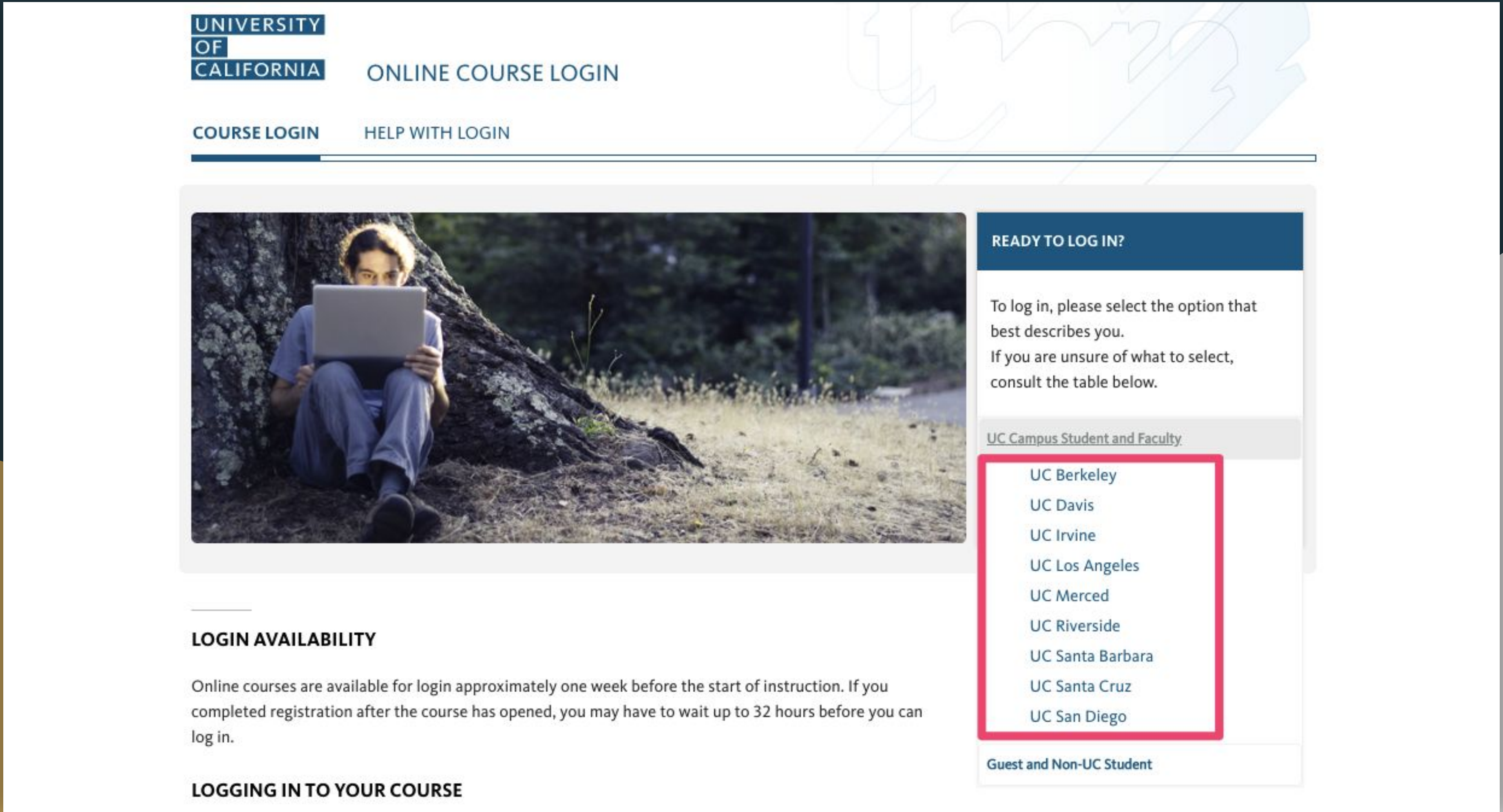
Identity & Authentication

Scott Kirkland
UC DAVIS



UNIVERSITY OF CALIFORNIA

ONLINE COURSE LOGIN

READY TO LOG IN?

To log in, please select the option that best describes you.
If you are unsure of what to select, consult the table below.

UC Campus Student and Faculty

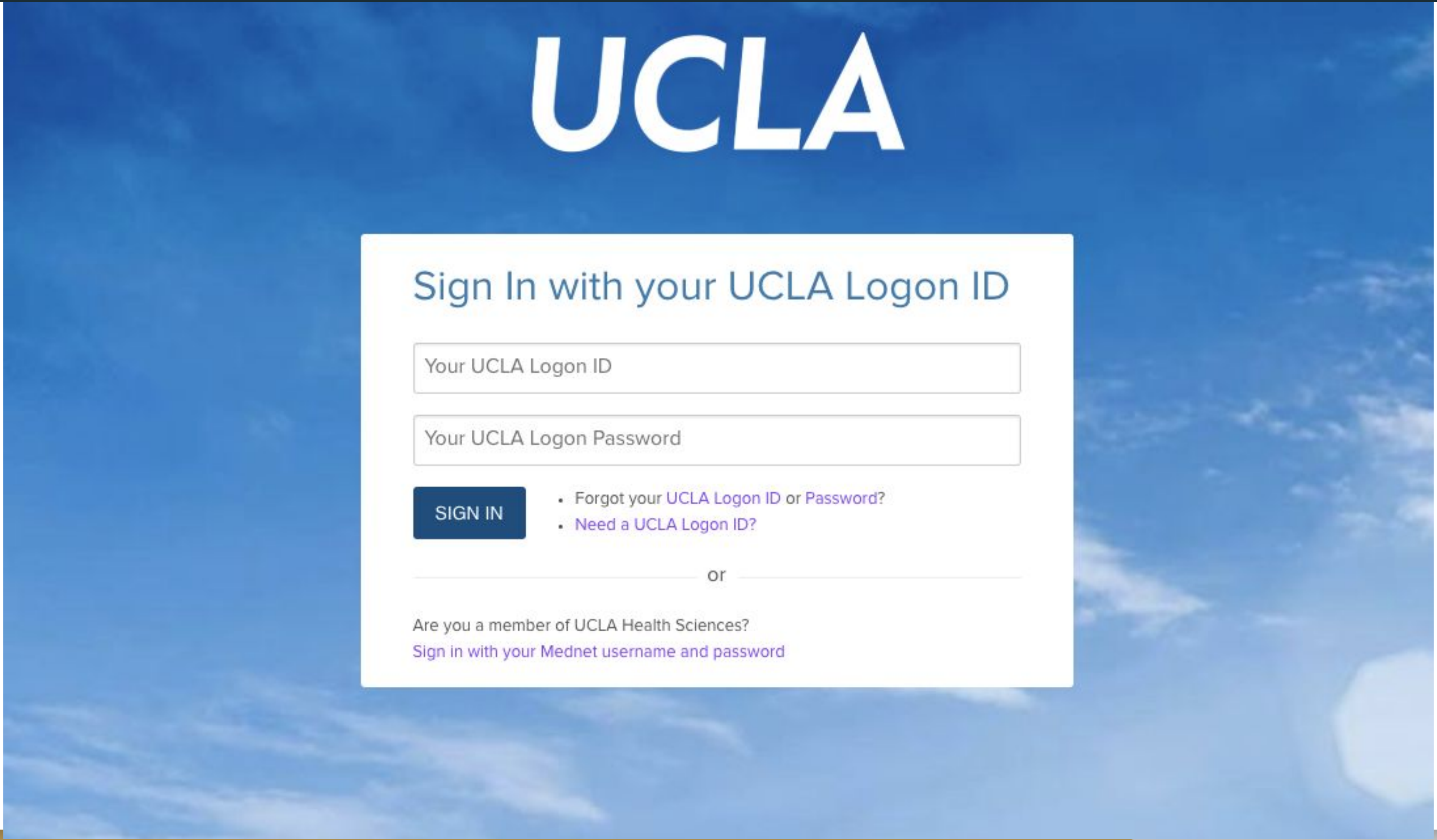
- UC Berkeley
- UC Davis
- UC Irvine
- UC Los Angeles
- UC Merced
- UC Riverside
- UC Santa Barbara
- UC Santa Cruz
- UC San Diego

Guest and Non-UC Student

LOGIN AVAILABILITY

Online courses are available for login approximately one week before the start of instruction. If you completed registration after the course has opened, you may have to wait up to 32 hours before you can log in.

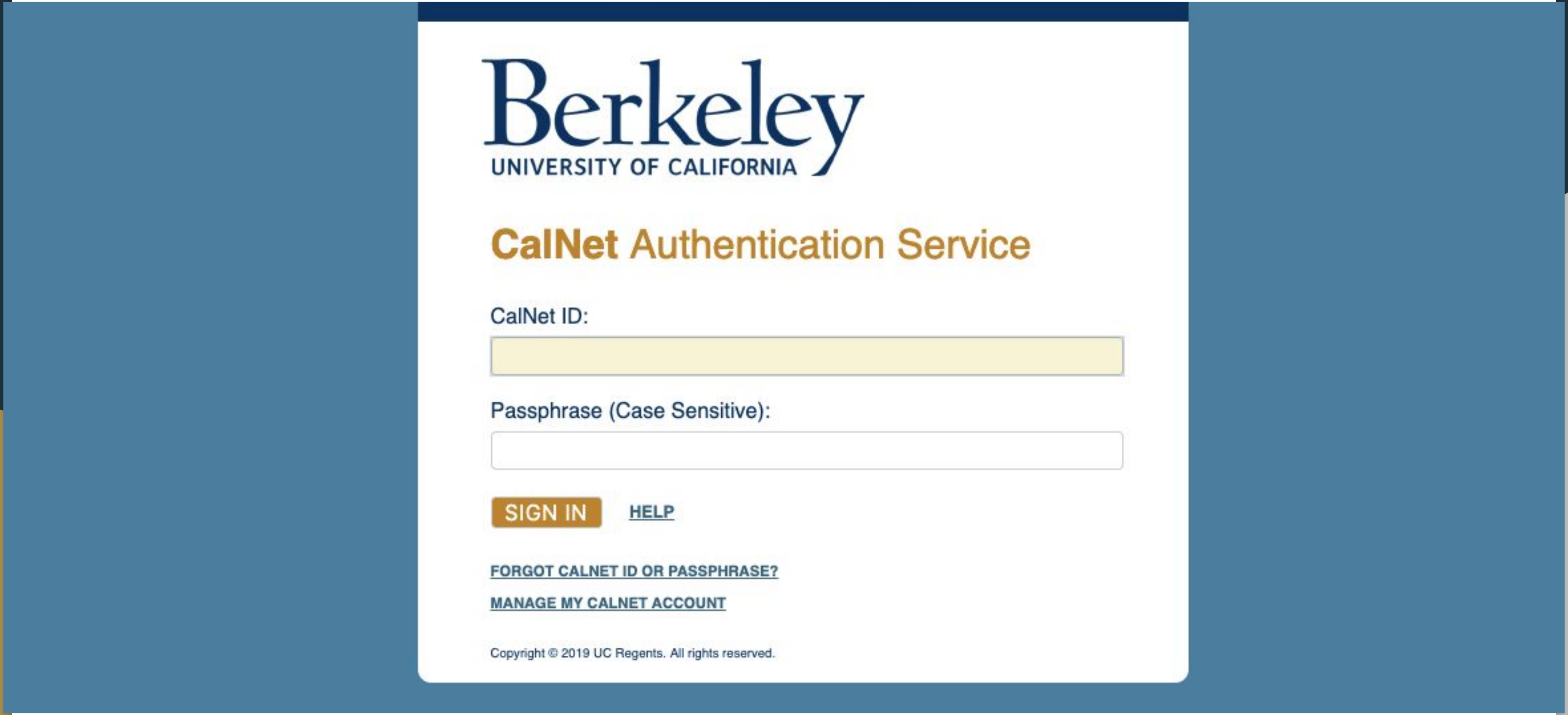
LOGGING IN TO YOUR COURSE



Sign In with your UCLA Logon ID

- Forgot your UCLA Logon ID or Password?
- Need a UCLA Logon ID?

Are you a member of UCLA Health Sciences?
Sign in with your Mednet username and password



Berkeley
UNIVERSITY OF CALIFORNIA

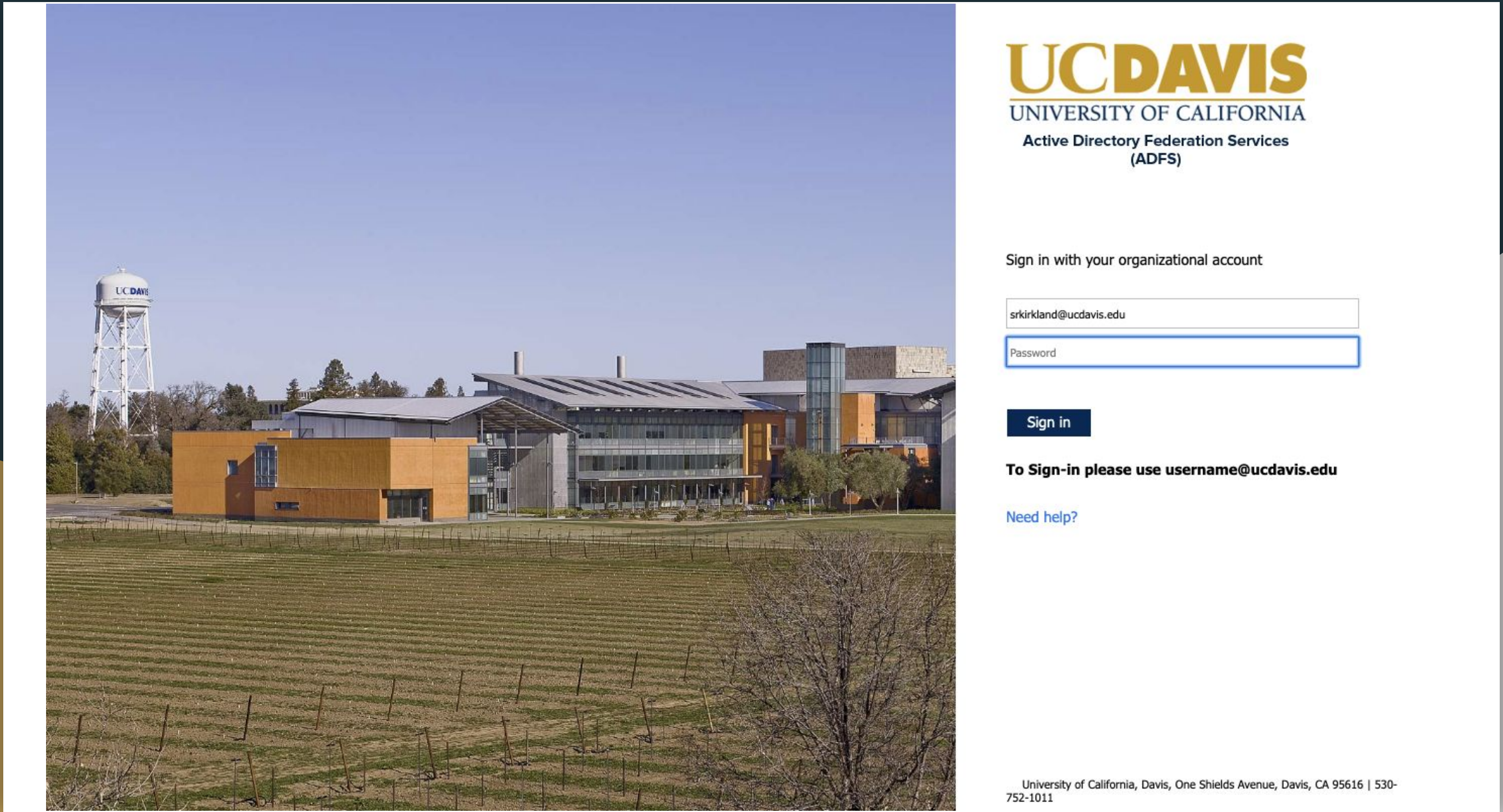
CalNet Authentication Service

CalNet ID:

Passphrase (Case Sensitive):

FORGOT CALNET ID OR PASSPHRASE?

MANAGE MY CALNET ACCOUNT



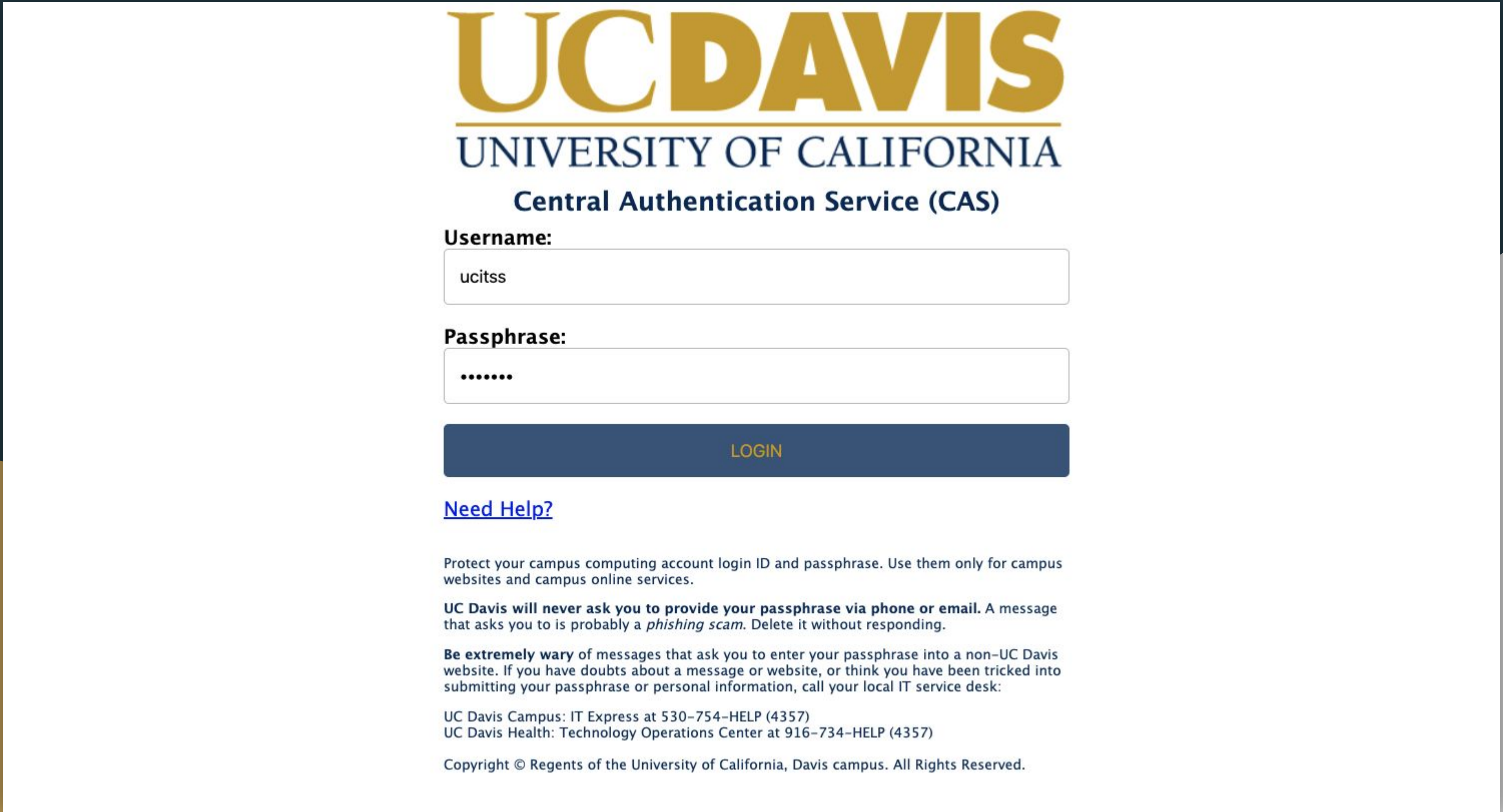
Active Directory Federation Services (ADFS)

Sign in with your organizational account

srkirkland@ucdavis.edu

To Sign-in please use username@ucdavis.edu

University of California, Davis, One Shields Avenue, Davis, CA 95616 | 530-752-1011



