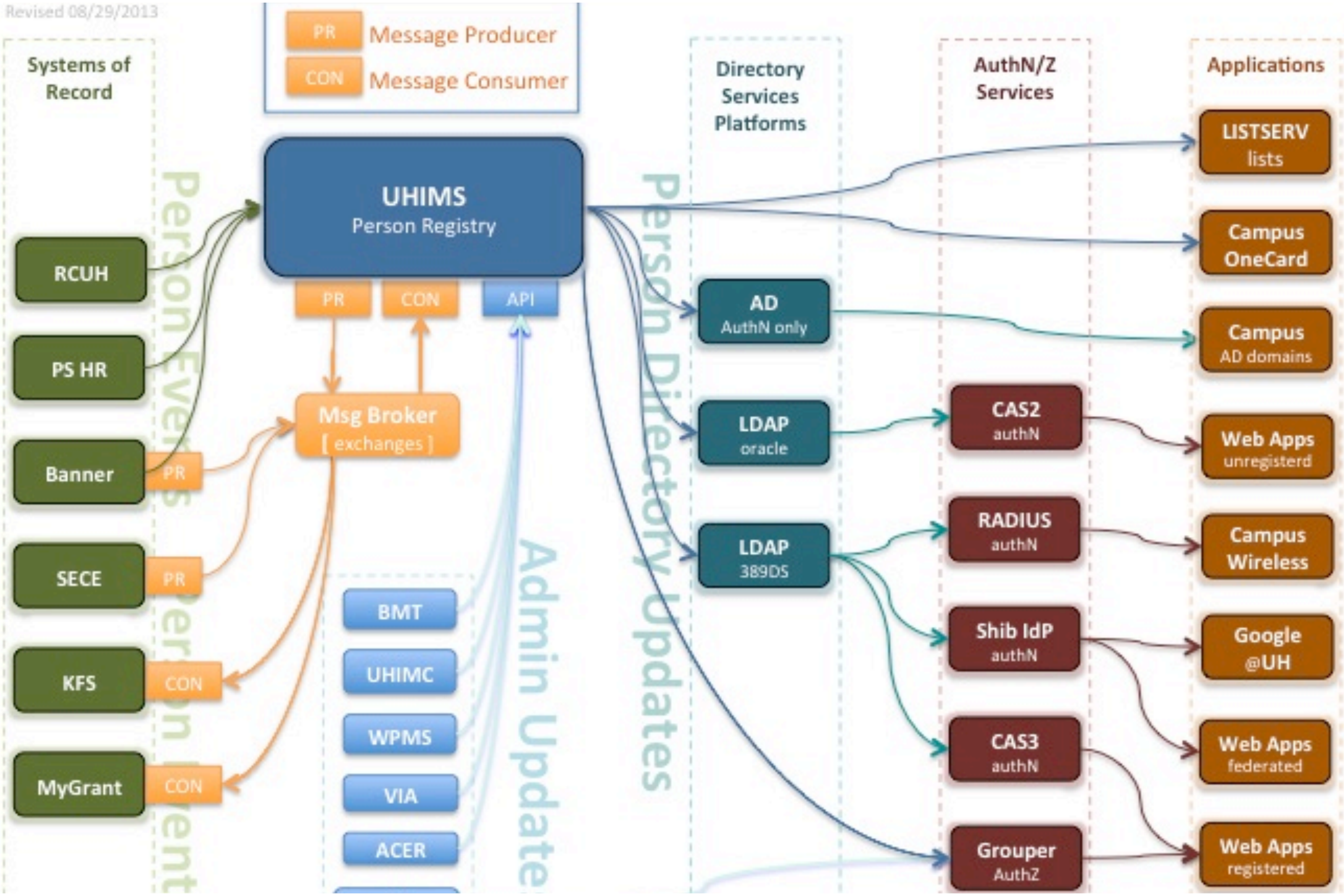
CAS

A quick introduction

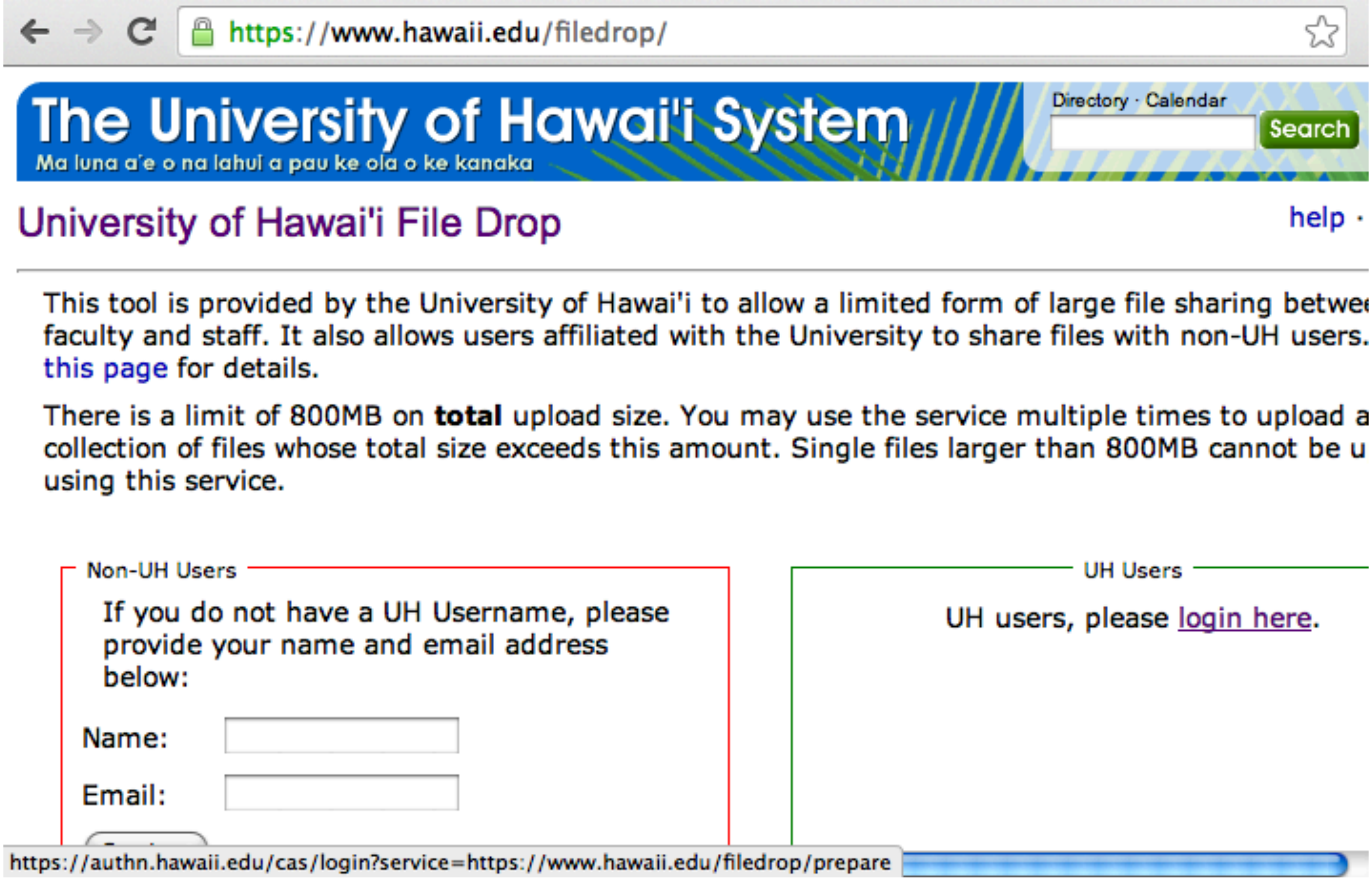
Julio Polo
University of Hawaiʻi
Information Technology Services
julio@hawaii.edu

