Authentication as a Service
Many applications now rely on “Authentication as a Service” where the authentication is handled by a separate application.

- Ex: “Login with Google” / “Login with Instagram” / ...
- Ex: Queue@Illinois ⇒ Login w/ Illinois
  - Shibboleth (UIUC login technology) provides user authentication without revealing any details except that the user!

Almost all “Single Sign On” technologies are enabled using Security Assertion Markup Language 2.0 (SAML2) protocols. There are three primary “actors” in this protocol:

1. [User Agent -- UA]:
2. [Service Provider -- SP]:
3. [Identity Provider -- IdP]:
4. [User Artifacts]:

The goal of SAML is to enable the Service Provider (SP) verification of an identity of a user via an Identity Provider (IdP).

- [SP Requirements]:
- [IdP Requirements]:

SAML2 Authentication Protocol:
1. The first stage of any SSO login is that the user must choose how the user wants to login. (User must initialize the login process.)

   **Step 1:** You visit Queue@Illinois

   ![Example Image](https://shibboleth.illinois.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZL...)

   - The HTTP redirect from the SP to the IdP contains a unique session token to identify this session.

2. Once you have chosen the SSO service to login with, the SP redirects the request to the IdP:

   **Step 2:** Click Login with Illinois

3. The IdP asks the SP for the user artifacts requested:

   **Step 3:** IdP asks SP for user artifacts requested
4. The user completes authentication with the IdP:

**Step 4: User logs in with the IdP**

- This might include 2FA or any other steps for login.

5. The user is redirected back to the SP with the session token and SAMLResponse (XML document with means to verify):

**Step 5: Logged in user redirected back to the SP from the IdP**

Example:

```
POST https://queue.illinois.edu/Shibboleth.sso/SAML2/POST
RelayState: ss:mem:2e502ac4271f188de648aaa8cc8467f867b7563dd9ff95e5e4b97cf54f866
SAMLResponse: ...
```

Q: When logging in with SAML2, what information is shared **directly by the user** with the service provider?

Q: What information is **shared by the identity provider** with the service provider?

Q: If your login uses 2FA, who is responsible for the 2FA?

Q: When does the service provider communicate with the identity provider directly, without the user?

Q: What assumptions are made about this communications at all steps of the SAML2 protocol?

6. The SP communicates directly with the IdP to retrieve the requested credentials:

**Step 6: SP asks IdP to supply artifacts requested+approved**

- This often includes things like e-mail address, user name, or other profile information shared between two sites.

7. The user is redirected to the originally requested service:

**Step 7: SP redirects user to originally requested service**