UCDAVIS
UNIVERSITY OF CALIFORNIA

Central Authentication Service (CAS)

Username: ucitss

Passphrase: •••••••

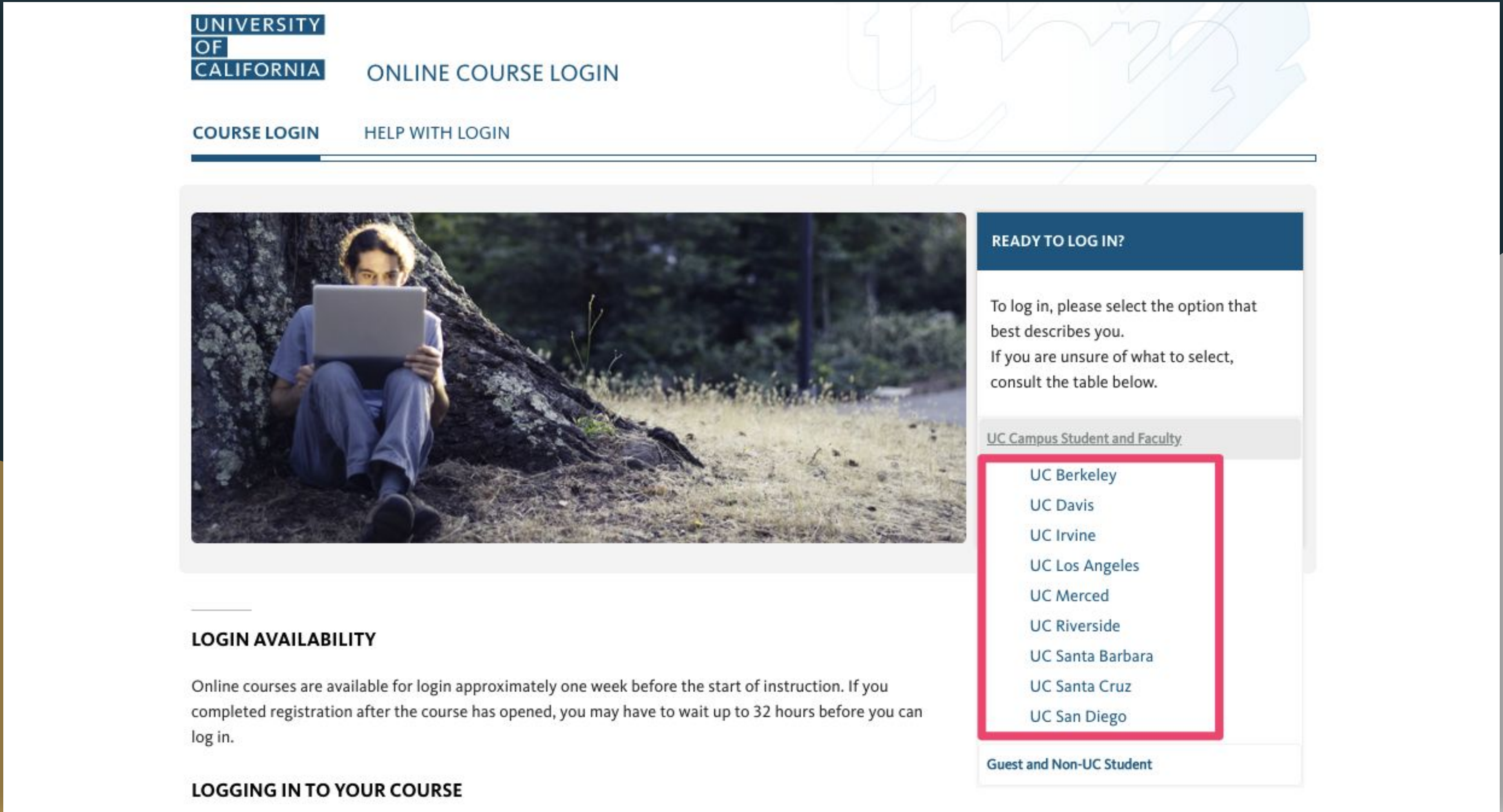
Protect your campus computing account login ID and passphrase. Use them only for campus websites and campus online services.

UC Davis will never ask you to provide your passphrase via phone or email. A message that asks you to is probably a *phishing scam*. Delete it without responding.

Be extremely wary of messages that ask you to enter your passphrase into a non-UC Davis website. If you have doubts about a message or website, or think you have been tricked into submitting your passphrase or personal information, call your local IT service desk:

UC Davis Campus: IT Express at 530-754-HELP (4357)
UC Davis Health: Technology Operations Center at 916-734-HELP (4357)

Copyright © Regents of the University of California, Davis campus. All Rights Reserved.



ONLINE COURSE LOGIN

READY TO LOG IN?

To log in, please select the option that best describes you.
If you are unsure of what to select, consult the table below.

UC Campus Student and Faculty

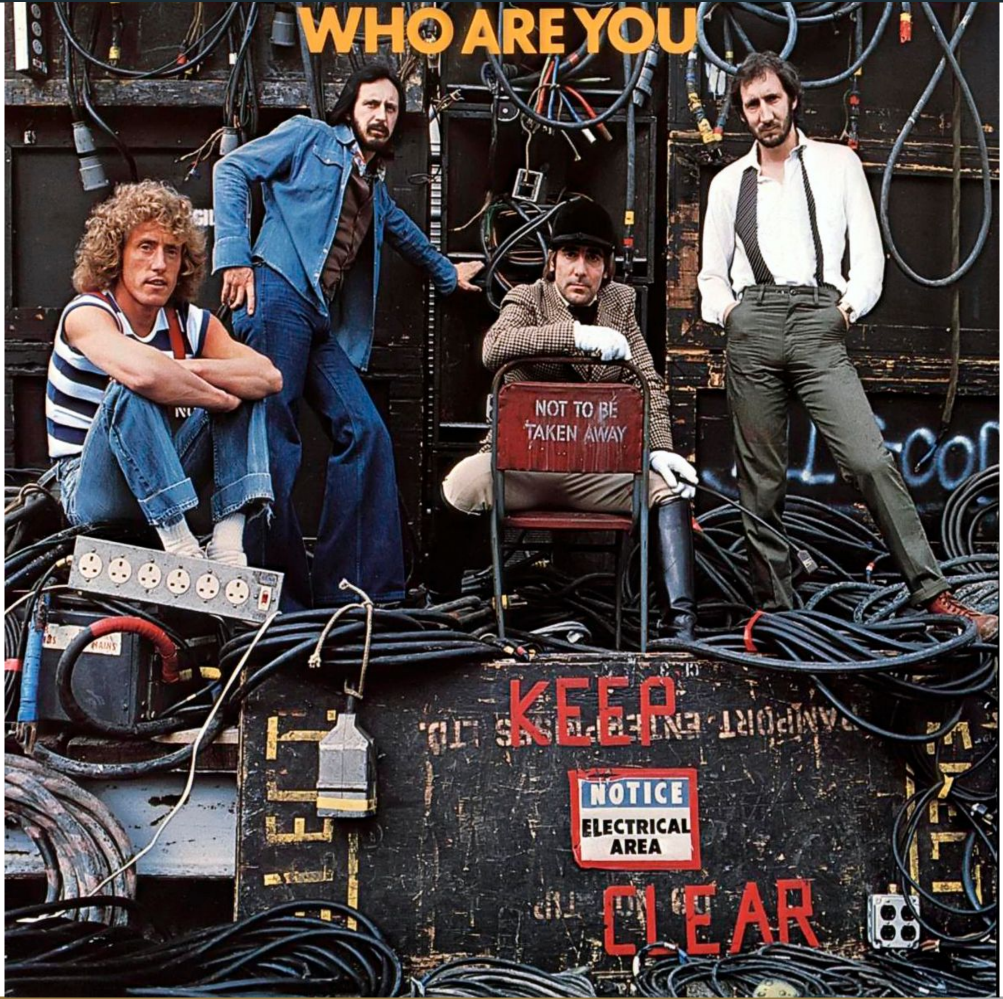
- UC Berkeley
- UC Davis
- UC Irvine
- UC Los Angeles
- UC Merced
- UC Riverside
- UC Santa Barbara
- UC Santa Cruz
- UC San Diego

Guest and Non-UC Student

LOGIN AVAILABILITY

Online courses are available for login approximately one week before the start of instruction. If you completed registration after the course has opened, you may have to wait up to 32 hours before you can log in.

LOGGING IN TO YOUR COURSE


WHO ARE YOU
NOT TO BE
TAKEN AWAY
KEEP
NOTICE
ELECTRICAL
AREA
CLEAR

Authentication @ the UCs

- CAS
- Shibboleth
- OAuth
- OpenID Connect
- SAML
- Federation
- JWTs
- Claims

Authentication @ the UCs

- CAS
- Shibboleth
- OAuth / OpenID Connect

Central Authentication Service

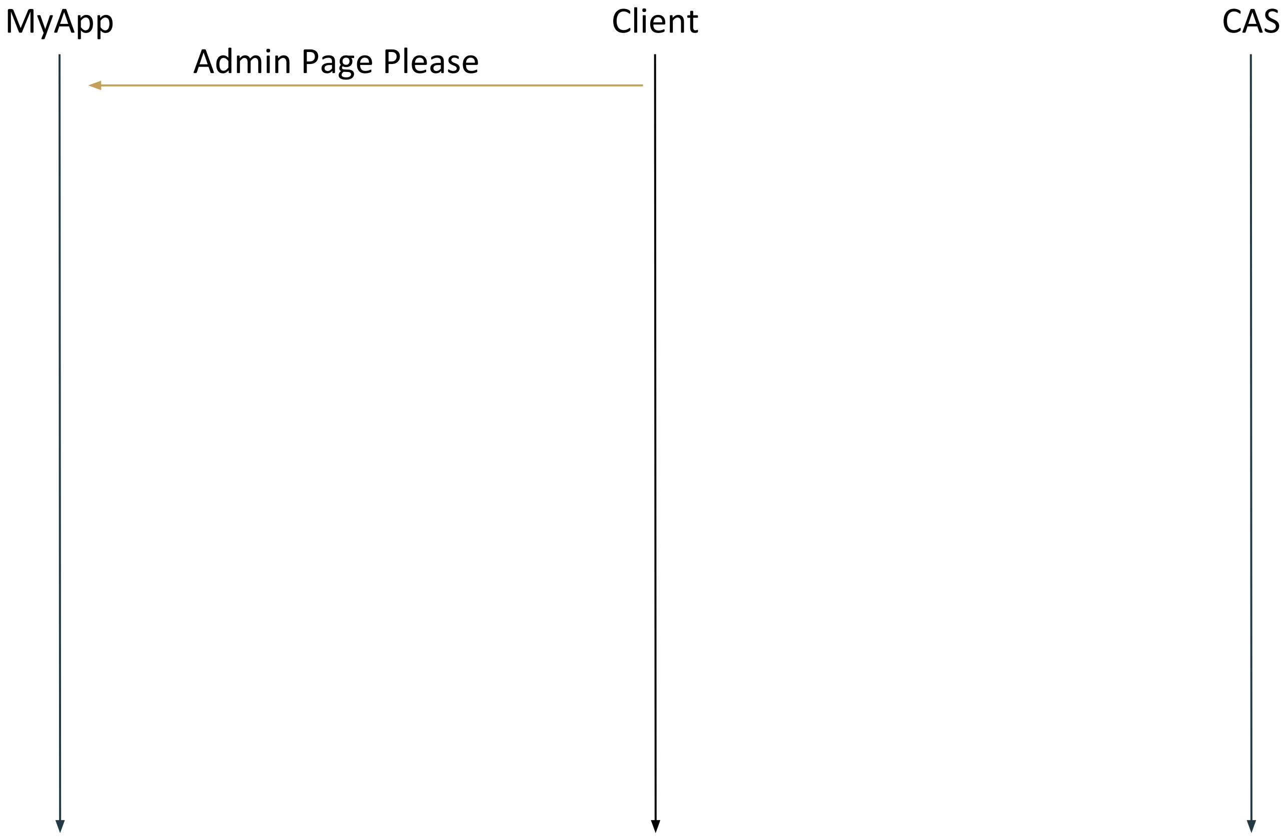
CAS

- Developed at Yale
- Now supported by Apero Foundation
- Used at many UC Campuses

Let’s talk CAS Protocol

- Fairly simple™ so we’ll start here
- Web-based login flow
- Includes backchannel validation

