# NanoHUB

## nanoHUB

The nanoHUB project is prototyping the use of GridShib in its community-based grid portal infrastructure. The nanoHUB integration is an important prototype TeraGrid use case.

Some important nanoHUB facts:

- nanoHUB maintains its own usernames and passwords (LDAP)
- nanoHUB maintains its own user attributes (LDAP)
- nanoHUB maintains its own Shibboleth Identity Provider (IdP)

Note: Although the nanoHUB portal is **not** Shib-enabled, nanoHUB leverages a Shib IdP to resolve attributes.

### Attribute pull

The current nanoHUB development environment implements GridShib attribute pull.

1. An unauthenticated browser user makes a request to the nanoHUB portal.
2. The nanoHUB portal authenticates the user via nanoHUB LDAP. Using the GridShib Authentication Assertion Client, the nanoHUB portal issues a SAML authentication assertion describing this act of authentication. The nanoHUB portal binds the authentication assertion to a proxy certificate signed by the nanoHUB community credential. Using this proxy certificate, the nanoHUB portal requests a service at the Grid SP.
3. The Grid SP authenticates the request and extracts the authentication assertion from the proxy certificate using the SAML Authentication Assertion PIP. Using the information in the authentication assertion, the Grid SP queries the nanoHUB IdP for attributes.
4. The nanoHUB IdP resolves attributes via nanoHUB LDAP and returns a SAML attribute response to the Grid SP.
5. Based on the attributes in the response, the Grid SP makes an access control decision and returns the requested service or an error, subject to policy.
6. The nanoHUB portal returns a response to the browser user.

### Attribute push

A future nanoHUB deployment may implement GridShib attribute push (which is still on the drawing board).

The sequence of steps below assumes the nanoHUB IdP continues to run as a service.

1. An unauthenticated browser user makes a request to the nanoHUB portal.
2. The nanoHUB portal authenticates the user via nanoHUB LDAP. Using the GridShib Authentication Assertion Client, the nanoHUB portal issues a SAML authentication assertion describing this act of authentication. Using the SAML Attribute Query Client, the nanoHUB portal queries the nanoHUB IdP for attributes.
3. The nanoHUB IdP resolves attributes via nanoHUB LDAP and returns a SAML attribute response to the nanoHUB portal.
4. The nanoHUB portal validates the response, extracts the attribute assertion, and binds both assertions (using an X.509 Binding for SAML) to a proxy certificate signed by the nanoHUB community credential. Using this proxy certificate, the nanoHUB portal requests a service at the Grid SP.

5. After authenticating the request, the Grid SP extracts and consumes the assertions from the proxy certificate. Based on the attributes in the assertion, the Grid SP makes an access control decision and returns the requested service or an error, subject to policy.
6. The nanoHUB portal returns a response to the browser user.

As mentioned above, nanoHUB may continue to run the IdP as a service, but this is not required since the IdP attribute resolver may be incorporated directly into the nanoHUB community portal. Along these lines, a NanoHUBTestbed is being developed to explore various deployment scenarios based on the GridShib SAML Tools.