About us:

www.hawaii.edu/bwiki/display/UHIAM/



CAS in action



https://www.hawaii.edu/filedrop/

The University of Hawai'i System
Ma luna a'e o na lahui a pau ke ola o ke kanaka
Directory · Calendar
Search

University of Hawai'i File Drop

This tool is provided by the University of Hawai'i to allow a limited form of large file sharing betwe faculty and staff. It also allows users affiliated with the University to share files with non-UH users. this page for details.

There is a limit of 800MB on **total** upload size. You may use the service multiple times to upload a collection of files whose total size exceeds this amount. Single files larger than 800MB cannot be u using this service.

Non-UH Users

If you do not have a UH Username, please provide your name and email address below:

Name:

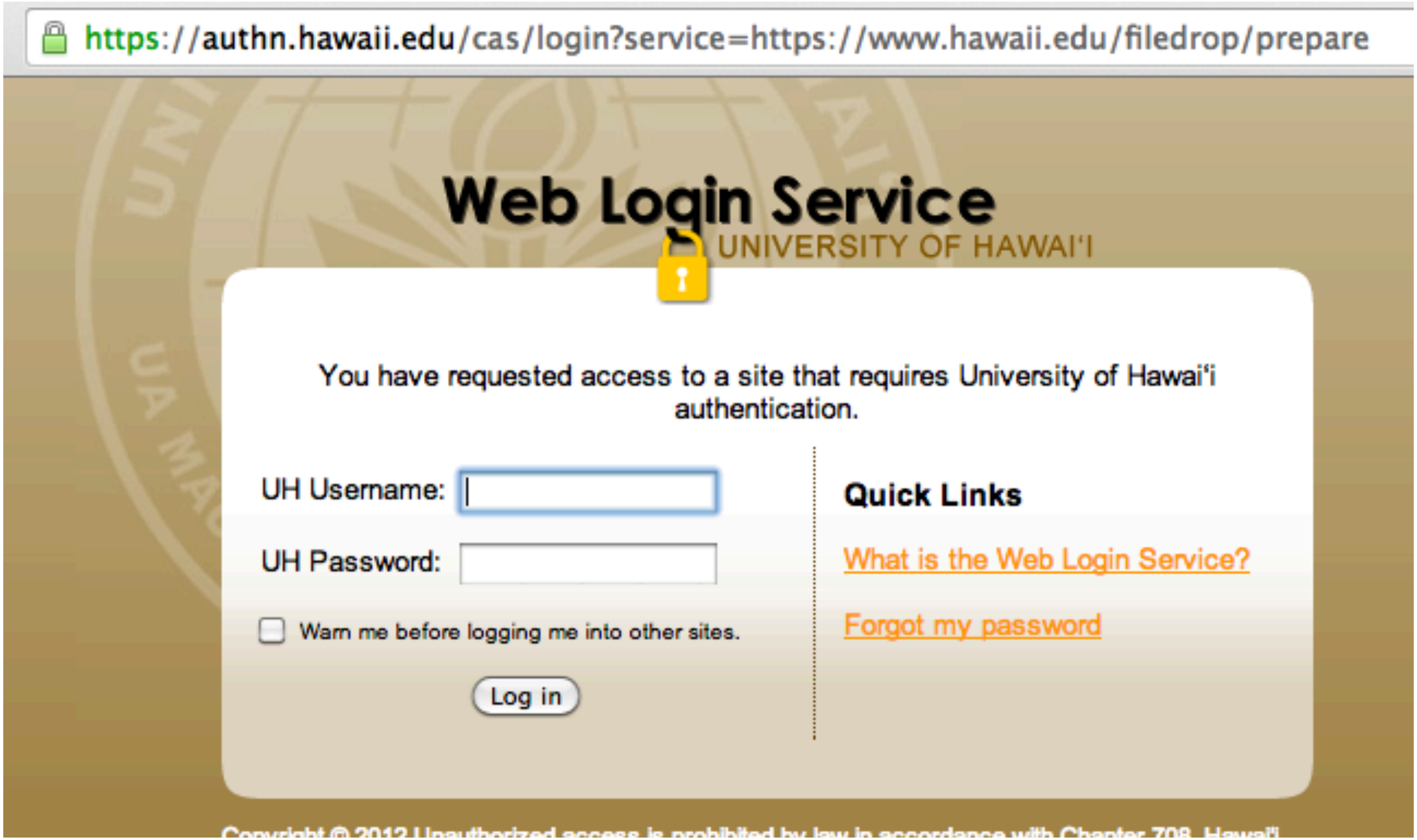
Email:

UH Users

UH users, please login here.

https://authn.hawaii.edu/cas/login?service=https://www.hawaii.edu/filedrop/prepare

CAS in action



https://authn.hawaii.edu/cas/login?service=https://www.hawaii.edu/filedrop/prepare

Web Login Service

UNIVERSITY OF HAWAI'I

You have requested access to a site that requires University of Hawai'i authentication.

UH Username:

UH Password:

□ Warn me before logging me into other sites.

Log in

Quick Links

What is the Web Login Service?

