



# Using Your Own Authentication System with ArcGIS Online

Daniel Urbach and Cameron Kroeker

ESRI USER CONFERENCE

GIS  
INSPIRING  
WHAT'S  
NEXT

# Agenda

- **The ArcGIS Platform**
- **What is SAML?**
- **Meet the Players**
- **Relationships Are All About Trust**
- **What Happens During SAML Authentication**
- **Demo**
- **Groups and Federation**
- **Questions?**

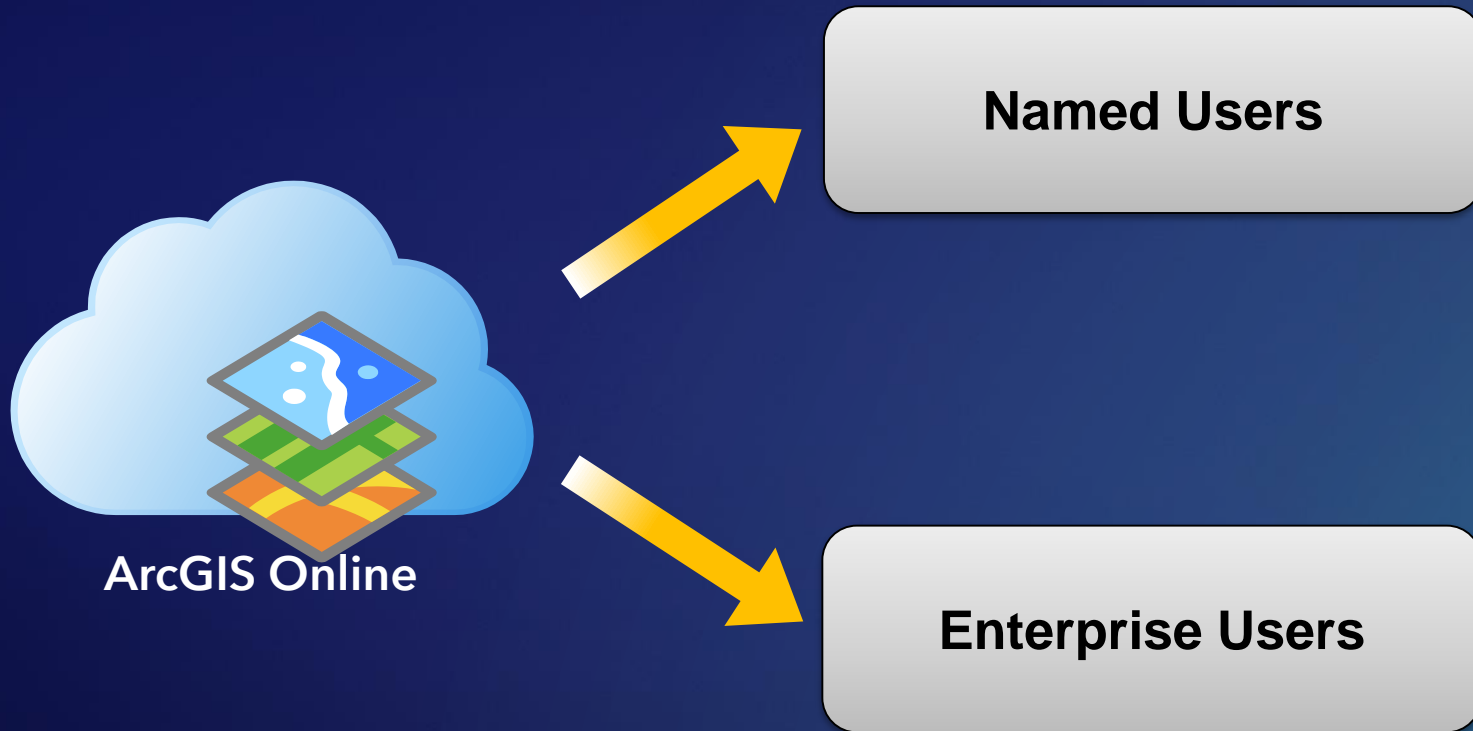
# The ArcGIS Platform

The image features a dark teal background with a subtle, light-colored topographic map pattern. In the center, the text "The ArcGIS Platform" is written in a clean, white, sans-serif font. The corners and sides of the image are decorated with abstract, overlapping geometric shapes in various shades of teal, blue, orange, and red, creating a modern and dynamic visual effect.

# The ArcGIS Platform



How to authenticate?



**SAML Authentication**

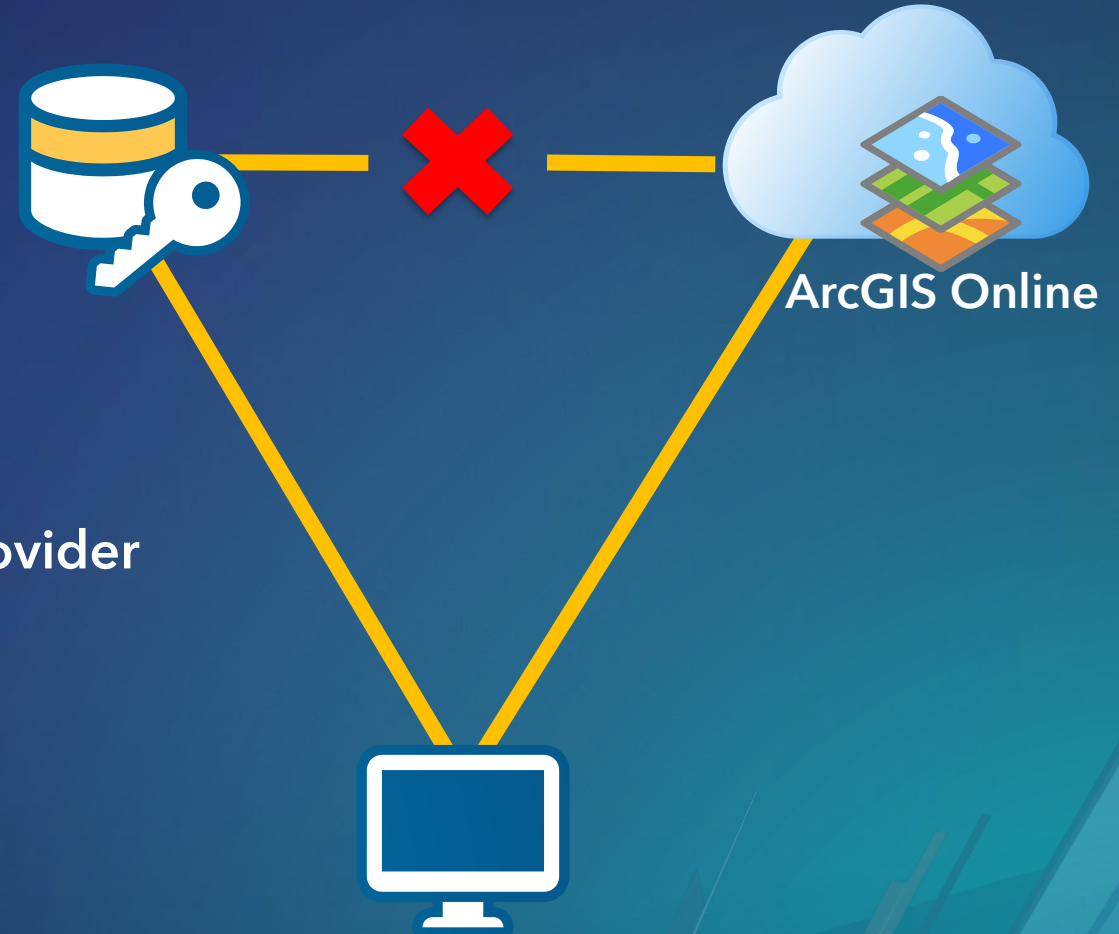




What is SAML?

