Session 2.1: Federations: Foundation

Scott Koranda

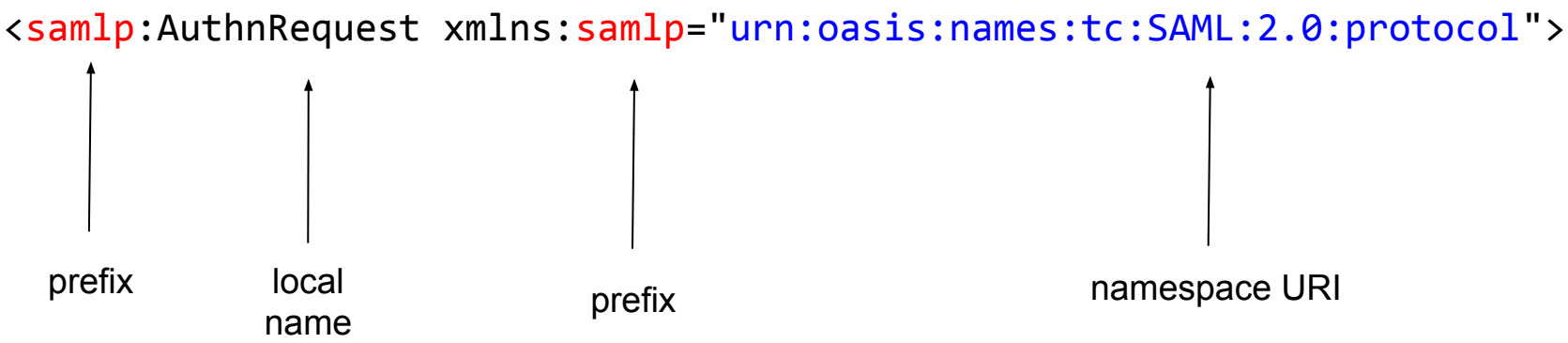
Support provided by the
National Institute of Allergy and Infectious Diseases

Scott Koranda's participation has been funded in whole or in part with federal funds from the National Institute of Allergy and Infectious Diseases (NIAID), National Institutes of Health (NIH), under Contract Nos. HHSN316201200160W/D14PD00002 & D13PD01160. The content of this presentation does not necessarily reflect the views or policies of the Department of Health and Human Services, nor does mention of trade names, commercial products, or organizations imply endorsement by the U.S. Government.

SAML

Thar be XML...

Quick Aside on XML Namespaces



These Two Elements Are The Same

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

<s:AuthnRequest
    xmlns:s="urn:oasis:names:tc:SAML:2.0:protocol">
```

These Two Elements Are NOT The Same

```
<samlp:AuthnRequest
    xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