Client: https://myapp.ucdavis.edu/admin



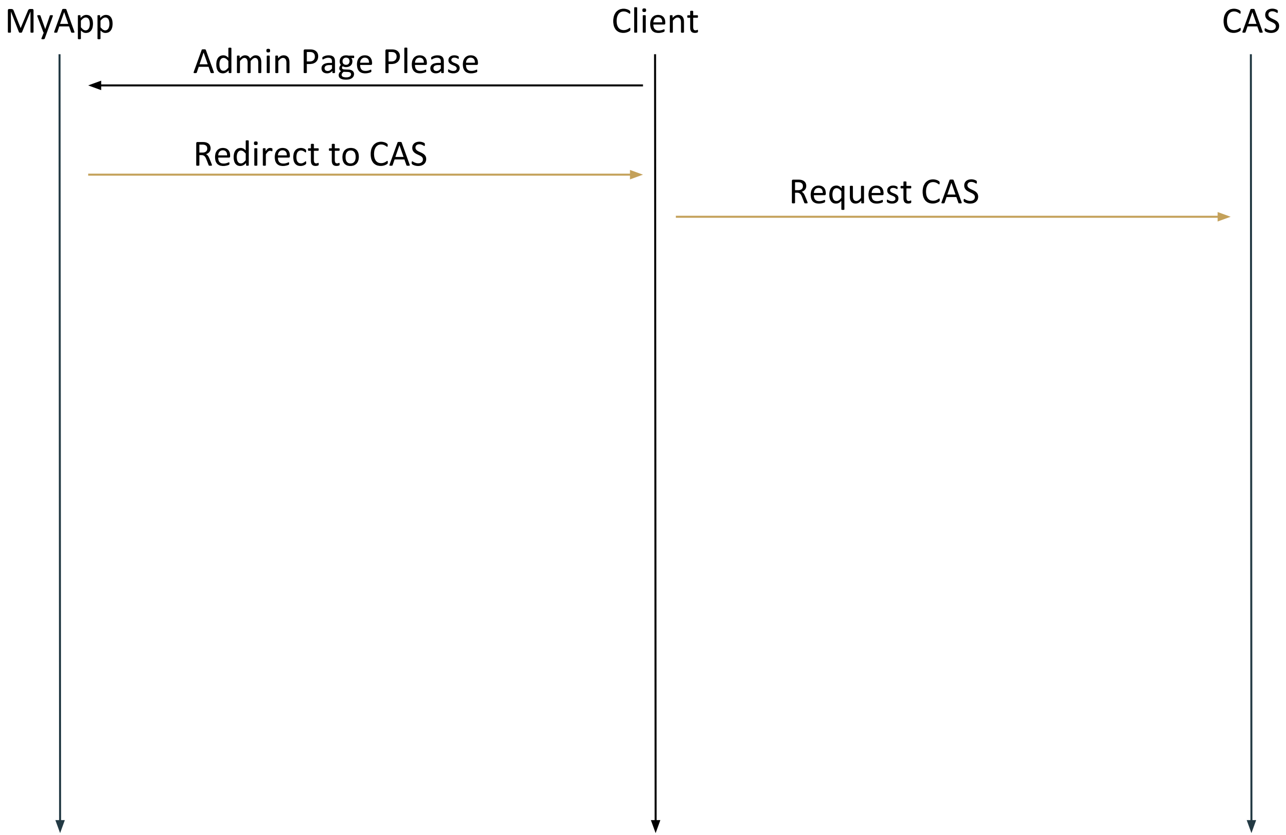
MyApp

Client

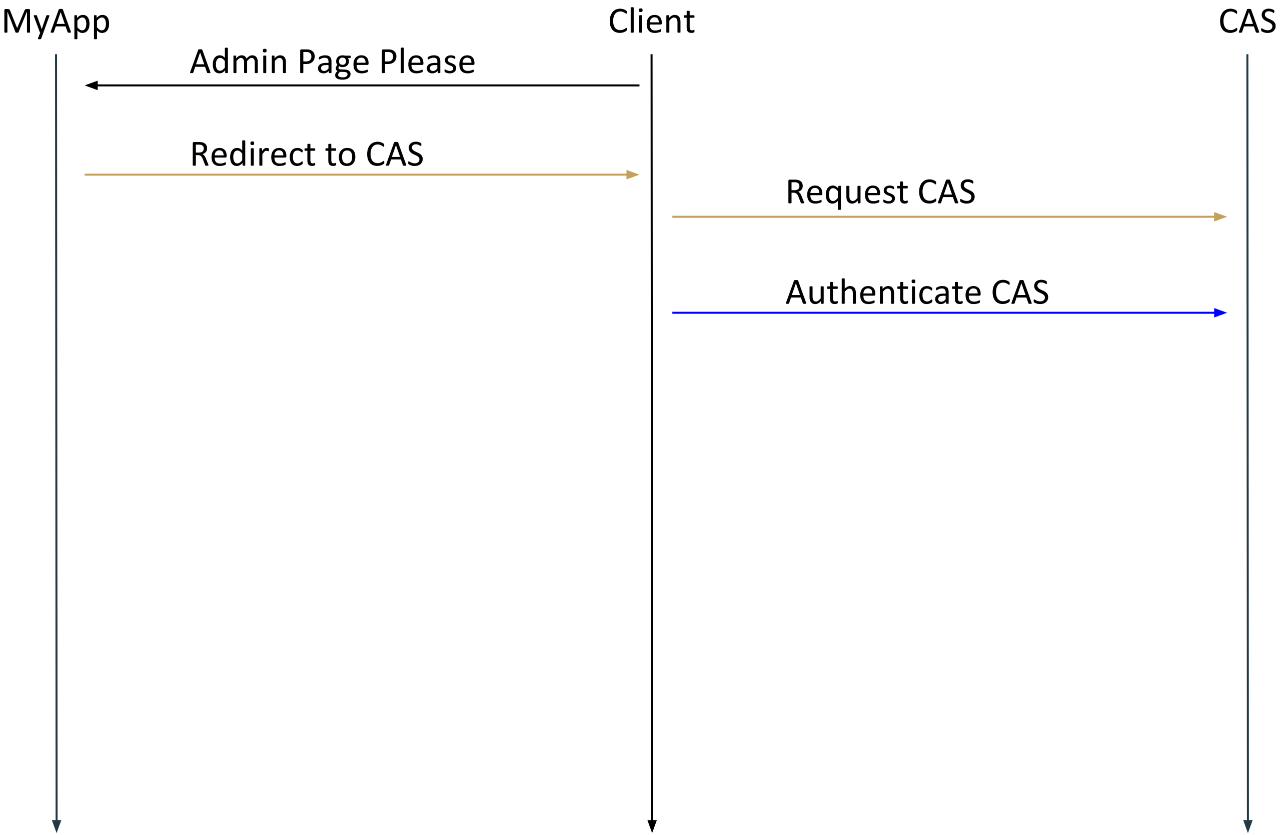
CAS

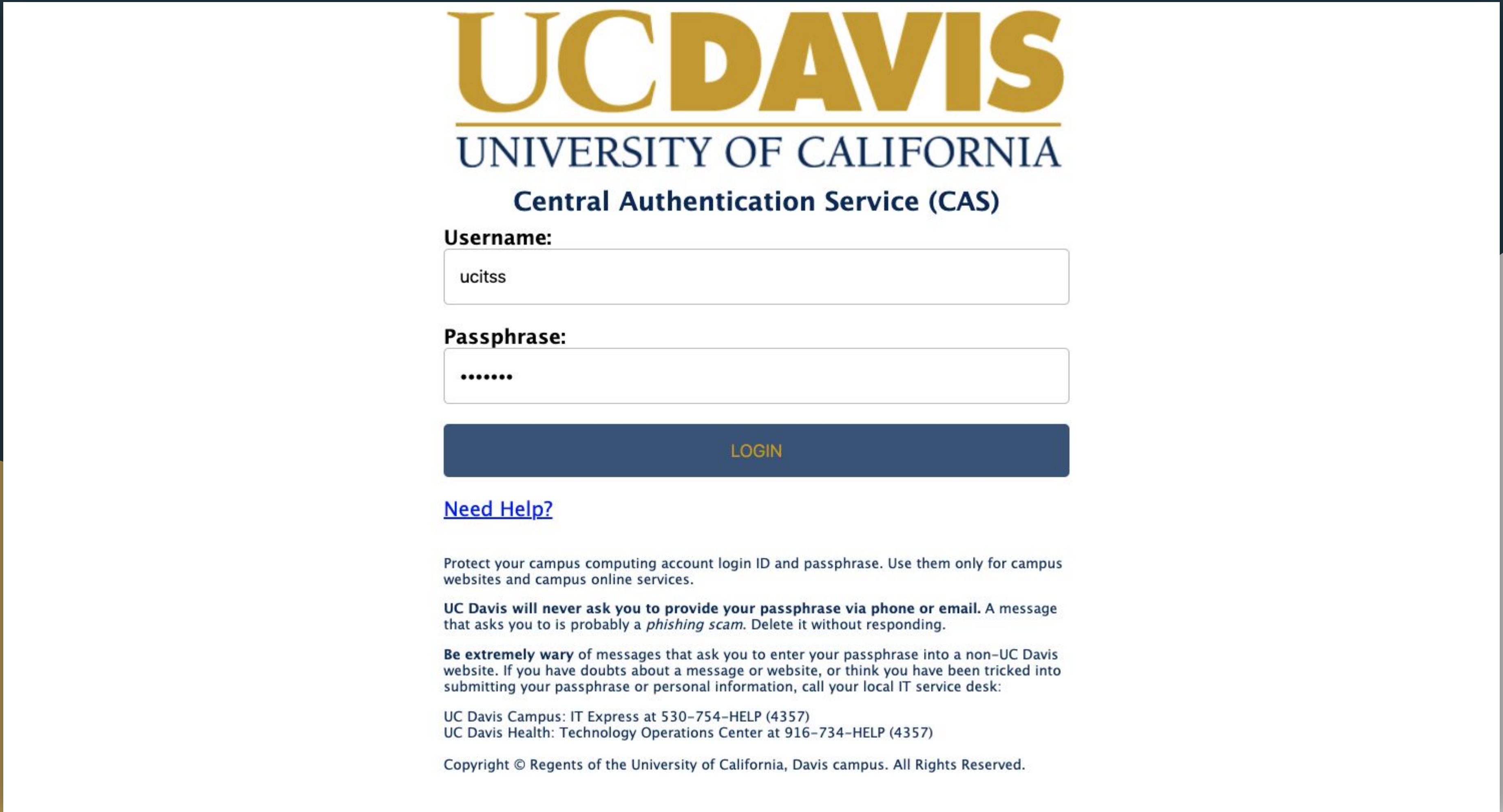
Admin Page Please

Server: https://cas.ucdavis.edu/cas/login?service=[myappurl]&state=[privatestate]



Server: https://cas.ucdavis.edu/cas/login?service=[myappurl]&state=[privatestate]





Central Authentication Service (CAS)

Username: ucitss

Passphrase: •••••••

Need Help?

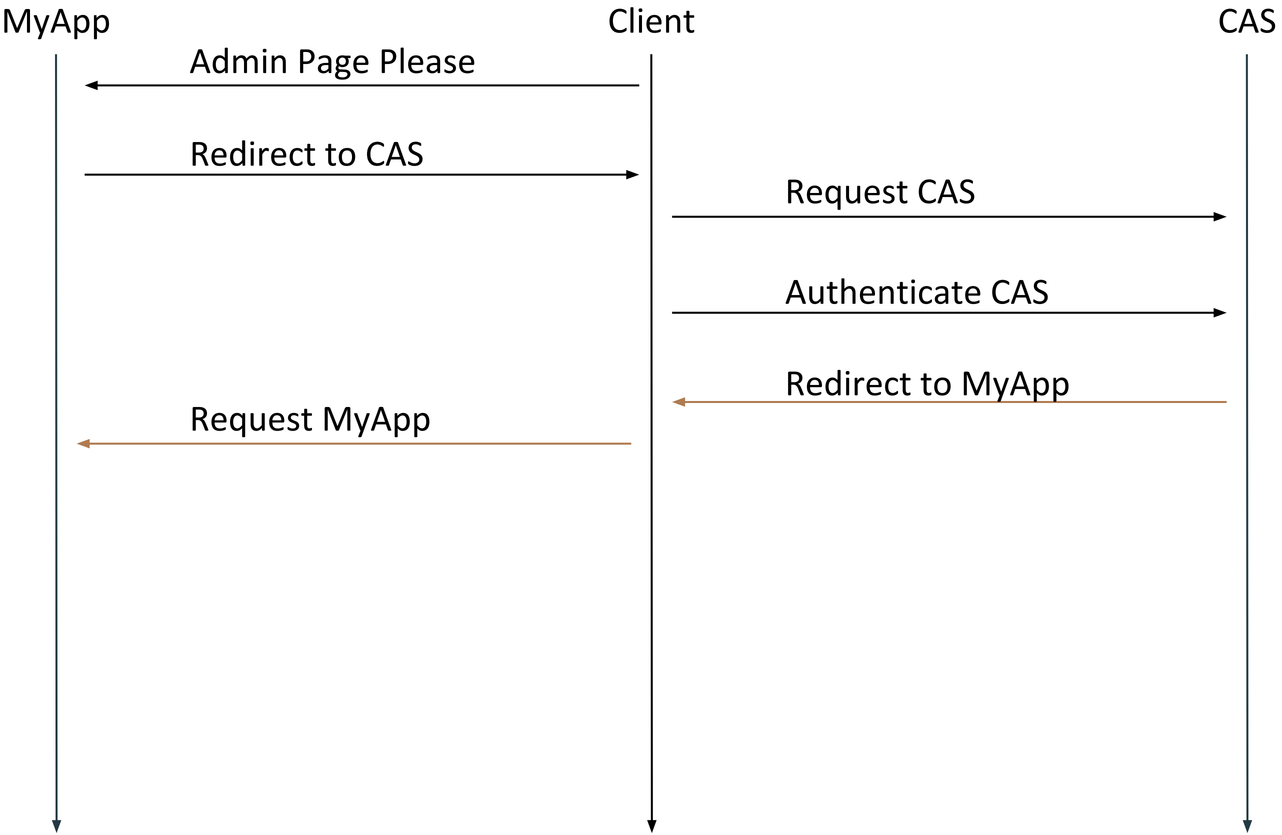
Protect your campus computing account login ID and passphrase. Use them only for campus websites and campus online services.

UC Davis will never ask you to provide your passphrase via phone or email. A message that asks you to is probably a *phishing scam*. Delete it without responding.

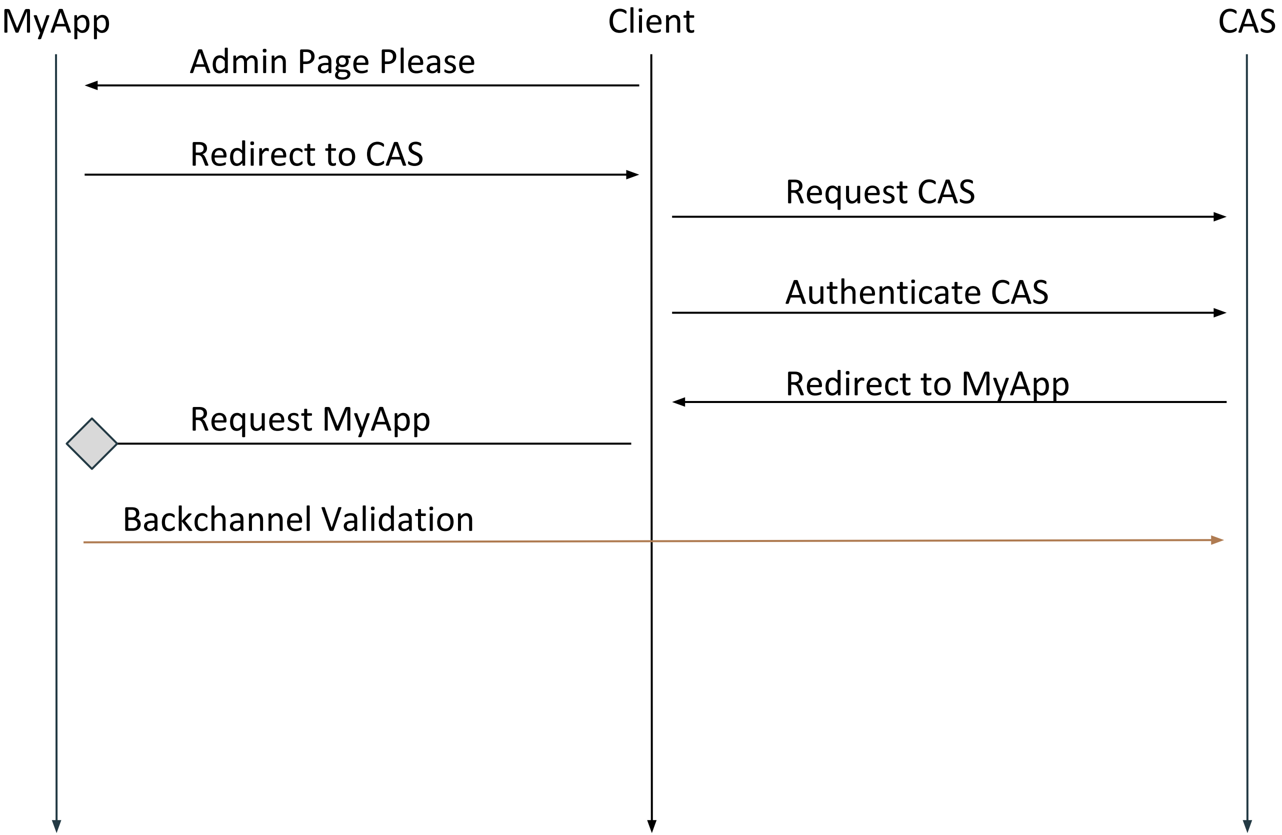
Be extremely wary of messages that ask you to enter your passphrase into a non-UC Davis website. If you have doubts about a message or website, or think you have been tricked into submitting your passphrase or personal information, call your local IT service desk:

UC Davis Campus: IT Express at 530-754-HELP (4357)
UC Davis Health: Technology Operations Center at 916-734-HELP (4357)

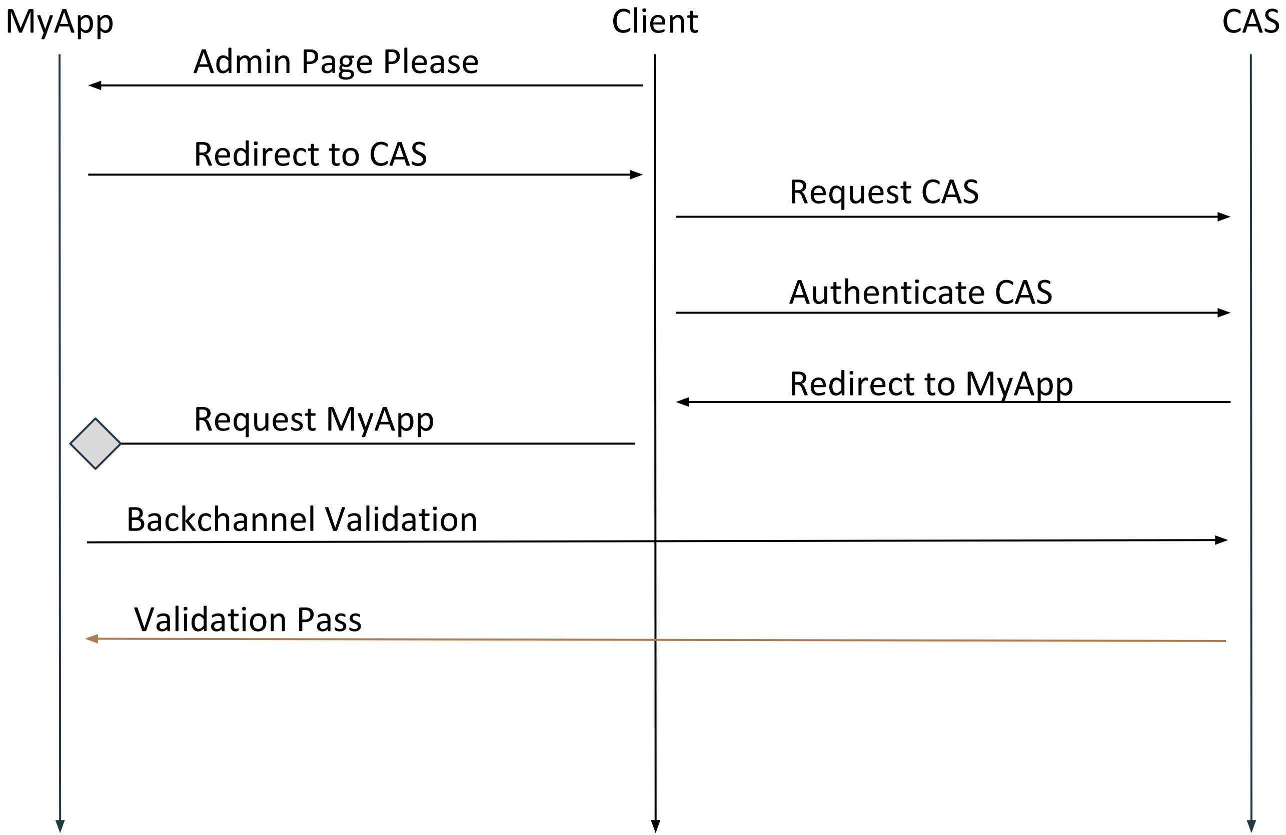
CAS: https://myapp.ucdavis.edu/login?state=[privatestate]&ticket=[casticket]



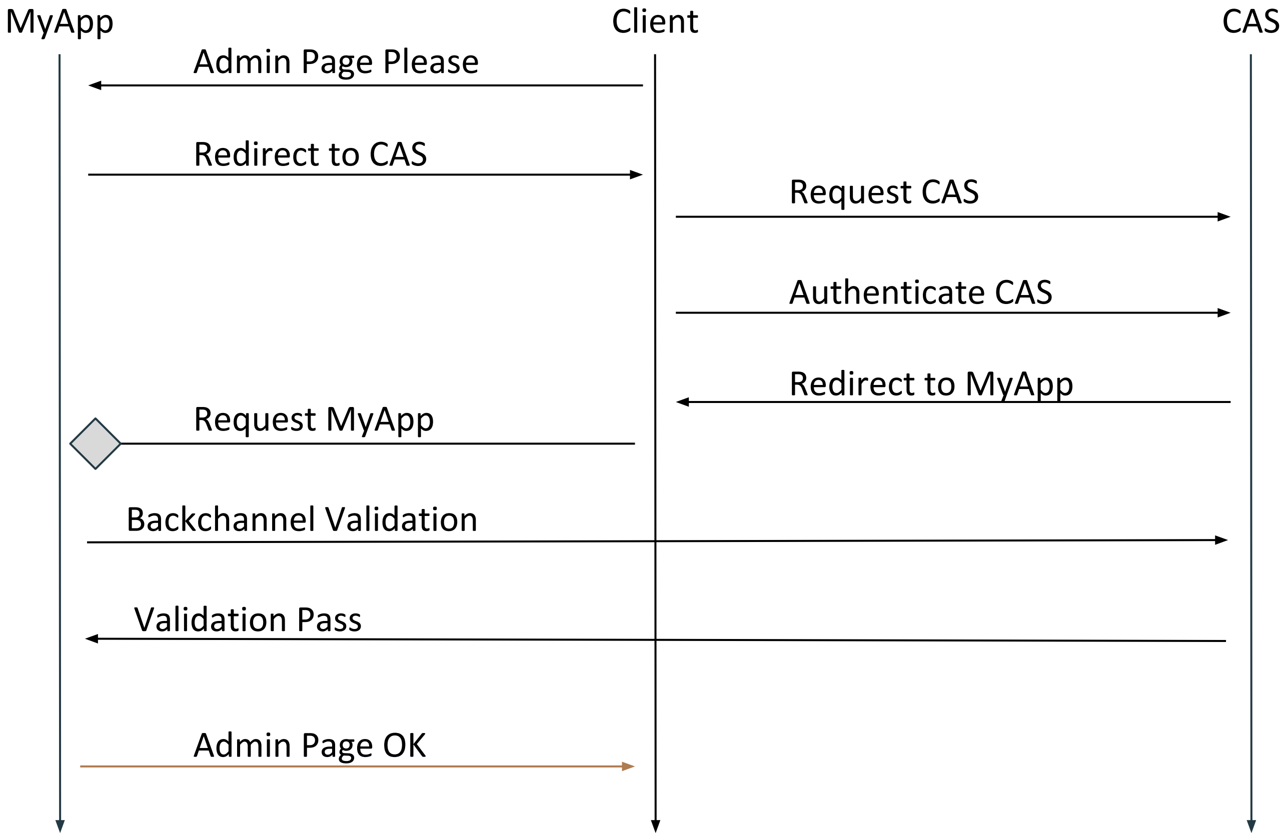
MyApp: https://cas.ucdavis.edu/cas/validate?service=[myappurl]&ticket=[casticket]



MyApp: Valid “yes + kerberos” response from backchannel



MyApp: https://myapp.ucdavis.edu/admin



CAS Timeline (DEMO)

Shibboleth

- Single Sign-On Platform
- Created & Supported by Internet2
- Used by every UC Campus
  - And 500+ other Educational & Research Institutions

SAML

- Shibboleth software implements Security Assertion Markup Language (SAML)
- Provides a federated single sign-on and attribute exchange framework

SAML

Shibboleth

- SAML is an XML based standard, including an:
    - XML language (tags)
    - XML message protocol.
- SAML 2.0, the current standard, was created in 2005.

Concepts

Shibboleth.