# What is SAML?

- Security Assertion Markup Language
- Based on XML and open source standard
- Web browser single sign-on
- Separating the Identity Store from the Service Provider



# SAML Request

- Identity of issuer making the request
- Format of username to return

```
<SAML2:AUTHNREQUEST xmlns:SAML2="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:SAML="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_NSZIFBNMGKNZUJMX"
  VERSION="2.0"
  ISSUEINSTANT="2018-07-03T21:12:04Z"
  PROTOCOLBINDING="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  ASSERTIONCONSUMERSERVICEURL="HTTPS://SAMLJACKSON.MAPS.ARCGIS.COM/SHARING/REST/OAUTH2/SAML/SIGNIN"
  > <SAML:ISSUER>SAMLJACKSON.MAPS.ARCGIS.COM</SAML:ISSUER> <SAML2:NAMEIDPOLICY FORMAT="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
    ALLOWCREATE="TRUE"
  />
</SAML2:AUTHNREQUEST>
```



# SAML Response

- Verification of authentication
- User attributes:
  - NameID
  - GivenName
  - Email Address
  - Groups

```
<SAML:RESPONSE ID="_C9C30E43-3E59-4DF3-89A4-235C6C20E819"
  VERSION="2.0"
  ISSUEINSTANT="2018-07-03T21:12:19.442Z"
  DESTINATION="HTTPS://SAMLJACKSON.MAPS.ARCGIS.COM/SHARING/REST/OAUTH2/SAML/SIGNIN"
  CONSENT="URN:OASIS:NAMES:TC:SAML:2.0:CONSENT:UNSPECIFIED"
  INRESPONSETO="_NSZIFBNMGKNZUJMX"
  XMLNS:SAML="URN:OASIS:NAMES:TC:SAML:2.0:PROTOCOL"
>
<ISSUER XMLNS="URN:OASIS:NAMES:TC:SAML:2.0:ASSERTION">HTTP://SUPT0003423.LARRY.DEVESRI.COM/ADFS/SERVICES/TRUST</ISSUER>
<SAML:STATUS>
  <SAML:STATUSCODE VALUE="URN:OASIS:NAMES:TC:SAML:2.0:STATUS:SUCCESS" />
</SAML:STATUS>
<SUBJECT>
  <NAMEID>SAMLJACKSON</NAMEID>
  <SUBJECTCONFIRMATION METHOD="URN:OASIS:NAMES:TC:SAML:2.0:CM:BEARER">
    <SUBJECTCONFIRMATIONDATA INRESPONSETO="_NSZIFBNMGKNZUJMX"
      NOTONORAFTER="2018-07-03T21:17:19.442Z"
      RECIPIENT="HTTPS://SAMLJACKSON.MAPS.ARCGIS.COM/SHARING/REST/OAUTH2/SAML/SIGNIN"
    />
  </SUBJECTCONFIRMATION>
</SUBJECT>
  <CONDITIONS NOTBEFORE="2018-07-03T21:12:19.410Z"
    NOTONORAFTER="2018-07-03T22:12:19.410Z"
  >
  <AUDIENCERESTRICTION>
    <AUDIENCE>SAMLJACKSON.MAPS.ARCGIS.COM</AUDIENCE>
  </AUDIENCERESTRICTION>
  </CONDITIONS>
  <ATTRIBUTESTATEMENT>
    <ATTRIBUTE NAME="HTTP://SCHEMAS.XMLSOAP.ORG/WS/2005/05/IDENTITY/CLAIMS/EMAILADDRESS">
      <ATTRIBUTEVALUE>SAMLJACKSON@JACKSON5.COM</ATTRIBUTEVALUE>
    </ATTRIBUTE>
    <ATTRIBUTE NAME="HTTP://SCHEMAS.XMLSOAP.ORG/WS/2005/05/IDENTITY/CLAIMS/GIVENNAME">
      <ATTRIBUTEVALUE>SAM L. JACKSON</ATTRIBUTEVALUE>
    </ATTRIBUTE>
    <ATTRIBUTE NAME="HTTP://SCHEMAS.XMLSOAP.ORG/CLAIMS/GROUP">
      <ATTRIBUTEVALUE>LARRY\DOMAIN USERS</ATTRIBUTEVALUE>
    </ATTRIBUTE>
  </ATTRIBUTESTATEMENT>
  <AUTHNSTATEMENT AUTHNINSTANT="2018-07-03T21:12:19.301Z"
    SESSIONINDEX="_0E8A5414-0DAD-4867-A08A-769725DF036B"
  >
  <AUTHNCONTEXT>
    <AUTHNCONTEXTCLASSREF>URN:OASIS:NAMES:TC:SAML:2.0:AC:CLASSES:PASSWORDPROTECTEDTRANSPORT</AUTHNCONTEXTCLASSREF>
  </AUTHNCONTEXT>
</AUTHNSTATEMENT>
</ASSERTION>
</SAML:RESPONSE>
```

# Meet the Players

Service Provider, Identity Provider and Client

# Meet the Players: Service Provider

- Provides web-based consumables to the end-user
- Requires authentication
- ArcGIS Online



# Meet the Players: Identity Provider (IdP)

- Provides cross-domain authentication
- Uses HTTP/HTTPS
- Active Directory Federated Services, OpenAM, etc
- Can authenticate via existing user stores (AD, LDAP, etc)



# Meet the Players: Identity Provider (IdP)

## Typical SAML Provider Architecture



External Domain(s)



Firewall



DMZ



Firewall



Internal Domain



# Meet the Players: Client

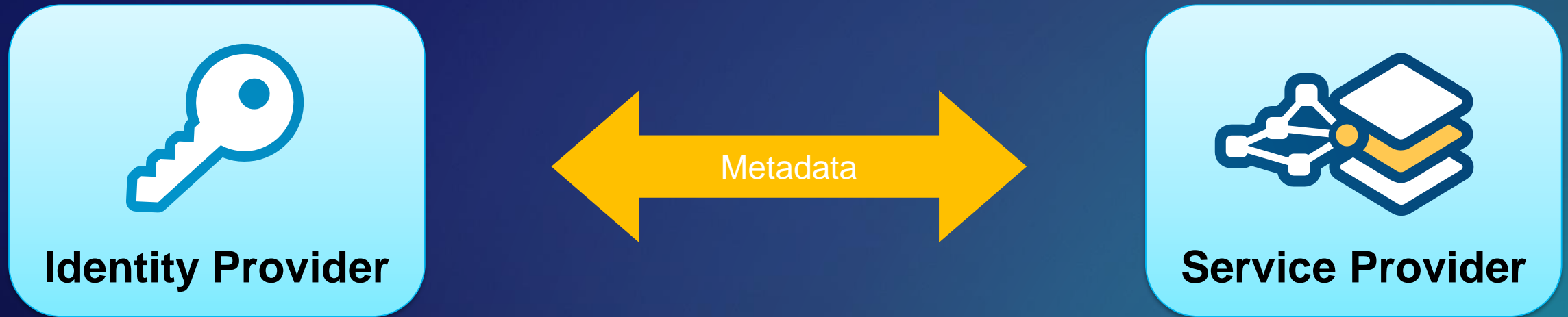
- Web browser
- ArcGIS for Desktop
- ArcGIS Pro
- Collector for ArcGIS



# Relationships Are All About Trust

The background features a dark teal gradient. On the left, there are several overlapping, semi-transparent geometric shapes in shades of teal, orange, and blue, creating a layered effect. On the right, a large, stylized graphic element consists of a red-to-orange gradient bar with several blue and teal rectangular blocks of varying heights and widths, resembling a bar chart or a data visualization. The overall aesthetic is modern and digital.

