ASTERICS DADI/OBELICS A&A Meeting. Trieste January 28-30, 2019

Demonstration of RAP

Franco Tinarelli (INAF-IRA), Sara Bertocco, Cristina Knapic, Elisa Londero (INAF-OATs).

RAP (Remote Authentication Portal) is a web application written in PHP completely independent of the applications that use it as an authenticator. The application caller is recorded in a file that contains the call-back address to return the data of the authenticated user.
The main features of the program are:

- authentication with different methods: eduGAIN, Google, Facebook, LinkedIn, X.509 (IGTF and TERENA-TACAR are allowed) and Local Login;
- account-linking;
- registration in MySQL or LDAP;
- editing of registered profiles.

Each of the features can be turned on or off as desired and shown or hidden in the user interface. The authentication mechanism is made more secure by associating the authentication request with a token, sent to the calling application that will use it as a key to request authentication information, with consequent elimination of transient data and token, immediately after sending.
Note that no password is sent by the authenticators to RAP and consequently to the application.
User registration can be done directly by RAP on its own tables associated with the calling application, or remotely on the DB of the same application. Similarly to the call-back address, the specific information of the DB also comes associated with the calling application in a client configuration file.
RAP can use either a relational DB or an LDAP for the registration of the users both locally and remotely for account-linking functionality. The use of LDAP allows, through a management procedure, to accredit users to login via SSH on workstations that use it as an authentication system. Subsequently the same functionality can be extended to the use of Kerberos for those applications that require its use.

Fig. 1 RAP: the interface

RAP is an Open Software and can be adapted and inserted in external applications, e.g. as implemented by the IA2 team.

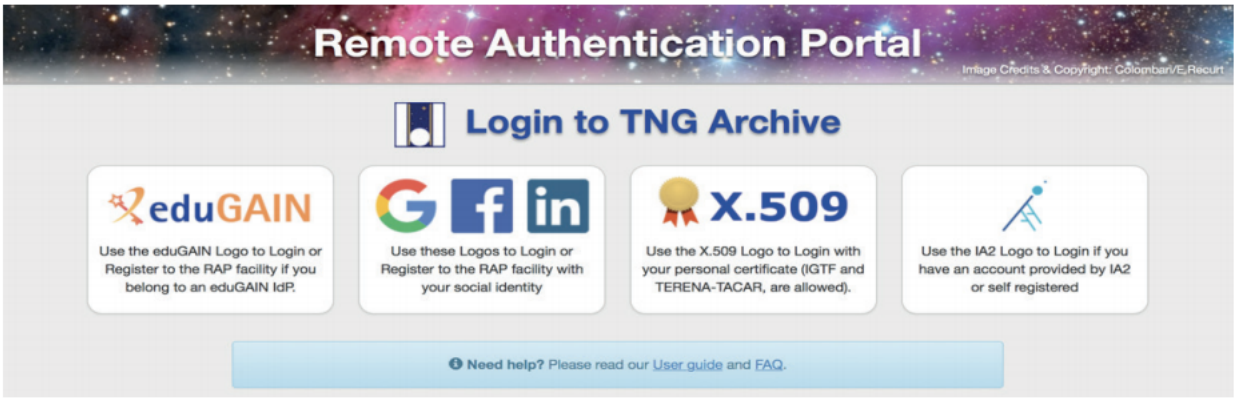

Fig.2 The IA2 implementation

Grouper was chosen by IA2 to organize the access permissions to the resources provided through its services. Grouper stores information about groups and permissions within a database, called registry. The Grouper installation used by IA2 currently relies on a MySQL database, however, since Grouper is based on ORM Hibernate technology, other RDBMS engines could be used. The RAP / Grouper suite, allows a user, authenticated and authorized to access the information contained her/his own proper archives portion.