Identity Provider (IdP)

- Authentication Authority
- User-identity source
- Centrally Installed

Service Provider (SP)

- Authentication Client
- Discovers IdP
- Web Server Installed

Authentication Flow

Shibboleth®

- Web based login flow
- Includes attribute release
- No backchannel validation needed

Step 0

- Need to install Service Provider (SP)
- Generally installed on web server
  - Works with IIS, Apache, Nginx and more
- Configure with shibboleth2.xml file

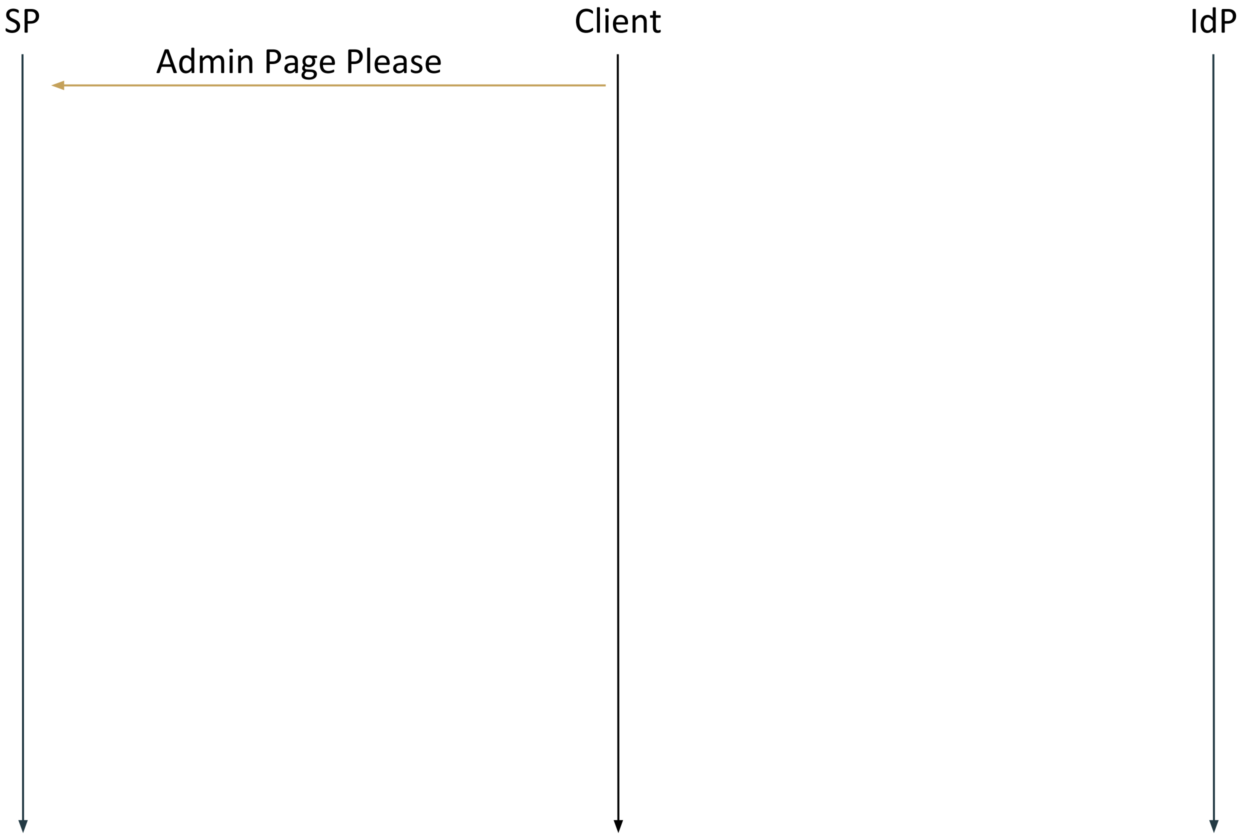
SP Config

- SP ID (URL)
- IdP location info
- Supported Protocols
- Signing Certificates/Keys
- User Attributes Desired

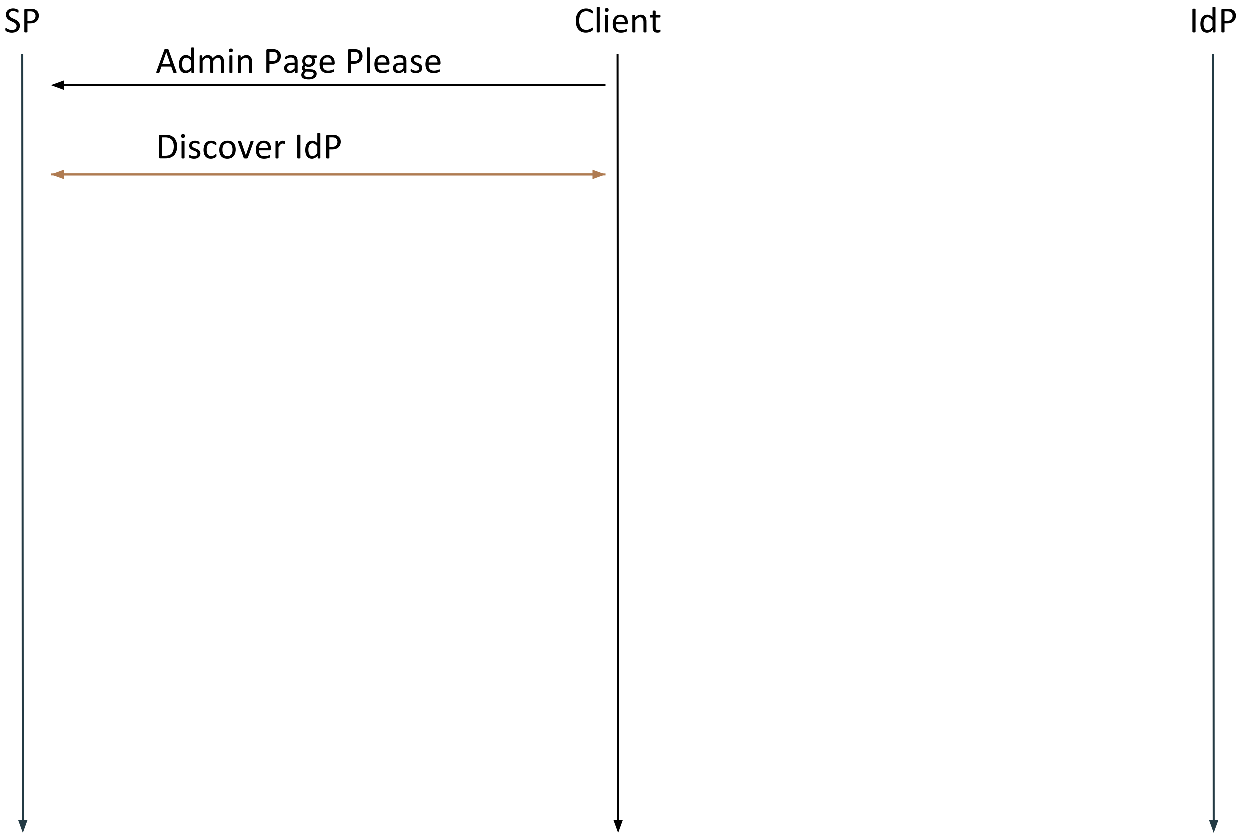
Authentication Flow

Shibboleth

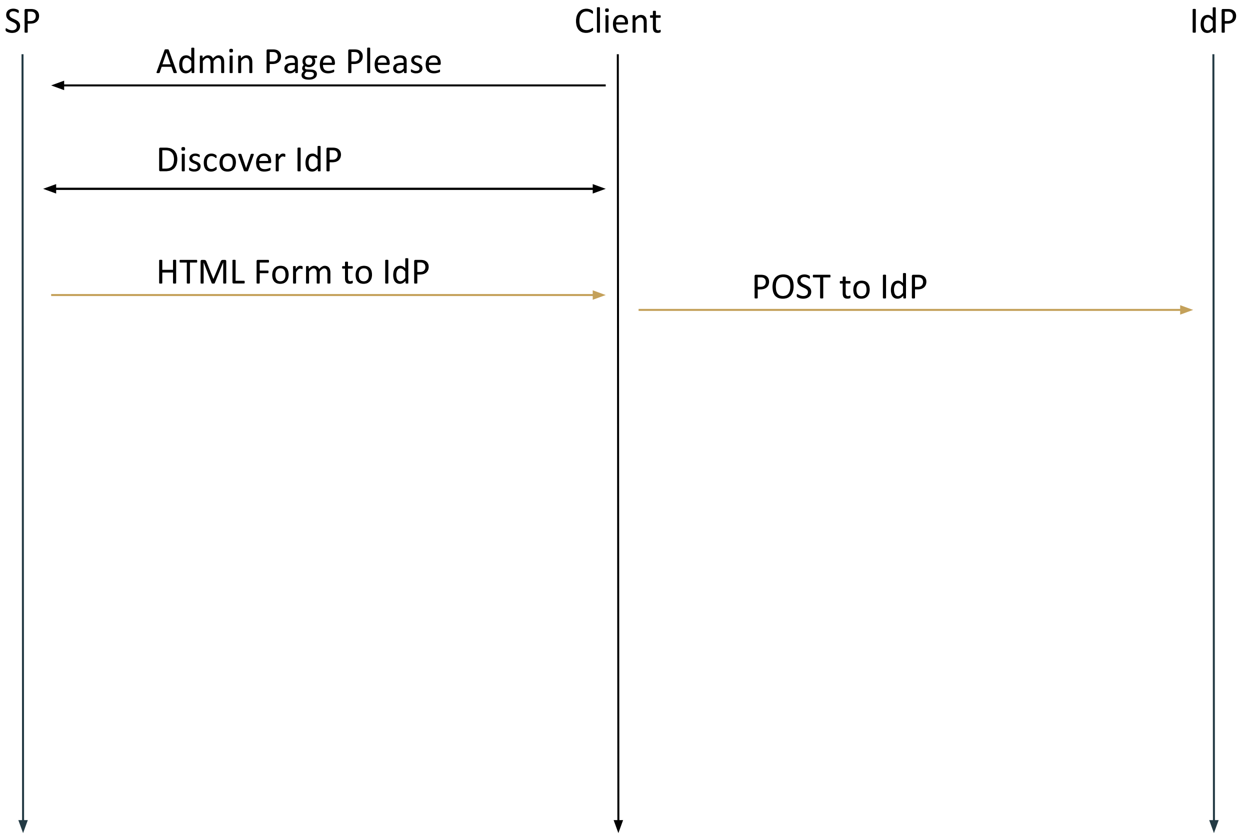
Client: https://myapp.ucdavis.edu/admin



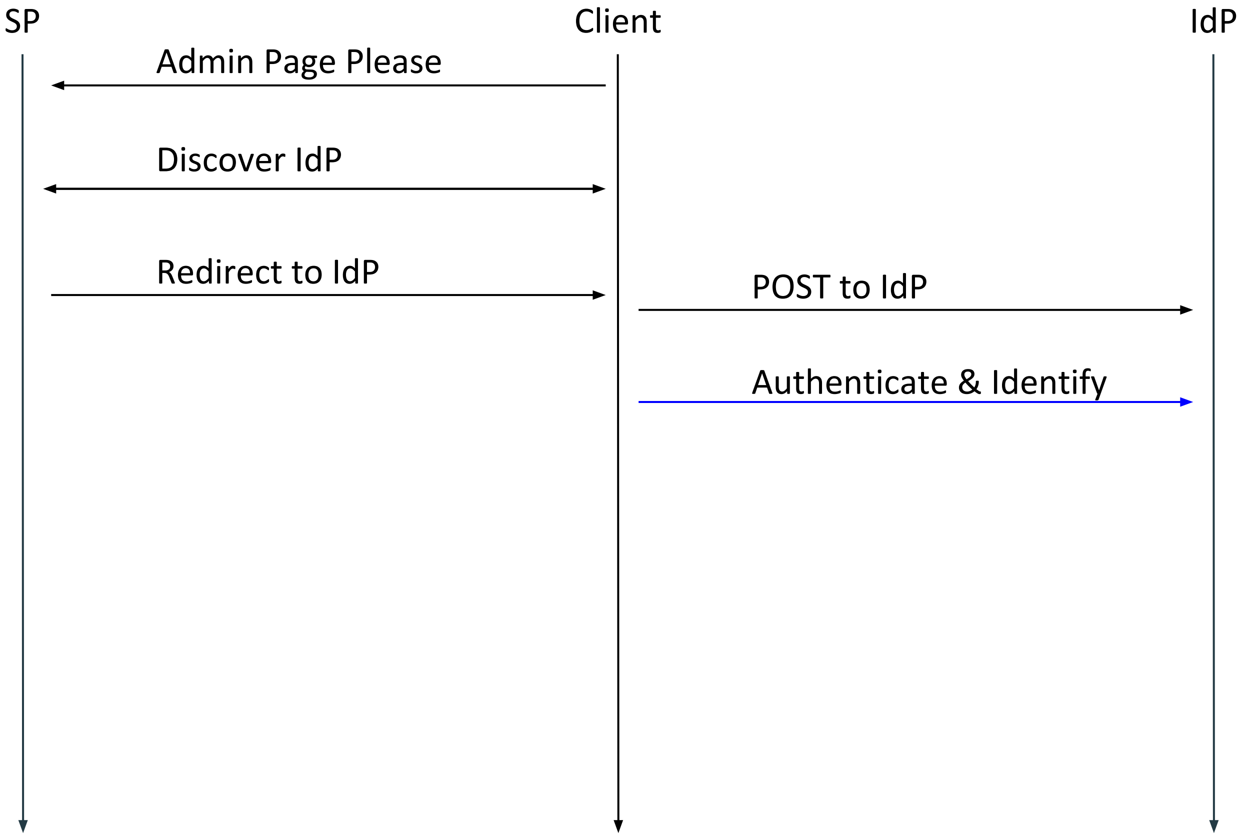
SP: https://????

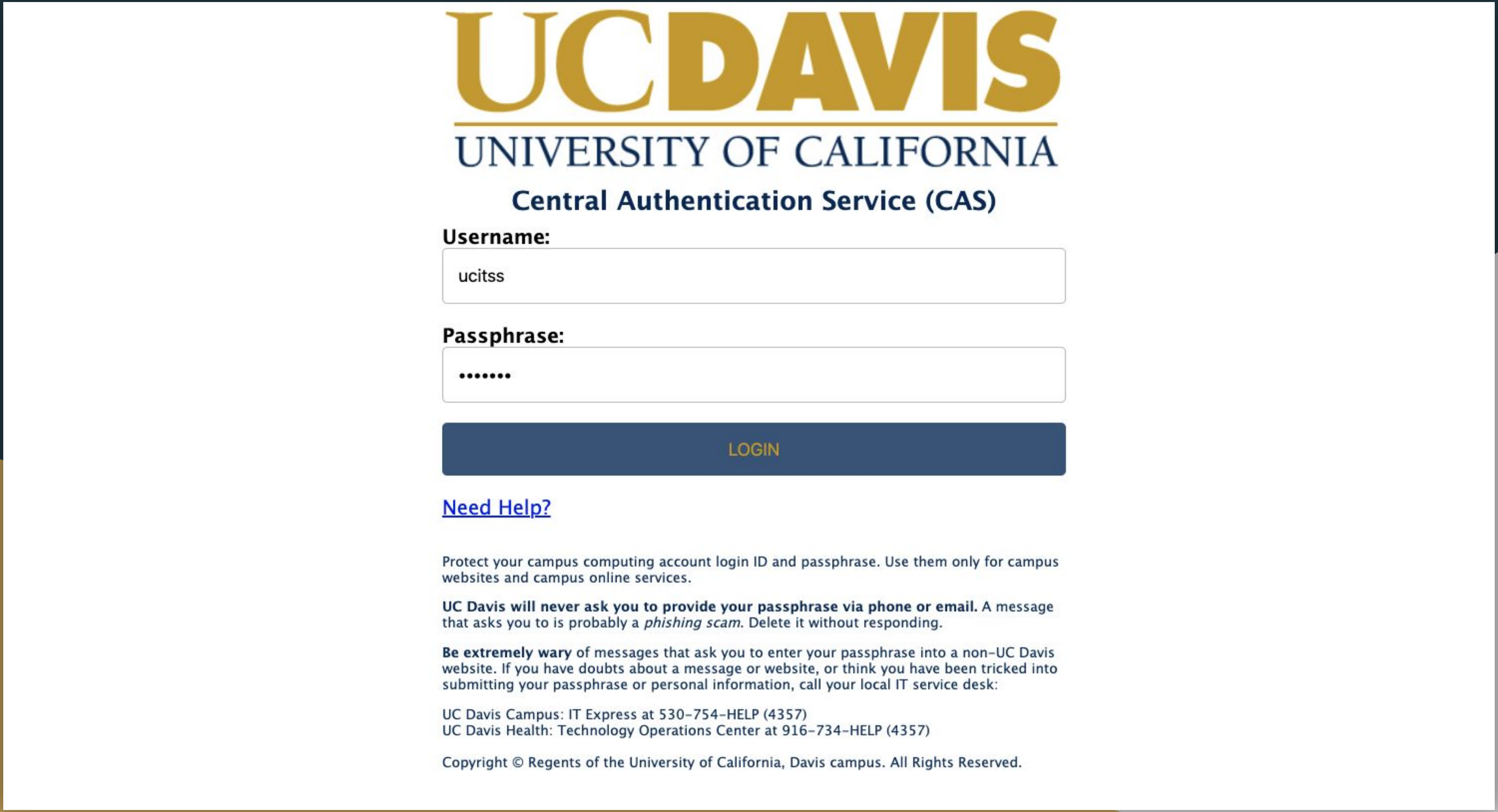


SP: https://shibboleth.ucdavis.edu/idp/profile/SAML2/POST/SSO



SP: https://shibboleth.ucdavis.edu/idp/profile/SAML2/POST/SSO





UCDAVIS
UNIVERSITY OF CALIFORNIA

Central Authentication Service (CAS)

Username: ucitss

Passphrase: •••••••

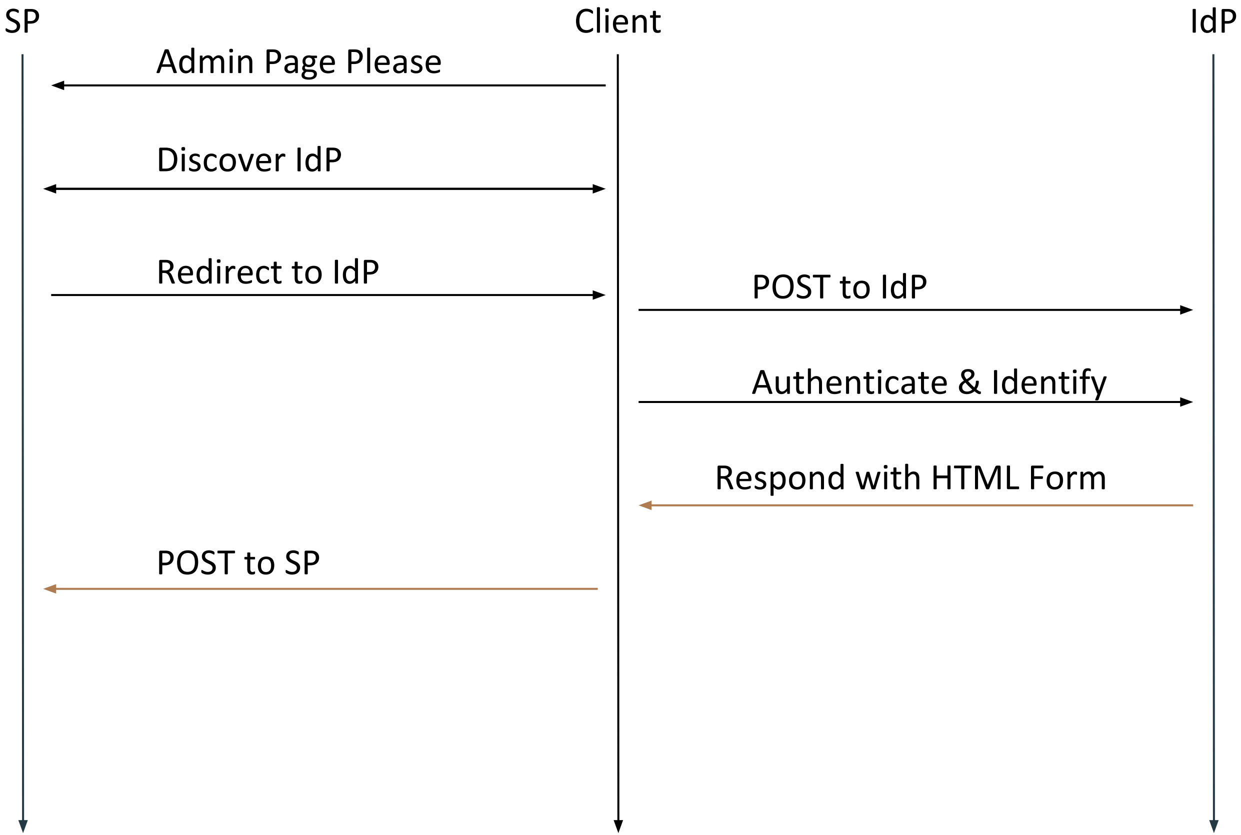
Protect your campus computing account login ID and passphrase. Use them only for campus websites and campus online services.

UC Davis will never ask you to provide your passphrase via phone or email. A message that asks you to is probably a *phishing scam*. Delete it without responding.