<AuthnRequest>
```

Multiple Namespaces

```
<md:EntityDescriptor
        xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
        entityID="https://login.sphericalcowgroup.com/idp/shibboleth">
```

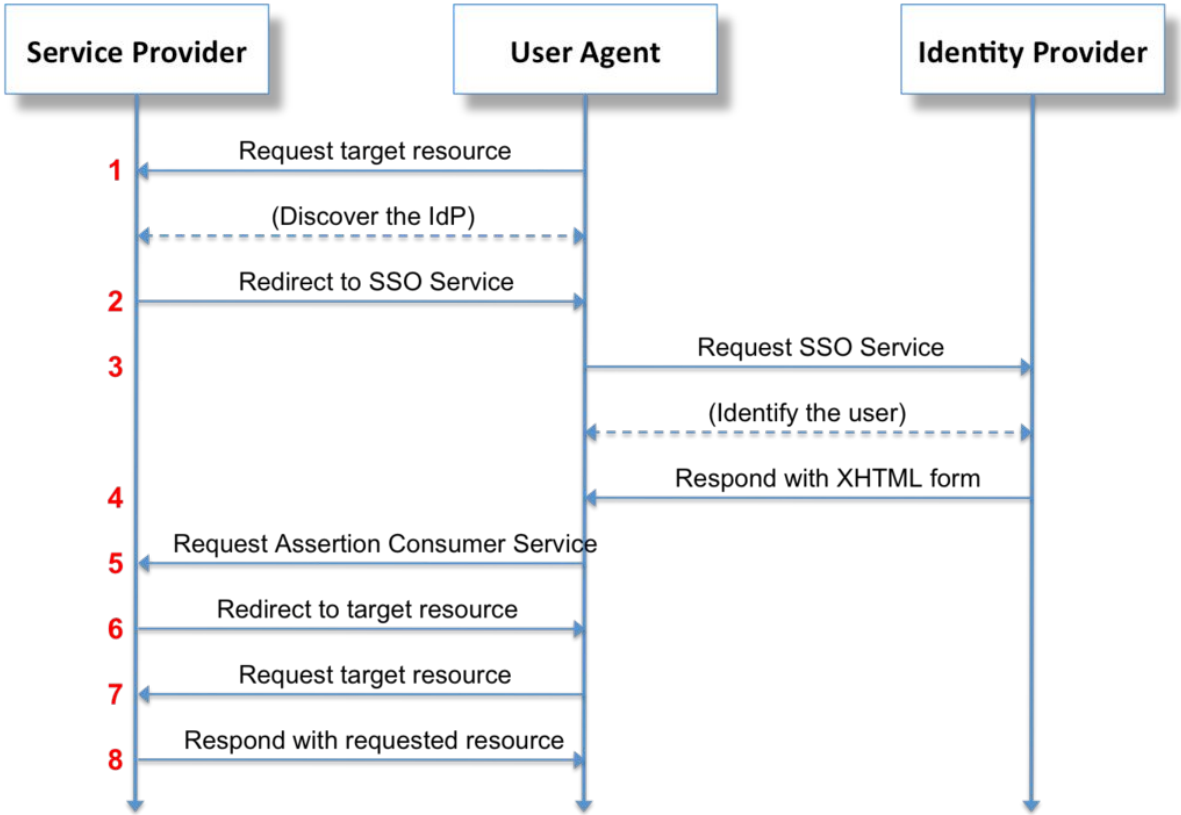
Default Namespace

