOT Subject . / DC=CH/DC=Cern/00=Orgunte	a subject				
1SSUEP : /DC=CH/DC=Cerh/OU=Computer	issuer : /DC=Ch/DC=Cern/DC=Cern/DC=Cern.cn				
DuNI the the TTYLICADVERYT attribute : /cms/kole=NULL/Capability=	TYULCAD.udfyy attribute : /cms/kole=NULL/capability=NULL				
attribute : /cms/integration/Kole=NULL	1				
attribute : /cms/uscms/Role=NULL/Capab	1				
timeleft : 11:59:54		<u> </u>			
uri : voms2.cern.ch:15002		1			
urt . volisz.cem.ch.1902		J			

eyJraWQiOiIyRkVDMzVDNjA3NjREMjc10TRFQkVDNEQ50DgyNENEOCIsInR5cCI6IkpXVCIsImFsZyI6 IlJTMjU2In0.eyJhdWQiOiJBTlkiLCJzdWIiOiJicmlhbi5ib2NrZWxtYW5AbGlnby5vcmciLCJ1aWQi OiJicmlhbi5ib2NrZWxtYW4iLCJ2ZXIiOiJzY2l0b2tlbjoyLjAiLCJuYmYiOjE3MjgzOTIyMjUsInNj b3BlIjoicmVhZDovZnJhbWVzIHJlYWQ6L3NoYXJlZCBnd2RhdGFmaW5kLnJlYWQgZ3JhY2VkYi5yZWFk IHJ1YWQ6L3N0YWdpbmcgcmVhZDova2FncmEgd3JpdGU6L3N0YWdpbmcvYnJpYW4uYm9ja2VsbWFuIHJ1 YWQ6L2xpZ28gZHFzZWdkYi5yZWFkIHJ1YWQ6L3ZpcmdvIiwiaXNzIjoiaHR0cHM6Ly9jaWxvZ29uLm9y Zy9pZ3duIiwiZXhwIjoxNzI4NDAzMDMwLCJpYXQi0jE3MjgzOTIyMzAsImp0aSI6Imh0dHBz0i8vY2ls b2dvbi5vcmcvb2F1dGgyLzRhZGQyNGIzMjUwNGYxNzQ3N2I3MzkyY2E3YWFiMGQ1P3R5cGU9YWNjZXNz VG9rZW4mdHM9MTcvODM5MjIzMDY4NSZ2ZXJzaW9uPXYvLjAmbG1mZXRpbWU9MTA4MDAwMDAifQ.oftMF WjL-dMuLWuCQQAWydSONLmozYdzg4BBQuJD-V6Pb2jylNTx9M7PUC2FRdMsqc8WyqcT2jPBiTKqZ4PCz UFujVXEJrvSr1qE0JTwWbGyBgUxHAWtJok1CAYduFf9sy9STioHi6ptFB9ZE6r0ivjZzhkEEEwJ-V4rk haLBn4w6YtVP3UzHkb0SwydQRDJkGd0t20zsEDu20ENqGvmwWPHLVs1uW5IZOtGXbfHSn1WN9_V6JJgB 00jYw2VszRONgLrNXMpw2KrLZ12rY1grX4U85Y2pFJjch2ynd1hIXF8s1E7arLXViDN1QnotaV9GcvXb fKm9SAzpBaQL_FXLw

"aud": "ANY", "sub": "brian.bockelman@ligo.org", "uid": "brian.bockelman", "ver": "scitoken:2.0", "nbf": 1728392225. "scope": "read:/frames read:/shared gwdatafind.read gracedb.read read:/staging read:/kagra write:/staging/brian.bockelman read:/ligo dqsegdb.read read:/virgo", "iss": "https://cilogon.org/igwn", "exp": 1728403030, "iat": 1728392230. "iti": "https://cilogon.org/oauth2/4add24b32504f17477b7392ca7a ab0d5? type=accessToken&ts=1728392230685&version=v2.0&lifetime =10800000'

FEARLESS SCIENCE

morgridge.org



A transition in Two Ways -> Philosophy

- Perhaps more important than credential format is a change in authorization philosophy: capability-based authorization instead of identity-mapping.
- Capabilities state what you are allowed to do.
 - Identity mapping states who you are and assumes the service can map that to a list of permissions.
 - Identity mapping requires out-of-band coordination across all the distributed endpoints to ensure identities are mapped correctly (meaning changes are hard to implement).
 - Identity mapping schemes are hard to attenuate (remove or limit permissions from the credential).
- Example capabilities for the WLCG:
 - compute.create: submit a job to a CE
 - storage.create:/store/user/bbockelm/foo.txt: create a specific file within the CMS space at a SE.





