

# Authentication with SAML2 (SSO Login)

**CS 240 - The University of Illinois**

Wade Fagen-Ulmschneider

November 18, 2021



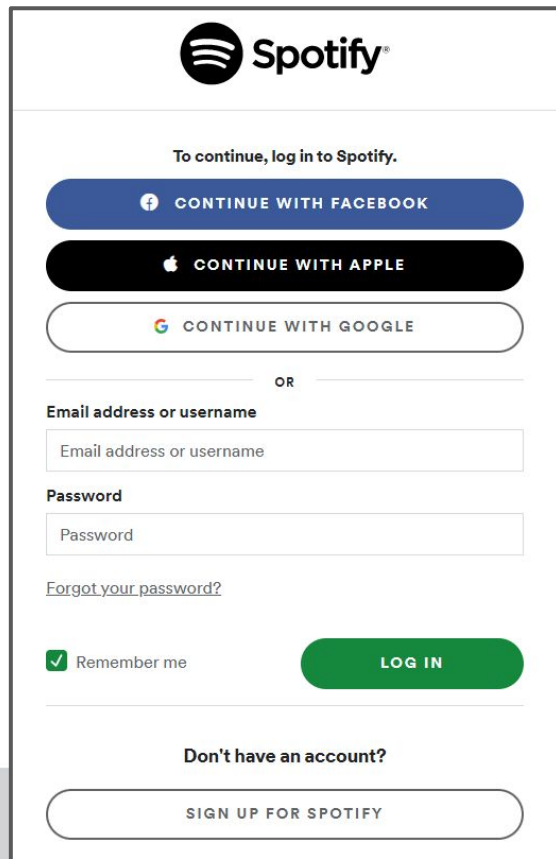
# Authentication as a Service

# Authentication as a Service

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

# Authentication as a Service

- Very commonly used: “Login with Google”, “Login with Apple”, etc|
- Used here at Illinois for UIUC login!



The image shows a screenshot of the Spotify login interface. At the top is the Spotify logo. Below it, the text "To continue, log in to Spotify." is displayed. There are three large, rounded buttons for social login: "CONTINUE WITH FACEBOOK" (blue), "CONTINUE WITH APPLE" (black), and "CONTINUE WITH GOOGLE" (white with a colored border). Below these is the word "OR" in a smaller font. The login form consists of two input fields: "Email address or username" and "Password". Below the password field is a link for "Forgot your password?". There is a "Remember me" checkbox with a checkmark and a green "LOG IN" button. At the bottom, there is a link for "Don't have an account?" and a "SIGN UP FOR SPOTIFY" button.



# Definitions

A photograph of a statue on a pedestal with the inscription "ALMA MATER" and "1863" below it, surrounded by a crowd of people. The entire image is overlaid with a semi-transparent orange filter.

# SAML2 Definitions

User Agent or **UA**:

# SAML2 Definitions

Service Provider (**SP**):

Identity Provider (**IdP**):

# SAML2 Definitions

User Artifacts:



# Goal of SAML2 Auth

SP Requirements:

IdP Requirements:

The background features a photograph of a large, classical-style statue of a woman, likely Alma Mater, standing on a pedestal. The statue is surrounded by a crowd of people, some of whom are looking towards the camera. The entire image is overlaid with a semi-transparent orange color. The text 'SAML2 Authentication Protocol' is centered in white, bold, sans-serif font.

# SAML2 Authentication Protocol

<b>Service Provider</b> (Ex: Queue@Illinois)		<b>User Agent</b> (You on Firefox)		<b>Identify Provider</b> (Univ. of Illinois)
---	--	---------------------------------------	--	---

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

--	--	--	--	--

<b>Service Provider</b> (Ex: Queue@Illinois)		<b>User Agent</b> (You on Firefox)		<b>Identify Provider</b> (Univ. of Illinois)
---	--	---------------------------------------	--	---

***Step 2: Click Login with Illinois***

--	--	--	--	--

<b>Service Provider</b>		<b>User Agent</b>		<b>Identify Provider</b>
(Ex: Queue@Illinois)		(You on Firefox)		(Univ. of Illinois)
<b><i>Step 3: IdP asks SP for user artifacts requested</i></b>				

<b>Service Provider</b>		<b>User Agent</b>		<b>Identify Provider</b>
(Ex: Queue@Illinois)		(You on Firefox)		(Univ. of Illinois)
<b><i>Step 4: User logs in with the IdP</i></b>				

<b>Service Provider</b> (Ex: Queue@Illinois)		<b>User Agent</b> (You on Firefox)		<b>Identify Provider</b> (Univ. of Illinois)
---	--	---------------------------------------	--	---

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

--	--	--	--	--



**Service Provider**

(Ex: Queue@Illinois)

**User Agent**

(You on Firefox)

**Identify Provider**

(Univ. of Illinois)

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

--	--	--	--	--

<b>Service Provider</b> (Ex: Queue@Illinois)		<b>User Agent</b> (You on Firefox)		<b>Identify Provider</b> (Univ. of Illinois)
---	--	---------------------------------------	--	---

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

--	--	--	--	--

<b>Service Provider</b> (Ex: Queue@Illinois)		<b>User Agent</b> (You on Firefox)		<b>Identify Provider</b> (Univ. of Illinois)

# Questions

The image features a central photograph of a statue of a woman in a long, flowing dress, standing on a pedestal. The statue is surrounded by a crowd of people, some of whom are looking towards the camera. The background consists of bare tree branches. The entire image is overlaid with a large, semi-transparent orange rectangle. The word "Questions" is written in a large, white, sans-serif font across the center of the orange overlay.

**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?

# Questions

The image features a central photograph of a statue of a woman in a long, flowing dress, standing on a pedestal. The statue is surrounded by a crowd of people, some of whom are looking towards the camera. The background consists of bare tree branches. The entire image is overlaid with a large, semi-transparent orange rectangle. The word "Questions" is written in a large, white, sans-serif font across the center of the orange overlay.