```
<EntityDescriptor
        xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
        xmlns:shibmd="urn:mace:shibboleth:metadata:1.0"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
        entityID="https://login.sphericalcowgroup.com/idp/shibboleth">
```

Security Assertion Markup Language

- Security framework and open standard defined by OASIS
  - series of technical documents and XML schemas
- Focus on SAML web browser single sign-on profile (SAML WebSSO)
- Focus still further on SAML2 Interoperability Deployment Profile V1.0
  - SAML2int
  - Designed by and for higher education and research to improve interoperability
  - https://kantarainitiative.github.io/SAMLprofiles/saml2int.html
  - Version 2 being proposed now...

SAML Web Browser SSO: Protocol Overview



SAML tracer – Add-ons for Firef

Mozilla Foundation (US) https://ad

Search

Developer Hub Register or Log in

Firefox Add-ons Explore Extensions Themes More...

Find add-ons

SAML tracer

by Olav Morken, Jaime Perez

Debug and view SAML messages

+ Add to Firefox

16,200 Users

16 Reviews

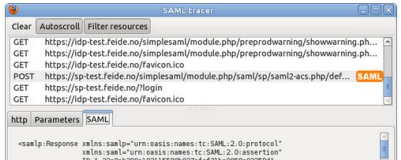
Overall Rating

Rate your experience

How are you enjoying your experience with SAML tracer?

Log in to rate this extension

Screenshots



Trace Your SAML Web SSO Flow

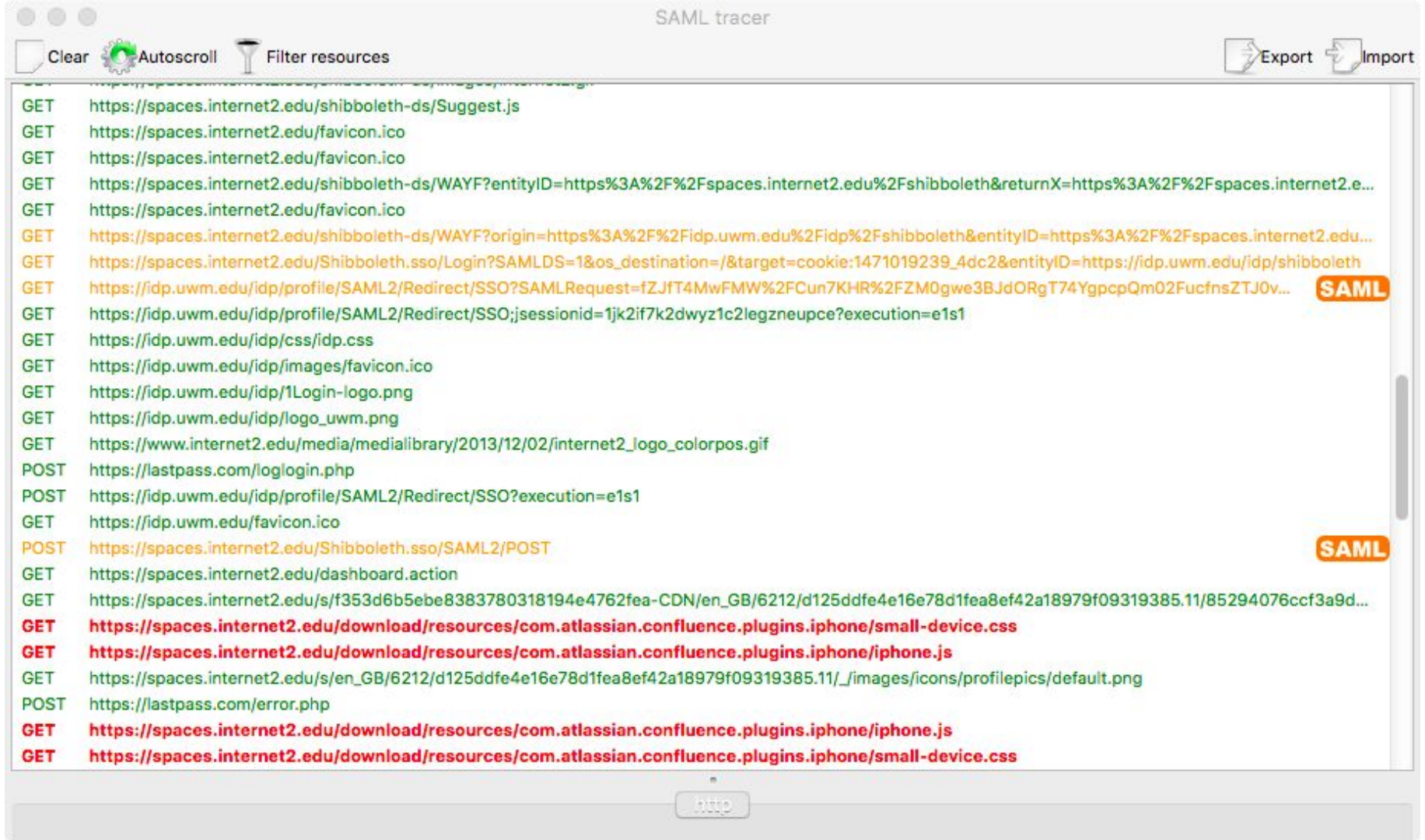
- SAML tracer Add-on for FireFox
- SAML DevTools extension for Chrome is also available
- Other tools useable but involve more work
  - LiveHTTPHeaders
  - Safari Web Inspector
  - Fiddler
  - Often combined with https://www.samltool.com/

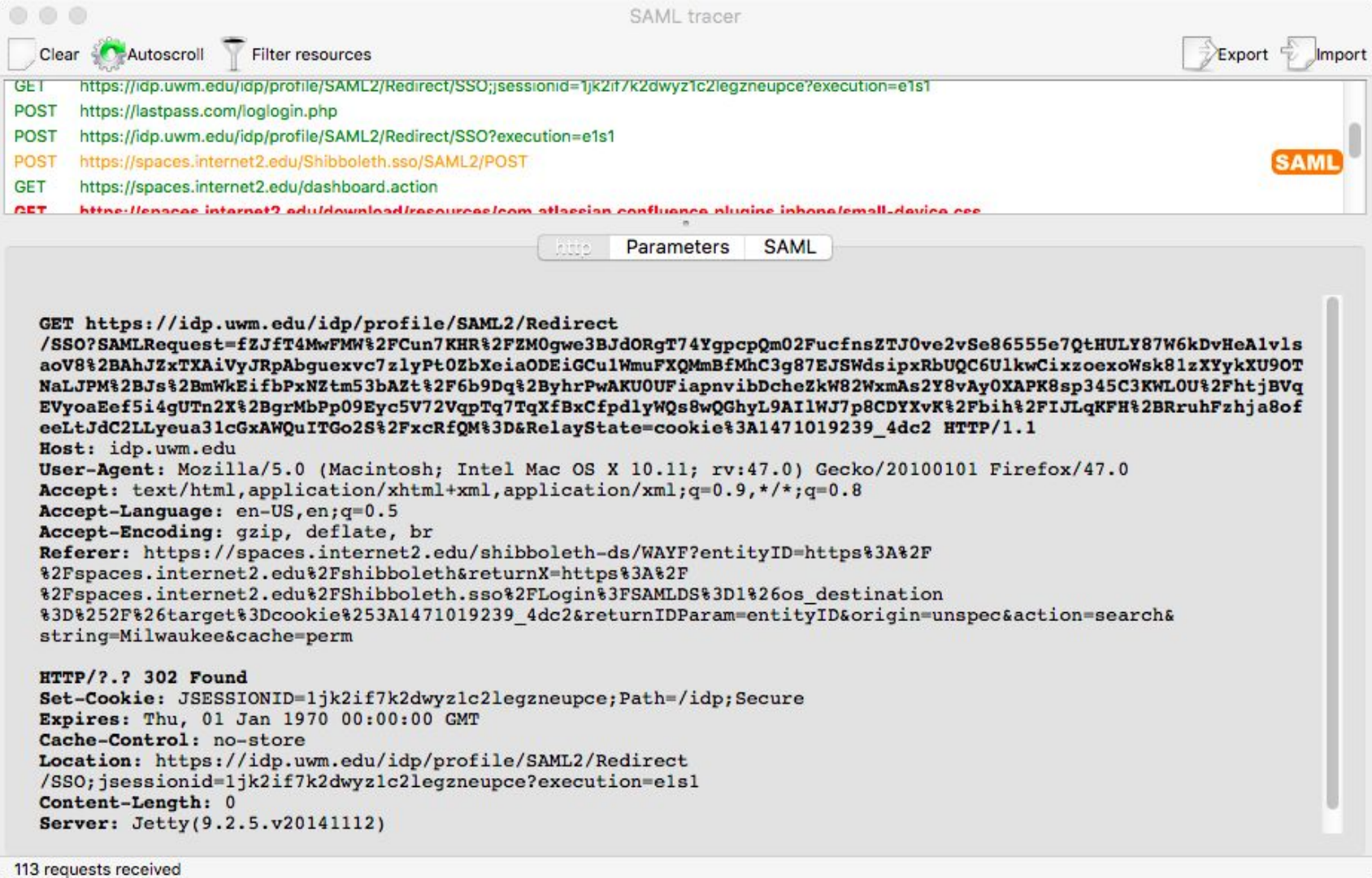
SAML Tracer Exercise

Start SAML Tracer and then browse to

`https://monitor.eduroam.org/`

Click "Login" and then choose your Identity Provider (login server) and authenticate.


SAML tracer
Clear
Autoscroll
Filter resources
Export
Import
GET https://spaces.internet2.edu/shibboleth-ds/Suggest.js
GET https://spaces.internet2.edu/favicon.ico
GET https://spaces.internet2.edu/favicon.ico
GET https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F%2Fspaces.internet2.edu%2Fshibboleth&returnX=https%3A%2F%2Fspaces.internet2.e...
GET https://spaces.internet2.edu/favicon.ico
GET https://spaces.internet2.edu/shibboleth-ds/WAYF?origin=https%3A%2F%2Fidp.uwm.edu%2Fidp%2Fshibboleth&entityID=https%3A%2F%2Fspaces.internet2.edu...