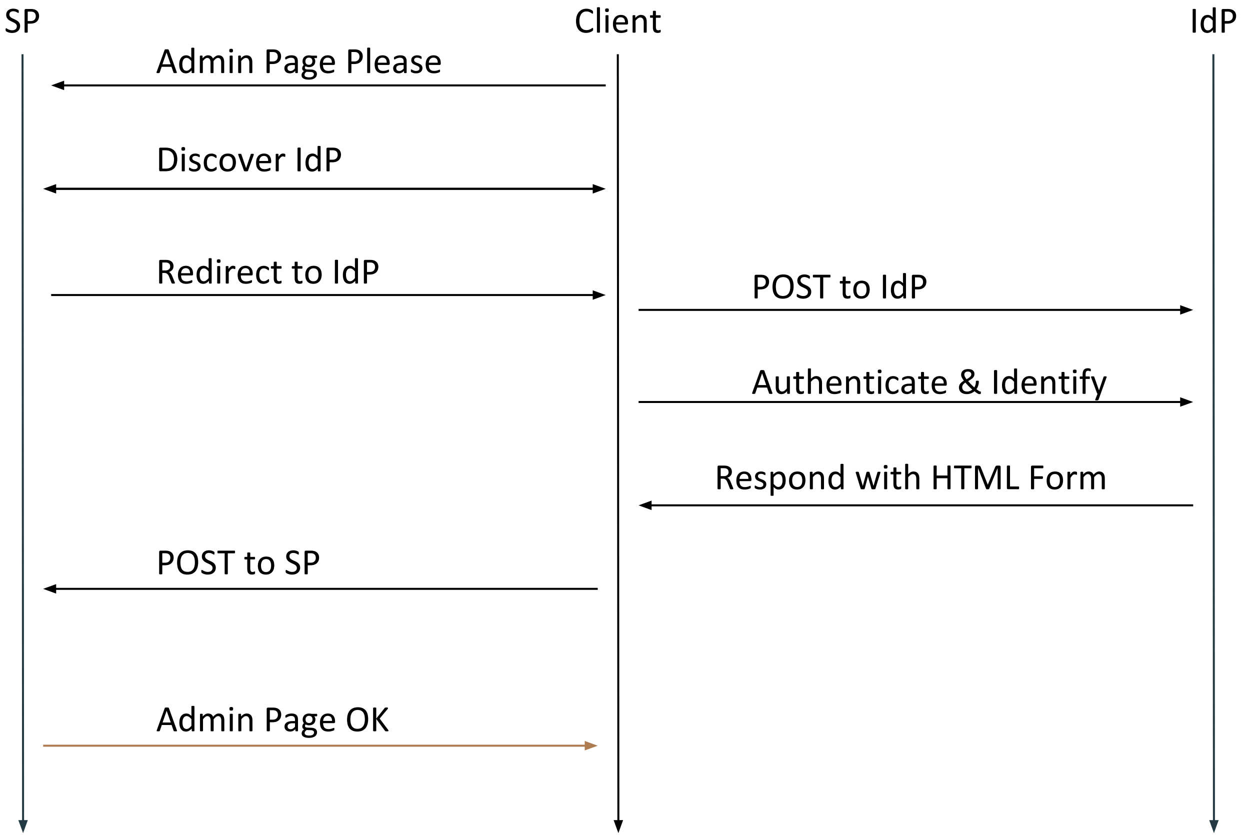
Be extremely wary of messages that ask you to enter your passphrase into a non-UC Davis website. If you have doubts about a message or website, or think you have been tricked into submitting your passphrase or personal information, call your local IT service desk:

UC Davis Campus: IT Express at 530-754-HELP (4357)
UC Davis Health: Technology Operations Center at 916-734-HELP (4357)

IdP: https://myapp.ucdavis.edu/login



SP: Hi Scott! Here’s https://myapp.ucdavis.edu/admin

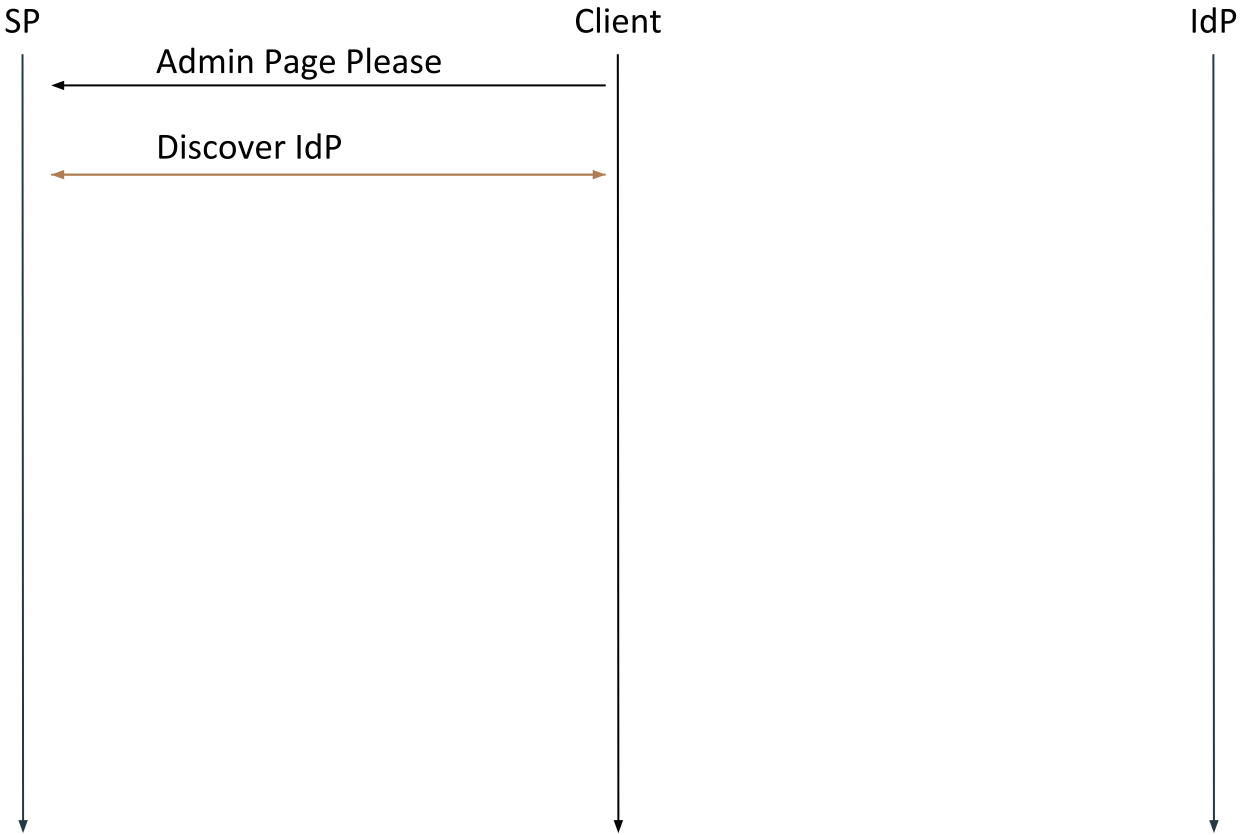


Shibboleth Timeline (DEMO)

Federation & Discovery

Shibboleth®

SP: https://????



Federation & Discovery

Shibboleth.

```
<SSO
entityID="https://shibboleth.ucdavis.edu
/idp">SAML2 SAML1</SSO>
```

Federation & Discovery

```
<SSO discoveryProtocol="SAMLDS"
discoveryURL="https://myapp-dev.ucdavis.
edu/shibboleth-ds/index.html">SAML2
SAML1</SSO>
```

Federation & Discovery

Shibboleth

```
<SSO discoveryProtocol="SAMLDS"
discoveryURL="https://wayf.incommonfederation.org/DS/WAYF">SAML2 SAML1</SSO>
```

InCommon

https://wayf.incommonfederation.org/DS/WAYF

- Hosts secure metadata for Education & Research Institutions
- Includes a directory, key & certificates, and technical guidelines
- Operated by Internet2

InCommon

Shibboleth®

- Identifiers
  - eduPersonUniqueId
  - eduPersonPrincipalName
- Mail attribute
  - mail
- Authorization attributes
  - eduPersonScopedAffiliation
  - eduPersonEntitlement

Review

- Web-based Authentication Flow
- Available on every UC Campus
- Implements SAML
    - Easy interop with external vendors

The Twitter Problem

- Authentication is great, but how we do distributed Authorization?
- Can we have a simpler protocol?
- Also I hear JSON is cool let’s use that

OAuth

- Developed by Twitter & Google & others
- Draft 2007, Published 2010
- Popular, but quickly surpassed by OAuth 2.0 in 2012

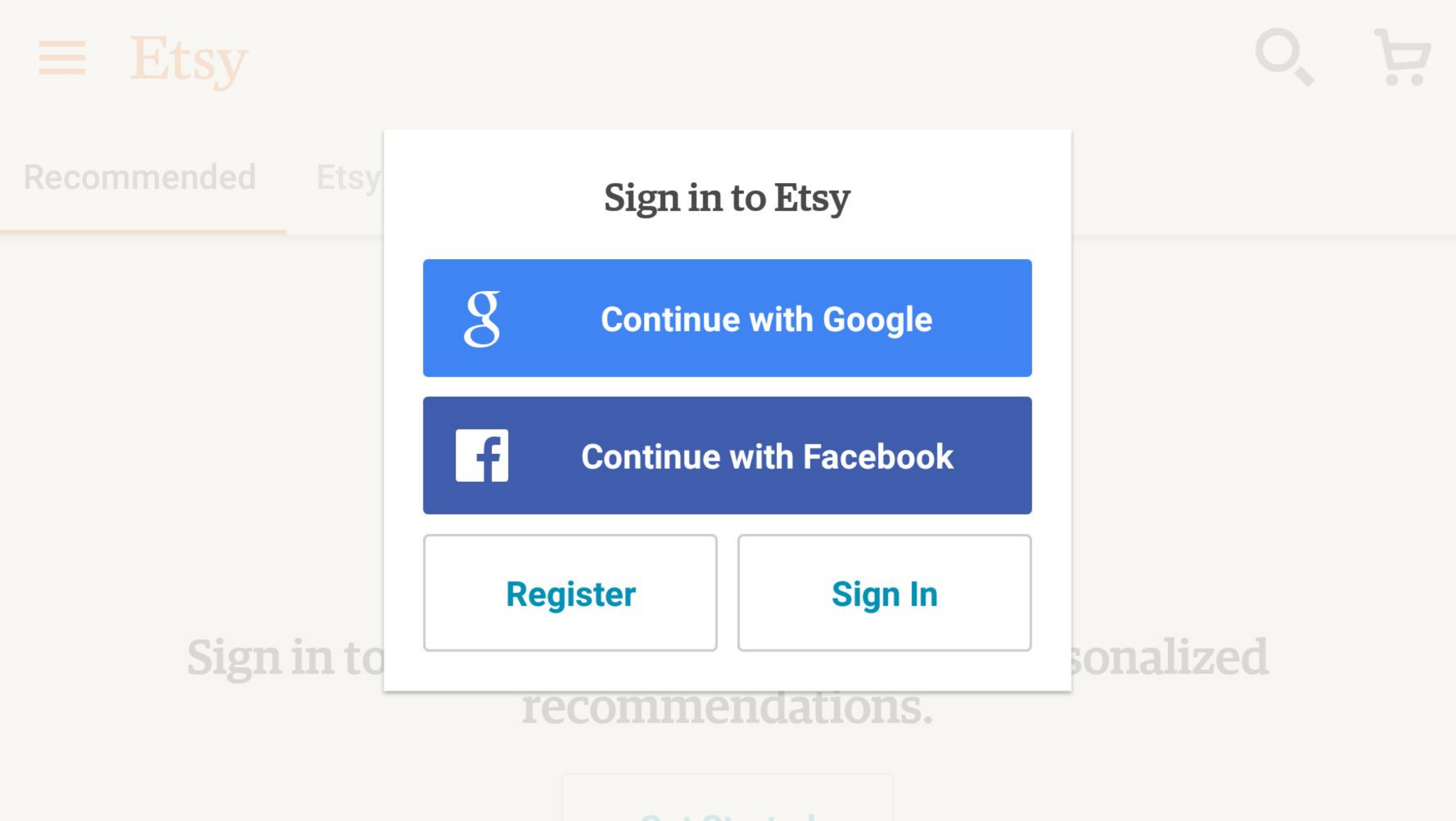
OAuth 2.0

- Supports many different authorization flows.
- Works with mobile apps, SPAs, IoT.
- Based on HTTP, uses TLS for security/encryption.
- Used at every major tech company as primary API auth.

Wait, I want to do Authentication!

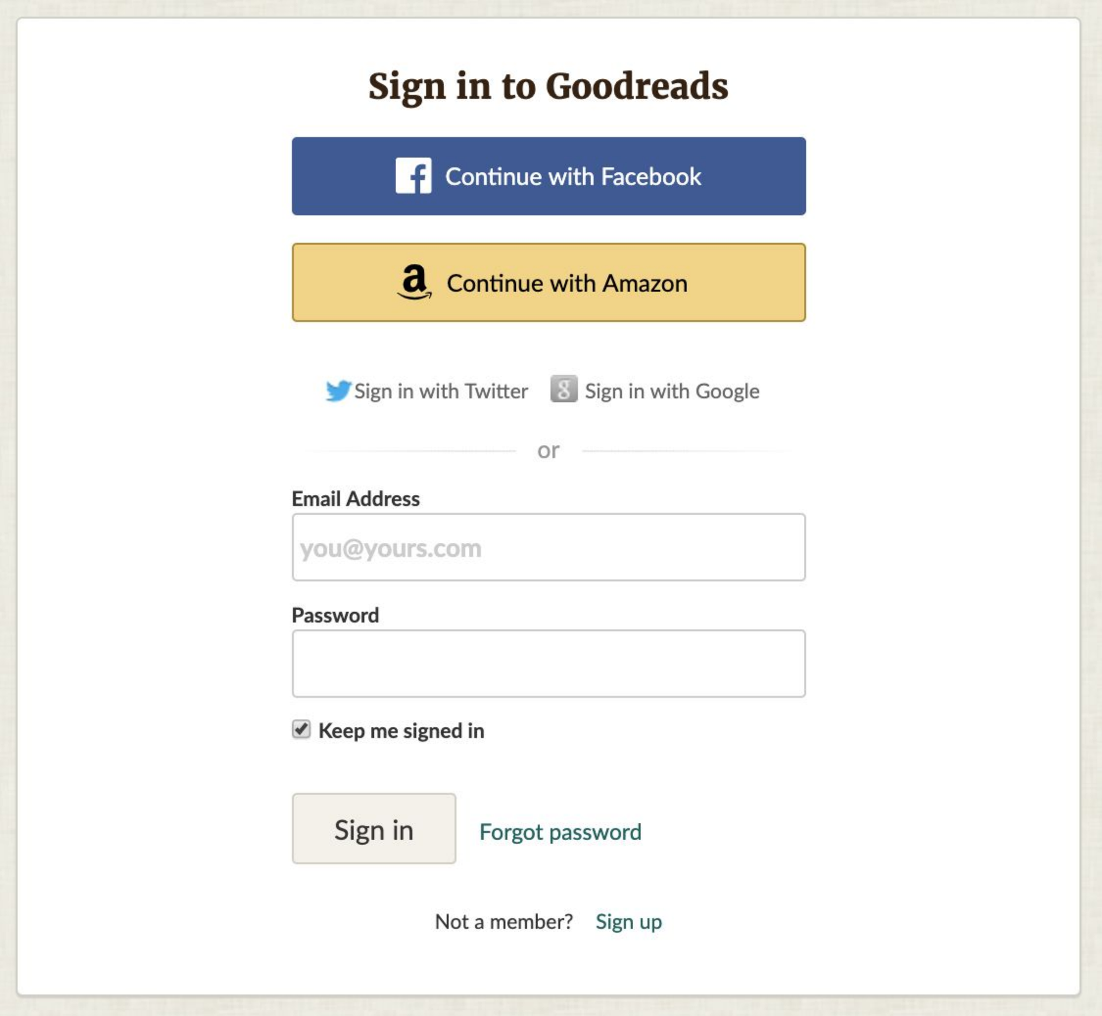
OpenID Connect

- Simple, thin layer on top of OAuth 2.0
- Goal is Single Sign-on across many sites (SSO)
- Widely used for “Social Login”



Sign in to Etsy

Sign in to sonalized recommendations.



Sign in to Goodreads

Email Address

you@yours.com

Password

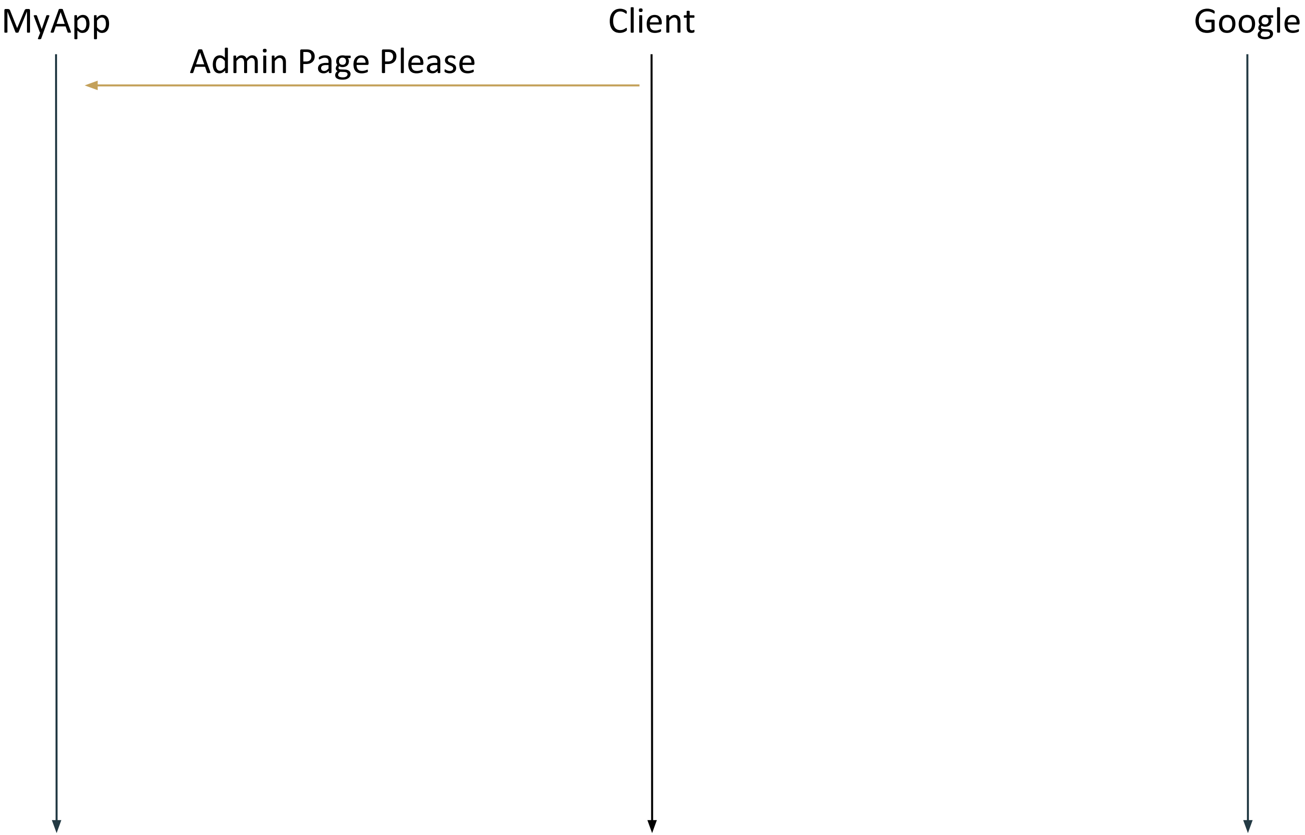
☑ Keep me signed in

Not a member? Sign up

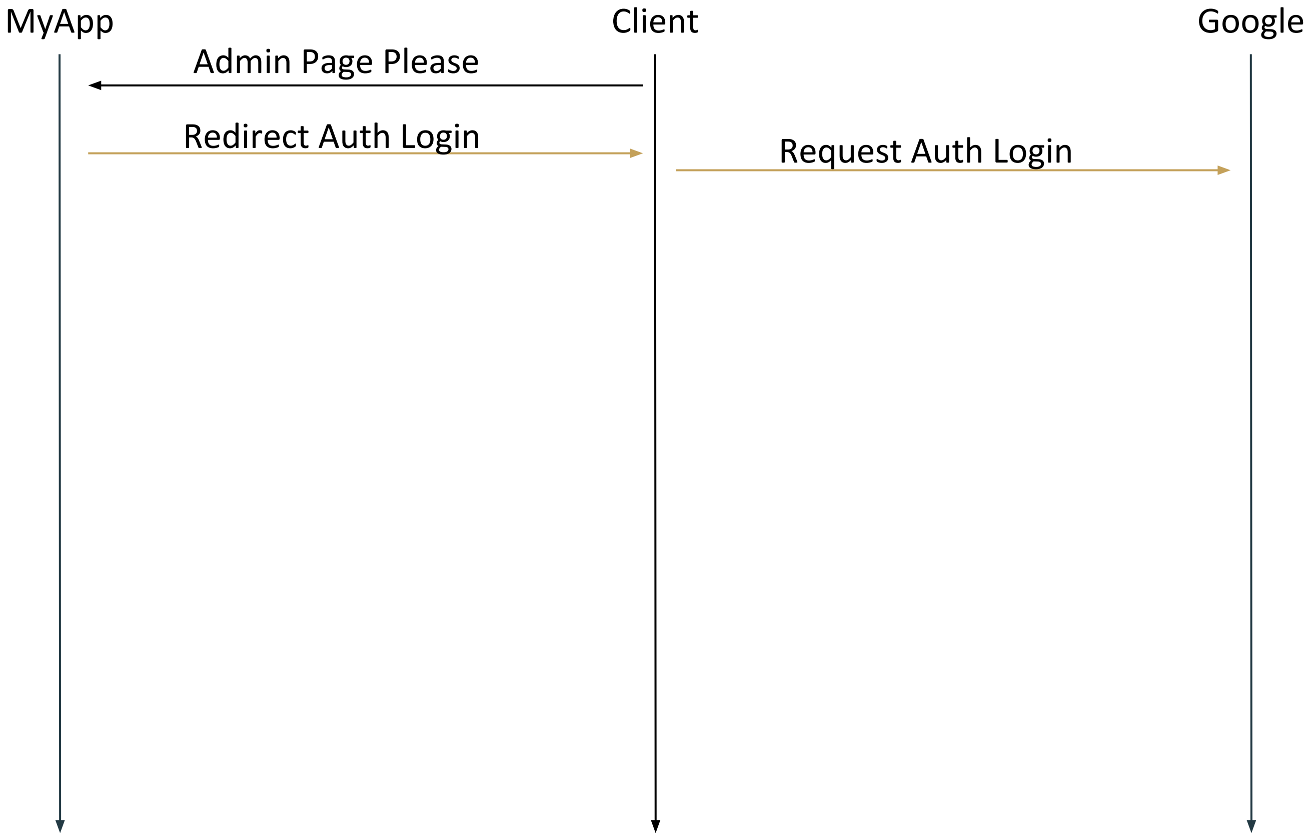
OpenID Connect Flow

- Web based login flow
- Client approved attribute grant
- Optional backchannel validation