CMS Strategy for the Token Transition

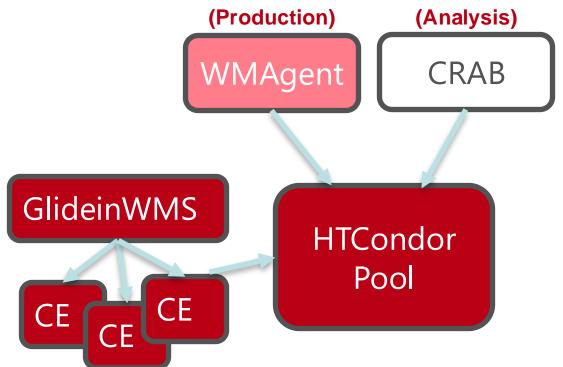
- Outside-in: start with the distributed services, verify they are working, and then convert CMS services.
 - Begin with services that are expert-centric (e.g., production system) and expand out to the user base (analysis tools, standalone laptop environments).
 - When possible, pick:
 - Standard protocols (OAuth2 for token acquisition)
 - Shared/external services (FTS, ETF)
 - Shared solutions (Rucio, Vault, HTCondor)
 - Minimize the CMS-specific technologies!
- Technology choices:
 - Token profile: WLCG Common JWT Profiles (<u>10.5281/zenodo.3460257</u>)
 - ► Token issuer: <u>IAM</u> instance operated by CERN IT.
 - Token provider: <u>HTVault</u> (a specially-configured, patched version of Vault)





Compute Ecosystem

- CMS uses the GlideinWMS software to interact with the Compute Entrypoints (CEs) at sites to build a HTCondor pool.
 - Status: GlideinWMS and HTCondor have been converted to token-based submission and internal authorization since 2022.
 - Status: Every CE but 3 ARC-CEs use tokens for pilot job submission. <u>159 CEs using tokens</u>.
- Once the HTCondor pool is constructed, the WMAgent component submits production jobs to the system and CRAB submits analysis jobs.
 - Status (WMAgent): Latest runtime will use tokens if present for reading data and stageout. Rollout of token-enabled version expected in the next quarter. Some central WMAgent services (e.g., deleting temporary files) not converted over.
 - Status (CRAB): Transition largely not started.