GET https://spaces.internet2.edu/Shibboleth.sso/Login?SAMLDS=1&os_destination=/&target=cookie:1471019239_4dc2&entityID=https://idp.uwm.edu/idp/shibboleth
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?SAMLRequest=fZJfT4MwFMW%2FCun7KHR%2FZM0gwe3BJdORgT74YgpcpQm02FucfnsZTJ0v... SAML
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO;jsessionid=1jk2if7k2dwyz1c2legzneupce?execution=e1s1
GET https://idp.uwm.edu/idp/css/idp.css
GET https://idp.uwm.edu/idp/images/favicon.ico
GET https://idp.uwm.edu/idp/1Login-logo.png
GET https://idp.uwm.edu/idp/logo_uwm.png
GET https://www.internet2.edu/media/medialibrary/2013/12/02/internet2_logo_colorpos.gif
POST https://lastpass.com/loglogin.php
POST https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
GET https://idp.uwm.edu/favicon.ico
POST https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST SAML
GET https://spaces.internet2.edu/dashboard.action
GET https://spaces.internet2.edu/s/f353d6b5ebe8383780318194e4762fea-CDN/en_GB/6212/d125ddfe4e16e78d1fea8ef42a18979f09319385.11/85294076ccf3a9d...
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/small-device.css
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/iphone.js
GET https://spaces.internet2.edu/s/en_GB/6212/d125ddfe4e16e78d1fea8ef42a18979f09319385.11/_/images/icons/profilepics/default.png
POST https://lastpass.com/error.php
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/iphone.js
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/small-device.css
http


SAML tracer
Clear
Autoscroll
Filter resources
Export
Import
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO;jsessionid=1jk2if7k2dwyz1c2legzneupce?execution=e1s1
POST https://lastpass.com/loglogin.php
POST https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
POST https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST
SAML
GET https://spaces.internet2.edu/dashboard.action
http
Parameters
SAML
GET https://idp.uwm.edu/idp/profile/SAML2/Redirect
/SSO?SAMLRequest=fZJfT4MwFMW%2FCun7KHR%2FZM0gwe3BJdORgT74YgpcpQm02FucfnsZTJ0ve2vSe86555e7QtHULY87W6kDvHeA1vls
aoV8%2BAhJZxTXAiVyJRpAbguexvc7zlyPt0ZbXeiaODEiGCu1WmuFXQMmBfMhC3g87EJSWdsipxRbUQC6U1kwCixzoexoWsk81zXYykXU9OT
NaLJPM%2BJs%2BmWkEifbPxNZtm53bAZt%2F6b9Dq%2ByhrPwAKU0UFiapnvibDcheZkW82WxmAs2Y8vAy0XAPK8sp345C3KWL0U%2FhtjBVq