Client: https://myapp.ucdavis.edu/admin



Client: https://accounts.google.com/o/oauth2/v2/auth?{params}

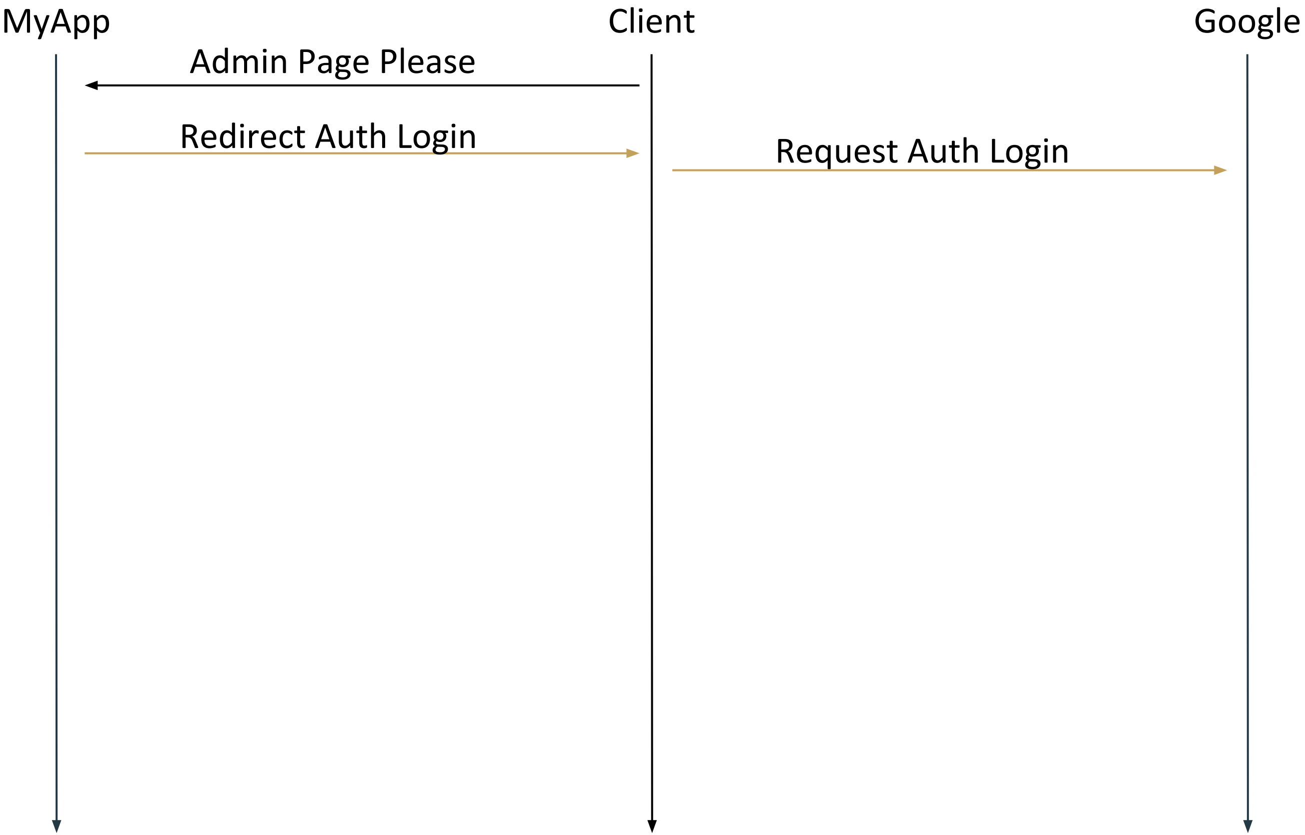


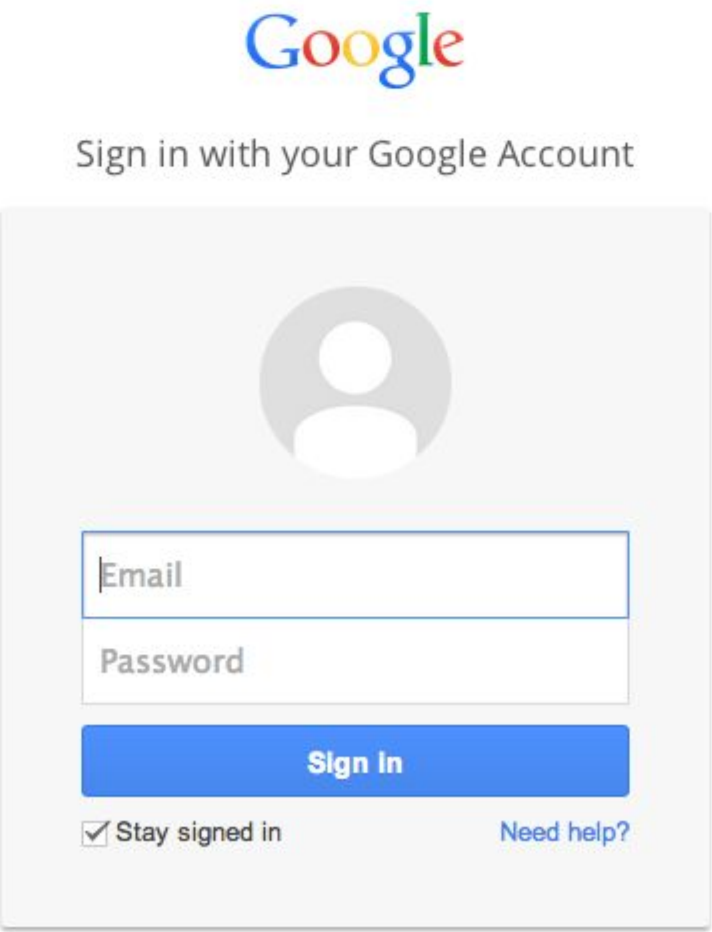
https://accounts.google.com/o/oauth2/v2/auth?{params}

Options

- request_type
- client_id
- scope
- state
- request_uri (not required)

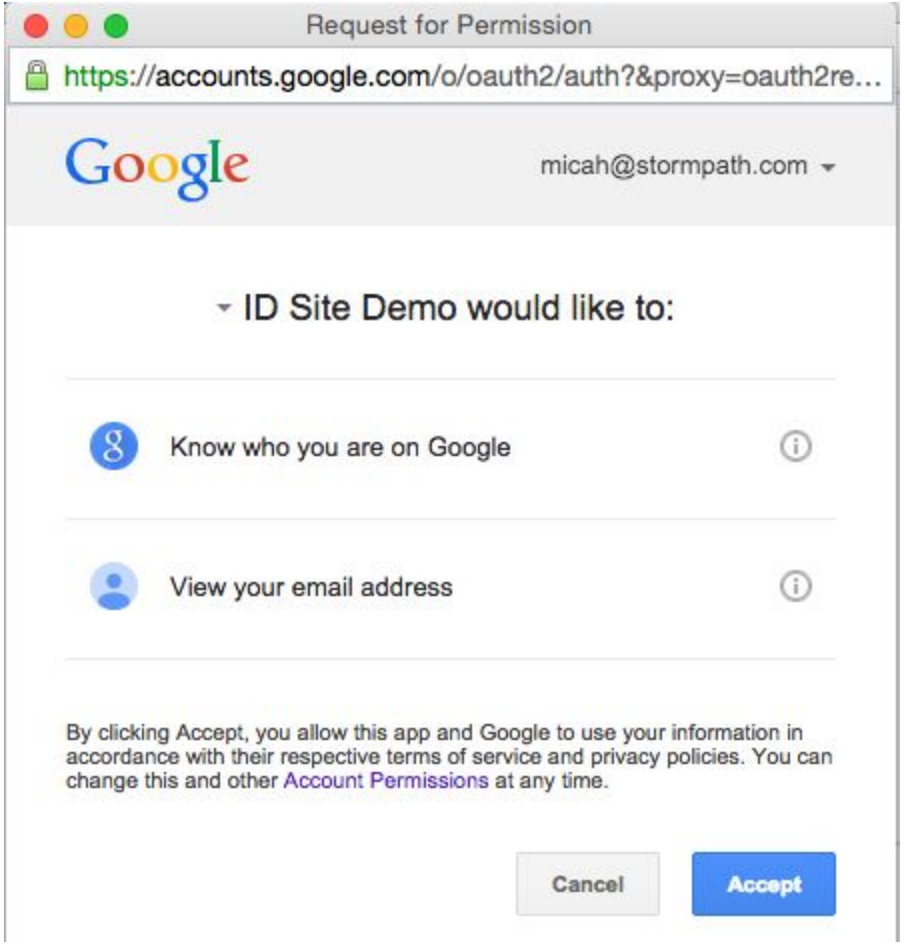
Client: https://accounts.google.com/o/oauth2/v2/auth?{params}





Sign in with your Google Account

☑ Stay signed in



Request for Permission

https://accounts.google.com/o/oauth2/auth?&proxy=oauth2re...

Google

micah@stormpath.com

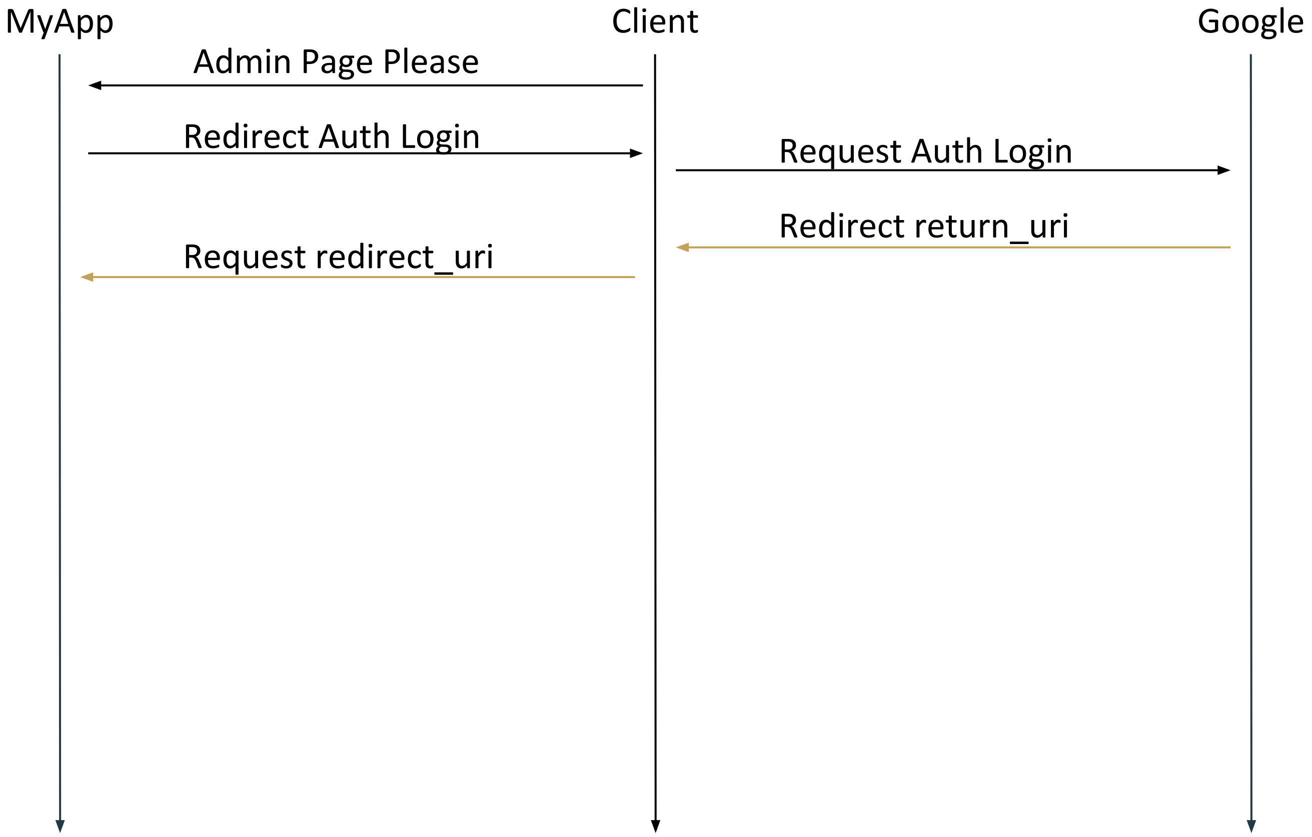
ID Site Demo would like to:

Know who you are on Google

View your email address

By clicking Accept, you allow this app and Google to use your information in accordance with their respective terms of service and privacy policies. You can change this and other Account Permissions at any time.

Client: https://myapp.ucdavis.edu/oauth?code=[auth_code]&state=[mystate]



MyApp

Client

Google

Admin Page Please

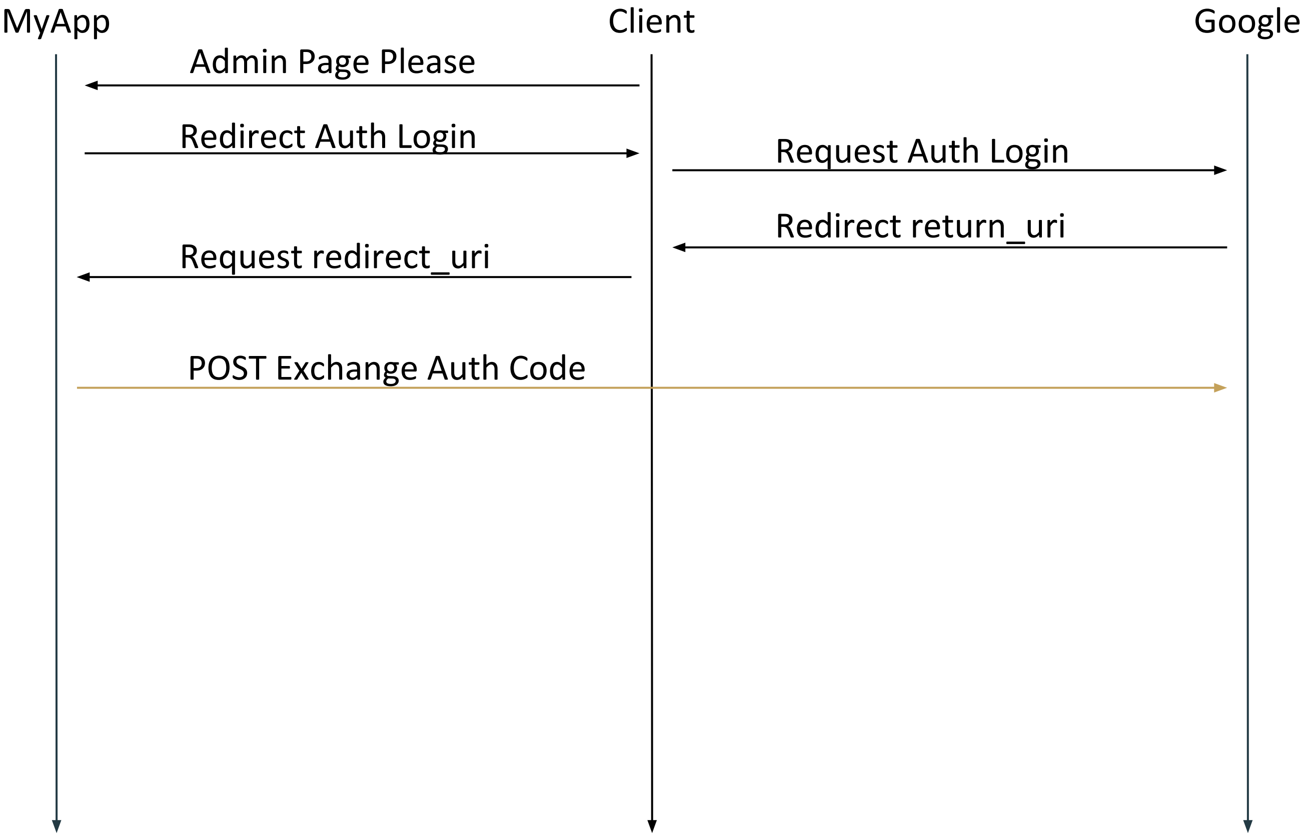
Redirect Auth Login

Request Auth Login

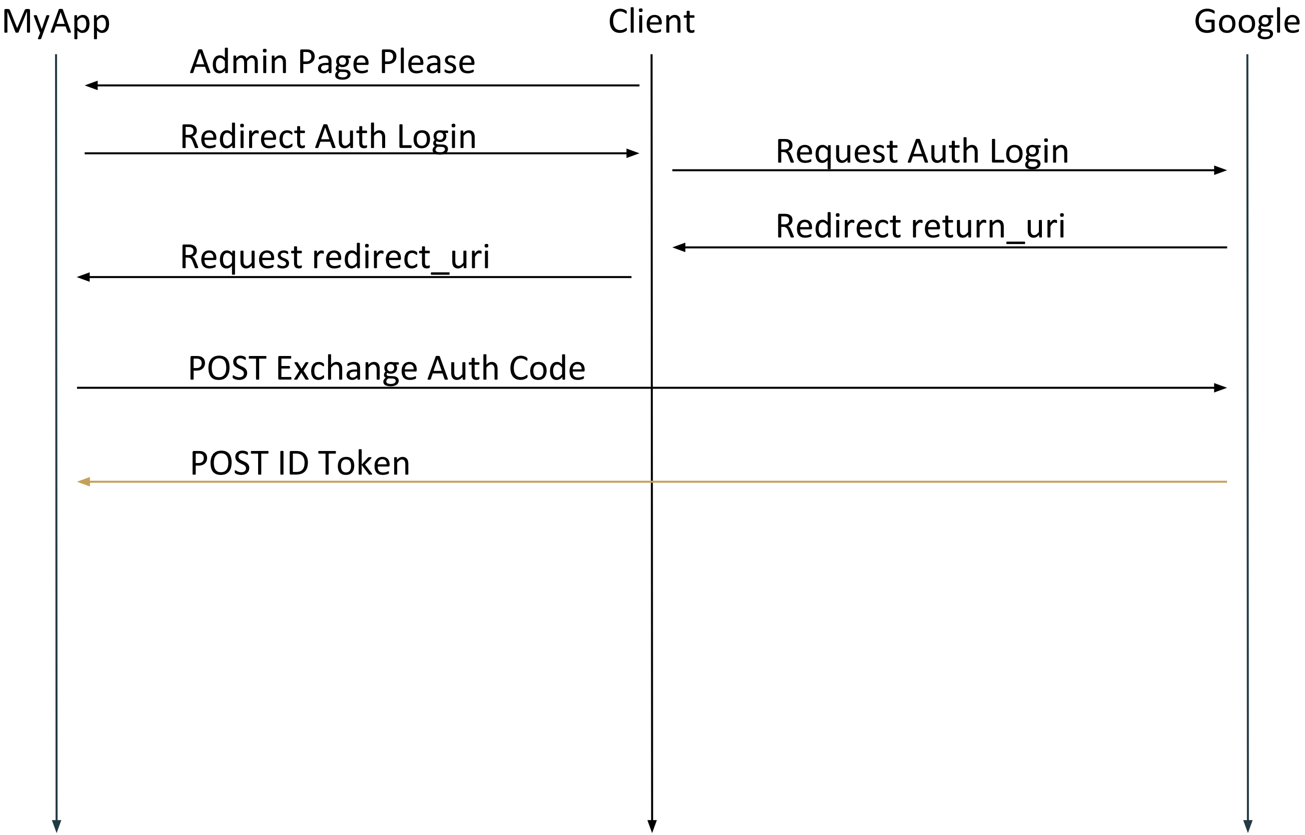
Redirect return_uri

Request redirect_uri

MyApp: https://www.googleapis.com/oauth2/v4/token?code=[auth_code]&client_id=[cid]



