

# Dissecting SAML Authentication

Dennis Smith and Gary Lee

Desktop



Web



Device



Clients



Access / Identity



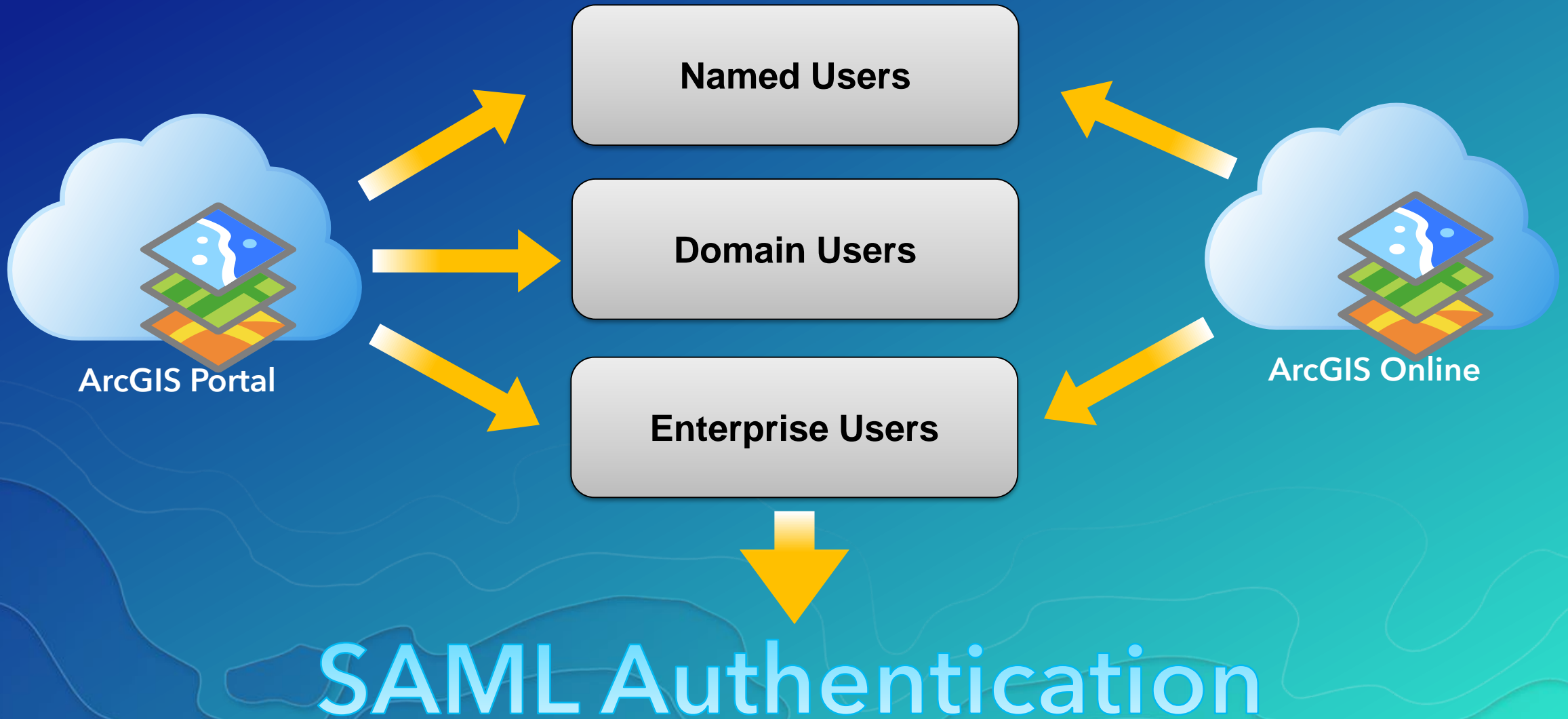
Server



Online Content and  
Services

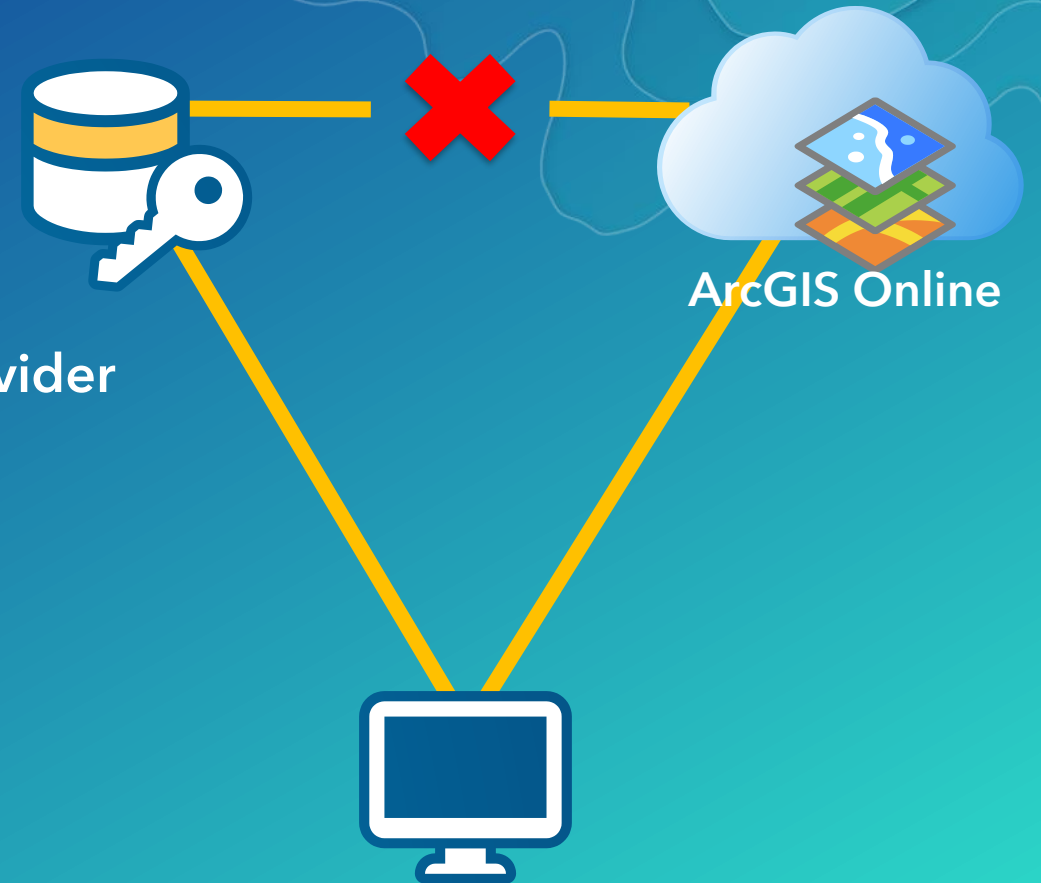
Services

How to authenticate?



# What is SAML?

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





