Token based Authentication & Authorisation

Questionnaire for CMS

Supporting information can be found at https://hackmd.web.cern.ch/s/rkyic3vtm

Security Infrastructure (Qs for the Computing Coordinator)

If there is an existing document that answers a question, please include a link in your response.

	Question	**Response**
1	Describe your current job submission workflow. As well as a general description, please focus on: - Which credentials are used? - How do users obtain and maintain their credentials? - Are the credentials transformed or exchanged? - How do users present their credentials, e.g. command line and/or web? - How is traceability and suspension ensured?	CMS uses X509 credentials (with VOMS extensions to attest membership in CMS) throughout the job submission workflow. Users register within VOMS-Admin and use voms-proxy-init to create credentials on submit hosts (such as lxplus); these are delegated to MyProxy, allowing the CMS analysis services (such as “CRAB task worker on the HTCondor submit host”) to access the proxy. Production workflows utilize credentials placed on the submit host; no MyProxy delegation is used there. The HTCondor submit host manages the proxies and delegates to the pilot jobs. Hence, each payload has access to the X509 credential corresponding to the user; the credentials on the worker nodes are primarily utilized for accessing storage - glexec is no longer used in CMS. CMS uses X509 client authentication

		exclusively for access to web services. We are in the process of enabling CERN SSO for more services. Suspension is handled through a combination of revoking certificates (removes access to storage) and removal of user jobs at the submit point. Traceability is achieved by sites recording storage access and central record keeping of where each payload was executed. No nicknames.
2	Which storage systems are you using? How is the read vs write access authorised? Who owns the data?	CMS primarily accesses storage via POSIX, GridFTP, and XRootD. For GridFTP and XRootD, reads and writes are authenticated via the X509 client auth. Authorization is handled by CMS posting a twiki page of the authorization mapping policy that sites are supposed to implement (for example: all CMS data can be read by any CMS user; users can only write to their own “home” directories); sites are left to their own means to correctly implement this. Users own their own data; production data is perceived as being owned “by the VO”.
3	Are authorisation policies managed and/or decisions made centrally (by the VO) or at sites?	Policies are made by the VO and implemented / managed by the sites.
4	Do you have a preference between using authorisation based on Groups/Roles vs Capabilities? (See supporting information)	We would like to move to a capabilities-based model.
5	What is the typical maximum walltime for a reasonable job? (See supporting information)	The maximum theoretical lifetime for a job is likely 7 days; I suspect 99.9% are limited to 48 hours. We target 8 hour long jobs.

		Jobs may stay in queue for a week or two.
6	Integration with CERN SSO is foreseen as an option - Would authentication to the membership management platform (VOMS-Admin replacement) through CERN SSO provide a good user experience for your researchers? - Are there any reasons why integration with CERN SSO may not make sense (please bear in mind that you do not need a full CERN account to log in through CERN SSO)?	Authentication based on CERN SSO would be a significant upgrade from the current system, particularly for web-based user agents. CERN SSO is still clunky for terminal-based user agents. We would prefer a hybrid workflow (c.f. OAuth2 device flow or the work done in SciTokens to integrate with HTCondor) that allow users to login via web browsers and link the web session to their terminal session.
7	What are you using VOMS or VOMS Admin for, in addition to authorisation proxy extensions? E.g. are there services that need to browse VOMS Admin for lists of users?	I do not believe VOMS-Admin is used beyond authorizing proxy extensions; it is possible there are some poorly-known use cases. It would be beneficial to work to discover and remove as much access as possible. It is not understood which sites rely on VOMS-Admin to list users (e.g., I believe EOS still does). We would prefer that this interface is not available long-term. We do know that OSG has no software remaining that relies on VOMS-Admin to generate gridmap files. The worldwide landscape remains murky.
8	What kind of additional services do you operate that impact grid authentication and authorisation? - Web Services, e.g. portals, authorisation services? - Standalone or command-line clients? - ...	Various web services rely on X509. Particularly, the “CMSWeb” hosting framework relies solely on X509, although we’re notably within a yearlong revamp to remove this requirement; CMSWeb is additionally starting to issue SciTokens as a path forward beyond X509. I envision that this becomes dual SciTokens / WLCG JWT once WLCG is ready for this in the future.

		Group membership management is now moving into CRIC for access to web services, given that VOMS extension support for browsers doesn't exist.
9	Wishlist?	We would prefer that the group and membership keep to CERN e-groups (or its replacement). That is, there should be nothing "separate and special" for the grid. Would like to see a coherent strategy for WLCG that includes the CRIC developers.
10	Any comments?	

User Management (Qs for the VO Managers)

	Question	**Response**
1	How many administrators are there (VOMS managers)? Who are these people?	Somewhere around 2-3.
2	Do you have concerns/complaints/suggestions regarding the current user management workflows?	Automation! We'd like zero difference between joining the CMS experiment and joining the computing infrastructure. For policy and security reasons, there may be a separate checkbox to enable or AUP to sign, but this shouldn't require a separate human workflow.
3	Wishlist?	
4	Any comments?	