MyApp: https://myapp.ucdavis.edu/oauth



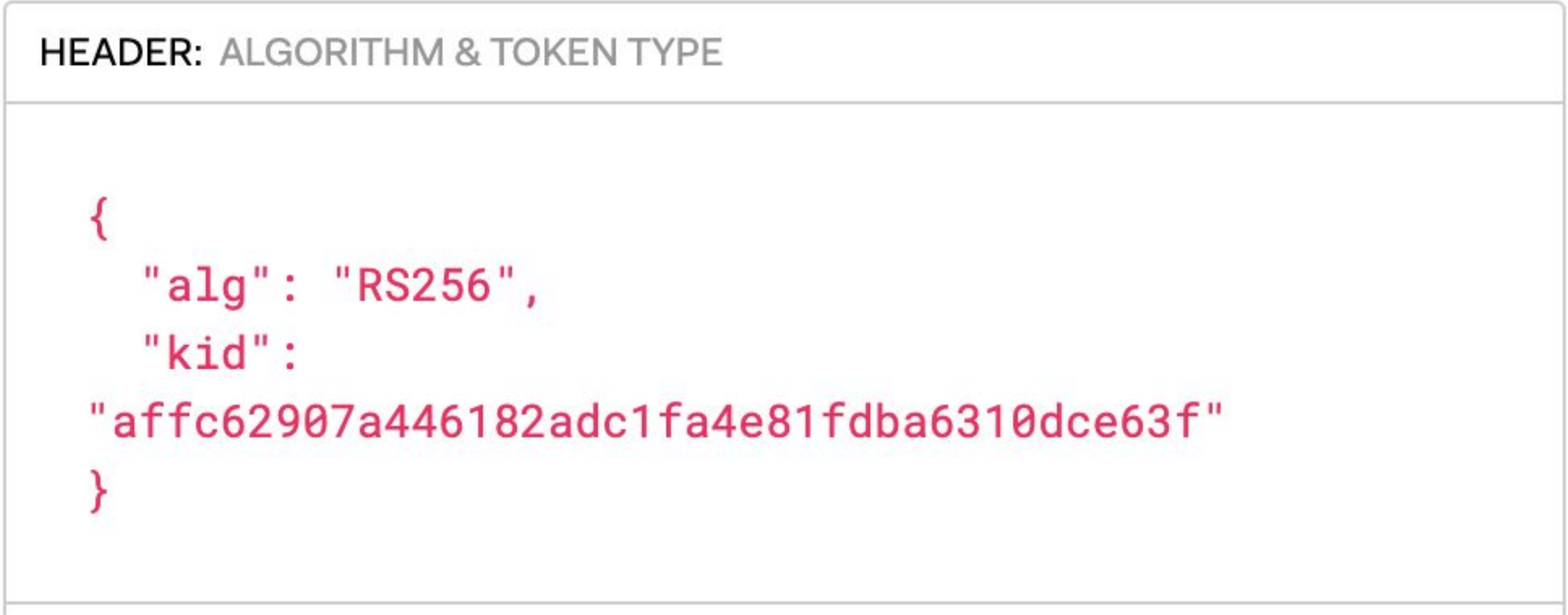
```
{
   "token_type": "Bearer",
   "expires_in": 3600,
   "id_token":
"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpX
VCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwi
bmFtZSI6IlNjb3R0IEtpcmtsYW5kIiwiZ
W1haWwiOiJzcmtpcmtsYW5kQHVjZGF2aX
MuZWR1IiwiYWZmaWxpYXRpb24iOiJTdGF
mZiIsImF3ZXNvbWVuZXNzIjoxMSwiaWF0
IjoxNTE2MjM5MDIyfQ.X5ReoSImK8rbQj
4-FxgyV-I6CXlnKMU1Gl2zDZdNCCE"
 }
```

JWT:
Industry standard RFC 7519 method for representing claims securely between two parties.

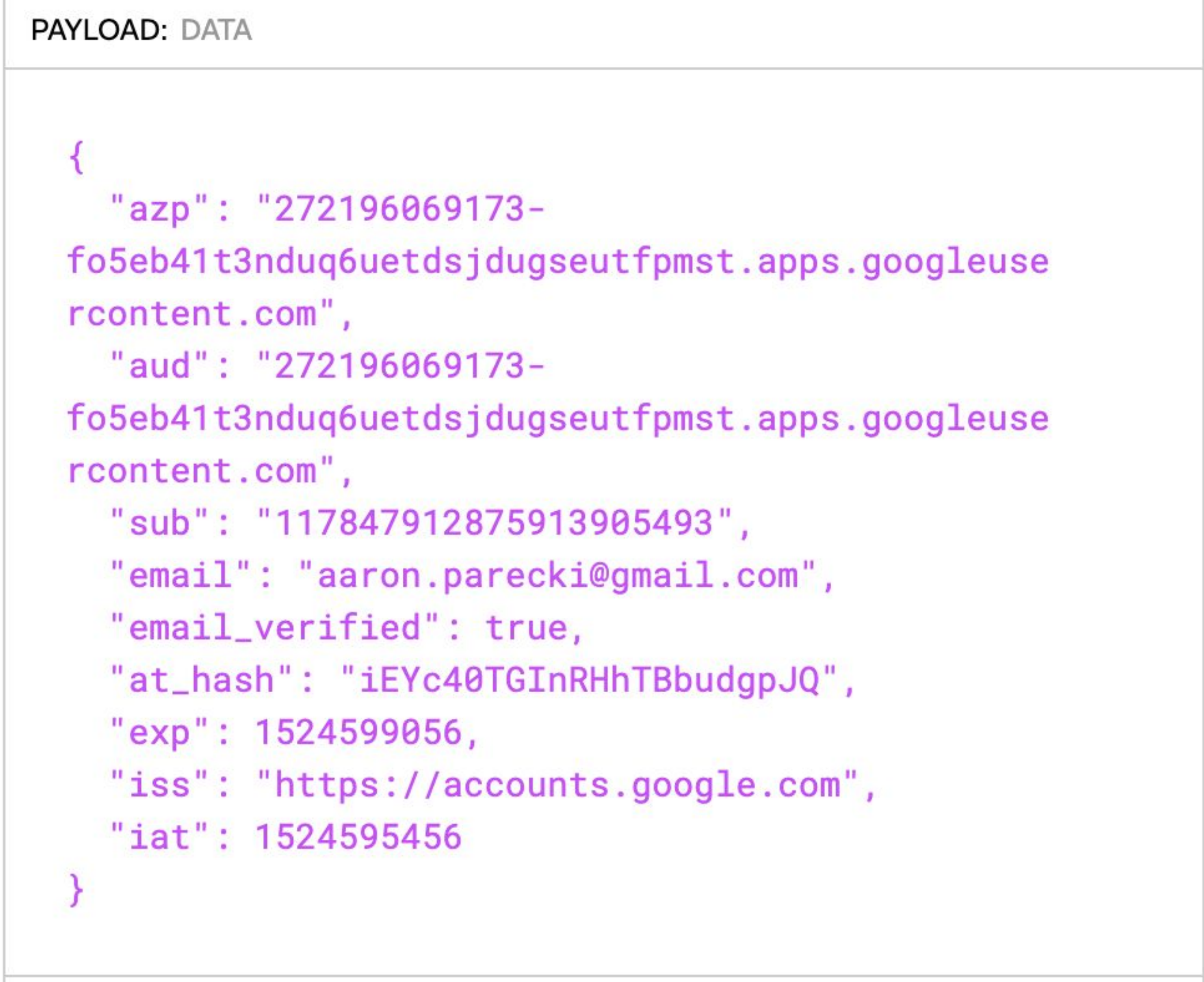
JWT

- Base64 Encoded
- 3 Parts, Separated by periods “.”
  - Header
  - Payload
  - Signature

```
eyJhbGciOiJSUzI1NiIsImtpZCI6ImFmZmM2Mjkw
N2E0NDYxODJhZGMxZmE0ZTgxZmRiYTYzMTBkY2U2
M2YifQ.eyJhenAiOiIyNzIxOTYwNjkxNzMtZm81Z
WI0MXQzbmR1cTZ1ZXRkc2pkdWdzZXV0ZnBtc3QuY
XBwcy5nb29nbGV1c2VyY29udGVudC5jb20iLCJhd
WQiOiIyNzIxOTYwNjkxNzMtZm81ZWI0MXQzbmR1c
TZ1ZXRkc2pkdWdzZXV0ZnBtc3QuYXBwcy5nb29nb
GV1c2VyY29udGVudC5jb20iLCJzdWIiOiIxMTc4N
Dc5MTI4NzU5MTM5MDU0OTMiLCJlbWFpbCI6ImFhc
m9uLnBhcmVja2lAZ21haWwuY29tIiwiZW1haWxfd
mVyaWZpZWQiOnRydWUsImF0X2hhc2giOiJpRVljN
DBUR0luUkhoVEJidWRncEpRIiwiZXhwIjoxNTI0N
Tk5MDU2LCJpc3MiOiJodHRwczovL2FjY291bnRzL
mdvb2dsZS5jb20iLCJpYXQiOjE1MjQ1OTU0NTZ9.
ho2czp_1JWsglJ9jN8gCgWfxDi2gY4X5-
QcT56RUGkgh5BJaaWdlrRhhN_eNuJyN3HRPhvVA_
KJVy1tMltTVd2OQ6VkxgBNfBsThG_zLPZriw7a1l
ANblarwxLZID4fXDYG-O8U-gw4xb-
NIsOzx6xsxRBdfKKniavuEg56Sd3eKYyqrMA0DWn
IagqLiKE6kpZkaGImIpLcIxJPF0-
yeJTMt_p1NoJF7uguHHLYr6752hqppnBpMjFL2YM
DVeg3jl1y5DeSKNPh6cZ8H2p4Xb2UIrJguGbQHVI
Jvtm_AspRjrmaTUQKrzXDRCfDROSUU-
h7XKIWRrEd2-W9UkV5oCg
```



```
{
  "alg": "RS256",
  "kid":
"affc62907a446182adc1fa4e81fdba6310dce63f"
}
```



```
{
  "azp": "272196069173-fo5eb41t3nduq6uetdsjdugseutfpmst.apps.googleusercontent.com",
  "aud": "272196069173-fo5eb41t3nduq6uetdsjdugseutfpmst.apps.googleusercontent.com",
  "sub": "117847912875913905493",
  "email": "aaron.parecki@gmail.com",
  "email_verified": true,
  "at_hash": "iEYc40TGInRHhTBbudgpJQ",
  "exp": 1524599056,
  "iss": "https://accounts.google.com",
  "iat": 1524595456
}
```

```
Î  IZ%'YCh ~Pq>zEA A%vZÑ   ^6r7q> U[LwcY1 _  2fej1– `cR8Å³H 1D
 _(jû         wwc*0
 Zr (N  Ä   'Li       qbhj/f
W9uË  HO }vPÉ  @uH&f QMD
5D'DR (Gv[$W
```

JWT

- Essentially Bearer Tokens, don’t lose them!
- Client sends along with authenticated requests
- Easy to self-generate

Self Generated JWT

```
eyJhbGciOiJIUzI1NiIsInR5cCI6Ik
pXVCJ9.eyJzdWIiOiIxMjM0NTY3ODk
wIiwibmFtZSI6IlNjb3R0IEtpcmtsY
W5kIiwiZW1haWwiOiJzcmtpcmtsYW5
kQHVjZGF2aXMuZWR1IiwiYWZmaWxpY
XRpb24iOiJTdGFmZiIsImF3ZXNvbWV
uZXNzIjoxMSwiaWF0IjoxNTE2MjM5M
DIyfQ.X5ReoSImK8rbQj4-FxgyV-
I6CXlnKMU1Gl2zDZdNCCE
```

```
{
  "sub": "1234567890",
  "name": "Scott Kirkland",
  "email": "srkirkland@ucdavis.edu",
  "affiliation": "Staff",
  "awesomeness": 11,
  "iat": 1516239022
}
```

Method GET

URL https://myapp.ucdavis.edu/admin/edit/1

Cookie Authorization:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwi
bmFtZSI6IlNjb3R0IEtpcmtsYW5kIiwiZW1haWwiOiJzcmtpcmtsYW5kQHVjZGF2a
XMuZWR1IiwiYWZmaWxpYXRpb24iOiJTdGFmZiIsImF3ZXNvbWVuZXNzIjoxMSwiaW
F0IjoxNTE2MjM5MDIyfQ.X5ReoSImK8rbQj4-FxgyV-I6CXlnKMU1Gl2zDZdNCCE

OIDC Flow (Demo)

OpenID®

Other Auth Providers

- SAML & OAuth/OIDC work with almost all authentication providers.
- Including Azure AD, ADFS, AWS SSO, Okta, Auth0, etc.

Shibboleth / SAML

- Web-based flow

OAuth / OIDC

- Web-based flow

Shibboleth / SAML

- Server Attribute Release

OAuth / OIDC

- Client Attribute Grant

Shibboleth / SAML

- XML Based Protocol

OAuth / OIDC

- JSON Based Protocol

Shibboleth / SAML

- Internal Cryptography

OAuth / OIDC

- Uses HTTPS/TLS

Shibboleth / SAML

- Web Server Install

OAuth / OIDC

- Mobile, Web, SPA, IoT flows

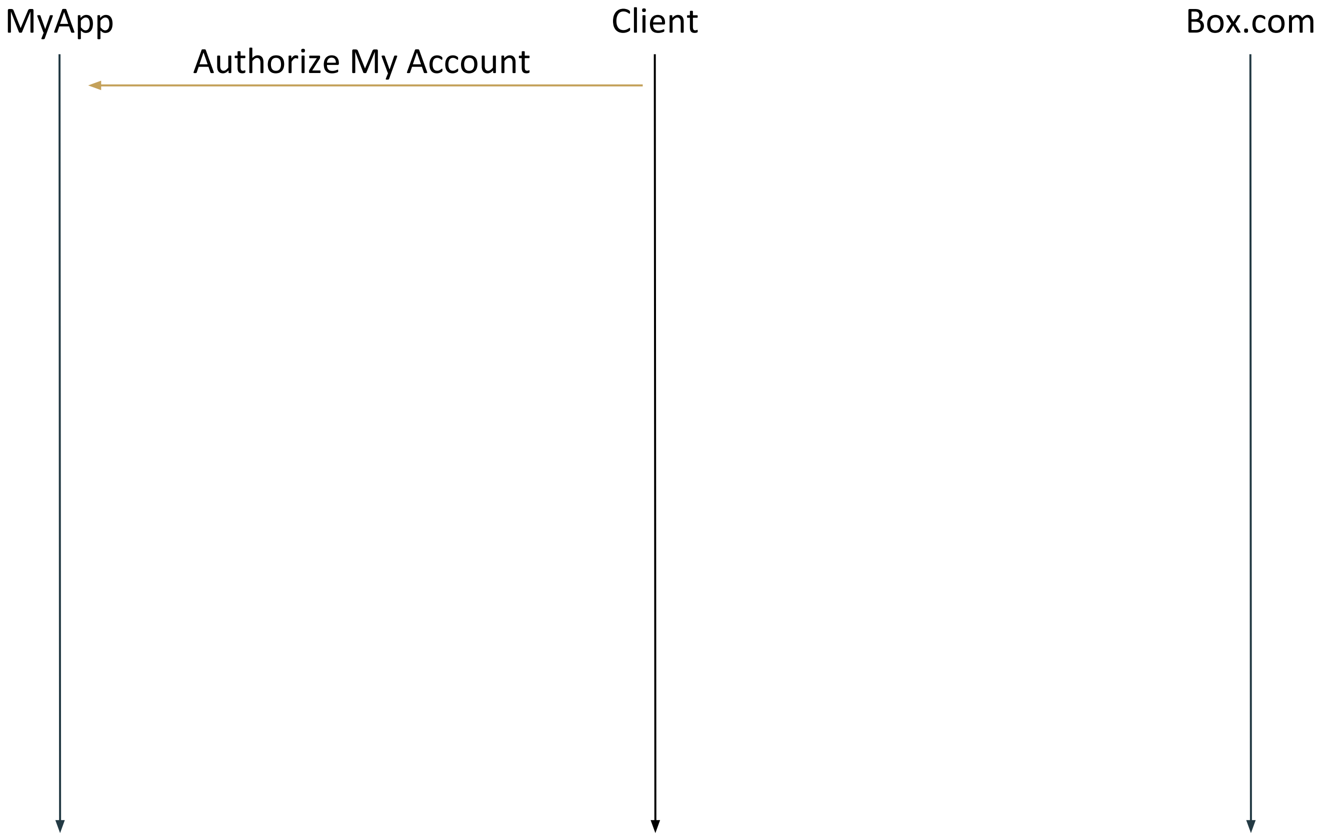
Thanks!