# 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, Portal for ArcGIS



## Meet the Players: Service Provider

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



# 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

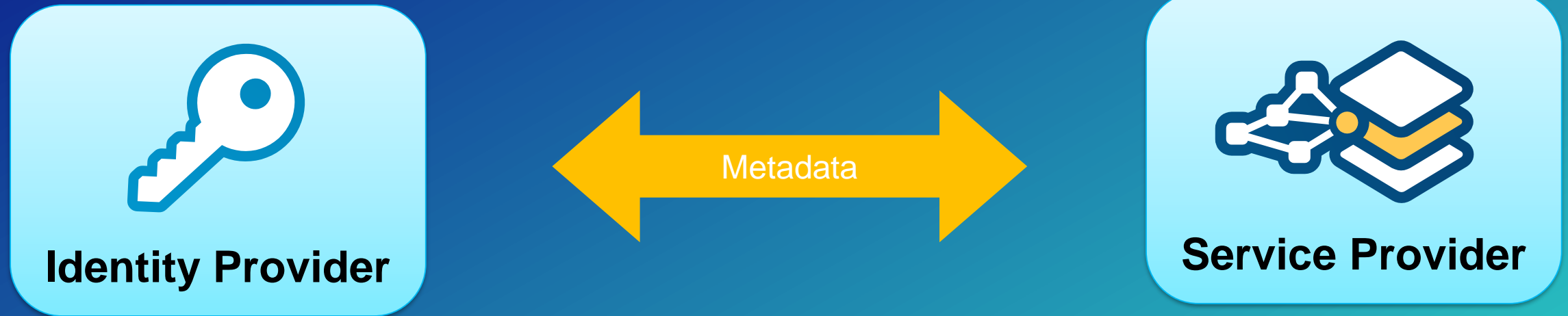
- Web browser
- ArcGIS for Desktop
- ArcGIS Pro
- Collector for ArcGIS