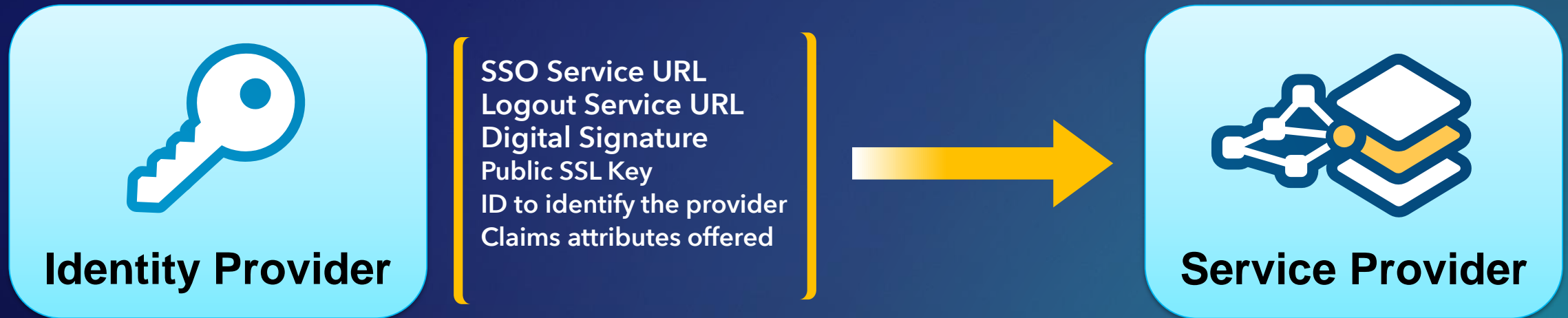
Relationships are all about Trust!



# Relationships are all about Trust!



# Relationships are all about Trust!





# What Happens During SAML authentication

The background features a dark teal gradient with abstract geometric patterns. On the left, there are diagonal lines in shades of teal and orange. On the right, there are more complex shapes, including a red-to-orange gradient area and several dark blue and teal rectangular blocks, some with thin white outlines. The overall aesthetic is modern and technical.

