Dissecting SAML Authentication

Dennis Smith and Gary Lee
How to authenticate?

ArcGIS Portal

ArcGIS Online

Named Users

Domain Users

Enterprise Users

SAML Authentication
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

Client

ArcGIS Online

External Domain(s)

Firewall

DMZ

IdP: ADFS

Firewall

Active Directory

Internal Domain
Meet the Players: Client

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

ArcGIS Online
Relationships Are All About Trust
Relationships are all about Trust!

Identity Provider

Metadata

Service Provider
Relationships are all about Trust!

Identity Provider

AssertionConsumerService URL
SingleLogoutService URL
Public SSL key
OrganizationName
OrganizationDisplayName
OrganizationURL

Service Provider
Relationships are all about Trust!

Identity Provider

SSO Service URL
Logout Service URL
Digital Signature
Public SSL Key
ID to identify the provider
Guides 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?

Service Provider
ArcGIS Online / Portal for ArcGIS

Client
Web Browser / Application

Identity Provider

- User accesses resource
- Authentication Request
- SAML token & attributes forwarded to SP
- User is logged into SP
- Authentication request forwarded to IdP
- SAML token returned to client
- User accesses resource
What happens during SAML authentication?

Authentication Request

Service Provider
ArcGIS Online / Portal for ArcGIS

Client
Web Browser / Application

User accesses resources

Authentication request

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
  <samlp:AuthnRequest
    ID="SWXGF1wzYcalhAY"
    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>
    <saml:NameIDPolicy Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
      AllowCreate="true"
    />
  </samlp:AuthnRequest>
```

Sign in to SAML Jackson

USING YOUR ENTERPRISE ACCOUNT

OR

USING YOUR ARCGIS ACCOUNT
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

Client
Web Browser / Application

Identity Provider

Authentication request forwarded to IdP
SAML token returned to client
What happens during SAML authentication?

Service Provider accepts SAML assertion

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

Service Provider
ArcGIS Online / Portal for ArcGIS

Client
Web Browser / Application

Identity Provider

User accesses login page on IdP

Redirected to SP with token and attributes

SAML token & attributes forwarded to IdP

User is logged into SP

You are signed in.

Sign in to one of the following sites:

samljackson.maps.arcgis.com

Sign in

Sign out from all the sites that you have accessed.

Sign out from this site.

Sign Out
Demo
Questions?