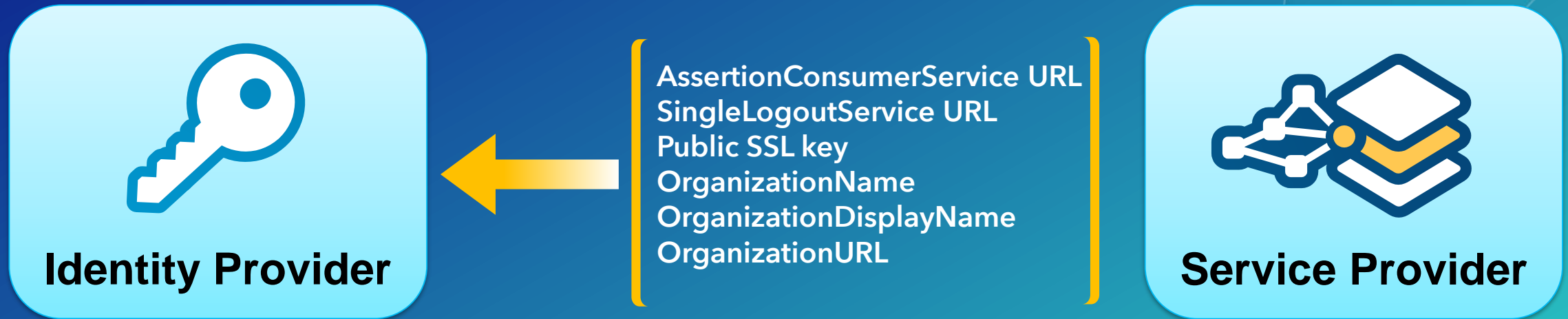
Relationships Are All About  
Trust



# Relationships are all about Trust!



# Relationships are all about Trust!





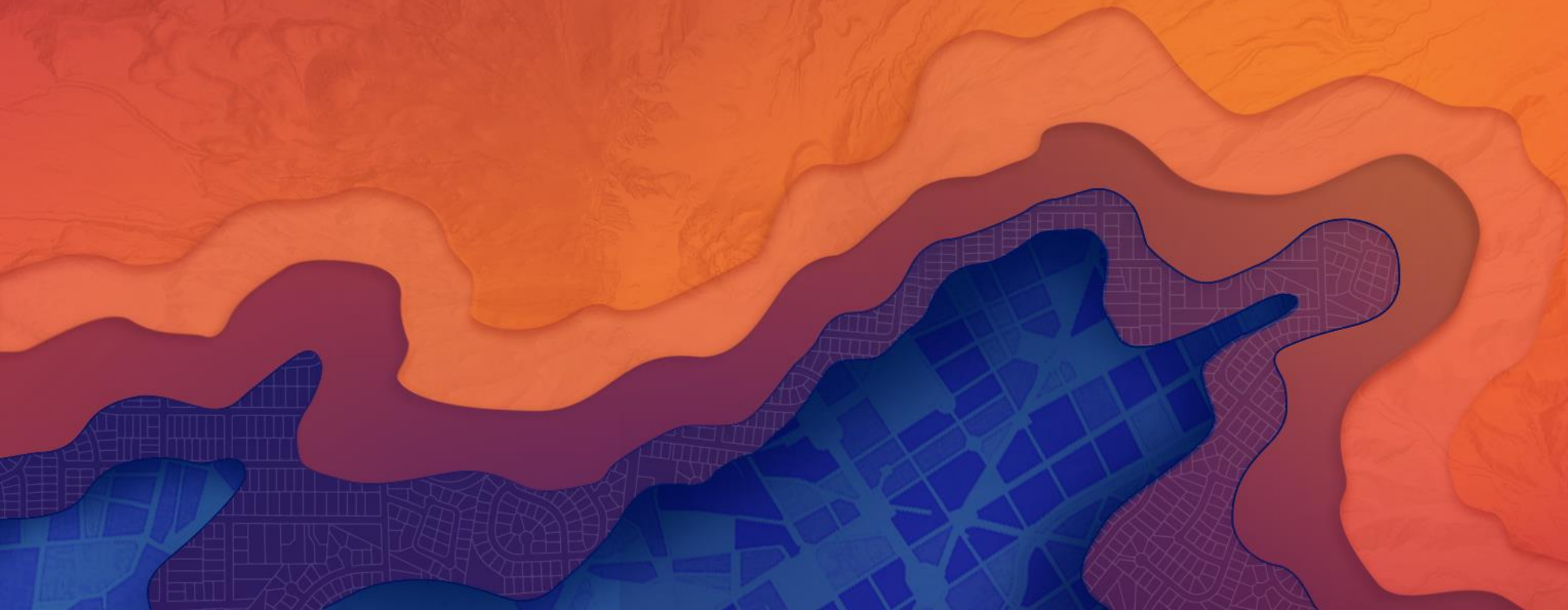
# Relationships are all about Trust!



SSO Service URL  
Logout Service URL  
Digital Signature  
Public SSL Key  
ID to identify the provider  
Claims attributes offered