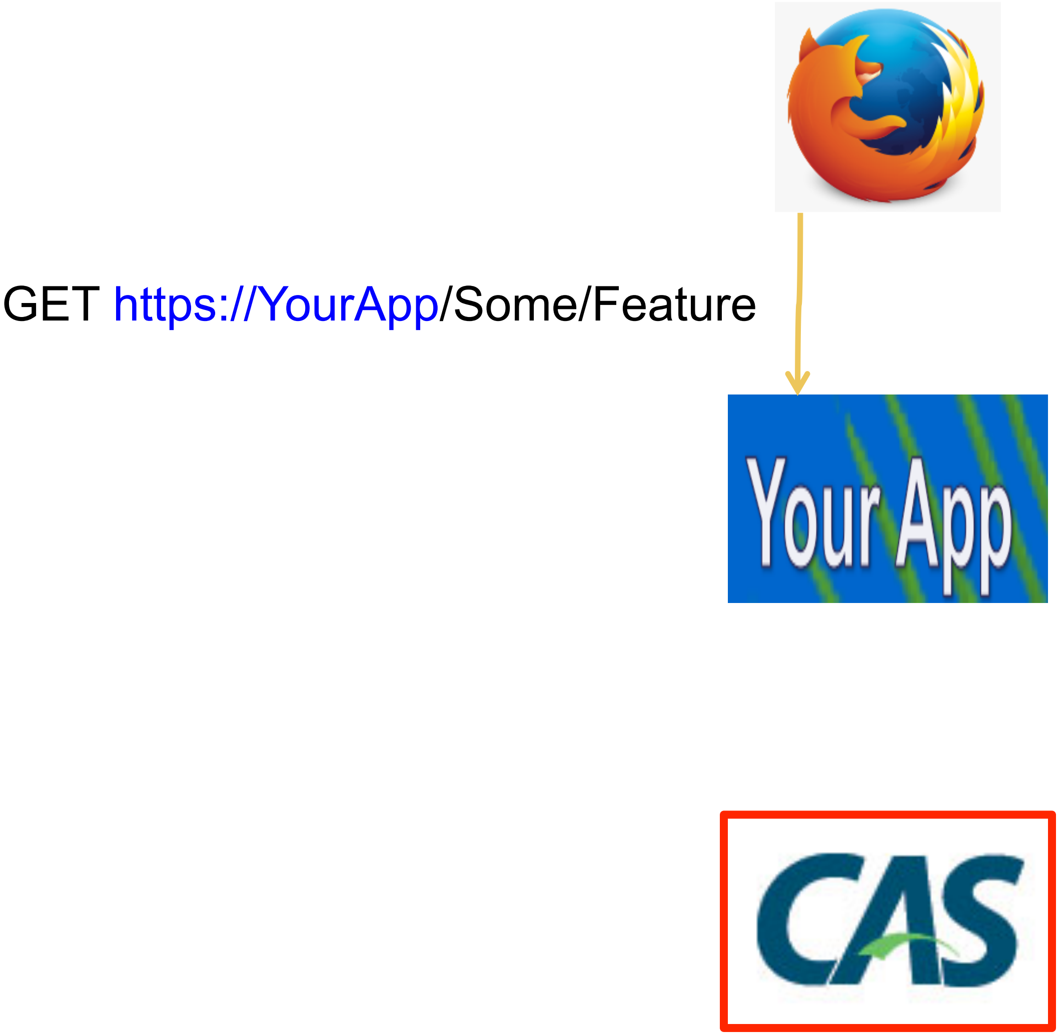
Forgot my password

Copyright © 2012 Unauthorized access is prohibited by law in accordance with Chapter 708, Hawai'i

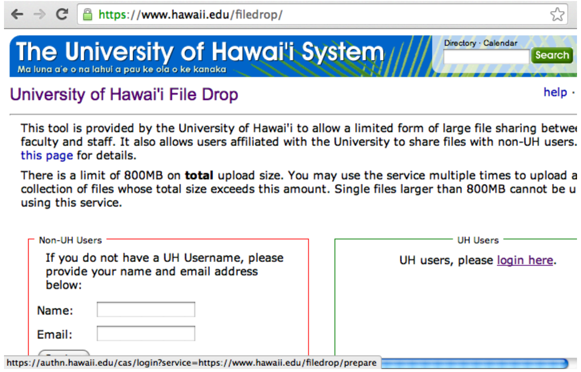
Why use CAS?

- Don't have to roll your own
  - Labor
  - Resources (account database)
  - Security, maintenance
  - Yet another password
- Security:
  - Password not revealed to app
- Convenience:
  - No login for subsequent apps (if SSO allowed)
- Consistency:
  - One official login page for all of UH

How does CAS work?


GET https://YourApp/Some/Feature

How does CAS work?



https://www.hawaii.edu/filedrop/
The University of Hawai'i System
Ma luna a'e o na lahui a pau ke ola o ke kanaka
Directory · Calendar
Search
help ·

University of Hawai'i File Drop

This tool is provided by the University of Hawai'i to allow a limited form of large file sharing betwe
faculty and staff. It also allows users affiliated with the University to share files with non-UH users.
this page for details.

There is a limit of 800MB on **total** upload size. You may use the service multiple times to upload a
collection of files whose total size exceeds this amount. Single files larger than 800MB cannot be u
using this service.

Non-UH Users

If you do not have a UH Username, please provide your name and email address below:

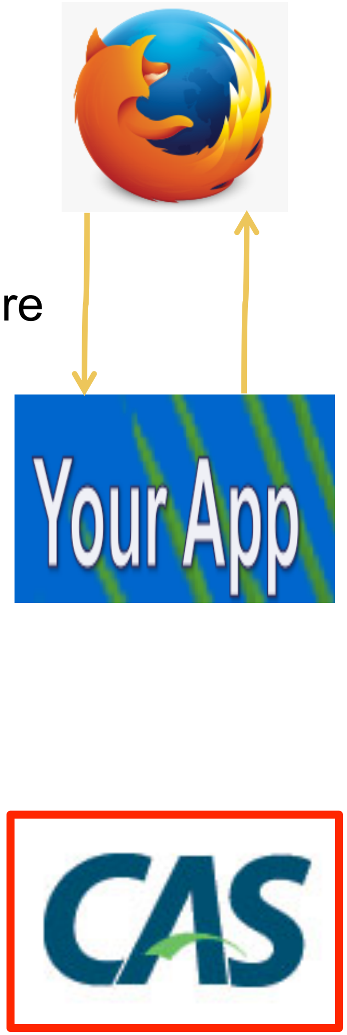
Name:

Email:

UH Users

UH users, please login here.

https://authn.hawaii.edu/cas/login?service=https://www.hawaii.edu/filedrop/prepare