# The SAML Login Experience

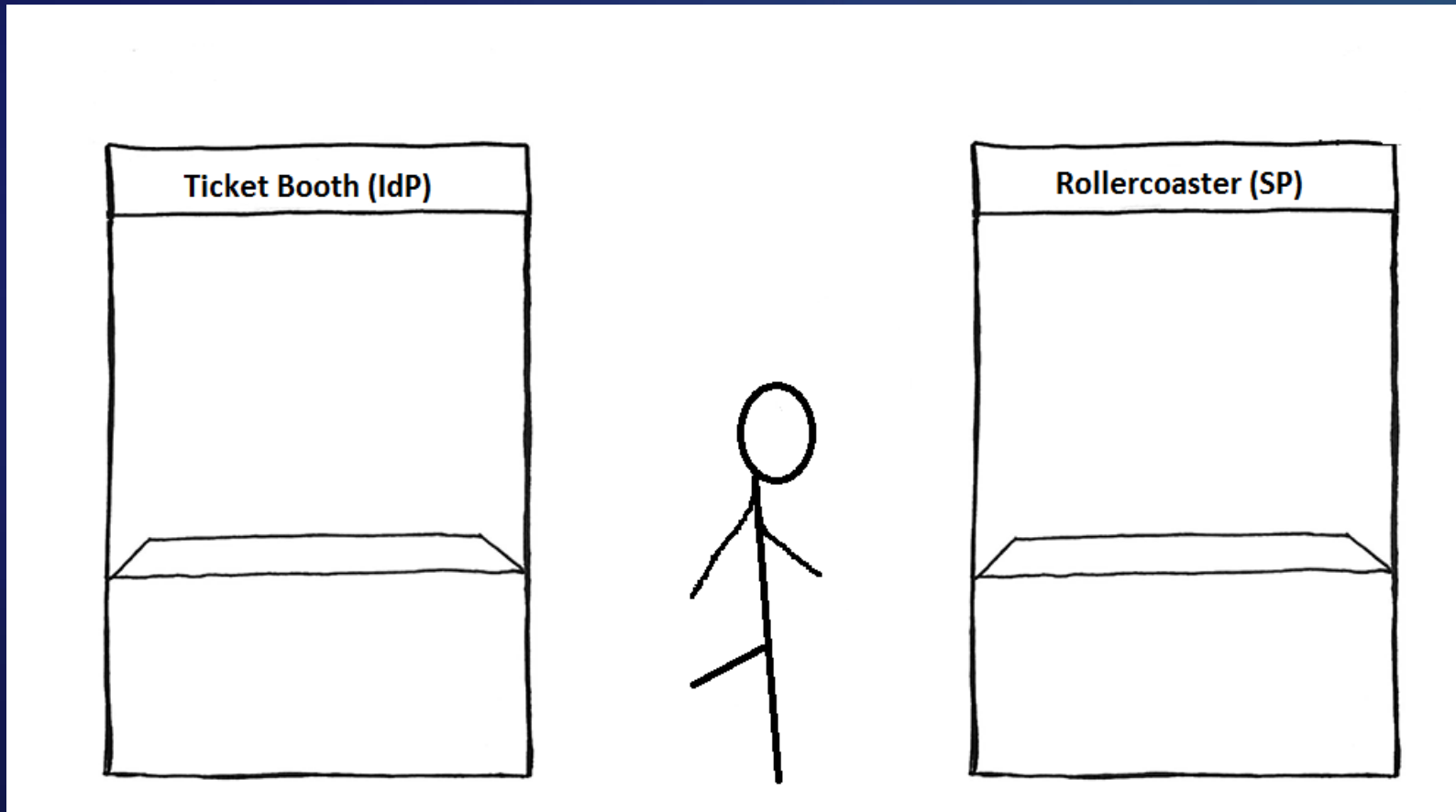


Service Provider Initiated Log On



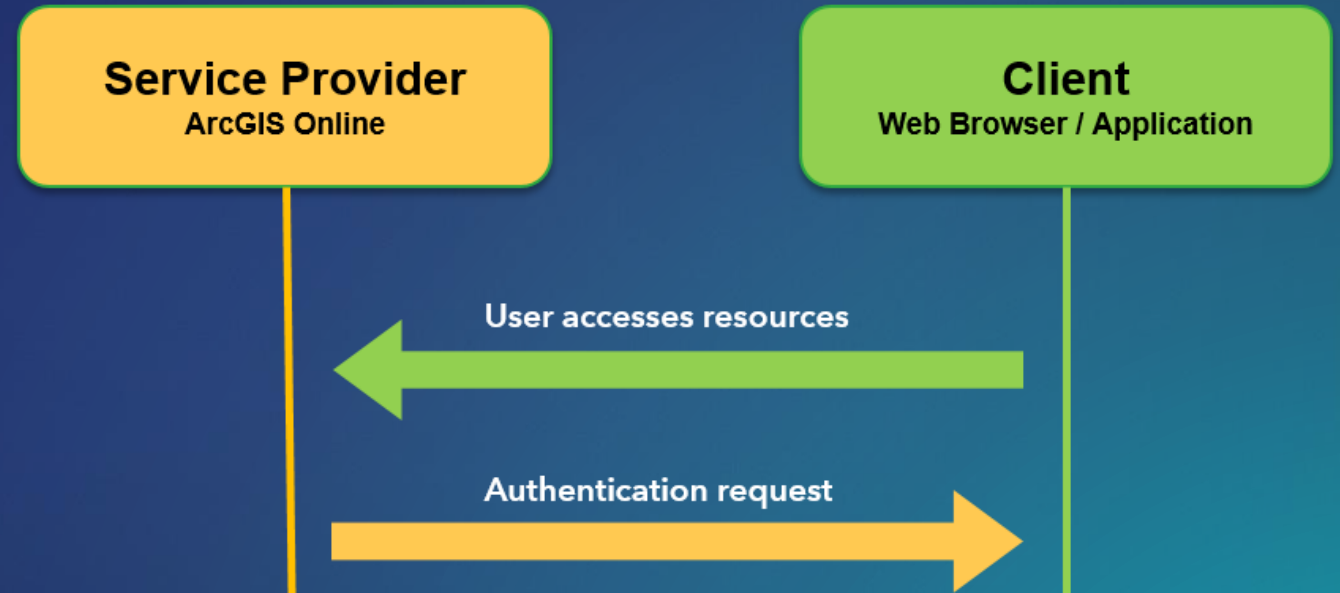
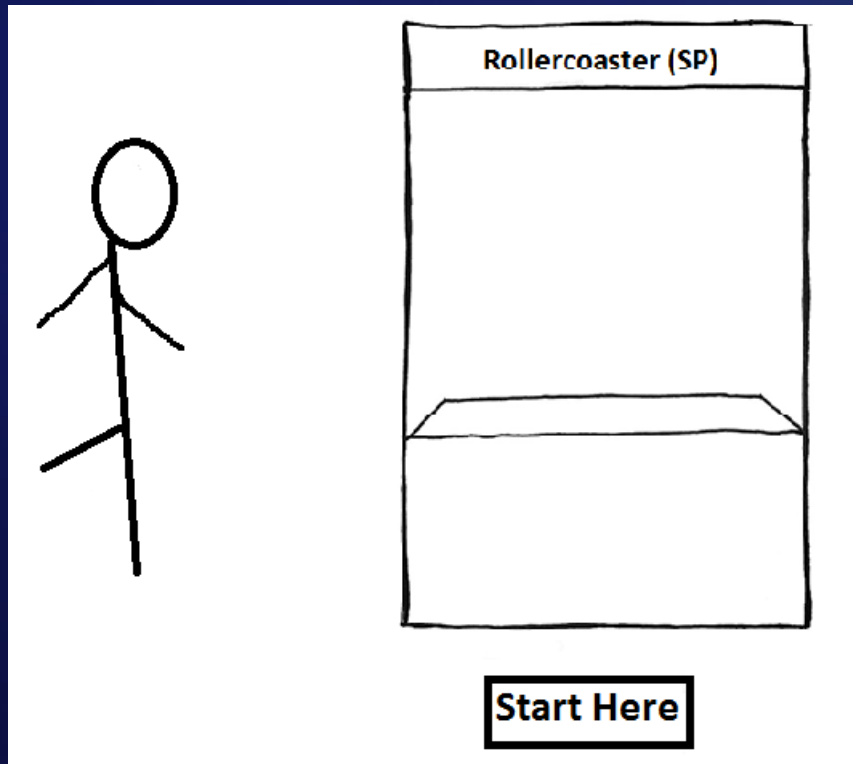
Identity Provider Initiated Log On

# What happens during SAML authentication?



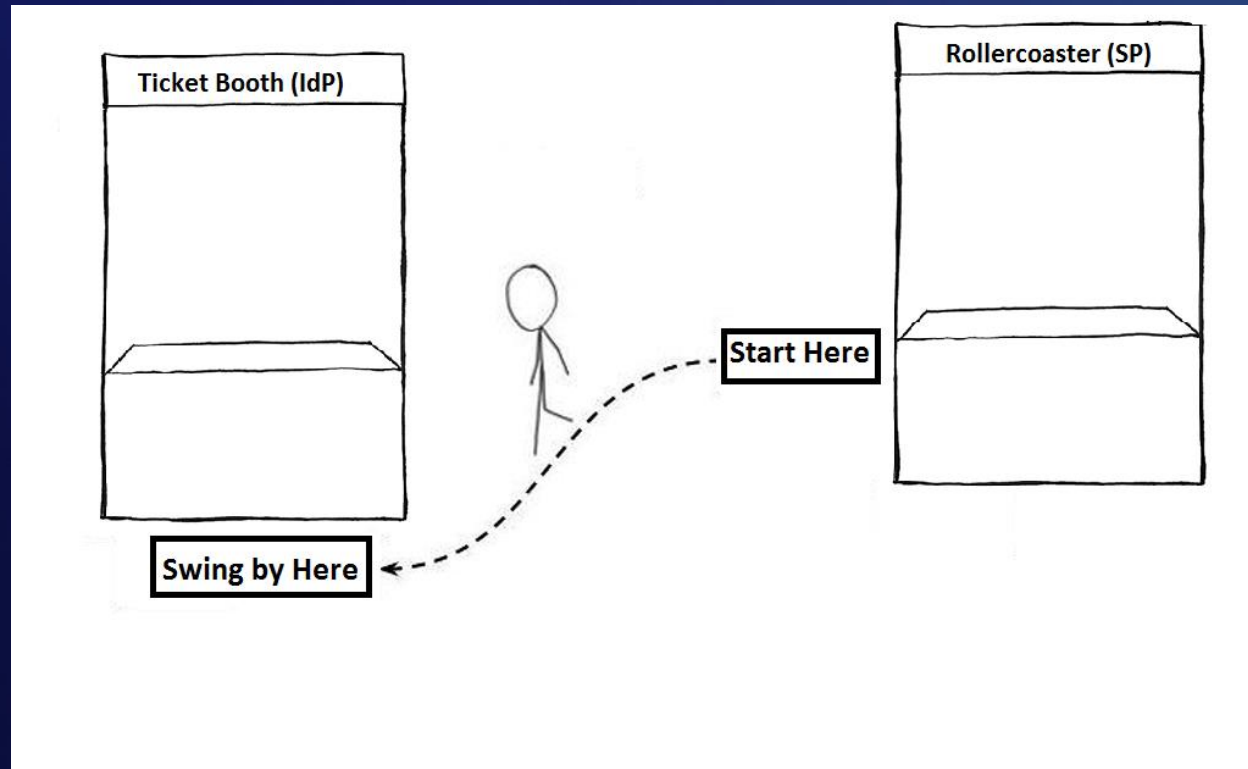
# What happens during SAML authentication?