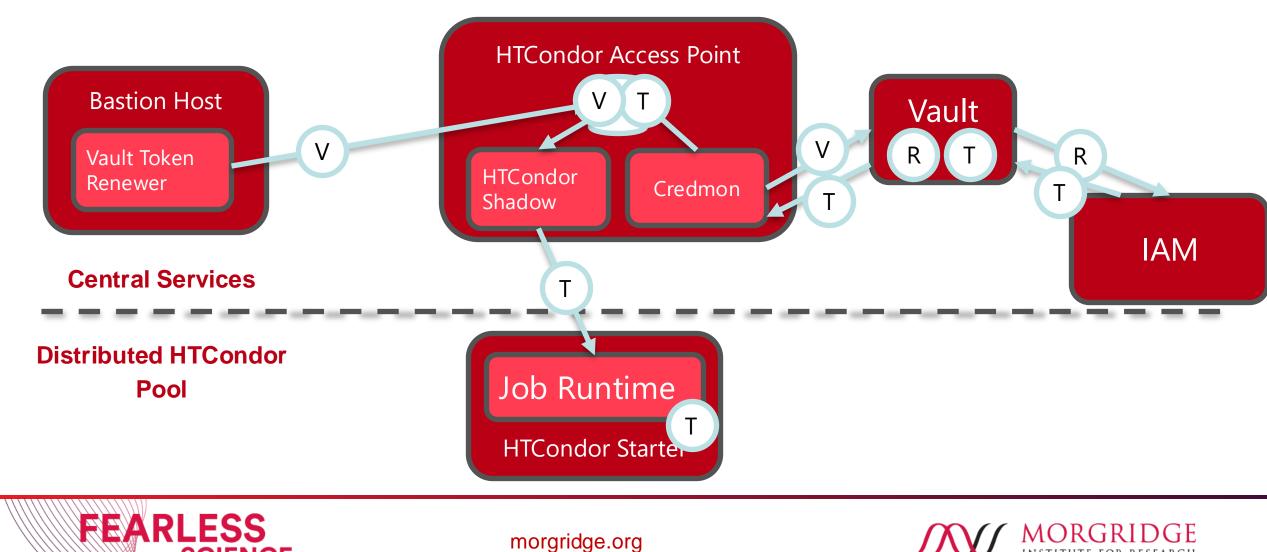




Tokens to the Job

SCIENCE

► WMAgent's runtime will use a token if present -- but how does a token get to the job?



9

INSTITUTE FOR RESEARCH

The Previous Slide, But in Words

- The HTCondor shadow process is responsible for maintaining the remote job's runtime; it sends a steady stream of new access tokens according to the job description. Only the needed access token goes to the job.
 - The shadow pulls the access token from an on-disk database maintained by the credmon.
 - ► The credmon periodically receives the token from the **HTVault** service, authenticating with a Vault token.
 - The HTVault service handles the OAuth2 flows, including exchanging a refresh token for a new access token from the IAM service.
 - The bastion host is managed by the CMS operator and periodically pushes new vault tokens to the HTCondor AP.

Status:

- Setup is in production for Fermilab experiments.
- CMS was able to reproduce the setup in test instances. <u>Rolling out this calendar year</u>.
- Finalizing the HTVault instance at CERN with IT.



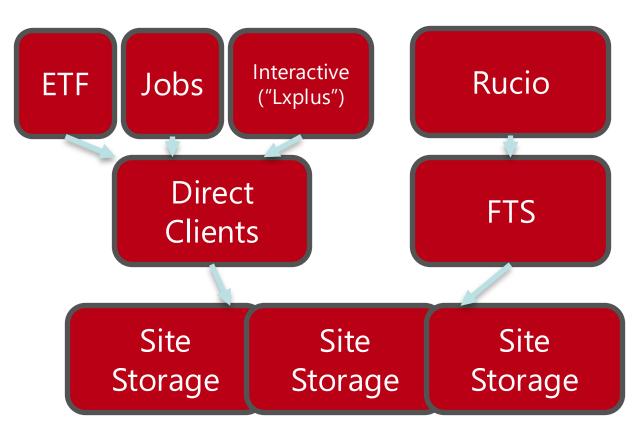


Storage Ecosystem

FEARLESS

SCIENCE

- The storage transition has been the most active one in 2024, focusing on bulk data transfers between sites (the "Rucio / FTS / SE" stack).
- Rucio uses the client credentials flow to acquire a token per dataset from IAM.
 - The token is passed to FTS which performs the OAuth2 token exchange flow with IAM to get a refresh token as well.
 - FTS uses the token to interact with site storage and drive the transfers.
 - Design and development needed for tape transfers.
- Status: Tested heavily in DC24; tweaks and adjustment through the summer; put into production in September 2024.





We continuously monitor token readiness at CMS storage endpoints using ETF and observe:

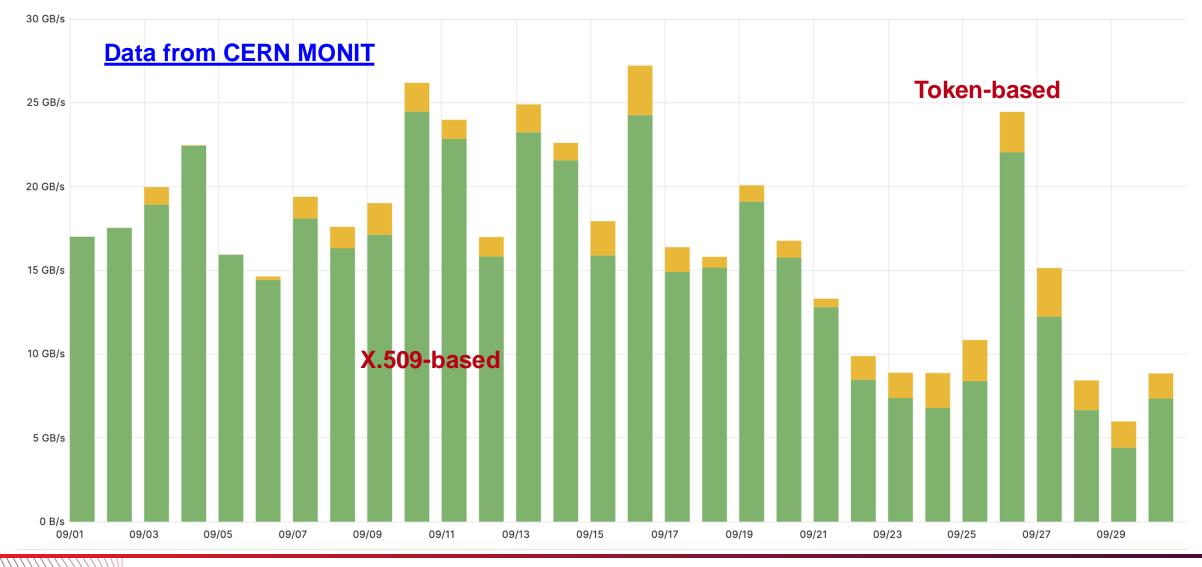
Technology	Site Count	Ready	Percent	Notes
XRootD (native)	15	15	100%	
SToRM	3	3	100%	Critical bug preventing FTS transfers
dCache	32	26	81%	
EOS	9	0	0%	Waiting on new release
DPM	2	0	0%	To be retired, not token-enabled

Over 30 sites are transferring with tokens in production!





Rucio-based transfers, September 2024



FEARLESS SCIENCE

morgridge.org



How else is storage accessed remotely?

- **Upload/download files via Rucio**: Implementation is in progress in Rucio; expected in winter 2024.
- Through the CMSSW physics application:
 - XRootD client libraries auto-discover token in environment; no code change needed.
 - AAA remote data access infrastructure mostly share endpoints with bulk data transfers. Most pieces are expected to "just work" but a rollout campaign is needed.
 - XCache works with tokens over HTTP but not xrootd protocol. Development needed.
 - Once HTVault is deployed at CERN, users will be able to acquire tokens via "htgettoken" in their interactive environments.
 - Planning to add a few creature comforts to automatically invoke this in environment setup or when starting a CMS-based container environment.
- ETF: Currently working; basis for our continuous testing!





CMS Web Services

- The CMSWeb suite of services provide access to CMS dataset metadata (DAS, DBS) and central production services infrastructure (ReqMgr).
 - The frontend service handles authorization, passes request to backend.
 - Authentication/authorization tightly integrated with X.509/GSI, SL7-based.
 - Significant recent investment to modernize/rework the frontend. Allows CMS to migrate of SL7 and opens the door for token auth. Status: New version being deployed.
- The WLCG profile defines various common storage & compute scopes: what scopes should be used for accessing various CMS features?
 - **Status**: We are in the process of defining the CMS-specific scopes for these services.
 - **Status**: Significant work to update client tooling ahead of us in 2025!





IAM Statistics

How busy is the CMS IAM instance?



- By far, the driver of the token usage is Rucio. We generate a token per dataset, as needed to transfer. We estimate half of the datasets transferred use tokens, meaning <u>we need to scale by only 2x</u> to hit the full expected scale.
 - ► By optimizing the issuing of refresh tokens, we could reduce the usage by 2x if needed.





Outlook

- Re-envisioning the authorization model for a mature ecosystem like CMS's is a huge undertaking!
 - Early R&D done in 2017; WLCG profile standardized in 2019; first production uses in 2021;
 - CE transition done in 2022; SE in production in 2024.
- Distributed services are in great shape, with few remaining endpoints missing support.
- CMS services and strategy came into sharp relief during mid-2024; we are executing on the plans now.
- By end-2025, likely all services will be in dual X.509 / token mode.

Will be ready to begin retiring X.509 in LS3!





Questions?

This presentation is supported by the National Science Foundation under Cooperative Agreement PHY-2323298. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

MORGRIDGE