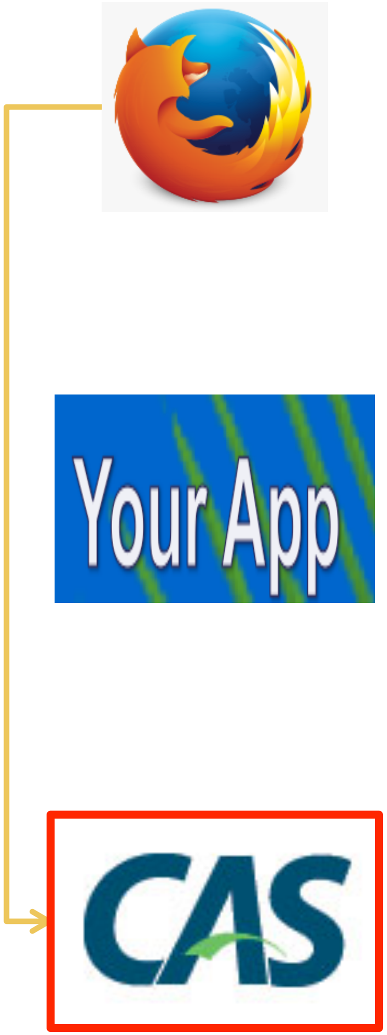


GET https://YourApp/Some/Feature

Provide link or redirect to your app's CAS login page:

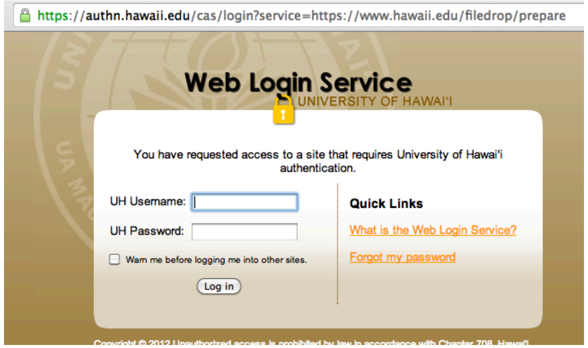
https://CAS/login?
service=https://YourApp/casfoo

How does CAS work?



GET https://CAS/login?
service=https://YourApp/casfoo

How does CAS work?



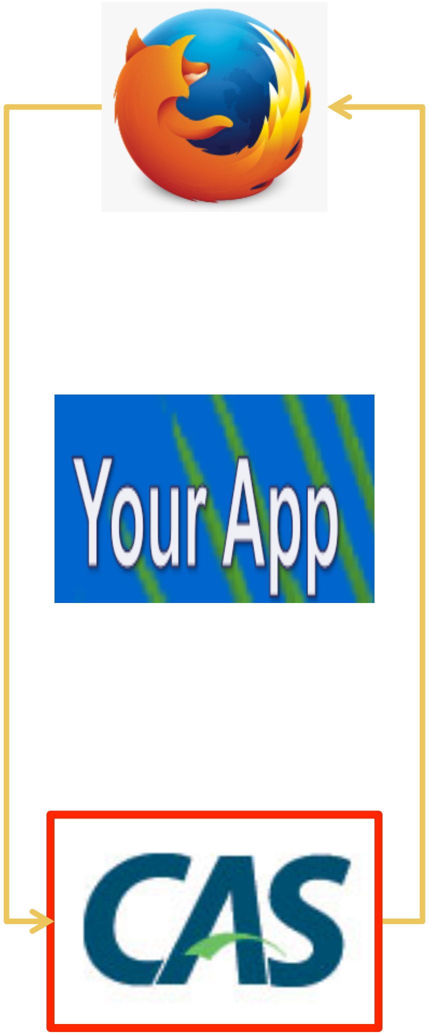
https://authn.hawaii.edu/cas/login?service=https://www.hawaii.edu/filedrop/prepare

You have requested access to a site that requires University of Hawai'i authentication.

UH Username:

UH Password:

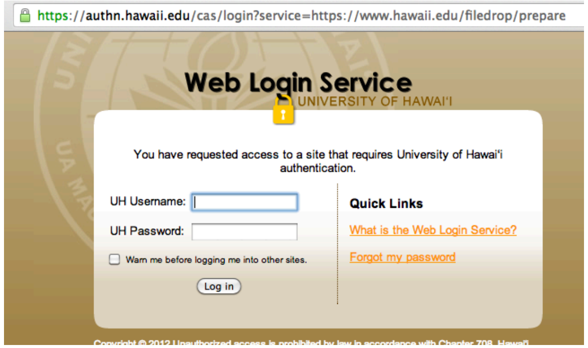
□ Warn me before logging me into other sites.



GET https://CAS/login?
service=https://YourApp/casfoo

Display CAS login page
(for your app)

How does CAS work?



https://authn.hawaii.edu/cas/login?service=https://www.hawaii.edu/filedrop/prepare

Web Login Service

UNIVERSITY OF HAWAI'I

You have requested access to a site that requires University of Hawai'i authentication.

UH Username:

UH Password:

□ Warn me before logging me into other sites.

Log in

Quick Links

What is the Web Login Service?

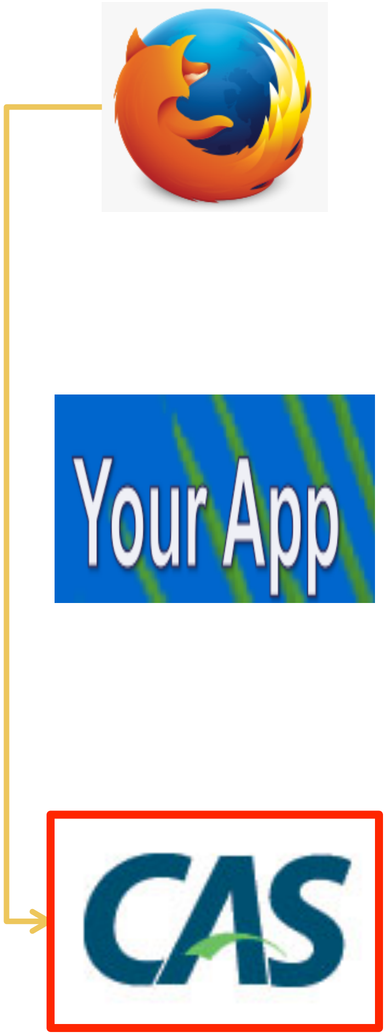
Forgot my password

Copyright © 2012 Unauthorized access is prohibited by law in accordance with Chapter 708, Hawai'i

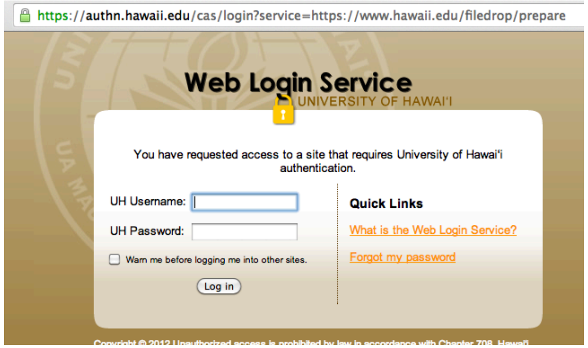
User enters username and password:

POST https://CAS/login?service=https://YourApp/casfoo

username=johndoe&pass...