## Authentication Request



# What happens during SAML authentication?

Authentication Request



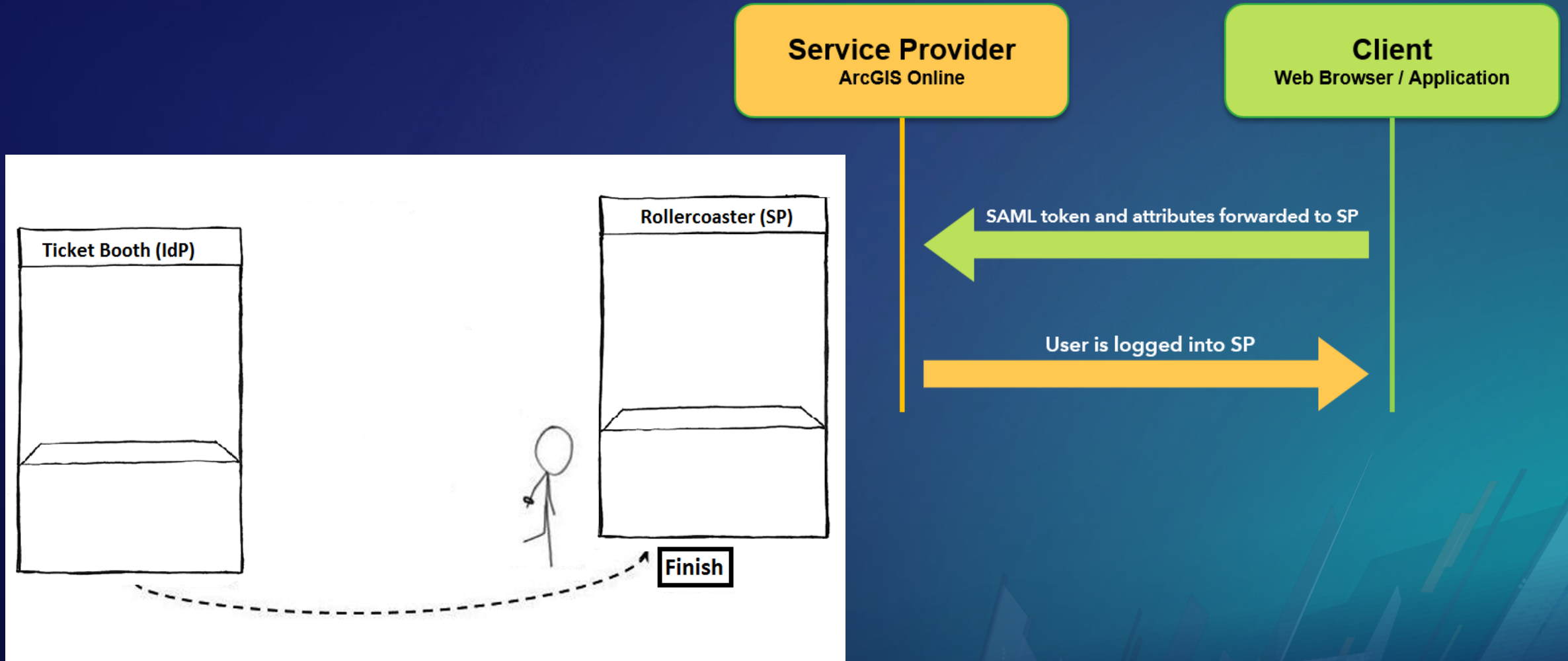
Authentication request forwarded to IdP

SAML token returned to client



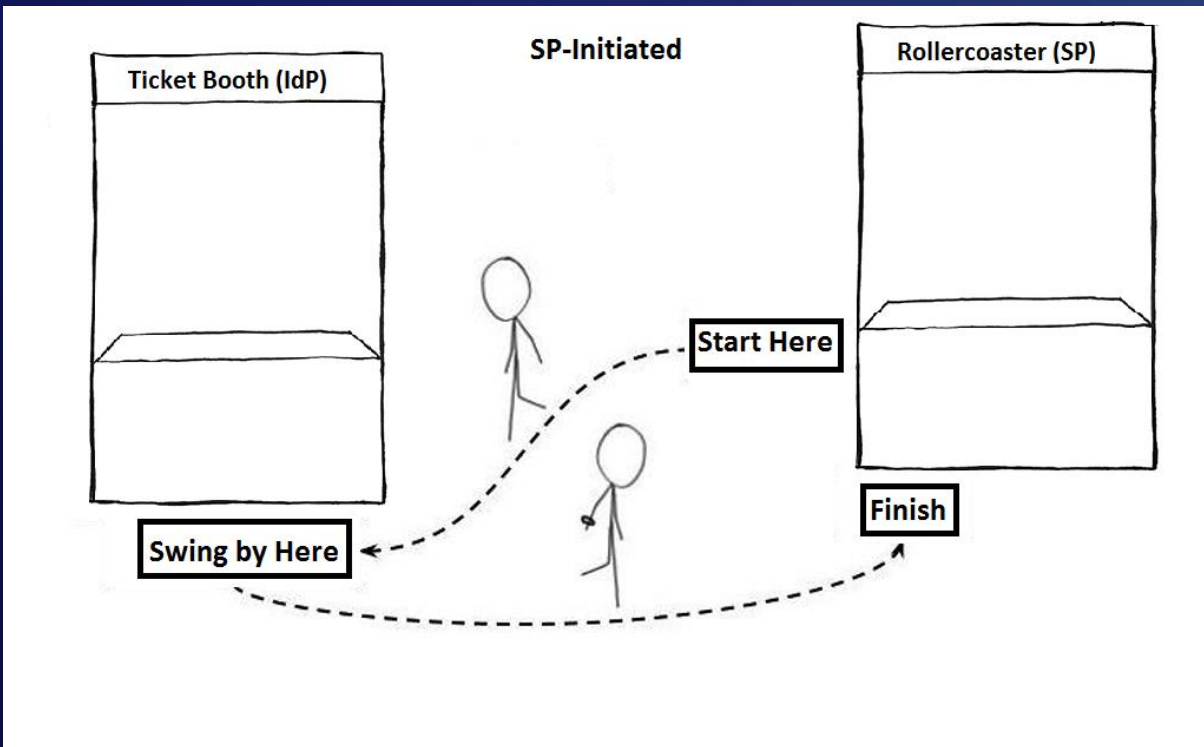
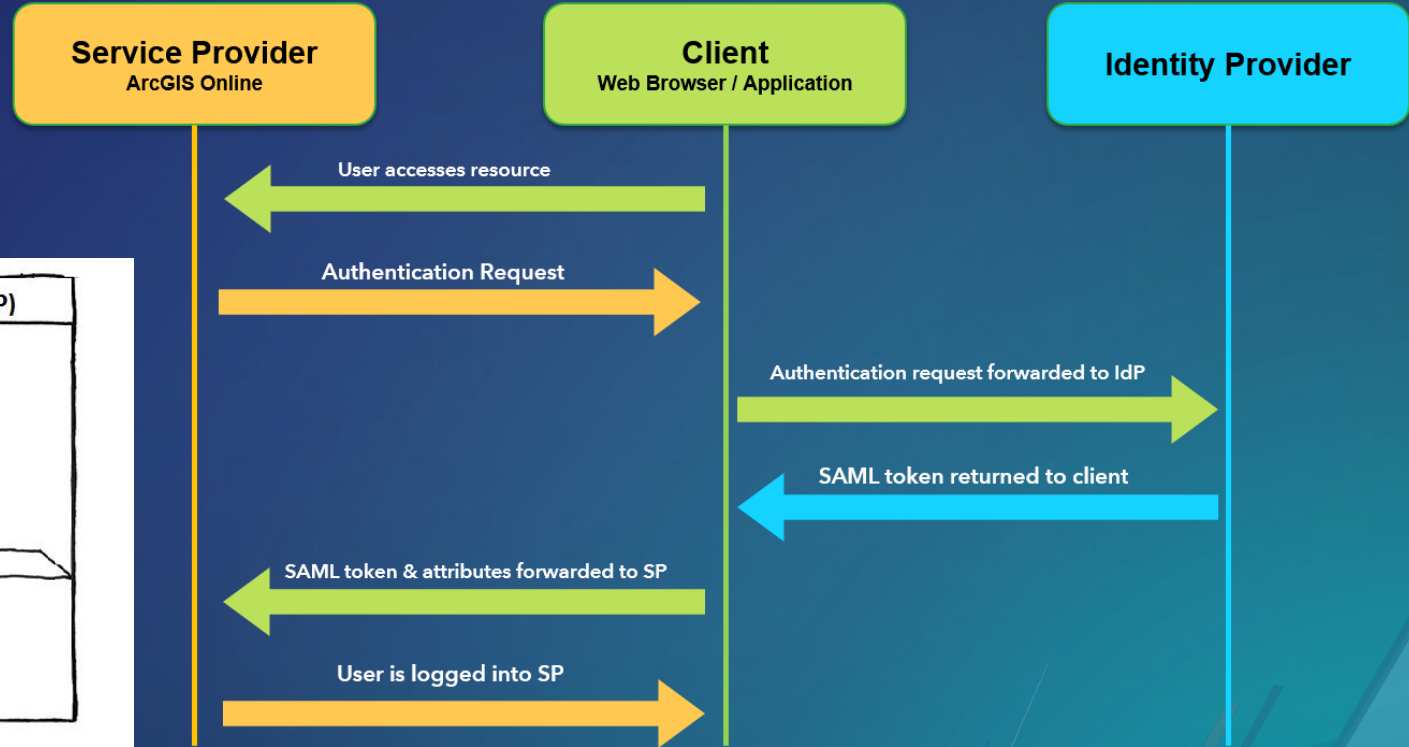
# What happens during SAML authentication?

