Token based Authentication & Authorisation

Questionnaire for ALICE

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?	https://docs.google.com/document/d/1XQvh2dxDivUstjQaS3K6tkpLyvXlEOR4QU8YtTzDqg4/edit The base X.509 certificates are obtained from the users' related CA (CERN or other institution), then the users register them in the ALICE VOMS instance. Once approved, the users can use them to interact with the Grid as described in the link above. In addition to the use-cases in the doc, the users can load the certificate into the browser and use alimonitor.cern.ch, which offers another Grid web client among other tools. Every user command is logged centrally. Blocking a particular DN centrally (every command call is processed by central services) is easy and immediate. In the new JAlien system, tokens are provisioned by the user providing their X509 user certificate and (optionally) a password.
2	Which storage systems are you using? How is the read vs write access authorised? Who owns the data?	https://docs.google.com/document/d/1XQvh2dxDivUstjQaS3K6tkpLyvXlEOR4QU8YtTzDqg4/edit Several software solutions: vanilla Xrootd,

		EOS, dCache, CASTOR, DPM. All are accessed via the Xrootd interface only. Data is owned by ALICE as VO, no particular users from the point of view of the storage system. Users and ownership are handled by the ALICE File Catalogue (ALICE internals). Read and write authorization is handled by the Central Services, creating envelopes(tokens) as described in the link above.
3	Are authorisation policies managed and/or decisions made centrally (by the VO) or at sites?	Fully controlled by the VO. The site has no group/roles mapping. The authorization decision is made by central services, that create the corresponding access envelope if approved.
4	Do you have a preference between using authorisation based on Groups/Roles vs Capabilities? (See supporting information)	For data access, we are fully using capabilities. As already mentioned, our model doesn't map group/roles to the sites. Each token grants access to a unique file operation, and we will keep this model as it is. For clients authz, the model is based on roles (user, pilot submitter and payload). In some aspects, groups/roles are used as capabilities, the difference is very subtle. While we don't use capabilities per se, roles are achieving the same effect for us. So we don't have a strong preference in this sense.
5	What is the typical maximum walltime for a reasonable job? (See supporting information)	The lifetimes vary a lot (from few minutes to many hours) but the hard limit is 24h.
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	We don't see SSO as a big advantage for the current workflows in ALICE that are mostly command-line based. X.509 certificates are not significantly different from ssh keys in this sense: both can have custom expiry times and have similar cryptographical properties, but for the X.509 certificates being signed. JAliEn uses X.509 user certificates from IGTF CAs and will ask for the certificate password once for the first client session, and/or then use the Token (a time restricted X.509 certificate) available locally on the machine and that can be automatically renewed.

	bear in mind that you do not need a full CERN account to log in through CERN SSO)?	Integrating the ALICE internal authentication and authorization into an external system will be complex and the control of something as essential should stay within the VO. However, for the web approach, we indeed consider SSO an interesting solution that is more user-friendly.
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?	We use it to keep track of all VO members and status, and keep a sub-list of trusted people. These trusted people will have role (*lcgadmin*) to operate Grid sites, which means they will be able to talk to the delegation/proxy services and interact with them from the sites, to generate proxies for the payloads in WLCG sites. The other role we have is the VOAdmin. But internally we have our own system, so we don't really rely on VOMS.
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? - ...	- MonaLisa monitoring (and Grid client) system (alimonitor.cern.ch) - (AliEn) user shell - ROOT clients - LDAP server (list of approved DNs), synced with VOMS - Central databases - There could be potentially any custom command-line tool that speaks to our Central Services (WebSocket + X.509)
9	Wishlist?	-
10	Any comments?	-

User Management (Qs for the VO Managers)

	Question	**Response**

1	How many administrators are there (VOMS managers)? Who are these people?	Latchezar Betev, Maarten Litmaath
2	Do you have concerns/complaints/suggestions regarding the current user management workflows?	-
3	Wishlist?	-
4	Any comments?	-