How does CAS work?



https://authn.hawaii.edu/cas/login?service=https://www.hawaii.edu/filedrop/prepare

Web Login Service

UNIVERSITY OF HAWAI'I

You have requested access to a site that requires University of Hawai'i authentication.

UH Username:

UH Password:

□ Warn me before logging me into other sites.

Log in

Quick Links

What is the Web Login Service?

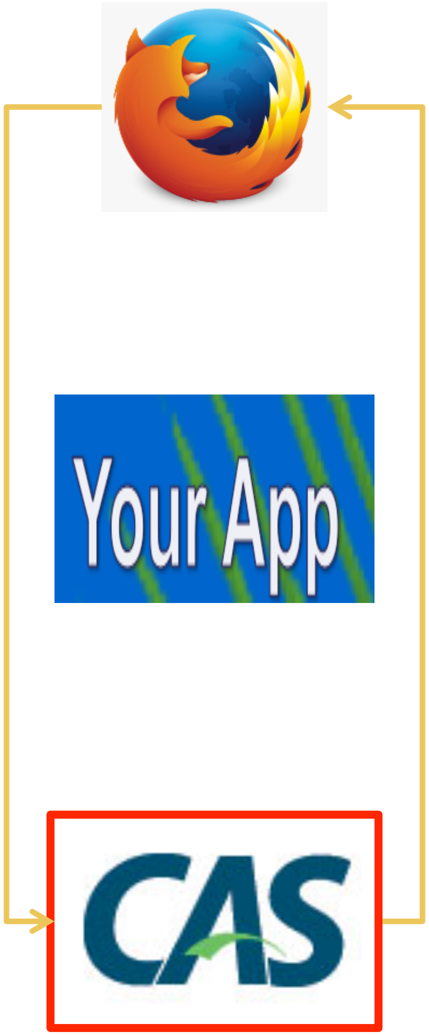
Forgot my password

Copyright © 2012 Unauthorized access is prohibited by law in accordance with Chapter 708, Hawai'i

User enters username and password:

POST https://CAS/login?service=https://YourApp/casfoo

username=johndoe&pass...

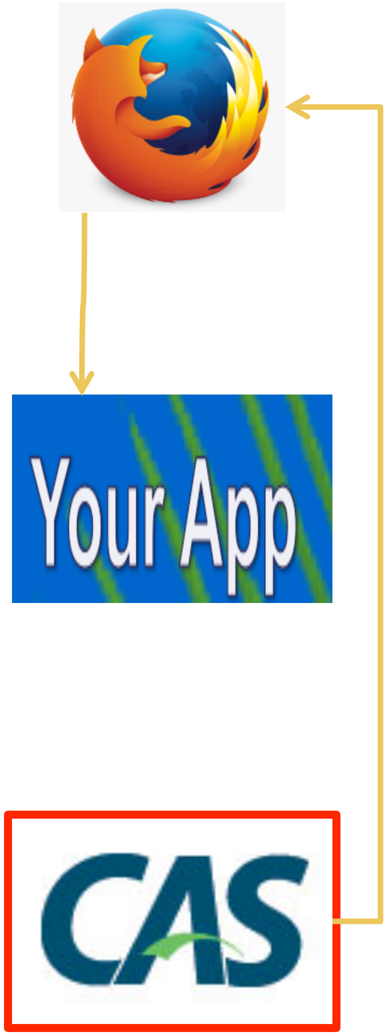


Redirect to app with this CAS ticket:

https://YourApp/HandleLogin?ticket=100

copyright © 2014 University of Hawai'i

How does CAS work?

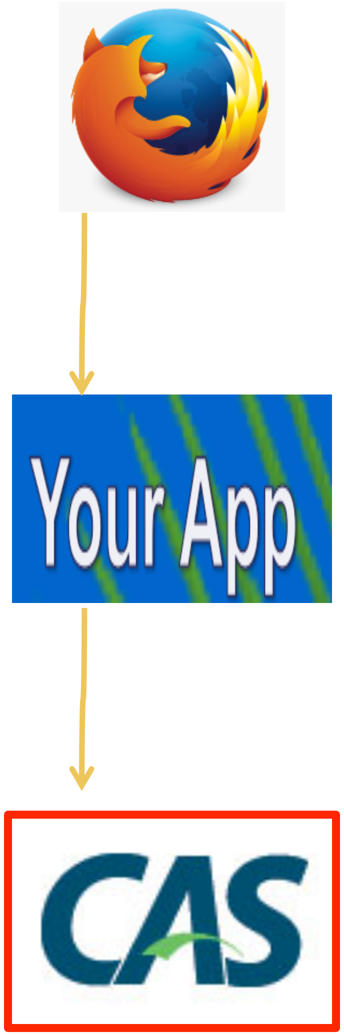


https://YourApp/HandleLogin?
ticket=100

Redirect to app
with this CAS ticket:

https://YourApp/HandleLogin?
ticket=100

How does CAS work?



https://YourApp/HandleLogin?ticket=100

Ask CAS to validate ticket:

POST https://CAS/samlValidate?TARGET=https://YourApp/HandleLogin

(SAML with ticket 100 here)

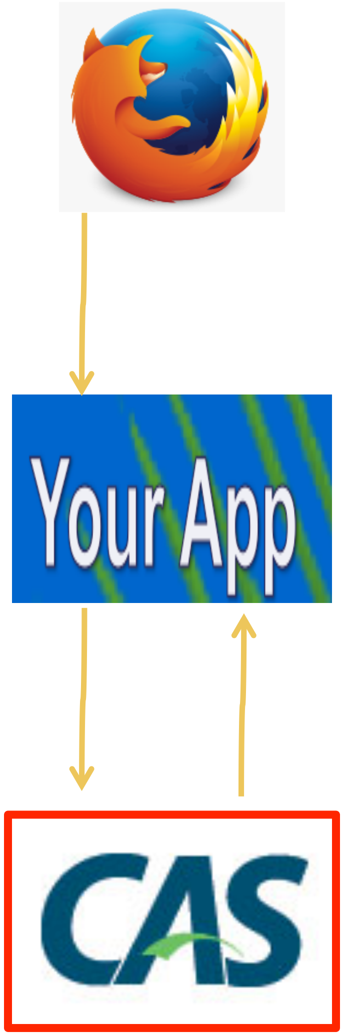
How does CAS work?