Service Provider accepts SAML assertion



# What happens during SAML authentication?

## Service Provider Initiated Log In






Demo



SAML Jackson

https://samjackson.maps.arcgis.com/home/index.html

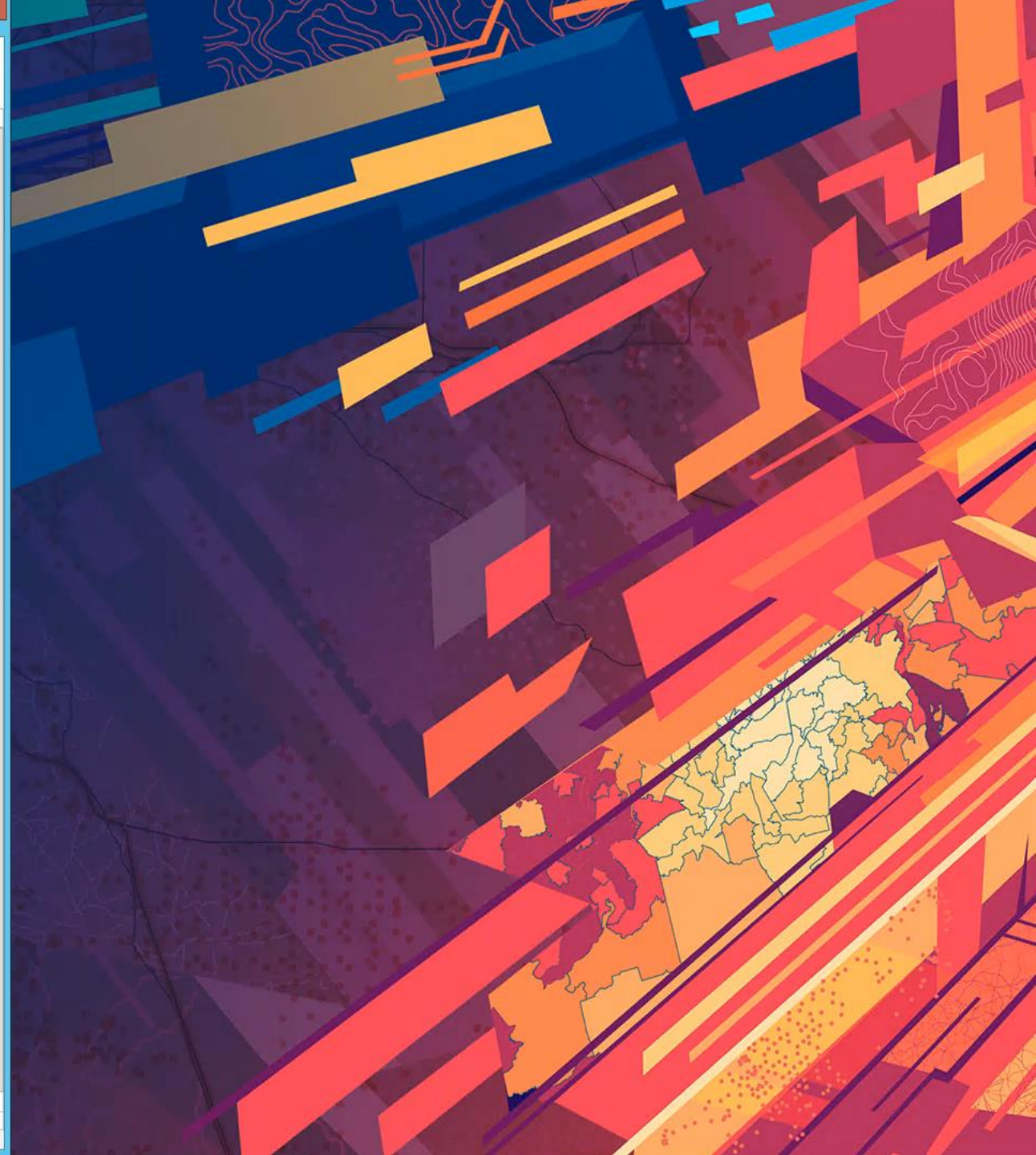
Home Gallery Map Scene Groups Sign In



# SAML Jackson

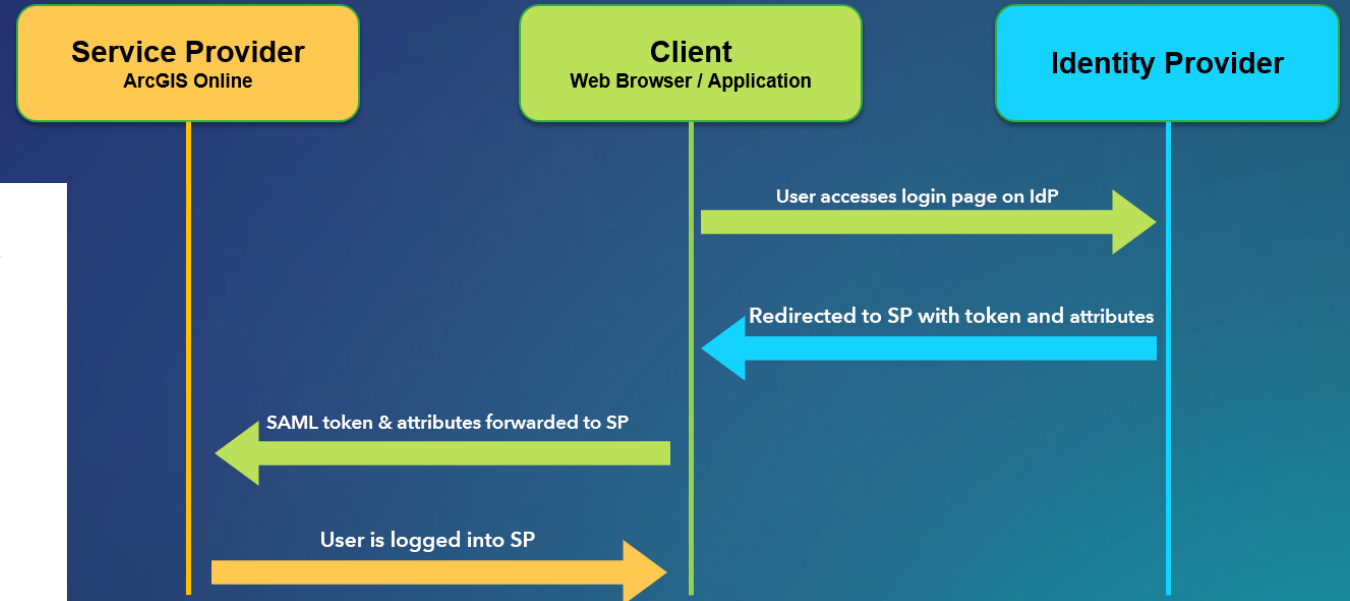
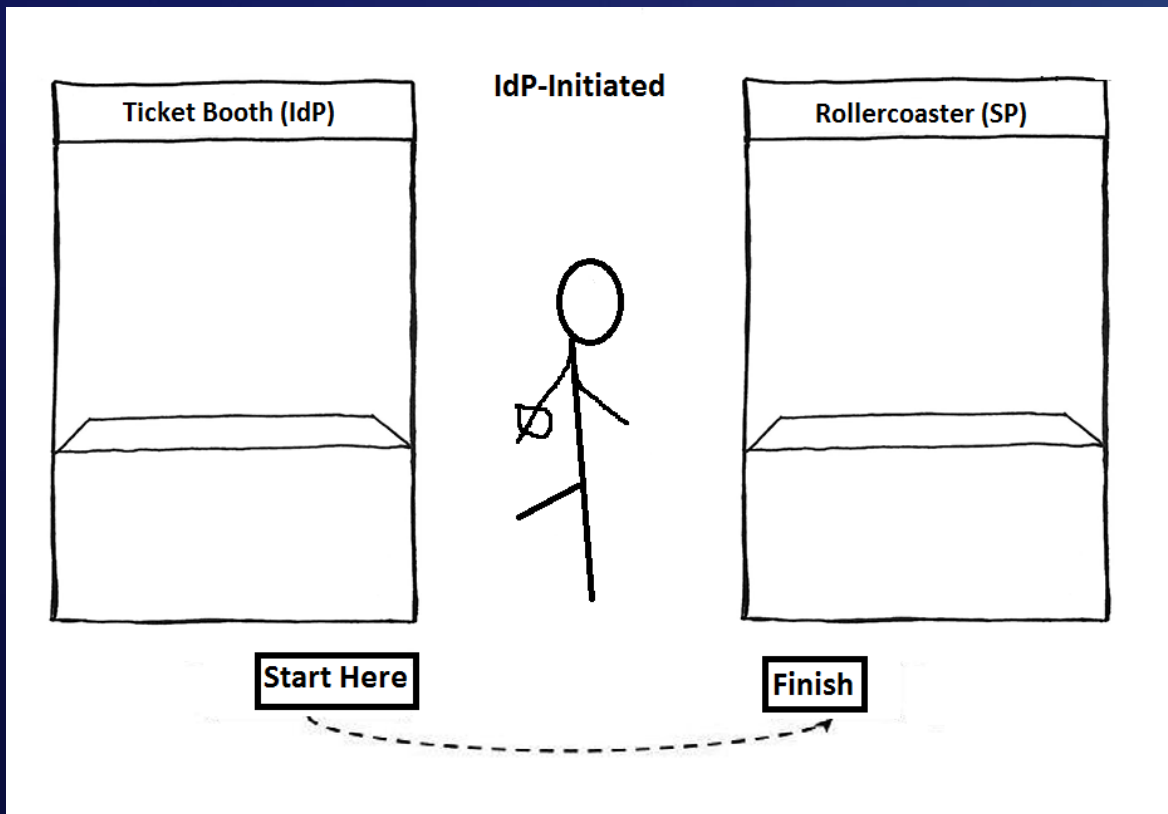
[Esri.com](#) | [Help](#) | [Terms of Use](#) | [Privacy](#) | [Contact Esri](#) | [Report Abuse](#)

This image shows a web browser window displaying the home page of a user named SAML Jackson. The browser's address bar shows the URL https://samjackson.maps.arcgis.com/home/index.html. The page features a navigation menu with links for Home, Gallery, Map, Scene, and Groups, along with a Sign In button and a search icon. A profile picture of SAML Jackson