# What Happens During SAML authentication

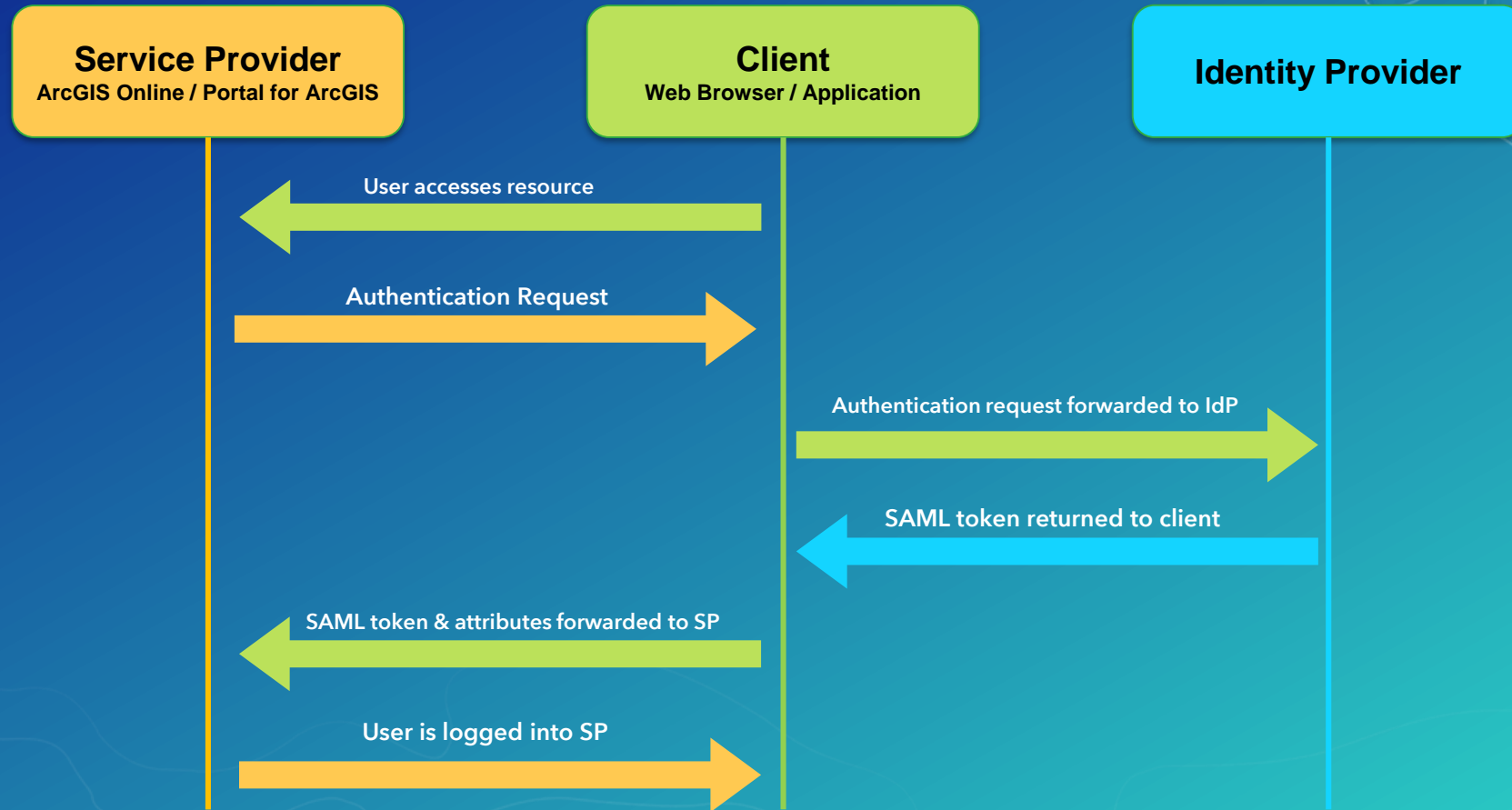


# What happens during SAML authentication?

- Requests sent via HTTP/HTTPS in XML format
- Client acts as the middleman between the SP and IdP
- Service Provider Initiated Log on
- Identity Provider Initiated Log on