https://YourApp/HandleLogin?ticket=100

Ask CAS to validate ticket:

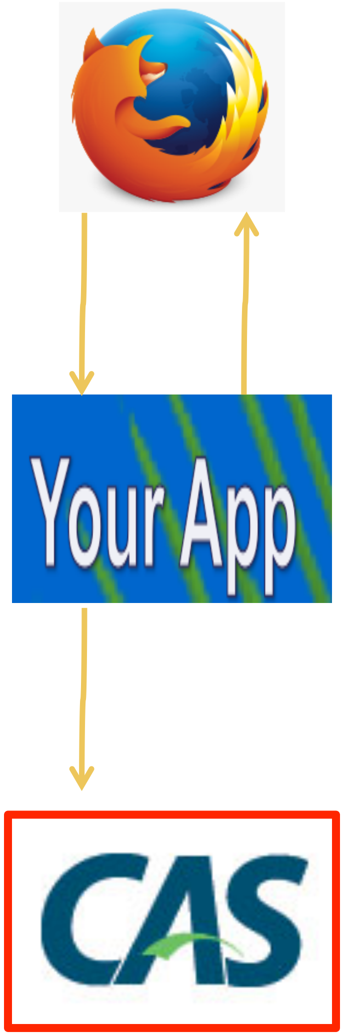
POST https://CAS/samlValidate?TARGET=https://YourApp/HandleLogin

(SAML with ticket 100 here)



CAS validation returns:
Valid?
If so, user attributes are:
uhUuid: (UH Number)
uid: (UH username)
cn, givenName, sn: (names)
uhOrgAffiliation: (e.g. eduPersonOrgDN=uhm, eduPersonAffiliation=student)

How does CAS work?



https://YourApp/HandleLogin?
ticket=100

Ask CAS to validate ticket:

POST https://CAS/
samlValidate?TARGET=https://
YourApp/HandleLogin

(SAML with ticket 100 here)

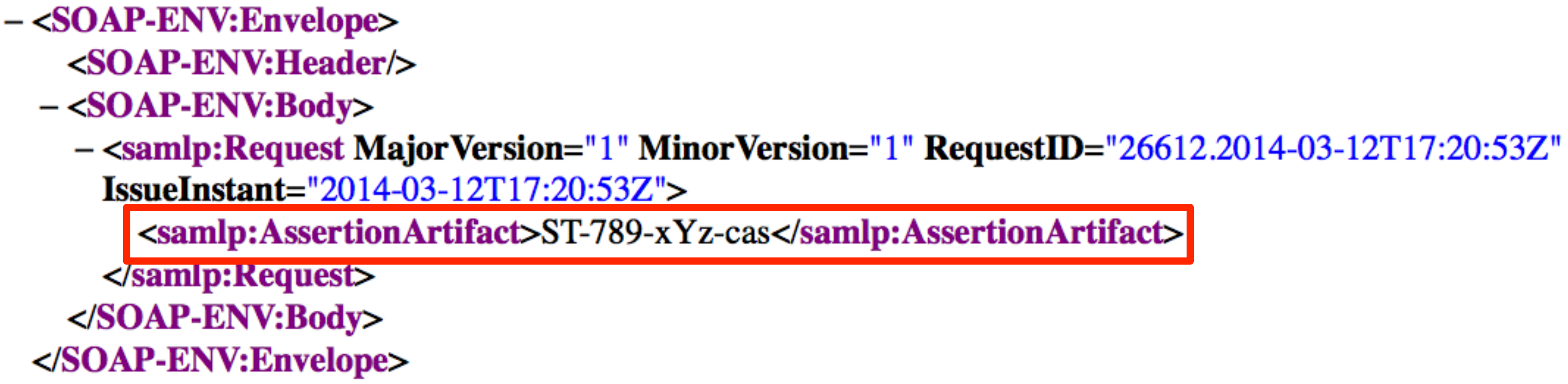
Display page for
https://YourApp/Some/Feature

or error page if validation failed

or error if authenticated user does not meet your app's criteria (e.g. not a student)

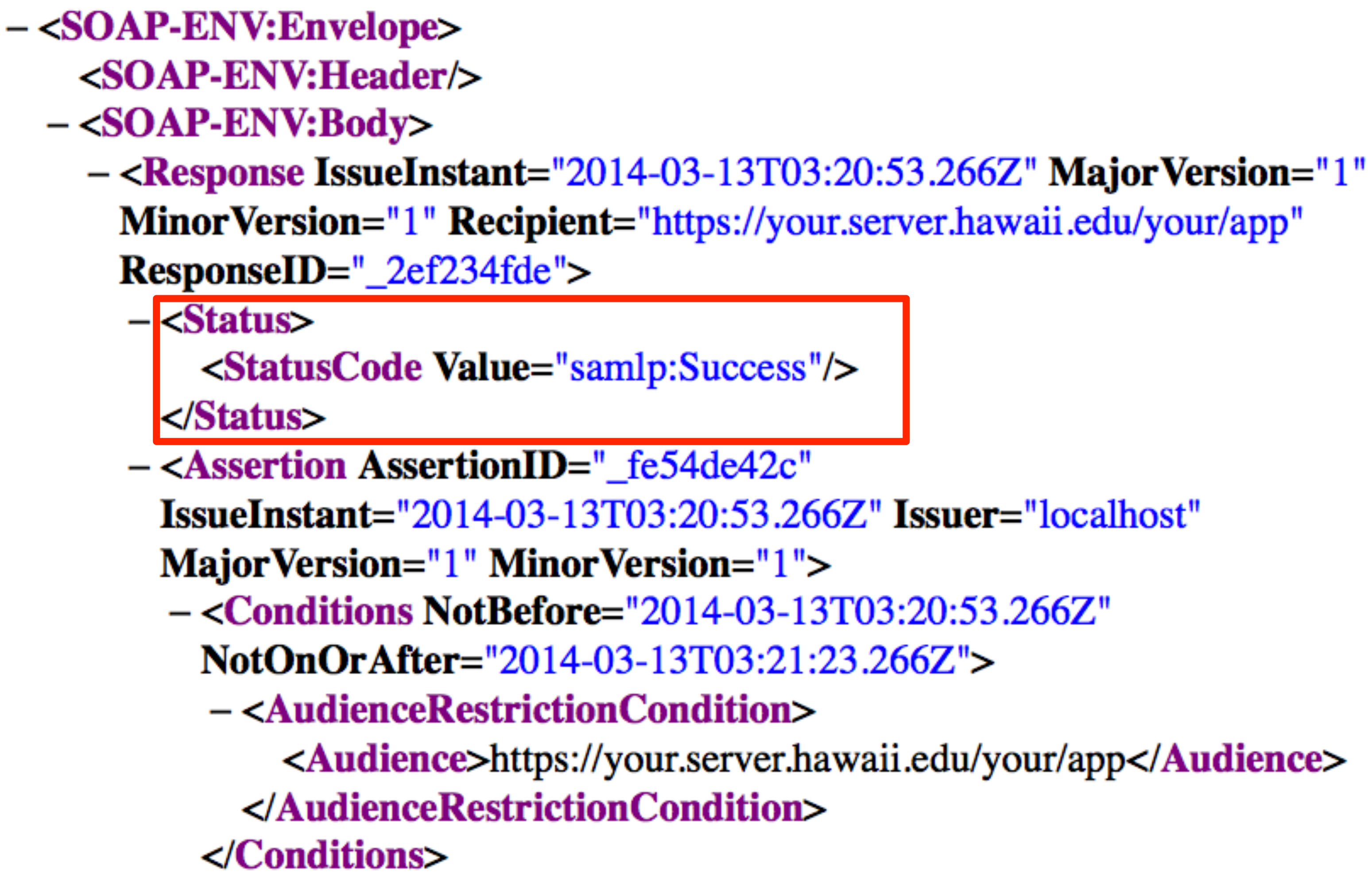
CAS validation returns:
Valid?
If so, user attributes are:
uhUuid: (UH Number)
uid: (UH username)
cn, givenName, sn: (names)
uhOrgAffiliation: (e.g.
eduPersonOrgDN=uhm,
eduPersonAffiliation=student)

