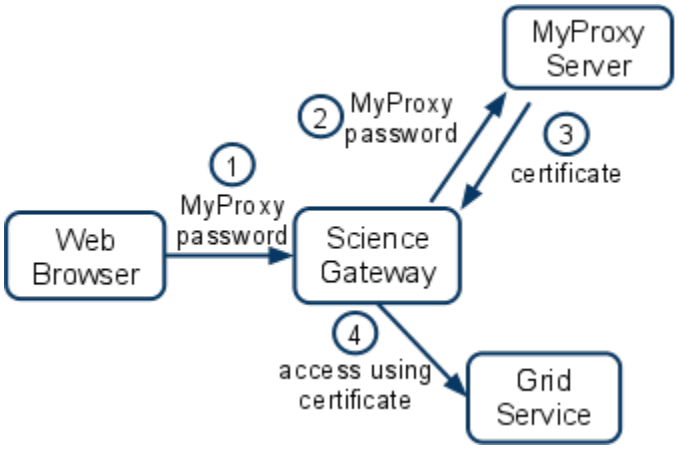
Proposal: OAuth for TG Gateways

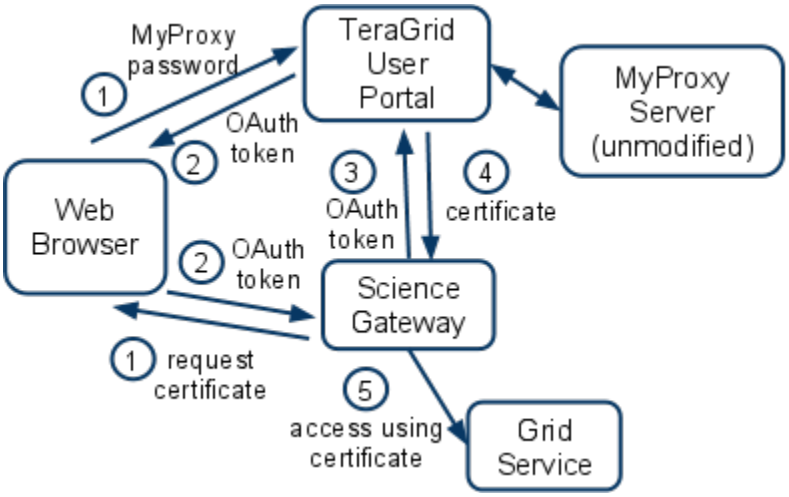
Jim Basney <jbasney@ncsa.uiuc.edu>
Mon Jan 10, 2011

Currently, when a TeraGrid science gateway allows a researcher to use his or her own TeraGrid account, rather than using a community account, the science gateway uses the TeraGrid MyProxy server as illustrated in the following figure:



The researcher provides his or her TeraGrid MyProxy username and password to the science gateway, which the gateway uses to obtain a (short-lived) certificate for the researcher from the TeraGrid MyProxy server, so the gateway can access grid services on the researcher's behalf, by authenticating with the researcher's certificate. A significant drawback to this approach is that it discloses the researcher's (typically long-lived) TeraGrid MyProxy password to the science gateway.

To address this drawback, TeraGrid could provide an OAuth service, integrated with the TeraGrid User Portal, as illustrated in the following figure:



When the science gateway requires a certificate to act on the researcher's behalf, it redirects

the researcher's browser to the TeraGrid User Portal (TGUP), where the researcher authenticates (as usual) and approves (or denies) use of his or her credentials by the science gateway. If the researcher successfully authenticates and approves the use, the portal redirects the researcher's browser back to the science gateway with a one-time-use OAuth token that the gateway uses to request a certificate from the TGUP OAuth service, so the gateway can access grid services on the researcher's behalf. The proposed TGUP OAuth service would implement the OAuth 1.0 protocol, which is not shown in full detail above, but is specified in RFC 5849. The TGUP OAuth service could optionally require registration of science gateways and only allow authenticated requests from registered gateways.

The result is that TG researchers only enter their TGUP password on the TGUP, rather than also at science gateway web sites.

Note that this approach applies to web browser interactions and does not impact use of myproxy-logon on the command-line.