FAQs for SSO (via SAML 2.0) Integrations

What is SAML?
SAML is the protocol used by Shibboleth and many other SAML implementations like Ping Identity or SimpleSAMLphp

What is metadata?
Metadata is information that describes how a particular entity communicates with the world. Metadata contains certificate information and endpoints.

When upgrading a production site, what does the NYU Identity Management (IdM) team have to do?
If the new site is going to reuse the URL, entityId and the certificate from the previous site, then IdM has nothing to do. If the new site is going to change any of these components, corresponding changes must occur on the Production IdP side too.

Note: If the SP site changes the certificate which is used for SSL (HTTPS), we do not have to do anything. If they change the certificate used for signing and encrypting the SAML assertions, then we need to have get new metadata with the new certificate information.

What does the SP-team need to do when the SP undergoes an upgrade?
If there is already a Shibboleth environment and they are moving it to a new host or upgrading the version of Shibboleth SP software, they should simply copy it to the new host. In addition, they should review what has changed between versions (SP Release Notes).

To test the new setup, they should provide the new metadata to the IdM team to be added to the QA IdP environment.

What is the standard attribute released?
uid is the standard technical name of the NetID, which is the user friendly name we use at NYU. It is unique and can be used to identify any person at the university.

Why is a certificate necessary?
The certificate is for SAML signing and encryption, not for SSL. It's not mandatory but highly recommended, especially when the information transmitted is more than just confirmation about successful authentication. The certificate can be self-signed for the production setup.

For information re: SSL certificates, send email to keymaster@nyu.edu.

What are the specs for the certificate?
x509 certificate in PEM (preferable) or DER format, 2k size with SHA-256 signature

What's the difference between idp-initiated vs sp-initiated?
This describes the SSO operation process flow. In an SP-initiated SSO flow is most common. Authentication request starts from the SP Security Domain and redirects the user to the IdP. IdP-initiated SSO flow starts from the IdP Security Domain with a SSO response and redirects the user to the SP.

Previous URL for egencia - (ex: IdP initiated)

New URL for egencia - (ex: SP initiated)
Can a QA SP connect to our Prod IdP?
NYU policy forbids non-production SPs to be integrated with our production IdP. We make exceptions in cases when there is no alternative but we impose restrictions - no performance testing -- only functional testing allowed, changes should be as few as possible, and the configuration is temporary.

In case a direct integration with our QA/Test IdP is necessary, we can use our production IdP with the test SP, with the restrictions above noted. When the production SP is ready, we will replace your test configuration with the production one.

Additional info

Test IdPs in Metadata - Test IdPs in InCommon metadata serve little or no purpose. Since test IdPs are indistinguishable from production IdPs to both relying parties and end users, the introduction of explicit test IdP metadata is strongly discouraged.
Errors that seems IdP-related

The IdP simply informs you about receiving a malformed request due to certain conditions. This either due to a user or an SP behavior issue.