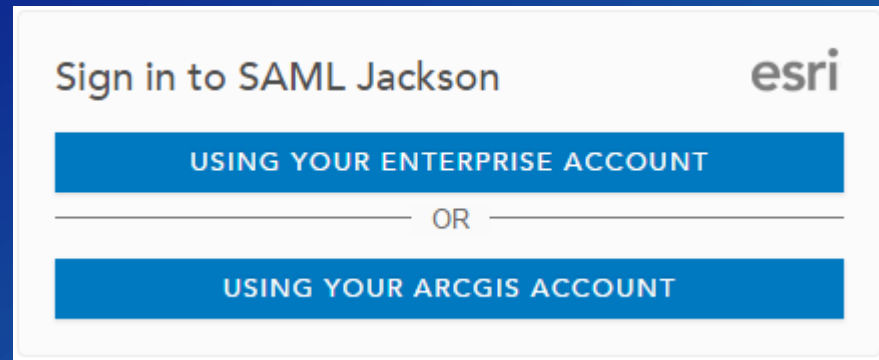


# What happens during SAML authentication?



# What happens during SAML authentication?

## Authentication Request

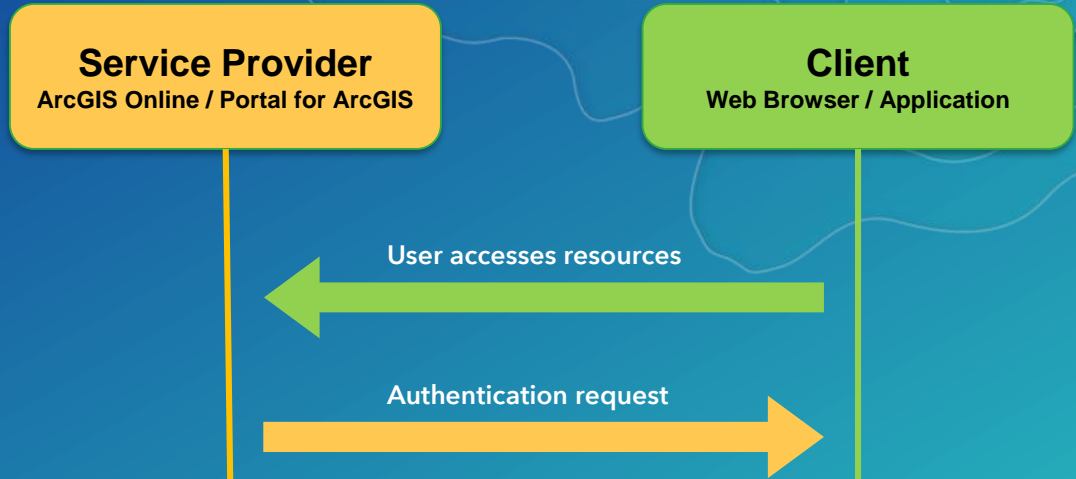


Sign in to SAML Jackson **esri**

USING YOUR ENTERPRISE ACCOUNT

OR

USING YOUR ARCGIS ACCOUNT



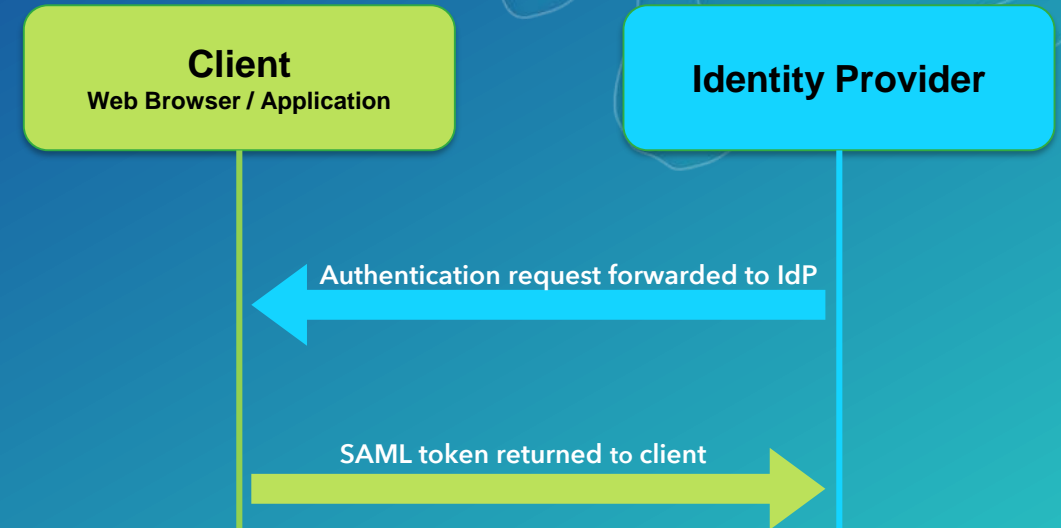
```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_MXHGFlwzfYcalbAY"
  Version="2.0"
  IssueInstant="2016-06-10T21:51:00Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  AssertionConsumerServiceURL="https://samljackson.maps.arcgis.com/sharing/rest/oauth2/saml/signin"
>
  <saml:Issuer>samljackson.maps.arcgis.com</saml:Issuer>
  <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
    AllowCreate="true"
  />
</samlp:AuthnRequest>
```



# What happens during SAML authentication?

## Authentication Request

1. IdP checks if user is currently authenticated
2. If user is not currently authenticated, user is challenged for credentials
3. IdP attempts to authenticate user
4. A SAML assertion is generated and sent to the AssertionConsumerService URL