EVyoaEef5i4gUTn2X%2BgrMbPp09Eyc5V72VqpTq7TqXfBxCfpdlyWQs8wQGhyL9AIlWJ7p8CDYXvK%2Fbih%2FIJLqKFH%2BRruhFzhja8of
eeLtJdC2LLyeua31cGxAWQuITGo2S%2FxcRfQM%3D&RelayState=cookie%3A1471019239_4dc2 HTTP/1.1
Host: idp.uwm.edu
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.11; rv:47.0) Gecko/20100101 Firefox/47.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://spaces.internet2.edu/shibboleth-ds/WAYF?entityID=https%3A%2F
%2Fspaces.internet2.edu%2Fshibboleth&returnX=https%3A%2F
%2Fspaces.internet2.edu%2FShibboleth.sso%2FLogin%3FSAMLDS%3D1%26os_destination
%3D%252F%26target%3Dcookie%253A1471019239_4dc2&returnIDParam=entityID&origin=unspec&action=search&
string=Milwaukee&cache=perm
HTTP/?.? 302 Found
Set-Cookie: JSESSIONID=1jk2if7k2dwyz1c2legzneupce;Path=/idp;Secure
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Cache-Control: no-store
Location: https://idp.uwm.edu/idp/profile/SAML2/Redirect
/SSO;jsessionid=1jk2if7k2dwyz1c2legzneupce?execution=e1s1
Content-Length: 0
Server: Jetty(9.2.5.v20141112)
113 requests received

SAML tracer

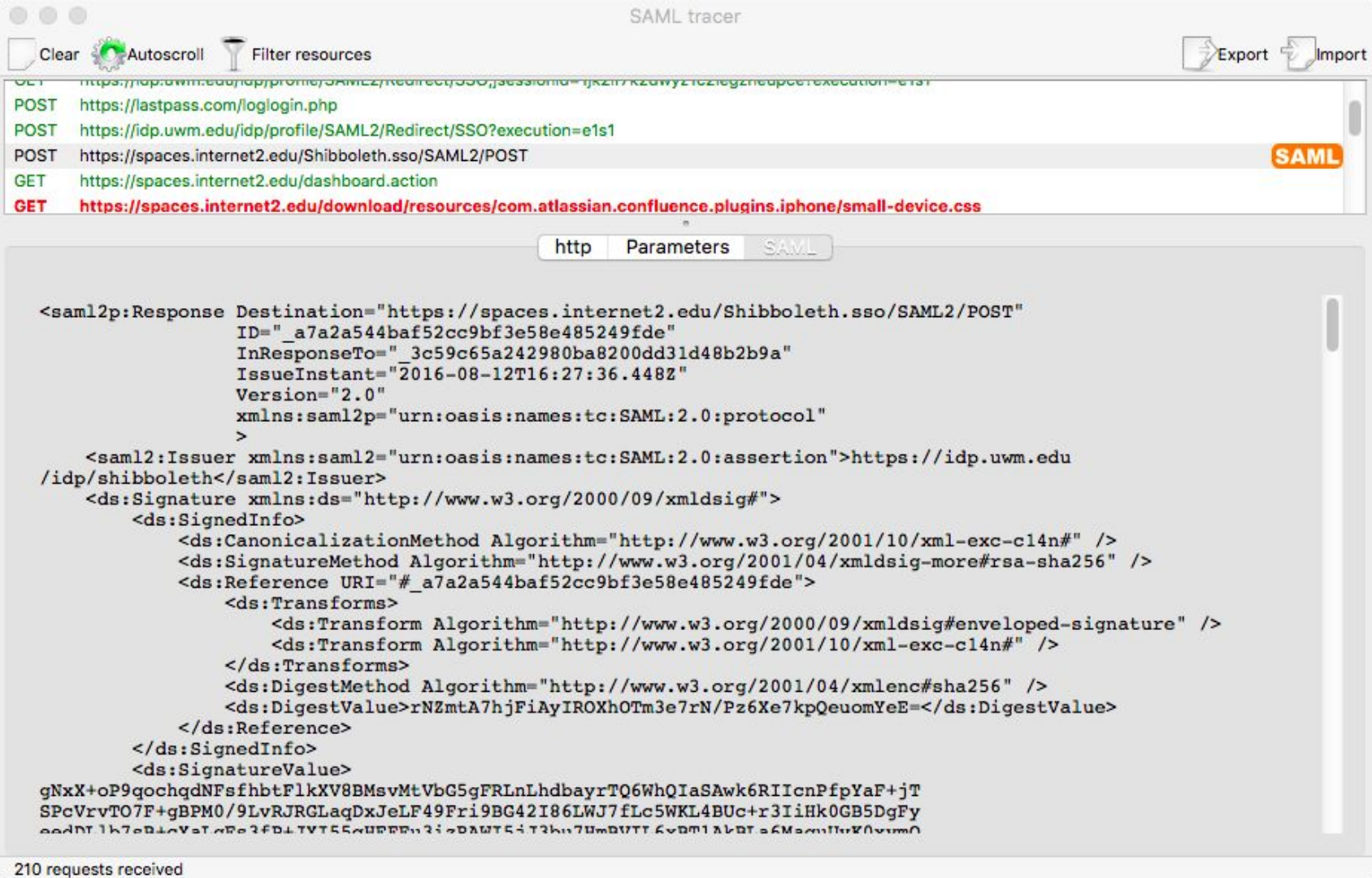
Clear Autoscroll Filter resources Export Import

GET https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO;jsessionid=1jk2if7k2dwyz1c2legzneupce?execution=e1s1
POST https://lastpass.com/loglogin.php
POST https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
POST https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST SAML
GET https://spaces.internet2.edu/dashboard.action
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/small-device.css

http Parameters SAML

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
                    AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
                    Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
                    ID="_3c59c65a242980ba8200dd31d48b2b9a"
                    IssueInstant="2016-08-12T16:27:34Z"
                    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                    Version="2.0"
                    >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">https://spaces.internet2.edu
/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

113 requests received


SAML tracer
Clear
Autoscroll
Filter resources
Export
Import
POST https://lastpass.com/loglogin.php
POST https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO?execution=e1s1