Scott Kirkland
UC DAVIS

Scott Kirkland
@srkirkland (UCTech)
github.com/srkirkland
srkirkland@ucdavis.edu

OAuth 2.0 Authorization Flow

Client: Authorize MyApp to use my Box Account



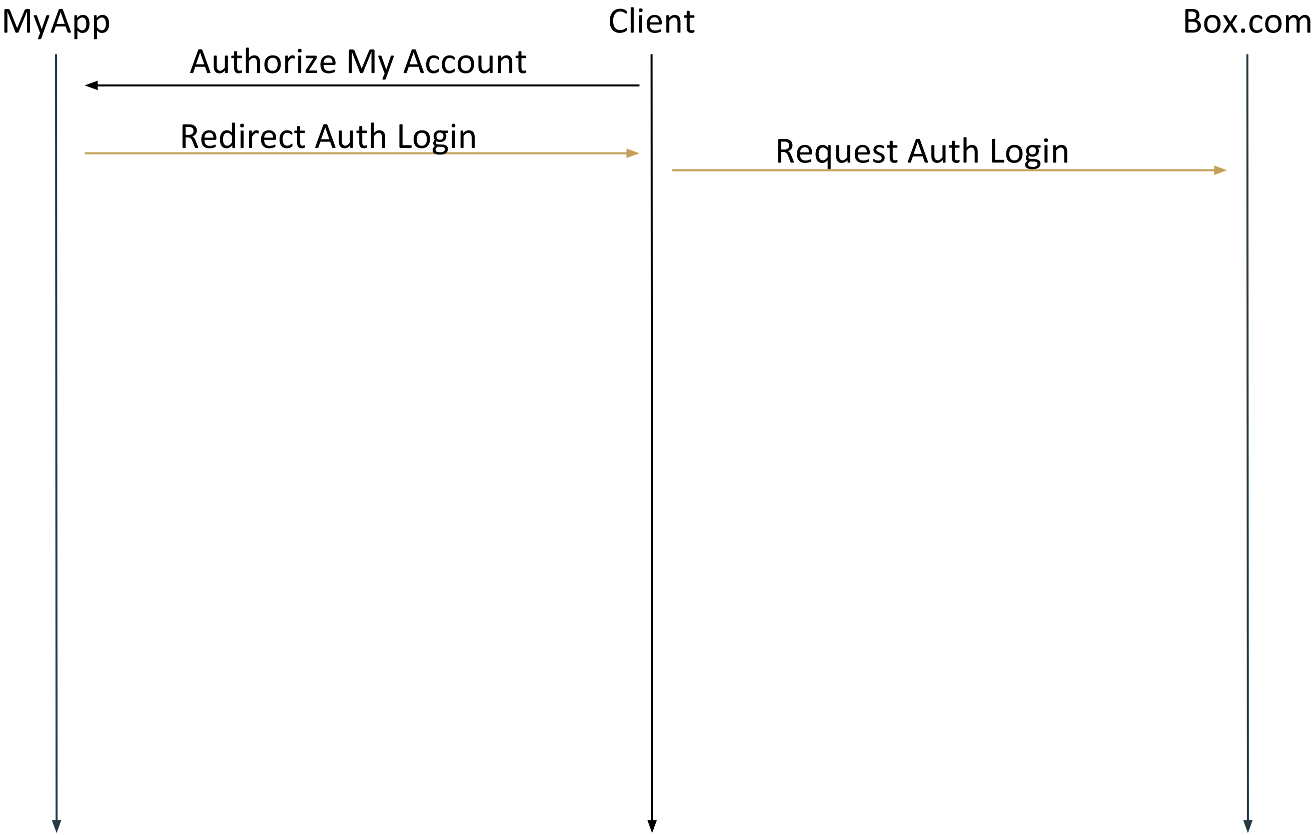
MyApp

Client

Box.com

Authorize My Account

Client: https://account.box.com/api/oauth2/authorize?{options}



MyApp

Client

Box.com

Authorize My Account

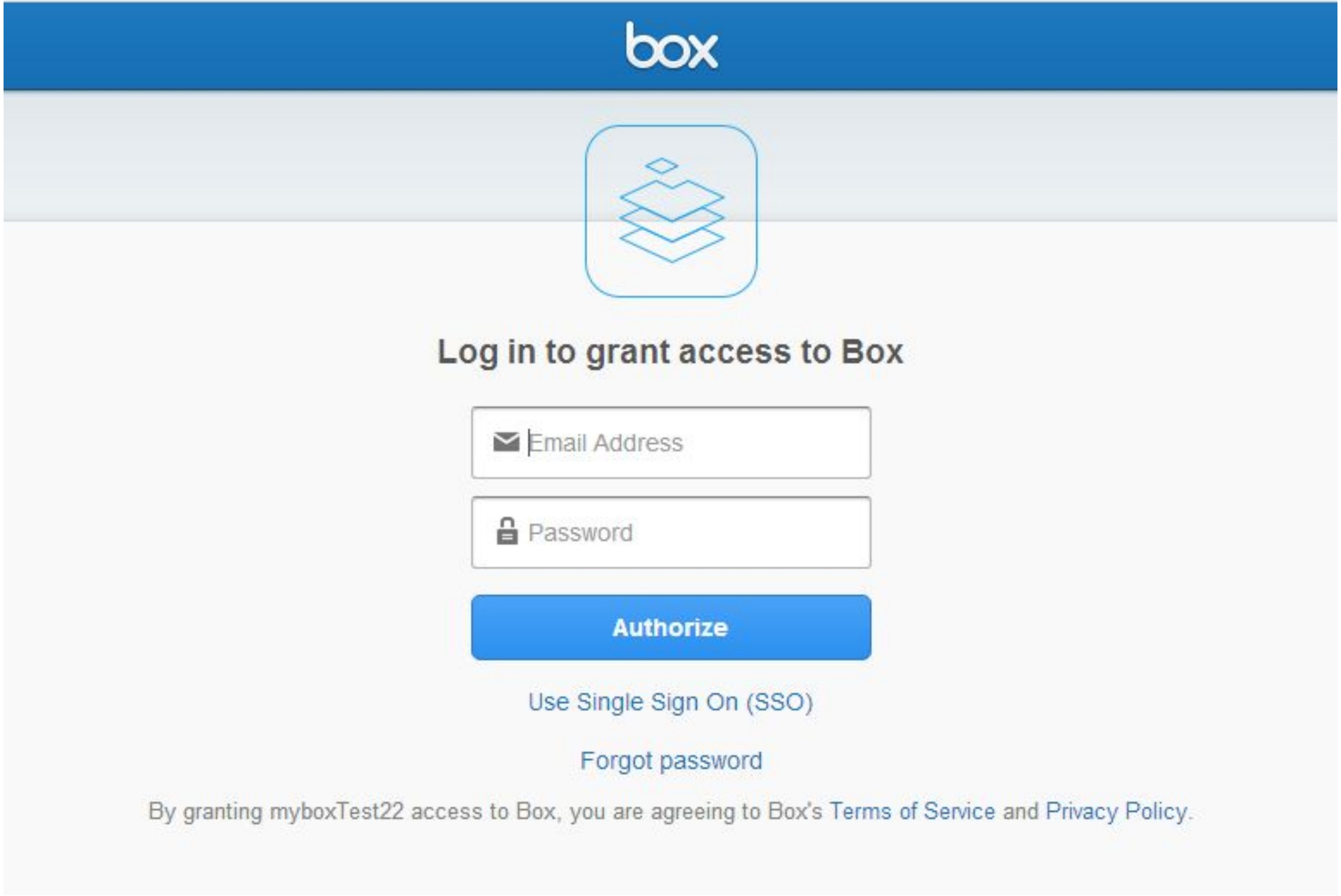
Redirect Auth Login

Request Auth Login

https://.../authorize?{options}

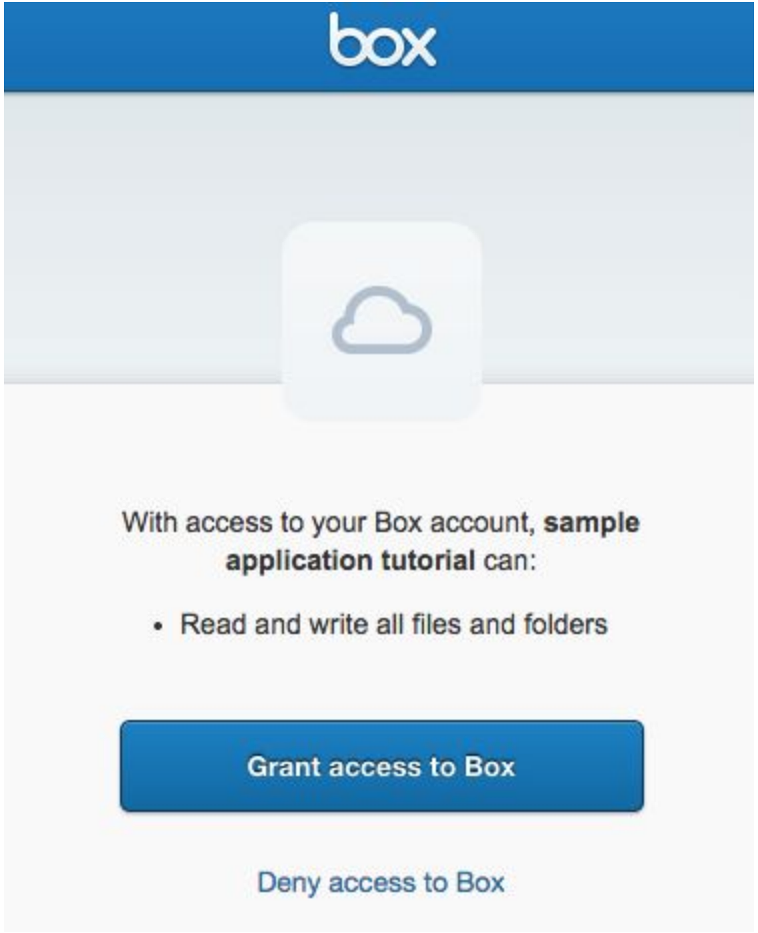
Options

- request_type
- client_id
- scope
- state
- request_uri (not required)



Log in to grant access to Box

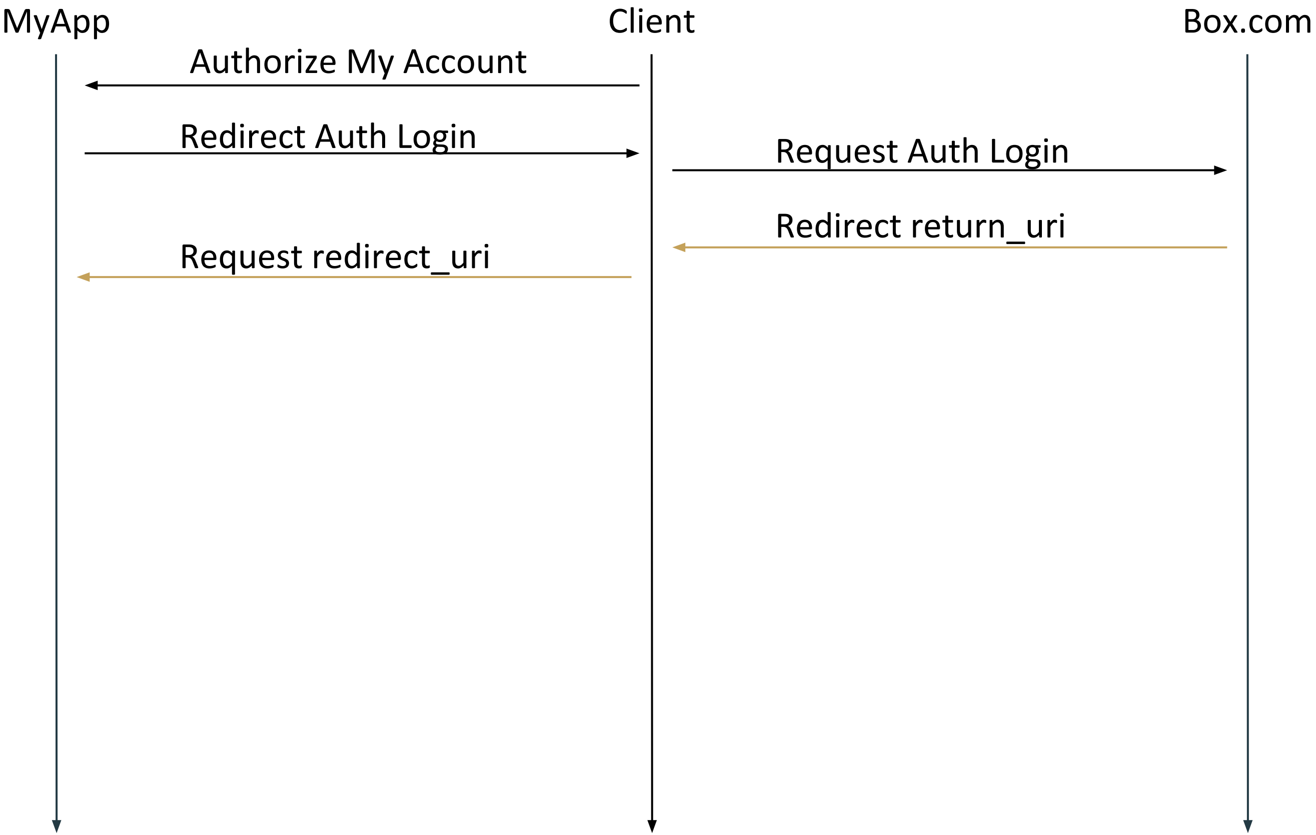
By granting myboxTest22 access to Box, you are agreeing to Box's Terms of Service and Privacy Policy.



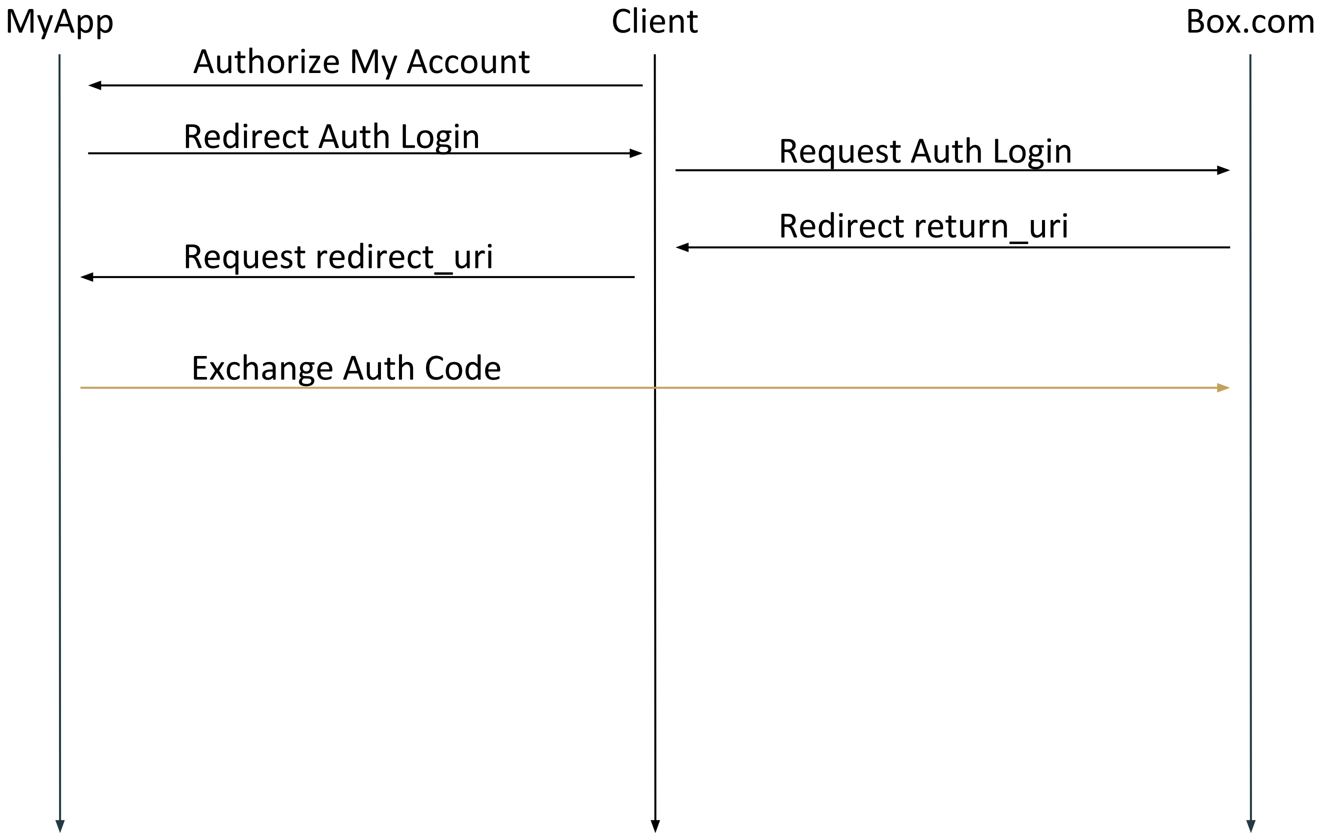
With access to your Box account, **sample application tutorial** can:

- Read and write all files and folders

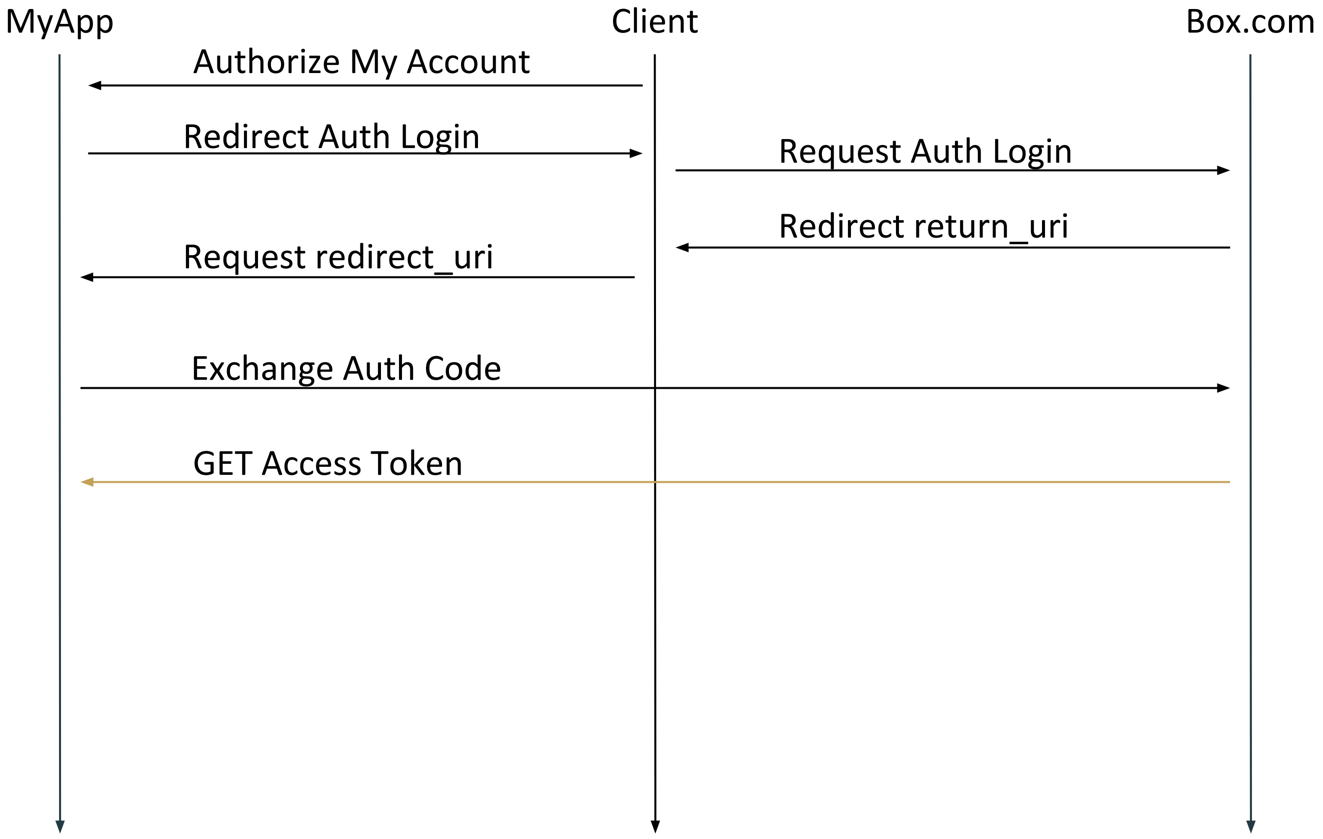
Client: https://myapp.ucdavis.edu/oauth?code=[auth_code]&state=[mystate]



MyApp: https://account.box.com/api/oauth2/token?code=[auth_code]&client_id=[cid]



MyApp: https://myapp.ucdavis.edu/oauth#access_token=[token]&state=[mystate]



Method	`GET`
URL	`https://api.box.com/2.0/folders/0/items`
Header	`Authorization: Bearer XueCAbegJQrp6fYp593jetd7ECnVCakj`

OAuth Review

- Only handles Authorization
- Access Token is bearer token
- Client “approved” scope release