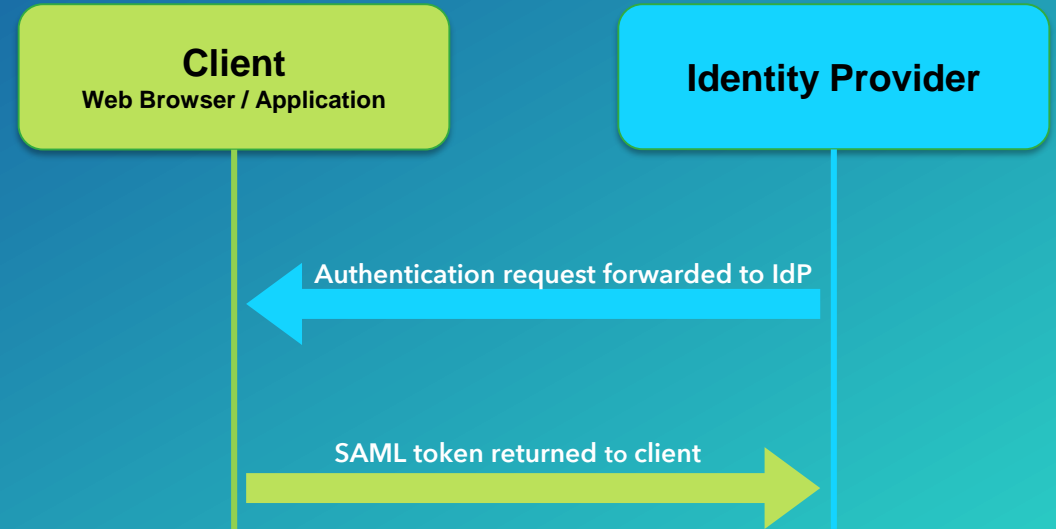


# What happens during SAML authentication?

## Authentication Response

```
<samlp:Response ID="_347a97d7-3c54-42af-803a-b1b0d30bff75"
  Version="2.0"
  IssueInstant="2016-06-17T15:38:35.916Z"

  Destination="https://samljackson.maps.arcgis.com/sharing/rest/oauth2/saml/signin"
  Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
  InResponseTo="_ietsFmljfxKxASck"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  >
    <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://red-inf-adfs-
d1.esri.com/adfs/services/trust</Issuer>
    ...
    <Subject>
      <NameID>dani7807</NameID>
      <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
        <SubjectConfirmationData InResponseTo="_ietsFmljfxKxASck"
          NotOnOrAfter="2016-06-17T15:43:35.916Z"
        />
      </SubjectConfirmation>
    </Subject>
    Recipient="https://samljackson.maps.arcgis.com/sharing/rest/oauth2/saml/signin"
    </SubjectConfirmation>
    </Subject>
    <Conditions NotBefore="2016-06-17T15:38:35.896Z"
      NotOnOrAfter="2016-06-17T16:38:35.896Z"
    >
      <AudienceRestriction>
        <Audience>samljackson.maps.arcgis.com</Audience>
      </AudienceRestriction>
    </Conditions>
    <AttributeStatement>
      <Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname">
        <AttributeValue>Daniel Urbach</AttributeValue>
      </Attribute>
      <Attribute
        Name="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress">
        <AttributeValue>Durbach@esri.com</AttributeValue>
      </Attribute>
    </AttributeStatement>
    <AuthnStatement AuthnInstant="2016-06-17T15:38:35.227Z"
      SessionIndex="_b5b4d81f-b440-432b-bf42-07af671d7970"
    >
      <AuthnContext>
        <AuthnContextClassRef>urn:federation:authentication:windows</AuthnContextClassRef>
      </AuthnContext>
    </AuthnStatement>
  </Assertion>
</samlp:Response>
```




# What happens during SAML authentication?

Service Provider accepts SAML assertion

[EDIT MY PROFILE](#)

## Cameron's Profile



**First Name**  
Cameron

**Last Name**  
Kroeker

**Email**  
CKroeker@esri.com

**Username**  
came7624\_samljackson

**Bio**  
Write something about yourself. You might include things like:

- Your organization
- Contact information
- Areas of expertise
- Interests
- Any other information you'd like others to know