POST https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST
SAML
GET https://spaces.internet2.edu/dashboard.action
GET https://spaces.internet2.edu/download/resources/com.atlassian.confluence.plugins.iphone/small-device.css
http
Parameters
SAML
<saml2p:Response Destination="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
ID="_a7a2a544baf52cc9bf3e58e485249fde"
InResponseTo="_3c59c65a242980ba8200dd31d48b2b9a"
IssueInstant="2016-08-12T16:27:36.448Z"
Version="2.0"
xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
>
<saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://idp.uwm.edu
/idp/shibboleth</saml2:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
<ds:Reference URI="#_a7a2a544baf52cc9bf3e58e485249fde">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
</ds:Transforms>
<ds:DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
<ds:DigestValue>rNZmtA7hjFiAyIROXhOTm3e7rN/Pz6Xe7kpQeuomYeE=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
gNxX+oP9qochqdNFsfhbtFlkXV8BMsvMtVbG5gFRLnLhdbayrTQ6WhQIaSAwk6RIIcnPfpYaF+jT
SPcVrvTO7F+gBPM0/9LvRJRGLaqDxJeLF49Fri9BG42I86LWJ7fLc5WKL4BUc+r3IiHk0GB5DgFy
210 requests received

SAML Message Transport

Many ways to transport a SAML message (request or response)

The different ways are referred to as **protocol bindings**

- HTTP-Redirect: SAML message passed by redirecting web browser to perform a GET from a URL with the SAML message passed in the query string
- HTTP-POST: SAML message passed by delivering it to the web browser and instructing the web browser to push it using HTTP POST (like a web form)

SAML Message Transport

- HTTP-Redirect and HTTP-POST use web browser to pass SAML message
- Since web browser is the transport agent called "front channel" bindings
- "Back channel" bindings also exist
  - Direct communication between service provider (SP) and identity provider (IdP)
  - HTTP Artifact binding
  - Much less common in higher education and research

Focus today on front channel bindings

SAML SP-Initiated Web SSO Flow

- Most SAML SSO flows initiated at SP
- SP uses the **HTTP-Redirect Binding** to redirect browser to the IdP
- Browser does a GET to the IdP HTTP-Redirect URL endpoint
- Authentication request included as query string
    - Base64 and URL encoded

Redirect Binding SAMLRequest