SAML in



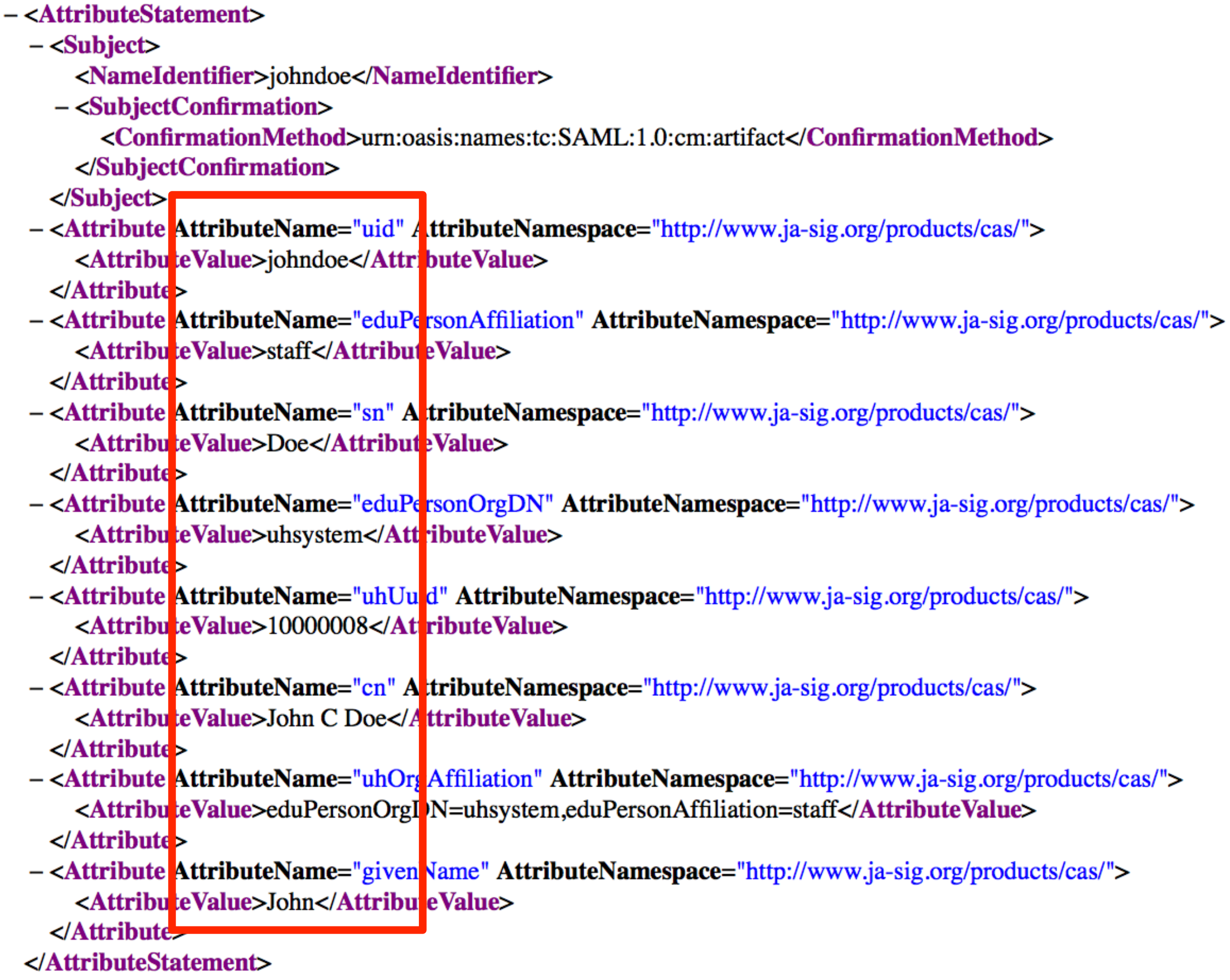
```
– <SOAP-ENV:Envelope>
    <SOAP-ENV:Header/>
  – <SOAP-ENV:Body>
    – <samlp:Request MajorVersion="1" MinorVersion="1" RequestID="26612.2014-03-12T17:20:53Z"
      IssueInstant="2014-03-12T17:20:53Z">
        <samlp:AssertionArtifact>ST-789-xYz-cas</samlp:AssertionArtifact>
      </samlp:Request>
    </SOAP-ENV:Body>
  </SOAP-ENV:Envelope>
```

