CS 240
Computer Systems

#24: SSO Authentication with SAML2

Nov. 18, 2021 · Wade Fagen-Ulmschneider

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.)*

Service Provider (Ex: Queue@Illinois)		**User Agent** (You on Firefox)		**Identify Provider** (Univ. of Illinois)
***Step 1:** You visit Queue@Illinois*				

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*				

Example:

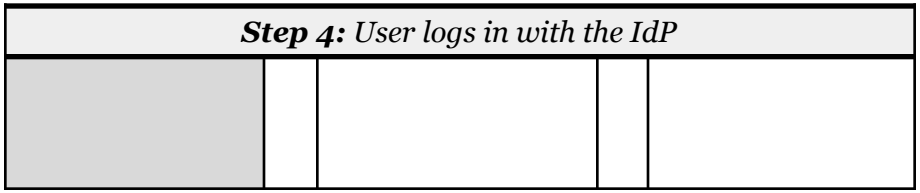
```
https://shibboleth.illinois.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZL
LbsIwEEV%2FJfKeOAkQBYsgUVgUiZaI0C66qYwzbSw5dupx%2Bvj7GgICNkje%2BfrM3CNPkTeqZfP
O1XoLXx2gC34bpZEdL3LSWc0MR4lM8waQOcHK%2BdOaJWHEWmucEUaRYI4I1kmjF0Zj14AtwX5LAS%
2FbdU5q51pklHp6B6FUSmojMYSqo2Ut93ujwNUhoqEHckKLTbkjwdKvIjU%2FQC8IvORvOLJqqd%2F
mQyo4QbZQSQvC0bLckGC1zMn7aDjiCSTpJB2LVIwnkI1EAqNJVEWcZ9XQxxA7WGl0XLucJFESD2J%2
Fsl2csmHGxukbCYpT6QepK6k%2F7xva9yFkj7tdMeiLvYLFYykfILPpwTM7DrZX5u9j%2BVk3mZ3Ne
AuhwFsrF1tTejWmn9myZ89dLQujpPgL5kqZn4UF7iAnMaGz%2Fsnt15j9Aw%3D%3D&RelayState=s
s%3Amem%3Ac3256315ff56005b1d8c043b1b889c3987cb5a0f92f9bfb8ee00cf435a7ec494
```

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

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

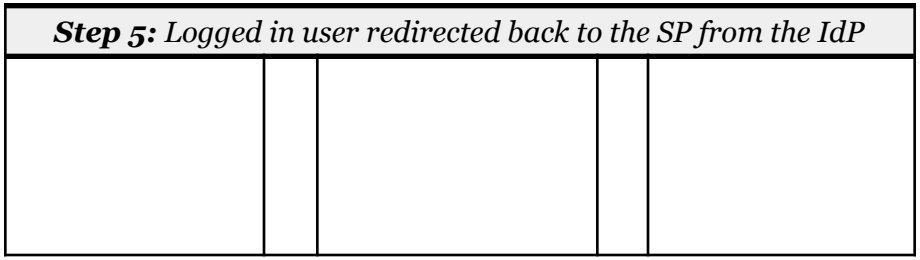
***Step 3:** IdP asks SP for user artifacts requested*				

4. The user completes authentication with the IdP:



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

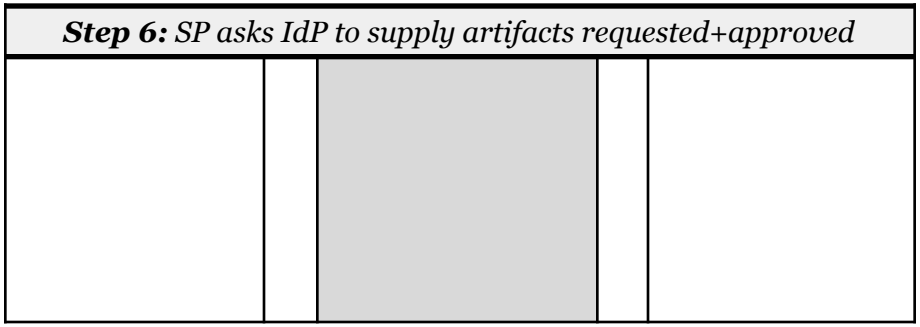
5. The user is redirected back to the SP with the session token and SAMLResponse (XML document with means to verify):



Example:

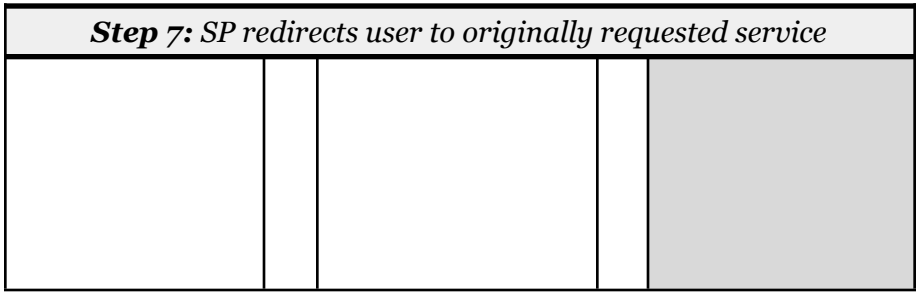
```
POST https://queue.illinois.edu/Shibboleth.sso/SAML2/POST
RelayState: ss:mem:2e502ac42718118de648aaa8ccc8607f067a7563dd0ff095ece0b97cf54f8606
SAMLResponse: ...<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
Destination="https://queue.illinois.edu/Shibboleth.sso/SAML2/POST"
ID="_0e70aa529e4f76658b6e7a21391a79f4" InResponseTo="_75b25f173ed91cd76fad5a8fd0acf4c6"
IssueInstant="2021-11-18T17:10:40.532Z" Version="2.0">...
```

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



- 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:



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?