```
GET https://login.sphericalcowgroup.com/idp/profile/SAML2/Redirect/SSO?
SAMLRequest=jZLLbsIwEEV%2FJfKeOAmmAosgpbAoEi2IpF10UznOQCw5dupx%2Bvj7hkdbukFd%2B%2Fqcm
WtPUTS65Vnna7OF1w7QBx%2BNNsiPBynpnOFWoEJuRAPIveR5dr%2FiSRjx1llvpdUkyBDBeWXN3BrsGnA5uD
cl4XG7SkntfYucUmkbYcQeQmxrcEoKLbXtqtCAp3mtytJq8HWIaOlBkdDNOi9IsOhnUkYc6L8sbffKXIDs%2B
97Zrg17B1VVS%2FvRdkrDGbSFSjmQvSZfk2C5SMlLHLMymkgZ3UzGiZSwG7JdBYyxUTyMJyzuY4gdLA16YXxK
kigeDyI2iEZFzPiI8YQ9k2BzbuBWmUqZ%2FfW6ylMI%2BV1RbAan5Z7A4XGxPkBm00Pp%2FCh2F89wHSu%2Bu
yez%2FzSNP01P6YXu5G75Q89fLjZWK%2FkZZFrb97kD4SElMaGz05W%2F%2F2X2BQ%3D%3D
&RelayState=ss%3Amem%3A53831b946af03f4a61a8729ecc370aa8a5e12fa9899a518371ac68f9882d9f
HTTP/1.1
```

SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
  Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
  ID="_3c59c65a242980ba8200dd31d48b2b9a"
  IssueInstant="2016-08-12T16:27:34Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
  >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- SP Issuer SAML entityID
- Every SP and IdP has unique entityID
- Best practice is URL syntax
- Older practice is URN

SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
  Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
  ID="_3c59c65a242980ba8200dd31d48b2b9a"
  IssueInstant="2016-08-12T16:27:34Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
  >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- Timestamp
- Prevent replay attacks
- Most systems tolerate some clock skew

SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
  Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
  ID="_3c59c65a242980ba8200dd31d48b2b9a"
  IssueInstant="2016-08-12T16:27:34Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
  >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- URL at the IdP that is meant to consume the request

SAML SP Authentication Request

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
  AssertionConsumerServiceURL="https://spaces.internet2.edu/Shibboleth.sso/SAML2/POST"
  Destination="https://idp.uwm.edu/idp/profile/SAML2/Redirect/SSO"
  ID="_3c59c65a242980ba8200dd31d48b2b9a"
  IssueInstant="2016-08-12T16:27:34Z"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
  Version="2.0"
  >
    <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
     https://spaces.internet2.edu/shibboleth</saml:Issuer>
    <samlp:NameIDPolicy AllowCreate="1" />
</samlp:AuthnRequest>
```