is displayed next to his name. At the bottom of the page, there are links for Esri.com, Help, Terms of Use, Privacy, Contact Esri, and Report Abuse. The browser window also shows standard navigation and window control buttons.



# What happens during SAML authentication?

## Identity Provider Initiated Log In



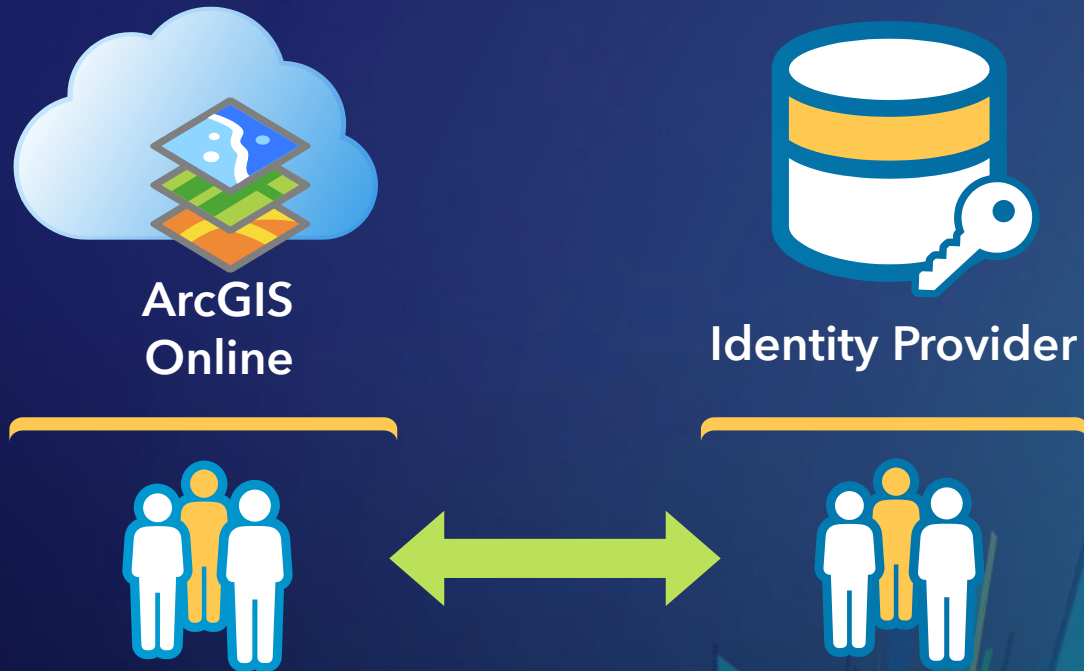


# Groups and Federation

The image features a dark teal background with a white title 'Groups and Federation' centered in the upper half. The design is decorated with abstract geometric elements: a cluster of overlapping lines in shades of teal and red in the top-left corner; a faint, light-colored grid pattern in the bottom-right; and several thick, diagonal bars in orange, dark blue, and light green in the bottom-right corner. The overall aesthetic is modern and technical.

