There is a short summary of two discussed scenarios for solving the problem of violation of the European privacy regulation by including non-encrypted user DN in the monitoring reports

Scenario	Pros	Contras
Instead of sending DN as it is, send MD5 hash of DN	The simplest solution	Might be not considered sufficient by the security experts, to be checked with Romain
There is a special unique attribute which is assigned to every user in VOMS and is being propagated to the clients with user proxy. This attribute is used instead of user DN in the UDP monitoring reports. Only privileged users are allowed to get mapping from VOMS through the SSL connection.	In case such a possibility is confirmed with VOMS developers and experts, this would work across VOs and various applications with fairly simple changes on the client side. Instead of retrieving user DN, the information producers would need to retrieve user_id attribute from the user proxy. Mapping is cached on the Dashboard side, therefore there is almost no overhead on the Dashboard side for data processing. Data producers do not need to know who are the privileged consumers who are allowed to perform mapping. Handling the dynamic list of privileged clients is fairly simple	There is still a possibility (analyzing data) to reconstruct mapping. Though changing mapping on regular basis might make it difficult
Perform encryption of user DN (+ date?) on the client side and decryption on the Dashboard side	This implementation is completely inline with the European law	Will certainly have a performance penalty both for data producers and data consumers. Need to understand how big would be an overhead to ensure the required performance. Would require more serious changes (than in the previous case) in both data producers and data consumers. In case there are multiple potential consumers of data , encryption should be done with several keys. So either producers know in advance who would consume their data or need to make a call to some central service to find it out, which is not desired, in particular when data is published from the WNs (job monitoring use case)

VOMS-based solution

Julia got in touch with Andrea Ceccanti in order to understand whether VOMS can provide required functionality. According to Andrea, any number user attributes can be created. What is missing is restricted access for a mapping between user and certain attribute. Andrea thinks it should not be too difficult to implement, but we need to provide clear requirements.

Wether everyone agrees that in terms of requirements we need:

- during creation of the new attribute make clear that this attribute requires restricted access
- restricted API which would provide user-attribute mapping based either on user or service certificate

Another question:

- Do we need approval of MB for pushing for implementation of these features in VOMS?

This topic: LCG > UserDNPrivacyDiscussion
Topic revision: r3 - 2014-12-12 - JuliaAndreeva

Copyright &© 2008-2021 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
or Ideas, requests, problems regarding TWiki? use Discourse or Send feedback