SAML out



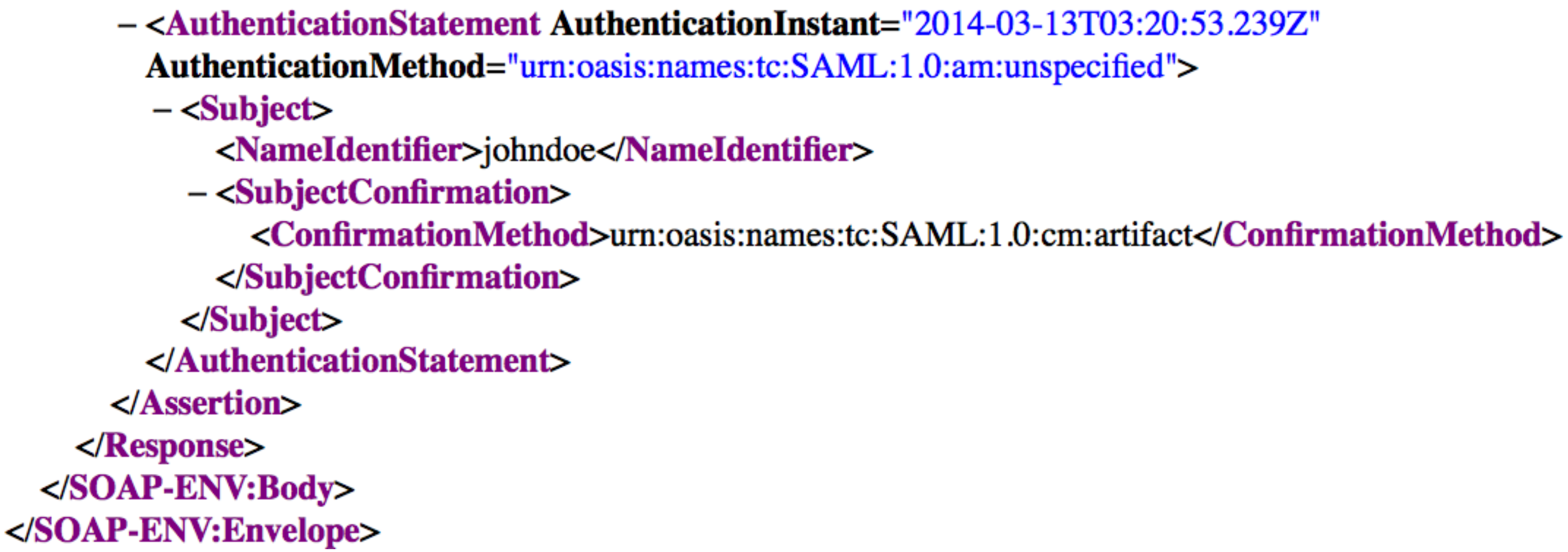
```
– <SOAP-ENV:Envelope>
    <SOAP-ENV:Header/>
  – <SOAP-ENV:Body>
    – <Response IssueInstant="2014-03-13T03:20:53.266Z" MajorVersion="1"
      MinorVersion="1" Recipient="https://your.server.hawaii.edu/your/app"
      ResponseID="_2ef234fde">
      – <Status>
          <StatusCode Value="samlp:Success"/>
        </Status>
      – <Assertion AssertionID="_fe54de42c"
        IssueInstant="2014-03-13T03:20:53.266Z" Issuer="localhost"
        MajorVersion="1" MinorVersion="1">
        – <Conditions NotBefore="2014-03-13T03:20:53.266Z"
          NotOnOrAfter="2014-03-13T03:21:23.266Z">
          – <AudienceRestrictionCondition>
              <Audience>https://your.server.hawaii.edu/your/app</Audience>
            </AudienceRestrictionCondition>
          </Conditions>
```

SAML out



```
– <AttributeStatement>
  – <Subject>
      <NameIdentifier>johndoe</NameIdentifier>
    – <SubjectConfirmation>
        <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:artifact</ConfirmationMethod>
      </SubjectConfirmation>
    </Subject>
  – <Attribute AttributeName="uid" AttributeNamespace="http://www.ja-sig.org/products/cas/">
      <AttributeValue>johndoe</AttributeValue>
    </Attribute>
  – <Attribute AttributeName="eduPersonAffiliation" AttributeNamespace="http://www.ja-sig.org/products/cas/">
      <AttributeValue>staff</AttributeValue>
    </Attribute>
  – <Attribute AttributeName="sn" AttributeNamespace="http://www.ja-sig.org/products/cas/">
      <AttributeValue>Doe</AttributeValue>
    </Attribute>
  – <Attribute AttributeName="eduPersonOrgDN" AttributeNamespace="http://www.ja-sig.org/products/cas/">
      <AttributeValue>uhsystem</AttributeValue>
    </Attribute>
  – <Attribute AttributeName="uhUuid" AttributeNamespace="http://www.ja-sig.org/products/cas/">
      <AttributeValue>10000008</AttributeValue>
    </Attribute>
  – <Attribute AttributeName="cn" AttributeNamespace="http://www.ja-sig.org/products/cas/">
      <AttributeValue>John C Doe</AttributeValue>
    </Attribute>
  – <Attribute AttributeName="uhOrgAffiliation" AttributeNamespace="http://www.ja-sig.org/products/cas/">
      <AttributeValue>eduPersonOrgDN=uhsystem,eduPersonAffiliation=staff</AttributeValue>
    </Attribute>
  – <Attribute AttributeName="givenName" AttributeNamespace="http://www.ja-sig.org/products/cas/">
      <AttributeValue>John</AttributeValue>
    </Attribute>
  </AttributeStatement>
```

SAML out



```
– <AuthenticationStatement AuthenticationInstant="2014-03-13T03:20:53.239Z"
   AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:unspecified">
  – <Subject>
      <NameIdentifier>johndoe</NameIdentifier>
    – <SubjectConfirmation>
        <ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:artifact</ConfirmationMethod>
      </SubjectConfirmation>
    </Subject>
  </AuthenticationStatement>
</Assertion>
</Response>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Logout

- https://CAS/logout
  - Terminates SSO, user must login again to CAS
  - Displays generic CAS logout page.

- https://CAS/logout?service=https://YourApp/logout
  - Terminates SSO, user must login again to CAS
  - Redirects to https://YourApp/logout
  - Your app should then invalidate the session for the user

Start using CAS

- Register your app URL
  - https://www.hawaii.edu/bwiki/display/UHIAM/Web+App+Registration+Form
- Use a CAS client
  - https://www.hawaii.edu/bwiki/display/UHIAM/CAS3+Developer+Documentation#CAS3DeveloperDocumentation-clients
- Our CAS page
  - https://www.hawaii.edu/bwiki/display/UHIAM/UH+Web+Login+Service+-+CAS+v3

Confused about CAS versions?

- UH CAS v3
  - aka CAS3
  - = CAS software version 3.x
    = implements CAS protocol 2

- Deprecated:
  - UH CAS v2
    - aka CAS2
      = CAS software version 2.x
      = implements CAS protocol 1
      + UH customizations