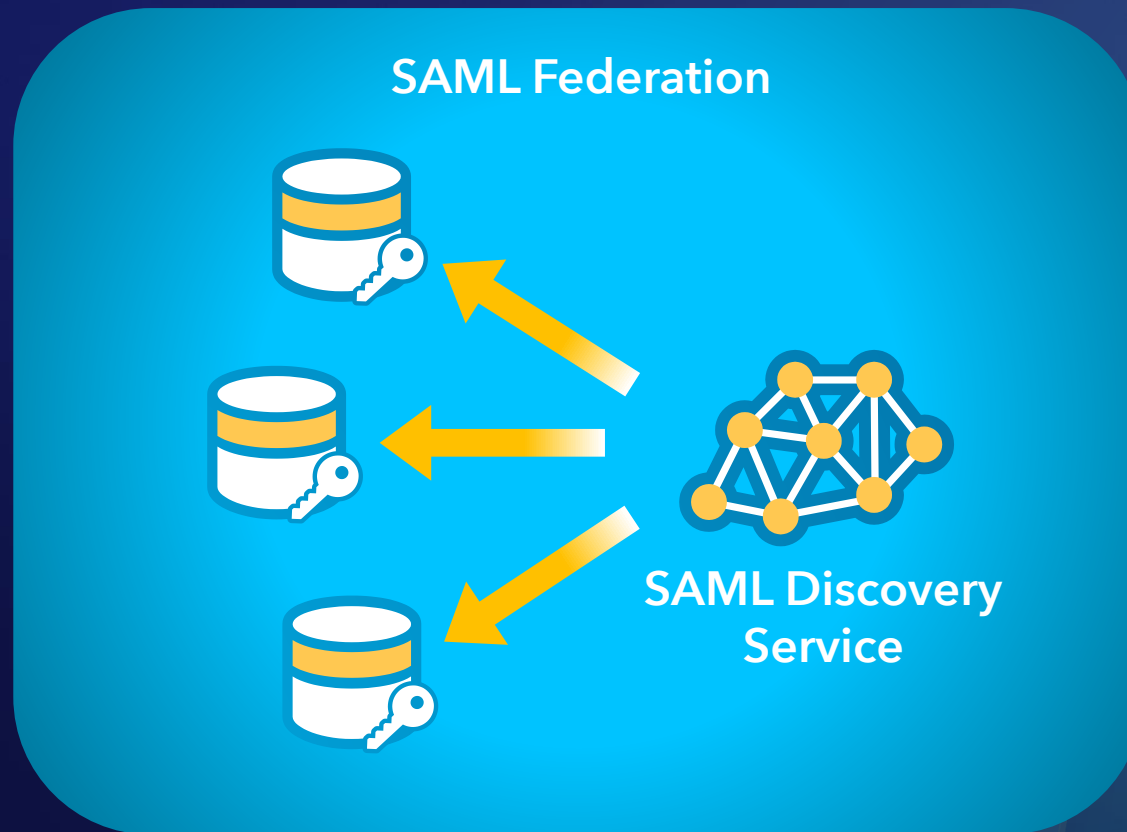
# New Feature: Enterprise Group Membership

- Allows enterprise groups to be linked to ArcGIS Online groups
- No need to invite users to a group!



# New Feature: SAML Federation

- Allows for flexibility in which IdP to use
- inCommon, Switchaai

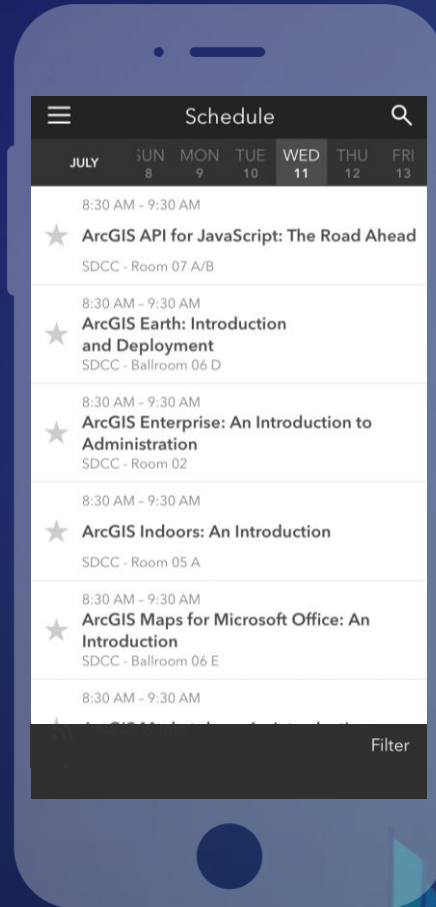


# Please Take Our Survey on the App

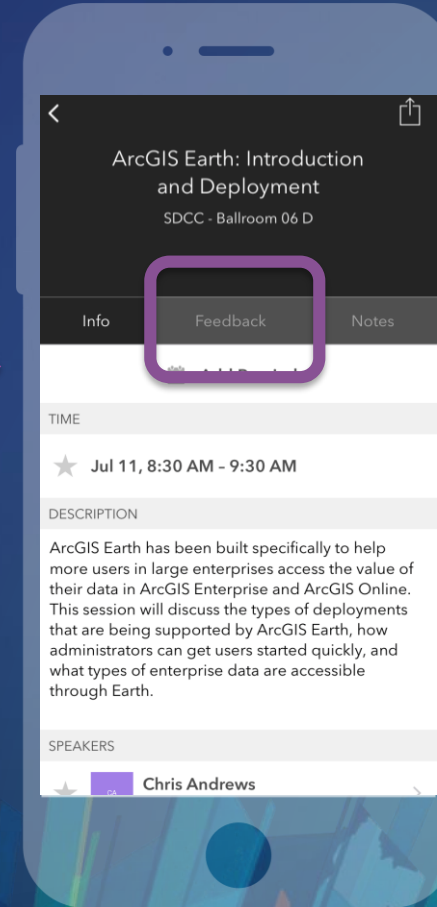
Download the Esri Events app and find your event



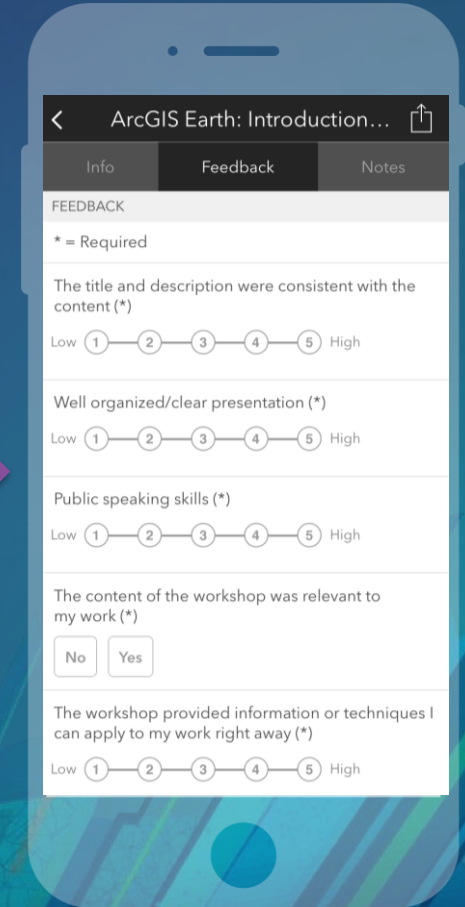
Select the session you attended



Scroll down to find the feedback section



Complete answers and select "Submit"







esri

THE  
SCIENCE  
OF  
WHERE