**Link Your ArcGIS Accounts**  
[Manage Linked Accounts](#)

**Who can see your profile?**  
Organization

**Language**  
English-English

**Region**  
United States

**Units**  
US Standard

**Level**  
2

**Role**  
Administrator

**Organization**  
SAML Jackson

**Organization URL**  
<https://samljackson.maps.arcgis.com>

**Licensed Products**  
ArcGIS Pro

**Service Provider**  
ArcGIS Online / Portal for ArcGIS

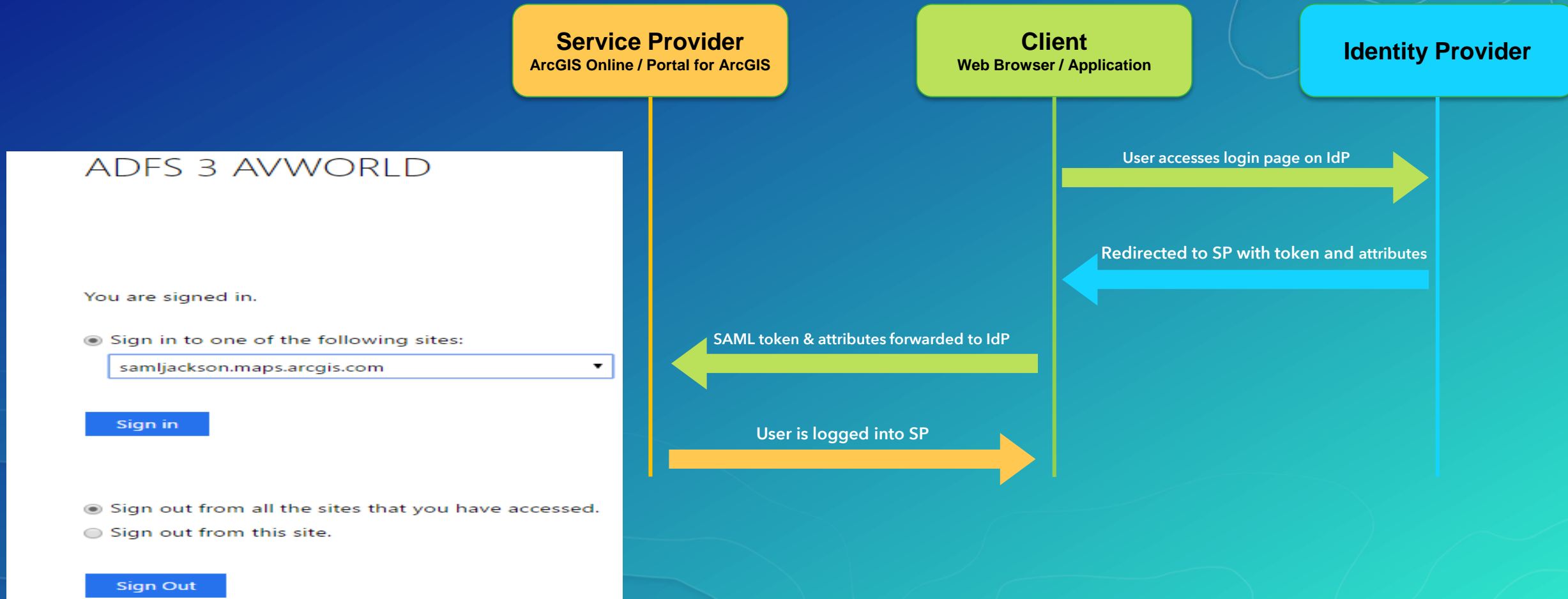
**Client**  
Web Browser / Application

SAML token and attributes forwarded to SP

User is logged into SP

# What happens during SAML authentication?

## Identity Provider Initiated Log In







Demo



The background is a solid blue color with subtle, wavy, organic patterns in lighter and darker shades of blue, creating a textured, water-like effect.

# Questions?



esri

THE  
SCIENCE  
OF  
WHERE