- SP URL where it expects to consume the response

SAML IdP Response

- IdP uses HTTP-POST binding to send response to SP
  - Base64 encoded XML payload returned to browser
  - **Browser does the POST**
- Most IdPs include Javascript to automate the POST
  - Turn off Javascript and you will see a button to click to force the POST

SAML IdP Response

- Response is usually digitally signed (XML digital signature)
  - SP can verify and trust the response
  - Prevent tampering
  - Response payload may also be encrypted (XML encryption)
  - Encrypted using the SPs SAML key
  - Hides details from user from snooping browsers
  - TLS transport not usually required but usually used
- Includes an assertion about the authentication event
  - Assertion may be encrypted if Response is not

```
<saml2p:Response Destination="https://comanage.sphericalcloud.net/Shibboleth.sso/SAML2/POST" ID="_0e81776e9959f4478402cae0fcdb8b2e"
InResponseTo="_114b09cc06982ccef34fde4445131941" IssueInstant="2018-04-05T14:54:29.730Z"
Version="2.0"xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol">
    <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">https://login.sphericalcowgroup.com/idp/shibboleth</saml2:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">SNIP</ds:Signature>
    <saml2p:Status>
        <saml2p:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </saml2p:Status>
    <saml2:Assertion ID="_94989a68c1ffd4e373bddfd93b8328f0" IssueInstant="2018-04-05T14:54:29.730Z" Version="2.0"
                    xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
        <saml2:Issuer>https://login.sphericalcowgroup.com/idp/shibboleth</saml2:Issuer>
        <saml2:Subject>SNIP</saml2:Subject>
        <saml2:Conditions NotBefore="2018-04-05T14:54:29.730Z" NotOnOrAfter="2018-04-05T14:59:29.730Z" >
            <saml2:AudienceRestriction>
                <saml2:Audience>https://comanage.sphericalcloud.net/shibboleth</saml2:Audience>
            </saml2:AudienceRestriction>
        </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2018-04-05T14:54:29.663Z" SessionIndex="_7dbbb6e0545f5c0283aff9242a95a034">
            <saml2:SubjectLocality Address="136.167.36.227" />
            <saml2:AuthnContext>
                <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml2:AuthnContextClassRef>
            </saml2:AuthnContext>
        </saml2:AuthnStatement>
        <saml2:AttributeStatement>SNIP</saml2:AttributeStatement>
    </saml2:Assertion>
</saml2p:Response>
```

AttributeStatement

```
<saml2:AttributeStatement>
  <saml2:Attribute FriendlyName="sn" Name="urn:oid:2.5.4.4" NameFormat=SNIP>
    <saml2:AttributeValue>Koranda</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="displayName" Name="urn:oid:2.16.840.1.113730.3.1.241" NameFormat=SNIP>
    <saml2:AttributeValue>Scott Koranda</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="givenName" Name="urn:oid:2.5.4.42" NameFormat=SNIP>
    <saml2:AttributeValue>Scott</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="eduPersonPrincipalName" Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat=SNIP>
    <saml2:AttributeValue>scott.koranda@ligo.org</saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute FriendlyName="mail" Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat=SNIP>
    <saml2:AttributeValue>scott.koranda@ligo.org</saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Attribute

```
<saml2:Attribute
  FriendlyName="sn"
  Name="urn:oid:2.5.4.4"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue>Koranda</saml2:AttributeValue>
</saml2:Attribute>
```

Attribute

```
<saml:Attribute
  Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml:AttributeValue xsi:type="xs:string">
  skoranda@sphericalcowgroup.com
  </saml:AttributeValue>
  <saml:AttributeValue  xsi:type="xs:string">
  scott@renu.ac.ug
</saml:AttributeValue>
</saml:Attribute>
```

SAML2 Attributes

- Higher ed and research leverage well defined standards
  - eduPerson schema managed by MACE-DIR
  - Standard LDAP schema like sn, givenName, mail
    - Borrow OIDs rather than reinvent new
- More later on attributes in higher ed and research federations like RENU